Faster Payments QIAT

Proposer: Thought Matrix Consulting, LLC dba Pencanarts

February 21, 2017

TABLE OF CONTENTS

Original Proposal 2

Q&A Response 63

Draft QIAT Assessment 80
  (Includes proposer comment in Appendix A & B) 96

Task Force comments 99

Proposer response to Task Force comments 107

Final QIAT Assessment 120
Final Version
March 2, 2016

Faster Payments Task Force Proposal

Money Modules™

4/30/2016
Submitted by: Ed Oppenheimer, Thought Matrix Consulting, LLC
CONTENTS

Background ..................................................................................................................................... 4
Purpose of the Template and Instructions for Use ................................................................. 5
  Proposal Review Process ........................................................................................................ 5
  Instructions for Submission and Proposal Review Process Timeline ................................... 6
  Legal Considerations ................................................................................................................ 7
Proposal Template ........................................................................................................................ 9
Executive Summary ....................................................................................................................... 9
Use Case Coverage ...................................................................................................................... 15
  Supported Use Case Coverage Summary ........................................................................... 15
  Cross-border Use Case Coverage (If Applicable) ............................................................... 17
  Proposal Assumptions (Optional) ......................................................................................... 18
Part A: Detailed End-to-End Payments Flow Description ....................................................... 21
  Part A, Section 1: Solution Description ................................................................................ 21
    1. Initiation ...................................................................................................................... 22
    2. Authentication ............................................................................................................ 28
    3. Payer Authorization ..................................................................................................... 30
    4. Approval by the Payer’s Provider ................................................................................ 31
    5. Clearing ........................................................................................................................ 32
    6. Receipt ........................................................................................................................ 33
    7. Settlement .................................................................................................................... 36
    8. Reconciliation .............................................................................................................. 36
  Part A, Section 2: Use Case Description ............................................................................... 38
  Part A, Section 3: Use Case by Effectiveness Criteria .......................................................... 41
Part B: Business Considerations ............................................................................................... 44
  1. Implementation Timeline ................................................................................................. 44
  2. Value Proposition and Competition ................................................................................ 45
  3. Integration Effort ............................................................................................................ 47
Part C: Self-Assessment Against Effectiveness Criteria ............................................................ 50
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubiquity</td>
<td>51</td>
</tr>
<tr>
<td>Efficiency</td>
<td>53</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>55</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>58</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>59</td>
</tr>
<tr>
<td>Governance</td>
<td>61</td>
</tr>
</tbody>
</table>
BACKGROUND

Strategy 2 of the Federal Reserve’s Strategies for Improving the U.S. Payment System paper is to “Identify effective approach(es) for implementing a safe, ubiquitous, faster payments capability in the United States”. The Faster Payments Task Force was created to support this strategy and has designed the Faster Payments Effectiveness Criteria (Effectiveness Criteria) and process for assessing alternative faster payments proposals.¹ The Effectiveness Criteria is consistent with Strategy 2, as well as the broader set of “desired outcomes” set out in the Strategies Paper. These desired outcomes include:

**Speed:** A ubiquitous, safe, faster electronic solution(s) for making a broad variety of business and personal payments, supported by a flexible and cost-effective means for payment clearing and settlement groups to settle their positions rapidly and with finality.

**Security:** U.S. payment system security that remains very strong, with public confidence that remains high, and protections and incident response that keeps pace with the rapidly evolving and expanding threat environment.

**Efficiency:** Greater proportion of payments originated and received electronically to reduce the average end-to-end (societal) costs of payment transactions and enable innovative payment services that deliver improved value to consumers and businesses.

**International:** Better choices for U.S. consumers and businesses to send and receive convenient, cost-effective and timely cross-border payments.

**Collaboration:** Needed payment system improvements are collectively identified and embraced by a broad array of payment participants, with material progress in implementing them.

All proposals submitted through the Task Force’s assessment process will be assessed against the Effectiveness Criteria to determine how well solutions can achieve the desired outcomes associated with improving the U.S. payments system.

¹ “Proposal” is defined in the Glossary of Terms as, “The written document that provides a detailed description of a faster payments solution, and demonstrates how it meets the Effectiveness Criteria for a faster payments solution”.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
PURPOSE OF THE TEMPLATE AND INSTRUCTIONS FOR USE

This proposal template has been developed to assist proposers in detailing their proposal for a full end-to-end faster payments solution. The template is designed to increase the consistency of information provided by proposers, as well as to provide the breadth and depth of information needed for the Qualified Independent Assessment Team (QIAT) to understand and assess a proposal against the Effectiveness Criteria. Proposers submitting proposals for assessment by the QIAT should use this template and complete all parts and sub-sections as described in the instructions.

This template includes three parts. Part A requires proposers to describe and illustrate (via a flow chart) what the solution does at each stage of the end-to-end payments process (from initiation of the payment through to the reconciliation of the payment). This description should be provided for the solution overall, as well as for each use case that is supported by the solution. Proposers will also be required to complete a table indicating which parts of the criteria each use case addresses (for example, the solution may enable contextual data capability for business-to-business payments, but not for person-to-person payments). Part B requires proposers to describe business considerations for the solution. These business considerations include: a detailed timeline to achieve initial implementation and then to achieve ubiquity; the intended value proposition of the solution and how it supports competition; and integration considerations. The detail in Part B will help the QIAT understand the feasibility of the solution and will help support its assessment against the Effectiveness Criteria. Part C requires proposers to provide a self-assessment and justification of how the solution meets each of the criteria outlined in the Effectiveness Criteria.

