# Faster Payments QIAT

Proposer: **nanoPay Corporation**

February 21, 2017

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Original Proposal</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revised Executive Summary (submitted after QIAT Q&amp;A period)</td>
<td>162</td>
</tr>
<tr>
<td>Q&amp;A Response</td>
<td>181</td>
</tr>
<tr>
<td>Draft QIAT Assessment</td>
<td>227</td>
</tr>
<tr>
<td>(Includes proposer comment in Appendix A &amp; B)</td>
<td>243</td>
</tr>
<tr>
<td>Task Force comments</td>
<td>251</td>
</tr>
<tr>
<td>Proposer response to Task Force comments</td>
<td>261</td>
</tr>
<tr>
<td>Final QIAT Assessment</td>
<td>262</td>
</tr>
</tbody>
</table>
Faster Payments Task Force Proposal

The MintChip Solution

April 30, 2016
Submitted by: nanoPay Corporation
Executive Summary .......................................................................................................................... 5
I. A Digital Cash Vision .................................................................................................................. 5
II. Digital Cash: A Better Alternative .................................................................................................. 5
III. What is MintChip? ......................................................................................................................... 7
IV. Bridging Gaps ............................................................................................................................... 7
   Continued end-user check writing: .............................................................................................. 7
   Challenges in converting businesses to electronic payments: ...................................................... 7
   Closed-payment communities: ..................................................................................................... 8
   Lack of contemporary features in traditional payment channels: ............................................... 8
   Faster payments: .......................................................................................................................... 8
   Obstacles in international payments: ............................................................................................ 8
   Mobile technology revolution: ..................................................................................................... 8
   Security concerns: ......................................................................................................................... 8
V. Technology Overview ................................................................................................................... 8
   The MintChip Ecosystem: ........................................................................................................... 8
   The MintChip ecosystem includes the following participants: .................................................... 10
VI. The MintChip Ecosystem is a Good Funds Model ....................................................................... 14
V. Loading Value into the MintChip Ecosystem ............................................................................. 15
VI. Removing Value from the MintChip Ecosystem ......................................................................... 15
VII. Security Overview of the MintChip Ecosystem ......................................................................... 16
VIII. Integration into Existing Financial Systems ............................................................................ 17
IX. Speed to Complete a Transaction ............................................................................................... 17
X. Transaction Cost ........................................................................................................................... 18
XI. Ease of access for new participants ............................................................................................ 19
XII. Ease of regulatory compliance .................................................................................................. 19
XII. Conclusion ................................................................................................................................. 20
USE CASE COVERAGE .................................................................................................................... 21
Supported Use Case Coverage Summary: ....................................................................................... 21
Cross-border Use Case Coverage: ................................................................. 22
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION ............... 23
Part A, Section 1: Solution Description .......................................................... 23
  MintChip Platform Overview: ............................................................... 23
  The MintChip ecosystem includes the following participants: ....................... 24
  MintChip Ecosystem is a Good Funds Model: ........................................... 28
  Loading Value into the MintChip Ecosystem: .......................................... 29
  Removing Value from the MintChip Ecosystem: ....................................... 30
  Security Overview of the MintChip Ecosystem: ....................................... 31
The 8 Stages of the end-to-end payment Process ........................................... 32
  1. Initiation: ......................................................................................... 32
  2. Authentication: ............................................................................... 37
  3. Payer Authorization: ......................................................................... 39
  4. Approval by the Payer’s Provider: ...................................................... 40
  5. Clearing: ......................................................................................... 40
  6. Receipt of the Payment ..................................................................... 41
  7. Settlement: ....................................................................................... 41
  8. Reconciliation: .................................................................................. 42
Part A, Section 2: Use Case Description: ......................................................... 43
  Business to Business (B2B): ................................................................. 43
  Business to Person (B2P): ..................................................................... 45
  Person to Business (P2B): ..................................................................... 46
  Person to Person (P2P): ........................................................................ 48
Part A, Section 3: Use Case by Effectiveness Criteria: ...................................... 49
Part B: BUSINESS CONSIDERATIONS: ......................................................... 52
  1. Implementation Timeline: ................................................................. 52
     MintChip Roadmap: ............................................................................. 53
     USD Deployment Timeline ................................................................. 56
  2. Value Proposition and Competition ..................................................... 57
Business to Business: ............................................................................................................ 59
Business to Person: ................................................................................................................ 68
Person to Business: .................................................................................................................. 78
Person to Person: ...................................................................................................................... 88
3. Integration Effort.................................................................................................................... 97
   Business to Business .............................................................................................................. 97
   Business to Person .................................................................................................................. 99
   Person to Business ................................................................................................................ 101
Part C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA ........................................... 106
   1. Ubiquity: .......................................................................................................................... 106
   2. Efficiency .......................................................................................................................... 117
   3. Safety and Security: ......................................................................................................... 124
   4. Speed (Fast): .................................................................................................................... 143
   5. Legal Framework .............................................................................................................. 146
   6. Governance: ................................................................................................................... 149
APPENDICES .......................................................................................................................... 150
   Appendix A: History of MintChip: ....................................................................................... 150
   Appendix B: European Definitions and Perspectives ............................................................ 152
   Electronic Money Issuing ....................................................................................................... 153
   Appendix C: Applicability of Regulation E .......................................................................... 154
   Appendix D: Financial Inclusion .......................................................................................... 158
   Appendix E: MintChip Payment Flow .................................................................................... 159
   Appendix F: Real time tax collection ................................................................................... 160
EXECUTIVE SUMMARY

I. A Digital Cash Vision

At nanoPay, we see a future where digital cash replaces banknotes and coins. Digital cash emulates all of the features and benefits of cash, while improving on its shortfalls. We also believe that digital cash can solve many of the issues facing existing payments systems without major changes current banking systems or the role of central banks. Most importantly, with widespread adoption of digital cash, we can both increase the velocity of money and broaden inclusion in the financial system without compromising that system’s integrity. Adoption of digital cash will mark the beginning of the obsolescence of “traditional” cash, in part because digital cash provides consumers and retailers with real-time payment certainty, irrevocability and a host of other enhancements that make it a superior choice to banknotes and coins.

More than changing the way we pay, we submit that digital cash is potentially a new component of money supply, which can stimulate economic growth by giving consumers, small- and medium-sized business and smaller banks and deposit-taking institutions a simple, cost-effective solution to their cash-flow problems.

Perhaps most exciting, digital cash, without the burden of high fees, has the potential to enable more people to participate in the formal economy by meeting the needs of the unbanked and underbanked. With almost eight per cent of households unbanked and a further twenty per cent underbanked, almost ninety-three million people in America are effectively disenfranchised from participating in the financial system in any meaningful way. This disenfranchisement has a profound effect on households, impacting anything from their ability to become homeowners, buy insurance, access credit, or avail themselves of low-cost financial services. A large population of unbanked and underbanked also lowers economic output because these populations cannot contribute to the economy is the same ways as those who are adequately banked. Digital cash can help address many of the reasons people are unbanked. With digital cash can create truly Frictionless® payments.

II. Digital Cash: A Better Alternative

Digital cash takes all of the advantages of cash and adds additional functionality that can only be achieved using a digital payments system:

---

1. Immediate settlement: Cash is settled the moment the cash is in the hands of the receiving party. Similarly, digital cash is settled at the moment it is received. Although cash is issued by the central bank, users in the cash ecosystem are not required to return the cash to the central bank for settlement or reconciliation. Digital cash enjoys this same advantage.

2. Non-repudiation and irrevocability – Once the receiving party has accepted the cash as legitimate, the transaction is irrevocable and complete. The transaction cannot be repudiated because it is considered final upon receipt of the cash. Digital cash enjoys these properties. There is no provision within the MintChip platform for chargeback or refund without the full agreement of both the sending and receiving parties. Like cash, in a digital cash ecosystem if goods are returned, a second payment must be made in the other direction to effectively reverse or unwind the transaction.

3. No physical constraints - Cash can only be used in person; it is nearly impossible to pay for goods and services online or remotely. Digital cash can easily support these use cases. Digital cash can be sent via email, text, or even by regular mail.

4. Better economic analysis – Since cash transactions are not necessarily reliably reported, it is difficult to tax these transactions or identify their economic impact. Central banks cannot know with accuracy where the cash is - or even if it is within their own borders. Digital cash illuminates these otherwise dark pools of cash and cash transactions. All transactions can be identified, the impact on the economy is transparent and appropriate taxes can be assessed.

5. More secure – Digital cash is secure at all times. It cannot be stolen, lost or intercepted by an unintended recipient.

6. Less expensive – Using cash is not without cost-less. It requires both physical and electronic security. Security is required in merchant stores, tills and to physically move the cash from place to place. It is also vulnerable to employee theft. Digital cash has a marginal transaction cost of close to zero, which in turn saves transactions costs for banks, consumers and merchants.

7. Origin of funds – It is nearly impossible to establish the flow of money from person to person with traditional cash because previous holders cannot be identified. With digital cash, these flows can be easily tracked.

8. Privacy: Traditional cash transactions are private (not to be conflated with anonymous - the receiving party can usually see you.) There is no record of the actual transaction itself; instead, a receipt is a proxy for cash transaction. Digital cash has all of the same privacy, but every transaction is logged and allows regulators and law enforcement (with
the appropriate authority) to manage the economy, protect consumers and prevent / investigate crimes.

III. What is MintChip?

MintChip is nanopay’s version of digital cash. It was originally created by the Royal Canadian Mint (RCM), which is a Federal Crown Corporation that is accountable to the Canadian Minister of Finance. Canada has withdrawn pennies from circulation and there are ongoing discussions about withdrawing the one-hundred-dollar banknote. With the coins and notes in circulation under threat of withdrawal, the RCM undertook to build a digital cash platform that would effectively cannibalize their own mandate to make coins - which it does exclusively for Canada and for over sixty-two other countries. The RCM hired Dr. David Everett, a world authority on payment systems and digital cash to create the MintChip platform. Everett’s mandate was to create a digital cash platform that was secure, scalable and regulator-friendly. In building a digital version of traditional cash, Everett consulted with law enforcement, regulators and the Bank of Canada. Meeting all of the regulator and central bank requirements was a necessary condition for the RCM to succeed with MintChip, but not a sufficient one. While MintChip was regulator-friendly, the RCM’s mandate did not permit the Mint to support a digital cash platform. An amendment to the RCM’s legislative mandate was therefore required, however the Federal Government declined to make the required changes. This refusal marked the beginning of a long sales process, which culminated in nanopay’s acquisition of the MintChip assets in December 2015. NanoPay launched MintChip in Canada in April 2016 and MintChip 2.0 is expected to be deployed in Summer 2016.

IV. Bridging Gaps

According to the Federal Reserve’s 2013 Consultation Paper, there is widespread agreement on current gaps in the payments system. We submit that the MintChip platform addresses, in one way or another, all of these gaps as well as others that were not identified and that will be discussed throughout this proposal.

**Continued end-user check writing:**

The MintChip platform provides a viable, low-cost alternative to checks and would reduce end-user check writing for a variety of reasons.

First, checks are often written today for individuals to easily pay other people (e.g. babysitters, family members and sole-proprietor businesses). The MintChip ecosystem supports these P2P transactions and allows for value to be received immediately, without having to account for the time it takes funds to clear or the possibility of counterfeit or fraudulent checks. For the Payer, they can be certain that funds have been debited from their account immediately, which helps with budgeting and avoiding NSF fees. As well, because the ecosystem can easily set up pre-authorized payments, scenarios where post-dated checks are required can also be accommodated.

**Challenges in converting businesses to electronic payments:**
The MintChip platform can be thought of as a platform that is layered on top of existing payments infrastructure. Because of this layering, businesses can easily connect to the platform with minimal changes to their existing billing and accounting systems. Because the MintChip ecosystem is capable of supporting the transmission of data (such as remittance information) along with value, end-to-end straight-through processing (including reconciliation and posting of payments) is possible for businesses of virtually any size.

Closed-payment communities:
While it is true that the MintChip ecosystem is a type of closed-payment community, as will be demonstrated below, the barriers to entry are so low that virtually any Entity can participate for low to no cost.

Lack of contemporary features in traditional payment channels:
The MintChip platform uses some of the most innovative contemporary payments features, such as near-real-time notification and settlement. Moreover, the scalability of the platform means that new innovations can be easily incorporated into the MintChip infrastructure without having to make costly upgrades to Participants’ legacy systems.

Faster payments:
As will be demonstrated below, the primary benefit of the MintChip platform is its ability to send payments virtually instantaneously, clearing and settling them in real time.

Obstacles in international payments:
The MintChip platform has been built with cross-border and multi-currency payments in mind. These payments will clear and settle within the ecosystem as quickly as domestic, single-currency payments.

Mobile technology revolution:
The MintChip platform is designed to be mobile-first, leveraging the worldwide ubiquity of smartphones and is primarily accessed via mobile device.

Security concerns:
The MintChip ecosystem is highly secure and leverages state-of-the-art cryptography. Indeed, the security of the platform is explored in great detail below.

V. Technology Overview

The MintChip Ecosystem:
The MintChip digital cash ecosystem was designed as an electronic payments platform to achieve the following objectives:

- Speed;
- Security;
• Efficiency;
• International Capabilities; and
• Collaboration Opportunities.

**Speed**

MintChip transactions are Peer-to-Peer transactions that do not require an intermediary and can clear and settle in near Real-Time.

**Security**

Regardless of transaction value, all MintChip transactions are completed in highly-secure Hardware Security Modules (HSMs), the same hardware used in today’s global payments systems. Value Transfer Messages (VTMs) are encrypted and signed using an approach backed by four patents. The cryptographic algorithms in MintChip can be dynamically upgraded across the entire ecosystem as future security threats are identified. International Capabilities

The MintChip ecosystem only allows for one Originator per fiat currency. Foreign exchange services and inter-country transactions are made possible by leveraging providers who act as Brokers in more than one country or fiat currency.

**Collaboration Opportunities**

The MintChip platform was designed as a global solution to create digital cash ecosystems built on a collection of robust, easy-to-use and open APIs to enable broad array of participants to create digital cash solutions.

MintChip platform leverages an asset transfer model to move value in Real-Time without an intermediary. Contrary to conventional payment systems where value is held by intermediaries, MintChip platform is a good funds peer-to-peer payment system that transfers value quickly and securely from one party to another.

This simple asset transfer model is more efficient than conventional payment systems and has clear benefits:

• Supports both Push/Pull transactions;
• The value transfer is instant and irrevocable;
• The model requires no intermediaries;
• Operates in both online and offline environments; and
• Immediate, irrevocable payment authorization.
The MintChip ecosystem includes the following participants:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>Manages: (1) operation of the stand-alone MintChip system component that creates MintChip value and Secure Asset Stores; (2) administration of the security parameters in the MintChip Ecosystem; and (3) pooled account that holds fiat currency for MintChip value sold to the Brokers</td>
</tr>
<tr>
<td>Technology Provider</td>
<td>The Owner of the MintChip platform that: (1) provides the system components for deployment by the Platform Operator and the Originator; (2) integration support for Brokers and Merchants; and (3) software enhancements, maintenance and support.</td>
</tr>
<tr>
<td>Platform Operator</td>
<td>Responsible for: (1) deployment and operation of the MintChip platform; and (2) administration of the operating rules, standards and protocols</td>
</tr>
<tr>
<td>Broker</td>
<td>A Provider (depository institution, regulated non-bank account provider) that: (1) buys and sells MintChip value from/to Originator; (2) enrolls End Users; (3) provides mechanisms for End Users to buy and sell MintChip value; and (4) provides currency conversion services (optional).</td>
</tr>
<tr>
<td>End User</td>
<td>An Entity that uses a payment service for the purpose of sending or receiving payments, such as a business, a Consumer, a government agency.</td>
</tr>
</tbody>
</table>
MintChip Ecosystem
(Diagram #1)

**Originator:**

The ecosystem has been built so that when the platform achieves a certain scale within a country, the Central Bank, or a branch/division of the Central Bank will act as the Originator within that ecosystem. It is the Originator’s role to create (or “mint”) MintChip value in the designated fiat currency. The system is built to support a single Originator for each currency created in the MintChip ecosystem. As part of the initial implementation, the Platform Operator may act as the Originator, however it is anticipated that a country’s Central Bank (or Federal Reserve) will eventually assume the Originator role.

**Broker:**

The ability to become a MintChip Broker is made available to new and existing providers in the current payment systems through open APIs. A Broker will use these APIs to provide End Users access the MintChip platform through their existing mobile applications or online services. It is anticipated the first Brokers in the MintChip ecosystem will be depository institutions, regulated non-bank account providers and large retailers. Lowering the barriers to entry through our open platform will encourage new participants who can focus on providing value-added services.

The Broker opens a MintChip account with the Originator and establishes one or more Secure Asset Stores (SAS) on the MintChip platform. The Broker pre-purchases MintChip value from the Originator to meet the needs of their End Users. This is done by the Broker transferring the
fiat currency to the Originator’s pooled account and the Originator loading the equivalent MintChip value into the Broker’s SAS.

The Broker’s role is then to sell or redeem MintChip value to and from (as the case may be) End Users who purchase MintChip value with fiat currency. The Broker is also the participant that establishes MintChip accounts for End Users. As the Brokers will be current Providers in the existing traditional financial and payments systems, they will be in a position to complete Know Your Customer (KYC) requirements and comply with applicable Anti-Money Laundering (AML) requirements at the time of End User registration. Through their existing billing systems, Brokers may charge the End User fees for participating in the ecosystem.

**End User**

End Users can be individual consumers, businesses, or government agencies. End Users open MintChip accounts with Brokers and are assigned Secure Asset Stores (SASs) to hold value in a specified currency. For this reason, End Users may have more than one SAS in the same or multiple currencies. For example, one SAS may contain USD and another may contain CAD. All transactions completed in the MintChip ecosystem are a transfer of value between two different SASs. Value Transfer Messages (VTMs) facilitate the exchange and represent the monetary value in transit. The VTM can only be consumed by the Receiver’s (Payee) SAS and is cryptographically encrypted and signed to prevent tampering. MintChip SASs are only able to exchange value with a SAS that shares the same currency.

**Secure Asset Store (SAS):**

The MintChip ecosystem also distinguishes itself from any other payment system by its use of a Secure Asset Store (SAS). A SAS can be thought of as a digital safe deposit box that contains:

1. A unique SAS identification number;
2. Identity information of the Entity associated to the SAS;
3. A ledger that tracks every transaction that occurs within the SAS; and

**Value Transfer Message (VTM):**

The MintChip technology is elegant in its simplicity and begins with a concept that is dramatically different from the concepts driving today’s payments systems. If you reduce payment transactions to packets of data and ensure that those packets are incredibly secure, then the manner in which those packets move from user to user can be flexible, low-risk, highly-adaptable and very efficient. The nature of today’s payment systems, built on legacy systems and in piecemeal fashion, means that system operators and participants must focus on ensuring end-to-end system security for each payment, which is costly, time-consuming, and ultimately means the particular network is only as secure as its weakest link.
The VTM is patented technology that is a highly-secure and small (52 bytes). The VTM contains four critical pieces of data required to complete a transaction:

- the Payer ID;
- the amount;
- the currency; and
- the Payee ID.

Every transaction must contain this information before a VTM can be created. Once created, the Message is encrypted and digitally signed in the HSM, which ensures the highest level of security. The patented technology within the VTM ensures that even if the VTM is captured during transmission and someone succeeds in breaking its encryption, the only information that is revealed is the intended Payee’s location. There are also multiple additional security features that both prevent the occurrence of a security breach, and identify breaches if they occur.

Value Transfer Message
(Diagram #2)
VI. The MintChip Ecosystem is a Good Funds Model

MintChip value in a MintChip account SAS represents Good Funds as it is backed by the fiat currency in the Originator’s pooled account.

MintChip Platform Overview
(Diagram #3)

Value is transferred into a SAS by converting USD funds into a digital representation of the currency through a MintChip Broker - creating MintChip value. As part of the conversion, the USD funds are deposited into the Originator’s pooled account, ensuring all MintChip value is backed by USD funds. This structure ensures that MintChip value is pegged to, and at par with traditional USD. This requirement also means that any transactions occurring on the MintChip platform follows a good funds model and virtually eliminates the risk of transacting within the platform. This model also reduces participant costs and system requirements that are required to verify payments in today’s payment ecosystems.
V. Loading Value into the MintChip Ecosystem

The conversion of funds from fiat currency outside the MintChip ecosystem to MintChip digital currency within the ecosystem can only be completed through a MintChip Broker. The Broker accesses the MintChip ecosystem using the open APIs and will embed the features and functionality of the platform within their own applications. The User will access the MintChip platform through the Broker’s application. The End User selects the “Load Value” option from the application and they will be presented with a list of the available funding sources that they have previously registered into their account when they established their MintChip account. Diagram # X outlines the potential funding sources the End User can use to load fiat currency into their SAS. It is important to note that a large portion of Brokers are anticipated to be existing financial institutions allowing users the capability to easily transfer funds between the End User’s accounts. (e.g. savings accounts, checking accounts, credit/debit card or line of credit).

Once the funding source is selected, the End User can select the amount they wish to load into their MintChip account and associated SAS. In most instances the funding source will be a deposit account held by the Broker (e.g. the End User’s retail bank). The Broker receives the funds from the MintChip End User and then delivers the MintChip value directly into the End User’s SAS.

Because these systems leverage existing methods for authenticating both End Users and the value they are attempting to load into the ecosystem, this onboarding process ensures the funds used to credit the individual SAS tied to the MintChip account are good funds.

VI. Removing Value from the MintChip Ecosystem

The conversion of digital currency from an End User’s MintChip account can only be completed through the User’s Broker. In a manner similar to loading value into the ecosystem, the End User accesses the MintChip platform from within the Broker’s application. The End User then selects “Value Unload” from the options menu. This option may either be presented within a consumer application or a business- specific application (for example, in the case of a merchant). The End User will enter the value of MintChip digital currency they wish to unload, and will be prompted to select one of the previously-registered accounts into which the funds will be deposited (e.g. a deposit account held at their financial institution). The Broker then initiates transfer of the MintChip value from End User’s SAS to the Broker’s SAS and deposits the equivalent amount in fiat currency into the End User’s selected account.
Ways to Load and Remove Value into a MintChip Account
(Diagram #4)

VII. Security Overview of the MintChip Ecosystem

The MintChip solution at its core is:
1. A distributed system of Secure Asset Stores (SASs); and
2. A messaging protocol that enables the trusted exchange of value between these Stores (Value Transfer Messages).

Central to the MintChip ecosystem, and the root of all trust in platform is the “Security Series”. This is a secured certificate that provides a shared signing authority, which enables trust in message authenticity and integrity.

The key differentiator between the MintChip platform and other digital cash systems is the patented technology that protects the transfer of assets (value) between two End Users (B2B, B2P, P2B, P2P). Regardless of value, all MintChip transactions are completed in highly-secure HSMs, the same hardware used in today’s global payments systems. VTMs are encrypted and signed using an approach backed by four patents. By securing VTMs, the MintChip ecosystem
is able to operate in a manner that allows for the completion of transactions offline, which is a unique feature in digital cash technology.

The MintChip platform has been built to ensure that the benefit of breaching its security is outweighed by the cost, effort, and resources necessary to do so. Because hacking the system is so costly and the potential return of it so low, hackers will look to other ecosystems, where return for their efforts could be much greater.

The VTM technology and the patented cryptography that protects the VTM can be quickly upgraded at any time, with no system downtime and at a very low cost. As technologies like quantum computing become available to potential hackers, post-quantum cryptography can be used to increase encryption surrounding the VTM, ensuring it remains secure against new hacking techniques.

The MintChip platform is ultimately user- and use-case-agnostic; designed to apply the same patented high security to each transaction regardless of its value. The technology supports transactions as small as 1/100 of a cent and as large as hundreds of millions of dollars. Moreover, the transaction that are completed are small in size (52 bytes) enabling the ability to store every transaction, separately in the SAS of both parties to the transaction. This rich supply of data means that compliance with virtually any regulatory regime is possible - which in turn enables the potential for global deployment of the platform.

VIII. Integration into Existing Financial Systems

The MintChip ecosystem enables End Users to exchange value quickly and securely. The system provides easy integration into international financial systems in the form of open connections points (on-ramps and off-ramps) that enable End Users to move money into and out of the MintChip digital cash system. These integration points are leveraged by End Users and provided by Brokers to facilitate payments and foreign exchange. The MintChip Application Programming Interface (API) leverages ISO 20022 message standards to simplify integration and process financial transactions.

IX. Speed to Complete a Transaction

Today, the speed of technology enables the transfer of information between two parties in near real time. Transactions within the MintChip platform are also performed at that same high speed. The platform is also a good funds model, which means the traditional processes of Payer Authorization, Approval by the Payer’s Provider, Clearing, Settlement and Reconciliation are handled very differently. The actual Clearing and Settlement between the parties of a transaction on today’s payment systems takes substantial time and parties can incur significant risk. On the MintChip ecosystem, Clearing and Settlement between parties is effectively completed with each transaction in real time and with finality. If there are funds within a Participant SAS they can initiate a transaction up to the value of their balance. As soon as the Payer initiates the transaction, that value is instantly removed from the Payer’s account balance and the Payer has no recourse or opportunity for repudiation. Effectively the payment is cleared, and immediately
upon the Payee receiving the funds the transaction is settled, and a digital receipt is issued. This process for completing a transaction is the same regardless of the user (Person, Business, or Government) or the use case. This makes the platform extremely flexible and cost-effective, as further detailed below.

X. Transaction Cost

The design of the current payment ecosystem is such that current participants can incur high costs associated with completing transactions. These costs exist primarily because of four factors:

1. Fraudulent transactions;
2. Requirement to secure the end-to-end ecosystem;
3. Number of participants in the ecosystem; and
4. Cost to scale.

While other factors add to the transaction cost, these are the primary drivers. The MintChip ecosystem addresses these issues in a very sophisticated, yet simple manner.

First, every transaction is completed in exactly the same manner. The design of the MintChip ecosystem is such that a Broker can easily connect to the MintChip platform through open API’s. Once connected, Brokers are simply gateways to the ecosystems, with a much more passive role when compared to today’s that has Brokers acting as active participants in transactions. This participation brings with it security costs incurred to reduce the risk of fraudulent transactions. By reducing the Broker’s role in transaction completion, it reduces transaction cost while increasing the overall security of the ecosystem.

Second, the MintChip ecosystem is focused on securing the VTM rather than securing the end-to-end communication channels through which the VTM travels. Recall that the VTM is the unique technology that enables secure transactions to occur. The ability to seamlessly and inexpensively upgrade cryptography at any time ensures the platform will remain secure, regardless of how quickly new technology evolves or the channel through which the VTM travels.

Third, the throughput capacity and scalability of the MintChip platform takes the real cost to complete a marginal transaction close to $0.00. The platform has been designed to cost-effectively scale as quickly as required. The current platform has the capability to complete thousands of simultaneous transaction per second. To scale the MintChip platform to a capacity of approximately 50,000 transactions per second would cost less than one million dollars and take less than 30 days.
XI. Ease of access for new participants

There are many barriers to entry for new entrants to participate in current payments systems, with cost and the regulatory compliance at the top of the list. Historically, payment-system participants have preferred to keep participation exclusive and restrictive. This strategy has effectively slowed the evolution of payments platform and kept transaction costs high.

The MintChip platform takes the opposite approach and has been built to encourage participants to access the system through open APIs. This openness enables existing participants the ability to migrate to a new platform and more importantly, allows new participants to enter the ecosystem. As previously described, the cost to complete a transaction on the MintChip platform approaches zero and by allowing access to many participants (both new and existing), market forces will drive the per-transaction cost for End Users as low as possible.

XII. Ease of regulatory compliance

Regulatory compliance is growing increasingly complex and burdensome for payments system participants. Strong regulatory frameworks are essential to reduce fraud and counteract money laundering and terrorist-financing efforts. Legacy payment systems can often struggle to keep up with a rapidly-changing regulatory landscape.

The MintChip platform was designed to address many of the regulatory compliance issues participants will face across the globe. At the foundation of regulatory compliance is the need to: authenticate the parties to a transaction; identify the value of the transaction; and record and store every transaction along with important data about the transaction. At the same time, a modern payment system must also protect End User privacy.

The MintChip platform design ensures that End Users establishing a MintChip account are identified and authenticated before establishing a SAS. The level of authentication can be increased based on the nature and value of the transactions the End User wishes to complete. This graduated authentication protocol ensures that all AML and KYC requirements can be achieved on the platform. Given that the funds in the MintChip ecosystem must be loaded through a Broker, End User authentication data can be validated with that Broker as well as through other sources.

Each MintChip account and associated SAS on the MintChip platform is linked to an authenticated End User and every transaction that occurs involving that specific SAS is stored within a ledger that sits within the specific SAS. This ledger can be accessed by regulatory enforcement agencies by following existing legal processes and procedures for access, which ensures the rights to privacy of the individual are protected.
Because the MintChip platform supports this level of regulatory compliance, the compliance burden is lessened for ecosystem participants.

**XII. Conclusion**

nanoPay is confident that the MintChip platform meets all of the Task Force’s desired outcomes of *speed*, *security*, *efficiency* and *international capability*. As evidenced in this Proposal, the platform can also be assessed as “Very Effective” against the majority of the outlined Effectiveness Criteria.

We look forward to taking a collaborative approach in working with a broad array of participants to make material progress in implementing our MintChip solution to support the improvement of the U.S. payment system.
## USE CASE COVERAGE

**Supported Use Case Coverage Summary:**

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>(B2B)</td>
<td>Y</td>
<td>Y</td>
<td>Any End User (Business, Consumer, Government) can create a MintChip account and Secure Asset Store (SAS). The MintChip ecosystem can transfer value between any two SASs. The MintChip platform can complete any transaction between any two parties, for any value, in any currency, in real-time.</td>
<td>The MintChip ecosystem can complete transactions as small as 1/100th of a cent, up to hundreds of millions of dollars.</td>
</tr>
<tr>
<td>(B2P)</td>
<td>Y</td>
<td>Y</td>
<td>The MintChip platform can complete any transaction between any two parties, for any value, in any participating currency, in real-time. Information can also be included with the payment.</td>
<td>Payments can be one-to-one or one-to-many and can be automated or <em>ad hoc</em>.</td>
</tr>
<tr>
<td>(P2B)</td>
<td>Y</td>
<td>Y</td>
<td>The MintChip platform can complete any transaction between any two parties, for any value, in any currency, in real-time. Remittance information can also be included along with the payment message to facilitate posting and Reconciliation of payments.</td>
<td>Payments can be made online or in-store. MintChip payment acceptance can be easily built into Merchant POS payment terminals or into the POS system.</td>
</tr>
<tr>
<td>(P2P)</td>
<td>Y</td>
<td>Y</td>
<td>The MintChip platform can complete any transaction between any two parties, for any value, in any currency, in real-time.</td>
<td>Person-to-person payments can be made domestically or cross-border.</td>
</tr>
</tbody>
</table>
## Cross-border Use Case Coverage:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business to Business (B2B)</strong></td>
<td>The MintChip ecosystem can be configured to support foreign exchange transactions and cross-border payments. The scalability and flexibility of the platform also mean that disclosure obligations that may differ between jurisdictions can also be accommodated as new participants are added.</td>
<td>Any user (Business, Consumer, Government) is capable of establishing a MintChip account or Secure Asset Store(SAS). The MintChip ecosystem is effectively user agnostic as all End User value is stored in an SAS. MintChip can transfer value between any two SAS regardless of user, currency, or value. Currently, nanoPay is in discussions with parties in Canada, the United States, England, and Brazil about deploying the MintChip ecosystem.</td>
</tr>
<tr>
<td><strong>Business to Person (B2P)</strong></td>
<td>The MintChip platform is capable of completing transactions between any user, in any currency, offered on the platform.</td>
<td>The MintChip ecosystem is effectively agnostic to the user as all End User value is stored in an SAS. MintChip can transfer value between any two SAS regardless of user, currency, or value.</td>
</tr>
<tr>
<td><strong>Person to Business (P2B)</strong></td>
<td>The MintChip platform is capable of completing transactions between any user, in any currency, offered on the platform.</td>
<td>The MintChip ecosystem effectively user agnostic as all SAS are similar on the platform. MintChip can transfer value between any two SAS regardless of user, currency, or value.</td>
</tr>
<tr>
<td><strong>Person to Person (P2P)</strong></td>
<td>The MintChip platform is capable of completing transactions between any user, in any currency, that uses the MintChip platform. Cross-border P2P transactions can be completely for a fraction of the cost of traditional methods and for the end-user, funds are guaranteed almost immediately.</td>
<td>The MintChip ecosystem effectively user agnostic as all SAS are similar on the platform. MintChip can transfer value between any two SAS regardless of user, currency, or value.</td>
</tr>
</tbody>
</table>
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

Part A, Section 1: Solution Description

*MintChip Platform Overview:*

The MintChip platform leverages an asset transfer model to move value in Real-Time without an intermediary. Contrary to conventional payment systems where value is held by intermediaries, the MintChip platform is a Good Funds peer-to-peer payment system that transfers value quickly and securely from one party to another. This simple asset transfer model is more efficient than conventional payment systems and has clear benefits:

- Supports both Push/Pull transaction models
- Value transfer is instant and irrevocable
- Requires no intermediaries
- Eliminates disputes and chargebacks
- Operates both online and offline
- Immediate irrevocable payment authorization

*MintChip Transaction Flows*

(Diagram #5)

- Originates — Creates & issues digital currency
- Creates security token
- Creates Secure Asset Stores (incl. parameters)
- Brokers — exchanges real US$ for MintChip US$
- Also could exchange MintChip US$ for US$ (not frequent)
- Currency brokers — exchange MintChip US$ for MintChip £
- End-Users exchange value in MintChip

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
The MintChip ecosystem includes the following participants:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>Manages:</td>
</tr>
<tr>
<td></td>
<td>1. Operation of the stand-alone MintChip system component that creates MintChip value, and Secure Asset Stores</td>
</tr>
<tr>
<td></td>
<td>2. Administration of the security parameters in MintChip Ecosystem</td>
</tr>
<tr>
<td></td>
<td>3. Pooled account that holds fiat currency of MintChip value sold to Brokers</td>
</tr>
<tr>
<td>Technology Provider</td>
<td>The Owner of the MintChip platform:</td>
</tr>
<tr>
<td></td>
<td>1. Provides the system components for deployment by the Platform Operator and the Originator</td>
</tr>
<tr>
<td></td>
<td>2. Integration support for Brokers and Merchants</td>
</tr>
<tr>
<td></td>
<td>3. Software enhancements, maintenance and support</td>
</tr>
<tr>
<td>Platform Operator</td>
<td>Responsible for:</td>
</tr>
<tr>
<td></td>
<td>1. Deployment and operation of the MintChip platform</td>
</tr>
<tr>
<td></td>
<td>2. Administration of the operating rules, standards and protocols</td>
</tr>
<tr>
<td>Broker</td>
<td>A Provider: (e.g. Depository institution, regulated non-bank)</td>
</tr>
<tr>
<td></td>
<td>1. Buys and sells MintChip value from/to Originator</td>
</tr>
<tr>
<td></td>
<td>2. Enrolls End Users</td>
</tr>
<tr>
<td></td>
<td>3. Provides mechanisms for End Users to buy and sell MintChip value</td>
</tr>
<tr>
<td></td>
<td>4. Provides currency conversion services (optional)</td>
</tr>
<tr>
<td>End User</td>
<td>An Entity using a payment service for sending or receiving payments (e.g. Business, Consumer, or Government agency)</td>
</tr>
</tbody>
</table>
MintChip Platform Overview

(Diagram #6)

**Originator:**
The ecosystem has been built so that when the platform achieves a certain scale within a country, the Central Bank, or a branch/division of the Central Bank will act as the Originator within the ecosystem. It is the Originator’s role to create (or “mint”) MintChip value in the designated fiat currency. The system is built to support a single Originator for each currency created in the MintChip ecosystem. As part of the initial implementation the Platform Operator may act as the Originator, however, it is anticipated that a country’s Central Bank (or Federal Reserve) will eventually assume the Originator role.

**Broker:**
The ability to become a MintChip Broker is made available to new, and existing providers in the current payment systems through open APIs. A Broker will utilize these APIs to provide access to End Users to the MintChip platform through their existing mobile applications or online services. It is anticipated the first Brokers in the MintChip Ecosystem will be depository institutions, regulated non-bank account providers and large retailers. Lowering the barriers to entry through our open platform will encourage new participants who can focus on providing value-added services.

The Broker opens a MintChip account with the Originator and establishes one or more Secure Asset Stores (SAS) on the MintChip platform. The Broker pre-purchases MintChip value from the Originator in order to meet the needs of their End Users. This is done by the Broker transferring the funds in fiat currency to the Originator’s pooled account, and the Originator loading the equivalent MintChip value into the Broker’s SAS.
The Broker’s role is then to sell or redeem MintChip value to and from (as the case may be) End Users, who use fiat currency. The Broker is also the participant that establishes MintChip accounts for End Users. As the Brokers will be current Providers in the existing traditional financial and payments systems, they will be in a position to complete Know Your Customer (KYC) requirements and comply with applicable Anti-Money Laundering (AML) laws and regulations at the time of End User registration. Through their existing billing systems, Brokers may charge the End User fees for participating in the ecosystem.

End User
End Users can be individual consumers, businesses, or government agencies. End Users open MintChip accounts with Brokers and are assigned Secure Asset Stores (SAS) to hold value in a specified currency. For this reason, End Users may have more than one SAS in the same or multiple currencies. For example, one SAS may contain USD and another may contain CAD. All transactions completed in the MintChip ecosystem are a transfer of value between two different SASs. Value Transfer Messages facilitate the exchange and represent the monetary value in transit. The VTM can only be consumed by the Receiver’s (Payee) SAS and is cryptographically encrypted and signed to prevent tampering. MintChip SASs are only able to exchange value with a SAS that shares the same currency.
Secure Asset Store (SAS):

The MintChip ecosystem also distinguishes itself from any other payment system by its use of a Secure Asset Store (SAS). A SAS can be thought of as a digital safe deposit box that contains:

1) A unique SAS identification number.
2) Identity information of the Entity associated to the SAS
3) A ledger that tracks every transaction that occurs within the SAS.
4) Secure storage for the MintChip digital currency.

Value Transfer Message (VTM):

The MintChip technology is elegant in its simplicity and begins with a concept that is dramatically different from the concepts driving today’s payments systems. If you reduce payment transactions to packets of data and ensure that those packets are incredibly secure, then the manner in which those packets move from user to user can be flexible, low-risk, highly adaptable and very efficient. The nature of today’s payment systems, built on legacy systems and built in piecemeal fashion, means that system operators and participants must focus on ensuring end-to-end system security for each payment, which is costly, time-consuming, and ultimately means the particular network is only as secure as its weakest link.

The technology in the MintChip platform that creates the data packets described above that distinguishes it from any other payment platform is the Value Transfer Message (VTM). The VTM is patented technology and is a highly secure method for securing payment information and value. This small (52 bytes) and extremely secure package of information contains four critical pieces of data required to complete a transaction:

- the Payer ID;
- the amount;
- the currency; and
- the Payee ID.

Every transaction must contain this information before a VTM can be created. Once created, the Message is encrypted and digitally signed in the Hardware Security Module (HSM), which ensures the highest level of security. The patented technology within the VTM ensures that, even if the VTM is captured during transmission, and someone succeeds in breaking its encryption, the only information that is revealed is the intended Payee’s location. There are also multiple additional security features that both prevent the occurrence of a security breach, and identify breaches if they occur.
**MintChip Ecosystem is a Good Funds Model:**

MintChip value in a MintChip account SAS represents Good Funds as it is backed by the fiat currency in the Originator’s pooled account.

Value is transferred into a SAS by converting USD funds into a digital representation of the currency through a MintChip Broker - creating MintChip USD. As part of the conversion, the USD funds are deposited into the Originator’s pooled account ensuring that each MintChip USD is backed by USD funds. This structure ensures that MintChip USD is pegged to, and at par with traditional USD. This structure also means that any transaction that occurs on the MintChip platform follows a good funds model and virtually eliminates the risk of completing transactions within the platform. This model also reduces participant costs and system requirements that are required to verify payments in today’s payment ecosystems.
Loading Value into the MintChip Ecosystem:

The conversion of funds from fiat currency outside the MintChip ecosystem, to MintChip digital currency inside the ecosystem can only be completed through a MintChip Broker. The Broker accesses the MintChip ecosystem using the open APIs. The Broker will then embed the features and functionality of the platform within their own applications. The User will access the MintChip platform through the Broker’s application. The User selects the “Load Value” option from the application and they will be presented with a list of the available funding sources that they have previously registered into their account when they established their MintChip account. Diagram # 6 outlines the potential funding sources the End User can use to load fiat currency into their SAS. It is important to note that a large portion of Brokers are anticipated to be existing financial institutions allowing users the capability to easily transfer funds between the user’s accounts. (e.g. savings accounts, checking accounts, credit/debit card or line of credit) (U.1).

Once the funding source is selected, the End User can select the amount they wish to load into their MintChip account and associated SAS. In most instances, the funding source, will be a deposit account held by the Broker (e.g. the End User’s retail bank). The Broker receives the funds from the MintChip End User and then delivers the MintChip value directly into the End Users SAS.

Because these systems leverage existing methods for authenticating both End Users and the value they are attempting to load into the ecosystem, this onboarding process ensures the funds used to credit the individual SAS tied to the MintChip account are good funds.
Removing Value from the MintChip Ecosystem:

The conversion of digital currency from a User’s MintChip account can only be completed through the User’s Broker. Similar to how the User loaded funds into the system, the User access the MintChip platform from within the Broker’s application. The User then selects “Value Unload” from the options menu. This option may either be presented within a consumer application or a business-specific application (for example, in the case of a merchant). The User will enter the value of MintChip digital currency they wish to unload, and will be prompted to select one of the previously registered accounts where they would like to receive the funds (e.g. a deposit account held at their financial institution). The Broker then initiates transfer of the MintChip value from End User’s SAS to the Broker’s SAS, and then deposits the equivalent amount in fiat currency into the End User’s selected account.

Payment Sources to Load Value into MintChip

(Diagram #9)
**Security Overview of the MintChip Ecosystem:**

The MintChip solution at its core is:

1. A distributed system of Secure Asset Stores (SASs); and
2. A messaging protocol that enables the trusted exchange of value between these Stores (Value Transfer Messages).

Central to the MintChip ecosystem and the root of all trust in platform is the “Security Series”. This is a secured certificate that provides a shared signing authority, which enables trust in message authenticity and integrity.

The key differentiator between the MintChip platform and other digital cash systems is the patented technology that protects the transfer of assets (value) between two End Users (B2B, B2P, P2B, P2P). Regardless of transaction value, all MintChip transactions are completed in highly-secure Hardware Security Modules (HSMs), the same hardware used in today’s global payments systems. Value Transfer Messages (VTMs) are encrypted and signed using an approach backed by four patents. By securing VTMs, MintChip is able to operate in a manner that allows for the completion of transactions offline, which is a unique feature in digital cash technology.

The MintChip platform has been built to ensure the benefit of breaching its security is outweighed by cost, effort, and resources necessary to do so. Because hacking the system is so costly and the potential return of it so low, hackers will look at other ecosystems, where return for their efforts could be much greater.

The VTM technology and the patented cryptography that protects the VTM can be quickly upgraded at any time, with no system downtime and at a very low cost. As technologies like quantum computing become available to potential hackers, post-quantum cryptography can be used to increase encryption surrounding the VTM, ensuring it remains secure against new hacking techniques.

The MintChip platform is ultimately user- and use-case-agnostic; designed to apply the same patented high security to each transaction regardless of its value. The technology supports transactions as small as 1/100 of a cent and as large as hundreds of millions of dollars. Moreover, the transaction that are completed are small in size (52 bytes) enabling the ability to store every transaction separately in the Secure Asset Store of both parties to the transaction. This rich supply of data means that compliance with virtually any regulatory regime is possible - which in turn enables the potential for global deployment of the platform.
The 8 Stages of the end-to-end payment Process

1. Initiation:
Initiation of a transaction on the MintChip platform can occur any time after the End User has established a MintChip account, and the associated Secure Asset Store (SAS) through their Broker. Once the MintChip account is established a User is capable of establishing multiple SASs associated to their single MintChip account.

MintChip Account Structure with Multiple Secure Asset Stores
(Diagram #10)
Once established an individual SAS is capable of receiving a transfer of MintChip at any time, from any other SAS on the system (U.1) (U.2). To send MintChip value to another End User on the platform, the End User only needs to have value in their SAS. The MintChip platform is a good funds model, this ensures the only prerequisite to initiating a transaction is that the MintChip account SAS must hold a value equal to, or higher than, the value the End User wishes to send to another User on the platform. (U.3) Access to the MintChip platform requires an Internet connection (e.g. Smartphone, Desktop, laptop, etc.) although a unique feature of the platform is the capability to complete an offline transaction which the platform is capable of doing and will be deployed shortly after the commercial launch. (U.1)

It is important to note, because all transactions occur between two different SASs, the ecosystem itself doesn’t differentiate between consumer, business, or government SASs. Because the platform is End User agnostic, all use cases (B2B, B2P, P2B, P2P) could potentially be supported by the ecosystem and the process for initiating a payment for any given use case is similar as outlined below. (U.6) The MintChip ecosystem utilizes an asset transfer architecture to move value in real time without an intermediary or central authority to facilitate the transaction. All Payer needs to initiate a transaction is the Payee’s MintChip identifier. This identifier is initially structured to be an email address, mobile phone number, and name - however, the platform has been designed so it could also be a Facebook username or any other identifier. If the Payer has sent funds to the Payee (Person, Business, or Government) in the past, their information will be saved securely within the MintChip application, for a better user experience. (U.2) (U.6)

If the End User is initiating a transaction directly with a physical merchant, or on-line, the User will complete their shopping and take their products to the Merchant for check out. The Merchant (retail or online) will then present a Value Request Message (VRM) for the total value of the goods purchased. This VRM initiates a payment transaction and the User initiates the payment by either scanning the VRM QR Code (IOS and on-line) or through NFC communication (Android). In either case the User needs only select “Pay Merchant” from the menu items within the application on their phone to initiate the transaction. (U.2)

Initiating a transaction is creating a Value Transfer Message (VTM) on the MintChip platform. Once the VTM has been created it is secured using the patented cryptographic methods that are detailed above. (S.7) (E.4) Once the VTM has been initiated by the End User the transaction data is securely stored within the User SAS. (S.9) Any information, at any stage of the transaction, residing on the MintChip platform, including personal and or transactional information, is secured through encryption. (S.7)
Users are capable of completing cross border payments using the MintChip platform. Once the platform has been deployed in a foreign country, completing a transaction between the home country and another country is very similar to a domestic transaction. (U.5) End Users can keep multiple MintChip Secure Asset Stores (SAS) in different currencies, or they can transact through a currency Broker, allowing the End User to select the most cost effective exchange rate. The Broker holds MintChip value in the different currencies and completes all transactions using only digital currencies. Once MintChip value is converted, the user is provided with the desired digital currency which can be exchanged for corresponding fiat currency. The process is fast, secure, and given the limited marginal cost of completing a transaction on the MintChip ecosystem, it can be completed very cost effectively.
Payment Flow for Currency Conversion
(Diagram #12)
Payment Sources to Receive Value from MintChip
(Diagram #13)

- Cash in Merchant
- Direct Debit
- Mobile Banking
- Cash from Agent
- ATM
- Online Banking
- Interac (Canada)
- Branch Banking
- Faster Payments (UK)
- ACH/EFT (Canada)
2. Authentication:

There are two distinct End-User authentication points in the MintChip ecosystem:

1. Transaction that occur within the MintChip ecosystem itself; and
2. Transactions into or out of, the ecosystem.

Both of these authentication pieces are discussed in detail below.