Proposers should refer to the Effectiveness Criteria when completing all parts of the proposal template.

Proposal Review Process

Once a proposal has been submitted, a qualitative assessment of the proposal against the Effectiveness Criteria will be conducted by the QIAT. During the assessment process, the

---

2 A full end-to-end faster payments solution (or “Solution”) is defined in the Glossary of Terms as, “The collection of components and supporting parties that enable the end-to-end payment process. A faster payments solution might include new components, the adaptation of existing components, and/or a combination of the two.

- Components include any of the following:
  - Rules, standards/protocols, and procedures
  - Physical or technical infrastructure, networks, systems and other resources needed by all parties to use or enable the rules, standards/protocols and procedures
  - Centralized or shared services, if any
  - Legal framework and enforcement mechanisms
- Parties include any of the following:
  - Governing bodies, operators, depository institutions, non-bank account providers and third-party service providers”.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
proposer will have the opportunity to provide additional information and/or a response to the assessment. The proposer may also choose to withdraw its proposal at any point in during this initial assessment meaning that the proposal will not be shared with the Faster Payments or Secure Payments Task Forces. No confidential or proprietary information should be shared in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report.

Following the completion of the QIAT’s assessment and the compilation of any responses received from the proposer, the assessment will be provided to the Faster Payments Task Force for review. The proposal will be reviewed in its entirety, including the assessment and the proposer response, and Task Force members may offer comments to the proposer and the QIAT. Similarly, the Secure Payments Task Force will review the proposal and provide comments on the security-related aspects to the proposer and the QIAT. The proposer may respond to Task Force comments and may revise its proposal for final QIAT review. The proposer may also choose to withdraw its proposal at this point meaning that the proposal will not be published as part of the final report.

The QIAT will finalize its assessment of the revised proposal with consideration given to comments by both Task Forces. Once the assessment has been finalized, the proposal, QIAT final assessment, and Task Force comments will be published in a final report along with corresponding material for all other solution proposals that underwent and completed the proposal review process.

**Instructions for Submission and Proposal Review Process Timeline**

Proposals should be provided in Word or PDF format, submitted on 8½ x 11 inch paper with 1 inch borders and Times New Roman font size 12. It is advised that proposers limit the total length of each proposal (including optional appendix) to a maximum of 200 pages. Proposers choosing to attach an optional appendix should ensure that it is highly organized with a table of contents and any reference to the appendix in the main body of the text should be clearly cross referenced. As noted above, the QIAT will have a dialogue with proposers and will request additional explanation if required. Proposals should be written to the primary audience of the QIAT, and the Faster Payments and Secure Payments Task Forces.

All inquiries regarding the proposal template and submission process should be directed to: FasterPaymentsTaskForce@chi.frb.org.

Instructions providing details on where proposals are to be submitted will be provided in a separate communication prior to the submission window opening on April 1.

The following table outlines the proposal assessment process and timeline. Key dates for proposers are indicated in bold type.
### Timeline and key dates

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Proposers to submit proposals</td>
</tr>
<tr>
<td></td>
<td>Proposal submission window open from 9am ET April 1, 2016 to 5pm ET April 15, 2016</td>
</tr>
<tr>
<td>2.</td>
<td>Draft 1 of QIAT assessment and discovery period between QIAT and proposers</td>
</tr>
<tr>
<td></td>
<td>Conducted from April 15, 2016 to July 7, 2016</td>
</tr>
<tr>
<td>3.</td>
<td>Proposers to provide written response to QIAT assessment or notification of decision to withdraw</td>
</tr>
<tr>
<td></td>
<td>Due no later than 5pm ET August 9, 2016</td>
</tr>
<tr>
<td>4.</td>
<td>Task Force review of proposal assessments commentary period</td>
</tr>
<tr>
<td></td>
<td>Conducted from August 10, 2016 to October 4, 2016</td>
</tr>
<tr>
<td>5.</td>
<td>Proposer to submit final revised proposal, and written response to Task Force comments or notification of decision to withdraw prior to public release</td>
</tr>
<tr>
<td></td>
<td>End-October 2016</td>
</tr>
<tr>
<td>6.</td>
<td>Final QIAT assessment provided to proposers</td>
</tr>
<tr>
<td></td>
<td>November 2016</td>
</tr>
<tr>
<td>7.</td>
<td>QIAT report of all fully assessed proposals including Task Force commentary and proposer responses</td>
</tr>
<tr>
<td></td>
<td>November 29, 2016</td>
</tr>
</tbody>
</table>

### Legal Considerations

All submissions are at the discretion of the proposer or proposers, and are subject to the terms outlined in the Faster Payment Task Force Proposal template and the terms of the Faster Payment Task Force Participation Agreement. Please limit your responses to matters reasonably necessary to the creation, development, and deployment of your proposed solution.

All Faster Payments Task Force Members who contribute to a proposal are considered to be proposers, and a proposal should identify all Task Force Members who have contributed. If a Secure Payments Task Force Member contributes to a proposal, that Secure Payments Task Force Member should sign a Faster Payments Task Force Agreement and be included as a proposer.