Transactions occurring within the MintChip ecosystem:

As described in the Initiation section above, for an End User to participate in the MintChip ecosystem, they must set up an account on the Web or by downloading a mobile application. Setting up a MintChip account requires multi-factor authentication to ensure overall security of the ecosystem. The following End User data is required:

1. Name;
2. E-mail address;
3. Mobile Phone Number; and
4. Mobile Phone Device Identifier. (captured through the process itself).

These identifiers are then linked directly to a specific MintChip account, which itself has a unique identifier. The End User data is then securely stored and a SAS is created and linked to the MintChip account. (S.7) (S.9) Before completing a transaction, a Payer’s End User data is Authenticated against the information stored for the MintChip account. (S.10) (S.7) (S.10) If an End User tries to complete a transaction from a different phone, the platform will deny the transaction until that device is registered.
Authentication at the Ecosystem On- and Off-Ramps:

The MintChip ecosystem is designed to operate and interact with the existing payments system. (U.2) (U.3) MintChip Brokers would be restricted to Providers that comply with regulatory requirements for financial institutions (e.g. depository institution or non-bank account providers). (S.7) Because these Brokers must authenticate their customers as part of their initial and ongoing KYC and AML requirements, there are assurances that funds being loaded into the ecosystem are loaded on a “Good Funds” basis. (S.7) (S.9) (S.10)

These authentication protocols will be leveraged when End Users top up their MintChip account (convert fiat currency to MintChip USD). Different layers of authentication can be used depending on the top up values, which can be set by individual Brokers or the ecosystem generally. End Users with low-value payment needs may be subject to less-rigorous authentication methods, which makes the ecosystem more accessible (U.1). (S.10) If an End User cannot be appropriately authenticated, they will not be able to carry out the currency conversion.
Similarly, when the End User unloads MintChip value as fiat currency to a depository account, the same authentication process occurs. AML concerns are addressed as the MintChip platform provides an audit trail that logs value taken out of the ecosystem. These off-ramps will have KYC requirements and AML rules to be in place to address money laundering concerns. However, we do anticipate that, the longer the platform is in operation and the more ubiquitous it becomes, transfers out of the ecosystem will become less critical, as Participants find more and more use cases for transferring funds within the ecosystem.

3. Payer Authorization:
Payer authorization for P2P, B2B and B2P transactions within the MintChip platform can occur in real-time on an *ad hoc* basis, or in a pre-authorized manner, with the Payer having established a Payee, payment amount and payment date ahead of time. *(U.2) (U.3)*

The Payer can not only view any upcoming/pre-authorized payment, they are able to cancel upcoming payments, or modify any of the relevant pre-authorized payment parameters up to the moment the transaction is completed. This differs from some current models where funds must be deposited days in advance of the payment being made, to avoid an NSF charge.

Payer authorization in a typical point-of-sale environment is also very straightforward. A merchant can accept payment via MintChip USD either by presenting a QR Code to the End User or by having an NFC MintChip-enabled terminal. The Payer either scans the QR code or places the phone near the terminal, confirms the transaction amount, and the transaction is authorized and irrevocable.

There are no incremental security controls enabled to provide Payer Authorization. All the security features and protocols previously defined remain in place for Payer Authorization and End User data protection. *(S.7) (S.9)*
4. Approval by the Payer’s Provider:

The MintChip platform replicates a cash transaction with a digital representation. Because the model is a good funds model, the approval by the Payer’s Provider is immediate. (F.1) Either the Payer can complete the transaction or not. If the Provider’s approval is provided, the payment is final and irrevocable. (S.3)

In this way, the MintChip ecosystem replicates a cash transaction and makes it more secure. Once a VTM is created, funds are immediately debited from the End User’s account, and only the Payee’s SAS can accept the transaction. The Payer is notified of the payment status promptly through their transaction history, which is accessible through the application. (F.5).

All transactions are completed using the same high-level End User security controls described in detail in Part A, (S.7) (S.9) regardless of the value of the transaction, be it fractions of a cent, or hundreds of millions of dollars.

5. Clearing:

There is no traditional Clearing in the MintChip platform because there is no communication between the Payer’s and Payee’s depository institution. As well, no netting occurs because the system considers payments on a transaction-by-transaction basis. Instead, a Payer identifies a Payee by email or mobile number and confirms the amount of a payment. Before the VTM is created, the MintChip platform looks up the SAS ID and any transaction limits for the account. The VTM is then created and the Clearing process is considered complete. (F.2) Within that VTM, a variety of payment standards can be accommodated (E.4).

The security controls and End-User data protection are the highest available, and can be seamlessly upgraded to keep pace with evolving security needs. Because all transactions are completed by the transfer of value from one SAS to another, all transactions are completed using the same high level security protocols for End-User data and transaction protection and security, regardless of the size of the transactions. (S.7) (S.9) The current product roadmap includes adding the option to provide an additional level of security for larger transactions, to provide an even higher comfort level for End Users.
6. Receipt of the Payment

It is important to recall, as discussed in detail above, that once the Payer initiates a transaction, only the intended Payee can receive the funds. (F.3). For the Payee (which can be virtually any Entity (U.1)), funds are available immediately upon accepting the transaction, at which point it can be considered complete. This finality is “always on” - meaning that transactions are considered to be good funds regardless of when the payment is received by the Payee, without holds or limits on availability (U.2). The payment status is visible to the Payer at all times and the Payee is made aware of an incoming transaction through a variety of mechanisms (F.5):

1. Via email notification to the Payee’s registered email address;
2. By Push Notification to the Payee’s mobile device;
3. Through immediate in-app notification of “Incoming Payment”;
4. Through a “Success” notification in-app upon acceptance of payment; and
5. By an update to the Payee’s transaction history - in both “Pending” and “Received,” as applicable.

The same security features that are in place for payment initiation and Payer authentication are in place at this stage of the transaction as well. (S.7) MintChip provides detailed transaction logging and audit trail to enable easy dispute resolution between parties. (S.5)

7. Settlement:

Because the MintChip platform uses a good funds model, settlement within the platform is seamless and can be virtually indistinguishable from transaction initiation, approval and clearing. Settlement is considered to have occurred once Payee accepts the transaction, whether such acceptance happens manually or in an automated fashion. (F.4) Settlement occurs between the two parties without a centralized authority or other third party involvement. (S.4) This approach eliminates risk for both the Payer and Payee. There is no lag in the funds availability to the payee and no settlement between underlying parties. All transactions on the MintChip platform are completed using the same security protocols as previously outlined. (S.7) (S.9)
8. Reconciliation:

The MintChip platform has an impact on traditional methods of creating and recording transaction information. Because value is transferred via VTM, payment information and payment value are inextricably linked and there is no opportunity for this information to be corrupted or altered in transit; Payees and Payers will receive identical information, which is recorded by each SAS. (U.3)(S.7)(S.9)

The SAS securely stores all of this transaction history. Because all transactions are electronic and take up a relatively small amount of server space the platform has the ability to save large volumes of transaction data for use at any given time. Unlike traditional records or Provider legacy systems, transaction records can be easily stored, organized and searched. This volume of transaction data can be accessed, with proper authority, to facilitate post transaction evaluation. (S.7)

In the event of an unauthorized, fraudulent, erroneous, or otherwise disputed payment, the transaction log from the relevant SAS will be pulled and a detailed transaction log can be reviewed. Each SAS can be traced backed to the identity attached to the MintChip account. If a fraudulent transaction has occurred, it can quickly be investigated and resolved. (E.7) (S.5)

Because the MintChip ecosystem is a good funds model built with the guiding principles of speed, efficiency and payment finality, the Payer is liable for unauthorized, fraudulent or erroneous transactions. A transaction can only be originated from an End User’s MintChip account. As described in Section 2 (Authorization,) there are multiple security features that have been established to ensure access to the End User’s account is protected, and the patented encryption technology ensures that both the information used to complete the transaction, as well as the information stored within the individual SAS is secured and protected at all times, and can be easily upgraded at any time. (S.7) (S.9) The MintChip ecosystem has not been designed as an alternative dispute mechanism to rule on issues that arise between End User’s. However, if there is evidence of fraud in the ecosystem, End Users will not be expected to bear the loss.
Part A, Section 2: Use Case Description:

The MintChip platform enables peer-to-peer payments across a broad range of use cases. While there are many similarities in the eight stages of the end-to-end payments lifecycle, there are subtle differences that make each use case unique.

**Business to Business (B2B):**

The MintChip platform has been designed with an open architecture to enable connection to any system capable of completing payments. In the case of an Enterprise ERP systems, MintChip digital currency would simply become another payment source within the ERP system. It is assumed for the purpose of this proposal that integration into any ERP or payments system would be similar.

The transaction flow for a B2B transaction outlined below is generic and based on a transaction between two businesses each with an ERP system. **B1-Payer → B2-Payee**
1. Initiation
   a. B2 has purchased goods or services from B1
   b. B1 ERP system creates electronic invoice and sends to B2
   c. B1 indicates MintChip USD as preferred payment source on invoice
   d. B2 enters invoice into ERP system, and selects MintChip USD as payment source
   e. B2 ERP registers B1 Company name (SAS identifier) invoice #, payment amount, and date for payment.

2. Authentication
   a. B1 ERP and B2 ERP systems authenticate against MintChip API
      i. On the selected payment date, B2 ERP identifies value to be paid to B1
      ii. B2 ERP connects to MintChip platform to confirm payment value is supported by digital cash account balance.

   a. If confirmed, B2 ERP system initiates creation of VTM for B1
   b. If not confirmed, B2 ERP notifies requirement to add additional digital cash into the SAS on the MintChip platform
   c. VTM is transferred to B2 on MintChip platform

6. Receipt
   a. B2 ERP system receives notification of payment of invoice from B1

7. Settlement
   a. B2 ERP captures invoice # contained in VTM and value and matches against value of original invoice delivered to B1.
   b. B2 ERP system accepts payment of invoice (automatically or ad hoc)
   c. If payment is complete B2 ERP records transaction and closes off invoice
   d. If payment is incomplete B2 ERP flags transaction for further investigation
   e. In either scenario VTM is accepted by B2

8. B2 ERP sends notification to B1 ERP on status of transaction
Business to Person (B2P):

For businesses that manage cash disbursements for temporary or seasonal workers, MintChip provides a solution to move cash to multiple employees at once.

Business to Person Transaction (8 Stages)
(Diagram #16)

1. Initiation
   a. Company Back Office System runs payroll and determines cash disbursements for the day, week
2. Authentication
   a. Back Office System authenticates against the MintChip API
   a. System identifies cash recipients
   b. System confirms sufficient balance in Payer’s MintChip account
   c. System creates VTMs and distributes to employees
4. Receipt
   a. Recipients receive notification of cash disbursement
5. Settlement
   a. Employees accept the cash disbursement to finalize the payment
6. Reconciliation
   a. Back Office System is notified of confirmed and pending payments
Person to Business (P2B):

MintChip acceptance by Merchants provides a cost-effective alternative to cash and existing payment options. Consumers can simply use their mobile phone to pay in-store at the Merchant POS terminals.

Person to Business Transaction (8 Stages)
(Diagram #17)

1. Initiation
   a. Person brings product to checkout counter at Merchant location
   b. Person open MintChip payment capability from within Broker’s mobile application
   c. Business scans and/or enters items value into POS system
   d. Business requests payment from Person
   e. Person indicates desire to pay using MintChip digital cash
   f. Business selects MintChip as payment source on POS system

2. Authentication
   a. Value of transaction is sent from POS system to integrated Pin Entry Device (PED)
   b. POS PED authenticates against the MintChip API

3. Payer Authorization

4. Approval by Payer’s Provider
5. Clearing
   a. PED device creates Value Request Message (VRM) to be sent via NFC or represented as a QR Code for value of purchase on the PED device screen.
   b. VRM includes SAS ID of the merchant and value of requested transaction
   c. Person selects “Pay Merchant” from menu screen within the mobile application
   d. For QR code scanning person prompted to “Scan Barcode” from Pay Merchant screen. Once selected application initiates camera and enables Person to scan barcode from PED device (VRM). For NFC-equipped devices person is prompted to press device against PED to communicate via NFC
   e. Once scanned/received, mobile application verifies payment amount, and Person is prompted to provide verification of the purchase value.
   f. Person can provide finger scan, or simple enable manual verification of transaction
   g. Once verified, screen prompts indicate “Processing Transaction”
   h. Upon verification the User application creates VTM for Merchant

6. Receipt
   a. Merchant PED device to confirm receipt of MintChip payment

7. Settlement
   a. VTM is transferred via PED to merchant MintChip account to complete transaction
   b. Payment transaction is complete

8. Reconciliation
   a. Once the transaction is complete Person is notified “Payment Accepted” and the message indicates, the value transferred, the identification of who it was transferred to, and the Person’s balance is debited the amount of the transaction.
   b. Merchant receives confirmation of completed payment via PED device and/or POS system.
   c. Within the individual SASs of both the merchant, and person, the transaction is registered in the individual ledgers.
**Person to Person (P2P):**

The MintChip platform provides APIs and mobile applications to enable person-to-person payment.

Person to Person Transaction (8 Stages)

(Diagram #18)

1. **Initiation**
   a. End User opens mobile application on their device to send a payment

2. **Authentication**
   a. End User is authenticated when they log in to the app
   b. End User’s mobile device is verified

3. **Payer Authorization**
4. **Approval by Payer’s Provider**
5. **Clearing**
   a. Enters the recipient’s email address to identify their MintChip account
   b. End User enters the amount and currency to transfer
   c. Value of payment is Authorized by comparing value of transfer request against MintChip account balance
   d. End User selects “Send” to initiate payment; VTM is sent to recipient via email, push notification or direct message

6. **Receipt**
   a. Recipient is notified that they have received a payment from the sender

7. **Settlement**
   a. Recipient accept payment to complete the transaction

8. **Reconciliation**
   a. Both sender and receiver have detailed logs in their transaction history to refer to in the event of a disputed payment
Part A, Section 3: Use Case by Effectiveness Criteria:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Authentication</td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.10</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Payer Authorization</td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td>S.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Clearing</td>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Receipt</td>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Settlement</td>
<td>S.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>E.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
PART B: BUSINESS CONSIDERATIONS:

1. Implementation Timeline:

The MintChip digital cash platform was deployed in Canada in Q1, 2015 and is currently live and focused on P2P and P2B use cases. MintChip can be deployed quickly in any target country once regulatory licenses are in place (E.3). MintChip open APIs are published and available today for providers to build digital cash solutions powered by MintChip. (U.1)(U.2)

The MintChip platform is comprised of the back-end system to process payments and open APIs that enable participants to integrate MintChip digital cash into existing and future payment systems. (U.1) MintChip also provides tools for Originators, Brokers and Regulators to monitor and manage digital cash transactions. (E.5)

MintChip is a good funds payment system that enables Real-Time payments that clear and settle instantly. There are two integration points required to extend the the MintChip Ecosystem and make it interoperable with traditional payments systems necessary to achieve ubiquity (U.1)(U.3):

1. On Ramps enable payment Participants to “withdraw” funds from existing accounts/payment sources to “deposit” funds into the MintChip ecosystem. MintChip currently connects to accounts including:
   a. Credit card payments
   b. Debit card payments
   c. Interac Online payments from Canadian bank accounts*

2. Off Ramps enable payment participants to “withdraw” funds from the MintChip Ecosystem to “deposit” funds into depository accounts. MintChip currently connects to accounts including:
   a. Direct deposit via EFT*

*Currently available in Canada only
MintChip Roadmap

The following product roadmap focuses on key areas of development to broaden the currently deployed platform functionality necessary for the MintChip platform to achieve safe, ubiquitous faster payments in the United States for all suggested use cases B2B, B2P, P2B and B2B.

The MintChip product roadmap is focused on six key areas of development:

1. **Interoperability**: The MintChip digital cash ecosystem has many benefits but to reach ubiquity and international adoption will require collaboration with central banks and banking systems globally. To do this it is critical to integrate into ACH in the United States for direct debit, direct deposit, as well as business to business and ecommerce payments. In addition, full support for the ISO 20022 messaging standard will ease integration and support more remittance data to accompany payments (U.1).

2. **Accessibility**: To complement existing MintChip open API architecture, mobile SDKs will be developed for iOS and Android that will simplify mobile application development and enable stakeholders to build a broad range of solutions that leverage the MintChip digital cash platform. (U.1) In addition, HTML code snippets will be created to simply integrate MintChip payments on a website accessible from any mobile device, tablet, or PC. (U.2)

3. **Security**: MintChip supports three cryptographic algorithms at any given time to enable the system to dynamically update security as the market requires. In addition, MintChip will be able to use different cryptographic algorithms depending on the value of a transaction to ensure the system is fit for purpose and balances security and performance. Integration with biometric security services will enhance the overall security of MintChip authentication of End Users, and will increase the security of the MintChip platform and reduce fraud risk. (E.5)

4. **Merchant Acceptance**: Digital cash will require merchant acceptance at POS. MintChip has established a partnership with one of the World’s leading POS terminal manufacturers, Ingenico. They have completed development of a stand-alone application we are in the process of completing field trials with, Ingenico is now finalizing integrated POS solutions, and we are initiating discussions with other global terminal providers including VeriFone. (U.1)(E.5)
5. **International**: To facilitate foreign exchange and cross-border money transfer the MintChip ecosystem will be expanded beyond Canada to include key countries in North America and Europe. The first phase of additional countries we are pursuing deployments in include: United States, Europe, Brazil, and Mexico. (U.1)(U.3)(E.3).

6. **Compliance**: The MintChip Platform manages a history of all payment transactions in ledgers in each Secure Asset Store. Transaction summary and exception reports enable the Originator to meet compliance reporting requirements of FinCEN in the U.S. and FINTRAC in Canada. A self-service regulator portal will be developed for regulators to monitor the digital cash system for fraudulent transactions and money laundering activity. (E.3)(U.3)

<table>
<thead>
<tr>
<th>MintChip Platform Roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Interoperability</td>
</tr>
<tr>
<td>Accessibility</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Merchant Acceptance</td>
</tr>
<tr>
<td>(Barcode) integration (NFC, Barcode)</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>UK Originator for GBP MintChip</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
USD Deployment Timeline

A MintChip environment can be deployed in a country within eight (8) weeks including:

8 Steps to MintChip Platform Deployment
(Diagram #19)

1. Hardware Provisioning
2. Datacenter/Networking Setup
3. Server/HSM Configuration
4. MintChip API/Database Installation
5. Secure Asset Store Generation
6. MintChip USD Value Creation
7. Security Audit
8. Final Testing
2. Value Proposition and Competition

We believe that the MintChip ecosystem will do for payments what the Internet did for regular mail. Indeed, this is a bold statement. Our value proposition reduces the transaction costs across all use cases to a fraction of current costs. In many instances, payments will be free. Alongside this reduced cost, the ecosystem will increase both the speed and security of payments.

The MintChip platform leverages an asset transfer model to move value in Real Time without an intermediary. Contrary to conventional payment systems where value is held by intermediaries, the MintChip platform is a Good Funds peer-to-peer payment system that transfers value quickly and securely from one party to another.

This simple model is more efficient than conventional payment systems and has a variety of benefits:

- Supports both Push/Pull transaction models;
- The value transfer is instant and irrevocable;
- Requires no intermediaries;
- Operates in both online and offline environments; and
- Immediate, irrevocable payment authorization

An additional value proposition of the MintChip platform is the ease with which the platform is available to any ecosystem participant (existing or new) through open, robust APIs and a user-friendly Software Development Kit (SDK). Because the ecosystem capabilities are equally available to all participants, competition within the payments landscape can be increased. (E.1) Under this model, competitors will compete with respect to the value-added services they provide to their customers instead of the cost and method in which a particular payment is completed. (E.2)

The MintChip technology is elegant in its simplicity and begins with a concept that is dramatically different from the concepts driving today’s payments systems. If you reduce payment transactions to packets of data and ensure that those packets are incredibly secure, then the manner in which those packets move from user to user can be flexible, low-risk, highly-adaptable and very efficient. The nature of today’s payment systems, built on legacy systems and in piecemeal fashion, means that system operators and participants must focus on ensuring end-to-end system security for each payment, which is costly, time-consuming, and ultimately means the particular network is only as secure as its weakest link.
Any End User (e.g. person, business, government agency) can register and create a unique SAS. The ecosystem facilitates the transaction between any two SASs the same manner every time - using the same security protocols that are implemented platform-wide (U.3). This SAS-based interaction means once an End User is on the platform, the process across all eight stages of the payment lifecycle are affected bilaterally; no other participants are required. This streamlined approach increases the speed and security of each transaction and reduces the cost, risk and complication that is associated with other payment systems.

The MintChip ecosystem does not rely on legacy systems or current payment-system participants like financial institutions to complete transactions. This enables the MintChip platform to cost-effectively scale, and through the open API structure many participants can access the system because of the relatively low barriers to entry. (E.2) Interaction with the existing infrastructure is limited to the loading and unloading of funds only; the legacy infrastructure does not play a role in the MintChip payments themselves.

There are three reasons why nanoPay has chosen a strategy that provides easy and open access to the MintChip ecosystem:

1. **Drives Ubiquity.** Open access means that all participants can send and receive payments in a cost-effective, efficient manner that ultimately drives increased adoption.

2. **Enables Competition:** With most users on one platform, participants will be free to focus on developing value-added services, rather than payment processing. More competition drives the development of superior products and services, benefitting all users.

3. **Cost Reduction:** An open system drives down the cost of payment transactions and, given the marginal cost of completing a transaction on the platform is close $0.00, nanoPay can offer ecosystem participation for a fraction of current rates. This low cost will provide Brokers great pricing flexibility, and as more Brokers use the platform, pricing and per-transaction costs will be driven down.

The MintChip platform provides a clear value proposition across all payment use cases through all eight stages of the payment lifecycle.
**Business to Business:**

Example Use Case:

1. Business completes payment to another business via ERP systems

Business to Business Transaction Flow
(Diagram #20)
## Stage #1 Initiation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reason for Adoption)</th>
</tr>
</thead>
</table>
| User #1 (Business Payer) | - Payments can be initiated and completed through existing ERP system  
- Cost of completing payment for businesses without ERP system much lower  
- MintChip digital cash simply a different payment source in ERP system  
- Streamlined process for initiating payment, which can include detailed remittance information  
- Businesses will adopt due to simple integration process and cost savings  
- Easy Process to customize recurring and one-time payments to vendors |
| User #2 (Business Payee) | - Payee can initiate transaction through Value Request Message (VRM), which is built into platform capabilities  
- If not initiating payment, no other activity required  
- Business Payee will adopt due to immediate payment, low cost of payment processing, and overall platform efficiency |
| Payment System (ERP)(POS) | - Minimal work for ERP/POS provider to build MintChip digital cash as an alternative payment source in platform. (SAP has confirmed this in multiple conversations)  
- Modification for a single customer makes it a potential feature for all other existing and new customers for the ERP/POS provider  
- Enabling another method to initiate/receive payment increases ERP/POS providers customer satisfaction |
| nanoPay (Proposer) | - Increased adoption by ERP/POS platforms enables easier adoption by additional Businesses using same ERP/POS platform  
- Increased users drives increased adoption across businesses, creating additional use cases (e.g. Payroll, Refund process, etc.) |
<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reason for Adoption)</th>
</tr>
</thead>
</table>
| Business (Payer)            | - Authentication occurs upon registering business on MintChip platform  
- Authentication process is easy for all businesses  
- All individual transactions are authenticated on the MintChip platform which is incremental to any existing Authentication processes used by the businesses |
| Business (Payee)            | - Authentication occurs upon registering business on MintChip platform  
- No additional requirement for Payee Authentication  
- All individual transactions are authenticated on the MintChip platform which is incremental to any existing Authentication processes used by the businesses |
| Payment System (ERP)(POS)   | - Minimal work for ERP/POS provider to Authenticate MintChip digital cash transaction (SAP has confirmed this in multiple conversations)  
- ERP/POS provider already uses Authentication process for each transaction, additional MintChip platform Authentication in incremental, providing additional security.  
- Modification for a single customer makes it a potential feature for all other existing and new customers for the ERP/POS provider.  
- Enabling another method to initiate/receive payment increases ERP/POS providers customer satisfaction. |
| nanoPay (Proposer)          | - Secure Authentication process increases customers’ confidence and drives increased adoption of the MintChip platform  
- Already investigating ways to increase Authentication process using bio-metrics which provides value added revenue opportunity for nanoPay |
## Stage #3 Payer Authorization

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reason for Adoption)</th>
</tr>
</thead>
</table>
| Business(Payer) | - The MintChip platform is a Good Funds model. Payer is Authorized to complete any transaction instantly, up to the value of funds in the account.  
- Payer can enable pre-authorized payments and Payer is sent confirmation immediately before payment being debited. Enabling last-second cancellation if required.  
- Businesses will adopt this platform as it provides simple integration and increased flexibility for Payer Authorization.  
- Businesses without ERP system will simply be Authorized on MintChip platform alone, a very quick and secure process.  
- MintChip platform can also Authorize individual users within a single business to complete transactions while ensuring all transactions are recorded. |
| Business(Payee) | - Payer Automatically Authenticated at transaction initiation ensures when the Payee receives the funds they are instantly available.  
- Payer will adopt the platform as it accelerates payment processing, they get their money faster. |
| Payment System (ERP) | - Minimal work for ERP provider to Authorize the payer to complete a transaction.  
- ERP provider already uses existing Payer Authorization process for each transaction, additional MintChip platform Authorization is incremental, providing additional security.  
- Modification for a single customer makes it a potential feature for all other existing and new customers for the ERP provider.  
- Enabling another method to initiate/receive payment increases ERP providers customer satisfaction. |
| nanoPay (Proposer) | - Simple Authorization process minimizes transaction cost, and increase pricing flexibility and potential profit margin by minimizing back end support requirements  
- Simple Authorization process helps drives increased platform adoption and a better user experience. |
## Stage #4 Approval by the Payer’s Provider

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reason for Adoption)</th>
</tr>
</thead>
</table>
| Business (Payer)          | - MintChip platform is a Goods Fund Model. No approval by the Payer’s provider is required.  
                          | - If funds are available, transaction can be initiated, once initiated, funds can only be received by the Payee, no additional approval is required.                                                                                       |
| Business (Payee)          | - Good Funds Model ensures when funds are received they are good and there is no additional risk to the Payee.  
                          | - Instant Settlement, no recourse or repudiation, combined with speed and low-cost of transactions.                                                                                                                                 |
| Payment System (ERP)      | - Good Funds Model, approval is instant.  
                          | - Minimal work for ERP provider to Authorize the Payer to complete a transaction.  
                          | - ERP provider already uses existing Payer Authorization process for each transaction, additional MintChip platform Authorization is incremental, providing additional security.  
                          | - Modification for a single customer makes it a potential feature for all other existing and new customers for the ERP provider.  
                          | - Enabling another method to initiate/receive payment increases ERP providers customer satisfaction.                                                                                                                                  |
| nanoPay (Proposer)        | - Good Funds Model eliminates requirement for Approval by Payer’s Provider making the process faster and easier for participants.  
                          | - Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
                          | - Back-end support costs are minimized                                                                                                                                                                                                     |
### Stage #5 Clearing

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition(Reason for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business (Payer)</td>
<td>- Good Funds Model, Clearing of each payment is virtually instant&lt;br&gt;- No additional clearing is required</td>
</tr>
<tr>
<td>Business (Payee)</td>
<td>- Good Funds Model, clearing is instant at time of payment initiating&lt;br&gt;- No additional clearing required&lt;br&gt;- Businesses will adopt this platform given the speed, certainty of payment and the cost savings associated with not having to monitor a clearing</td>
</tr>
<tr>
<td>nanoPay (Proposer)</td>
<td>- Good Funds Model eliminates requirement for traditional Clearing, making the process faster and easier for participants.&lt;br&gt;- Easy process minimizes transaction costs and increases flexibility around pricing and profitability&lt;br&gt;- Back-end support costs are minimized&lt;br&gt;- Delivers great user experience</td>
</tr>
</tbody>
</table>
### Stage #6 Receipt

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Business (Payer)**      | - MintChip provides transaction record/receipt immediately upon transaction initiation.  
- ERP system will determine how to handle MintChip transactions record/receipt  
- MintChip becomes an additional payment source within the ERP system  
- Non-ERP businesses will receive transaction record/receipt directly within MintChip application  
- Value to businesses is the instant creation of the receipt, the flexibility to work within existing ERP system and/or the ability for complete records stored in the businesses Secure Asset Store that can be easily accessed. |
| **Business (Payee)**      | - MintChip transaction record/receipt available to Payee immediately upon Payer transaction initiation.  
- ERP system will determine how to handle MintChip transactions record/receipt  
- Non-ERP businesses will receive transaction record/receipt directly into MintChip Secure Asset Store immediately upon receipt of funds  
- Value to businesses is the instant availability of the receipt, the flexibility to work within existing ERP system and/or the ability for complete transaction records/receipts to be stored in the businesses Secure Asset Store that can be easily accessed. |
| **Payment System (ERP)(POS)** | - No change to current receipt process. MintChip digital cash simply becomes a separate payment source.                                                                                                                                 |
| **nanoPay (Proposer)**    | - Platform’s ability to generate receipts instantly provides a strong user experience that will drive adoption of the platform.  
- Storage of all transactional activity by platform participants enables the ability to comply with all regulatory requirements enabling our ability to work with government agencies to secure support for platform adoption.  
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
- Back-end support costs are minimized  
- Opportunity to partner with analytics companies exists to provide value added services to participants on the platform. |
### Stage #7 Settlement

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Business (Payer)     | - MintChip is a Good Funds Model enabling Instant Settlement  
- Instant settlement is a very strong reason for adoption of the MintChip Platform  
- Great user experience  
- Low cost transaction with  
- Payments are irrevocable - finality of settlement |
| Business (Payee)     | - Instant settlement is a very strong reason for adoption of the MintChip Platform  
- Payee is assured of the value, no repudiation  
- Great user experience  
- Low cost transaction with  
- Payments are irrevocable - finality of settlement |
| Payment System       | - No involvement in Settlement by ERP system or POS system                                                                                                                                 |
| nanoPay (Proposer)   | - Good Funds Model minimizes traditional settlement requirements, making the process faster and easier for participants.  
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
- Instant settlement minimizes back-end support costs  
- Delivers great user experience |
### Stage #8 Reconciliation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Business (Payer)** | - All transaction information stored in ledgers within the Secure Asset Store  
- All data available for review under appropriate circumstances  
- Secured transaction data as outlined previously  
- Incremental data history and storage to any existing system  
- Value proposition is the easy access to any required transaction data  
- Business will feel confident in knowledge that any erroneous transactions can be investigated.  
- Easy to reconcile accounts and support electronic ledger  
- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity. |
| **Business (Payee)** | - All transaction information stores in ledgers within the Secure Asset Store  
- All data available for review upon following Due Process  
- Secured transaction data as outlined previously  
- Incremental data history and storage to any existing system  
- Value proposition is the easy access to any required transaction data  
- Business will feel confident in knowledge that any type of erroneous transactions can be investigated.  
- Easy to reconcile accounts and support electronic ledger  
- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity. |
| **Payment System (ERP)(POS)** | - Platform data incremental to transaction ERP/POS data  
- Reason for Adoption is the value added service to customers |
**nanoPay**  
(Proposer)

- Distributed ledger distribution model enables access to all transactional data for every user, for every transaction making reconciliation thorough, fast, and simple
- Enables resolution to any fraudulent, or otherwise disputed transactions which provides a good user experience, driving adoption.
- Opportunity exists to use transactional data to generate user insight and various economic trends creating an additional revenue source.

**Business to Person:**

Example Use Case:


Business to Person Transaction Flow  
(Diagram #21)
## Stage #1 Initiation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Business (Payer)                 | - Initiating payment can be completed through existing ERP system  
- MintChip digital cash becomes additional payment source in ERP system  
- Cost of completing (initiating) payment (Check) for businesses without ERP system greatly reduced.  
- Greater security than payment via check, instant availability of funds for Payee, easy to track receipt of payment  
- Streamlined process for initiating payment which may include remittance information |
| Person (Payee)                   | Payee will adopt due to immediate payment, low cost of payment processing, and overall platform efficiency.                                                                                                                           |
| POS System Provider              | No difference to current initiation process                                                                                                                                                                                                                           |
| PIN Entry Device Manufacturer    | No difference to current initiation process                                                                                                                                                                                                                           |
| Payment Processor                | No difference to current initiation process                                                                                                                                                                                                                           |
| nanoPay (Proposer)              | Increased adoption by ERP platforms enables easier adoption by Businesses using same ERP platform.  
Increased users drives increased adoption across businesses and creates other potential use cases (e.g. Payroll, Refund process, etc.)                                                                 |

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
### Stage #2 Authentication

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Business (Payer)**          | - Authentication occurs upon registering business on MintChip platform  
- Authentication process is easy for all businesses  
- All individual transactions are authenticated on the MintChip platform which is incremental to any existing Authentication processes used by the business |
| **Person (Payee)**            | - Authentication occurs on SAS registration.  
- Transactional authentication occurs on each access to platform                                                                                                           |
| **POS System Provider**       | - POS system only requires additional tender type to facilitate transaction  
- No additional incremental work required for Authenticating-                                                                                                             |
| **PIN Entry Device Manufacturer** | - No incremental work required                                                                                                                                               |
| **Payment Processor**         | - No incremental work required                                                                                                                                               |
| **nanoPay (Proposer)**        | - Secure Authentication process increases customers’ confidence and drives increased adoption of the MintChip platform  
- Already investigating ways to increase Authentication process using bio-metrics which provides value added revenue opportunity for nanoPay |
## Stage #3 Payer Authorization

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business (Payer)</strong></td>
<td>- The MintChip platform is a Good Funds model. Payer is Authorized to complete any transaction, instantly, up to the value of funds that exist in their SAS.</td>
</tr>
<tr>
<td></td>
<td>- Payer can enable pre-authorized payments and payer is sent confirmation immediately before payment being debited.</td>
</tr>
<tr>
<td></td>
<td>- Businesses will adopt this platform as it provides simple integration and increased flexibility for Payer Authorization.</td>
</tr>
<tr>
<td></td>
<td>- Businesses without ERP system will simply be Authorized on MintChip platform alone, a very quick and secure process.</td>
</tr>
<tr>
<td></td>
<td>- MintChip platform also has the capability to Authorize individual users within a single business to complete transactions while ensuring all user transactions are recorded.</td>
</tr>
<tr>
<td><strong>Person (Payee)</strong></td>
<td>- Payer Automatically Authorized at transaction initiation ensures when the Payee receives the funds they are instantly available.</td>
</tr>
<tr>
<td></td>
<td>- Payer will adopt the platform as it accelerates payment processing, they get their money faster.</td>
</tr>
<tr>
<td><strong>POS System Provider</strong></td>
<td>- No incremental work required</td>
</tr>
<tr>
<td></td>
<td>Value added service to customer</td>
</tr>
<tr>
<td><strong>PIN Entry Device Manufacturer</strong></td>
<td>- No incremental work required</td>
</tr>
<tr>
<td><strong>Payment Processor</strong></td>
<td>- No incremental work required</td>
</tr>
<tr>
<td><strong>nanoPay (Proposer)</strong></td>
<td>- Simple Authorization process minimizes transaction cost, and increases pricing flexibility and potential profit margin by minimizing back end support requirements. Simple Authorization process helps drives increased platform adoption and a better user experience.</td>
</tr>
</tbody>
</table>
### Stage #4 Approval by Payer’s Provider

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Business (Payer)**         | **MintChip platform is a Goods Fund Model. No approval by the Payer’s provider is required.**  
|                              | **If funds are available, transaction can be initiated, once initiated funds are good and can only be received by the Payee.**                                                                                                               |
| **Person (Payee)**           | **Good Funds Model ensures when funds are received they are good and there is no additional risk to the Payee.**  
|                              | **Instant Settlement, No recourse or repudiation combined with speed and cost of transactions are strong reasons the platform will be adopted.**                                                                                      |
| **POS System Provider**      | **Good Funds Model, approval is instant, POS system will process transaction as if they had received traditional cash.**                                                                                                           |
|                              | **POS system providers will want to meet their customer’s demands by enabling another payment source through the POS system.**                                                                                                               |
| **PIN Entry Device Manufacturer** | **Facilitates communication only, not involved directly in approval process**                                                                                                                                                          |
| **Payment Processor**        | **No incremental work required**                                                                                                                                                                                                       |
| **nanoPay (Proposer)**       | **Good Funds Model eliminates requirement for Approval by Payer’s Provider making the process faster and easier for participants.**                                                                                                       |
|                              | **Easy process minimizes transaction costs and increases flexibility around pricing and profitability**                                                                                                                              |
|                              | **Back-end support costs are minimized**                                                                                                                                                                                                  |
## Stage #5 Clearing

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business(Payer)</td>
<td>- Good Funds Model, payment instantly cleared</td>
</tr>
</tbody>
</table>
| Person(Payee)     | - Good Funds Model, clearing is virtually instant  
- No additional clearing required  
- Payee has instant access to full value of transaction, with no holds on funds  
- Payment is more secure than check  
- Timing of receipt of payment is predictable, ensured  
- Businesses will adopt this platform given the speed and certainty around a payment and the cost savings associated with not having to monitor a payment clearing process |
| POS Provider      | - Good Funds Model, payment instantly cleared  |  |
| Payment Processor | - No involvement Required  |  |
| nanoPay (Proposer)| - Good Funds Model eliminates requirement for traditional Clearing Process making the process faster and easier for participants.  
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
- Back-end support costs are minimized  
- Delivers great user experience |
### Stage #6 Receipt

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Business (Payer)             | - MintChip provides transaction record/receipt immediately upon transaction initiation.  
                               | - ERP system will determine how to handle MintChip transactions record/receipt  
                               | - MintChip simply becomes a separate payment source within the ERP system  
                               | - Non-ERP businesses will receive transaction record/receipt directly within MintChip application utilized to complete transaction  
                               | - Value to businesses is the instant creation of the receipt, the flexibility to work within existing ERP system and/or the ability for complete records stored in the businesses Secure Asset Store that can be easily accessed. |
| Person (Payee)               | - MintChip transaction record/receipt available to Payee immediately upon Payer transaction initiation.  
                               | - Person will receive transaction record/receipt directly into MintChip Secure Asset Store immediately upon receipt of funds  
                               | - Value to person is the instant availability of the receipt, the ability for complete transaction records for all activity (Credits and Debits) within the Secure Asset Store that can be easily accessed via the MintChip application. |
| POS System Provider          | Transaction records incremental to existing records  
                               | - No incremental activity required                                                                                                                                                                                                  |
| PIN Entry Device (PED)       | - No incremental activity required                                                                                                                                                                                                   |
| Payment Processor            | - No incremental activity required                                                                                                                                                                                                   |
| nanoPay (Proposer)           | - Platforms ability to generate receipts instantly provides a strong user experience that will drive adoption of the platform.  
                               | - Storage of all transactional activity by platform participants enables the ability to comply with all regulatory requirements enabling our ability to work with |
government agencies to secure support for platform adoption.

- Easy process minimizes transaction costs and increases flexibility around pricing and profitability
- Back-end support costs are minimized
- Opportunity to partner with analytics companies exists to provide value added services to participants on the platform.

## Stage #7 Settlement

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business (Payer)</td>
<td>- MintChip is a Good Funds Model enabling Instant Settlement of the transaction</td>
</tr>
<tr>
<td></td>
<td>- No inter-bank settlement required</td>
</tr>
<tr>
<td></td>
<td>- Instant settlement is a very strong reason for adoption of the MintChip Platform</td>
</tr>
<tr>
<td></td>
<td>- Receiver is assured of the value, no repudiation</td>
</tr>
<tr>
<td></td>
<td>- Great user experience</td>
</tr>
<tr>
<td></td>
<td>- Low cost transaction</td>
</tr>
<tr>
<td></td>
<td>- Payments are irrevocable - finality of settlement</td>
</tr>
<tr>
<td>Person (Payee)</td>
<td>- MintChip is a Good Funds Model enabling Instant Settlement</td>
</tr>
<tr>
<td></td>
<td>- Instant settlement is a very strong reason for adoption of the MintChip Platform</td>
</tr>
<tr>
<td></td>
<td>- Receiver is assured of the value, no repudiation</td>
</tr>
<tr>
<td></td>
<td>- Great user experience</td>
</tr>
<tr>
<td></td>
<td>- Low cost transaction</td>
</tr>
<tr>
<td></td>
<td>- Payments are irrevocable - finality of settlement</td>
</tr>
<tr>
<td>POS System Provider</td>
<td>- Not involved in settlement process</td>
</tr>
</tbody>
</table>
### PIN Entry Device Manufacturer
- Not involved in settlement process

### Payment Processor
- Facilitates information exchange only, not directly involved in settlement process

### nanoPay (Proposer)
- Good Funds Model minimizes traditional settlement requirements making the process faster and easier for participants.
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability
- Instant settlement minimizes back-end support costs
- Delivers great user experience

### Stage #8 Reconciliation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business (Payer)</td>
<td>- All transaction information stores in ledgers within the Secure Asset Store</td>
</tr>
<tr>
<td></td>
<td>- All data available for review upon following Due Process</td>
</tr>
<tr>
<td></td>
<td>- Secured transaction data</td>
</tr>
<tr>
<td></td>
<td>- Incremental data history and storage to any existing system</td>
</tr>
<tr>
<td></td>
<td>- Value proposition is the easy access to any required transaction data</td>
</tr>
<tr>
<td></td>
<td>- Users will feel confident in knowledge that any type of erroneous transactions can be investigated.</td>
</tr>
<tr>
<td></td>
<td>- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity.</td>
</tr>
<tr>
<td>Person (Payee)</td>
<td>- All transaction information stores in ledgers within the Secure Asset Store</td>
</tr>
<tr>
<td></td>
<td>- All data available for review upon following Due Process</td>
</tr>
<tr>
<td></td>
<td>- Secured transaction data as outlined previously</td>
</tr>
<tr>
<td></td>
<td>- Incremental data history and storage to any existing system</td>
</tr>
</tbody>
</table>
### Value proposition
- Easy access to any required transaction data
- Users will feel confident in knowledge that any type of erroneous transactions can be investigated.
- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity.