Proposers should identify the proprietary intellectual property contained in its proposal. This identification should include whether the proposer owns the intellectual property or whether the intellectual property has been licensed or will require licensing from another entity (in the event the proposer has licensed technology from another entity), the terms the proposer will license its intellectual property under and the terms of license(s) required from other entities. These terms could include FRAND, royalty bearing, or non-royalty bearing, by way of example. Such disclosures should be made under Part C, sub-section 5 “Legal Framework” (justification for L.5, Intellectual property criterion), which asks whether a proposal has undertaken or will undertake a due diligence review for the subject matter disclosed by a proposal, and an approach to resolve or manage any risks that arise from third-party intellectual property rights implicated by a proposal. In making these disclosures, proposers should identify any technology that is disclosed by its proposal, which the proposer has knowledge potentially infringes or
misappropriates the intellectual property of any other entity or person, and the basis on which the proposer has this knowledge.

If a proposer does not currently have access to Federal Reserve System (FRS) services referenced in a proposal or the proposal relies upon new or the expansion of existing FRS services, the proposal must clearly acknowledge that the FRS has not in any way committed to provide the services to the proposer.

Proposers are reminded of their obligations to comply with applicable anti-trust laws in preparing their proposals. Proposers should not share confidential or proprietary information in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report. While all information contained in a proposal is ultimately at the discretion of the proposer(s), if a proposer inadvertently includes confidential or proprietary information in a proposal, the proposer should immediately notify the QIAT.
TMC PROPOSAL FOR THE FASTER PAYMENTS TASK FORCE

EXECUTIVE SUMMARY

Provide a high-level description of what the solution does from end to end. In providing the description, proposers should highlight the main improvements the solution achieves over existing payment systems; that is, they should define the gaps in the current payment systems that the solution intends to address and what features of the solution address these gaps.

Please also include the definition of the solution’s baseline features, and a description of the direction of the payment flow (for example, whether, the payment is “pushed” by the payer to the payee, the payee’s provider “pulls” the payment out of the payer’s account, or both).

Money Modules™ (MM) is an electronic currency designed to replace most worldwide financial transaction processes. It allows accurate monitoring of aggregate payment flows, provides remarkable flexibility for adapting innovation, provides robust security, and conforms to the principles of ISO 20022 by using XML tagged fields for storage and movement of funds.

MM is a collection of standardized software and data modules and the electronic wallets that host them. Central banks issue the currency and other government agencies regulate electronic wallets and the creation and implementation of new modules. Different governments may share legal modules governing the currency for faster flow of payments or each government may require modules for MM currency hosted or circulating in their jurisdiction.

The fundamental Money Module™ (FMM) is a block chain and each record within the chain contains the issuer, a unique transaction identification number, the issuer’s public electronic signature, the date issued, the fiat currency type, date issued, and amount. As it moves from central bank to commercial bank, to retail bank each recipient imbeds the same information in the block chain. Each new financial institution recipient likely will break the currency down into smaller amounts but the block chain always shows the existent module’s ancestry. The block chain conforms to the ISO 20022 tagged structure, however the actual tags need creation by a technical standards committee and international recognition of the structure. The sum of each derived currency issued to the public will equal the
original issued amount and a government agency or a central bank may query circulating currency to determine the fact. Once financial institutions (FI) issue the currency to their customers and it circulates, each new transaction contains the ancestry and transaction history within the FMM.

Access to read and write to the FMM is only allowed by the security module which does so upon instruction from an authorized electronic wallet (EW) or other source approved by the issuing central bank. Any other access immediately revokes the signature of the central bank and renders the currency useless.

Other critical modules include a transmission module, a reception module, a legal controller module, an insurance module, and a broadcast response module. For the currency to succeed and meet the effectiveness criteria it must have human processes that allow new commercial modules that enhance end user convenience such as accounting modules, seller discount data, EDI data, or other elements that can be stripped later by authorized wallets as configured by EW users. Governments may wish to add their own tax modules that either track taxable transactions or strip value and transmit it to the taxing agency dictated by a configurable setting or a mandatory requirement controlled by the legal module.

Electronic wallets host, transmit, and receive the currency. These devices have attributes and elements appropriate for various types of users such as central banks, financial institutions, commercial payers, consumers, or any self-identified group. Defined human processes approve new proprietary or public domain functions for authorized wallets. International government committees approve functions for wallets used in cross border transactions; appropriate local government agencies approve new wallets used in specific geographic areas. All wallets must recognize their jurisdiction for a payment by a standard call received by the governing jurisdiction before becoming operational. Mobile wallets moving across jurisdictions must determine if new jurisdictional rules apply by making a new call out to the governing jurisdiction based on current geographical position relative to the last transaction.

This template requires the proposer to describe the mechanics of a transaction with obsolete terms such as “push” or “pull” transactions. The architecture of MM...
consists of three separate phases: issuance, circulation, and redemption. Each phase uses the mechanics of payment vs demand and gross real time payment systems, but circulating currency does not need an intermediary such as a financial institution or a commercial payment firm to complete a payment. The consequence of eliminating intermediaries is a faster, cheaper, and safer payment system which is easily adoptable worldwide. Although circulating MM does not need intermediaries, payment firms and financial institutions will play a major role in creating innovative solutions to meet payment needs not just to recreate current deferred netting system or payment token features but to improve the ability of payers and payees to configure their payment applications, thus enhancing their payment positions, and increasing the time MM circulate before redemption.