### POS System Provider
- MintChip transactional data will be incremental to any POS reconciliation data
- Reason for Adoption is the value added service to customers

### PIN Entry Device (PED) Manufacturer
- MintChip transactional data will be incremental to any PED reconciliation data
- Reason for Adoption is the value added service to customers

### Payment Processor
- MintChip transactional data will be incremental to any Payment Processor reconciliation data
- Reason for Adoption is the value added service to customers

### nanoPay (Proposer)
- Distributed ledger distribution model enables access to all transactional data for every user, for every transaction making reconciliation thorough, fast, and simple
- Enables resolution to any fraudulent, or otherwise disputed transactions which provides a good user experience, driving adoption.
- Opportunity exists to use transactional data to generate user insight and various economic trends creating an additional revenue source.
**Person to Business:**

Example Use Case:

1. Consumer makes a purchase at a bricks-and-mortar retail location.
## Stage #1 Initiation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person (Payer)    | - Person can enable access to MintChip platform by simply downloading application through Broker’s site.  
- Initiating transaction to business easily completed by selecting “Pay Merchant” from menu  
- Person then simply scans (IOS) or Taps (Android) phone on PIN Entry Device (PED) to initiate transaction.  
- Push payments to other Payees (billers) also easy to complete, certainty that biller receives notification of payment in real time  
- Electronic digital cash transaction provides convenient method to initiate and complete transaction.  
- No need for physical card only mobile device  
- No reliance on provision of credit, danger of overdraft or NSF  
- Business will provide incentive to Person to use low-cost transaction method |
| Business (Payee)  | - Initiating payment can be completed through existing POS system  
- MintChip digital cash simply becomes different payment source in POS system  
- Cost of initiating payment for businesses exactly same as current process, MintChip digital cash simply becomes another tender/payment type  
- Capability exists to complete pre-authorized payments  
- Low-to-no interchange fee  
- No chargeback rights, no increased “card not present” transactions  
- Lower fraud risk - mobile device more secure than card  
- Businesses will adopt platform for reduced transaction costs and minimal integration work required. |
| POS System Provider | - Required to add additional tender type within POS system  
- Value added system capability that will drive customer satisfaction |
### PIN Entry Device (PED) Manufacturer
- Integration required to route transaction to MintChip platform
- Partnership already established with Ingenico
- PED manufacturer can share in monthly fees charged to business

### Payment Processor
- Potential integration required to route transaction to MintChip platform
- Value added service provided to existing customer
  -- Potential opportunity for small share of monthly revenue

### nanoPay (Proposer)
- Increased adoption by businesses enables easier adoption by Persons to participate on the platform.
- Easy payment initiation process will help drive increased platform adoption

## Stage #2 Authentication

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person (Payer)</td>
<td>- Authentication occurs on SAS registration.</td>
</tr>
<tr>
<td></td>
<td>- Transactional authentication occurs on each access to platform</td>
</tr>
<tr>
<td>Business (Payee)</td>
<td>- Authentication occurs on SAS registration.</td>
</tr>
<tr>
<td></td>
<td>- Transactional authentication occurs on each access to platform</td>
</tr>
<tr>
<td></td>
<td>- More robust than PIN, signature and PIN or signature</td>
</tr>
<tr>
<td>POS System Provider</td>
<td>- Not involved in authentication</td>
</tr>
<tr>
<td>PIN Entry Device Manufacturer</td>
<td>- Not involved in authentication</td>
</tr>
<tr>
<td>Payment Processor</td>
<td>- Not involved in authentication</td>
</tr>
<tr>
<td></td>
<td>- Value added service to business</td>
</tr>
<tr>
<td></td>
<td>- Potential Revenue Generation</td>
</tr>
</tbody>
</table>
nanoPay (Proposer)  
- Secure Authentication process increases customers’ confidence and drives increased adoption of the MintChip platform  
- Already investigating ways to increase Authentication process using bio-metrics which provides value added revenue opportunity for nanoPay

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person (Payer)                   | - Payer Automatically Authorized upon entry into the MintChip platform  
- Good Funds model immediately authorizes transactions up to the balance of funds within a person’s Secure Asset Store  
- Payer will adopt the platform as value of possible transaction is immediately known and visible and it allows them to send their money faster providing a great user experience |
| Business (Payee)                 | - Payer Automatically Authorized at transaction initiation ensures when the Payee receives the funds they are instantly available.  
- Payer will adopt the platform as it accelerates payment processing, they get their money faster.  
- lower fraud rates than traditional form factors |
| POS System Provider              | - Not involved in Payer authorization                                                                                                                                                                                                |
| PIN Entry Device(PED)Manufacturer | - Not involved in Payer authorization                                                                                                                                                                                                |
| Payment Processor                | - Not involved in Payer authorization                                                                                                                                                                                                |
| nanoPay (Proposer)               | - Simple Authorization process minimizes transaction cost, and increases pricing flexibility and potential profit margin by minimizing back end support requirements. Simple Authorization process helps drives increased platform adoption and a better user experience. |
### Stage #4 Approval by the Payer’s Provider

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person (Payer)</td>
<td>- MintChip platform is a Goods Fund Model. No approval by the Payer’s provider is required.</td>
</tr>
<tr>
<td></td>
<td>- If funds are available, transaction can be initiated, once initiated funds are good and can only be received by the Payee.</td>
</tr>
<tr>
<td>Business (Payee)</td>
<td>- Good Funds Model ensures when funds are received they are good and there is no additional risk to the Payee.</td>
</tr>
<tr>
<td></td>
<td>- Instant Settlement, no recourse or repudiation combined with speed and cost of transactions are strong reasons the platform will be adopted.</td>
</tr>
<tr>
<td></td>
<td>- Low-to-no interchange cost</td>
</tr>
<tr>
<td>POS System Provider</td>
<td>- Not involved in Approval by Payer’s provider</td>
</tr>
<tr>
<td>PIN Entry Device Manufacturer</td>
<td>- Not involved in Approval by Payer’s provider</td>
</tr>
<tr>
<td>Payment Processor</td>
<td>- Not involved in Approval by Payer’s provider</td>
</tr>
<tr>
<td>nanoPay (Proposer)</td>
<td>- Good Funds Model eliminates requirement for Approval by Payer’s Provider making the process faster and easier for participants.</td>
</tr>
<tr>
<td></td>
<td>- Easy process minimizes transaction costs and increases flexibility around pricing and profitability</td>
</tr>
<tr>
<td></td>
<td>- Back-end support costs are minimized</td>
</tr>
</tbody>
</table>
### Stage #5 Clearing

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person (Payer)</td>
<td>- Good Funds Model, clearing is virtually instant at time of payment initiation  &lt;br&gt;- No additional clearing required  &lt;br&gt;- Person will adopt this platform given the speed and certainty in sending a payment  &lt;br&gt;- Never a question of funds not being able to be received provides certainty for the Person and provides an excellent user experience  &lt;br&gt;- No NSF fee or overdraft/over limit concerns</td>
</tr>
<tr>
<td>Business (Payee)</td>
<td>- Good Funds Model, clearing is instant at time of payment initiating  &lt;br&gt;- No additional clearing required  &lt;br&gt;- Businesses will adopt this platform given the speed and certainty around a payment and the cost savings associated with not having to monitor a payment clearing process</td>
</tr>
<tr>
<td>POS System Provider</td>
<td>- Clears transaction similar to a cash transaction  &lt;br&gt;- Provides value added service to customer</td>
</tr>
<tr>
<td>PIN Entry Device (PED)</td>
<td>- Not directly involved in the clearing process</td>
</tr>
<tr>
<td>Payment Processor</td>
<td>- Not directly involved in the clearing process</td>
</tr>
<tr>
<td>nanoPay (Proposer)</td>
<td>- Good Funds Model eliminates requirement for traditional Clearing Process making the process faster and easier for participants.  &lt;br&gt;- Easy process minimizes transaction costs and increases flexibility around pricing and profitability  &lt;br&gt;- Back-end support costs are minimized  &lt;br&gt;- Delivers great user experience</td>
</tr>
</tbody>
</table>
## Stage #6 Receipt

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Person (Payer)**   | - Person will receive transaction record/receipt directly into MintChip Secure Asset Store immediately upon initiating transaction  
                       - Value to person is the instant availability of the receipt, the ability for complete transaction records for all activity (Credits and Debits) within the Secure Asset Store that can be easily accessed via the MintChip application.                                      |
| **Business (Payee)** | - MintChip transaction record/receipt available to Payee immediately upon Payer transaction initiation.                                                                                                                                  
                       - ERP or POS system will determine how to handle MintChip transactions record/receipt  
                       - Non-ERP or POS system businesses (e.g. online) will receive transaction record/receipt directly into MintChip Secure Asset Store immediately upon receipt of funds  
                       - Value to businesses is the instant availability of the receipt, the flexibility to work within existing ERP/POS systems and/or the ability for complete transaction records/receipts to be stored in the businesses Secure Asset Store that can be easily accessed.  
                       - Transaction records can be maintained regardless of distribution channel utilized to complete transaction with person.                                                                 |
| **POS System Provider** | - MintChip simply an additional payment type within POS system. This has been confirmed and implemented with multiple POS providers.                                                                                      |
| **PIN Entry Device (PED) Manufacturer** | - Facilitates communication with MintChip platform to enable transaction  
                       - Delivers transaction information directly to POS system  
                       - Partnership agreement already in place with Ingenico  
                       - Value Proposition for PED manufacturer includes sharing in monthly revenue charge to Business by nanoPay  
                       - Value added service to customer base |
### Payment Processor
- Directs transaction information to MintChip platform to enable transaction
- Communicates through PED device with POS system for transaction completion
- Value proposition includes sharing in monthly revenue charged to Business by nanoPay

### nanoPay (Proposer)
- Platforms ability to generate receipts instantly provides a strong user experience that will drive adoption of the platform.
- Storage of all transactional activity by platform participants enables the ability to comply with all regulatory requirements enabling our ability to work with government agencies to secure support for platform adoption.
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability
- Back-end support costs are minimized
- Opportunity to partner with analytics companies exists to provide value added services to participants on the platform.

### Stage #7 Settlement

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person (Payer) | - MintChip is a Good Funds Model enabling virtually Instant Settlement because there is no need for inter-bank transfer within the ecosystem.  
                 - Instant settlement across the platform is a very strong reason for adoption of the MintChip Platform  
                 - Great user experience  
                 - Low cost transaction  
                 - Payments are irrevocable - finality of settlement                                               |
| Business (Payee)| - Lack of inter-bank settlement means value available instantly  
                 - Receiver is assured of the value, no repudiation                                                |
### In Pursuit of a Better Payment System

**Faster Payments Task Force**

|                | -Great user experience  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-Low cost transaction</td>
</tr>
<tr>
<td></td>
<td>Payments are irrevocable - finality of settlement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>POS System Provider</th>
<th>-Not directly involved in the settlement process</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>PIN Entry Device Manufacturer</th>
<th>-Not directly involved in the settlement process</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Payment Processor</th>
<th>-Facilitates information exchange only, not directly involved in settlement process</th>
</tr>
</thead>
</table>

| nanoPay (Proposer) | -Good Funds Model minimizes traditional settlement requirements making the process faster and easier for participants.  
|---------------------|--------------------------------------------------------------------------------|
|                     | -Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
|                     | -Lack of inter-bank settlement minimizes back-end support costs  
|                     | -Delivers great user experience |

### Stakeholder Value Proposition (Reasons for Adoption)

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition</th>
</tr>
</thead>
</table>
| Person(Payer) | -All transaction information stores in ledgers within the Secure Asset Store  
|             | -All data available for review when applicable  
|             | -Secured transaction data as outlined previously  
|             | -Incremental data history and storage to any existing system  
|             | -Value proposition is the easy access to any required transaction data  
|             | -Users will feel confident in knowledge that transaction errors can be investigated.  
|             | -Immediate electronic notification of transaction across multiple platforms provides |

---

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
<table>
<thead>
<tr>
<th>Role</th>
<th>Features</th>
<th>Value Proposition</th>
</tr>
</thead>
</table>
| Business (Payee)                   | - All transaction information stores in ledgers within the Secure Asset Store  
- All data available for review upon following Due Process  
- Secured transaction data as outlined previously  
- Incremental data history and storage to any existing system  
- Value proposition is the easy access to any required transaction data  
- Users will feel confident in knowledge that any transaction errors can be investigated.  
- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity. |                                                                                   |
| POS System Provider                | - MintChip transactional data will be incremental to any POS reconciliation data  
- Reason for Adoption is the value added service to customers |                                                                                   |
| PIN Entry Device (PED) Manufacturer | - MintChip transactional data will be incremental to any PED reconciliation data  
- Reason for Adoption is the value added service to customers |                                                                                   |
| Payment Processor                  | - MintChip transactional data will be incremental to any Payment Processor reconciliation data  
- Reason for Adoption is the value added service to customers |                                                                                   |
| nanoPay (Proposer)                 | - Distributed ledger distribution model enables access to all transactional data for every user, for every transaction making reconciliation thorough, fast, and simple  
- Enables resolution to any fraudulent, or otherwise disputed transactions which provides a good user experience, driving adoption.  
- Opportunity exists to use transactional data to generate user insight and various economic trends creating an additional revenue source. |                                                                                   |
**Person to Person:**

The MintChip ecosystem was designed so that all payments occur on a bilateral basis, making it ideal for peer-to-peer (P2P) payments. End Users register with accounts and are provided a Secure Assets Store (SAS) specifically tied to their identity. Transactions on the MintChip platform are simply a transfer of value between two SASs. P2P transactions are completed in real time and can be initiated quickly and easily through the MintChip application. Every transaction is processed in the same manner, is subject to the same security requirements, and delivers the same user experience. (U.3)

For the End Users, the overall value of the MintChip ecosystem is the combination of convenience, speed, irrevocability and low cost. And, while a Broker is required for the topping-up and offloading MintChip USD, there are no intermediaries involved in the clearing and settlement of funds within the MintChip ecosystem.

Example Use Case:

Person to Person transfer using same currency

---

Person to Person Transaction Flow
(Diagram # 23 )
## Stage #1 Initiation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Person (Payer)</strong></td>
<td>- Person can enable access to MintChip platform by simply downloading application through Brokers site. &lt;br&gt; - Initiating transaction to another person as simple as selecting “Sending Money” from menu, or selecting person from list of favorites within the application &lt;br&gt; - Once Payee is selected Payer simply enters amount to transfer then presses “Send” to initiate payment. &lt;br&gt; - Electronic digital cash transaction provides convenient method to initiate and complete transaction. &lt;br&gt; - No need for physical card only mobile device.</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>Value Proposition (Reasons for Adoption)</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
</tbody>
</table>
| Person (Payer) | - Simple, one-time, account registration process on MintChip ecosystem.  
                  - Authentication occurs upon opening application.  
                  - If Person is using application embedded within a Broker application the Person will have to be Authenticated by the Broker in addition to the MintChip Authentication  
                  - Already in discussion to utilize biometric authentication of user.  
                  - Increased Authentication provides Payer confidence in the platform security and provides an excellent user experience. |
| Person (Payee) | - Simple, one-time, account registration process on MintChip ecosystem.  
                   - Authentication occurs upon opening application.  
                   - If Person is using application embedded within a Broker application the Person will have to be Authenticated by the Broker in addition to the MintChip Authentication.  
                   - Already in discussion to utilize biometric authentication of user.  
                   - Increased Authentication provides Payee confidence in the platform security and provides an excellent user experience. |
| nanoPay (Proposer) | - Secure Authentication process increases customers’ confidence and drives increased adoption of the MintChip platform  
                        - Already investigating ways to increase Authentication process using bio-metrics which provides value added revenue opportunity for nanoPay  
                        - Simple process adds secure and increased capabilities to investigate fraudulent or suspicious transactions further driving compliance with regulations |
### Stage #3 Payer Authorization

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Person(Payer)** | - Payer Automatically Authorized upon entry into the MintChip platform  
| | - Good Funds model immediately authorizes transactions up to the balance of funds within Payer’s Secure Asset Store  
| | - Payer will adopt the platform as the value of possible transaction is immediately known and visible.  
| | - Process is as simple as using cash and provides a great user experience  
| **Person(Payee)** | - Payee will always receive good funds, full amount available for immediate use  
| | - No risk of payment being returned NSF  
| | - Funds are immediate and received with certainty providing a great user experience  
| **nanoPay (Proposer)** | - Simple Authorization process minimizes transaction cost, and increases pricing flexibility and potential profit margin by minimizing back end support requirements - Simple Authorization process helps drives increased platform adoption and a better user experience. |

### Stage #4 Approval by the Payer’s Provider

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Person(Payer)** | - MintChip platform is a Goods Fund Model. No approval by the Payer’s provider is required.  
| | - If funds are available, transaction can be initiated, once initiated funds are good and can only be received by the Payee.  
| | - People will adopt this platform due to the speed and certainty of a transaction.  
| **Person(Payee)** | - Good Funds Model ensures when funds are received they are good and there is no additional risk to the Payee. |
- Instant Settlement, No recourse or repudiation combined with speed and cost of transactions are strong reasons the platform will be adopted.

**nanoPay (Proposer)**
- Good Funds Model eliminates requirement for Approval by Payer’s Provider making the process faster and easier for participants.
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability
- Back-end support costs are minimized
- Delivers great user experience

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| **Person(Payer)** | - Good Funds Model, clearing is instant at time of payment initiation  
- No additional clearing required  
- Person will adopt this platform given the speed and certainty in sending a payment  
- Never a question of funds being received provides certainty for the Person and provides an excellent user experience  
- No clearing process required  
- Fast  
- No hassle  
- No risk of receiving invalid funds  
- Funds immediately available upon receipt |
| **Person(Payee)** | - Good Funds Model, clearing is instant at time of payment initiating  
- No additional clearing required Payee know the funds are good  
- Simplicity of receipt of funds will drive adoption |
### In Pursuit of a Better Payment System

**Faster Payments Task Force**

| nanoPay (Proposer) | - Good Funds Model eliminates requirement for traditional Clearing Process making the process faster and easier for participants.  
| | - Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
| | - Back-end support costs are minimized  
| | - Delivers great user experience |

#### Stage #6 Receipt

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person (Payer) | - MintChip transaction record/receipt delivered into Payer Secure Asset Store immediately upon transaction initiation.  
| | - Value Proposition to person is the instant availability of the receipt, the ability for complete transaction records for all activity (Credits and Debits) within the Secure Asset Store that can be easily accessed via the MintChip application.  
| | - Great user experience  
| | - Simple and convenient way to store paperless receipts/transaction.  
| | - Multiple notifications ensure user is aware of all account activity  
| | - Transaction data can be leveraged for other electronic uses (budgeting, projecting, etc....) |
| Person (Payee) | - MintChip transaction record/receipt available to Payee immediately upon Payer transaction initiation.  
| | - Person will receive transaction record/receipt directly into MintChip Secure Asset Store immediately upon receipt of funds.  
| | - Value to person is the instant availability of the receipt, the ability for complete transaction records for all activity (Credits and Debits) within the Secure Asset Store that can be easily accessed via the MintChip application.  
| | - Great user experience  
<p>| | - Simple and convenient way to store paperless receipts/transaction. |</p>
<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person(Payer) | - MintChip is a Good Funds Model enabling Instant Settlement because there is no need for inter-bank settlement  
- Instant settlement is a very strong reason for adoption of the MintChip Platform  
- Receiver is assured of the value, no repudiation  
- Great user experience  
- Low cost transaction with  
- Payments are irrevocable - finality of settlement |
| Person(Payee) | - MintChip is a Good Funds Model enabling Instant Settlement  
- Instant settlement is a very strong reason for adoption of the MintChip Platform  
- Receiver is assured of the value, no repudiation |

- Multiple notifications ensure user is aware of all account activity  
- Transaction data can be leveraged for other electronic uses (budgeting, projecting, etc....)  
- Platforms ability to generate receipts instantly provides a strong user experience that will drive adoption of the platform  
- Storage of all transactional activity by platform participants enables the ability to comply with all regulatory requirements enabling our ability to work with government agencies to secure support for platform adoption  
- Easy process minimizes transaction costs and increases flexibility around pricing and profitability  
- Back-end support costs are minimized  
- Opportunity to partner with analytics companies exists to provide value added services to participants on the platform.

**Stage #7 Settlement**

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person(Payer) | - MintChip is a Good Funds Model enabling Instant Settlement because there is no need for inter-bank settlement  
- Instant settlement is a very strong reason for adoption of the MintChip Platform  
- Receiver is assured of the value, no repudiation  
- Great user experience  
- Low cost transaction with  
- Payments are irrevocable - finality of settlement |
| Person(Payee) | - MintChip is a Good Funds Model enabling Instant Settlement  
- Instant settlement is a very strong reason for adoption of the MintChip Platform  
- Receiver is assured of the value, no repudiation |
Great user experience
Low cost transaction with
Payments are irrevocable - finality of settlement

nanoPay (Proposer)
Good Funds Model minimizes traditional settlement requirements making the process faster and easier for participants.
Easy process minimizes transaction costs and increases flexibility around pricing and profitability
Instant settlement minimizes back-end support costs
Delivers great user experience

Stage #8 Reconciliation

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Value Proposition (Reasons for Adoption)</th>
</tr>
</thead>
</table>
| Person (Payer) | - All transaction information stores in ledgers within the Secure Asset Store  
- All data available for review when required  
- Secured transaction data as outlined previously  
- Incremental data history and storage to any existing system  
- Value proposition is the easy access to any required transaction data  
- Users will feel confident in knowledge that any transaction errors can be investigated.  
- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity. |
| Person (Payee) | - All transaction information stores in ledgers within the Secure Asset Store  
- All data available for review when required  
- Secured transaction data as outlined previously  
- Incremental data history and storage to any existing system  
- Value proposition is the easy access to any required transaction data |
- **Users** will feel confident in knowledge that any transaction errors can be investigated.
- Immediate electronic notification of transaction across multiple platforms provides user immediate knowledge of fraudulent activity.

| nanoPay (Proposer) | - Distributed ledger distribution model enables access to all transactional data for every user, for every transaction making reconciliation thorough, fast, and simple
- Enables resolution to any fraudulent, or otherwise disputed transactions which provides a good user experience, driving adoption.
- Opportunity exists to use transactional data to generate user insight and various economic trends creating an additional revenue source. |
3. Integration Effort

The MintChip ecosystem is a self-contained end-to-end payment system. Key points of integration are required to support each use case (B2P, B2B, B2P, P2P). These integration points are critical to: 1) provide on and off-ramps to connect to existing payments industry depository or non-bank account providers; and 2) connect to key stakeholder systems.

**Business to Business**

MintChip open APIs enable stakeholders to integrated good funds digital cash payments into existing systems for use cases such as:
- Invoicing their customers
- Enterprise Resource Planning
- Tax Accounting platforms

Business to Business Transaction Flow
(Diagram #24)
<table>
<thead>
<tr>
<th>Lifecycle Stage</th>
<th>Integration</th>
<th>Effort</th>
</tr>
</thead>
</table>
| Initiation              | - End User (Payer and Payee) creates MintChip digital cash accounts to facilitate transfer  
- ACH integration to move money from Business Account to MintChip digital cash account to process payment (U.1)  
- Integration to ERP system for invoicing End User (Payee) to send invoice (payment request) to Payer  
- End User (Payer) initiates payment from ERP system selecting digital cash as payment source (E.2)  
- ACH integration to move money from Payee’s MintChip digital cash account to Business Account to process deposit (U.1)                                                                 | - weeks |
| Authentication          | - Payer and Payee are authenticated using email address and mobile phone number                                                                                                                                                                                                                                                           | - n/a  |
| Payer Authorization     | - Payee create a Value Request Message that sends payment request to Payer  
- Payer authorizes the payment in MintChip  
- Value Transfer Message is generated to send payment to Payee                                                                                                                                                                                                                     | - n/a  |
| Approval by the Payer’s Provider | - MintChip is a Good Funds system and therefore a balance lookup is required to determine the maximum amount of a payment that can be processed                                                                                                                                                                                                                         | - n/a  |
| Clearing                | - Clearing in instantaneous, as both the Payer and Payee account information resides on the same MintChip platform so payment information to confirm the transaction for settlement is included in the Value Transfer Message.                                                                                                                                                  | - n/a  |
| Receipt                 | - Payee will received immediate notification of the payment using Email or Direct Messaging                                                                                                                                                                                                                                             | - n/a  |
| Settlement              | - When a Value Transfer Message is created, value is immediately debited from the Payer’s Secure Asset Store. The Value Transfer Message can only                                                                                                                     | - n/a  |
be accepted by the Payee. Once accepted (manually or automatically), the
digital cash is loaded into the Payee’s Secure Asset Store, and at that point
the Settlement is completed.

| Reconciliation | -One Settlement is complete, a detailed record of the transaction is stored in
the ledger of both the Payer and Payee’s Secure Asset Store. MintChip
digital cash payments are irrevocable and disputed payments must be
resolved by each party. | -n/a |

**Business to Person**

MintChip open APIs enable stakeholders to integrated good funds digital cash payments into
existing systems for use cases such as:

- Wage disbursements
- Insurance, health care, claim settlement
- Cash back provided by Retailers

**Business to Person Transaction Flow**

(Diagram # 25)
# Business to Person Lifecycle Stage

<table>
<thead>
<tr>
<th>Lifecycle Stage</th>
<th>Integration</th>
<th>Effort</th>
</tr>
</thead>
</table>
| **Initiation**               | - End User (Payer and Payee) creates MintChip digital cash accounts to facilitate transfer  
                                - ACH integration to move money from Business Account to MintChip digital cash account to process payment (U.1)  
                                - Integration to Enterprise Back End or ERP system to set up and manage payments  
                                - End User (Payer) triggers manual or automated payments from Back End or ERP system selecting digital cash as payment source (E.2)  
                                - ACH integration to move money from Payee’s MintChip digital cash account to Business Account to process deposit (U.1)                                                                 | - weeks   |
| **Authentication**           | - Payer and Payee are authenticated using email address and mobile phone number                                                                                                                                 | -n/a      |
| **Payer Authorization**      | - Payer authorizes the payment in MintChip  
                                - Payer creates Value Transfer Message that sends payment to Payee                                                                                                                                 | -n/a      |
| **Approval by the Payer’s Provider** | - MintChip is a Good Funds system and therefore a balance lookup is required to determine the maximum amount of a payment that can be processed                                                                                                                                 | -n/a      |
| **Clearing**                 | - Clearing in instantaneous, as both the Payer and Payee account information resides on the same MintChip platform so payment information to confirm the transaction for settlement is included in the Value Transfer Message                                                                 | -n/a      |
| **Receipt**                  | - Payee will receive immediate notification of the payment using Email or Direct Messaging                                                                                                                                 | -n/a      |
| **Settlement**               | - Digital cash is immediately debited from the Payer’s Secure Asset Store and loaded into a Value Transfer Message that can be only be accepted by the Payee. Once accepted, the digital cash is loaded into the Payee’s                                                                 | -n/a      |
Secure Asset Store and at that point the Settlement is completed.

| Reconciliation | -One Settlement is complete, a detailed record of the transaction is stored in the ledger of both the Payer and Payee’s Secure Asset Store. MintChip digital cash payments are irrevocable and disputed payments must be resolved by each party. | -n/a |

**Person to Business**

MintChip open APIs enable stakeholders to integrated good funds digital cash payments into existing systems for use cases such as:

- Bill payments
- POS payments at bricks-and-mortar retailer
- Online ecommerce purchase

**Person to Business Transaction Flow**

(Diagram #26)
<table>
<thead>
<tr>
<th>Lifecycle Stage</th>
<th>Integration</th>
<th>Effort</th>
</tr>
</thead>
</table>
| Initiation     | - End User (Payer and Payee) creates MintChip digital cash accounts to facilitate transfer  
- ACH integration to move money from End User’s depositary Account to MintChip digital cash account (U.1)  
- Payment Processor integration to enable in-app top up of MintChip account from credit and debit cards (U.1)  
- Integration to Merchant POS to accept MintChip digital cash as payment tender type (integrated POS) (E.2)  
- Integration to POS Payment Terminal to accept MintChip digital cash as payment tender type (standalone) (E.2)  
- End User (Payer) initiates payment from Mobile App to Merchant using NFC, barcode, Bluetooth as similar delivery mechanism (U.1)(E.2) | - weeks |
| Authentication | - Payer (Consumer) is authenticated using email address and mobile phone number  
- Payee (Merchant) are authenticated using TLS Certificates loaded onto the POS Payment Terminal | - n/a |
| Payer Authorization | - Payee (Merchant) creates a Value Request Message via NFC, Barcode, or Bluetooth that sends payment request to Payer  
- Payer authorizes the payment in MintChip  
- Payer creates Value Transfer Message that sends payment to Payee | - n/a |
<p>| Approval by the Payer’s Provider | - MintChip is a good funds system and therefore a balance lookup is required to determine the maximum amount of a payment that can be processed | - n/a |
| Clearing | - Clearing is instantaneous, as both the Payer and Payee account information reside on the same MintChip platform so payment information to confirm the transaction for settlement is included in the Value Transfer Message | - n/a |</p>
<table>
<thead>
<tr>
<th>Receipt</th>
<th>-Payee will received immediate notification of payment by Direct Messaging</th>
<th>-n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settlement</td>
<td>-Settlement in instantaneous. Digital cash is immediately debited from the Payer’s (Consumer) Secure Asset Store and Payee’s (Merchant or Biller) Secure Asset Store.</td>
<td>-n/a</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>-One Settlement is complete, a detailed record of the transaction is stored in the ledger of both the Payer and Payee’s Secure Asset Store. MintChip digital cash payments are irrevocable and disputed payments must be resolved by each party.</td>
<td>-n/a</td>
</tr>
</tbody>
</table>
MintChip open APIs enable stakeholders to integrate good funds digital cash payments into existing systems for use cases such as:

- P2P payments domestically
- Bill splitting
- P2P payments cross-border (optional foreign exchange)

Person to Person Transaction Flow
(Diagram # 27)

<table>
<thead>
<tr>
<th>Lifecycle Stage</th>
<th>Integration</th>
<th>Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>- End Users create MintChip digital cash accounts to send P2P payments</td>
<td>- weeks</td>
</tr>
<tr>
<td></td>
<td>- ACH integration to move money from End User’s depositary Account to MintChip digital cash account (U.1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Payment Processor integration to enable top up of MintChip account from credit and debit cards (U.1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- End User (Sender) initiates payment from Mobile App or Web application to Recipient (E.2)</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>-Sender and Recipient are authenticated using email address and mobile phone number</td>
<td>-n/a</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| Payer Authorization    | -Payer authorizes the payment in MintChip by selecting Recipient and amount to send  
                           -Payer creates Value Transfer Message that sends payment to Payee | -n/a |
| Approval by the Payer’s Provider | -MintChip is a Good Funds system and therefore a balance lookup is required to determine the maximum amount of a payment that can be processed | -n/a |
| Clearing               | -Clearing is instantaneous, as reside on the same MintChip platform so payment information to confirm the transaction for settlement is included in the Value Transfer Message. | -n/a |
| Receipt                | -Payee will received immediate notification of the payment using Email or Direct Messaging | -n/a |
| Settlement             | -Digital cash is immediately debited from the Payer’s Secure Asset Store and loaded into a Value Transfer Message that can be only be accepted by the Payee. Once accepted, the digital cash is loaded into the Payee’s Secure Asset Store and at that point the Settlement is completed. | -n/a |
| Reconciliation         | -One Settlement is complete, a detailed record of the transaction is stored in the ledger of both the Payer and Payee’s Secure Asset Store. MintChip digital cash payments are irrevocable and disputed payments must be resolved by each party. | -n/a |
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

1. Ubiquity:

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Consideration</strong></td>
<td><strong>(Check One)</strong></td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.1 Accessibility</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.2 Usability</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.3 Predictability</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.4 Contextual data capability</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.5 Cross-border functionality</td>
<td>✔</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.6 Applicability to multiple use cases</td>
<td>✔</td>
</tr>
</tbody>
</table>
**Justification for U.1 Accessibility:**

MintChip ecosystem meets and exceeds the definition of Accessibility as outlined in the glossary provided.

The MintChip ecosystem enables any Entity (Person, Business, Financial Institution or Government Agency) to pay or be paid by any other Entity within the MintChip ecosystem in compliance with applicable US laws.

The entire MintChip ecosystem is accessible for any participant, existing or new, through open APIs and very robust SDKs in a number of common programming languages.

**U.1.1**

Providers connected to the MintChip platform (via the open API) can use any type of payment Account with funds in US dollars or any other fiat currency, to enable any Entity to make a payment. Accordingly, the MintChip platform can facilitate payments to/from all types of Accounts based in the United States held at all Depository Institutions and Regulated Non-bank Account Providers.

**U.1.2**

Any Entity can make a payment to any Payee providing that they know their electronically identifiable. This could be an account number, business number, email address, mobile phone number or even a social media identifier. The Payee is notified about the payment, and if he/she does not have a MintChip account they can open it through a simple process and accept the payment. The Payer is notified once when the payment is accepted by the Payee.

**U.1.3**

The MintChip platform supports multiple currencies and Providers acting as Foreign Exchange Brokers that enable End Users to make payments in the currency of their choice. End-Users can have multiple SASs with different currencies connected to a single account.
The MintChip platform can be used for low value transactions by Regulated non-bank Providers focusing on unbanked and underserved at no cost. These Providers can connect to the MintChip platform as Brokers to enable faster and cheaper (free for low value) payments. Consumers would open MintChip accounts with Brokers and use their existing cash-in/out mechanisms for withdrawals/deposits. The platform also supports private transactions. nanoPay is happy to work with Providers, NGOs and State/Federal Governments to allow free money transmission for the unbanked and underserved.

MintChip combines simplicity, security and scalability to offer Providers a compelling economic use case with low technical barriers to implementation. Our plan is to work with Providers, End-Users and software developers to achieve widespread adoption. We have already built and deployed the platform in Canada. We are working with three of the top five banks which represent [xx%] of consumer accounts in Canada to offer our platform to their End-Users. We have also agreed with the largest payment terminal provider (that has 85% market share) to put our MintChip platform on their new and existing terminals, making retail acceptance close to ubiquitous from the outset. Finally, we will provide an SDK and open source our smartphone apps for iOS and Android, allowing any merchant (End-User) or broker (Provider) to build their own smartphone app. The primary driver for End-User adoption is the economic benefit of low cost or even free transactions. Providers can participate in the MintChip ecosystem without charge.
U.1.6

Transactions that occur within the MintChip ecosystem do not require multiple operators or networks to complete a transaction. The system has been designed without a requirement for a central entity to be involved at the transaction level. There is therefore no interoperability required for transaction that occur on the platform.

_Justification for U.2 Usability:_

The mobile application required to interface with the MintChip platform provides a very simple user experience. This application is used for any transaction involving an End User who is an individual Customer (P2P, B2P, P2B). In the case of B2B transactions, the MintChip ecosystem has been designed to integrate into existing business-based ERP systems, or other existing systems used to complete transactions. Usability is maximized in these scenarios by enabling easy integration to the MintChip ecosystem.

The MintChip ecosystem also increases usability for End Users (Business and Government) who want to integrate the platform into their existing business to enable payments. The simple and open APIs and the robust SDKs allow these End Users to easily access and use the MintChip ecosystem. There is a sample mobile application that is available to inspire development, including the source code for this app. The ecosystem for merchant transactions supports NFC, and web-based integrations can be screen-reader friendly, both features that benefit the visually impaired.

U.2.1

The MintChip Solution is available to end users in a variety of circumstances, through a variety of channels, devices and platforms. The only application for which the MintChip ecosystem is not capable of completing a transaction is in the case of an in-person transaction without a mobile device or access to the internet. While MintChip has been designed to be mobile first, it can be used in a browser or on any device with a secure element. Uniquely, MintChip supports offline transactions on dongles, other secure integrated circuits or mobile phones without cellular or Wi-Fi reception. An End User could create the modern equivalent of a paper check by creating a VTM (which can be represented as a QR code), print that code on a piece of paper and use that printout to complete a face-to-face transaction. End Users can complete transactions through online (ecommerce), in person (p2p, self-serve or retail) or via any messaging platform (including, but not limited to email, social media or text message). In the future End Users will also be able to transact over the voice channel of a phone. Business End Users could use the MintChip Solution via their ERP or SAS commerce systems.
U.2.2

When a user registers a MintChip account and an associated SAS, they must provide a simple identifier (e.g. email, phone number, Facebook ID) that ties them to their MintChip account. Any entity can complete a transaction with any other entity simply by knowing their identifier. End users will also be able to use this identifier before initiating a transaction to confirm they are sending a payment to the intended Payee. In the P2P use case, if the intended receiver is not authenticated, the sender is asked if they want to invite the Payee to the MintChip solution.

U.2.3

The MintChip platform is available 24 x 7 x 365. End Users can initiate a payment at any time. In retail and online transactions are automatically accepted and the funds received are good funds immediately. In a P2P payment, the sent funds are marked as pending until accepted by the receiving End User. Once accepted these funds are added to the receiver’s available funds immediately.

U.2.4

At the core the MintChip Solution is an open API allowing anyone to build the appropriate interface. We have built smartphone apps for iOS and Android. These apps will be open sourced, allowing Providers to use our code and build their own branded smartphone apps around this code. The interface is simple and easy to use and the interface has been designed to include the following:

- Large Fonts to highlight account balance;
- Universal Icons to represent transactions options;
- Sounds verification for certain transactions;
- Color to bring awareness to certain features and transactions;
- Use of verification pop up screens to confirm transactions;
- Multiple channels of messaging to confirm transaction activity;
- Use of Country Flags to indicate currency type;
- Picture identifiers attached to contacts to confirm identity; and
- Minimal language specific prompts that can easily support conversion to any language required.

It is important to note that MintChip will make its mobile application available to any Entity that wishes to use it, however in most situations the MintChip capability will be built into existing applications. Consistency in user interface experience will be ensured through guidelines included in the platform rules. The existing smartphone apps have been tested in Accessibility mode and all features work as intended.
**Justification for U.3 Predictability:**

The simplicity of the MintChip platform means that predictability is easily achieved. The same functionality will be available to all End Users, regardless of the way in which they participate in the ecosystem. All payments will be sent and received in the same manner and rights, roles and responsibilities will be clearly defined from the moment the End User opens a MintChip account. Using the MintChip platform will be much like using an ATM today; regardless of where you are and the superficial differences from institution to institution, withdrawing cash is essentially the same experience worldwide. MintChip payments will be no different. All MintChip features are based on API endpoints, which dictate the functionality. Please see the high level summary of API endpoints below:

MintChip Platform API Endpoint

(Diagram #29)
U.3.1

Any Entity using the MintChip Platform will use the same API endpoints, ensuring consistency of operation. The core features of registration, security, cash-in, cash-out, transaction logs and transactions use RESTful APIs to deliver consistent core components irrespective of channel, device or Provider. This ensures predictability for the End-User experience for the baseline features.

U.3.2

An email address is a prerequisite to participation in the MintChip ecosystem, which means that End Users can be provided with up-to-date initial disclosures before they complete a transaction. The disclosure requirements can also easily be tailored to comply with a particular jurisdiction's consumer protection and commercial law requirements.

Digital disclosure also means that End User notices can easily be updated, modified and pushed out to at any time. Moreover, because End Users interact with the system each time they send or receive a payment, they can easily be made aware of important changes. Before sending each payment, they can also be reminded of:

- The timing of the payment (i.e. that the payment is sent immediately unless future-dated);
- The irrevocability of the payment once it has been sent;
- Any applicable fees charged by the Provider; and
- Additional disclosures that may be required by law or regulation.

Providers will be responsible for providing disclosure to their customers, so End User communications will have look, feel and use of language consistent with their Provider’s communications. nanoPay terms and conditions clearly explain the risks, costs, rights and timing. Any End User fees are also communicated at the time of a transaction (this could vary for ERP or internet of things applications).

U.3.3

The MintChip ecosystem uses the same standard communication and messaging protocols across the entire platform regardless of the Provider (Broker) that is facilitating access to the platform. Transaction messaging is ISO 20022 compliant, making a Provider’s compliance easily achieved without a significant overhaul of current systems.
U.3.4

Through the API the MintChip ecosystem delivers core features consistently regardless of the End User’s choice of channel, device, form factor or Provider. This ensures predictability for the End User experience for all platform features.

U.3.5

Error Resolution protections for all End Users are clearly defined and articulated. The MintChip platform was designed to imitate the properties of cash, so the risks will be familiar to anyone who has used cash. This simplicity of principle of operation greatly reduce the unknown and potential anxiety of End Users.

U.3.6

We refer to MintChip as **Digital Cash**. Hence when we load MintChip Digital Cash (*cash-in*), it is akin to withdrawing cash, except from a smartphone rather than an ATM or branch. We also refer to *cash-out* (offloading funds from MintChip into a Provider based account) as a deposit since the End User is putting funds into their Bank or non-bank account.

Note that digital cash is not the same a virtual or cryptocurrency in our lexicon. Please see Appendix B for the ECB definition on digital cash, emoney and the EMI directives. Since there is no specific regulation for electronic money or digital cash in Canada, where our solution is already deployed, we have followed the European EMI guidelines. We have also created a UK-based entity that is in the process of applying for an EMI license.

**Justification for U.4: Contextual Data Capabilities:**

U.4.1

Each transaction has a link that The MintChip VTM allows for a metadata link. This link stores data in a nonlinear database providing ultimate flexibility for the metadata. It is also possible to have these data validated, although this is not a feature of the current platform. Banks, service providers or other third parties could use this metadata to build in the data validation. Loyalty is more robust as our company was started with combination of loyalty and payments in mind. A single use token can represent both the payments and the loyalty identifying. Messages can be included in any transactions and can also include a link to a third party platform or application.

U.4.2

Our platform currently allow export of all transaction data into a format that can be received by most accounting and personal finance systems. We fully intend to integrate with widely used personal and business platform including, but not limited to Quickbooks, Freshbooks and Wave
Accounting. We will also integrate directly into large ERPs like Oracle and SAP (we have already started these discussions). We will make our APIs available to any other platform that would like to integrate. One of the truly exciting capabilities within the MintChip platform is to be able to pay many parties at the same time, effectively splitting the payment amongst receiving parties. For example, at a restaurant, and End User could make a single payment, but in near real time, the payment could be split into the waiter’s tip, the restaurant’s revenue and the taxes sent directly to the relevant tax authority. If the restaurant was a franchise, you could go one step further and automatically pay the franchisor. See Appendix E Real Time tax collection.

U.4.3

By default, messaging is ISO 20022 compliant, but this is not a limiting factor as any additional information or links can be associated with the transaction and store in the flexible transaction log.

_Justification for U.5: Cross Border Functionality_

The MintChip ecosystem is capable of being implemented in any country. Deployment in a given country requires the platform to meet all regulatory requirements in that country. The Royal Canadian Mint has distributed coins to over 72 countries and it was their intention to deploy MintChip their existing customers, the central banks of these countries.

Once deployed in a foreign country, completing a transaction between the home country and another country is very similar to a domestic transaction. End Users (Person, Business, Government) can keep multiple MintChip Secure Asset Stores (SASs) in different currencies or they can transact through a currency Broker. The Broker holds digital currency value in the different currencies and completes all transactions through the digital currency. Once funds are converted the user is then provided the digital currency which can be exchanged for another fiat currency in that value. The process is fast, secure, and given the limited marginal cost of completing a transaction on the MintChip ecosystem it can be completed cost effectively.

U.5.1

The MintChip Solution is very convenient. In a cross-border P2P funds transfer (money transmission) the sender sends in their home currency. If the receiver’s SAS is in a different currency, the platform will see if there is a default currency broker selected. If not the receiver will be given a choice of currency broker to select from. Currency broker Providers will publish their rates, so the receiver can choose the best rates at which to exchange the MintChip funds. The fees associated with the exchange of funds will be well below bank and money transfer fees. Since the market for exchange brokers has many players, this will be competitive. Market forces of brand, trust and rates will determine which exchange broker gets the most business. End Users
(consumers, small and large businesses and NGOs) will benefit from low rates and a competitive market for their business. If the default broker has already been selected by the receiver, the funds exchange will occur in near real time. The MintChip platform has additional security for high value transfers. Since MintChip value can only be received by the intended receiver, there is no possibility of intercepting the funds or the wrong party stealing the funds. nanoPay is building a regulatory portal which reports anomalies and suspicious transactions. This portal will allow the regulators or law enforcement to investigate further. KYC, AML and other appropriate laws will apply to any Provider using the MintChip platform for cross-border.

U.5.2

We are currently working on integration to European, Brazilian and Canadian banks. We will work with EFT, ACH and SWIFT providers to ensure that funds can be received into non-participating banks accounts globally. In addition, we will work with other faster payments providers to allow direct integration. While all funds are good funds in the MintChip ecosystem, we will work with banks and payment provides globally to expedite good funds in their systems.

U.5.3

Fee disclosure is transparent. Exchange rates are published by the brokers. An account of the transaction will be made available to both parties. In P2P the receiver will select the exchange broker, in retail or online payments, the exchange broker is selected by the payer. Full disclosure is made in the terms and conditions as well as at the time of the transaction.

U.5.4

The MintChip platform allows funds to be received in the same currency or any other currency. Receivers can open a SAS in any currency, allowing them to receive the funds in any currency available within the MintChip Ecosystem. Currency broker Providers can buy and sell any currencies that are available in the MintChip ecosystem.

U.5.5

The MintChip platform has already been launched in Canada after a 6-month pilot within the Royal Canadian Mint - employees and visitors were able to buy food in the cafeteria and gifts in the gift shop. At the time or writing, MintChip smartphone apps are available in iOS and Android and allow both retail and P2P capabilities. The app usage is currently restricted to Canada and the Canadian Dollar. We have a subsidiary company in the UK that will launch in the UK after acquiring an EMI license, which can be passported into the whole Eurozone. MintChip should be available in the USA in 2016.
**Justification for U.6:**

Any digitally recognizable End User (Person, Business, or Government) on the MintChip ecosystem can create an account within the MintChip ecosystem, through a Provider. After adding funds to their Secure Asset Store they will be able to transact.

MintChip has already been deployed in two use cases in Canada:

- P2P - paying a friend, colleague or relative,
- P2B - retail and online, allowing a retailer to accept an *ad hoc* payment retail or remote Real Time payments.

We are currently in discussions with trade and retail finance solutions to provide *ad hoc* large B2P payments. Most of our commercial agreements include the ability to be able to pay for services we purchase with MintChip (just-in-time supplier payments). We will soon start to pay our employees (full-time, contract and part-time) using MintChip.

The platform is made open to any participant with any transaction application. The simple and open API’s and the robust SDK enable any participant to easily access and use the MintChip ecosystem. The source code for the mobile application is also available for any participant to build into their existing application. This transaction could be in traditional currency; however, the platform has the ability to transfer any two assets. (loyalty points, mortgages, etc.) This enables the MintChip platform to complete an endless number of use cases. It is not the intention of nanoPay to find all the potential use cases for which the platform is applicable, rather it is our strategy to ensure the MintChip ecosystem can enable any transaction, for any use case possible, and then ensure everyone can easily access the ecosystem.
## Efficiency

### Self-assessed rating:

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Efficiency</td>
<td>Enables competition</td>
<td>✔</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Capability to enable value-added services</td>
<td>✔</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Implementation timeline</td>
<td>✔</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Payment format standards</td>
<td>✔</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Comprehensiveness</td>
<td>✔</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Scalability and adaptability</td>
<td>✔</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Exceptions and investigations process</td>
<td>✔</td>
</tr>
</tbody>
</table>
Justification for E.1 Enables Competition:

E.1.1
The MintChip ecosystem is available to any Provider, new or existing, who wants to participate in the payments ecosystem. There is limited capital cost required for a Provider to connect to the MintChip ecosystem which will drive increased adoption across a variety of Providers. Providers are able to access the MintChip platform through open APIs and a robust SDK. Any Provider electing to use this platform has complete pricing discretion on the End User transaction/service fees they charge. The MintChip cost to complete a transaction is a fraction of a cent, therefore Providers will be able to easily manage their margin requirements and it is anticipated that transaction pricing will be driven to a fraction of current transaction costs through competition as more Providers adopt the MintChip platform.

E.1.2
The MintChip ecosystem is an open ecosystem. The platform itself provides no restrictions on an Entity’s ability to move between different providers. Providers access the MintChip ecosystem through open APIs and enable their users to access the platform’s capabilities. MintChip does not put any limitations on Entity’s ability to move to a different Provider, however the Provider itself may place certain restrictions on Entity’s ability to move. MintChip Platform Operator does not have any influence over the provider’s policies.

E.1.3
MintChip platform operating rules require Providers to disclose in advance to End Users all information necessary for End Users to understand the total cost of using their services.

E.1.4
Because it is a Good Funds model, the participation criteria for the MintChip ecosystem can be much broader than other, non-funded systems. Moreover, participation is scalable - small and large institutions are free to participate in the platform. There are no volume or value requirements. So long as the Broker can fully-fund the value in their MintChip account, they can on-board End Users onto the platform. Because of the interaction between the Broker and the Originator, the Broker cannot get MintChip value without transferring the same value in fiat currency to the Originator’s pooled account. The MintChip platform operator will ensure any Provider meets participation requirements prior enabling access to the MintChip ecosystem.
Justification for E.2 Capability to enable value added services:

E.2.1
The MintChip platform provide open Payment and Broker APIs to enable any Provider to create value-added solutions or integrate directly into their payment systems. In addition, the MintChip platform will comply with ISO 20022 to support interoperability to existing payment systems.

E.2.2
Any Provider is allowed to provide value-added services built into their application that uses standard MintChip platform APIs, as long as they comply with operating standards and participation requirements.

E.2.3
MintChip platform operating rules require Providers to clearly disclose to their customers the value added services they implemented on top of the baseline MintChip platform services are optional.

Justification for E.3 Implementation:

E.3.1
Our organization is venture backed. We have sufficient funds to deploy and continue developing our platform for the next two years. We have launched our platform in Canada already and will also be receiving revenue from our initial customers, including retailers, banks and telecoms companies. Our lead investor is the Private Equity arm of a large investment bank with the resources to support us through to the end of the implementation. We are happy to provide the details of our funding in a more private document.

Justification for E.4 Payment format standards:

E.4.1
The MintChip Solution will comply with the ISO 20022 messaging standard to provide for easy integration and support of additional remittance data to accompany payments. The Solution can interface and interoperate with existing formats and future standards.

The MintChip Solution is flexible enough to allow any off-ramp to require certain fields. These fields could even be completed after the funds have been received in MintChip, but are required to move the funds into the receiver’s off-ramp, either a bank or another payments ecosystem. Let’s say for example an Indian Bank requires the identity number of the receiver to be entered
before the funds can be put into a bank account, we can allow the API to request this data prior to completing the transaction. The funds will be good funds and available for use in MintChip, but the receiver would have to enter their identity number prior to receiving the funds. Through some basic machine learning we could then require this at the beginning the second time round and make it part of the VTM.

E.4.2

Cross-border payments will take place between two MintChip platforms in different currencies utilizing standard message formats.