Value from any MM can be pooled with other MM values in an electronic wallet (EW) and combined with original FMM issuance elements for new transactions as long as the value is equal to or less than the original issuance amount. The EW keeps track of funds used from an original issuance amount and ensures that value used does not exceed value issued. Any attempt to exceed the original issued value causes revocation of the MM. Payers can make payments using small residual values with separate MMs.

Firms and individuals redeem MM by submitting MM values to financial institutions which use gross real time payment systems to convert aggregate values in EW to the local fiat currency either as cash or a value held in a conventional account. Redemption removes all FMM data from an EW and moves them to government archival storage units or destroys the data archiving only the original FMM ancestry.

The choices governments make about access and retention of MM data affect consumer usage because payer privacy concerns govern usage of payment systems. Increasing module size and complexity also increases the actual time for transactions although in most cases delays will be measured in microseconds. It is possible to express proposed legislation for use in MM legal modules as the number of branch statements plus the number of compare statements multiplied by time for processing for average or specific devices equals the delay to transaction finalization.
Part A of this proposal contains precise details of the three phases of MM (issuance, circulation, and redemption or ICR) and the interactions between MM and EW. ES diagrams 1 and 2 show only a high level view of these processes.

**ES Diagram 1: MM Issuance, Circulation, and Redemption**

Much of the optional functionality will reside as logic in the EW however each FMM will have an associated security function that revokes the signature of the issuing central bank if tampering or attempts to tamper with any element of FMM is detected. The Central Bank Module (CBM) contains all functions as dictated by law but in my opinion contains a minimum of the following:

- Response to aggregate Measurement Requests
- Revocation
- New MM creation (equal or less than current value)
ES Diagram 2: EW and MM Structure

- Government Required Functions
- FMM & Protection logic
- Payment Industry Features
- Electronic Wallet
- Issuer Seal
- Central Bank I/O
- Break Out Logic
- Block Chain
What does MM replace that currently makes US payment systems slow, expensive, and risky. MM provides the following advantages over current US payment systems:

- Gives new central bank controls over money supply
- Removes commercial or FI intermediaries between private transactions
- Provides an ability for private insurance companies to protect payers and payees effectively and efficiently, thus removing the requirements for government regulation
- Lowers the risks inherent with time differentials between clearing and settlement
- Creates a clear and authorized infrastructure for cross border payments
- Creates a method for mitigating the effects of systemic failure of current systems
- Increases security
- Reduces credit, legal, liquidity, vulnerabilities
- Allows new legal requirements an immediate avenue for implementation
- Reduces demand for cash or checks
- Provides a method for precise legal review of private transactions without compromising expected privacy
- Provides accommodations for future requirements
- Allows greatly enhanced measurement of aggregate payment dynamics

The details of this solution follow. This solution would not be possible in most countries because central banks and government authorities do not allow critical inspection of monetary dynamics much less criticism or thoughts on enhancement of current payment systems. The Federal Reserve Banks openly embraced public criticism setting an example for a process based on openness and consensus to improve a broken system. To say I commend for this effort is so understated it is ridiculous, but it is the best I can do.
USE CASE COVERAGE

Supported Use Case Coverage Summary

In the table below, identify (by entering a “Y” or an “N”) which use cases the solution intends to support for payments within the United States and a description of the specific type of payments the solution supports (example provided in the table below). Also indicate for each use case whether the solution offers cross-border functionality. Blanks will be assumed as “N”.

<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>Example: Business to Person (B2P)</td>
<td>Y</td>
<td>N</td>
<td>The solution assists business and governments to make payments. Payments supported include: social security, government pensions and employee wages.</td>
<td>Note that the solution targets regular income payments to individuals. It would not be suitable for all types of business-to-person payments, such as ad hoc legal settlement payments or medical insurance claims.</td>
</tr>
<tr>
<td>Business to Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>The solution provides businesses exact control over payment by providing commercial firms a platform to host custom built applications hosted by the electronic wallet (EW).</td>
<td>For example, large value payments can be scheduled and authorized by employees on a routine basis without the loss of control such as dual participation if an employee (part of the duo) goes on vacation.</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>The solution provides a platform for payments by retail establishments and corporate back offices to private persons. Customized EWs provide accurate and precise accounting for smaller value payments.</td>
<td>For example, mail-in rebate payments can easily be tracked to determine if the consumer met the requirements of the offer. Employee fraud will be extraordinarily difficult to perpetuate with the correct programming of the EW.</td>
</tr>
</tbody>
</table>
## 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>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>The solution provides the same ability to pay businesses as electronic bill presentment and payment offered by modern FI.</td>
<td>The proposed solution eliminates postal, ACH, and administrative costs incurred by FI or payers. Costs for owning and operating EW are minimal.</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>The solution provides small or large value traceable payments and allows persons to account for any payment with methods they chose.</td>
<td>Easily replaces checks or cash as typical payment methods for these types of transactions.</td>
</tr>
</tbody>
</table>
Cross-border Use Case Coverage (If Applicable)

For those use cases supporting cross-border, provide the jurisdictions and systems with which the solution interoperates in the table below.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>Any government party to standards propagated by international standard bodies.</td>
<td>EW makes call to government portals on initiation of EW functions or on detecting change of legal jurisdiction by use of GPS.</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Any government party to standards propagated by international standard bodies</td>
<td></td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Any government party to standards propagated by international standard bodies</td>
<td></td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Any government party to standards propagated by international standard bodies</td>
<td></td>
</tr>
</tbody>
</table>
Proposal Assumptions (Optional)

Proposers may choose to provide a list of assumptions used in the creation of their proposal. Assumptions should be limited to those that are unique to the proposal and cannot be adequately addressed elsewhere in the document. The QIAT will take into account any assumptions listed in making their assessment of the proposal.