E.4.3

MintChip platform APIs will use ISO 20022 standard which allow for cost effective integration.

E.4.4

ISO 20022 is an evolving standard and MintChip will continue to support in the future. With the wide adoption of ISO 20022, MintChip will future-proof integration enabling the platform to adapt to future needs and standards.

E.4.5

All external APIs will be published and are designed to consistent with open standards. We see compliance with ISO 20022 as a necessary, but not sufficient standard and the platform allows for further modification or additions to grow the platform going forward. The mobile applications will all be open source allowing anyone to build on them, improve them or even write their own applications.

Justification for E.5 Comprehensiveness

E.5.1

The MintChip ecosystem is a Good Funds digital cash system that enables all relevant aspects of the end-to-end payment process. The platform is extremely efficient at doing this as previously outlined in Section A of this document.

Loading and unloading of MintChip value is based on standard payment mechanisms supported by the participating Brokers.

E.5.2

The MintChip Solution is architected to deliver a full and comprehensive payment solution—initiation through to Payer’s Approval all key elements of the solution, however the concepts of clearing, settlement and reconciliation are not required in a digital cash transaction. MintChip
supports reconciliation, but at an aggregate level comparing the float with the total funds in the ecosystem. Receipt is a key part of the transaction, but in retail the transaction settles in near Real Time, removing the need to keep reporting incomplete transactions. The technical design of MintChip is open, flexible and feature-rich.

Usability - the MintChip platform supports every use case from P2P payments to inter-bank settlement and everything in between. The MintChip API is flexible and designed for third parties to build new services and applications.

Reliability - MintChip is hosted at both Amazon Web Services (AWS) and Peer1, and provides complete redundancy including power, network, hardware and software/service-level redundancy of both APIs and databases. The HSMs are clustered but distributed and stateless allowing load balancing based on physical location or load. Many of MintChip’s executives come from a telecom background where five 9s was the expected availability.

Performance - the MintChip platform can currently support thousands of transactions per second. The last six months were spent making the platform more robust and scalable, removing bottlenecks, performance testing, and implementing highly scalable technologies built on a future-proof architecture. The platform is build using state-of-the-art developer tools and open source operating systems to deliver a flexible solution that really delivers performance at any scale.

Information security protocols - all data sent between API micro services and within the network is encrypted using a variety of techniques. Communication between APIs is encrypted via TLS tunnels, network traffic from employee workstations is encrypted via VPN (and remote administration via SSH), and traffic between data centers is encrypted via a VPN (in some cases multiple VPNs). Sensitive payloads are also encrypted (within their TLS tunnels), and sensitive data that needs to be stored is likewise encrypted, with private keys for all encryption residing in secure locations and never leaving the server where the key is stored. Public access to points of entry in the system are encrypted using commercial TLS certificates. In addition, enterprise-grade firewalls have been setup to protect the network, and protocols that permit plain-text transmission are blocked.

Operations - our executive team has significant experience at scale, having run a wireless operator with 25,000 employees and nearly $5bn in revenue per quarter. The architecture of the platform has been designed to support horizontal scaling, allowing resources to be added as needed - including on-the-fly in some cases. Execution at scale is our secret sauce!
**Justification for E.6 Scalability and adaptability:**

**E.6.1**

The technical design of the MintChip platform is capable of completing any transaction use case that involves the transfer of value between two different parties. The use cases of P2P and P2B are already live in Canada and we expect B2P and B2B transactions to be live in the next quarter.

**E.6.2**

One of the strong differentiators of the MintChip platform is the capability to quickly scale throughput capacity at a very low cost. The current transaction capacity of the today’s platform is thousands of transactions per second. The current capacity of the Visa system on a **Global basis** is approximately 50,000 transactions per second. The MintChip platform can scale to that similar throughput with a modest investment in additional hardware and short implementation times.

The speed and cost to scale the MintChip platform far exceeds traditional payments platforms allowing MintChip to deliver payments at a marginal cost of very close to zero.

**E.6.3**

The MintChip platform is designed in the latest technologies, databases and operating systems. All MintChip functionality is achieved through a series of internal and external endpoints which are RESTful APIs. MintChip is a platform that is designed for banks, payment service providers and other third parties to build upon. It is by definition regulator friendly and offers regulators tools and capabilities to monitor and investigate that have never been available before.

**Justification for E.7 Exceptions and investigations process:**

**E.7.1**

The MintChip platform is constantly looking for anomalies in the ecosystem, which are flagged and reported. Secure Asset Stores can be locked to protect the consumer and members of our customer success team or support team can help to manually re activates the SAS. Why discrepancies over amounts should be settled between merchant and consumer, our support team is available to confirm how much was paid, to whom and when. Since all transactions are validated by the consumer before payment, errors should be minimized, but brokers can do analysis and resolve exceptions.

**E.7.2**

The MintChip ecosystem uses a Distributed Ledger system for tracking and storing all transactions that occur on the platform. Each transaction for an independent Secure Asset
Store(SAS) is stored in a ledger within that individual SAS. Every transaction or activity associated with the SAS is stored and retained in perpetuity. The fact information is never deleted ensures the platform can facilitate tracing any previous transactions, at any point in time, regardless of whether a SAS is still in active mode, or is dormant.

This transaction data is both securely stored and backed up and exists in different locations in perpetuity.

E.7.3

The MintChip platform actively looks for anomalies and patterns.
### Self-assessed rating:

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
<th>Proposal Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.1</td>
<td>Risk management</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.2</td>
<td>Payer authorization</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.3</td>
<td>Payment finality</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.4</td>
<td>Settlement approach</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.5</td>
<td>Handling disputed payments</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.6</td>
<td>Fraud information sharing</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Security controls</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>S.8</td>
<td>Resiliency</td>
<td>✔</td>
</tr>
</tbody>
</table>
Safety and Security | S.9 | End-user data protection | ✔ | 139
Safety and Security | S.10 | End-user/provider authentication | ✔ | 139
Safety and Security | S.11 | Participation requirements | ✔ | 141

**Justification for S.1 Risk Management:**

MintChip has a Risk Management Framework (RMF). The RMF consists of policies and procedures that are mostly enforced through the ecosystem itself. Policies and Procedures are simplified for digital cash, for example there is counterparty risk in a transaction because the ecosystem is always good funds and nanoPay does not extend, provide or facilitate credit. Even legal risks are simplified because the ecosystem is reduced from four parties to two.

**S.1.1**

Since the platform is centrally managed it would be relatively easy to make the necessary changes to comply with any unexpected change or application of the law. For example, all security is centrally managed, we can upgrade the cryptography without impacting any consumer or merchant. API or client application updates that conform to new regulations can be pushed out, and these changes communicated with MintChip users via a variety of communication mediums.

**S.1.2**

MintChip payments are often compared to traditional cash transactions. Like a traditional cash transaction, settlement occurs when the payee has received and acknowledged the receipt of his/her cash. The same is true with MintChip, except the cash is digital information. Unlike traditional cash, this digital information cannot be “lost” in the same way, but in the event that it is not received it can be resent as many times as necessary (it never expires), and the ecosystem is monitored for unclaimed value. VTM create and accept requests are both logged - these and every other transaction can be accounted for, and appropriate action taken beyond contacting the payee managed by working with MintChip support infrastructure.
S.1.3

MintChip transactions are logged, and this data is carefully replicated and managed to provide complete reliability and redundancy in the event of systems failure. In the event of a human failure, such as inputting an incorrect (but valid) transaction value, these are the responsibility of the parties involved, although the MintChip platform’s support infrastructure can help support these cases on a case-by-case basis making appropriate interventions as appropriate and legally permissible.

S.1.4

There are many checks and balances in place to minimize fraud, for example (in no particular order):

**First-party fraud:**

- Device ID required for transactions and transactions being blocked if this device ID changes and the account owner hasn’t authorized access to the device
- Strong password requirements
- Email, phone, and address verification

**Second-party fraud:**

- Enforcement of biometric authentication
- Monitoring and revocation of authentication (TLS) certificates
- Multi-factor authentication required for administrative access, such as merchant and broker administration

**Third-party fraud:**

- Access tokens required and validated by the APIs involved in transactions
- Application registration and access controls via the industry standard OAuth2
- Disassembly of VTMs to validate their authenticity, matched against issuing security series certificate
- PCI compliance for adding funds to a MintChip account using a credit card
- Address and name verification for credit card usage, as well as velocity checks

**Systemic fraud:**

- Enforced deprecation of insufficiently secure cryptography
● Multiple levels of transaction limit threshold enforcement
● Use of hardware security modules (HSMs) providing physically tamper-proof controls over cryptography used for creating and accepting VTMs, generated using proprietary HSM firmware
● Extensive security surrounding the creation of SAS, including file encryption (occurring offline), and multiple passwords required to authorize the creation of these accounts
● SAS/account blocking

S.1.5
The MintChip platform itself is very secure and as such most of the risk occurs in the cash-in (withdrawal) and cash-out (deposit) interfaces with bank and non-bank providers. The largest risk is related to KYC and we believe that there are already ample incentives for bank and non-bank Providers to do a good job in eliminating money laundering. The largest incentive to Providers and Operators to manage the other Participants risk, is the ability to participate in the ecosystem. Participants which do not pull their own weight and ensure that they are not bringing risk to the ecosystem will be excluded.

S.1.6
There is a quarterly review of all risks and compliance within the ecosystem. This is a board level agenda item that is taken seriously by our board and investors. Internally the platform includes controls to highlight and reports anomalies, which are investigated immediately as issues surface. MintChip will continue to evolve to manage risks and threats.

Justification for S.2 Payer Authorization:

S.2.1
The Payer authorizes each MintChip transaction by Authenticating and then Authorization. Retail payment authorization is normally achieved using Touch ID (iOS) and Android’s fingerprint scanner. Monthly recurring charges can be authorized in the same way, even if they were pre-authorized.

Transactions that enable users to load value onto the MintChip ecosystem through their Broker (Depository Institution/Regulated Non-bank Account Provider) will adhere to the authorization requirement of those separate institutions.

S.2.2
There is a MintChip API endpoint used for generating a Value Request Message (VRM) which enables a merchant or vendor to request a payment from an End User. This could be used in
combination with an invoice, emailed or sent via a push notification directly to a smartphone app.

There is a registration process prior to being able to automate the sending of VRMs, this registration process requires the requesting merchant to provide company, amount range, frequency and account details. On receipt, the consumer (or End-User) can agree or change the amount range, frequency and finally decide to accept the merchant’s request for payment.

On a recurring basis, the merchant will call the API with the desired amount and any associated metadata required. These metadata and the amount are presented to the End User.

The Consumer (End-User) then has an opportunity to:

1. Pay the requested amount in full,
2. Pay another amount,
3. Delay the payment, or
4. Decline to pay.

The End-User authorizes the payment using their fingerprint or Touch ID. Explicit authorization by the End-User is required for processing recurring VRMs in this manner.

S.2.3

The MintChip platform notifies the Payer and requests approval prior to any value transfer. This pre-approval of transactions can be revoked at any time. The merchant is notified if the pre-approval is revoked.

**Justification for S.3 Payment Finality:**

S.3.1

The MintChip platform is a good funds digital cash system. A Payer can complete a transaction up to the value contained within their SAS. The Payer identifies the Payee and the amount to be paid. Once the Payer confirms this payment, a Value Transfer Message (VTM) is created and the payment is irrevocable and final. There is no capability within the MintChip ecosystem for the Payer to retrieve the value transferred or stop the payment once sent.

The MintChip ecosystem itself has no native concept of lending, credit or overdraft. Like cash, you can only spend the digital cash you have. However, third-parties can build custom applications built around lending their own funds. One exciting aspect to MintChip digital cash is that you can spend these funds (as MintChip digital cash) in near Real Time.

S.3.2
As a way of paying merchants for goods and services, the MintChip platform functions in a manner that is similar to traditional cash. Any rules applicable in a particular jurisdiction that apply to cash payments made to merchants today will continue to apply within the MintChip ecosystem. As well, nanoPay anticipates that any future requirements particular to digital currency (maintaining an audit trail, etc.) will also apply.

With respect to irrevocability, once the Payment message is sent by the Sender, it cannot be recalled, withdrawn or amended - it is already irrevocable. The sender can see the funds have been deducted from their SAS and that there is a pending transaction. The Receiving party is not required to accept the funds immediately and, if too much was sent in error, cannot be compelled to send the funds back. Once the Receiver accepts the payment message (VTM), the funds are automatically added into the receiver's MintChip SAS and the payment becomes final. The sender’s transaction log is updated to indicate that the transaction is no longer pending. The funds are already good funds and can be used immediately.

Clear and simple terms and conditions will describe the payment flow and point of irrevocability to all ecosystem participants.

S.3.3

The system is designed to support existing consumer protection frameworks, not supplant them. However, it is important to note that this system is being built as a digital equivalent to cash, and not as an extension of existing card networks. As a result, there is no plan to develop chargeback and dispute-resolution frameworks. Transparency, speed, low-cost efficiency, finality of payment are the driving factors and the focus will be on ensuring that payments are not made in error in the first place.

- Easy-to-use interface
- Clear indication of the final amount sent to the Payee before that payment is sent

Please see Appendix C for detail on Regulation E.

**Justification for S.4 Settlement Approach:**

The MintChip ecosystem settles in real time within the ecosystem. Like cash, there is no post-event settlement between Depository Institutions and Regulated Non-bank Account providers. MintChip deals in cash and does interface with Depository Institutions but in much the same way as cash:

- **MintChip cash-in = Bank Withdrawal.** Today, consumers withdraw cash from the banks using ATMs or by visiting a branch. With MintChip digital cash, End Users can
withdraw using their smartphones. Instead of the ATM providing cash, MintChip creates
digital cash and uses a smartphone to send/receive money and pay merchants.

● **MintChip cash-out = Bank Deposit.** If a friend gives you $20 you would probably not
run to your bank and deposit it, but rather you would spend it at the next opportunity at a
merchant. But if you sold your car for $10,000 and were paid in cash, you would
probably go to the bank and deposit the cash. This is because it is generally not safe to
carry that much cash around and you have an opportunity to earn interest on the funds. If
someone sends you $20 in MintChip digital cash, you would probably send it on to
someone else or spend it in-store. If someone paid you $10,000 in MintChip, you would
probably deposit it in your bank account. This can be done at the click of a button on
your smartphone.

**MintChip Cash-in and Cash-out**

(Diagram #30)

Like cash, MintChip settles at the time of the transaction within the ecosystem. When an
End User wants to cash-out and deposit their funds into a depository account, settlement is
still effected immediately. Because the End User holds a MintChip account and deposit
account with the same Broker, and because all MintChip value is backed by traditional cash,
a cash-out is simply a ledger entry for the Broker (an “on us” transaction for the Broker).
The situation is slightly more complicated in the case of cross-border transactions where an End User wants to cash-out and deposit funds that they have received from another jurisdiction. While the MintChip value is still considered good funds, the End User will use the services of a MintChip Forex Broker that will have MintChip accounts in multiple currencies (buy and sell). This will enable the Broker to receive funds in USD and return funds in CAD as an example. This transaction can settle in near Real-Time if both SASs are funded.

S.4.1

The only time a settlement between Depository Institutions needs to take place is when cash-in (withdrawal) and cash-out (deposit) occur at different institutions. MintChip will settle between End Users accounts during the day with sufficient frequency determined by changes in balances between institutions compared with normal trends. MintChip is always a good funds model, so there is no concept of a participating FI having insufficient funds to settle. It is our intention to move from 1-2 times daily net settlement to more frequent gross settlements.

S.4.2

Consumers will always have 24x7x365 access to funds. The FI settlement process is outside of the MintChip ecosystem and does not impact end users, whether they are businesses or consumers.

S.4.3

Originators will be the Central Bank - backing all of the funds in the ecosystem. Settlement within the platform does not require central bank involvement and for the most part, loading and cashing out of the ecosystem will not involve central bank involvement - any more than central banks are not involved in settlement for individual account holders today. Because settlement occurs on a per-transaction basis, there is no netting of positions across FIs at the end of the day - the central bank therefore does not have to move funds between FI settlement accounts every night (which is what BoC does for FIs today). What the central bank would do, is ensure that each Broker only purchases as much MintChip value as it can safely back.

**Justification for S.5 Handling Disputed Payments:**

S.5.1

The MintChip Solution has a strong but simple framework for handling disputes. The platform has significant checks and balances to ensure that the number of disputes can be minimized, there remain circumstance in which a framework is required.
Unauthorized Payments

In is difficult to do an unauthorized transaction is the End-User is using a smartphone that requires a fingerprint. This suggests that the entire device would have to be hacked and either the End-User is being coerced into providing their fingerprint or someone has the same fingerprints. So to do an unauthorized payment the bad actor would have to have both the smartphone and the fingerprints of the End User.

Erroneous payments

These would occur either through user error or an incorrect payment request that was approved by the End-User. Human errors would be dealt with in a similar way as cash errors are today, except that a real time transaction record would be available to both parties. In cash one might say “you have given me change for a $10, but I gave you a $20”, in a busy store the server would probably give you the benefit of the doubt and give you a $10 note to correct the error. Human error can easily be corrected by a payment back to the payer correcting the amount. With Real Time transaction records, there can be no doubt how much was paid. Any disputes can be settled by a quick support query.

Fraudulent transactions

Fraud is difficult on the platform itself, so most fraud will occur at the weaker points of cash-in and cash-out. A stolen credit card could be used to load a MintChip and the value used before the credit card was reported stolen. It should be relatively easy to identify the perpetrator though since they would have given their mobile phone number, email address and phone ID at registration. To cash out they would have provided their bank account and would have provided significant KYC in advance.

If an End-User is concerned that their smartphone has been compromised, their Provider can lock the SAS and prevent any transactions. With the value of a smartphone around $800 most End Users will be more interested in retrieving their phones than how much money a hacker can transfer.

S.5.2

The MintChip ecosystem does not have an impact on any existing consumer protection rules and regulations that Brokers are currently required to adhered to. In the ecosystem, the Provider is simply the conduit for the payment, but doesn’t add an additional layer to the consumer protection regime. In this manner, MintChip digital cash is very much like traditional cash; it allows for the orderly exchange of value, but does not add to the Consumer Payer’s Provider’s regulatory burden.
In fact, the MintChip platform can help support and enhance a Broker’s compliance with the regulatory regime, by providing a very secure payment method and robust audit trail to aid in the investigation of any disputes or error corrections. Moreover, the ecosystem allows for the tracing of all transactions across the platform. If fraudulent transactions have occurred, those parties who have contributed to the fraud can immediately be shut out of the ecosystem.

S.5.3

Our framework allows the End-User to request their funds back, but in an online transaction this will require them to disclose their identity to the Payee. The Payee can of course have a valid reason not to return the funds. If required by law, the Provider could facilitate this process.

S.5.4

The MintChip solution will always adhere to the laws. Ecosystem roles are clearly defined in the Executive Summary (see page xx). The best mechanism is however to prevent the errors and fraud in the first place.

S.5.5

Consumers are well protected from fraud and errors. At a click of the button within the app, they can make an appeal and speak to the merchant. Providers can assist with Consumer End-Users with this process and see the details of any payment.

Justification for S.6 Fraud Information Sharing:

All systemic fraud will be identified and removed centrally. This is relatively easy to do, since it is a single payments ecosystem. Bad actor information can be shared between brokers (banks) and other ecosystem participants.

S.6.1

User identity is based on digital credentials such as a user’s email address and mobile device ID, or a POS device’s ownership. MintChip shares blacklist data on fraudulent credit cards or bank accounts used to move value in and out of a MintChip SAS, and regularly explores ways to share internal transaction profiles with partners well-positioned to help identify potential fraud based on suspicious looking activity. This information is shared between MintChip brokers.

S.6.2
Credit card and bank account blacklist data is shared via secure channels with partners via techniques such as PGP/GPG encryption of files and secure transit via secure FTP (SFTP), including within automated workflows. MintChip platform internal transaction records are kept private and confidential.

S.6.3

Internal events that are triggered, such as transaction limits being met, are logged and reported to administration in an automated workflow. Unique status codes are used to help identify these events, in addition to their probable causes. As the MintChip platform does not manage and control the credit card networks or banks used to move funds in and out of MintChip, specific events cannot be triggered within these respective systems, but unusual activity seen within the MintChip platform is recorded, and proper communication channels exist for reporting this activity to partners managing credit card and/or bank systems impacted by fraud attempts.

S.6.4

Access to transaction history is available to regulators via an administrative portal, where access is granted by showing a legally binding warrant, or other suitable proof of identity and/or legal justification. This access requires multi-factor authentication, and each search is properly logged, flagged, and associated with the user requesting this information to provide a complete information trail.

S.6.5

Recycle language on portal access, adding stuff about support for multiple levels of access where brokers can see transactions occurring within their brokerage, and regulators and law enforcement for transactions covered by warrant.

S.6.6

The MintChip platform does have a centralized log of all data and this includes anything that is fraud related.

S.6.7

Since the data is all aggregated in a centralized repository, trends and patterns not visible at the individual participant level can be identified and participants can be alerted.
**Justification for S.7 Security Controls:**

**S.7.1**

Identity/Access/Authentication

There are multiple authentication methods enforced depending on the type of user and device(s) being used to contact the API.

User accounts are based on email addresses, and this email address cannot be changed for that account by the user. Users have to validate their email address at account creation time by clicking on a link sent to this address which includes a unique token set by the MintChip API and recorded by the MintChip database.

For consumers, an email address and password paired with their static and immutable device token are presented to the API, where the email, (hashed) password, and device tokens are matched against records in the MintChip database. If a device token changes, users will be required to associate their new device with their account. There is a fixed number of devices that can be associated with an account and a fixed number of requests within a time period. Authorizing devices and resetting passwords requires having an email sent to the user’s email address, which will include a link containing a unique token set by the MintChip API and recorded in the MintChip database.

Merchant authentication is based on TLS certificates. The designated merchant admin (typically the merchant acquirer) uses a web-based portal to register their devices, and at registration time these signed certificates are issued by our crypto API micro service specifically for the secure asset store associated with the device, which is also assigned a device ID. Using the web-based portal, the merchant admin can download these certificates, which is necessary to install them on each individual device. Access to the web-based portal requires two-factor authentication, and access from a new IP address needs to be authorized via an email sent to the owner’s account. Authentication takes place by the merchant’s app presenting the public certificate as an HTTP header, the MintChip API validating the certificate by verifying its signature, making sure it matches the device ID it was issued for (and by extension for the merchant it was generated for). The POS terminals should be physically tamper-proof, but in the event a terminal is ever compromised, MintChip network/security operations will revoke the certificate, rendering it unusable by the MintChip API, thereby blocking all transactions.

Both consumer and merchant accounts include two tiers of transaction limits (providing redundancy and extra layers of security), and the higher level tier reflects the ability of the
MintChip platform to evaluate the ID of the user based on what information they’ve provided. If they choose to provide additional information (e.g. government photo ID), the transaction limits will be increased at the discretion of the company. The storage and transmission of personal information is encrypted via our crypto API micro service (AES-256). Merchants have no access to this information.

There is an extensive amount of cryptography applied to creating and validating transactions via VTMs, generating and loading secure assets stores, and controlling the cryptographic ciphers supported by the underlying HSMs used to sign VTMs. The design of MintChip allows us to update the underlying HSM firmware and cryptographic methods supported by the ecosystem to strengthen the underlying encryption layers as new methods of encryption are devised.

The platform is ISO 27000 and SOC Type 1 and Type 2 compliant.

**S.7.2**
Data retention/physical security

MintChip transaction data will be retained indefinitely, but as per legal requirements the last seven years are made available to users/account holders. Beyond this period MintChip will encrypt and archive database dumps of these transaction logs for permanent storage.

The HSMs do not store any persistent data relating to individual accounts.

The server environment where the MintChip platform is housed is an Amazon Web Services (AWS) and collocated data center hybrid ecosystem. The collocated data center is where the HSMs and Canadian personal information is housed, the transaction logs, and all production MintChip APIs and databases reside in AWS within multiple regions.

Employees that have access to production data have been carefully vetted, and each employee is provided only with the access they need to fulfill their job responsibilities. For sensitive actions such as secure asset store account creation, multiple high level employees are required to be present and enter their own complex passwords to authenticate these requests.

The MintChip network is segmented into several VLANs, which are monitored regularly for network intrusion and suspicious activity. There are several layers to the API architecture, the bulk of the micro service APIs not exposed to public network traffic. The VLANs and communication between VLANs are managed by hardware switches and firewalls, which tag
packets.

In the event of a network intrusion, there is still limited damage that can occur given the nature VTMs are generated, signed, and accepted by the underlying HSMs for a single usage (meaning obtaining a VTM generated for another user is of no value), and that every transaction and interaction with the HSMs is logged both at the API and HSM connectivity layers. Therefore, each transaction attempt can be properly accounted for and traced to individual users/accounts.

S.7.3
Risk Management

● Leverage existing KYC and AML requirements (internal FI policies and external requirements)
● Brokers are free to establish limits within their own risk tolerance levels (either system-wide or on a per-customer basis)
● Managed like any other account type for each Broker, so would interact seamlessly with existing risk/governance framework
● MintChip platform encourages innovation and collaboration and will be managed transparently - so all parties will be encouraged to contribute to ongoing improvements to the system.

Justification for S.8 Resiliency:

S.8.1
Availability Metrics

Complete redundancy is built into MintChip:

● A pool of HSMs, including health checks of individual HSMs
● Redundancy across multiple physical regions for all APIs (both located in Amazon Web Services and collocated data centers), bridged together by site-to-site VPNs
● Database replication and sharding strategies across multiple regions, bridged together by site-to-site VPNs
● Pairs of network switches and firewalls
● AWS-provided redundancy of key services such as DNS, data storage
Network monitoring and backup networks (both located in AWS and collocated data centers)

With this architecture operating as it should, there should be no realistic scenario where service becomes available for more than a minute (or whatever period of time is required for a health check to fail)

S.8.2
Disaster Recovery

The MintChip platform spans across multiple physical regions which are bridged together with site-to-site VPNs. Health checks are performed on individual nodes within each physical environment, as well as the networks themselves so that in the event of a disaster, another region will be able to provide access to the platform and all data at reduced overall capacity. Encrypted data snapshots are retained in Amazon S3, which provides redundancy of data access suitable for DR scenarios.

In the event of a physical security breach, the HSMs controlling the cryptography behind the MintChip platform are tamper resistant and the installed firmware designed to self-delete in the event of physical access obtained via brute force.

S.8.3
Systemic Failure

The MintChip platform has no real dependencies on other market players, with exception to on and off-ramps for loading and offloading traditional currency housed by banks. However, the method in which top-ups and cash-outs occur is managed by industry accepted protocols, legally vetted frameworks such as PCI-compliance in the case of credit card transactions, and no proprietary techniques or communication occurring outside of rigid, controlled channels.

S.8.4 and S.8.5
Business continuity and Resiliency

By providing a public API and using this as an economic driver, nanoPay is committed to thoroughly documenting all application/API/firmware code. There are no absolute dependencies on any external companies, as by having ample documentation the MintChip firmware can be ported to another HSM vendor, and any partnerships with payment gateways and/or KYC verification services replaced by competitors. There are several patents
controlling the IP of proprietary underlying MintChip technology, and a willingness to open APIs and workflows surrounding the core capabilities of creating and accepting value.

MintChip supports a variety of integrations with partners so that these dependencies do not exist, and flexibility to make changes is always present.

**Justification for S.9 End-User Data Protection:**

**S.9.1**

Data is protected by restricting network access, physical access, and visibility to the naked eye by way of encryption (and encoding) of data storage. Internal access is managed by thorough vetting of employees, and not exposing data that is not necessary to fulfill job requirements.

**S.9.2**

Unique and public identifiers separate from SAS identifiers, such as email addresses, are used by end users for transactions, thereby abstracting and concealing SAS IDs and establishing a sense of privacy (although inflicting damage would require knowing a lot more than just a SAS ID). MintChip supports using multiple kinds of unique IDs, so an appropriate one can be enforced based on context, business, and security considerations.

**S.9.3**

As per 9.2 no account information needs to be shared.

**Justification for S.10 End-User/Provider Authentication:**

The MintChip platform is designed to work with consumers who are banked and those that are not. Since most pundits agree that a key deterrent to financial inclusion is the high bar for KYC, we have developed a graduated identification system. This serves to protect and identify those will bank accounts but also include the 2 billion people that are today financially excluded. The most interesting fact for us is that at least 1.7 billion of those without financial services are electronically identifiable through social media. So we use social media, a phone number, an email address and a device identifier to identify consumers for a limited set of services. This limited set has low thresholds in terms of retail transactions, money transfers and other limits. To have access to our full set of services a consumer would at least have been through a bank’s KYC process. Additional KYC and AML is required to be able to send large sums of funds both domestically and abroad.
S.10.1

MintChip has a very robust End-User and Provider Authentication system. Internal device IDs, telephone numbers, authentication (TLS) certificates, and email addresses are all used to initially authenticate the device to the platform based on account type (i.e. merchant or consumer access). This then completes a device profile which needs to be updated by the account owner when any aspect has changed, including the telephone number (by changing SIM card), or the device is replaced. Upon device validation, an access token is created. For consumer devices/accounts the access token lasts for a finite period of time after which the user will have to log in again, and for merchant devices/accounts the (signed) TLS certificates are valid until they expire or are revoked. The consumer’s access token allows the consumer to look at previous transactions and send money P2P within their limits. To purchase in retail, the consumer is required to use finger or thumb print to authorize a transaction. Their personal information can only be changed after entering their password and using their thumb print to authenticate them. All data is encrypted on MintChip servers, including the Personal Identifiable Information and all of their transaction data.

S.10.2

MintChip transfers value through a VTM. The VTM is only created after the intended receiver has been identified. The VTM is then cryptographically locked only to be opened and accepted by the intended receiver. If someone attempts to send funds to someone (via email for example) to someone who is not registered, it will confirm that they are not currently registered, and provide options to invite users to MintChip. Addresses to existing users are matched against address book entries to prevent typos in input.

S.10.3

MintChip is aligned with regulatory guidance and industry standards, including ANSI, ISO-2700, W3C, soc type 1 and 2 security. [Joe please confirm]

S.10.4

MintChip authentication techniques (and cryptographic ciphers used for transactions) vary depending on account type (merchant or consumer), and risk assessment of transactions based on the involved value. These techniques are applied to both validating users, as well as specific actions.

S.10.5

Biometric user authentication is required by the end-user to re-authenticate transactions based on risk assessment. (the stuff below is just a repeat of stuff already said)
The End User is authenticated at enrollment and then again when changing any of their credentials, including their phone number or device. They are authenticated when opening the app and then again when processing a transaction. There can be a second level or factor of authentication for higher value or higher risk transactions.

**S.10.6**

The MintChip platform is specifically designed to be able to update the security series of the platform. This can mean changing the cryptography or other key components of the security architecture. MintChip is designed to be able to any of the three most recent security series to conduct a transaction, allowing control over when cryptographic ciphers are deprecated, and when client applications should be forced to update. These changes are not seen by the End-User - functionality / user experience is unchanged.

**Justification for S.11 Participation Requirements:**

**S.11.1**

The good funds model means that a variety of participants of virtually any size, could participate in the ecosystem. While the solution contemplates traditional financial institutions from acting as Brokers, the system does not need to be limited in such a manner.

Other smaller, non-deposit-taking institutions could participate as Brokers. The data they are required to gather could vary depending on the size of payments that they wish to facilitate. So long as an Originator was willing to issue MintChip USD to an Entity, they could act as a Broker.

However, alternative providers could also set up indirectly, by establishing pooled accounts with their Brokers. This would allow a non-traditional participant to set up their own MintChip USD account, register individual End Users and allow them to exchange USD for MintChip USD. Those End Users, having established their own SASs, could then send payments in the same manner as an End User with a one-to-one relationship with a Broker. Because there is no clearing and settlement of the payment *per se*, there is no disadvantage to dealing with an “indirect” Broker.
S.11.2

The Solution’s participation requirements should be adequate to ensure that all compliant Depository Institutions and Regulated Non-bank Account Providers have the operational, financial, and legal capacity to fulfill their obligations, including to other Providers, on a timely basis (see S.4).

As above, the food funds model, combined with the immediacy of each payment means that all participants can, at any time, fulfill all of their obligations to every other participant in the ecosystem.

S.11.3

The Solution should have processes to monitor and ensure compliance by all Providers against these requirements. Funds in the float will be reconciled with funds in the ecosystem to look for anomalies and ensure integrity.

Only the Originator in each ecosystem can issue MintChip currency. At all times, the Originator safeguards the underlying, backing currency that supports the ecosystem. Because of the nature of the platform, currency cannot be manufactured by any other party. As well, because all payments occur in real-time, there can be no run on a particular Broker and they can never be in a shortfall position.
4. Speed (Fast)

1. Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: fast approval, fast clearing, fast availability of good funds to payee, fast settlement among depository institutions and regulated non-bank account providers, and prompt visibility of payment status.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.1</td>
<td>Fast approval</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.2</td>
<td>Fast clearing</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.3</td>
<td>Fast availability of good funds to payee</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.4</td>
<td>Fast settlement among depository institutions and regulated non-bank account providers</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.5</td>
<td>Prompt visibility of payment status</td>
</tr>
</tbody>
</table>
**Justification for F.1 Fast Approval:**

End Users in the MintChip ecosystem are only able to send payments to the maximum value contained in their Secure Assets Store (SAS). If the desired transaction exceeds the value within the End Users SAS, the transaction is denied. There is no other approval process required.

**Justification for F.2 Fast Clearing:**

The MintChip platform manages SASs for both the Payer's and Payee's Provider. When the VTM is delivered to Payee to accept, the payment information is available to the Payee's provider as their app notifies the Payee to either accept the payment, or that the payment is received (if auto acceptance is enabled). In any case, the clearing is very fast as VTM creation and delivery to the Payee for acceptance is near instant.

**Justification for F.3 Fast availability of Good Funds to the Payee:**

The MintChip ecosystem is a good funds model. A User is approved to initiate and complete a transaction up to the value contained within their SAS. Once the VTM is created by the Payer the value is immediately and irrevocably available to the Payee only. The value is credited to the Payee’s SAS immediately upon receipt of the VTM.

**Justification for F.4 Fast Settlement among Depository Institutions and Regulated Non-bank Account Providers:**

**F.4.1**

Because of the good funds model with MintChip value in any SAS being fully pre-funded by fiat currency in the Originator’s pooled account, there is no lag between transaction Finality to the Payee at the time the payment VTM is received by the Payee’s SAS and inter-Provider Settlement, as the settlement is completed at the time the VTM is received/processed by the Payee’s SAS. The system is available to participants on a 24x7x365 basis with no impact on risk.

**F.4.2**

As above, because of the nature of the MintChip platform, there are no settlement issues because settlement is part and parcel of the payment itself - completed when the VTM is received/processed by the Payee’s SAS. The location of payment recipient’s account is irrelevant and the 24x7x365 nature of the platform means that there is no issue sending payments inter-time zone.

**F.4.3**
The ecosystem does not contemplate deferred settlement. Since all transactions happen in real-time and are cleared and settled instantaneously, there is no need to defer settlement. Therefore, there is no need to develop mechanisms to mitigate deferred-settlement risk.

**Justification for F.5 Prompt Visibility of Payment Status:**

**F.5.1 & F.5.2**

Ensuring immediate visibility to transaction activity provides for excellent user experience. Each transaction is instantly communicated to the user multiple ways. The user interface provides a transaction confirmation notice immediately to the Payer upon a successful transaction being sent. The Payee receives a push notification, email, and in-application notification that funds are available for receipt. Once the Payee accepts the VTM from the Payer, they are immediately provided a transaction Confirmation notice with the value of the transaction. The application also immediately provides a log of the transaction in the User’s transaction history immediately upon the Payer sending the VTM, and Immediately upon the Payee accepting the VTM. In addition to the above, the User’s account balance is immediately updated when the funds are sent, or received. All these activities provide the promptest, visual communication possible for transactions.

In the case of Business-based transactions, all the same prompts and visual notifications are possible within the platform. Ultimately, the business itself and the integration process with any required systems will dictate the level of notification in a business environment.
5. Legal Framework

_Self-assessed rating:_

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.1</td>
<td>Legal framework</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.2</td>
<td>Payment system rules</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.3</td>
<td>Consumer protections</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.4</td>
<td>Data privacy</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.5</td>
<td>Intellectual property</td>
</tr>
</tbody>
</table>
**Justification for L.1:**

Because of the simplicity of the MintChip ecosystem, a complex legal framework is not necessary to adequately protect participants. Because clearing, settlement and reconciliation are all instantaneous, rules regarding responsibilities and liabilities throughout those stages of a transaction are no longer necessary. Existing legislation that governs participants’ KYC and AML requirements will continue to apply, particularly during the participant-registration process. Within the ecosystem itself, payment rules are required, rather than a freestanding, newly-developed legal framework.

A regulatory framework will have to be developed to ensure that the Broker account held by the Originator are regularly reconciled. The fact that MintChip functions as a good funds ecosystems means that it is crucial that all MintChip USD is accounted for by the Originator. The good funds assurance means that little additional regulatory control is required to protect the ecosystem. In the absence of regulations in Canada, we have been following the European derivatives for electronic money and payment services directives. This includes protecting the ecosystem from the bankruptcy of asset manager holding the float (or pool). Additional “regulatory capital” may be required, but in the medium term we will invest the float in short term treasury bills, making the digital cash de facto backed by the same government that backs the fiat currency. This also means that no funds are on the balance sheet of the asset manager and thus not at risk. Finally, because there is no lending or leverage of the float, there is always a real dollar for every dollar of digital cash.

With respect to disputes involving the transaction that has given rise to the payment item (e.g. a store purchase or insurance payment), the MintChip ecosystem can provide a robust audit trail and secure vault for payment information. However, it is not intended to supplant existing consumer protection or dispute resolution regimes.

It is our understanding that Regulation E 12 CFR 205 does not apply to stored value products, and that the law applying to digital currencies generally is under development. Because of the scalability and flexibility of the MintChip platform, a variety of legal models could be supported depending on the specific use case. MintChip has been designed to facilitate appropriate regulatory control and guidance, rather than operate in a regulatory vacuum.
**Justification for L.2:**

The MintChip ecosystem can be supported by simply, principles-based payment rules that focus on the security of the on- and off-ramps into and out of the system. Within the system itself, few rules are needed because so many of the integration points have been eliminated. Once the End User has been properly authenticated, movement within the ecosystem does not require additional rules-based support.

With respect to the relationship between the Broker and Originator, detailed payments rules would need to be developed to support the regulatory regime described in L.1 above.

**Justification for L.3:**

Before completing a single transaction on the MintChip platform, each End User will be made aware that, as a Sender they are responsible and liable for every transaction that they send. The ecosystem has not been established to adjudicate consumer disputes. The real-time finality of MintChip cash means that there will be limited opportunity for error correction after a payment has been completed. Receiving parties must be able to rely on that immediate finality for the ecosystem to function as quickly and efficiently as possible.

However, nothing about the MintChip platform precludes the application of existing consumer protection regulations. In particular, laws related to distance contracts, electronic agreements would continue to apply.

**Justification for L.4:**

The robust security of the MintChip ecosystem also extends to participant personal and payment information and data. Moreover, the paperless nature of the system means that all data is secured in a central digital location, which removes needless duplication of personal information. The digitization of the information also means that Broker front-line employees do not have to be granted access to any more information than they are required to access on a case-by-case basis.

**Justification for L.5:**

Because the MintChip platform provides Open APIs and is fully-customizable, parties will own their respective intellectual property. The MintChip platform will not leverage any third-party IP and all participants’ IP rights should be well-protected by existing regulations/contract.
6. Governance:

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Governance</td>
<td>G.1</td>
<td>Effective governance</td>
</tr>
<tr>
<td>Governance</td>
<td>G.2</td>
<td>Inclusive governance</td>
</tr>
</tbody>
</table>

**Justification for G.1:**

The MintChip platform can be thought of a passive conduit with the objectives of supporting fast, efficient, low-cost payments. The rules that surround the on- and off-ramps will be developed by working with regulators and will follow existing law-making processes, which will support transparency, consultation - all of which supports the FPTF’s Public Policy Objectives.

**Justification for G.2:**

MintChip was designed to be regulator-friendly. Indeed, nanoPay believes that appropriate regulation can facilitate, rather than innovation within the MintChip ecosystem. The open APIs, etc.… mean that the system is designed to support transparency and foster competition. The more open access also fosters this transparency. The MintChip platform levels the playing field by allowing for more participants than might otherwise be permitted. Different participants with different needs bring a wider view and unique experiences that can inform policy-making.
APPENDICES

Appendix A: History of MintChip:

The Royal Canadian Mint (RCM) was founded in January 1908, as a Crown Corporation of the Government of Canada. The RCM has over 100 years of experience in currency and coinage production. The RCM is the world’s most diversified mint; between 1980 and 2005 produced over 52 Billion coins for over 62 different countries. In 2014 alone, the RCM produced over 2.4 billion coins for 17 different countries. If there is one organization on the planet that truly understands cash, it is the Royal Canadian Mint.

In 2012, Forecasting the decline of coinage both domestically and in foreign markets, along with a corresponding increase in the use of technologically-driven payment methods, the RCM commissioned the development of the world’s first regulator-friendly digital currency. Leveraging their century of experience and expert knowledge in regulatory requirements around the world, the Royal Canadian Mint developed very specific criteria for the digital currency they felt would best meet the needs of the changing payments landscape. The RCM then reached out to the top cryptocurrency experts across the globe to assist them in building a digital currency that met their high expectations.

David Everett, from Littlehampton, England, is arguably one of the world’s leading experts in the development of cryptocurrency and digital cash ecosystems. From 1990 to 1993, Everett played a key role in the design and development of the Mondex product. Mondex was one of the world’s first electronic currencies - developed even before widespread use of the Internet. Over the last twenty-five years, David has been focused on building digital currency ecosystems, having held key roles in the design and development of digital currency products like (Swift, add a couple more here)

This world-leading expertise and experience made Everett the ideal complement to the highly-experienced team the RCM had assembled to build the MintChip digital cash ecosystem and he worked on the product from 2012 to 2015. In 2014, after internal trials, the RCM determined that the MintChip ecosystem was ready for external market trials.

The MintChip ecosystem can enable transaction ranging from fractions of a cent to hundreds of millions of dollars. The digital cash ecosystem built by the Royal Canadian Mint can replace both the coinage produced by the RCM, it can also replicate the any currency of any denomination, including the notes produced by the Bank of Canada.

The Bank of Canada has the federal mandate to produce Canadian banknotes, which are effectively used to control the country's money supply. With the RCM’s creation of a digital cash
ecosystem, the Mint would also be in a position to produce digital notes, which could impact the country’s money supply. There would be the opportunity for confusion, as two government bodies would effectively have the same mandate. A change in the RCM’s mandate would be required to allow them to produce digital currency and such a change requires amendments to the Mint’s enabling legislation as well as changes to the Bank of Canada’s mandate. After the MintChip ecosystem had been built and was ready for trial two items were clarified: first, it became clear that the Canadian government was not prepared to amend the RCM’s mandate, which would have allowed it to commercialize the MintChip platform; and second, the Bank of Canada did not want to be responsible for commercializing and operating a digital cash ecosystem. For those reasons, the RCM put the MintChip out to bid within Canada. nanoPay entered the initial bidding process in April of 2015, and after multiple rounds of bidding, were awarded the exclusive negotiation opportunity with the RCM in August of 2015. In December of 2015, the deal closed and nanoPay acquired the assets of the MintChip ecosystem.
Appendix B: European Definitions and Perspectives

Definition of Digital Cash

In the Executive Summary we define our version of what digital cash is, but there is frequently a language problem in understanding what is meant by the terms digital cash, electronic money, virtual currency and cryptocurrency. These terms are often used interchangeably, this has consequences of misunderstanding of both our intent and our solution. So to clarify we have borrowed from the Europeans who have differentiated between these:

The ECB website defines e-money as “Electronic money (e-money) is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions.”

In October 2012 the ECM publish a paper on virtual currencies titled “Virtual Currency Schemes”, which defines the difference between our digital cash (electronic money) and cryptocurrencies quite well: “A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. Depending on their interaction with traditional, “real” money and the real economy, virtual currency schemes can be classified into three types: Type 1, which is used to refer to closed virtual currency schemes, basically used in an online game; Type 2 virtual currency schemes have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can subsequently be used to buy virtual goods and services, but exceptionally also to buy real goods and services; and Type 3 virtual currency schemes have bidirectional flows, i.e. the virtual currency in this respect acts like any other convertible currency, with two exchange rates (buy and sell), which can subsequently be used to buy virtual goods and services, but also to purchase real goods and services.

Virtual currency schemes differ from electronic money schemes insofar as the currency being used as the unit of account has no physical counterpart with legal tender status. The absence of a distinct legal framework leads to other important differences as well. Firstly, traditional financial actors, including central banks, are not involved. The issuer of the currency and scheme owner is usually a non-financial private company. This implies that typical financial sector regulation and supervision arrangements are not applicable. Secondly, the link between virtual currency and traditional currency (i.e. currency with a legal tender status) is not regulated by law, which might be problematic or costly when redeeming funds, if this is even permitted. Lastly, the fact that the currency is denominated differently (i.e. not euro, US dollar, etc.) means that complete control of the virtual currency is given to its issuer, who governs the scheme and manages the supply of money at will.”
Electronic Money Issuing


According to the European Commission's website, E-money is:

“Electronic money is a digital equivalent of cash, stored on an electronic device or remotely at a server. One common type of e-money is the 'electronic purse’, where users store relatively small amounts of money on their payment card or other smart card, to use for making small payments. But e-money can also be stored on (and used via) mobile phones or in a payment account on the internet.

The E-Money Directive (2009/110/EC) (EMD) aims to:

- enable new, innovative and secure electronic money services to be designed
- provide market access to new companies
- foster real and effective competition between all market participants.

This should benefit consumers, businesses and the wider European economy.

The directive focuses on modernising EU rules on electronic money, especially bringing the prudential regime for electronic money institutions, into line with the requirements for payment institutions in the Payment Services Directive.

*The E-Money Directive entered into force in all EU countries on 30 April 2011.*

See full Directive
Appendix C: Applicability of Regulation E

Today, digital cash is not regulated in a consistent manner from one jurisdiction to another. Similarly, mobile payments have often confounded regulators, who have struggled with regulating a technology that has been proven to evolve faster than the speed of regulatory drafting. Issues like customer liability and the security of biometric authentication, as well as its impact on fraud, have challenged consumer protection regimes.

The American regulatory landscape is equally challenging when it comes to digital cash and mobile payments. While it is possible that certain provisions of Regulation E could be interpreted broadly to apply to MintChip digital cash in certain instances, the Regulation was simply not drafted with a digital-cash ecosystem in mind. It could also be asserted by some parties that MintChip value is another form of stored or prepaid value and as such, falls outside of the provisions of Reg E.

nanoPay believes that MintChip digital cash differs from stored value products. It is designed to be pegged to fiat currency, ubiquitous and “Broker agnostic.” Digital cash in the MintChip platform is more secure than stored value products, accommodates the transmission of remittance information along with the payment itself and allows for a robust audit trail. These features make MintChip digital cash a unique payment type that is not adequately addressed by today’s regulatory framework. However, MintChip was designed to be regulatory-friendly. As such, we are seeking assistance from the Federal Reserve on the development of regulatory regime that would establish adequate safety and soundness of a digital cash ecosystem, while still allowing innovation and competition to flourish.