For example, as noted in the “Practical and Conceptual Considerations” section of the Faster Payments Effectiveness Criteria, many of the criteria require the solution proposer to describe various elements of the payment system rules for the proposed solution. In a multi-operator environment, it is possible that a single entity will be given rule-making authority by multiple operators that desire a standardized ruleset. Solution proposers planning to pursue such an approach may list this rule-making authority as an assumption. However, it should be noted that for the purposes of meeting the Effectiveness Criteria related to “Legal Framework”, proposers should coordinate with either the designated rule maker or articulate preferences for rules when preparing their solution proposal, even though rules may not be finalized until later.

This solution requires far less assumptions than current payment systems that require intermediaries for all transactions except cash transactions. The solution requires

- Use of a tagged data protocol (such as ISO 20022),
- Authorizing bodies for proposed EW functions,
- Acceptance by central banks
- Clear and transparent requirements for government inspection of private transactions
- Independent governance of payment flows by skilled payment system professionals that understand the macro economic effects of policy implementation
- Creation of a permanent, secure, payment data archive of spent FMM for use in the aggregate by economic researchers and for use by fraud investigators or law enforcement officials looking at specific transaction history.
- Accessibility of wireless networks to create peer to peer topologies for circulating cyber currencies
- Insurance firms willing to create rates for varying values hosted in EWs
- Public trust
Part A of the solution requires a description of only the circulating currency and leaves no place for description of issuance of electronic currency nor a redemption or retirement of active or spent currency. However, without those associated payment streams the proposed solution cannot exist.

There is not enough space to describe all the technical details of the missing payment flows, however, a brief description of these important components follow.

ES Diagram 1 (p.12 in the executive summary) depicts all three payment flows, issuance, circulation, and redemption (ICR). The issuance cycle allows a central bank to issue large value FMM to correspondent financial institutions (FI), which in turn issue subsets of these large value FMM to the public or retail FI. The breakout of smaller values from larger values works the same as described in Part A of the solution, however there are other elements of issuance that will make this solution receive ubiquitous demand.

A central bank has the ability to issue the currency at a discounted price from the actual value of the issuance. This feature allows central bank to implement policy based on the discounted rate of issuance. For example, if the central bank decides that inflation of prices is rising too quickly, they can increase the discount rate for issued FMM and make it a fee instead of a discount rate, discouraging correspondent FI from purchasing more of the currency or passing the costs to the public thus reducing the currency in circulation. Of course traditional methods for payment still exist such as gross real time payments or deferred netting payments, however it is expected that most retail purchases using discretionary funds will be from MM which will slow as the price of the currency rises prompting retailers to keep prices the same or lower them to attract payers.

The other aspect of issuance is the central bank receives real currency for virtual currency, in effect central banks receive an interest fee loan that may never have to be repaid because payees may always choose to spend the circulating currency and not redeem it for its face value. These funds can therefore exist either partially or fully as part of the reserves required by
correspondent FI. This feature allows central banks to also restrict or increase money in circulation by changing the ratio of reserve funds from purchased currency funds or the RF/CF ratio.

Central banks can also control the amount of currency in circulation by creating incentives for MM holders to redeem their currency instead of holding FMM in EW. Typically, however FMM will be redeemed for cash or immediate transfer of the value into standard accounts for no fee or incentive payment.

Payers can also expend all the value from FMM (in a process described in part A of this solution) and the resulting no value FMM will be sent to a depositary for use by economic researchers or criminal investigators. It will contain a history of all expenditures used during its existence.

Not all solution assumptions need to be met, however the absence of assumed requirements affects the conformity of the solution to the effectiveness criteria.
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

Part A is composed of three sub-sections:

- Section 1 focuses on the broad solution, looking across the eight stages of the payment lifecycle.
- Section 2 focuses on the details of the solution by describing the solution’s supported use cases across the eight stages of the payment lifecycle.
- Section 3 provides a summary table of whether the Effectiveness Criteria are addressed by each supported use case.

Part A, Section 1: Solution Description

In this section, the proposer should describe what the solution does at each of the eight stages of the end-to-end payments process (lifecycle stages). These eight stages compose the numbered sub-sections, below. For some solutions, the stages of the lifecycle may not occur as separate steps – they may occur simultaneously. The steps also may not occur in the order presented below (for example, receipt may be before or after settlement). Proposers may therefore choose to combine some steps in their description, instead of addressing all eight stages separately, or to re-order the sub-sections below as required to best describe their solution.

Proposers should include flow diagrams of the messaging and payment flows and the roles of stakeholders (end users, technology providers, processors, including the proposer(s) of the solution) through the eight lifecycle stages of the solution. In completing this section, proposers

3 Definitions of some of the terms used below are either defined in the Effectiveness Criteria or in the Glossary of Terms.
should refer to the Effectiveness Criteria that relate to each of the eight stages (as noted in the instructions for each sub-section).

Any additional description or materials to support the explanation of the solution may be provided as an optional Appendix.