**Authority and purpose**

States that the primary objective of the regulation is to protect individual consumers who engage in electronic fund transfers; it is possible that MintChip could be considered an EFT rather than a stored value card and a such much of Regulation E should be applicable.

**Coverage**

Lists the types of transactions covered by the regulation--those initiated through an electronic terminal, telephone, computer, or magnetic tape to either order, instruct, or authorize a financial institution to debit or credit an account. These transfers include, but are not limited to, PoS and ATM transfers, direct deposits or withdrawals, telephone transfers, and transfers initiated through a debit card transaction. *We do not believe that Digital Cash or MintChip transactions fit within any of these descriptors. We assume that the Coverage descriptions will be updated to specifically include or exclude Digital Cash.*
General disclosure requirements; jointly offered services

States that a financial institution may combine the disclosure information required by the regulation with that required by other laws such as the Truth in Lending Act or the Truth in Savings Act as long as it is clear and understandable and is in a written form that consumers can keep. *We do not think this will be applicable to MintChip.*

Issuance of access devices

Stipulates that a depository institution may issue an access device (such as a debit card) only if a consumer has requested it either orally or in writing. **MintChip is an app or device provided by the Provider, so this will continue to apply to them. MintChip does have a generic app, and the End User can download this app.**

Liability of consumer for unauthorized transfers

Limits a consumer's liability for unauthorized electronic fund transfers, such as those arising from loss or theft of an access device, to $50; if the consumer fails to notify the depository institution in a timely fashion, the amount may be $500 or unlimited. **Even if the End User’s smartphone was lost or stolen, this would not allow the thief to transact. The SAS can be locked if the Provider is notified by the End User.**

Initial disclosures

Requires financial institutions to provide to consumers’ initial disclosures of the terms and conditions of EFT services. Institutions must disclose the consumer's liability for unauthorized EFTs, the types of EFTs the consumer may make, and any limit on the frequency or dollar amount; fees charged by the institution; and error-resolution procedures. Institutions must also provide a summary of various consumer rights under the regulation. *We do not think this will be applicable to MintChip.*

Change-in-terms notice; error-resolution notice

States that if there are adverse changes in fees, the consumer's liability, types of transfers available, or limits on transfers, the institution must provide a change-in-terms notice at least twenty-one days before the changes take effect. The institution must periodically send a reminder of the error-resolution procedures. It may send a detailed notice annually or provide an abbreviated notice with each account statement. *We believe that this should apply to MintChip.*

Receipts at electronic terminals; periodic statements

States that consumers must be provided documentation in two forms: terminal receipts and periodic statements. Consumers must receive a receipt when they initiate an electronic transfer and monthly in the form of periodic statements. Both documents must include the type of
electronic transfer; the amount and date of the transaction; the location of the terminal; and other
information. MintChip offers no paper statements, but the transaction data is available either
through the smartphone or can be downloaded in various formats, including but not limited to
CSV and common accounting packages.

Preauthorized transfers

Requires financial institutions to provide the consumer with some form of notice that electronic
transfers that recur at substantially regular intervals, such as the direct deposit of salaries or
benefits, and the preauthorized payment of bills, occurred as scheduled. This should apply to
MintChip, although the process and notifications are more timely. Consumers also have more
opportunities to recognize fraud and prevent payments that should not happen.

Procedures for resolving errors

States that if a consumer notifies an institution that an error involving an EFT has occurred, the
institution must investigate and resolve the claim within specified deadlines. Errors covered by
this requirement include unauthorized EFTs, incorrect EFTs, and the omission from an account
statement of an EFT that should have been included. This should apply to MintChip and we will
certainty provide timely resolution.

Relation to other laws

States that with regard to the issuance of access devices, consumer liability, and the unsolicited
issuance of credit cards, the financial institution must take into account the provisions set forth in
Regulation Z, Truth in Lending. In addition, the Federal Reserve Board shall determine whether
the request of a state, financial institution, or other interested party is preempted by state laws
relating to electronic fund transfers. Only state laws that are inconsistent with the act and this
regulation are preempted, and then only to the extent of the inconsistency. MintChip is not
involved in lending, credit or overdraft.

Administrative enforcement; record retention

Indicates which federal agency enforces the regulation for particular classes of institutions.
Records are to be retained for a period of not less than two years from the date disclosures are
required to be made or an action is required to be taken. Records are to be kept within this
regulation.

Electronic fund transfer service provider not holding consumer's account

States that a person who provides an electronic fund transfer service to a consumer but does not
hold the consumer's account is subject to many of the same requirements set forth in the
regulation. This does apply and is to be observed.
Electronic fund transfer of government benefits

States that a government agency is subject to the requirements of the regulation if directly or indirectly it issues an access device to a consumer for use in initiating an electronic fund transfer of government benefits from an account, other than needs-tested benefits in a program established under state or local law or administered by a state or local agency. This should apply.
Appendix D: Financial Inclusion

With over 90 million people in America that are either unbanked or underbanked, we have to believe that the biggest opportunity to improve the payments system is with this category. If we could make it cheaper and easier to be part of the formal economy, tax revenue would increase, these households would benefit from insurance and credit to protect their families and improve their standard of living, while paying less for financial services. The most alarming fact is how much this group of people pay for their financial services. Also looking at the table form the FDIC below, it is shocking that of the reasons given for not having a bank account, “Do not have enough money” and “account fees are too high or unpredictable” accounted for 57.5% and 30.8% respectively. The MintChip platform can help with both of these concerns, ID & credit problems, privacy and product concerns.

On a global scale over 2 billion people are financially excluded and 1.7bn of these are digitally recognizable through social media.

Reasons Households Were Unbanked

(Diagram #31)

Appendix E: MintChip Payment Flow

MintChip Payment Flow

(Diagram #32)
Appendix F: Real time tax collection

With MintChip it is possible to achieve a number of innovations in consumption tax. Firstly, if we can deliver payments with a marginal cost of close to zero and in doing so reduce the use of cash, we could reduce the tax gap (tax not paid on cash transactions). Note that even if you had a lower tax rate for digital cash payments, a Government would collect higher total taxes. This would also mean law enforcement could focus on cash as the only remaining use for cash would be for nefarious means.

Secondly as described in Section C, we could pay consumption tax in Real Time directly to the tax authority. This has a number of impacts:

- Small businesses would not have to collect and account for tax if we made it a part of the payments platform,
- Small businesses would also not be able to spend the tax they were supposed to collect and then have cash flow issues when they have to remit,
- With Real Time tax collection Federal and State Governments would know a lot more about their economies in Real Time,
- Steady and predictable tax income would allow for better budgeting and no year-end surprises.

Finally, if the tax was built into the payments platform, it would give state and even city tax authorities to vary local taxes to fund projects. Cities wanting to attract more businesses could lower taxes and others wanting to do large capital projects could raise them. Instead of all the retailers having to change the POS systems, it could just be a single click of a button on the MintChip platform.
Faster Payments Task Force Proposal

Revised Executive Summary: MintChip Solution

April 30, 2016 (revised August 24, 2016)
Submitted by: nanoPay Corporation
EXECUTIVE SUMMARY

I. A Digital Cash Vision
In our original submission to the Task Force, we focused the bulk of our discussion on the MintChip Platform as a digital replacement for banknotes and coins. In that submission, we posited that with widespread adoption of digital cash, the velocity of money is increased and inclusion in the financial system is broadened, without compromising that system’s integrity. Moreover, we stated that digital cash can solve many of the issues facing existing payments systems without requiring major changes to current banking systems or the role of central banks.

We submitted that digital cash was particularly exciting because, without the burden of high fees, it has the potential to enable more people to participate in the formal economy by meeting the needs of the unbanked and underbanked. With almost eight per cent of households unbanked and a further twenty per cent underbanked, almost ninety-three million people in America are effectively disenfranchised from participating in the financial system in any meaningful way. Affordable access to digital cash can help address many of the reasons people are unbanked.

Before going into a more fulsome consideration of the direct, collateralized bearer asset transfer model, it is still helpful to gain a thorough understanding of digital cash generally and the MintChip Platform specifically.

II. Digital Cash: An Introduction

Digital cash should be implemented as a fully collateralized bearer instrument to leverage all of the advantages of cash and add additional functionality that can only be achieved using a digital payments system. In this submission it is assumed that digital cash is implemented using this direct, collateralized bearer asset model.

1. Immediate settlement: Cash is a bearer instrument so it is settled the moment the cash is in the hands of the receiving party. Similarly, digital cash is settled at the moment it is received by the Payee.

2. Non-repudiation and irrevocability – Once the receiving party has accepted the cash as legitimate, the transaction is irrevocable and complete. The transaction cannot be repudiated because it is considered final upon receipt of the cash. Digital cash enjoys these properties.

1 M. Bruhna & I. Loveb: The Economic Impact of Banking the Unbanked: Evidence from Mexico; Federal Reserve: Consumers and Mobile Financial Services 2015, March 2015.
3. No physical constraints - Cash can only be used in person; it is nearly impossible to pay for goods and services online or remotely. Digital cash can easily support remote use cases as it can be sent via email, text, or even by regular mail.

4. Better economic analysis – Since cash transactions are not necessarily reliably reported, it is difficult to tax these transactions or identify their economic impact. Central banks cannot know with accuracy where the cash is - or even if it is within their own borders. Digital cash illuminates these otherwise dark pools cash transactions. All transactions can be identified, the impact on the economy is transparent and appropriate taxes can be assessed.

5. More secure – Digital cash is secure at all times. It cannot be stolen, lost or intercepted by an unintended recipient.

6. Less expensive – Using cash is not without cost. It requires both physical and electronic security. This security is required in stores, tills and to physically move the cash from place to place. It is also vulnerable to employee theft. Digital cash has a marginal transaction cost of close to zero, which in turn saves transaction costs for banks, consumers and merchants.

7. Privacy: Traditional cash transactions are private (not to be conflated with anonymous - the receiving party can usually see you.) There is no record of the actual transaction itself; instead, a receipt is a proxy for cash transaction. Digital cash has all of the same privacy, but every transaction is logged and allows regulators and law enforcement (with the appropriate authority) to manage the economy, protect consumers and prevent / investigate crimes.

III. What is MintChip?

MintChip is nanoPay’s version of a digital cash platform that has since been broadened into a direct, collateralized bearer asset transfer system. It securely stores and instantly transfers any form of digital assets between users on a single, verifiable platform. It was originally created by the Royal Canadian Mint (RCM), which is a Federal Crown Corporation accountable to the Canadian Minister of Finance. Canada has withdrawn pennies from circulation and there are ongoing discussions about withdrawing the one-hundred-dollar banknote. With the coins and notes in circulation under threat of withdrawal, the RCM undertook to build a digital cash platform that would effectively cannibalize their own mandate to make coins - which it does exclusively for Canada and for over sixty other countries. The RCM hired Dr. David Everett, a world authority on payments systems and digital cash to create the MintChip Platform. Everett’s mandate was to create a digital cash platform that was secure, scalable and regulator-friendly. In building a digital version of traditional cash, Everett consulted with law enforcement, regulators and the Bank of Canada. Meeting all of the regulator and central bank
requirements was a necessary condition for the RCM to succeed with MintChip, but not a sufficient one. While MintChip was regulator-friendly, the RCM’s mandate did not permit the Mint to support a digital cash platform. An amendment to the RCM’s legislative mandate was required; however the Federal Government declined to make the mandated changes. This refusal marked the beginning of a long sales process, which culminated in nanoPay’s acquisition of the MintChip assets in December 2015. nanoPay launched MintChip in Canada in April 2016, and MintChip 2.0 was deployed in Summer 2016.

IV. Bridging Gaps

According to the Federal Reserve’s 2013 Consultation Paper, there is widespread agreement on current gaps in the payments system. We submit that the MintChip Platform addresses, in one way or another, all of these gaps as well as others that were not identified and that will be discussed throughout this proposal.

1. **Continued end-user check writing:**

The MintChip Platform provides a viable, low-cost alternative to checks and would reduce end-user check writing for a variety of reasons.

Today, checks are often written today for individuals to pay other people (e.g. babysitters, family members and sole-proprietor businesses). The MintChip ecosystem supports these P2P transactions and allows for value to be received by the Payee immediately, without having to account for the time it takes funds to clear or the possibility of counterfeit or fraudulent checks. The Payer can be certain that funds have been debited from their account immediately, which helps with budgeting and avoiding NSF fees. As well, because the ecosystem can easily set up pre-authorized payments, some scenarios where post-dated checks are required can also be accommodated.

2. **Challenges in converting businesses to electronic payments:**

The MintChip Platform is a platform that can be layered on top of the existing payments infrastructure. Because of this layering, businesses can easily connect to the platform with minimal changes to their existing billing and accounting systems. Because the MintChip ecosystem is capable of supporting the transmission of data (such as remittance information) along with value, end-to-end straight-through processing (including reconciliation and posting of payments) is possible for businesses of virtually any size. As will be discussed in greater detail below, the Platform is also capable of moving most assets in the same peer-to-peer fashion, which adds to the flexibility of the solution.
3. *Closed-payment communities:*

While it is true that the MintChip ecosystem is a type of closed-payment community, as will be demonstrated below, the barriers to entry are so low that virtually any Entity can participate for low to no cost.

4. *Lack of contemporary features in traditional payment channels:*

The MintChip Platform uses some of the most innovative contemporary payments features, such as near-real-time notification and settlement. Moreover, the scalability of the platform means that new innovations can be easily incorporated into the MintChip infrastructure without having to make costly upgrades to Participants’ legacy systems.

5. *Faster payments:*

As will be demonstrated below, the primary benefit of the MintChip Platform is its ability to send payments virtually instantaneously, clearing and settling them in real time.

6. *Obstacles in international payments:*

The MintChip Platform has been built with cross-border and multi-currency payments in mind. These payments will clear and settle within the ecosystem as quickly as domestic, single currency payments.

7. *Mobile technology revolution:*

The MintChip Platform is designed to be mobile-first, leveraging the worldwide ubiquity of smartphones and is primarily accessed via mobile device.

8. *Security concerns:*

The MintChip ecosystem is highly secure and leverages state-of-the-art cryptography. The security of the platform is explored in great detail below.
V. Direct, Collateralized Bearer Asset Transfer: A Broader Vision

Before proceeding with a detailed review of the MintChip technology, it is crucial to note that we have broadened our vision of the MintChip solution significantly. Since our initial response to the Task Force, we have continued to work with the Platform to refine the technology and develop new use cases that have applications beyond simply cash replacement. As a result, the MintChip Platform has evolved from moving digital cash to a payment platform that leverages a *direct, collateralized bearer asset transfer model* to move *any* form of digital asset or other value between participants’ Secure Asset Stores.

For the purposes of the MintChip Platform, direct, collateralized bearer asset transfer simply means that an asset can be irrevocably transferred from one party to another without the need for an intermediary. The asset being transferred is also fully collateralized. With our Platform, further benefits are that the transfer is also highly secure and virtually instantaneous.

As a result of our further expansion of the Platform, the Task Force will notice a refinement and a broadening of our responses to the follow-up questions. It is important to note that our continued broadening of the Platform should not be taken as an indication that nanoPay has lessened its commitment to digital cash. We firmly believe that digital cash is the way of the future and that our Platform could facilitate the transition to cashless society. However, that transition is not likely to happen in isolation. For digital cash to truly gain a foothold, a variety of technological advances must also occur to the broader payments ecosystem. The MintChip Platform, with its low implementation costs, scalability and broad range of possible use cases, is ideally positioned to facilitate the gradual transition to a digital cash economy.

V. Technology Overview

**The MintChip Ecosystem:**

The MintChip ecosystem was designed as an electronic payments platform to achieve the following objectives:

- **Speed**;
- **Security**;
- **Efficiency**;
- **International Capabilities**; and
- **Collaboration Opportunities**.
**Speed**
MintChip transactions are Peer-to-Peer transactions that do not require an intermediary and can clear and settle in near Real-Time.

**Security**
Regardless of transaction value, all MintChip transactions are completed in highly-secure Hardware Security Modules (HSMs), the same hardware used in today’s global payments systems. Value Transfer Messages (VTMs) are signed using an approach backed by various patents. The cryptographic algorithms in MintChip can be dynamically upgraded across the entire ecosystem as future security threats are identified.

**International Capabilities**
The MintChip ecosystem only allows for one Originator per fiat currency. Foreign exchange services and cross-border transactions are made possible by leveraging providers who act as Brokers in more than one country or fiat currency.

**Collaboration Opportunities**
The MintChip Platform was designed as a global solution to create payments ecosystems built on a collection of robust, open and easy-to-use APIs to enable broad array of participants to create novel direct asset transfer solutions.

The Platform leverages a direct bearer asset transfer model to move value in real time without an intermediary. The model means that, contrary to conventional payments systems where value is held by intermediaries, the MintChip Platform is a good funds peer-to-peer payment system that transfers value quickly and securely from one party to another.

This direct bearer asset transfer model is more efficient than conventional payment systems and has clear benefits:

- It supports both Push and Pull transactions;
- The value transfer is instant and irrevocable;
- The model requires no intermediaries;
- It operates in both online and offline environments; and
- There is immediate, irrevocable payment authorization.
The MintChip ecosystem includes the following participants and allows a participant to play one or more roles:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>Manages the: (1) operation of the stand-alone MintChip Platform component, which creates MintChip value and Secure Asset Stores; (2) administration of the security parameters in the MintChip Ecosystem; and (3) pooled account that holds fiat currency for MintChip value sold to the Brokers.</td>
</tr>
<tr>
<td>Technology Provider</td>
<td>The Owner of the MintChip Platform that: (1) provides the system components for deployment by the Platform Operator and the Originator; (2) integration support for Brokers and Merchants; and (3) software enhancements, maintenance and support.</td>
</tr>
<tr>
<td>Platform Operator</td>
<td>Responsible for the: (1) deployment and operation of the MintChip Platform; and (2) administration of the operating rules, standards and protocols.</td>
</tr>
<tr>
<td>Broker</td>
<td>A Provider (depository institution, regulated non-bank account provider) that: (1) buys and sells MintChip value from/to Originator; (2) enrolls End Users; (3) provides mechanisms for End Users to buy and sell MintChip value; and (4) provides currency conversion services (optional).</td>
</tr>
<tr>
<td>End User</td>
<td>An Entity that uses a payment service for the purpose of sending or receiving payments, such as a business, a Consumer, or a government agency.</td>
</tr>
</tbody>
</table>
**Originator:**
The ecosystem has been built so that when the platform achieves a certain scale within a country, the Central Bank, or a branch/division of the Central Bank may act as the Originator within that ecosystem. It is the Originator’s role to create (or “mint”) MintChip value in a designated currency. The system is built to support a single Originator for each currency created in the ecosystem.

**Broker:**
The Broker role is made available to new and existing providers in the current payment systems through open APIs. A Broker will use these APIs to provide End Users access the MintChip Platform through their existing mobile applications or online services. It is anticipated the first Brokers in the MintChip ecosystem will be depository institutions, regulated non-bank account providers and large retailers. Lowering the barriers to entry through our open platform will encourage new participants who can focus on providing value-added services.

A Broker opens a MintChip account with the Originator and establishes one or more Secure Asset Stores (SAS) on the MintChip Platform. The Broker pre-purchases MintChip value from the Originator to meet the needs of their End Users. This is done by the Broker transferring fiat currency or value to the Originator’s pooled account and the Originator loading equivalent MintChip value into the Broker’s SAS.

The Broker’s role is then to sell or redeem MintChip value to and from (as the case may be) End Users who purchase MintChip value with fiat currency. The Broker is also the participant that establishes MintChip accounts for End Users. Because Brokers will be current Providers in the
existing traditional financial and payments systems, they will be in a position to complete Know Your Customer (KYC) requirements and comply with applicable Anti-Money Laundering (AML) requirements at the time of End User registration. Through their existing billing systems, Brokers may charge the End User fees for participating in the ecosystem.

**End User**
End Users can be individual consumers, businesses, governments or government agencies. End Users open MintChip accounts with Brokers and are assigned Secure Asset Stores (SASs) to hold value in a specified currency. For this reason, End Users may have more than one SAS in the same or multiple currencies. For example, one SAS may contain USD and another may contain CAD. All transactions completed in the MintChip ecosystem are a transfer of value between two different SASs. Value Transfer Messages (VTMs) facilitate the exchange and represent the monetary value in transit. The VTM can only be consumed by the Receiver’s (Payee) SAS and is cryptographically encrypted and signed to prevent tampering. MintChip SASs are only able to exchange value with a SAS that shares the same currency.

**Secure Asset Store (SAS):**
The MintChip ecosystem also distinguishes itself from other payments system through its use of Secure Asset Stores (SAS). A SAS can be thought of as a digital safe deposit box that contains:

1. A unique SAS identification number;
2. Identity information for the Entity associated with the SAS;
3. A ledger that tracks every transaction that occurs within the SAS; and
4. Secure storage for the MintChip value.

**Value Transfer Message (VTM):**
The MintChip technology is elegant in its simplicity and begins with a concept that differs dramatically different from the concepts driving today’s payments systems. If you reduce transactions to packets of data and ensure that those packets are incredibly secure, then the manner in which those packets move from user to user is flexible, low-risk, highly-adaptable and very efficient. The nature of today’s payments systems, built on legacy systems and in piecemeal fashion, means that system operators and participants must focus on ensuring end-to-end system security for each payment, which is costly, time-consuming and ultimately means that a particular network is only as secure as its weakest link.

The VTM is patented technology that is small but highly-secure. The VTM contains the four critical pieces of data required to complete a transaction:

- Payer ID;
- amount;
Every transaction must contain this information before a VTM can be created. Once created, the Message is digitally signed in the HSM, which ensures the highest level of security. The patented technology within the VTM ensures that even if the VTM is captured during transmission and someone succeeds in breaking its encryption, the only information is revealed is the intended Payee’s location. There are also multiple additional security features that both prevent the occurrence of a security breach and identify breaches if they occur.
VI. The MintChip Ecosystem is a Good Funds Model

MintChip value in a MintChip account SAS is backed by an equivalent value of fiat currency in the Originator’s pooled account.

Value is transferred into a SAS by converting USD funds into a digital representation of the currency through a MintChip Broker - creating MintChip value. As part of the conversion, the USD funds are deposited into the Originator’s pooled account, ensuring all MintChip value is backed by USD funds. This structure ensures that MintChip value is pegged to, and at par with traditional USD. This requirement also means that any transactions occurring on the MintChip Platform follows a good funds model and virtually eliminates the risk of transacting within the platform. This model also reduces participant costs and system requirements that are required to verify payments in today’s payment ecosystems.
V. Loading Value into the MintChip Ecosystem

The conversion of funds from fiat currency outside the MintChip ecosystem to MintChip digital currency within the ecosystem can only be completed through a MintChip Broker. The Broker accesses the MintChip ecosystem using the open APIs and embeds the features and functionality of the platform within their own applications.

There are two options for funding digital cash payments, which will enable different user experiences:

<table>
<thead>
<tr>
<th>“Standalone Account Model”: End User transfers funds to digital cash for multiple subsequent payments</th>
<th>“Integrated Account Model”: Digital Cash payments are funded to/from an account on a one-to-one basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Used mainly by non-bank brokers.</td>
<td>● Deposit-taking institutions are uniquely positioned to allow real-time digital cash payments tied to a traditional account. (e.g. DDA, LOC/CC).</td>
</tr>
<tr>
<td>● The End User is explicitly aware of their digital cash balance.</td>
<td>● Seamless End User experience: ○ there is no separate digital cash balance to maintain; and ○ digital payments are made from/to the linked account.</td>
</tr>
<tr>
<td>● The End User transfers funds to and from digital cash to maintain a balance.</td>
<td>● Digital cash balance is kept at zero, with one-to-one funding to and from the account to make payments.</td>
</tr>
<tr>
<td>● Payments are made from the digital cash balance.</td>
<td></td>
</tr>
</tbody>
</table>

**Standalone Account Model:**

In the Standalone Account Model, the End User accesses the MintChip Platform through the Broker’s application. The End User selects the “Load Value” option from the application and they will be presented with a list of the available funding sources that they have previously registered into their account when they established their MintChip account. Diagram # X outlines the potential funding sources the End User can use to load fiat currency into their SAS. It is important to note that a large portion of Brokers are anticipated to be existing financial institutions allowing users the capability to easily transfer funds between the End User’s accounts. (e.g. savings accounts, checking accounts, credit/debit card or line of credit).
Once the funding source is selected, the End User can select the amount to load into their MintChip account and associated SAS. In most instances the funding source will be a deposit account held by the Broker (e.g. the End User’s retail bank). The Broker receives the funds from the MintChip End User and then delivers the MintChip value directly into the End User’s SAS. As mentioned above, these transfers may also happen seamlessly, without End User initiation.

**Integrated Account Model:**

With the Integrated Account Model, the Platform can be seamlessly integrated into the Broker’s existing mobile application. In this case, the End User does not need to load value into their individual SAS. Instead, the End User’s SAS is automatically set to zero until they initiate a transaction. Upon initiation:

1. The Broker/bank transfers the transaction amount from the End User’s DDA to digital cash:
   - the bank debits the consumer DDA and credits its suspense account; and
   - initiates value transfer from the Bank SAS to the End-User SAS.
2. A digital cash payment is completed:
   - This is simply a standard VTM; the End-User SAS has the balance equal to the transaction amount and the transaction is successfully completed.

In this Model, the End User has effectively had funds “loaded” into the MintChip Platform to transact across the Platform with digital cash transactions deducted from their DDA on one-to-one basis without having to take any additional steps. From an End-User perspective, they do not even have to be made aware of the existence of the Platform or intentionally trigger its use.

Because these systems can leverage existing methods for authenticating End Users and the value being loaded into the ecosystem, this onboarding process ensures the funds used to credit the individual SAS tied to the MintChip account are truly good funds.

**VI. Removing Value from the MintChip Ecosystem**

The conversion of digital currency from an End User’s MintChip account can only be completed through the User’s Broker.

With the Standalone Account Model, in a manner similar to loading value into the ecosystem, the End User accesses the MintChip Platform from within the Broker’s application. The End User then selects “Value Unload” from the options menu. This option may either be presented within a consumer application or a business- specific application (for example, in the case of a merchant). The End User will enter the value of MintChip digital currency they wish to unload, and will be prompted to select one of the previously-registered accounts into which the funds will be deposited (e.g. a deposit account held at their financial institution). The Broker then
initiates transfer of the MintChip value from End User’s SAS to the Broker’s SAS and deposits the equivalent amount in fiat currency into the End User’s selected account.

With Integrated Account Model, as with loading value into the ecosystem, value can be removed seamlessly, without requiring End-User initiation.

Different ways in which value can be loaded into the ecosystem.

VII. Security Overview of the MintChip Ecosystem

The MintChip solution at its core is:
1. A distributed system of Secure Asset Stores (SASs); and
2. A messaging protocol that enables the trusted exchange of value between these Stores (Value Transfer Messages).

Central to the MintChip ecosystem and the root of the trust in the platform is the “Security Series”. This is a secured certificate that provides a shared signing authority, which assures participants of message authenticity and integrity.

The key differentiator between the MintChip Platform and other electronic payments systems is the patented technology that protects the transfer of assets (value) between two End Users. Regardless of value, all MintChip transactions are completed in highly-secure HSMs, the same hardware used in today’s global payments systems. VTMs are encrypted and signed using an
approach backed by four patents. By securing VTMs, the MintChip ecosystem is able to operate in a manner that allows for the completion of transactions offline, which is a unique feature unique to the Platform.

The MintChip Platform has been built to ensure that the benefit of breaching its security is outweighed by the cost, effort, and resources necessary to do so. Because hacking the system is so costly and the potential return of it so low, hackers will look to other ecosystems, where return for their efforts could be much greater.

The VTM technology and the patented cryptography that protects the VTM can be quickly upgraded at any time, with no system downtime and at a very low cost. As technologies like quantum computing become available to potential hackers, post-quantum cryptography can be used to increase encryption surrounding the VTM, ensuring it remains secure against new hacking techniques.

The MintChip Platform is ultimately user- and use-case-agnostic; designed to apply the same patented high security to each transaction regardless of its value. The technology supports transactions as small as 1/100 of a cent and as large as hundreds of millions of dollars. Moreover, the transactions are small enough to allow for the storage of transaction in the SAS of both parties. This rich supply of data means that compliance with virtually any regulatory regime is possible - which in turn enables the potential for global deployment of the Platform.

VIII. Integration to Existing Financial Systems

The MintChip ecosystem enables End Users to exchange value quickly and securely. The system provides easy integration into financial systems in the form of open connections points (on-ramps and off-ramps) that enable End Users to move money into and out of the MintChip ecosystem. These integration points are leveraged by End Users and provided by Brokers to facilitate payments and foreign exchange. The MintChip Application Programming Interface (API) leverages ISO 20022 message standards to simplify integration and process financial transactions.

IX. Speed to Complete a Transaction

Today, the speed of technology enables the transfer of information between two parties in near real time. Transactions within the MintChip Platform are also performed at that same speed. Because the Platform transacts only in good funds, the traditional processes of Payer Authorization, Approval by the Payer’s Provider, Clearing, Settlement and Reconciliation are handled very differently. The actual Clearing and Settlement between the parties of a
transaction on today’s payment systems takes substantial time and parties can incur significant risk. On the MintChip ecosystem, Clearing and Settlement between parties is effectively completed with each transaction in real time and with finality. If there are funds within a Participant SAS, they can initiate a transaction up to the value of their balance. As soon as the Payer initiates the transaction, that value is instantly removed from the Payer’s account balance and the payment is irrevocable. Effectively the payment is cleared, and immediately upon the Payee receiving the funds the transaction can be considered settled, and a digital receipt is issued. This process for completing a transaction is the same regardless of the user (Person, Business, or Government) or the use case. This makes the platform extremely flexible and cost-effective, as further detailed below.

X. Transaction Cost

The design of the current payment ecosystem is such that current participants can incur high costs associated with completing transactions. These costs exist primarily because of three factors:

1. Fraudulent transactions;
2. Requirement to secure the end-to-end ecosystem; and
3. Cost to scale.

While other factors add to the transaction cost, these are the primary drivers. The MintChip ecosystem addresses these issues simply.

First, every transaction is completed in exactly the same manner. The design of the MintChip ecosystem is such that a Broker can easily connect to the MintChip Platform through open API’s. Once connected, Brokers can avail themselves of the enhanced security the Platform provides, reducing the risk and cost associated with fraudulent transactions while increasing the overall security in the ecosystem.

Second, the MintChip ecosystem is focused on securing the VTM rather than securing the end-to-end communication channels through which the VTM travels. Recall that the VTM is the unique technology that enables secure transactions to occur. The ability to seamlessly and inexpensively upgrade cryptography at any time ensures the platform will remain secure, regardless of how quickly new technology evolves or the channel through which the VTM travels.

Third, the throughput capacity and scalability of the MintChip Platform takes the real cost to complete a marginal transaction close to $0.00. The platform has been designed to cost-effectively scale as quickly as required. The current platform has the capability to complete thousands of simultaneous transaction per second. To scale the MintChip Platform to a capacity of approximately 50,000 transactions per second would cost less than one million dollars and take less than 30 days.
XI. Ease of access for new participants

There are many barriers to entry for new entrants to participate in current payments systems, with cost and the regulatory compliance at the top of the list. Historically, payments system participants have preferred to keep participation exclusive and restrictive. This strategy has effectively slowed the evolution of payments platforms and kept transaction costs high.

The MintChip Platform takes the opposite approach and has been built to encourage participants to access the system through open APIs. This openness enables existing participants the ability to migrate to a new platform and more importantly, allows new participants to enter the ecosystem. As previously described, the cost to complete a transaction on the MintChip Platform approaches zero and by allowing access to many participants (both new and existing), market forces will drive the per-transaction cost for End Users as low as possible.

XII. Ease of regulatory compliance

Regulatory compliance is growing increasingly complex and burdensome for payments system participants. Strong regulatory frameworks are essential to reduce fraud and counteract money laundering and terrorist-financing efforts. Legacy payment systems can often struggle to keep up with a rapidly-changing regulatory landscape.

The MintChip Platform was designed to address many of the regulatory compliance issues participants will face across the globe. At the foundation of regulatory compliance is the need to: authenticate the parties to a transaction; identify the value of the transaction; and record and store every transaction along with important data about the transaction. At the same time, a modern payments system must also protect End-User privacy.

The MintChip Platform design ensures that End Users establishing a MintChip account are identified and authenticated before establishing a SAS. The level of authentication can be increased based on the nature and value of the transactions the End User is completing. This graduated authentication protocol ensures that all AML and KYC requirements can be met. Given that the funds in the MintChip ecosystem must be loaded through a Broker, End-User authentication data can be validated with that Broker as well as through other sources.

Each MintChip account and associated SAS on the MintChip Platform is linked to an authenticated End User and every transaction that occurs involving that specific SAS is stored within a ledger that sits within the specific SAS. This ledger can be accessed by regulatory enforcement agencies by following existing legal processes and procedures for access, which ensures the rights to privacy of the individual are protected.
Because the MintChip Platform supports this level of regulatory compliance, the compliance burden is lessened for ecosystem participants.

XII. Conclusion

nanoPay is confident that the MintChip Platform meets all of the Task Force’s desired outcomes of speed, security, efficiency and international capability. As evidenced in this Proposal, the platform can also be assessed as “Very Effective” against the majority of the outlined Effectiveness Criteria.

We look forward to taking a collaborative approach in working with a broad array of participants to make material progress in implementing our MintChip Solution to support the improvement of the U.S. payment system.
Faster Payments Task Force Proposal
Response to Preliminary Assessment

August 24, 2016
Submitted by: nanoPay Corporation
# Table of Contents

**Introduction** .................................................................................................................. 4

**Responses to Preliminary Assessment Questions** .............................................................. 5

**Efficiency** ............................................................................................................................. 11

- E.1.1 ........................................................................................................................................ 11
- E.3.1 ........................................................................................................................................ 11
- E.3.1 ........................................................................................................................................ 11
- E.3.1 ........................................................................................................................................ 11
- E.6.2 ........................................................................................................................................ 15
- E.7.2 ........................................................................................................................................ 15
- E.7.3 ........................................................................................................................................ 15

**Risk Management** .............................................................................................................. 16

- S.1.3 ........................................................................................................................................ 16
- S.1.5 ........................................................................................................................................ 17
- S.3.3 ........................................................................................................................................ 17
- S.4.1 ........................................................................................................................................ 18
- S.5.1 ........................................................................................................................................ 19
- S.5.4 ........................................................................................................................................ 20
- S.6.1 ........................................................................................................................................ 20
- S.6.7 ........................................................................................................................................ 20
- S.7.3 ........................................................................................................................................ 20
- S.8.1 ........................................................................................................................................ 21
- S.8.2 ........................................................................................................................................ 21
- S.8.3 ........................................................................................................................................ 22
- S.8.4 ........................................................................................................................................ 22
- S.8.5 ........................................................................................................................................ 23
- S.9.1 ........................................................................................................................................ 23
- S.10.6 ..................................................................................................................................... 23
Introduction

Before proceeding with a detailed review of the MintChip technology and formal response to the questions provided in the Preliminary Assessment, it is crucial to note that we have broadened our vision of the MintChip Solution significantly. Since our initial response to the Task Force, we have continued to work with the Platform to refine the technology and develop new use cases that have applications beyond simply cash replacement. As a result, the MintChip Platform has evolved from moving digital cash to a payment platform that leverages a direct, collateralized bearer asset transfer model to move any form of digital asset or other value between participants’ Secure Asset Stores (SASs).

For the purposes of the MintChip Platform, direct, collateralized bearer asset transfer simply means that an asset can be irrevocably transferred from one party to another without the need for an intermediary. The asset being transferred is also fully collateralized. With our Platform, further benefits included a transfer that is also highly secure and virtually instantaneous.

As a result of our further expansion of the Platform, the Task Force will notice a refinement and broadening of our responses to the follow-up questions. It is important to note that our continued evolution of the Platform should not be taken as an indication that nanoPay has lessened its commitment to digital cash. We firmly believe digital cash is the way of the future and that our Platform could facilitate the transition to a cashless society. However, that transition is not likely to happen in isolation. For digital cash to truly gain a foothold, a variety of technological advances must also occur to the broader payments ecosystem. The MintChip Platform, with its low implementation costs, scalability and broad range of possible use cases, is ideally positioned to facilitate the gradual transition to a digital cash economy.
Responses to Preliminary Assessment Questions

Ubiquity

**U.1.3**

*What happens when a Payee does not have a SAS set up to accept a given currency?*

If a Payee has a MintChip SAS in a currency that differs from the currency the Payer is trying to send them, the Platform has been designed to facilitate the payment as follows:

When the Payer first identifies the recipient, they will receive a message indicating that the Payee does not have an SAS in the appropriate currency. The Payer will then be provided with an option to select in which currency to send the payment. Depending on the currency chosen, the Payer (on send) or Payee (on receipt) will be directed to a FOREX Broker to convert the funds and complete the transaction.

If the Payee does not have a SAS in any currency (i.e. does not participate in the MintChip ecosystem), they will be asked to set up a SAS, which is easy to do and requires minimal personal information. The process and requirements for establishing an account are outlined in detail in our original proposal. (Part A, Section 1, Solution Description)

**U.1.5**

*How are providers motivated to participate and to make the solution available to End Users? How are governments motivated to provide the proper licenses? Who is the originator if not the government?*

How are providers motivated to participate and to make the solution available to end-users?

Reduce Costs:

- The Platform provides the lowest-cost transaction platform for Providers, which can immediately reduce their transaction costs.
- Lower costs allow Providers to develop new products and/or extend services to End Users who would previously not have been profitable or viable customers.
- The Platform can be layered on top of existing technology, minimizing any cost associated with building new systems.

Develop Value-Added Services (Platform for innovation):

- The open nature of the Platform allows Providers to easily integrate it into their existing mobile banking/wallet applications to provide an improved user experience and other value-added features (e.g. faster and lower cost payments, built-in loyalty).
● The Platform allows Providers to create new use cases for all types of End Users, including consumers, businesses and governments.
● The MintChip Platform is ISO 20022 ready, so Providers could be able to offer their business customers straight through processing in early 2017.
● The core transaction Platform may support and be a more efficient method to complete many internal transactions for the Providers (e.g. making payment between subsidiaries and affiliates).

How are governments motivated to provide the proper licenses?

The MintChip Platform was purpose-built to comply with regulatory requirements on a global basis. The licensing requirements will vary based on the use case the Platform is supporting and the country in which the Platform is operating. In many instances a license won't be required. In those use cases where licenses such as Money Transmission Licenses or E-money licenses are required, nanoPay will apply for and comply with the relevant licenses. Note that in many instances, the Platform will simply be providing a service to licensed Brokers and Providers. In these cases, nanoPay will simply be acting as a third-party service provider. As such, some licensing requirements may not apply.

Generally, governments may be motivated to license the MintChip Platform because:
● The digital cash use case delivers real-time settlement, which increases the velocity of money in the ecosystem, leading to a more efficient payments system and the accompanying economic benefits that efficiency provides.
● A digital cash platform provides visibility for government agencies into individual transactions which in a cash environment are very difficult to see. The effectively serves to increase the taxation opportunity on many transaction that today occur without government knowledge.
● The MintChip Platform allows Merchants to make real-time tax payments. At the time of the transaction, the tax component of the payment can automatically be sent directly to the appropriate tax authority. Real-time tax payments remove the burden of collection and calculation from the merchant and allow more predictable tax revenue for the authority. Real-time economic data can also be captured.
● The open architecture and flexibility of the Platform promote innovation by both existing and new ecosystem participants.
● MintChip is a viable fiat-based alternative to bitcoin and other cryptocurrencies. This digital cash platform offers millennials and early adopters a secure, instant payment method within the existing financial system.

Who is the Originator if not the government?

As outlined in this documents, the MintChip Platform has multiple use cases that do not require a government to assume the role of Originator. In use cases where an Originator is not a governmental body, it is anticipated that pooled funds will be protected by being held by an Asset Manager to ensure
that pooled funds are invested only in instruments where the principal is guaranteed. nanoPay assumes that, if Platform ubiquity is achieved and the corresponding pooled funds held by the Originator are material to the economy, the central bank will want to play an active role in the ecosystem, initially as a regulator, and perhaps even as the Originator.

Any asset manager could act as the Originator, whose primary purpose is to collateralize the digital cash. We are working with our lead investor to identify the best way of ensuring confidence in the ecosystem.

Note that the Originator role is applicable only to a digital cash deployment of the Platform. If an FI deployed the technology for a closed loop use cases that FI would be the Originator and would be subject to the same deposit requirements as it is today.

U.3.5

Please provide more detail about the error resolution process.

What are the rights and liabilities of the Payer and Payee?

While we continue to believe an efficient, modern system is one that minimizes the number of errors and disputes, our thinking has evolved as we’ve gained experience and traction in the Canadian market. To that end, we believe it is essential that all parties to a given transaction know how errors will be dealt with, where responsibilities lie and how liability will be allocated. Indeed, a robust error-corrections process will incentivize users to adopt the new Platform by minimizing uncertainty and reassuring user of the Platform’s legitimacy. nanoPay believes error corrections and dispute resolutions should happen quickly and efficiently and be automated as much as possible.

Errors in the MintChip system can be categorized as either customer- (End User) or system-generated errors.

Customer (End User)-generated Errors:

These errors include issues like sending a payment to the wrong Payee, or sending the wrong payment amount. The Platform includes confirmation logic to provide customers with opportunities to identify and correct information before confirming a payment. If, in spite of this logic, an error is still generated, the Payer is instructed to initiate an automated resolution process to correct the issue. This process allows the Payer to request a full or partial repayment by sending a payment request (i.e. a MintChip VRM- Value Request Message) to the Payee. If the Payee does not complete the VRM and resolution cannot be reached, then a formal dispute resolution process can be initiated with the Broker. However, the Broker cannot compel the Payee to return funds unless the End Users have agreed to participate in a dispute resolution process. The finality of the MintChip payment means some errors will not be resolved through the MintChip Platform. However, it is also the case today with other payment methods, including cash and other electronic peer-to-peer transfer platforms.
Practically, we anticipate most customer-generated errors to be corrected through the VRM process. In the case of peer-to-peer transfers, Payers are likely to have some type of relationship with the Payee and the dispute should be easy to resolve. In the case to C2B payments, businesses are motivated to correct errors in an effort to keep the relationship with their customer.

System-generated Errors:

These errors include all those not generated by End-User customers. System-generated errors are corrected by Brokers, who have access to an Administration Portal where they can review and confirm transactions and request any necessary corrections be completed by the Platform provider. End Users will be prompted to contact their Broker to initiate an investigation and resolution process in these instances. In the event of system-generated errors, Platform rules will clearly articulate that impacted End Users and Brokers will be made whole.

End-User Customer Responsibilities:

End Users also have responsibilities when participating in the Platform. These responsibilities will be laid out in clear and simple language in the initial Terms and Conditions presented to End Users. Among those responsibilities are the requirements to verify:

the transaction amount before sending the payment;
Payee information;
their account information and transaction history.

Customer End Users also have a responsibility to regularly verify their transaction history for accuracy and to promptly report any errors or suspicious transactions as well as any lost or stolen mobile devices.

End-User Customer Protections:

When assessing End User rights and protections, the MintChip Platform will leverage the compliance guidelines laid out in Regulation E for Electronic Funds Transfer, which provides the general framework and an agreed upon standards that establishes the liabilities, and responsibilities of participants in electronic fund transfer systems.
**U.4.1**

*How do the metadata links work and what type of contextual data can be associated with the payment?*

nanoPay uses ISO 20022 messages to link contextual data to MintChip payments and is in the process of applying to register MintChip ISO 20022 payments messages to create VTM payments and VRMs (payment requests). These messages are based almost entirely on the existing payment message fields adopted by this ISO standard for other financial institutions, with slight alterations to account for a digital, direct asset transfer model (e.g. multiple forms of ID used to initiate the request and/or associate it with a SAS). There are hundreds of fields, including fields for line item SKU data, trade settlement and agreement data, and trade delivery data.

These fields can be included in a payment, which will be transformed into an XML-formatted ISO 20022 payment message that can be sent to a third party. As well, a message itself can be sent as an alternative to the usual payload used for initiating a payment or payment request. ISO 20022 contextual metadata is provided as a part of the transaction history for any SAS.

**U.4.2**

*How would MintChip integrate contextual data with interfacing business and personal finance systems? What is the integration approach/process?*

The MintChip Platform has adopted the ISO 20022 standard to deliver payments messages to business and personal finance systems supporting this format. MintChip VTM can embed a link to ISO 20022 contextual data for every payment. In the event a system does not yet support ISO 20022, interfaces can be easily created to access the contextual data using the MintChip API. The first interface will be the ability to export all transactions in QIF format.

*What is the integration approach/process?*
We have initiated conversations with key providers of business and personal finance systems to integrate both payment requests and metadata for received payments.

**U.4.2**

*Please provide more details on how MintChip would enable payment to many parties at the same time?*

The MintChip Platform supports processing digital payments in batch. Users can upload a CSV file of pending payments, including Payee information as well as the date, time and payment amount. Additional contextual data can be linked to the payment based on ISO 20022 standard messages.

A MintChip batch payment endpoint is also available as part of the API to enable developers to programmatically process batch payments directly from their existing systems.
Smaller companies might choose the simple CSV solution, while larger organizations will probably use the batch payment API endpoint.

In addition, MintChip supports the capability to distribute a single payment to multiple recipients. For example, a payment in a restaurant could be divided automatically between the restaurant itself, the server, the tax authority and the franchisor. This functionality would not necessarily be made apparent to the End User, who would simply be paying for their meal.

U.5.2

*How will the Solution address interoperability differences in messaging standards, languages, character sets, mandatory data elements, party/account identifiers, regulatory considerations, and timing of settlement and good funds availability?*

MintChip has implemented support for ISO 20022 payment system messages to address interoperability with international financial systems to ensure funds can be received into non-participating bank accounts. MintChip payments can be based on any unique identifier specific to that account, such as an email address, phone number, or unique merchant ID, and all transactions are initiated via standard data formats such as JSON (and XML in the case of ISO 20022) via RESTful APIs. API payloads support the UTF-8-character set, allowing for the potential to localize payload fields and response objects. A web portal can be made available to federal regulators and law enforcement for tracking potential fraud (including the flow of money that enters and leaves the system) and broker funds are carefully monitored to ensure MintChip maintains a good funds model, with each transaction reconcilable with the Broker bank accounts. Note in a digital cash implementation, all funds are good funds and transactions are settled immediately. If funds were sent to an End User with an account at a non-participating Provider, funds would be moved by ACH/EFT.

U.5.5

*Will the UK’s exit from the EU affect this plan? If so, how? How long will the EMI license take to obtain? Does the proposer already have an originator in the U.S. to launch in 2016? Is the central bank included in the launch?*

We do not expect Brexit to impact the EMI license passport function in the short-term. The EMI licensing process is quite onerous and will likely take nanoPay the better part of a year to complete.

In the U.S., we have a few possible Originator alternatives, including our lead American investor. While the central bank does not have to be included in the launch, it could be included as a sponsor if the Federal Reserve was amenable to such a course of action.
Efficiency

E.1.1

*If an End User has multiple SAS accounts, can they use the same alias for all? Are SAS accounts portable from one Provider to another?*

Yes, end users can have a single alias that links to multiple SASs. These can be in the same currency or different currencies. The MintChip Platform can support the transfer of SASs between Brokers and providers if enabled by the customers’ Brokers.

E.3.1

*What is the revenue model for generating revenue from existing customers? If more funding is needed after two years, what will the proposer do to obtain that funding? What are the implementation and ubiquity hurdles that will arise, and what are the plans to overcome them? Which providers will adopt the solution?*

Our revenue model for the retail environment is a small, fixed per-transaction fee charged to the Merchant. Our revenue model for banks and other providers is a combination of an integration fee or license along with volume-based pricing. Our lead investor is a well-known U.S. investment bank and we are planning on raising additional funds in 2017, ahead of deployment in the American market.

In terms of funding required for scale, the Platform can today complete more transactions per second than the UK Faster Payments system in its current implementation. To scale this further will simply require additional HSM hardware. The rest of our Platform is fully scalable both horizontally and vertically, which means there is no requirement for additional funding ahead of scaling.

With respect to Providers, implementation is significantly easier and more cost-effective than other solutions because the Platform does not require changes to their core systems. We will encourage the participation of Banks, Retailers, POS providers, Payment Terminal Providers, Processors, Regulators, and consumers. There are varied issues in dealing with each participant.

There are a number of use cases that present minimal barriers to entry and where the volume and value of transactions are much higher. For example, B2B transactions in vertical markets offer an easy starting point for our Platform.

E.3.1

*What feedback have you gotten from Providers and businesses on adopting MintChip, whether in the U.S. or based on your experience in other countries? What partnerships do you have in place for adoption*
of the MintChip Solution? How dependent is the implementation plan on a mandate from the Federal Reserve?

Feedback:

The initial feedback we’ve received from Providers, consumers and businesses adopting the MintChip Platform in Canada has been very positive. Outlined below are both the positive feedback and areas for improvement we have received.

<table>
<thead>
<tr>
<th>Consumers</th>
<th>Merchants</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Positive:</strong></td>
<td></td>
</tr>
<tr>
<td>Application very easy to download and set-up</td>
<td>Very simple Platform to operate</td>
</tr>
<tr>
<td>Loading funds is very easy</td>
<td>Cash-out process works well</td>
</tr>
<tr>
<td>P2P feature is incredibly fast and simple</td>
<td>Easy to train employees</td>
</tr>
<tr>
<td>Excellent End User experience</td>
<td></td>
</tr>
</tbody>
</table>

| Areas to Improve: | |
| Need more merchants to accept MintChip | Charging separate devices is frustrating (Note: Merchants were supplied a separate device to accept payments. This is no longer required once Ingenico terminal integration is completed) |

**Partnerships:**

**Ingenico:** A global manufacturer of payment terminals. They have developed a software application to enable any Telium II (iWL250 & iWL255 initially, iCT250 soon) which represents 75% of their existing deployed terminals, to accept a MintChip digital cash payment. We will be further partnering with them to assist in discussions with Merchants for deployment in both North America and on a global basis as our business develops.

**Global Payments:** Unique to Canada, processors must certify any application on a Payment Terminal. We have partnered with Global Payment to enable deployment in Canada with their users. In addition, we will be working with them for marketing and promoting the application to their retail partners.
Federal Reserve Implementation Dependency:

The MintChip Platform has broad application across all applicable use cases (P2P, B2P, P2B, B2B) and the technology can be used for a wide variety of specific use cases within each of these broad areas. The only use cases identified that are dependent on the Federal Reserve (as a potential regulator) is the use of digital cash, which after significant market adoption may warrant Federal Reserve involvement in the ecosystem. The EU has long had a Directive that address e-money, allowing for the licensing and regulation of digital cash. In Canada, digital cash is not yet regulated, although we are working (alongside other interest parties) with the Bank of Canada and Department of Finance to develop a regulatory framework.

The majority of use cases will have no dependency on the Federal Reserve. The MintChip Platform is an open Platform that partners will access through open APIs. The Platform will operate behind partners’ existing applications, which are already operational and meet existing Federal Reserve and regulatory or governmental requirements.

E.3.1

What are the implementation and ubiquity hurdles you expect to arise and plans to overcome those hurdles? Which Entities do you expect to adopt the Solution and with what sequence?

What are the implementation and ubiquity hurdles you expect to arise and plans to overcome those hurdles?

It is important to note there are multiple uses cases for the MintChip Platform and the majority of applications do not present implementation or ubiquity hurdles. However, the use case that involves MintChip becoming a replacement for traditional fiat currency (digital cash) does face many ubiquity and implementation hurdles.

Implementation Hurdles:
1. There are multiple parties required for the consumer-to-merchant application (Payment terminal, Bank, Merchants, Processors, Consumers, Regulators). Aligning all of these parties and coordinating the implementation of the payments technology is a hurdle.
2. Gaining a thorough understanding of the MintChip technology and the existing payments ecosystem has taken time and resources.

Ubiquity Hurdles:
1. There is inertia associated with existing payments systems and services.
2. Multiple Banks and Merchants must use the service for it to be attractive to consumers.
3. Consumer understanding of a new payment technology takes time.
4. There is marketplace confusion related to alternative payment methods.
There are multiple strategies and tactics that will be deployed to achieve ubiquity in the marketplace.

1. We will work with regulators and central banks to gain support for the Platform.
2. We have an existing partnership with Ingenico and an MOU with Global Payments.
3. We are developing pricing strategies to establish the Platform as the most cost effective available for completing a transaction.
4. We plan to enable free P2P transactions to drive organic growth of users.
5. Providing an open architecture to enable new and existing partners to easily build out new and different use cases.
6. We are in the process of working to secure relationships with large banks and large retailers to help drive adoption.

We have chosen a strategy that involves working with key players in the ecosystem, rather than working around them. This is a much longer path to driving acceptance of the Platform, however we believe in partnering with these players, who will always have critical roles in the ecosystem, it will ultimately drive increased ubiquity in a shorter period of time.

*Which Entities do we expect to adopt the Solution and with what sequence?*

We are talking to a variety of different entities simultaneously to encourage adoption and acceptance of the Platform. Based on our progress in Canada, the first entities we expect to adopt the Platform are Providers, including Banks and Regulators. The various use cases, ease of implementation and the low cost associated with both integration and on-going transactional costs will drive adoption by banks. The ability of the Platform to meet with any potential regulatory requirements on a global basis will drive acceptance of the Platform by regulators, appreciating the fact they will unlikely openly promote the Platform.

We expect Merchants and Consumers to adopt the Platform as more Providers offer the MintChip Platform. We continue to speak with large retailers because the potential savings for merchants are significant while the implementation costs are minimal. For Merchants, there is little downside to adopting the Platform. As we move forward, our Solution will operate seamlessly alongside existing banking applications, which means that consumer adoption will increase in line with Broker adoption. In some instances, consumers won’t be aware the the MintChip Platform is powering their mobile payment application.

From a demographic perspective, we believe that adoption will roughly mirror the demographic distribution of smartphone owners, particularly those owners who are Millenials. This demographic is open to new technologies and are constantly looking for applications that will make their life easier.
E.6.2

What is nanoPay’s approach to “quickly scaling throughput capacity at very low cost?”

The MintChip Platform architecture has been purpose-built to enable rapid deployments of net new environments and increase the throughput capacity of existing environments in a matter of days. Platform computing resources can be added by spinning up additional VMs and/or deploying additional HSMs to be added to HSM pools. The overhead of the Node.js APIs themselves are minimal. MintChip runs on the highly-scalable PostgreSQL transactional database that supports horizontal scaling, enabling additional resources to be added as needed. Performance metrics for both API code and raw HSM performance are tracked on an ongoing basis to help refine auto-scaling triggers, and budget for new HSMs to support Platform growth. HSMs can reside within multiple data centers to help address issues of network latency, bridged together with site-to-site VPN tunnels. Networking performance and latency is also carefully monitored, including VPN performance and encryption overhead. Hardware is provisioned according to business growth projections and can set to meet loads at peak times or periods of stress.

E.7.2

How do Providers/Brokers request and receive transaction data? Please elaborate on the case management tools made available by the solution.

Providers and brokers can review transaction data through their secure MintChip web-based portal, which requires multi-factor authentication to access. The Portal ensures that information is created, recorded and can be retained indefinitely to facilitate appropriate post-transaction evaluation.

The MintChip Portal acts as an ecosystem dashboard for the Broker and provides overall system administration and case management tools. These tools allow Brokers to view and manage MintChip SASs, assign/revoke user access, review transactions as well as manage operations, define business rules and manage disputes. This Portal will allow Brokers to easily access an End User’s transaction history and associated information so that exceptions can be reviewed and rectified if necessary. Through the Portal, Brokers will be able to communicate with the Platform operator to allow for transaction verification and validation and to resolve exceptions across the Platform.

E.7.3

How are patterns flagged and reported? To whom are they reported? Please describe the system used.

The MintChip system operates in a fully-collateralized model and therefore exceptions to watch for are synchronization errors between MintChip value in the system and the collateralized value in pooled account(s). The system has checks in place to validate the integrity of the MintChip value stores and to automatically notify the Platform administrator of system errors and anomalies to investigate and
exceptions to resolve. The fundamental requirement of the system is the value state of the MintChip system must remain unchanged after a transaction has taken place.

In addition, fraud and money laundering pattern detection is a critical requirement and nanoPay is investigating machine learning and stream computing partners that review exception data to spot patterns beyond the level on an individual end user.

**Risk Management**

**S.1.3**

*Please share more details on the risk management framework’s provisions for operational risk, including lines of defense, vulnerability assessment, risk monitoring, etc.*

MintChip has a dual risk management system; the internal system, which contains settable controls on the value transactions that when breached, will cause an exception to be handled by the system. These controls include the allowed maximum balance, the number of debit and credit transactions as well as the cumulative transaction value. The system allows for these value to be reset subject to security approval.

In addition to the internal system, there is an operator risk management system that monitors the MintChip platforms transactions. Each VTM includes a TAC, which is an encrypted data block that monitors the state of the MintChip SAS that created the VTM. This data block contains the following information,

- Current Balance;
- Currency Code;
- Number of credit transactions;
- Number of debit transactions;
- Highest balance value;
- Highest credit transaction value;
- Highest debit transaction value;
- Cumulative credit transaction value; and
- Cumulative debit transaction value.

The operator risk management team - who have access to the crypto key, are able to decode these messages and can verify the overall integrity of the system by analyzing these parameters. Given the complete transaction history referred to previously, these TACs provide further cross-checking, auditable data.
Our initial process will be to sample all transactions, however as the system matures, a lower number (e.g. 10% of transactions) will be validated. It should be noted in an extreme disaster recovery mode, the SASs could be rebuilt from these transaction logs. This risk management team will also look for behavioural patterns as part of their monitoring process.

The MintChip cryptographic security system is dynamic and allows the operators to transparently move the transaction system from one security domain to another. At any one time the system is managing three security domains. A security domain allows changes in the cryptographic algorithm, mechanism and key sizes. All cryptographic operations take place in a trusted hardware environment.

S.1.5

Besides the threat of exclusion from the system, what other incentives are used to motivate providers and operators to contain and address risk they pose to other participants?

The nature of the MintChip Platform is such that Brokers pose no risk to each other or any ecosystem participants. It is the Originator, who maintains the pooled accounts and provides participants with digital cash who bears the systemic risk as well as the risk of value loss due to any MintChip system security failure. The Originator is therefore financially motivated to minimize such risk. End Users, Brokers, Merchants and other consumers do not bear this risk and are motivated to promote the brand image for sound commercial reasons, to minimize reputational risk and continue to access the MintChip Platform.

S.3.3

*What options/recourse does a Payer have if there is a payment dispute?*

Firstly, we offer a mechanism to request the return of a payment made in error. Assuming both parties are acting in good faith, it will be relatively easy for the payee to return the funds. We can provide an endpoint to allow this only for transactions that were successfully sent to the wrong party or for the wrong amount.

Failing this return request, the Payer may contact their Broker to explain the circumstances and the Broker will have some tools allowing limited investigation. They may have to work with another Broker or the Originator in extreme cases.

Large payments will not be able to be made without an accompanying invoice or metadata. This will confirm the amounts and reasons for the payment. It should also allow the Payer to confirm that funds are being sent to the correct Payee and verify the amount with additional authentication.
S.4.1

What is the method of settlement between institutions for cash-out? Is it guaranteed that there are funds to settle? For example, if the user has $10 in digital currency, does the FI have to have $10 sitting in the bank? Or can the FI use the $10 for something else and risk not having sufficient funds?

In answering this question, we will more thoroughly outline the Platform’s settlement approach than in our original response to S.4.1. This revised response will correct certain omissions and clarify one of the unique features of the MintChip Platform, which is the elimination of between-Broker settlement. It is our intention the explanation below supersedes the response in our original Proposal.

MintChip Platform Summary:

MintChip digital currency is a fully collateralized, bearer asset held in immutable Secure Asset Stores that belong to Brokers and End Users. The collateral is fiat currency deposited in the Originator’s pooled account(s). As a payment in digital currency on the MintChip Platform is a direct value/asset transfer between End Users’ SASs, the transaction is instant and final/irrevocable and includes settlement (digital currency is transferred from the payer’s SAS to the payee’s SAS).

In summary, the MintChip Platform ensures that:

- There is no settlement between Brokers (institutions) - in digital currency or fiat currency.
- There is no counterparty or settlement risk because every dollar of digital currency is fully backed by a dollar of fiat currency in the Originator’s pooled account.

Note that these features are present both for transactions in the same currency and transactions that include currency exchange (FOREX).

A More Detailed Explanation:

For a Broker to acquire digital currency, they must transfer the equivalent amount in fiat currency to the Originator’s pooled account (a bank account or funds held in a segregated account at an asset manager, owned and managed by the Originator). This means every dollar of digital currency in any SAS owned by any Broker or End User is backed by a dollar in fiat currency in the Originator’s pooled account (i.e. a good funds model, which means MintChip digital currency is a fully collateralized bearer instrument).

Because payment in digital currency on the MintChip Platform is a direct value/asset transfer between End Users’ SASs, the transaction is instant and final/irrevocable and settlement (digital currency is transferred from the payer’s SAS to the payee’s SAS). Accordingly, there is no need for inter-Broker settlement because there are no transaction intermediaries.
If a Broker wants to redeem (cash-out) digital currency, they must transfer some amount of digital cash to the Originator, receiving the equivalent amount of fiat currency from the Originator’s pooled account to the Broker’s operating account.

When a Broker sells digital currency to End Users, they deposit fiat currency received from that End User into their Broker operating/suspense account. At redemption, the Broker pays the End Users in fiat currency from that operating account. This is a type of standard treasury management for the Broker and they can manage this activity with their usual liquidity ratios. If at any given time the Broker has high digital currency balance in the Broker SAS and low fiat currency balance in the operating account, the Broker can redeem digital currency for fiat currency from the Originator.

If a Broker faces an unusually high volume of End-User digital currency redemptions, they may have liquidity issues with their operating account. The Broker can manage this by redeeming digital currency for fiat currency from the Originator taking into account fiat currency settlement time between the Originator’s pooled account and the Broker’s operating account. In the worst case, the cash-out for certain End Users may be delayed. This is similar to going to a branch to withdraw a larger amount of cash - the branch may not have the full value in-branch and the customer may have to return the following day to collect their withdrawal.

In summary, it is irrelevant whether the Broker provides cash-out services to its own End User or another Broker’s End User. Digital currency received from the End User represents good funds that Broker can keep to further trade with End Users, or redeem at any time for fiat currency directly with the Originator. There is no settlement of any kind between Brokers (in either digital or fiat currency).

S.5.1

What options does a Payer have if there is a payment dispute?

As a first step, the Platform has a mechanism to request the return of a payment made in error. Assuming both parties are acting in good faith, it is relatively easy for the Payee to return the funds. We can provide an endpoint that will allow this for transactions that were successfully sent to the wrong party or for the wrong amount.

Failing this, the Payer may contact their Broker to explain the circumstances and the broker will have some tools allowing limited investigation. They may have to work with another Broker or the Originator in extreme cases. Note however that a Broker will not be able to compel a Payee to return funds they have received. The attempt to recover amounts sent in error can be made only on a best-efforts basis.

Large payments will not be permitted without an accompanying invoice or similar metadata. This mechanism will allow for confirmation of the payment amount as well as the reasons for making the payment. It will also provide the Payer with the ability to confirm that funds are being sent to the correct Payee and to verify the transaction amount.
A more detailed explanation of our approach to Error Corrections for specific End Users and types of errors can be found in our response to U.3.5 and disputed payments can be found in our response to L.3.1.

S.5.4

As the proposer’s approach to fraud is more focused on prevention than remediation, will businesses and governments require more protections to adopt the solution?

As discussed in our responses to U.3.5, L.3.1 and S.5.1, our approach to error correction, possible fraud and payment disputes has evolved as we have continued to develop the Platform. The ecosystem is appropriately focused on both prevention and remediation and the Brokers and End Users will not require additional protections to adopt the solution.

S.6.1

What information sharing is required from Brokers to the MintChip Platform?

Brokers will be required to notify nanoPay on a timely basis of known and suspected fraudulent accounts and possible AML activity. nanoPay will provide real-time fraud alerts and manage a centralized blacklist and database of blocked accounts and share this information with the broader ecosystem. Reporting will be managed through the MintChip administration Portal, which provides a secure, encrypted reporting process and simplifies flagging this suspicious activity and problematic accounts.

S.6.7

Please describe the Solution’s fraud monitoring capabilities.

Further to our response to S.1.3, MintChip SASs provide a detailed transaction history that is fully auditable and can be monitored for behavioural patterns to help identify fraud. In addition, each VTM includes an encrypted Transaction Authentication Code (TAC) that checks the authenticity of MintChip payments and provides a reference point to validate transactions. This architecture provides the foundation of our fraud monitoring capabilities and enables fraud models to be developed, implemented, refined and updated as required.

In addition, MintChip employs run-rate monitors, tracks usage and sets a variety of different thresholds. We also build and maintain blacklists to identify End Users who have engaged in fraudulent or suspicious activity. This blacklist is exposed through the MintChip API and is shared securely across Brokers and Providers.
S.7.3

*How will the proposer ensure that providers follow security protocols when registering an End User?*

The MintChip Platform employs mechanisms for multi-factor authentication and identity verification that is meant to supplement existing KYC obligations to provide appropriate due diligence for Brokers to know their customers.

Moreover, the Solution uses Brokers who have existing relationships with End Users. Banks and other financial institutions have AML, KYC and data privacy requirements that they must comply with. Using the Platform to complete payments will not absolve Participants of these regulatory requirements.

While anyone can receive MintChip value, to use the funds or move them to a DDA, the End User will have to be appropriately authenticated by their Provider. If this authentication is not possible, the Platform will require identification before allowing the End User to transact.

S.8.1

*What past examples or models of resiliency at the scale required for MintChip to work are there to give confidence to the ability to ensure high availability and security against cyber-attacks?*

The MintChip Platform does not have a single point of failure and is designed to achieve high availability. The security of the system has been assessed by independent security analysts, who did not identify any significant or systemic issues. Annual penetration tests are performed to identify and assess potential system vulnerabilities.

Visanet is a good example of a High Integrity, High Availability system with a throughput capability of 56,000 transactions per second. The security of the Platform is at least comparable to that of EMV payments but has the added advantage of a single endpoint. MintChip VTMs pass from one SAS to another. All cryptographic operations are executed within HSMs operating in secure data centres. These HSMs are state independent and can be added or replaced as required from bonded stock. The root cryptographic security operations are never online but are carried out in a secure data centre with no network or unauthorized user physical access.

With the MintChip Platform, single points of failure are eliminated by hosting our services in distributed datacenters with redundant hardware and software components. The MintChip application firewall and API gateway ensure appropriate rate limiting and DoS attack mitigation, and every request to our APIs and databases is traceable to a user, and in turn their device, IP address, and personally identifiable information (phone, email, etc.). All data is encrypted, including data that is stored and collected in databases, and important information such as personally identifiable information resides in an immutable database allowing us to track revisions to this data over time.
Extensive performance testing has been conducted on our API clusters to assess what would be required to overwhelm each worker process, and the testing concluded that, while concentrated attacks could cause temporary slowdowns, fine-tuned auto-scaling triggers assure complete availability of all APIs. Further, large self-replicating database clusters assure the same with database data. The encryption ciphers we use are non-proprietary and these ciphers are upgraded over time to stay ahead of current theories on how to break/bypass this encryption.

S.8.2

*What percent of capacity will be covered in the event of a disaster? Please comment on how long it would take for the back-up plan to take over.*

MintChip servers are hosted in multiple geographically distributed datacenters with redundant network connectivity. In the event of a disaster, we expect 100% of our capacity will be recovered. Our planned Recovery Time Objective (RTO) is <= 4 hours.

S.8.3

*Are there mechanisms in place to prevent an adverse solution event from causing other participants to fail?*

MintChip is a fully-collateralized system and all operations are atomic; as such there is no counterparty risk or risk of contagion. If a participant were to fail, all obligations would be met as outgoing payments would have already been funded. Therefore, the failure will have no impact on the remaining participants from a risk perspective.

S.8.4

*What resources are devoted to business continuity and resiliency? Please share details on the resources (human and financial) allocated to business continuity and disaster recovery.*

We are in the process of creating a business continuity plan in the form of a manual that will be updated as our organization grows and changes. Core elements of the manual include People, Technical and Recovery.

From an internal staffing perspective, our operations team are primarily focused on uptime and performance. All components of our platform are tested thoroughly before being deployed. We run multiple platforms including development, staging, demo, sandbox and production. Should any release fail in spite of prior testing, the platform can be rolled back to the previous working version. Our developers also provide peer source code review before delivery to Quality Assurance (QA), which is done by a separate team. As well, most of our stack is based on open systems, so we are not supplier or partner dependent.
Our operations team monitors all platforms and ensures uptime standards are met. Our objective is five nines (99.999%) platform availability, although many components have been designed to function even when offline.

**S.8.5**

*Please share the frequency and nature of contingency tests. Would a partner be immediately available if another partner needed to be replaced?*

MintChip technology risk management guidelines require annual contingency tests of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in accordance with industry best practices to minimize disruptions to the system arising from a serious incident. The BCP and DRP are tested by simulating plausible disaster scenarios and major system outages caused by system faults, hardware malfunction, operating errors or security incidents. The results of contingency tests are recorded and used to improve the processes. All employees, select partners and vendors are included to assess the effectiveness of the plans.

*Would a partner be immediately available if another partner needed to be replaced?*

nanoPay has identified and selected partners that would be available in the event that a chosen partner would need to be replaced.

**S.9.1**

*What data protection requirements are made of providers?*

The MintChip system will mandate that providers be responsible for providing data protection controls as governed by applicable Federal and/or State laws. These requirements will ensure all participants have robust controls and mechanisms in place to protect sensitive information. Compliance with those requirements will be monitored via annual self-assessment of the Participants.

**S.10.6**

*Please share plans for the evolution of authentication methods, including the resources (financial and human) dedicated to it.*

The MintChip Platform currently employs two-factor authentication to verify End-User identity. This authentication includes email, password and the delivery of a PIN to verify a User’s mobile phone number. In Q4 2016, the Platform will add biometric authentication to its suite of possible authentication measures. This enhanced authentication will allow the Platform to better control payment authorization and access to the MintChip system as the threat landscape evolves. As a technology provider, we are committed to using cutting-edge authentication methods and have planned partnerships with a variety of third parties that specialize in End User authentication. A large portion of
our technology budget is earmarked for these authentication partnerships. Because of the small size of our organization, we have chosen to partner with other providers rather than dedicate full-time human resources to create our own authentication protocols.

S.11.1

How would pooled accounts established by non-traditional providers through brokers create SASs for end-users?

MintChip allows Brokers to set-up non-traditional providers as “indirect” Brokers. This set up includes the following:

- Establishing an indirect Broker SAS (via API);
- Registering an indirect Broker as a sponsored Broker on the MintChip Platform, which allows indirect Broker access to the Platform API, where it can establish End User SASs logically associated with the indirect Broker (via API).
- Establishing an operating bank account for the indirect Broker that will be used for that Broker to trade digital currency with the “direct” Broker and End Users (pooled account).

S.11.3

What are the current or planned processes to monitor and ensure providers’ compliance with participation requirements?

The MintChip Platform operator will ensure any Provider meets participation requirements before enabling access to the MintChip ecosystem (see proposal, section E.1.4, last sentence). To ensure continued compliance with the participation requirements, Providers will have to complete a self-assessment questionnaire for annual review by the MintChip Platform operator. As part of the compliance review, the MintChip Platform operator may request additional information and on-site audit to ensure that the compliance criteria are met.

Fast

F.4.1

What is the solution’s approach to settlement? What methods are used, and how is risk managed?

The Platform’s approach to settlement is explained in detail in our answer to question S.4.1 above, where we detail a unique feature of the MintChip Platform that eliminates the settlement between Brokers (Depository Institutions and Regulated Non-Bank Account Providers). MintChip digital currency is a fully collateralized bearer asset held in immutable Secure Asset Stores belonging to Brokers and End Users. The collateral held is fiat currency, which is deposited in the
Originator’s pooled account. Because payment in digital currency on the MintChip Platform is a direct value/asset transfer between End Users’ SASs, the transaction is instant and final/irrevocable with settlement included (digital currency is transferred from the payer’s SAS to the payee’s SAS). As such:

- There is no settlement between Brokers (institutions) - in digital currency or fiat currency.
- There is no counterparty or settlement risk since every cent of digital currency is fully backed by a cent of fiat currency in the Originator’s pooled account.

This concept applies to both transactions in the same currency and transactions that include currency exchange (FOREX).

**F.4.2**

*What happens if cash-in (withdrawal) is with a U.S. provider and cash-out (deposit) is with a provider in another country?*

As discussed in our responses to questions S.4.1. and F.4.1. above, payment in digital currency on the MintChip Platform is a direct value/asset transfer between End Users’ SASs. The transaction is instant and final/irrevocable with settlement included (digital currency is transferred from the payer’s SAS to the payee’s SAS). There is no settlement between Brokers/Providers as the good funds model applies for cross border transactions in the same currency and transactions in different currencies. All Brokers (those that transact only in one currency, and those that provide FOREX services) transact exclusively with the Originators for digital currencies they support. Payments that include FOREX are performed in near real-time as they include one additional value transfer between the End User and the FOREX Broker.

The cross-border FOREX scenario can be better explained by looking at a specific example:

- A USD Broker has USD digital currency in a USD Broker SAS obtained from a USD Originator. This currency is obtained by the USD Broker transferring USD fiat currency to the USD Originator’s pooled account.
- A CAD Broker has CAD digital currency in a CAD Broker SAS obtained from CAD Originator. This currency is obtained by the CAD Broker transferring CAD fiat currency to the CAD Originator’s pooled account.
- A FOREX Broker has multiple SASs in different digital currencies (e.g. USD, CAD, EUR...) and maintains the various floats by trading with the Originators of those currencies.
  - The USD digital currency held in the FOREX Broker USD SAS was obtained from the USD Originator by the FOREX Broker transferring USD fiat currency to the USD Originator’s pooled account.
  - Similarly, the CAD digital currency held in the FOREX Broker CAD SAS was obtained from the CAD Originator by the FOREX Broker transferring CAD fiat currency to the CAD Originator’s pooled account.
- Note: *Fiat currency transfers between the Brokers and the Originators are done using existing payment and settlement mechanisms.*
● US-based End User A performs USD 100 cash-in with USD Broker. As a result, End User A has USD100 worth of digital currency in his USD SAS, which is covered by USD100 in fiat currency sitting in the USD Originator’s pooled account (as per the Platform's good funds model).

● End User A sends USD10 to Canadian End User B who has CAD SAS managed through CAD Broker.

● End User B is notified that he has a pending transaction for USD10 worth of digital currency and is prompted to convert it to CAD digital currency to deposit it into the CAD SAS.
  ○ The FOREX Broker provides the exchange rate (e.g. 1.3), offering to convert USD10 digital currency to CAD13 digital currency.
  ○ End User B approves the rate/transaction.
  ○ USD10 digital cash is transferred to the FOREX Broker’s USD SAS.
  ○ CAD13 digital cash is transferred from the FOREX Broker’s CAD SAS to End User B’s CAD SAS.

● End User B then initiates a CAD13 cash-out with CAD Broker.
  ○ CAD13 worth of digital cash is transferred from End User B’s SAS to CAD Broker SAS.
  ○ The CAD Broker then transfers CAD13 worth of fiat currency to End User B using the supported payment mechanism (e.g. deposit to End User B’s DDA if End User B has a DDA with Broker B, or EFT/ACH if at another bank).

Legal

L.2.3
What is the proposer’s approach for processes L.2.3 and L.2.4?

Because the MintChip Platform is capable of being deployed for a wide variety of uses, it is difficult to articulate a precise set of Payment System Rules and how they would be enforced and monitored. Depending on the Originator and the scale of the Solution, monitoring could range from simple annual self-assessments to the implementation of a full set of legally binding regulations. Self-assessments could be implemented in combination with spot-audits by the Originator or an independent assessment body (which could be a regulator). Participants would be notified of potential rule changes and would be encouraged to submit feedback regarding changes and updates.

A full regulatory solution could be implemented in countries where the central bank acts as an Originator. In such an instance, the regulatory scheme would likely resemble that of the EU’s E-Money Directive, which is a detailed, prescriptive set of rules governing the actions of all participants in a digital cash system.
**L.3.1**

*Please describe the process for resolving disputes.*

As described in our responses to U.3.5, L.3.1 and S.5.1 above, the Platform has a mechanism to request the return of a payment made in error. Assuming that the both parties are acting in good faith, it is relatively easy for the Payee to return the funds. We can provide an endpoint that will allow this for transactions that were successfully sent to the wrong party or for the wrong amount.

Failing this, the Payer may contact their Broker to explain the circumstances and the broker will have some tools allowing limited investigation. They may have to work with another Broker or the Originator in extreme cases. Note however that a Broker will not be able to compel a Payee to return funds they have received. The attempt to recover amounts sent in error can be made only on a best-efforts basis.

Large payments will not be permitted without an accompanying invoice or similar metadata. This mechanism will allow for confirmation of the payment amount as well as the reasons for making the payment. It will also provide the Payer with the ability to confirm that funds are being sent to the correct Payee and to verify the transaction amount.

Disputes involving an End User and Broker that progress beyond the mitigants described above would be resolved using the existing dispute-resolution mechanisms in place for financial institutions today. For example, the relevant provisions of Regulation E would protect End User consumers. In Canada, End User consumers are protected by a variety of financial consumer protection guidelines and Codes; they would continue to be protected when transacting on the MintChip Platform.

Disputes involving corporate End Users and Brokers would be subject to the same rules and regulations that protect these Users today; the use of the MintChip Platform will not lessen the obligations Brokers have to their customers today.

Disputes that are not related to payment errors and that occur between two End Users that cannot be resolved using the mitigants described above must be resolved outside of the MintChip Platform. Implementing some type of chargeback process simply isn’t possible for a Platform that supports collateralized, direct bearer asset transfers; the emphasis is on speed and finality and not on resolving disputes between End Users.

**L.3.2**

*What are the payment system rules and procedures for error resolution related to consumer claims?*

Please see our responses to section U.5.3 and L.3.1 for a fulsome discussion of our proposed error-correction procedures.
L.3

Will consumers adopt this solution given its limited consumer protections?

We believe that consumers will be adequately protected when using the MintChip Platform. As described in our answer to question L.3.1 above, Canadian consumers are protected by a variety of Codes of Conduct and other financial consumer protection guidelines when accessing their DDA. These measures also extend to the MintChip Platform when End Users are enrolled with FI Brokers (virtually all customer End Users). As a result, Canadian customers are very well protected when transacting electronically. We anticipate the same situation in the United States. Consumers should be adequately protected when accessing their DDAs for payment; the Platform that they use to access it should not impact their protections.

While it is true the Solution does not have chargeback processes, we believe the speed, low cost, cross-border capabilities and other value-added services will help drive consumers to adopt the Platform in instances where their FI does not offer the Integrated Account Model to its customers.

L.4.4

How do end-users obtain visibility into the data collected on them?

The Terms and Conditions End Users agree to will clearly articulate the data that the Platform collects before agreeing to use the Platform. Because of the online nature of the Solution, End Users will be able to easily make changes to and verify their personal information, including the degree to which that data is shared within the ecosystem. They will also have real-time access to transaction and payment history through the mobile application.

In Canada, FIs must have a clearly articulated Privacy Code that enumerates the types of personal information that are collected and the ways in which the information is used. The Terms and Conditions of the MintChip Platform incorporate the terms of these Privacy Codes in Canada. In other jurisdictions, similar controls will be adopted to comply with local privacy protection regulations.

L.5

Has MintChip patented any components of its solution for which it may be necessary to do so?

Yes, nanoPay has patented certain components of the Solution in the United States and continues to pursue patents on additional, novel payment solutions. A full list of our worldwide patents is attached as Appendix B.
L.5

Are there any potential intellectual property issues that could hinder this solution’s success?

No, there are currently no intellectual property issues that would hinder the solution’s success. The technology is well-protected by a variety of different patents.

Governance

G.1

Please provide more details regarding effective governance, including decision and rule-making processes that are transparent and support both the Solution’s objectives and Public Policy Objectives. In doing so, please specifically address how the Solution supports the four effective governance sub-criteria.

Please note that this response is intended to address the questions with respect to both G.1 and G.2.

Our original submission did not go into great detail with respect to effective governance. As mentioned in the introduction to this document, our thinking has continued to evolve since drafting our first response to the Task Force. While we continue to support a coordinated effort to the adoption of digital cash by central banks, we recognize the MintChip Platform can be used to address a variety of use cases. It is helpful to consider these use cases along a sort of spectrum that represents their breadth, ranging on one end from a systemically-important, pseudo utility-type payment system, to a narrow direct-asset-transfer solution that is deployed for a very specific use case like the one described in Appendix A.

This spectrum also impacts the range of governance models nanoPay could employ depending on the particular deployment. For instance, a systemically important Platform that processes a high volume of high-value transactions or involves an origination-point at a central bank would require the development of a fulsome governance structure set up to take into account the interests of a wide variety of users, minimize conflicts of interest and establish an independent board of directors.

More specifically, as a systemically important Platform, it would be difficult (or impossible) for nanoPay to remain solely in control of the solution. The Federal Reserve and other regulators would have to be involved in the development of the appropriate governance model, which could involve establishing: an association to oversee the Solution; committees and user and stakeholder groups to provide feedback and input to the Solution; appropriate Board structure (e.g independent or quasi-independent); and appropriate guiding policy objectives. A purely profit-driven corporate structure would be difficult to support. Shareholder expectations would be difficult to balance against user needs and input.

However, at the opposite end of the spectrum, a narrow, contained solution does not require as many checks and balances in place to enforce what is essentially simply a contractual arrangement. For these
use cases there is no market failure of information asymmetry that needs to be governed. Competitive, market pressures and general good governance should be the relevant driving forces for these types of corporate solutions.

Of course most implementations of the Solution will fall somewhere in between the extreme ends of the spectrum. In these instances, the governance structure would reflect the solution’s place on the spectrum. Participant feedback would be actively solicited and considered, an independent auditor could oversee portions of the Platform. Payment rules would be made public and any proposed changes would be subject to a consultation period. Most importantly, it will be crucial to strike a balance between participation, consultation and the need for a payments provider to be nimble and quick to evolve to keep pace with the rapidly evolving payments landscape.

G.2

Please provide more details regarding inclusive governance, including input and representation from diverse stakeholders, and support for the public interest. In doing so, please specifically address how the Solution supports the five inclusive governance sub-criteria.

Please see our response to Question G.1.
Appendix A: Clarification re: Original Proposal

**U.2 Usability**

In the preliminary assessment the Rationale section under section U.2 Usability indicates “The solution is usable as long as access to a wireless mobile device or internet connection is available (U.2.1)”

It is important to clarify that one of the unique features of the Platform is the capability to be used in an off-line environment. The Platform can complete transactions using the secure element of a mobile device, or any other device with a secure element. There are specific parameters that can be established for off-line transactions like the number of transactions completed and/or dollar volume of transactions. The transactions are recorded and stored within the SAS on the device’s secure element. Once the device is back online, the transactions are completed and the parameters are reset.

**E.2 Capability to enable value-added services**

The Rationale under this proposal suggests “The proposal would be strengthened by illustrating 2-3 examples of potential value-added services.”

**Additional Use Case Examples:**
The following use cases are examples where the MintChip Platform is capable of providing a solution to an existing payment pain point for the partner.

**B2B: Use Cases:**
In these use cases, the MintChip Platform is used to complete the transaction while integrating with an existing payment system. Once the solution is enabled by one party, this service capability is available to others with similar systems.

1. **Banks**: Branch-to-Branch transfers for both Domestic and International locations.

2. **CETFIA**: (Canadian Electronically Traded Funds Association) Looking to ensure settlement is reduced from 3-5 business days down to real time.

**B2P: Use Cases:**
In these use cases, the MintChip Platform is accessed via APIs from the partner’s existing application. The partner then builds the described value-added service into their existing offering.

1. **Retailer**: Electronic Gift Card/Stored-Value Card. Allows customers to use an electronic stored card that is more cost-effective than existing gift card networks.
2. **Financial Services**: Vendor looking to provide real-time consumer loans at Point of Purchase and immediately deliver digital funds, cost effectively, and in real time.

3. **Grocery Store**: Enablement of real-time coupon settlement to Grocery store at time of consumer coupon redemption.

**P2B Use Cases:**
The MintChip Platform could easily be used to support these value added services.

1. **Utility Services**: Utilize Platform to complete real-time digital cash transaction to minimize need for utility service disruption due to late payment.

2. **Sole Proprietor Solution**: Enable small and sole proprietor businesses to accept digital cash payments in retail or online environments from consumers simply by downloading merchant application and registering an account.

**P2P Use Cases:**
nanoPay will not build these value-added applications itself, but the platform is easily able to support them.

1. **Multiparty Bill Sharing**: Platform has the ability to not only split a bill among a group but to also, auto request payment at certain intervals, and track received and outstanding funds.

2. **Sports Betting Pools**: User groups can be established for activities such as sports pools and Platform can be used for real-time cash distribution and collection.
Preliminary Assessment: Additional Points

The following section specifically address points raised in the Preliminary Assessment, while these issues are addressed in the answers above we felt it valuable to specifically call them out in this section and specifically reference where in the document we have answered these questions.

Executive Summary of the Proposal

Areas for Improvement and enhancements:

U.1 Accessibility:
“The solution hinges on the willingness of the Federal Reserve to be the Originator (and create new monetary policy). Adoption has challenges unless the central bank issues a mandate to accept MintChip digital currency as legal tender since depository institutions would give up revenue associated with current payment systems and other new security and technical infrastructure would need to be built.”

We address the motivation for Providers to participate in the MintChip Platform in our response to U.1.5, above.

U.2 Usability:
“Although the solution builds on existing systems, it is not interoperable and does not leverage existing systems to reach users who are not yet enrolled in the payment system—though unbanked customers could potentially purchase MintChip in exchange for cash at a broker merchant”

As discussed throughout this revised submission and in our Revised Executive Summary, the MintChip Solution can be implemented in a way that is seamlessly integrated with Providers’ existing payment systems. New End Users are therefore easy to enroll in the case of the Integrated Account Model. With respect to the Standalone Account Model, Providers can simply add another account for End User to transact across the MintChip Platform.

The proposer’s overall ability to deliver proposed solution:

“The Solutions is partially deployed in Canada, with three of the top five Canadian banks currently leveraging MintChip. It is working on integration with European and Brazilian banks as well, so there is high confidence in ability to deliver the technical solution.”

The platform has been deployed in a geographically controlled area of Toronto. There are currently 15 merchants accepting MintChip as a form of payment. Users are able to download the application. nanoPay is currently operating as the Broker to enable users to load funds from various sources into digital cash within the applications. Merchants and or Users can then cash out digital cash into the bank account of any Canadian Bank.
In addition, nanoPay is in discussions with all five of Canada’s major banks, with three banks each being at various stages of Proof of Concepts. The platform is fully operational and capable of delivering the proposed solution today, in any country.
## Appendix B

**MINTCHIP PATENT PORTFOLIO**

The following is a list of the MintChip Patents as of **December 18, 2015**.