1. **Initiation**

> Describe how and when end users can initiate and/or receive payments, and to which accounts payments can be initiated and received. Indicate whether there are any pre-requisites or limitations to initiating or receiving a payment (e.g., enrollment,) and, if applicable, how those pre-requisites are met. Include whether the solution provides the ability to make multi-currency and/or cross-border payments, and describe the process for foreign currency conversion. Indicate for each use case, the channels, devices and platforms through which end users can access and use the solution (e.g., remote with a mobile device, online, etc.). Describe any consumer protections; for example, whether and at what point there would be disclosure of end-user fees.

In this sub-section the proposer should also describe the capability and steps required for contextual data to be transferred or associated with the payment. Also describe any security features associated with initiation, including protecting sensitive information. Proposers should include flow diagrams of the messaging and payment flows through the end-to-end payment process of their solution in this section.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to initiation: U.1 (Accessibility); U.2 (Usability); U.3 (Predictability); U.4 (Contextual data capability); U.5 (Cross-border functionality); U.6 (Applicability to multiple use cases); E.4 (Payment format standards); S.7 (Security controls); S.9 (End-user data protection).

Money Modules (MM) are a combination of the Fundamental Money Module (FMM), restricted access software and an electronic wallet (EW); effectively the solution is a combination of secure data and secure algorithms. Initiation of payments comes from the man/machine interface provided by firms and customized by users. Payers can program EW to initiate payments on any criteria the man/machine interface provides, such as time, receipt of funds, total value hosted by the EW less expected payments, prioritized payments based on user choice, expected demands from other EW (or other payment methods), or any scenario users may require. Payments can be pushed or pulled from EW, however, all initiation of payments will follow basic logic before transfer of funds. Diagram 1 shows the logic of all payment initiation.
Diagram 1: MM Initiation Logic
Prior to the execution of initiation logic, payers may configure their EW to their own requirements. Payers may allow payee EW to pull funds or they may simply push them at the designated time, either immediately or after satisfying other criteria for payment. Operators of corporate EW can implement all types of security procedures that become criteria for payment. Table 1 shows the use cases and potential methods for initiation.
# Table 1: Potential Use Cases for triggering Payment Initiation

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Example Features</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Business to Business (B2B)| - Two Person control over payment configuration  
- Capability to increase security for values exceeding Ceilings  
- Unlimited Number of concurrent payments  
- Use of Foreign FMM for payment to payee residing in the same foreign location  
- Allowance for payment on receipt of invoice either immediately or after the elapse of time  
- Duplication of corporate treasury controls in the EW  
- Use of insurance modules to mitigate risk | Commercial firms will create EW modules to meet the specifications of businesses. Some of these modules such as insurance modules will be standard interfaces that will fit in the EW but not configurable by the businesses, however, most modules will be configurable by the EW owner and provide great flexibility over the security, timing, and cost of payments. |
| Business to Person (B2P)  | - Limits to value without executive level approval  
- Same abilities as B2B payments | Can originate payments from same EW as B2B                                                                                                               |
| Person to Business (P2B)  | - Initiation with same functions and options as B2B  
- Ability to allow Business to pull payments from EW |                                                                                                                                                           |
| Person to Person (P2P)    | - All functions and options previously described  
- Flexibility to add features demanded by payers and payees such as programmatically determining tax liability and submitting simultaneous tax payment and P2P payment  
- Low cost insurance makes Regulation E obsolete |                                                                                                                                                           |

Since central banks control the FMM issued, conversion costs (if any) occur during redemption and not during circulation. Users can negotiate a conversion based not on the current conversion rate but on the negotiated value of the purchase. For example, if a payer from the US negotiates an amount of dollars with a payee from the European Union the resulting FMM delivered to the foreign payee contains the negotiated value in dollars which the payee can convert to euros or
reuse as a dollar denominated value. Because conversions of value only occur during redemption, standard bodies creating the format for the FMM, may wish to consider the reasonability of only expressing value as the number of the lowest possible value for the currency. For example, In the US, the Federal Reserve issues FMM values expressed as number of cents. Representing currency as a floating point expression allows outside manipulation of currency value by using differing implementations for floating point value in EW applications.

The EW functions do not create FMM for transfer, EW applications make a standard call to a module created by central banks and coupled with the FMM to create the FMM for transfer and residual FMM retained within the payer EW. The module depicted in ES Diagram 2 as Break Out Logic (BOLMM) receives arguments as designated by standards committees to select an FMM or FMMs that are equal to or greater than the value or values needed for payment, create new FMM based on the block chain, move the requested value for transfer, and update the resident FMM value with the residual value and payment details. Any attempt to manipulate the BOLMM or the FMM outside of the standard calls will cause immediate revocation of the money module, although other MM resident in the same EW will be unaffected by such tampering. If insurance modules are not resident in the EW than the BOLMM if operational transfers the revoked FMM to the central bank archives flagged as a revoked money module. If insurance modules exist and can operate then the BOLMM places the revoked FMM on a special transport module which will work with standard logic designed by the insurance industry. Standards committees also will determine how the EW will function if the BOLMM of a MM does not operate and there are no resident insurance modules, although considerations for safe transport to the central bank archives or the revocation of the EW seal are reasonable in such instances.