<table>
<thead>
<tr>
<th>Family Member ID</th>
<th>DIPS Ref. No.</th>
<th>Cntry</th>
<th>Application No.</th>
<th>Registration No.</th>
<th>Title</th>
<th>Status</th>
<th>Next Action</th>
<th>Due Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>T22613-0002-WO-CN</td>
<td>200943/00030</td>
<td>CN</td>
<td>201080041424.2</td>
<td></td>
<td>ASSET STORAGE AND TRANSFER SYSTEM FOR ELECTRONIC PURSES</td>
<td>Pending</td>
<td>Status Check</td>
<td>30-Dec-15</td>
<td>Waiting for Allowance or Further Action - Response to Office Action filed June 30, 2015</td>
</tr>
<tr>
<td>T22613-0002-WO-IN</td>
<td>200943/00031</td>
<td>IN</td>
<td>1771/CHENP/2012</td>
<td></td>
<td>ASSET STORAGE AND TRANSFER SYSTEM FOR ELECTRONIC PURSES</td>
<td>Pending</td>
<td>Status Check</td>
<td>26-Feb-16</td>
<td>Waiting for First Office Action - Examination Requested - Aug 22,</td>
</tr>
<tr>
<td>Application Numbers</td>
<td>Priority Numbers</td>
<td>Application Date</td>
<td>Title</td>
<td>Status</td>
<td>Action Date</td>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>-------</td>
<td>--------</td>
<td>-------------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0002US</td>
<td>200943/00005</td>
<td></td>
<td>Asset Storage and Transfer System for Electronic Purses</td>
<td>Never Filed</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0002US-PRV</td>
<td>200943/00004</td>
<td>61/243,203</td>
<td>Asset Storage and Transfer System for Electronic Purses</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0002WO</td>
<td>200943/00006</td>
<td>PCT/CA2010/000435</td>
<td>Asset Storage and Transfer System for Electronic Purses</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0003-WO</td>
<td>200943/00008</td>
<td>PCT/CA2010/001434</td>
<td>Trusted Message Transfer Protocol and System</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Number</td>
<td>Country</td>
<td>Application Number</td>
<td>Country</td>
<td>Application Number</td>
<td>Country</td>
<td>Application Number</td>
<td>Country</td>
<td>Application Number</td>
<td>Country</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>-------------------</td>
<td>---------</td>
<td>-------------------</td>
<td>---------</td>
<td>-------------------</td>
<td>---------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>T22613-0003-WO-CA</td>
<td>CA</td>
<td>200943/00022</td>
<td>CA</td>
<td>200943/00022</td>
<td>CA</td>
<td>200943/00022</td>
<td>CA</td>
<td>200943/00022</td>
<td>CA</td>
</tr>
<tr>
<td>37</td>
<td></td>
<td>2,771,816</td>
<td></td>
<td>TRUSTED MESSAGE TRANSFER PROTOCOL AND SYSTEM</td>
<td></td>
<td>Pending</td>
<td></td>
<td>Maintenance Fees</td>
<td>17-Sep-16</td>
</tr>
<tr>
<td>T22613-0003-WO-CN</td>
<td>CN</td>
<td>200943/00023</td>
<td>CN</td>
<td>200943/00023</td>
<td>CN</td>
<td>200943/00023</td>
<td>CN</td>
<td>200943/00023</td>
<td>CN</td>
</tr>
<tr>
<td>10816517.6</td>
<td></td>
<td>TRUSTED MESSAGE TRANSFER PROTOCOL AND SYSTEM</td>
<td></td>
<td>Pending</td>
<td></td>
<td>Maintenance Fees</td>
<td>17-Sep-16</td>
<td>Waiting for Allowance or further Office Action Response to Office Action filed March 26, 2015</td>
<td></td>
</tr>
<tr>
<td>T22613-0003-WO-IN</td>
<td>IN</td>
<td>200943/00028</td>
<td>IN</td>
<td>200943/00028</td>
<td>IN</td>
<td>200943/00028</td>
<td>IN</td>
<td>200943/00028</td>
<td>IN</td>
</tr>
<tr>
<td>2012-529075</td>
<td></td>
<td>TRUSTED MESSAGE TRANSFER PROTOCOL AND SYSTEM</td>
<td></td>
<td>Issued</td>
<td></td>
<td>Maintenance Fees</td>
<td>05-Dec-17</td>
<td>Good Standing</td>
<td></td>
</tr>
<tr>
<td>10-2012-7006914</td>
<td></td>
<td>TRUSTED MESSAGE TRANSFER PROTOCOL AND SYSTEM</td>
<td></td>
<td>Pending</td>
<td></td>
<td>Status Check</td>
<td>07-Sep-16</td>
<td>Waiting for First Office Action - Examination Requested - September 7, 2015</td>
<td></td>
</tr>
<tr>
<td>T22613-0004-CA</td>
<td>CA</td>
<td>200943/00009</td>
<td>CA</td>
<td>200943/00009</td>
<td>CA</td>
<td>200943/00009</td>
<td>CA</td>
<td>200943/00009</td>
<td>CA</td>
</tr>
<tr>
<td>2,714,784</td>
<td></td>
<td>MESSAGE STORAGE AND TRANSFER SYSTEM</td>
<td></td>
<td>Pending</td>
<td></td>
<td>Maintenance Fees</td>
<td>17-Sep-16</td>
<td>Waiting for First Office Action - Examination Requested March 19, 2015</td>
<td></td>
</tr>
</tbody>
</table>

37
<table>
<thead>
<tr>
<th>Application Code</th>
<th>Application Number</th>
<th>Nationality</th>
<th>Application Number</th>
<th>Status</th>
<th>Date</th>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>T22613-0004-WO</td>
<td>200943/00013</td>
<td>WO</td>
<td>PCT/CA2011/050138</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>T22613-0004-WO-AU</td>
<td>200943/00045</td>
<td>AU</td>
<td>2011235531</td>
<td>Pending</td>
<td>Order of Acceptance</td>
<td>05-Aug-16</td>
<td>First Office Action Reported October 6, 2015 Response should be filed ASAP</td>
</tr>
<tr>
<td>T22613-0004-WO-CN</td>
<td>200943/00041</td>
<td>CN</td>
<td>201180026994.9</td>
<td>Pending</td>
<td>Status Check</td>
<td>21-Mar-16</td>
<td>Waiting for Allowance or further Office Action Response to Office Action filed March 17 2015</td>
</tr>
<tr>
<td>T22613-0004-WO-HK</td>
<td>200943/00068</td>
<td>HK</td>
<td>13111266.9</td>
<td>Pending</td>
<td>Status Check</td>
<td>30-Mar-16</td>
<td>Waiting for CN Grant</td>
</tr>
<tr>
<td>T22613-0004-WO-IN</td>
<td>200943/00042</td>
<td>IN</td>
<td>2713/KOLNP/2012</td>
<td>Pending</td>
<td>Status Check</td>
<td>13-Feb-16</td>
<td>Waiting for First Office Action - Examination Requested Sept 13, 2013</td>
</tr>
<tr>
<td>Application ID</td>
<td>Filing Date</td>
<td>Country</td>
<td>Application Number</td>
<td>Title</td>
<td>Status</td>
<td>Pending Date</td>
<td>Request Date</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>---------</td>
<td>---------------------</td>
<td>-------</td>
<td>--------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>T22613-0004-WO-US</td>
<td>200943/00046</td>
<td>US</td>
<td>13/637,328</td>
<td>MESSAGE STORAGE AND TRANSFER SYSTEM</td>
<td>Issued</td>
<td>Maintenance Fees</td>
<td>11-May-18</td>
</tr>
<tr>
<td>T22613-0005-US-PRV</td>
<td>200943/00010</td>
<td>US</td>
<td>61/437,147</td>
<td>CONTROLLED DOMAINS SECURITY</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>T22613-0005-WO</td>
<td>200943/00020</td>
<td>WO</td>
<td>PCT/CA2012/050043</td>
<td>CONTROLLED DOMAINS SECURITY</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>T22613-0005-WO-AU</td>
<td>200943/00061</td>
<td>AU</td>
<td>2012210978</td>
<td>CONTROLLED DOMAINS SECURITY</td>
<td>Pending</td>
<td>Opposition Period</td>
<td>26-Feb-16</td>
</tr>
<tr>
<td>T22613-0005-WO-EP-HK</td>
<td>200943/00073</td>
<td>HK</td>
<td>14105155.4</td>
<td>CONTROLLED DOMAINS SECURITY</td>
<td>Pending</td>
<td>Status Check</td>
<td>08-Mar-16</td>
</tr>
<tr>
<td>Application Number</td>
<td>Office Action Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0006-US-PRV</td>
<td>Maintenance Fees 25-Feb-19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0006-WO</td>
<td>Waiting for First Office Action - Examination Requested - Feb 26, 2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0006-WO-AU</td>
<td>Maintenance Fees 27-Jan-16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0006-WO-CN</td>
<td>Maintenance Fees 27-Jan-16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T22613-0006-WO-CN</td>
<td>Maintenance Fees 28-Jan-16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ELECTRONIC TRANSACTION RISK MANAGEMENT**

- **JP**: Pending Status Check 23-Mar-16
- **US**: Issued Maintenance Fees 25-Feb-19
- **PRV**: Expired N/A N/A N/A
- **WO**: Expired N/A N/A N/A
- **AU**: Pending Maintenance Fees 27-Jan-16
- **CA**: Pending Maintenance Fees 27-Jan-16
- **CN**: Pending Status Check 28-Jan-16

**CONTROLLED SECURITY DOMAINS**

- **JP**: Pending Office Action 20-Jan-16
- **KR**: Waiting for Allowance or Further Office Action - Response for Office Action sent September 23, 2015

**Maintenance Fees**

- **US**: 25-Feb-19
- **PRV**: N/A
- **WO**: N/A
<table>
<thead>
<tr>
<th>Application Number</th>
<th>Related Application Numbers</th>
<th>发明名称</th>
<th>Status</th>
<th>Fee Due Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>T22613-0007-PCT</td>
<td>200943/00049</td>
<td>USING BAR-CODES IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>T22613-0007-US</td>
<td>200943/00048</td>
<td>USING BAR-CODES IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Issued</td>
<td>Maintenance Fees</td>
<td>24-Aug-18</td>
</tr>
<tr>
<td>T22613-0007-US-PROV</td>
<td>200943/00037</td>
<td>USING BAR-CODES IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Expired</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Application Number</td>
<td>Priority Number</td>
<td>Country Code</td>
<td>Application Number</td>
<td>Patent Title</td>
<td>Status</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>--------------</td>
<td>--------------------</td>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>T22613-0007-WO-CN</td>
<td>200943/00076</td>
<td>CN</td>
<td>201380015249.3</td>
<td>USING BAR-CODES IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending</td>
</tr>
<tr>
<td>T22613-0007-WO-EP-HK</td>
<td>200943/00095</td>
<td>HK</td>
<td>15101074.0</td>
<td>USING BAR-CODES IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending</td>
</tr>
<tr>
<td>T22613-0008-US</td>
<td>200943/00050</td>
<td>US</td>
<td>13/845,911</td>
<td>AUTOMATED FOREX FUNCTION IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending</td>
</tr>
<tr>
<td>T22613-0008-US-PROV</td>
<td>200943/00038</td>
<td>US</td>
<td>61/612,779</td>
<td>AUTOMATED FOREX FUNCTION IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Expired</td>
</tr>
<tr>
<td>Publication Code</td>
<td>Application Date</td>
<td>Country Code</td>
<td>Application No.</td>
<td>Title</td>
<td>Status</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>--------------</td>
<td>-----------------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>T22613-0008-WO</td>
<td>200943/00051</td>
<td>WO</td>
<td>PCT/CA2013/050223</td>
<td>AUTOMATED FOREX FUNCTION IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Expired</td>
</tr>
<tr>
<td>T22613-0008-WO-CN</td>
<td>200943/00083</td>
<td>CN</td>
<td>201380015252.5</td>
<td>AUTOMATED FOREX FUNCTION IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending</td>
</tr>
<tr>
<td>T22613-0008-WO-EP-HK</td>
<td>200943/00096</td>
<td>HK</td>
<td>15101072.2</td>
<td>AUTOMATED FOREX FUNCTION IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending</td>
</tr>
<tr>
<td>Application No.</td>
<td>Priority No.</td>
<td>Filing Date</td>
<td>Title</td>
<td>Status</td>
<td>Check Date</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>T22613-0009-US</td>
<td>200943/00052</td>
<td>US 13/846,032</td>
<td>EXTERNAL LOG STORAGE IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending Status Check</td>
<td>18-Feb-16</td>
</tr>
<tr>
<td>T22613-0009-US-PROV</td>
<td>200943/00039</td>
<td>US 61/612,783</td>
<td>EXTERNAL LOG STORAGE IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Expired N/A N/A N/A</td>
<td>-</td>
</tr>
<tr>
<td>T22613-0009-WO</td>
<td>200943/00053</td>
<td>WO PCT/CA2013/050224</td>
<td>EXTERNAL LOG STORAGE IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Expired N/A N/A N/A</td>
<td>-</td>
</tr>
<tr>
<td>T22613-0009-WO-CN</td>
<td>200943/00090</td>
<td>CN 201380015258.2</td>
<td>EXTERNAL LOG STORAGE IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending Status Check</td>
<td>12-May-16</td>
</tr>
<tr>
<td>T22613-0009-WO-EP-HK</td>
<td>200943/00097</td>
<td>HK 15101069.7</td>
<td>EXTERNAL LOG STORAGE IN AN ASSET STORAGE AND TRANSFER SYSTEM</td>
<td>Pending Status Check</td>
<td>03-Aug-16</td>
</tr>
<tr>
<td>Application Number</td>
<td>Filing Date</td>
<td>Country</td>
<td>Application Number</td>
<td>Publication Date</td>
<td>Status</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>---------</td>
<td>--------------------</td>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>T22613-0010-WO</td>
<td>200943/00071</td>
<td>WO</td>
<td>PCT/CA2014/050527</td>
<td>Pending</td>
<td>National Filings</td>
</tr>
<tr>
<td>T22613-0011-WO</td>
<td>200943/00072</td>
<td>WO</td>
<td>PCT/CA2014/050528</td>
<td>Pending</td>
<td>National Filings</td>
</tr>
</tbody>
</table>
Faster Payments QIAT

DRAFT ASSESSMENT

Property of the Federal Reserve Bank of Kansas City and the Federal Reserve Bank of Chicago (“Banks”)

Not for distribution or publication without the express written permission of the Banks
Faster Payments QIAT

DRAFT ASSESSMENT

Proposer: nanoPay Corporation

Description of Solution: nanoPay’s MintChip is digital cash that has been broadened into a direct, collateralized bearer-asset-transfer system. Essentially, it securely stores and transfers any form of digital asset between users on a single, verifiable platform—i.e., a closed-loop system. Originally created by the Royal Canadian Mint (RCM), MintChip is already in limited operation in Canada.

MintChip digital currency will be transferred using Secure Asset Stores or SASs (electronic wallets). The SASs will be loaded using existing payment instruments. Since all transactions operate under a good-funds model, there should be no clearing, settlement, or liquidity risk.

The MintChip solution includes the following participants:

- The Originator manages (1) operation of the stand-alone MintChip system component that creates MintChip value and Secure Asset Stores (SAS), (2) administration of the security parameters in the MintChip system, and (3) a pooled account that holds fiat currency for MintChip value sold to brokers.

  Note: the proposal originally suggests that the Federal Reserve should be the Originator (though as part of initial implementation, the Platform Operator may act as the Originator). In the addendum to the original proposal, the proposer notes that the Solution does not require the government to play the role of Originator. In use cases where the Originator is not the government, the pooled funds will be protected by being held at an Asset Manager and funds will only be invested in instruments where the Principle is guaranteed.

- The Technology Provider owns the MintChip platform that provides: (1) the system components for deployment by the Platform Operator and the Originator; (2) integration support for Brokers and Merchants; and (3) software enhancements, maintenance, and support.

- The Platform Operator is responsible for deploying and operating the MintChip platform and for administering operating rules, standards, and protocols.

- The Broker is a depository institution or regulated non-bank account provider that: (1) buys and sells MintChip value from/to Originator, (2) enrolls end-users, (3) provides mechanisms for end-users to buy and sell MintChip value, and (4) provides currency conversion services (optional).

While MintChip has many use cases, the QIAT has conducted the assessment based on the use case where it is a platform for Providers to transfer digital assets (in this case cash) between end users SAS, not the use case of a digital fiat currency.

EXECUTIVE SUMMARY OF THE PROPOSAL

Major strengths of the solution:

- The solution requires only a payee’s MintChip identifier and a mobile device or internet connection for use, making it ubiquitous throughout providers.

- The solution allows end-users to switch freely among brokers and puts no limitations on smaller players. It is also open-source to all services that comply with its operating standards.
It is hosted by AWS (Amazon Web Services) and Peer1, which assures complete redundancy and access to all aspects of the end-to-end payment process.

- The proposal provides concrete figures to support the argument that the solution is quickly scalable at low cost.
- The solution provides real-time funds availability and immediate settlement. The solution operates at no settlement risk since it relies on prepaid funds. It supports the capability to shut down the payment system in the event of fraud risk and uses shared blacklist data to limit risk.
- The broadened definition of MintChip offers the opportunity to open the system to use cases beyond the traditional payments use cases.

**Areas for improvement and enhancement:**
- The solution does not hinge on the Federal Reserve’s willingness to serve as the Originator (and to create new monetary policy), but the Fed’s serving in this role is desirable as a means to drive adoption in the solution’s early days. Without MintChip as a digital fiat currency, adoption may have challenges, since depository institutions will have to forfeit the revenue associated with current payment systems and build new security and technical infrastructure.
- Solution is highly dependent on confidence in the Asset Manager that protects the pooled funds to collateralize the digital cash. Risk and regulatory considerations are needed to ensure the safety and security of the funds held at the Asset Manager, as well as provider incentive to give up funds to be held at the Asset Manager.
- The solution is not clear on how payments reach any and all payees, specifically how payments reach those that currently do not have an SAS. Two aspects of the solution do enable quick enrollment, however: 1) unbanked customers could potentially purchase MintChip in exchange for cash at a broker merchant; 2) payees can choose to open a MintChip account via a Secure Asset Store (SAS).
- The proposal leaves dispute scenarios ambiguous. In the event of fraud, the solution does not provide businesses with 100% protection, as it focuses on prevention rather than remediation.
- The solution’s settlement approach within the system is clear; however, more information is needed on the “cash out” process, particularly what happens if an end user has more MintChip to exchange for fiat currency than the provider holds, and the process for the provider to exchange MintChip for funds at the Asset Manager.
- The proposal does not adequately explain the solution’s governance plan and approach.

**Use cases addressed:**
- The solution addresses all four major use cases (P2P, P2B, B2P, and B2B). It can be built into the POS transaction flow directly into the POS terminal.

**The proposer’s overall ability to deliver proposed solution**
- nanoPay launched MintChip in Canada in April 2016, and MintChip 2.0 is expected to be deployed in summer 2016. The solution is partially deployed in Canada, with 15 merchants accepting MintChip as a form of payment in a geographically controlled area of Toronto. Additionally, the proposer is in discussions with all five of Canada’s major banks, three of which are in various stages of Proof-of-Concept efforts. nanoPay is working on integrating with European and Brazilian banks as well. With these steps already underway, the proposer seems well positioned to deliver the technical solution.
Ubiquity

U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution requires only the payee’s MintChip identifier—an email address, mobile phone number, name, or even a Facebook username—to send and receive payments (U.1.2). MintChip thus does not require multiple operators or networks and is ubiquitous. The broker (see Description of Solution, above) can be a depository institution or a regulated non-bank entity (U.1.1), effectively opening the solution to both banked and unbanked customers of the payments system (U.1.4). Additionally, any account or means of payment (including cash) can fund the SAS through a broker (U.1.1), as long as the broker accepts that form of payment. End-users can set up multiple SASs within their MintChip account to accept/send payments in different currencies; if a payer or payee does not have a SAS for a given currency, they are directed to a FOREX broker to convert funds and complete the transaction (U.1.3). MintChip supports any currency as long as the source of funds works with that currency.

Since MintChip does not require multiple operators or networks, no interoperability is required for transactions that occur on the platform (U.1.6). The system does not depend on the operator apart from issuing the currency.

The proposer plans to “work with providers, end-users and software developers to achieve widespread adoption” (page 108), but the incentives for providers to participate are not clear (U.1.5). In particular, confidence in the Asset Manager where pooled funds are held and secured is critical to Provider adoption and the proposal indicates that it is still working with the lead investor to identify the best way to ensure confidence in the system.

U.2 Usability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution is usable as long as access to a wireless mobile device or internet connection is available (U.2.1). Only the MintChip identifier is needed to initiate payments (U.2.2), and the solution can be accessed to do so 24x7x365 (U.2.3). Retail and online transactions are automatically accepted, and the funds received are good funds immediately (U.2.3). In a P2P (person-to-person) payment, the sent funds are marked as pending until the receiving end-user accepts them.

As long as the end-user is comfortable with using a mobile device for payments, the system should be easy to use (U.2.4). Guidelines included in the platform rules help to ensure consistency in user interfaces.

U.3 Predictability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:
The solution uses RESTful APIs to deliver core components—registration, security, cash-in, cash-out, transaction logs and transactions—consistently across channels, devices, and providers (U.3.1, U.3.-4). It leverages digital disclosure to meet disclosure requirements (U.3.2).

The MintChip system uses the same standard communication and messaging protocols across the entire platform, no matter which provider is facilitating access to that platform (U.3.3). The solution’s transaction messaging is compliant with ISO20022, the international standard format for payment messaging.

The solution includes confirmation capabilities to allow an end-user to correct errors prior to sending a payment; however, errors will still occur. The solution allows the payer to initiate an automated resolution process, which lets him/her request full or partial repayment by sending a request for payment to the payee. If the issue is not resolved, a formal dispute can be initiated through a broker. Resolution processes are also in place for system-generated errors.

U.4 Contextual data capability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution is based on ISO20022, which makes it a conduit for expanded remittance data (e.g., line-item SKU data, trade settlement and agreement data, and trade delivery data) (U.4.1) and allows all transaction data to be exported into a format receivable by account and personal finance systems, as well as large ERP systems (U.4.2). Though the message format is standardized using ISO 20022, any information or links can be associated with the transaction and stored in the flexible transaction log (page 113) (U.4.3). Further, the system has the capability to handle batch payments (e.g., payroll files) as well as the ability to distribute a single payment to multiple recipients.

The Proposal can be strengthened by clarifying exactly how remittance data is linked to the transaction.

U.5 Cross-border functionality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution is currently rolled out in Canada, and the proposer is working to integrate it with European, Brazilian, and Canadian banks. The proposer plans to work with EFT, ACH, and SWIFT providers to ensure that funds can be received into non-participating bank accounts globally (U.5.2). The Royal Canadian Mint mints coins for 72 countries, providing a logical avenue for MintChip roll-out and broader foreign deployment.

However, the solution has not yet rolled out in the United States (but is expected to in 2016). Cross-border functionality is intuitively possible in MintChip, but it has yet to be launched and executed. One concern is that the use of the MintChip app is currently restricted to Canada and the Canadian Dollar. A subsidiary company exists in the UK that will launch there after acquiring an EMI license, which can be expanded into the broader Eurozone (U.5.5).
As mentioned, the solution’s platform does allow users to open a SAS in any currency and to receive funds in any currency (U.5.4). Advance fee disclosures are considered in the solution’s terms and conditions (U.5.3).

**U.6 Applicability to multiple use cases**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution supports all use cases, although only two (P2P and P2B, person-to-business) have been introduced into the Canadian market.

**Efficiency**

**E.1 Enables competition**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution allows users to freely choose brokers (E.1.1). It does not limit an entity’s ability to move among providers (E.1.2) or set up any barriers to small players (although these players might be limited by an inability to pre-load funds) (E.1.4). The MintChip platform’s operating rules require providers to disclose in advance to end-users all of the information needed to understand the total cost of using their services (E.1.3). The solution allows end users to have a single alias that links to multiple SASs.

**E.2 Capability to enable value-added services**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution is open-source for all services and providers that comply with operating standards (E.2.1-2). The MintChip platform’s operating rules require providers to clearly disclose to their customers that the value-added services they have added to baseline MintChip services are optional (E.2.3). The open payment and broker APIs enable the creation of value-added services. One aspect to consider, though, is MintChip’s purported irrevocability of payment. This irrevocability could be perceived as an obstacle to the basic value-added service of dispute/chargeback handling.

The proposal would be strengthened by illustrating two to three examples of potential value-added services.

**E.3 Implementation timeline**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
**Rationale:**

The solution has already been partially launched in tightly controlled geographical areas of Toronto and will receive revenue from initial customers, such as banks, retailers, and telecom companies. The revenue model currently is geared toward the retail environment and is based on a small, fixed, per-transaction fee charged to the merchant. The revenue model for banks combines an integration/license fee with volume-based pricing. The idea of exploring least-resistance uses cases (e.g., B2B transactions in specific industry verticals) could prove a logical launching point.

The proposal clearly articulates implementation-specific hurdles, but ubiquity hurdles exists (E.3.1) as well (e.g., inertia associated with existing payment systems and services, the need for multiple bank and merchants to accept the solution, etc.).

The Proposal can be strengthened by providing an air-tight business case for merchants to adopt it, as well as a clear articulation of why banks will choose to leverage the solution (E.3.1).

**E.4 Payment format standards**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution is ISO 20022-compliant (E.4.3-4) and flexible enough to allow any off-ramp to require certain fields (E.4.1). The system is unique in that it allows certain fields to be completed after the funds have been received in MintChip. To enable ongoing development, the platform allows for further modification or additions (E.4.4). All external APIs will be published and are designed to be consistent with open standards (E.4.5).

The mobile applications will all be open-source so that anyone can build on them, improve them, or even write their own applications. The solution’s ISO 20022-compliant format should make cross-border interoperability easier (E.4.2).

**E.5 Comprehensive**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution is a good-funds model that enables all aspects of the end-to-end payment process (E.5.1). Because MintChip is a digital currency, clearing, settlement, and reconciliation are not required (E.5.2).

**E.6 Scalability and adaptability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

One of MintChip’s greatest differentiators is its ability to scale up its throughput capacity quickly at a very low cost (E.6.2). The solution has the potential to scale to Visa’s capacity in just a few weeks with an investment of just $1M USD. Today’s MintChip platform can process thousands of transactions per second; the current capacity of the Visa system globally is
approximately 50,000 transactions per second. MintChip’s technical design supports projected use cases (E.6.1) and is readily adaptable to ongoing developments (E.6.3).

While the technical design contains auto-scaling triggers rooted in performance metrics for both API code and raw HSM (hardware security module) performance, the proposal can be enhanced by providing estimates of projected demand, peak-hour spikes, latent capacity in the network, etc. (E.6.2)

E.7 Exceptions and investigations process

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution stores and tracks all transaction information (E.7.2) and provides alerts, shared logs, and tools for regulators/investigators to handle exceptions (E.7.1).

MintChip’s web portal allows providers and brokers to query stored data. It has sufficient multi-factor authentication to be able to control access effectively. The solution can be enhanced by building the capability to proactively push this kind of information to those who need it. The web portal tool also provides the ability to manage SASs, assign/revoke user access, review transactions, define business rules, and manage disputes.

A synchronization error between the MintChip value in the system and the collateralized value in pooled accounts is the primary type of error that should be monitored for. The Proposer is also exploring the possibility of incorporating machine-learning capability and stream-computing partners into the exceptions process.

The proposal can be strengthened by building capability into the web portal that proactively pushes exceptions data to the provider and by clearly articulating and describing the tools available to support the exceptions and investigations process (E.7.1).

Safety and Security

S.1 Risk management

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Because the solution operates on a good-funds model, settlement risk is essentially non-existent, because transactions are settled immediately and can only be executed with available good funds (S.1.2). The consequences of human error (e.g., inputting an incorrect transaction value) are the responsibility of the parties involved (S.1.3). The solution leverages existing incentives for brokers to comply with AML (anti-money laundering regulations) and KYC (know-your-customer regulations). Reviews of risks and compliance with the payment system are conducted quarterly (S.1.6).

The solution has a dual risk management system: (1) an internal system that contains configurable controls such as maximum balance allowed, maximum debit and credit transactions, etc. and (2) an operator risk system that monitors the MintChip platform’s
transactions. Additionally, 10% of transactions will be sampled at any given time to confirm that the system in working well.

The proposal can be strengthened by providing detail about specific operational risks other than human error (S.1.3) and by describing the remediation process for erroneous, fraudulent, or unauthorized transactions (S.1.4). It can be further enhanced by clearly articulating the “incentives” for brokers and providers to comply with risk requirements (S.1.5).

S.2 Payer authorization

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Payers authorize each MintChip transaction via their smartphones, typically using the Touch ID for iOS devices or the fingerprint scanner for Android devices (S.2.1). The solution allows payers to pre-authorize payments (S.2.2), and payers can revoke pre-authorization or change pre-authorization parameters easily and quickly (S.2.3). The same authentication process is applied to pre-authorized transactions, adding another layer of security to the payment process.

S.3 Payment finality

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Transparency, speed, low-cost efficiency, and finality of payment are the driving factors of this solution, and so it focuses on ensuring that erroneous payments are not made in the first place. MintChip relies on prepaid funds, and the SAS is debited immediately when a payment is initiated (S.3.1).

The system is intended to be a digital equivalent to cash, not an extension of existing card networks. A mechanism is in place to request the return of an erroneous payment. If the return request is denied, the payer may contact his/her broker, who will have tools to conduct limited investigations. As a control mechanism, large payments will not be sent without accompanying invoice or metadata that confirms the amounts and the reasons for the payment.

S.4 Settlement approach

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Because the solution backs all value with traditional cash, settlement between depository institutions only needs to take place when cash-out (deposit) and cash-in (withdrawal) occur at different institutions (page 131) (S.4.1). This also means that there is no inter-provider risk, as MintChip is always loaded with fiat currency good funds (S.4.2).

Because the end-user holds a MintChip account and deposit account with the same broker, and because traditional cash backs all MintChip value, a cash-out is simply a ledger entry for the broker (i.e., an “on-us” transaction for the broker). MintChip will settle between end-user accounts during the day, with frequency determined by changes in balances between institutions as compared to normal trends (S.4.1).
In rare instances, the broker may have a liquidity issue with its operating account if the volume of currency redemptions is abnormally high. This scenario is basically no different from visiting a bank branch with an unusually large withdrawal that exceeds the branch’s cash on hand; in such a situation, the customer simply has to return to the branch the next day to collect the full value.

More information on how the credit and liquidity risk of the Asset Manager that protects the pooled funds is needed, particularly how the funds are segregated, invested, monitored.

S.5 Handling disputed payments

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

If a user believes that his/her smart phone has been compromised, s/he can shut down the SAS through the provider (S.5.1). If fraudulent transactions have occurred, the perpetrators can be immediately shut out of the system. Generally, though, for disputed payments the solution relies on the existing consumer protection laws that both banks and regulated non-bank account providers already follow and does not offer any of its own protection policies or processes (S.5.2, S.5.5).

A framework is in place that allows end-users to request their funds back (S.5.3), but for an online transaction this request will require the end-user to disclose his/her identity to the payee. A payment can be returned in real time as long as the payee agrees to it (or is forced by law).

One unique aspect of the solution is that a customer can click a button within the app to contact and appeal directly to the merchant about a disputed payment (S.5.5).

While the solution defines the roles, responsibilities, and liabilities for losses to businesses and governments, the solution’s focus is on loss prevention rather than remediation. The proposal can be strengthened by establishing and articulating clear SLAs for disputed payments (S.5.1).

S.6 Fraud information sharing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution uses blacklist data on fraudulent credit cards and bank accounts (S.6.2) to share internal transaction profiles with partners, and transaction history is stored and accessible to resolve payment disputes (S.6.6). End-users’ PII (personally identifiable information) is excluded from information-sharing (S.6.1). The solution provides real-time fraud alerts by requiring brokers to notify nanoPay “on a timely basis” of known and suspected fraudulent accounts (S.6.3).

As a measure of consumer protection, consumers can click on a button within the app to contact merchants directly about disputed payments (S.6.5). Providers can assist consumer end-users with this process and see the details of any payment (page 134).

The proposal should consider implementing a policy of providing differential access based on the various parties’ roles and responsibilities (S.6.5). The solution can be improved by taking a more active role in the information-sharing process while offering other value-added services such as data aggregation and analysis (S.6.2). A potential fraud service could be a centralized, opt-in sharing service, with appropriate value-add on the back end.
S.7  Security controls

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
In the current, Canadian implementation, the solution uses Amazon Web Services’ (AWS) co-located data center hybrid system for security controls. The HSMs [hardware security modules—“the same hardware used in today’s global payments systems” (page 9)] and Canadian personal information are housed in the data center. The transaction logs, all production MintChip APIs, and production databases reside in multiple regions (7.1-2).

The proposal can be enhanced by detailing how the solution will ensure that providers follow the security protocols when registering an end-user (e.g., through administration of operating rules and minimum security standards) (S.7.2). While the proposal introduces the possibility of integration with POS terminals, it would be beneficial to explain this integration will be achieved.

In addition, the proposal needs to provide more information on how the Asset Manager where pooled funds are held and secured will have strong technical, operational and managerial security controls (S.7.1-S.7.3).

S.8  Resiliency

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution’s architecture (pages 137-138) for redundancy—if operating as it should—ensures that the solution will never be unavailable for “more than a minute” (page 138). The proposal can be enhanced by providing specific target metrics (S.8.1). In case of disaster, the solution has solid contingency plans and will provide access to the platform and all data in another region (see S.7), albeit in a reduced capacity (S.8.2).

The system is designed to prevent systemic risk (S.8.3), since the MintChip platform “has no real dependencies on other market players, with the exception of on- and off-ramps for loading and offloading traditional currency housed by banks” (page 138). The ramps are “managed by industry-accepted protocols, legally vetted frameworks such as PCI-compliance in the case of credit card transactions, and [the fact that no proprietary techniques or communication occurs]…outside of rigid, controlled channels,” according to the proposal (page 138).

Independent security analysts have assessed the system’s security. Annual penetration tests identify system vulnerabilities. The solution avoids having any single point of failure by maintaining hosted environments in distributed data centers with redundant hardware and software.

S.9  End-user data protection

Very Effective  Effective  Somewhat Effective  Not Effective
Rationale:

MintChip relies on existing consumer protection regulations, which are sufficient for this solution. Provider and operator requirements are not articulated, but it is assumed that existing provider requirements on data protection are adequate to meet S.9.1. Data is encrypted, and access to it is restricted (S.9.2-3). End-users do not share PII with one another at any time during the payment process (S.9.2-3). It is the assessors’ interpretation that MintChip works through a central directory that holds broker names and aliases—the extent of the sensitive information it holds—and that brokers hold the remaining information.

S.10 End-user/provider authentication

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:

End-users are authenticated at enrollment and then again when changing any of their credentials, including their phone number or device. They are authenticated when opening the app and then again when processing a transaction. The solution uses social media, phone numbers, email addresses, and device identifiers to authenticate consumers and their devices for a limited set of services with low payment thresholds. To have access to the full set of services, a consumer must go through a bank’s KYC process. Additional KYC and AML processes are required if the end-user wishes to send large sums domestically or abroad (S.10.1). Merchants have access to a broader set of services.

The solution has robust mechanisms to ensure that payments reach their intended payees (S.10.2). It aligns with regulatory guidance and industry standards for end-user authentication (S.10.3), and it has strong end-user authentication controls with risk-weighting (pp. 38, 53, 135) (S.10.4-5). The proposal states that cryptography and “key components of the security architecture” can be updated as needed (page 141) but does not share plans for adopting new authentication methods as the threat landscape evolves (S.10.6).

S.11 Participation requirements

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:

The solution contemplates traditional FIs as brokers, but alternative providers can offer MintChip services indirectly by establishing pooled accounts with their brokers, although they must have enough capital to prepay all of the MintChips. Alternative providers could set up their own MintChip USD account and then register individual end-users and allow them to exchange USD for MintChip USD (S.10.1). Because there is no clearing and settlement of the payment per se, there is no disadvantage to dealing with an “indirect” broker.

The proposal can be strengthened by describing whether participation requirements ensure that FIs and non-banks have the operational, financial, and legal capacity to fulfill their obligations (S.11.2) and by detailing its processes for monitoring and ensuring providers’ compliance with participation requirements (S.11.3).
**Speed (Fast)**

**F.1 Fast approval**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Immediate approval comes through the use of a good-funds model. Only pre-funded transactions may be executed. Once the payment is authorized, the value is exchanged between parties and accounts.

**F.2 Fast clearing**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Clearing occurs when the VTM (value transfer message) is delivered to the payee to accept. The VTM immediately makes the payment information available to the payee’s provider so that they may notify the payee. Clearing is nearly instant and aligns with the VTM.

**F.3 Fast availability of good funds to payee**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Once the payer creates the VTM, the value is immediately and irrevocably available to the payee and only the payee.

**F.4 Fast settlement among depository institutions and regulated non-bank account providers**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Payment in digital currency (i.e., MintChip) in the solution is a direct value/asset transfer between end-user SASs; therefore, the transaction is instant and irrevocable, with settlement included. The MintChip-to-fiat currency conversion process is clearly explained, addressing even the rare instance when a MintChip redemption amount may exceed a broker’s pooled account value.

Regarding payments across time zones (F.4.2), the proposal says, “The location of [the] payment recipient’s account is irrelevant, and the 24x7x365 nature of the platform means that there is no issue sending payments inter-time zone” (page 144).
F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The transaction is communicated in multiple ways to end-users. The user interface provides an immediate confirmation notice to the payer (F.5.1). The payee receives a push notification, email, and in-app notification that funds are available for receipt (F.5.2).

---

**Legal**

**L.1 Legal framework**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposal maintains that a legal framework for the solution is unnecessary, stating, “Because of the simplicity of the MintChip ecosystem, a complex legal framework is not necessary to adequately protect participants. Because clearing, settlement and reconciliation are all instantaneous, rules regarding responsibilities and liabilities throughout those stages of a transaction are no longer necessary. Existing legislation that governs participants’ KYC and AML requirements will continue to apply, particularly during the participant-registration process. Within the ecosystem itself, payment rules are required, rather than a freestanding, newly-developed legal framework” (page 147).

The solution manages regulatory capital by investing the float in short-term treasury bills, which means that no funds are at risk, and there is always a real dollar for every dollar of digital cash. In the absence of regulations in Canada, the proposer has been following the European derivatives for electronic money and payment services directives. These derivatives include protecting the payment system from the bankruptcy of the asset manager holding the float (or pool). Additional “regulatory capital” may be required, but in the near term, the proposer will invest the float in short-term treasury bills, making the digital cash backed de facto by the same government that backs the fiat currency (page 147) (L.1.1).

**L.2 Payment system rules**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution requires detailed payment rules to govern the relationship between the broker and operator and to support its regulatory regime, but these rules have yet to be developed (L.2.1). The proposer envisions monitoring of system rules potentially occurring along a spectrum of approaches (e.g., annual self-assessments, self-assessments with spot audits, full set of legally binding regulations, etc.) (L.2.3).

The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
L.3  Consumer protections

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The dispute-handling process, as discussed in previous sections, involves a request for the return of an erroneous payment. Absent a clear resolution, the payer may escalate to involve the broker. The solution will rely on existing consumer protection laws and regulations, as it does in its Canadian solution.

The proposal can be improved by detailing the protection laws and regulations that the proposer will rely on to provide adequate consumer protections and by clearly articulating how end users and providers can establish additional, option consumer protections for payments that may exceed existing protections (L.3.3)

L.4  Data privacy

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The nature and type of end-user data required for security, compliance, and authentication are clearly articulated in descriptions of the transaction process (L.4.3). A Terms and Conditions agreement for end-users clearly articulates the data that the solution collects (L.4.4).

The proposal can be strengthened by laying out an approach to dealing with privacy violations (L.4.1-2).

L.5  Intellectual property

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution is already in use in Canada, but this does not prevent IP protection claims from arising in other places. The proposer is clearly taking steps to ensure the security of intellectual property, as evidenced by the full back-up of patents provided (more than 85 patents). Each party owns its own IP, and existing IP regulations should be sufficient.

Governance

G.1  Effective governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposal does not present a clear path, plan, or details for the solution’s governance model. Given the spectrum of use cases to which MintChip applies, the proposer suggests governance potentially occurs along a spectrum of governance models that best serve the needs of the solution. For example, a systemically important solution would require a complete governance
structure, but a narrow, contained solution does not require as many checks and balances in place.

The Proposal can be strengthened by articulating a tangible plan for governance—with details on what the governance model will include—to serve as a path forward until a model can be constructed and implemented (G.1.1-4).

### G.2 Inclusive governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The proposal does not present a clear path, plan, or details for the solution’s governance model. Given the spectrum of use cases to which MintChip applies, the proposer suggests governance potentially occurs it is logical to mirror an effective governance model along a spectrum of governance models that best serve the needs of the solution. The Proposal can be strengthened by articulating a tangible plan for governance—with details on what the governance model will include—to serve as a path forward until a model can be constructed and implemented. The proposer should take steps to ensure a clear vision of inclusion is built into the governance model to allow for: (1) the inclusion of public interest (G.2.1), (2) influence and input by a wide range of stakeholders (G.2.2 and G.2.4), (3) inclusion of governing bodies that fairly represent stakeholders' risks and interests (G.2.3), and (4) a clear approach to address conflicts, both real and perceived (G.2.5).
### APPENDIX A: ASSESSMENT SUMMARY

<table>
<thead>
<tr>
<th>Assessment</th>
<th>UBIQUITY</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
<td></td>
</tr>
<tr>
<td>U.1: Accessibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2: Usability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.3: Predictability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.4: Contextual data capability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.5: Cross-border functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.6: Multiple use case applicability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment</th>
<th>EFFICIENCY</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
<td></td>
</tr>
<tr>
<td>E.1: Enables competition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2: Capability to add value-added services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.3: Implementation timeline</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.4: Payment format standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.5: Comprehensive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.6: Scalability and adaptability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.7: Exceptions and investigations process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment</th>
<th>SAFETY AND SECURITY</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
<td></td>
</tr>
<tr>
<td>S.1: Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment</th>
<th>SAFETY AND SECURITY (cont’d)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
<td></td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>S.10: End-user/provider authentication</strong></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>S.11: Participation requirements</strong></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SPEED (FAST)

| **F.1: Fast approval** | ✓ |
| **F.2: Fast clearing** | ✓ |
| **F.3: Fast availability of good funds to payee** | ✓ |
| **F.4: Fast settlement** | ✓ |
| **F.5: Prompt visibility of payment status** | ✓ |

### LEGAL

| **L.1: Legal framework** | ✓ |
| **L.2: Payment system rules** | ✓ |
| **L.3: Consumer protections** | ✓ |
| **L.4: Data privacy** | ✓ |
| **L.5: Intellectual property** | ✓ |

### GOVERNANCE

| **G.1: Effective governance** | ✓ |
| **G.2: Inclusive governance** | ✓ |
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

QIAT Draft Assessment Response

As we have progressed through the Task Force review process, it has become apparent to us that there are certain areas the QIAT has identified as apparent weaknesses in the MintChip Solution. Admittedly, when we submitted our initial response to the Task Force, the MintChip Platform showed vast, but undeveloped and relatively unexplored potential. As the product has matured, so has our thinking on the two areas identified as perceived weaknesses: Asset Management and Governance.

We take the opportunity in this Appendix B to further develop our thinking on the protection of the pooled fund (Asset Management) and to present a tangible and robust governance framework for nanoPay to adopt moving forward.

We have also highlighted some sections of the Draft Assessment Executive Summary that we believe are misstatements or inaccurate descriptions of our Solution. Those sections follow immediately below.

A. Executive Summary: Areas for Improvement and Enhancement

(i) Second Bullet:

“Solution is highly dependent on confidence in the Asset Manager that protects the pooled funds to collateralize the digital cash. Risk and regulatory considerations are needed to ensure the safety and security of the funds held at the Asset Manager, as well as provider incentive to give up funds to be held at the Asset Manager.”

nanoPay Comments:

There should be no negative impact on a provider for transferring the funds to the Asset Manager. A MintChip digital cash balance should be recognized as fiat funds on the provider’s balance sheet (i.e. characterized simply as overnight deposits*) because the digital balance is collateralized with fiat currency in the pooled account held at the Asset Manager. Accordingly, transfers to and from digital cash should be part of the normal treasury management and have no impact on the provider’s capital ratios/requirements. Funds transfers between banks/providers and the Asset Manager could be done by Fedwire or CHIPS as needed to manage the digital and fiat currency balances.


“Electronic money (e-money) is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-
money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions.

The amount outstanding of e-money issued by euro area MFIs is included in the item “overnight deposits” on the MFI balance sheet.”

(iii) Third Bullet:

“The question is around how all Entities choosing to use the Solution can be sure payments can reach any and all Payees - if an end user does not have a SAS (and so does not use MintChip), but an existing MintChip user wants to send money to that end user, how can they do it? Is there any notification that reaches that end user to enroll? We can clarify the wording to better reflect the intent.”

As originally outlined in our original proposal (Part A, Section 1, Solution Description), the MintChip ecosystem uses a universal identifier to link a Person, Business or Government to a Secure Asset Store (SAS). A MintChip account is currently set up to be an email address, mobile phone number and name, however the platform has been designed so it could also be a Facebook username or another common universal identifier.

To initiate a transaction, a Payer must know the Payee’s MintChip identifier. The MintChip Platform will use this information to determine the SAS ID to send a payment. In the event that a Payee does not have a SAS in the MintChip ecosystem, the Platform notifies the Payer that the recipient does not have a MintChip account and is prompted to enter a payment notification destination (e.g. mobile phone number). A SAS is then generated by the system and can be claimed by the Payee. The Payee will receive a Value Transfer Message (VTM) with the payment and instructions with respect to claiming the funds, which involves creating a MintChip account. The Payee can then choose to move the funds to their bank account via ACH payment. In the event that a Payee chooses not to receive the funds, the Payer will be refunded the payment after 30 days or immediately, if the Payee declines the payment.

(iii) Fifth Bullet:

QIAT advised via e-mail that the bullet will outline the need for clarification as follows:

“The settlement within the system is clear. Two things are unclear: 1) "cash out" settlement - for example, a user of the system accumulates a large amount of MintChip and wants to cash out. However, the amount is more than what their bank holds. Does the customer just come back tomorrow for the rest (like what would happen at a branch today)? And how does their bank get the cash from the Asset Manager? and 2) more information on the risk management of the Asset Manager holding the pooled funds”

In the above case, the process is as follows:

- The End User requests a cash out;
- MintChip digital cash is transferred from the End User’s SAS to the Broker (Bank’s) SAS;
The Broker transfers digital cash to the Originator;
- The Originator transfers fiat currency to the bank using Fedwire (real-time payment); and
- The Broker/Bank credits the End User's deposit account for the redeemed value of digital currency (book transfer, effective immediately)

The cash out settlement process is a single seamless transaction for the user. The above is all completed in real-time as transfers made over Fedwire are irrevocable and immediately effective, because the Federal Reserve Bank (FRB) guarantees the payment to the receiving bank as soon as the transfer message is sent.

B. Two Specific Clarifications

As mentioned above, it is apparent that the remaining concerns with the nanoPay Solution tend to focus around two or three recurring themes. One of the most important themes focuses on questions relating to the existence of an Asset Manager, which is crucial to the implementation of MintChip as a digital cash solution. Because concerns surrounding an Asset Manager arise across multiple Effectiveness Criteria, we have chosen to add additional detail in one place, consolidating our comments for easier reference.

(i) The Asset Manager: A Familiar Concept

The QIAT raises concerns with the Asset Manager-concept throughout the Draft Assessment either directly (U.1, S.4, S.7) or indirectly through questions concerning organizational governance.

The concerns with an Asset Manager focus on the security of the pooled funds, credit and liquidity risk of the Asset Manager (particularly with respect to segregation, investment and monitoring of the pooled funds) and the technical, operational and managerial security controls around the pooled fund.

In considering the appropriate treatment and protection of a potentially large pooled fund of fiat currency, we have propose drawing on the regulatory framework established by the European Union’s E-Money Directive (2009/110/EC), which has been in place since 2011. The Directive sets out a detailed regulatory framework for handling pooled accounts. A similar framework would be suitable for the MintChip Solution.

Before being permitted to carry on a full-scale business, to protect the pooled account, the Federal Reserve (or other relevant regulator) should satisfy themselves that an organization establishing a pooled account and using an Asset Manager (an Originator in the MintChip Platform) would be required to: have sufficient initial capital (to be established by the Regulator); be an American-incorporated entity with a head office located in the United States or a corporate entity with a head office outside the United States and a significant branch presence located in the US; have robust and clearly-articulated governance arrangements around MintChip value issuance, including clear organization structure with well-defined lines of responsibility; have sound internal control mechanisms; ensuring the
directors and people responsible for the management of the MintChip value and other services are of good repute and possess appropriate knowledge and skills to issue such digital cash and provide associated payment services; and perhaps most importantly, demonstrate the establishment of appropriate procedures and policies for safeguarding the pooled account.

In addition to the above criteria, the Originator would also be required to submit a business plan that set out how the organization intends to carry out its business, including details regarding marketing strategy, resources, records maintenance, risk assessment mechanisms and details regarding the procedures, policies, processes, systems and controls that it will put in place to manage the day-to-day running of the business.

The Protection of the Pool

Ensuring the robustness of the organization managing the pooled account is the first step to ensuring the account is protected. However, beyond that assessment, some guidelines would have to be established by the Regulator to ensure consumers are adequately protected and the pool is safe at all times.

As above, the E-Money Directive and accompanying Regulations are instructive. The Regulations require all funds received in exchange for digital cash (e-money) are appropriately safeguarded. If an Originator was to become insolvent, the Regulations require that claims of e-money holders or other users are paid from the asset pool formed from the pooled funds above all other creditors.

The E-Money Regulations permit two types of pooled-account-safeguarding, both of which could be explored in the United States: a segregation protection method and an insurance/guarantee method.

In a segregated method, the Originator would be required to segregate its pooled account from any other funds it held, including working capital and funds used for other unrelated services. The funds in the pooled account must then be invested only in secure, low risk and liquid assets, which could be approved by the Regulator. The account would also be held at an authorized custodian and such funds would have to be clearly identifiable as assets requiring safeguarding by such a custodian. Moreover, the account must not be used to hold any other funds or assets, including funds that are received for foreign exchange. This requirement would mean that, for each country in which the Originator carried on business, a separate segregated account would have to be established in that country. Robust record-keeping requirements would also be implemented to ensure that, at any time, the pooled accounts and their balances can be easily identified.

In the insurance/guarantee method, the relevant funds must be either covered by an insurance policy with an authorized insurer, or covered by a guarantee from an authorized insurer or authorized credit institution. For this method, it is important to note a policy or guarantee would cover the entire pooled account and not simply funds held overnight or longer. Moreover, in the event of an insolvency, the proceeds of a policy or guarantee would
be payable into a separate account held by the Originator. This account must also be subject to the same types of segregation as described above.

In addition to these two methods of protecting pooled accounts, an organization like nanoPay must be run in such a way that risk of loss or reduction of the pooled account is minimized. An independent auditor must be appointed to ensure none of the organization safeguards have been breached. nanoPay would also conduct regular internal reconciliations between end user accounts and the pooled account and have a clear procedure for reconciling any discrepancies.

Governance

In the digital cash model that has been proposed, it is clear there is a need for transparent and robust governance models. Currently nanoPay operates in Canada, where digital cash is not regulated. As such, aside from general governance best practices, a more formal articulation of principles of good governance has not been necessary. As the company expands its operations into the United States, Europe and South America, a tangible governance plan has been developed, particularly as the company functions as an Originator. This plan is informed by the governance principles articulated in the Payment Services Directive, E-Money Directive and accompanying Regulations and includes:

- Policies regarding minimum board size (e.g. not less than three, one of whom is the CEO);
- Policies regarding Board responsibilities with respect to internal control and risk management within the corporation;
- A requirement for Directors and the CEO to have a minimum level of experience within payments services. An additional requirement for the CEO to also hold relevant education in business, finance or payments services;
- Policies and procedures regarding risk management, AML procedures and KYC requirements for Brokers;
- Restrictions on outsourcing key functions; and
- Clear policies and procedures around protecting the pooled fund (as discussed in the Asset Manager section above).

In addition to these specialized governance requirements, nanoPay is committed to upholding general governance best practices in each of the jurisdictions in which it operates.

C. Isolated Area of Concern

Finally, the QIAT Draft Assessment related the Solution as “Somewhat Effective” with respect to Payment system rules, stating: The proposal can be strengthened by clearly articulating the process for changing the rules (L.2.1) and discussing how the payment system rules will be enforced and monitored. (L.2.3)
To clarify the process around rule development and amendment, nanoPay submits the following:

Because of the cutting edge technology employed by nanoPay and the rapidly evolving payments landscape, the rules will be evaluated annually or bi-annually by a committee composed of participants, nanoPay employees and industry and consumer groups. Rules that are earmarked for revision by the committee will be published for comment, along with a policy paper or relevant research supporting proposed amendments by interested parties. Comments will be considered and incorporated in subsequent drafts. The final approval of revised Rules lies with the nanoPay board, with input from management.

With respect to enforcement and monitoring, annual attestations from all participants will be required. Spot assessments will also be conducted.
Please share your concerns about this proposal’s assessment against the Effectiveness Criteria.

This is a technical digital currency solution; however I am not sure I agree with all QIAT "very effective" ratings given the identified limitations for the unbanked/underbanked, unclear dispute resolution solution and merchant protection particularly without a government "originator" design as originally proposed.

Closed-loop digital cash system. Real-time and rapidly scalable. Able to easily switch among providers. Easy to access with unique customer ID from any computer or mobile. Zero settlement risk. Prefers for Fed to be an originator of digital fiat currency. Pooled funds requires trust in asset manager. Seems very limited, similar to mPESA.

Proposal attempts to be inclusive for consumer and non-banked payments—not business to business. Defers the legal structure and governance to central bank. Lacks effective dispute resolution process, KYC and AML effectiveness. Positive good funds model. Concerned that perception of being totally secure because operating in AWS cloud—maybe secure infrastructure, but did not describe how it plans to protect the application and customer data.

Does not meet criteria for ubiquity.

Innovative digital currency would be a new component of the money supply, without the burden of high fees, with real-time payment certainty, irrevocability and enhancements. Digital closed-loop technology, based on a good funds model, replaces bank notes and coins, without major changes to current bank systems or role of central banks. Leverage market of “80% unbanked and 20% underbanked, 93 million in America. Mint Chip, was originally created by Royal Canadian Mint (RCM). While innovative, the QIAT highly overrated the solution. It falls short of being “very effective/effective” as it was rated. The reviewers Disagree with the QIAT rating for the Effectiveness Criteria.

The proposal is not in conformance with the requirements of a full solution proposal. The requirements were designed to ensure that McKinsey and Task Force time and resources are focused on end-to-end solution proposals that can be thoroughly and credibly assessed against the criteria. This proposal does not meet the requirements. Proposal has answered all sections of the template but in many cases the response does not provide information that would allow the QIAT to evaluate the proposal. The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a "detailed discussion of why the rating is justified and how the solution meets each criterion" (page 22 of template). It does not include specific information in Part C as to how or why the proposed solution meets each of the criteria. As a result, the QIAT is unable to evaluate the solution with the information provided. Altering the existing process defined to offer an opportunity for the proposer to include more explicit information in its submission to make the proposal “assessable” would be unfair to proposers who provided complete proposals before the submission deadline. A few
of the reasons why the proposal did not meet the requirements are as follows: The solution does not adequately explain: a governance plan, how remittance data is linked to the transaction, operational risks, SLAs for disputed payments and identification protection of payee, pooled funds security, plans to adopt new authorization models.

Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

Ubiquity and governance are not fully addressed. Role of banks appears cumbersome.

I generally agree with the assessment provided. I see the proposal being challenging to implement given that FIs will have to become brokers in the Nanopay system and therefore lose an element of control with their customers. I think the FIs will continue to want to own the overall relationship and income stream. I struggle to see this proposal working with the current core software providers who serve smaller FIs as they may not see a value prop in supporting. No rules or governance structure mentioned.

Some questions with S5, handling disputed payments, as dispute resolution was cited as being ambiguous and an area for improvement. Should not be assessed as being "effective."

This solution does appear to be simple yet challenging at the same time in regards to digital currency. It does save on costs for both consumer and financial institutions and provides a real-time process for moving of funds but not depositing into your bank account.

Agree with the dispute resolution that is needs more guidance.

The solution provided no governance model within the solution to be “somewhat effective.”

I agree with the assessment from McKinsey.

Accessibility criteria rated too highly as there is not an adoption plan nor capability to have a payee reach any other account in the US in order to send payment. Value-added services is rated too highly as it is not apparent how various participants could participate in those services without all adopting such services consistently. Rules and governance are rated too highly, as they are not described nor developed.

There does seem to be a high degree of connection to European regulatory framework initiatives. This, along with the related disconnection to the US style of central banking seems to place a friction on the adoption of this solution approach. Further, there seems to be a strong connection to the creation of additional regulatory frameworks in the US styled after a consolidated central banking model common in the EU and other countries. However, the creation of, and adherence to, has a cost to both society and the participants implementing the solution. It would seem better to adapt the solution to the existing regulatory framework and be able to adjust as that morphs into the future. This proposal assessment seems accurate absent the basic thesis described in these comments which will have
potential severe effect on the ability for the scheme to work in a framework with some fundamental differences in approach.

Proposer attempts to be inclusive and provide an end-to-end solution would cobbling of existing user identifiers into a new identification form, thereby driving a form of interoperability. However, the scheme does not go far enough to suggest a workable legal structure and governance model. Instead, nanoPay foists those details on the back of the central banking authority (e.g., the Fed). QIAT picked up on this flaw but still extended pretty generous ratings in these areas.

Agree that dispute resolution procedures need more specifics—the proposal's focus is almost solely on prevention, with not enough information about remediation.

(1) Saves on transaction costs of physical cash (2) more secure (3) more transparent ecosystem (4) can switch freely between “brokers” (5) speed criteria (6) 24x7x365 (7) real-time funds availability and immediate settlement (8) uses shared fraud data to mitigate risk (9) no interoperability required for transactions on the platform.

Agree as assessed. In general, it is a very simple, yet effective solution.

Need development of Governance as noted by QIAT.

Overall I agree with the assessment. Not sure I agree with the specific rating for handling disputed payments but otherwise they were right on target.

The company and its product appear to be changing and evolving in near real time, which causes concern on the part of this reader.

In the self assessment section I found the justification statements contradictory to some of the earlier statement. In addition new information is provided as part of the assessment justification.

The primary access is via a mobile device—usage of POS seems cumbersome and time consuming in the checkout line.

The proposed solution relies on interaction with the ACH network.

**TASK FORCE SOLUTION-ENRICHING COMMENTS**

**Ubiquity**

Thank you for your submission. In my opinion it might be a better design to have clearly defined government control of digital currencies, with your solution providing the technology to drive that process. I find your scalability and real-time settlement and funds availabilities to be well conceived.

Your solution provides a good option for cross-border needs. Concern arises, however, when I consider the impact on the American consumer who is banked and who does not want to deal with the overhead
of a new funding account (and maintaining an adequate balance there vs. what is already in his checking account). I fear this will lead to adoption challenges.

I struggle with the ability to make the solution work in today's payment world. Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. The use of the solution relies on these organizations to support FIs becoming brokers and FIs to lose interchange income. To date, core providers have been unwilling to do this without significant compensation, choosing instead to provide their own solutions and I am not sure banks will implement without interchange. I would like to see a road map for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium-sized financial institutions.

Good solution for mobile and extension of API, as well as meeting most use cases.

The solution could be enriched by describing how payments reach any and all payees, specifically those who do not have access to a Secure Asset Store (SAS).

There are some very positive points to the proposal. However there are also a few questions. There are some lingering questions about the cash-out process. How does payment reach those that do not have an SAS? How are they notified? This solution focuses on brokers for cash out, but could the system use the current ATM network instead?

As an end-user I am concerned about costs. To get providers to join there has to be value for them but there also has to be value for consumers to adopt a new payment methodology. In the middle is the broker who will also charge fees. Even if fees are lower per transaction, will there still be value for end-users after costs of uploading and cashing out are factored in? Ceilings for fees?

What are the incentives for providers to join? How does this help them?

More fully describe how ubiquity – reaching all accounts in the country – achieved. Describe how integration into ACH is achieved (p 54).

U.1 Accessibility – Somewhat Effective, heavily dependent on the “broker”(s) who are replacing the operators or networks in this model, and even any foreign currency is dependent on the “FOREX broker.” It will be difficult to achieve adoption and confidence in this digital currency.

U.2 Usability – Somewhat Effective, assuming the solution is adopted.

U.3 Predictability – Somewhat Effective, the resolution process shifts to the broker, which I think is a risk since the user opening a formal case has results that will depend on the broker’s reputation and overall service to the users/participants.

U.4 Contextual data capability – Somewhat Effective, no remittance data capabilities were shared.

U.5 Cross-border functionality – Somewhat Effective, must establish a Mint Acct or Secure Asset Store (SAS).
U.6 Applicability to Multiple Use Cases – Somewhat Effective, P2P and P2B have been introduced in Canada, but there are still other cases (e.g., B2B) which could be challenging for this model.

Relies on FED to be at least initial originator.

FIs have to forfeit payment revenue to build new security/technical infrastructure.

FI resistance will impede adoption.

Merchant adoption/time to get on board.

Have you considered a method to fund receivers that don't have a SAS?

Viability may depend on the Fed as Operator.

Page 34 – Requires platform to be deployed in that foreign country and end-user to be established – how are those accounts accessed?

Page 176 Using the integrated account model, how would an end-user transfer MintChip Digital currency received into their account to their DDA account?

Efficiency

It appears the solution would be best implemented if done so by the FED. The proposal could be enhanced if there are mechanisms that the solution could be rolled out without extensive assistance from the FED.

Routing method unclear. Proposer should define intentions within solution.

Describe how a single business’s ERP system knows how an incoming payment and related information from any other business’s ERP system will be formatted.

E.1 Enables competition – Somewhat Effective, as the solution is bound to “brokers” it might be difficult for competitive solutions to co-exist.

E.2 Capability to enable value-added services – Somewhat Effective, value-added services might be a challenge without knowing how the “potential value added services” will be effective for the participants.

E.3 Implementation timeline—Somewhat Effective, given the innovation and being a digital currency, it will be challenging to implement, as B2B is their most compelling use case, but adoption can be a hurdle in alignment during an implementation with the banks and merchants.

E.4 Payment format standards – Effective, although ISO 20022, there is still specific field formatting that will need to be executed at the transaction life cycle “after the funds have been received” and this will require compliance so solution format can be interoperable even with cross-border transactions.
E.5 Comprehensive – Somewhat Effective, although this digital currency does not require “clearing, settlement, and reconciliation” due to the model based on “good-funds,” it is still yet not proven how sound the model is in the market place with merchants and the B2B transactions.

E.6 Scalability & adaptability – Not Effective, solution states that they can quickly – in just a matter of weeks – scale up to “Visa’s” capacity; but there is a $1M invest costs in USD to scale up to this level, and it will be difficult to invest those funds unless there was a massive adoption and no estimates of metrics were provided. FIs will potentially have to invest heavily in infrastructure while forfeiting payment revenue.

E.7. Exceptions and investigations process – Somewhat Effective – interesting model, but it seems limited to monitoring “synchronization error” between MintChip “value in the system and the collateralized value in pooled accounts,” and no real-time information is available to those parties affected as part of the transaction.

Long-term funding could be an issue and a concern.

Safety and Security

The reference to hosting the solution in AWS solves and provides a secure infrastructure perception. Would like to see additional emphasis on how NanoPay plans to protect the application and customer/account/payment data from a safety and security perspective. Need to demonstrate how you plan to execute this in a public cloud environment against the growing number of attacking hackers.

The solution could be enriched by describing the Rules needed to support the Asset Manager and the pooled funds to collateralize the digital cash, the system’s overall handling of disputed payments, and fraud monitoring.

Describe who specifically is responsible for investigation with potential fraudulent transactions, and how that party gathers information and communicates with the impacted individual (p 43).

S.1 Risk Management – Somewhat Effective, based on “good funds model” and will rely heavily on the brokers being in compliance with regulations and will conduct a quarterly review. Given that this digital currency is in the start-up stage and does not have significant adoption yet, an “Effective” rating will be overstating their risk processes, as there are other human errors that can negatively impact a digital currency transaction that have not been addressed.

S.2 Payer Authorization & S.3 Payment finality – Somewhat Effective, the proposer believes that the authorization and finality will be aligned with the overall transaction objectives, but I’m concerned that there is no historical proven volume and value of transactions to back up this proposed process. Even at the Payment Finality stage, there is a burden pushed to the “broker” who can only limited investigation.

S.4 Settlement Approach – Somewhat Effective, although based on the model of “good funds” there is no need for the traditional reconciliation of any stages in the payments processes, including settlement,
in the case of MintChip, even the exchange of funds “in-out” balances are maybe done in real time during the day, but other hours the true balances of the accounts are “determined by changes in balances between institutions”- which raises a question if this could impact overall transactions when financial institutions are closed?

S.5 Handling disputed payments – Not Effective, solution relies on existing “consumer protection laws” but does not offer any internal process or policies as to how MintChip will work protecting the end-user along with their brokers. They only stated that end-user can dispute a transaction directly with the merchant, but leaves all the dispute and liability at the end to the user. This shift of responsibility takes away a motivating factor of why a user would be motivated to use this digital currency, which does not offer much recourse to the user.

S.6 Fraud information sharing – Somewhat Effective, “solution uses blacklist data” but at the end the sharing burden placed at the individual “broker” level to share information but it does not offer a true centralized internal platform where this information can be shared among all participant brokers and merchants who accept MintChip to prevent fraud at the initiation point of the transaction.

S.7 Security controls – Somewhat Effective, given that the solution is in the start-up stage, there are integration levels that could be beneficial at the “POS terminals” and at the provider level to ensure protocols are adhered to.

S.9 End-User data protection – Somewhat Effective – relies on “existing consumer laws” but there is not much the model offers in terms of policy and a true process to protect the data at the broker’s level.

S. 11 Participation requirements – Not Effective, is very vague, first bringing in their core brokers, and then stating that maybe FIs and other solution providers can participate but tie to “indirect brokers” with not much information as to the obligations.

Unique approach to security using SAS identifiers as well as multiple kinds of unique IDs, which further enhances the security of each ID. Also appreciate that MintChip requires no account information needs to be shared. There is a reference to the user being able to send money within their limits. It is not clear, but if this is meant to imply that the user is empowered to set limits on the transaction amounts, I think that is a great concept for payments systems to consider. Different consumers have different ideas about what amount would be problematic for them in the event of fraud or an error, so allowing users to customize that aspect might be powerful.

Requiring authentication for each time the application is opened and for each transaction provides a high level of security.

Dispute process.

Relies on banks to capture KYC/AMC and that is very inconsistent depending on the bank’s risk model.

As the primary access is through a mobile device Page 37 - What if the phone is damaged, lost or stolen?
Page 133 S.6 – How would systemic fraud be identified and removed centrally?

Page 141—Regulatory and compliance could be an issue for non-traditional participants.

Page 145 – Is the value of the SAS insured like FDIC?

Page 196 – S1.3 – Big Brother can/could gain a whole lot of information from the TAC.

Page 196 – Who are and where are the Risk management team?


**Speed (Fast)**

F.4 Fast settlement among depository institutions & regulated non-bank account providers – Somewhat Effective, given that the model is pre-funded in the day time hours, there seems to be no issue, but after hours, it was earlier indicated in S.4 “but other hours the true balances of the accounts are determined by changes in balances between institutions,” which raises a question if this could impact overall transactions when financial institutions are closed? This creates a contradiction with what is stated in F.4.

Would have been good to have seen real throughput and latency numbers on identified hardware configurations.

**Legal**

I would have liked to see some suggested implementations for a legal framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution could be enriched by describing the overall payment system Rules needed to make the proposed solution successful.

L.1 Legal framework – Somewhat Effective, proposer states “legal framework is not necessary”; however, given the laws, regulations, AML, KYC requirements and other elements tied to each transaction in the global payment ecosystem, it will be difficult to operate for a long time without some type of Legal Framework structure that could address potential issues with this digital currency.

L.2 Payment system rules – Not Effective, rules are not yet developed, and although the proposer “envisions monitoring of system rules,” a more solid structure of Payment System as foundation for their relationship with their most important partners, which are the brokers.

L.3 Consumer protections – Somewhat Effective, proposer relies on existing consumer protection laws, shifting all liability to the consumer and existing laws, with not much regard to the responsibility of their MintChip solution towards the consumer.
L.4 Data privacy – Somewhat Effective, information in reference to data privacy violations not included, and can beneficial for all parties.

L.5 Intellectual property – Somewhat Effective, proposer states that it has 85+ patents, and it seems that various party owned different IPs, thereby creating a potential conflict of IP ownership in the future. A possible agreement between all the IP patents owners outlining how they will resolve any future conflicts so that the MintChip would not be affected, and caused a disruption in the solution, along with the brokers, and other participants and end-users should receive considered evaluation.

This section could use more adaptation to the US-based environment as it exists today without calling for additional regulatory frameworks and compliance thereto.

Some of the patent requests have been pending since 2013, many in 2015—some expiring in 2016—it would have been good to have provided a up-to-date list when responding to the follow-up questions and assessment provide is there a current a up-to date list?

**Governance**

I would have liked to see some suggested implementations for a governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution could be enriched by articulating the overall governance model needed to make the solution effective and inclusive, especially given the new technology described to support a digital currency, as a collateralized bearer-asset-transfer system.

Governance was severely lacking overall. Clearly it was mentioned because it had to be but was not a priority. There is a need for some sort of governance plan which outlines who will run the system and how issues/changes to the system will be vetted and decided upon. This is critical to potential adoption. Please present at least a suggested model.

Inclusive governance was lacking. Saying that different participants with different needs will inform policy-making means absolutely nothing without additional guidance. Will end-users be involved in the decision-making process and at what percentage of total participation? Also, if multiple levels of governance, at what levels will end-users be involved? As a public system there is some level of open accountability?

Governance and dispute resolution procedures should be clearly explained with more details.

Provide more information to be responsive to the criteria.

G.1 Effective governance & G.2 Inclusive governance – Not Effective – very vague, the proposer only stated “potentially occurs along a spectrum of governance models that best serve the needs of the solution.” – Inclusive, very vague as well – “potentially occurs it is logical to mirror an effective
governance model along the spectrum of governance models that best fit the needs of the solution.” Believe the QAIT rated too generously on Governance.

This section could use more adaptation to the US-based environment as it exists today without calling for additional regulatory frameworks and compliance thereto.

The open platform concept that allows more participants than legacy systems is encouraging, but I would be more comfortable if the proposal explicitly stated that the governing body would have proportional representation from all stakeholder groups.

I understand that the details of governance would get decided as the Originator of the system is determined.

Governance needs to be developed to strengthen proposal.
Proposer responses to the Task Force comments were optional and not all proposers chose to respond
Faster Payments QIAT

FINAL ASSESSMENT
Faster Payments QIAT

FINAL ASSESSMENT

Proposer: nanoPay Corporation

Summary Description of Solution:
nanoPay’s MintChip is digital cash that has been broadened into a direct, collateralized bearer-asset-transfer system. Essentially, it securely stores and transfers any form of digital asset between users on a single, verifiable platform—i.e., a closed-loop system. Originally created by the Royal Canadian Mint (RCM), MintChip is already in limited operation in Canada.

MintChip digital currency will be transferred using Secure Asset Stores or SASs (electronic wallets). The SASs will be loaded using existing payment instruments. Since all transactions operate under a good-funds model, there should be no clearing, settlement, or liquidity risk.

- The MintChip solution includes the following participants:
  - The Originator manages (1) operation of the stand-alone MintChip system component that creates MintChip value and Secure Asset Stores (SAS), (2) administration of the security parameters in the MintChip system, and (3) a pooled account that holds fiat currency for MintChip value sold to brokers.
  - Note: the proposal originally suggests that the Federal Reserve should be the Originator (though as part of initial implementation, the Platform Operator may act as the Originator). In the addendum to the original proposal, the proposer notes that the Solution does not require the government to play the role of Originator. In use cases where the Originator is not the government, the pooled funds will be protected by being held at an Asset Manager and funds will only be invested in instruments where the Principle is guaranteed.
  - The Technology Provider owns the MintChip platform that provides: (1) the system components for deployment by the Platform Operator and the Originator; (2) integration support for Brokers and Merchants; and (3) software enhancements, maintenance, and support.
  - The Platform Operator is responsible for deploying and operating the MintChip platform and for administering operating rules, standards, and protocols.
  - The Broker is a depository institution or regulated non-bank account provider that: (1) buys and sells MintChip value from/to Originator, (2) enrolls end-users, (3) provides mechanisms for end-users to buy and sell MintChip value, and (4) provides currency conversion services (optional).

While MintChip has many use cases, the QIAT has conducted the assessment based on the use case in which it is a platform for providers to transfer digital assets (in this case, cash) between end-users’ SASs, not the use case in which it serves as a digital fiat currency.

EXECUTIVE SUMMARY OF THE PROPOSAL

- Major strengths of the solution:
  - The solution requires only a payee’s MintChip identifier and a mobile device or internet connection for use, making it ubiquitous throughout providers.
  - The solution allows end-users to switch freely among brokers and puts no limitations on smaller players. It is also open-source to all services that comply with its operating standards. It is hosted by AWS (Amazon Web Services) and Peer1, which assures complete redundancy and access to all aspects of the end-to-end payment process.
The proposal provides concrete figures to support the argument that the solution is quickly scalable at low cost.

The solution provides real-time funds availability and immediate settlement. The solution operates at no settlement risk since it relies on prepaid funds. It supports the capability to shut down the payment system in the event of fraud risk and uses shared blacklist data to limit risk.

The broadened definition of MintChip offers the opportunity to open the system to use cases beyond the traditional payments use cases.

**Areas for improvement and enhancement:**

- The solution does not hinge on the Federal Reserve’s willingness to serve as the Originator (and to create new monetary policy), but the Fed’s serving in this role is desirable as a means to drive adoption in the solution’s early days. Without MintChip as a digital fiat currency, adoption may have challenges, since depository institutions will have to forfeit the revenue associated with current payment systems and build new security and technical infrastructure.

- Solution is highly dependent on confidence in the Asset Manager that protects the pooled funds to collateralize the digital cash. Risk and regulatory considerations are needed to ensure the safety and security of the funds held at the Asset Manager, as well as provider incentive to give up funds to be held at the Asset Manager

- Although the solution builds on existing systems, it is not interoperable and does not leverage existing systems to reach users who are not yet enrolled in the payment system. Two aspects of the solution do enable quick enrollment, however: 1) unbanked customers could potentially purchase MintChip in exchange for cash at a broker merchant; 2) payees could open a MintChip account via a Secure Asset Store (SAS).

- The proposal leaves dispute scenarios ambiguous. In the event of fraud, the solution does not provide businesses with 100% protection, as it focuses on prevention rather than remediation.

**Use cases addressed:**

- The solution addresses all four major use cases (P2P, P2B, B2P, and B2B). It can be built into the POS transaction flow directly into the POS terminal.

**The proposer’s overall ability to deliver proposed solution**

- nanoPay launched MintChip in Canada in April 2016, and MintChip 2.0 is expected to be deployed in summer 2016. The solution is partially deployed in Canada, with 15 merchants accepting MintChip as a form of payment in a geographically controlled area of Toronto. Additionally, the proposer is in discussions with all five of Canada’s major banks, three of which are in various stages of Proof-of-Concept efforts. nanoPay is working on integrating with European and Brazilian banks as well. With these steps already underway, the proposer seems well positioned to deliver the technical solution.
Ubiquity

U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution requires only the payee’s MintChip identifier—an email address, mobile phone number, name, or even a Facebook username—to send and receive payments (U.1.2). MintChip thus does not require multiple operators or networks and is ubiquitous. The broker (see Description of Solution above) can be a depository institution or a regulated non-bank entity (U.1.1), effectively opening the solution to both banked and unbanked customers of the payments system (U.1.4). Additionally, any account or means of payment (including cash) can fund the SAS through a broker (U.1.1), as long as the broker accepts that form of payment. End-users can set up multiple SASs within their MintChip account to accept/send payments in different currencies; if a payer or payee does not have a SAS for a given currency, they are directed to a FOREX broker to convert funds and complete the transaction (U.1.3). Upon initial payment, the platform triggers the creation of a SAS that can be claimed by the payee, thereby adding a new user to the network. MintChip supports any currency as long as the source of funds works with that currency.

Since MintChip does not require multiple operators or networks, no interoperability is required for transactions that occur on the platform (U.1.6). The system does not depend on the operator apart from issuing the currency.

The proposer plans to “work with providers, end-users and software developers to achieve widespread adoption” (p. 108), but the incentives for providers to participate are not clear (U.1.5). In particular, confidence in the Asset Manager where pooled funds are held and secured is critical to provider adoption, and the proposal indicates that it is still working with the lead investor to identify the best way to ensure confidence in the system—for example, by regulating e-money and educating consumers to shape any perception of confidence in the Asset Manager.

U.2 Usability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution is usable as long as access to a wireless mobile device or internet connection is available (U.2.1). Only the MintChip identifier is needed to initiate payments (U.2.2), and the solution can be accessed to do so 24x7x365 (U.2.3). Retail and online transactions are automatically accepted, and the funds received are good funds immediately (U.2.3). In a P2P (person-to-person) payment, the sent funds are marked as pending until the receiving end-user accepts them.

As long as the end-user is comfortable with using a mobile device for payments, the system should be easy to use (U.2.4). Guidelines included in the platform rules help to ensure consistency in user interfaces.
U.3 Predictability

**Very Effective**

**Rationale:**
The solution uses RESTful APIs (application programming interfaces) to deliver core components—registration, security, cash-in, cash-out, transaction logs and transactions—consistently across channels, devices, and providers (U.3.1, U.3.4). It leverages digital disclosure to meet disclosure requirements (U.3.2).

The MintChip system uses the same standard communication and messaging protocols across the entire platform, no matter which provider is facilitating access to that platform (U.3.3). The solution’s transaction messaging is compliant with ISO 20022, the international standard format for payment messaging.

The solution includes confirmation capabilities to allow an end-user to correct errors prior to sending a payment; however, errors will still occur. The solution allows the payer to initiate an automated resolution process, which lets him/her request full or partial repayment by sending a request for payment to the payee. If the issue is not resolved, a formal dispute can be initiated through a broker. Resolution processes are also in place for system-generated errors.

U.4 Contextual data capability

**Very Effective**

**Rationale:**
The solution is based on ISO 20022, which makes it a conduit for expanded remittance data (e.g., line-item SKU data, trade settlement and agreement data, and trade delivery data) (U.4.1) and allows all transaction data to be exported into a format receivable by account and personal finance systems, as well as large ERP systems (U.4.2). Though the message format is standardized using ISO 20022, any information or links can be associated with the transaction and stored in the flexible transaction log (p. 113) (U.4.3). Further, the system has the capability to handle batch payments (e.g., payroll files) as well as the ability to distribute a single payment to multiple recipients.

The proposal can be strengthened by clarifying exactly how remittance data is linked to the transaction.

U.5 Cross-border functionality

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale:**
The solution is currently rolled out in Canada, and the proposer is working to integrate it with European, Brazilian, and Canadian banks. The proposer plans to work with EFT, ACH, and SWIFT providers to ensure that funds can be received into non-participating bank accounts globally (U.5.2). The Royal Canadian Mint mints coins for 72 countries, providing a logical avenue for MintChip’s roll-out and broader foreign deployment.

However, the solution has not yet rolled out in the United States (but is expected to in 2016). Cross-border functionality is intuitively possible in MintChip, but it has yet to be launched and
executed. One concern is that the use of the MintChip app is currently restricted to Canada and the Canadian dollar. A subsidiary company exists in the UK that will launch there after acquiring an EMI license, which can be expanded into the broader Eurozone (U.5.5).

As mentioned, the solution’s platform does allow users to open a SAS in any currency and to receive funds in any currency (U.5.4). Advance fee disclosures are considered in the solution’s terms and conditions (U.5.3).

The proposal can be enhanced by explaining how collateral fiat currency is cleared and settled.

### U.6 Applicability to multiple use cases

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution supports all use cases, although only two (P2P and P2B, person-to-business) have been introduced into the Canadian market.

### Efficiency

#### E.1 Enables competition

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution allows users to freely choose brokers (E.1.1). It does not limit an entity’s ability to move among providers (E.1.2) or set up any barriers to small players (although these players might be limited by an inability to pre-load funds) (E.1.4). The MintChip platform’s operating rules require providers to disclose in advance to end-users all of the information needed to understand the total cost of using their services (E.1.3). The solution allows end-users to have a single alias that links to multiple SASs.

#### E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution is open-source for all services and providers that comply with operating standards (E.2.1-2). The MintChip platform’s operating rules require providers to clearly disclose to their customers that the value-added services they have added to baseline MintChip services are optional (E.2.3). The open payment and broker APIs enable the creation of value-added services. One aspect to consider, though, is MintChip’s purported irrevocability of payment. This irrevocability could be perceived as an obstacle to the basic value-added service of dispute/chargeback handling.

The proposal would be strengthened by illustrating two to three examples of potential value-added services.
E.3 Implementation timeline

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution has already been partially launched in tightly controlled geographical areas of Toronto and will receive revenue from initial customers, such as banks, retailers, and telecom companies. The revenue model currently is geared toward the retail environment and is based on a small, fixed, per-transaction fee charged to the merchant. The revenue model for banks combines an integration/license fee with volume-based pricing. The idea of exploring least-resistance uses cases (e.g., B2B transactions in specific industry verticals) could prove a logical launching point.

The proposal clearly articulates implementation-specific hurdles, but ubiquity hurdles exist as well (e.g., inertia associated with existing payment systems and services, the need for multiple banks and merchants to accept the solution, etc.) (E.3.1).

The proposal can be strengthened by providing an air-tight business case for merchants to adopt it, as well as a clear articulation of the reasons why banks would choose to leverage the solution (E.3.1).

---

E.4 Payment format standards

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution is ISO 20022-compliant (E.4.3-4) and flexible enough to allow any off-ramp to require certain fields (E.4.1). The system is unique in that it allows certain fields to be completed after the funds have been received in MintChip. To enable ongoing development, the platform allows for further modification or additions (E.4.4). All external APIs will be published and are designed to be consistent with open standards (E.4.5).

The mobile applications will all be open-source so that anyone can build on them, improve them, or even write their own applications. The solution’s ISO 20022-compliant format should make cross-border interoperability easier (E.4.2).

---

E.5 Comprehensive

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution is a good-funds model that enables all aspects of the end-to-end payment process (E.5.1). Because MintChip is a digital currency, clearing, settlement, and reconciliation are not required (E.5.2).

---

E.6 Scalability and adaptability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
**Rationale:**

One of MintChip’s greatest differentiators is its ability to scale up its throughput capacity quickly at a very low cost (E.6.2). The solution has the potential to scale to Visa’s capacity in just a few weeks with an investment of just $1M USD. Today’s MintChip platform can process thousands of transactions per second; the current capacity of the Visa system globally is approximately 50,000 transactions per second. MintChip’s technical design supports projected use cases (E.6.1) and is readily adaptable to ongoing developments (E.6.3). While the technical design contains auto-scaling triggers that are rooted in performance metrics for both API code and raw HSM (hardware security module) performance, the proposal can be enhanced by providing estimates of projected demand, peak-hour spikes, latent capacity in the network, etc. (E.6.2)

**E.7 Exceptions and investigations process**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution stores and tracks all transaction information (E.7.2) and provides alerts, shared logs, and tools for regulators/investigators to handle exceptions (E.7.1).

MintChip’s web portal allows providers and brokers to query stored data. It has sufficient multi-factor authentication to be able to control access effectively. The solution can be enhanced by building the capability to proactively push this kind of information to those who need it. The web portal tool also provides the ability to manage SASs, assign/revoke user access, review transactions, define business rules, and manage disputes.

A synchronization error between the MintChip value in the system and the collateralized value in pooled accounts is the primary type of error that should be monitored for. The proposer is also exploring the possibility of incorporating machine-learning capability and stream-computing partners into the exceptions process.

The proposal can be strengthened by building capability into the web portal that proactively pushes exceptions data to the provider and by clearly describing the tools available to support the exceptions and investigations process (E.7.1).

**Safety and Security**

**S.1 Risk management**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Because the solution operates on a good-funds model, settlement risk is essentially non-existent, because transactions are settled immediately and can only be executed with available good funds (S.1.2). The consequences of human error (e.g., inputting an incorrect transaction value) are the responsibility of the parties involved (S.1.3). The solution leverages existing incentives for brokers to comply with AML (anti-money laundering regulations) and KYC (know-your-
customer regulations). Reviews of risks and compliance with the payment system are conducted quarterly (S.1.6).

The solution has a dual risk management system: (1) an internal system that contains configurable controls such as maximum balance allowed, maximum debit and credit transactions, etc. and (2) an operator risk system that monitors the MintChip platform’s transactions. Additionally, 10% of transactions will be sampled at any given time to confirm that the system is working well.

The proposal can be strengthened by providing detail about specific operational risks other than human error (S.1.3) and by describing the remediation process for erroneous, fraudulent, or unauthorized transactions (S.1.4). It can be further enhanced by clearly articulating the “incentives” for brokers and providers to comply with risk requirements (S.1.5).

S.2 Payer authorization

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Payers authorize each MintChip transaction via their smartphones, typically using the Touch ID function for iOS devices or the fingerprint scanner for Android devices (S.2.1). The solution allows payers to pre-authorize payments (S.2.2), and payers can revoke pre-authorization or change pre-authorization parameters easily and quickly (S.2.3). The same authentication process is applied to pre-authorized transactions, adding another layer of security to the payment process.

S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Transparency, speed, low-cost efficiency, and finality of payment are the driving factors of this solution, and so it focuses on ensuring that erroneous payments are not made in the first place. MintChip relies on prepaid funds, and the SAS is debited immediately when a payment is initiated (S.3.1).

The system is intended to be a digital equivalent to cash, not an extension of existing card networks. A mechanism is in place to request the return of an erroneous payment. If the return request is denied, the payer may contact his/her broker, who will have tools to conduct limited investigations. As a control mechanism, large payments will not be sent without accompanying invoice or metadata that confirms the amounts and the reasons for the payment.

S.4 Settlement approach

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Because the solution backs all value with traditional cash, settlement between depository institutions only needs to take place when cash-out (deposit) and cash-in (withdrawal) occur at
different institutions (p. 131) (S.4.1). This also means that there is no inter-provider risk, as MintChip is always loaded with fiat currency good funds (S.4.2).

Because the end-user holds a MintChip account and deposit account with the same broker, and because traditional cash backs all MintChip value, a cash-out is simply a ledger entry for the broker (i.e., an “on-us” transaction for the broker). MintChip will settle between end-user accounts during the day, with frequency determined by changes in balances between institutions as compared to normal trends (S.4.1).

Pooled funds will be protected via two options available under the E-Money Regulations: (1) a segregated model that requires the Originator to segregate its pooled accounts from other funds that it holds, including working capital and funds used for other unrelated services; and (2) an insurance/guarantee method that ensures that the relevant funds are covered either by an insurance policy with an authorized insurer or by a guarantee from an authorized insurer-of-credit institution.

S.5 Handling disputed payments

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

If a user believes that his/her smart phone has been compromised, s/he can shut down the SAS through the provider (S.5.1). If fraudulent transactions have occurred, the perpetrators can be immediately shut out of the system. Generally, though, for disputed payments the solution relies on the existing consumer protection laws that both banks and regulated non-bank account providers already follow and does not offer any of its own protection policies or processes (S.5.2, S.5.5).

A framework is in place to allow end-users to request a return of funds (S.5.3), but for an online transaction this request will require the end-user to disclose his/her identity to the payee. A payment can be returned in real time as long as the payee agrees to it (or is forced by law). One unique aspect of the solution is that a customer can click a button within the app to contact and appeal directly to the merchant about a disputed payment (S.5.5).

While the solution defines the roles, responsibilities, and liabilities for losses to businesses and governments, the solution’s focus is on loss prevention rather than remediation. The proposal can be strengthened by establishing and articulating clear SLAs (service-level agreements) for disputed payments (S.5.1).

S.6 Fraud information-sharing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution uses blacklist data on fraudulent credit cards and bank accounts to share internal transaction profiles with partners (S.6.2), and transaction history is stored and accessible to resolve payment disputes (S.6.6). End-users’ PII (personally identifiable information) is excluded from information-sharing (S.6.1). The solution provides real-time fraud alerts by requiring brokers to notify nanoPay “on a timely basis” of known and suspected fraudulent accounts (S.6.3).

As a measure of consumer protection, consumers can click on a button within the app to contact merchants directly about disputed payments (S.6.5). Providers can assist consumer end-users with this process and see the details of any payment (p. 134).
The proposal should consider implementing a policy of providing differential access based on the various parties’ roles and responsibilities (S.6.5). The solution can be improved by taking a more active role in the information-sharing process while offering other value-added services such as data aggregation and analysis (S.6.2). A potential fraud service could be a centralized, opt-in sharing service, with appropriate value-add on the back end.

S.7 Security controls

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

In the current, Canadian implementation, the solution uses Amazon Web Services’ (AWS) co-located data center hybrid system for security controls. The HSMs [hardware security modules—“the same hardware used in today’s global payments systems” (p. 9)] and Canadian personal information are housed in the data center. The transaction logs, all production MintChip APIs, and production databases reside in multiple regions (7.1-2).

The proposal can be enhanced by detailing how the solution will ensure that providers follow security protocols when registering an end-user (e.g., through administration of operating rules and minimum security standards) (S.7.2). While the proposal introduces the possibility of integrating with POS terminals, it would be beneficial to explain how this integration will be achieved.

S.8 Resiliency

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution’s architecture (pp. 137-138) for redundancy—if operating as it should—ensures that the solution will never be unavailable for “more than a minute” (p. 138). The proposal can be enhanced by providing specific target metrics (S.8.1). In case of disaster, the solution has solid contingency plans and will provide access to the platform and all data in another region (see S.7), albeit in a reduced capacity (S.8.2).

The system is designed to prevent systemic risk (S.8.3), since the MintChip platform “has no real dependencies on other market players, with the exception of on- and off-ramps for loading and offloading traditional currency housed by banks” (p. 138). The ramps are “managed by industry-accepted protocols, legally vetted frameworks such as PCI-compliance in the case of credit card transactions, and the fact that no proprietary techniques or communication [occurs]…outside of rigid, controlled channels,” according to the proposal (p. 138).

Independent security analysts have assessed the system’s security. Annual penetration tests identify system vulnerabilities. The solution avoids having any single point of failure by maintaining hosted environments in distributed data centers with redundant hardware and software.

S.9 End-user data protection

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
**Rationale:**

MintChip relies on existing consumer protection regulations, which are sufficient for this solution. Provider and operator requirements are not articulated, but it is assumed that existing provider requirements on data protection are adequate to meet S.9.1. Data is encrypted, and access to it is restricted (S.9.2-3). End-users do not share PII with one another at any time during the payment process (S.9.2-3). It is the assessors’ interpretation that MintChip works through a central directory that holds broker names and aliases—the extent of the sensitive information it holds—and that brokers hold the remaining information.

**S.10 End-user/provider authentication**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

End-users are authenticated at enrollment and then again when changing any of their credentials, including their phone number or device. They are authenticated when opening the app and then again when processing a transaction. The solution uses social media, phone numbers, email addresses, and device identifiers to authenticate consumers and their devices for a limited set of services with low payment thresholds. To have access to the full set of services, a consumer must go through a bank’s KYC process. Additional KYC and AML processes are required if the end-user wishes to send large sums domestically or abroad (S.10.1). Merchants have access to a broader set of services.

The solution has robust mechanisms to ensure that payments reach their intended payees (S.10.2). It aligns with regulatory guidance and industry standards for end-user authentication (S.10.3), and it has strong end-user authentication controls with risk-weighting (pp. 38, 53, 135) (S.10.4-5). The proposal states that cryptography and “key components of the security architecture” can be updated as needed (p. 141) but does not share plans for adopting new authentication methods as the threat landscape evolves (S.10.6).

**S.11 Participation requirements**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution contemplates traditional FIs as brokers, but alternative providers can offer MintChip services indirectly by establishing pooled accounts with their brokers, although they must have enough capital to prepay all of the MintChips. Alternative providers could set up their own MintChip USD account and then register individual end-users and allow them to exchange USD for MintChip USD (S.10.1). Because there is no clearing and settlement of the payment per se, there is no disadvantage to dealing with an “indirect” broker.

The proposal can be strengthened by describing whether participation requirements ensure that FIs and non-banks have the operational, financial, and legal capacity to fulfill their obligations (S.11.2) and by detailing its processes for monitoring and ensuring providers’ compliance with participation requirements (S.11.3).
Speed (Fast)

F.1 Fast approval

<table>
<thead>
<tr>
<th>Rating</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast approval</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
Immediate approval comes through the use of a good-funds model. Only pre-funded transactions may be executed. Once the payment is authorized, the value is exchanged between parties and accounts.

F.2 Fast clearing

<table>
<thead>
<tr>
<th>Rating</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast clearing</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
Clearing occurs when the VTM (value transfer message) is delivered to the payee to accept. The VTM immediately makes the payment information available to the payee’s provider so that they may notify the payee. Clearing is nearly instant and aligns with the VTM.

F.3 Fast availability of good funds to payee

<table>
<thead>
<tr>
<th>Rating</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast availability of good funds to payee</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
Once the payer creates the VTM, the value is immediately and irrevocably available to the payee and only the payee.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

<table>
<thead>
<tr>
<th>Rating</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast settlement</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
</tr>
</tbody>
</table>

Rationale:
Payment in digital currency (i.e., MintChip) in the solution is a direct value/asset transfer between end-users’ SASs; therefore, the transaction is instant and irrevocable, with settlement included. The MintChip-to-fiat currency conversion process is clearly explained, addressing even the rare instance when a MintChip redemption amount may exceed a broker’s pooled account value.

Regarding payments across time zones (F.4.2), the proposal says, “The location of [the] payment recipient’s account is irrelevant, and the 24x7x365 nature of the platform means that there is no issue sending payments inter-time zone” (p. 144). The proposal can be enhanced by discussing the process that occurs when providers in different countries exchange payments.
F.5  Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Rating</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td></td>
</tr>
<tr>
<td>Effective</td>
<td></td>
</tr>
<tr>
<td>Somewhat Effective</td>
<td></td>
</tr>
<tr>
<td>Not Effective</td>
<td></td>
</tr>
</tbody>
</table>

Rationale:
Information about the transaction is communicated in multiple ways to end-users. The user interface provides an immediate confirmation notice to the payer (F.5.1). The payee receives a push notification, email, and in-app notification that funds are available for receipt (F.5.2).

---

Legal

L.1  Legal framework

<table>
<thead>
<tr>
<th>Rating</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td></td>
</tr>
<tr>
<td>Effective</td>
<td></td>
</tr>
<tr>
<td>Somewhat Effective</td>
<td></td>
</tr>
<tr>
<td>Not Effective</td>
<td></td>
</tr>
</tbody>
</table>

Rationale:
The proposal maintains that a legal framework for the solution is unnecessary, stating, “Because of the simplicity of the MintChip ecosystem, a complex legal framework is not necessary to adequately protect participants. Because clearing, settlement and reconciliation are all instantaneous, rules regarding responsibilities and liabilities throughout those stages of a transaction are no longer necessary. Existing legislation that governs participants’ KYC and AML requirements will continue to apply, particularly during the participant-registration process. Within the ecosystem itself, payment rules are required, rather than a freestanding, newly-developed legal framework” (p. 147).

The solution manages regulatory capital by investing the float in short-term treasury bills, which means that no funds are at risk, and there is always a real dollar for every dollar of digital cash. In the absence of regulations in Canada, the proposer has been following the European derivatives for electronic money and payment services directives. These derivatives include protecting the payment system from the bankruptcy of the asset manager holding the float (or pool). Additional “regulatory capital” may be required, but in the near term, the proposer will invest the float in short-term treasury bills, making the digital cash backed de facto by the same government that backs the fiat currency (p. 147) (L.1.1).

L.2  Payment system rules

<table>
<thead>
<tr>
<th>Rating</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td></td>
</tr>
<tr>
<td>Effective</td>
<td></td>
</tr>
<tr>
<td>Somewhat Effective</td>
<td></td>
</tr>
<tr>
<td>Not Effective</td>
<td></td>
</tr>
</tbody>
</table>

Rationale:
The solution requires detailed payment rules to govern the relationship between the broker and operator and to support its regulatory regime, but these rules have yet to be developed (L.2.1). The proposer envisions a spectrum of potential approaches to monitoring system rules (e.g., annual self-assessments, self-assessments with spot audits, full set of legally binding regulations, etc.) (L.2.3).

Rules will be evaluated annually or bi-annually by a committee made up of participants, nanoPay resources, and industry and consumer groups. All participants will be required to provide annual attestation.
L.3 Consumer protections

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The dispute-handling process, as discussed in previous sections, involves a request for the return of an erroneous payment. Absent a clear resolution, the payer may escalate to involve the broker. The solution will rely on existing consumer protection laws and regulations, as it does in its Canadian iteration.

The proposal can be improved by detailing the protection laws and regulations that the proposer will rely on to provide adequate consumer protections and by clearly articulating how end-users and providers can establish additional, optional consumer protections for payments that may exceed existing protections (L.3.3)

L.4 Data privacy

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The nature and type of end-user data required for security, compliance, and authentication are clearly articulated in descriptions of the transaction process (L.4.3). A terms and conditions agreement for end-users clearly articulates the data that the solution collects (L.4.4).

The proposal can be strengthened by laying out an approach to dealing with privacy violations (L.4.1-2).

L.5 Intellectual property

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution is already in use in Canada, but this does not prevent IP protection claims from arising in other places. The proposer is clearly taking steps to ensure the security of intellectual property, as evidenced by the full back-up of patents provided (more than 85 patents). Each party owns its own IP, and existing IP regulations should be sufficient.

Governance

G.1 Effective governance

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The proposal does not present a clear path, plan, or details for the solution’s governance model. Given the spectrum of use cases to which MintChip applies, the proposer suggests that governance could potentially occur along a spectrum of governance models that best serve the
needs of the solution. For example, a systemically important solution would require a complete governance structure, but a narrow, contained solution does not require as many checks and balances.

The proposer does recognize the need for strong governance principles, including: (1) board size; (2) board responsibilities for internal control and risk management; (3) requiring the directors and CEO to have a minimum level of payment services experience; (4) policies for risk management, AML, and KYC; (5) restrictions for outsourcing key functions; and (6) policies for protecting the pooled fund.

G.2 Inclusive governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The proposal does not present a clear path, plan, or details for the solution’s governance model. Given the spectrum of use cases to which MintChip applies, the proposer suggests that governance could occur along a spectrum of governance models that best serve the needs of the solution.

The proposal can be strengthened by articulating a tangible plan for governance—with details on what the governance model will include—to serve as a path forward until a model can be constructed and implemented. The proposer should take steps to ensure that a clear vision of inclusion is built into the governance model to allow for: (1) the consideration of public interest (G.2.1), (2) influence and input by a wide range of stakeholders (G.2.2 and G.2.4), (3) inclusion of governing bodies that fairly represent stakeholders’ risks and interests (G.2.3), and (4) a clear approach to address conflicts, both real and perceived (G.2.5).