FI and users may wish to use the transport mechanisms resident in BOLMM, and MM but not use an EW as a conduit for BOLMM and MM. There are no barriers preventing MM users to initiate payment from or receive payment from an entity other than EW. FI or other users can receive MM and immediately redeem them without storing them in an EW. Additionally, users may request payment from an account and allow the entity that holds funds to initiate a transfer to an EW. Some transactions may only use BOLMM and MM as a transport mechanism and immediate issuance and redemption occur without the use of EW thus creating a non-circulating transaction. Spent FMM from such non-circulating transactions still become residents of the central bank archives.

Contextual data preservation is a function of the EW. It provides a new resource for marketing, research, and the right of user anonymity as prescribed by law. Businesses, governments, or users place contextual data within data stores resident on their EW or any data storage facility. Users can accept or decline the values for storage on their EW.
Security of MM begins with the BOLMM and seal protections within the central bank electronic signature. Tamper resistance technology cannot remain static; it evolves with attacking methods or becomes irrelevant. Central banks write the BOLMM logic and retire older and revoked MM. Central banks must retain public trust by providing the currency with nominal revocation logic appropriate for current and past threats. The EW provides whatever intrusion detection or user validation functions users demand. Properly configured EW will allow central banks to replace MM with updated BOLMM logic (FMM cannot change without user approval). Users present revoked MM to their insurers or to their central bank and replacement of value remains a function of regulations and law.

Accessibility of MM is governed by central banks.

Usability of MM is governed by providers of EW. I make the assumption that commercial firms will profit providing enhanced EW functions.

Revocation of MM or counterfeit MM will be extremely rare. Storage of MM outside of EW will be within FI. Government certifies EW functionality and EW need to update their legal modules when new or when in a new legal jurisdiction.

EW can store and index contextual data as required by users.

Governments determine requirements for cross-border functionality; this solution will work across borders if governments agree to standards required by this solution.

MM functions well regardless of its user requirements.

MM requires standards development. Many of the tagged fields used in ISO 20022 are appropriate for MM storage, transfer, and conversion. However, new fields such as velocity, acceleration, or opt-out will be needed for commercial firms to provide new functions for their users.

MM provides nominal security.

Users pay for the security they require. EW controls access and prevents intrusion. Insurance firms provide assurance that monetary value contained within EW will be replaced if users meet the terms of their policies. The price for security and insurance policies increase with stored value in EW and the level of anonymity required by users.

Users can easily place software from consumer protection advocates or other entities in EW. Each module placed in the queue of logic required by the user or by law slows down initiation of payment and thus increases impatience with the lapse of time for payment finality. Note although transfer of payment by peer-to-peer technology is almost instantaneous, user customization will delay the initiation of payment.
2. **Authentication**

Describe how the identity of an end user and provider would be authenticated. Describe any security features associated with authentication, including protecting sensitive information.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to authentication: U.2 (Usability); U.3 (Predictability); S.7 (Security controls); S.9 (End-user data protection); S.10 (End-user/provider authentication).

The solution provides several levels of protection to end users and providers (payers and payees) and allows delay of finalization of payment until the payer accepts all conditions of payment. Once the payer accepts all conditions of payment and value transfers as a MM to a payee device or account, the payment is final. Reversal of payment only occurs if a court orders such a reversal or the payee agrees to the reversal. Reversals initiate as described above in A.1.

There are two types of authentication required by this solution. The MM, specifically the BOLMM must detect if tampering of the associated value of the FMM occurred and revoke the central bank seal if tampering occurred. The security provided in volume 2 of the Europay, MasterCard, Visa standards are adequate, however, elliptical curve cryptography (ECC) instead of public key interchange (PKI) may be a more appropriate foundation for validation of the FMM and central bank seal used in a worldwide circulating electronic currency. Regardless, this author wants to encourage further discussion of asynchronous encryption and electronic signatures appropriate for architecture of circulating electronic currency.

The BOLMM authenticates the EW; the EW authenticates the MM. There are multiple approaches for this fundamental function. The function of mutual authentication evolves over time depending on threat and risk to value. The ratio of risk to value governs the price of the EW, but cannot govern the price of the MM. Central banks must absorb costs associated with the maintenance, production, and immediate distribution of BOLMM to all circulating MM. Political or pluralistic forces thus govern costs associated with BOLMM although central banks must pay those costs as required. With luck, common sense will prevail.

Firms provide authentication modules to the EW, and users adapt those modules as they see fit. For example, if I’m king of the hill and as rich as Croesus, then I may purchase an EW with all the trimmings, however if I’m one of the 99%, I may purchase functions appropriate for my sociological function, or for the risks perceived as a consumer, or acting on behalf of an

---

4 EMV; *Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management*; (Version 4.3, November 2011)
organization. Since actual perceived risks govern costs associated with EW, market forces provide adequate security for authentication and not the solution itself. If users want insurance firms to protect value, then insurance firms will want to provide modules resident in EW to govern the risk to value ratio. Market forces will create innovators to sell authentication solutions to insurance firms and EW providers. Government creates independent bodies composed of knowledgeable individuals to certify authentication solutions within a reasonable time frame (under 3 weeks). Independent certification bodies operate with funds received from application fees. Fees for certifying authentication modules must be proportionate to applicant resources.

Experts considering authentication approaches in either the MM or the EW (i.e. for the value contained within the FMM or access to that value) need a framework for their considerations. That framework needs development from central banks using consensus among technical experts for the method to certify new authentication modules. Once the framework for certification exists, the independent certification agencies use the framework to approve or disapprove authentication designs. Central banks will weigh costs and non-economic factors to determine the need for a permanent body of revolving payment system architects continuously monitoring the effectiveness of the authentication framework and to propagate changes to certifying bodies as attacks change.

The critical component of authentication is that is flexible and allows multiple methods by different firms or individuals. At a minimum the BOLMM protects MM from tampering and EW logic should detect counterfeit MM. The MM solution allows query logic authored by the central bank issuing the MM. For example, an EW needs receipt instantaneously to a validation request of unique transaction number contained in the FMM and its check sum or cyclical redundancy count or a random verification method indexed by the last transaction ID. Another function of the EW may be central bank validation of the central bank seal contained in the MM. A logic module contained within the MM may also directly establish a circuit with a central bank hosting validation and other functions such as response to central bank requests on aggregate MM geographical locations. Tight, flexible, and multiple authentication methods allow public confidence in aggregate measurements methods imbedded in circulating currency. Misuse by government of private financial data will cause public rejection of digital currency. It is vital that currency users have the capability to turn off central bank monitoring with the consequential associated risks such as insurers decline of coverage. Users determine their own risks and mediation of those risks but there is a likely predictable ratio between value and authentication approach. This value/authentication ratio (V/A) affects pre-initiation time; speed counts in lower value transactions whereas consensus of payers and security controls, not timing considerations, control the issuance, circulation, and redemption of higher value MM.

U.2 (Usability): Firms and individuals control the usability of EW. Functions within the MM increase time for validation and authentication of currency; too many government functions within the BOLMM will delay initiation of funds transfer.
U.3 (Predictability); BOLMM may change in an instant dictated by central bank action. Value can only change when authorized by EW or other authorized initiating source. Users have switch to turn off central bank aggregate monitoring. Insurance rates govern user vulnerability to financial loss.

S.7 (Security controls); Configurable.

S.9 (End-user data protection); Configurable

S.10 (End-user/provider authentication). Configurable.

3. Payer Authorization

Detail how and when payments would be authorized by the payer. If the solution allows pre-authorization, detail the process for establishing pre-authorization, and the process and timeframes within which a payer can revoke pre-authorization or change relevant parameters for pre-authorization.

Payers authorize payment by configuring their EW to their requirements. Payers can select the timeframe for payment or allow payees to control debits from payer EW. Payers revoke payment on demand until the payment moves to payees. All payer parameters may be changed prior to payment; MM move in real time.

U.2 (Usability); Users determine the controls for their EW and the amount of time needed to authorize a payment. Payers determine their controls based on choices offered by commercial firms, consumer protection agencies, or other entities. Authentication modules may run in series and will allow users to make prepayment procedures arduous or non-existent, or somewhere between two extremes.

U.3 (Predictability); Once payers authorize payment, MM transfer to a new platform (including EW) become final. The payee becomes potential payer although the history of the transaction exists in the FMM unless payers turned off central bank monitoring functions. If users masked the transaction from public scrutiny the FMM contains only the date, time, and value of MM; users details such as the EW unique identifier, location, or other pertinent details do not exist.

S.2 (Payer authorization); Payers configure their own authorization procedures using software hosted in the EW. FI or large value payers create procedures for transfer of MM to payees.

S.7 (Security controls); Configurable

S.9 (End-user data protection; Configurable
4. Approval by the Payer’s Provider

Detail the process for approval of the payer’s provider (depository institution or regulated non-bank account provider), including how long approval will take from the point of completion of payment initiation, and the point at which the payment becomes final and irrevocable. Describe the consumer protections around payer approval and the assurance of good funds. Also describe any security features associated with approval, including protecting sensitive information, and detecting and limiting unauthorized, fraudulent or erroneous payments.

Payers do not need approval to transfer MM to payees. Payers or payees may send or receive details of proposed payments. Technical standard committees need to propose standards for transmission of proposed sales; once again ISO 20022 works well as template for such a standard. The pre-sale messaging protocol provides a reference to those wishing to scrutinize transactions to determine the exact context of an exchange. Movement of MM can be tied to final acceptance of the conditions of a sale.

Intermediary FI issuing MM to the public may wish to provide software to payer EW and may wish to couple their commercial offerings with the guarantee of insurance firms accepted by central banks issuing the MM. Payers do not need to accept services offered by financial firms to move payment, and do not need the presence of pre-sale messages. Payers and payees tailor the anonymity of their MM movement as allowed by law. Redeeming FI can refuse MM because of anomalies existent in the seal, FMM, or BOLMM, but must record the refusal in public archives. FI refusing to redeem MM must base their refusal on standards propagated by a cooperating international community of central banks and cannot base refusal on any anonymous sections contained within FMM.

FI redemption is instantaneous. EW transmits MM to FI, FI determine the authenticity of the MM, FI move value of redeemed MM to originating holder account of choice. Recording of redemptions in the central bank archive becomes a matter of law. Funds flow from redeeming bank to MM user account by gross real time payment.

Payment is final when an EW or FI receive MM from an authorized source and confirm the authenticity of value. The payment is final when MM become resident in an EW or redeemed by an FI. If communications fail, and the MM does not move to the intended peer, then the payment is not final. If an FI or EW do not affix the MM to storage because MM failed validation, then notification of the non-payment event becomes broadcast as required by law and the details of the refused MM become public record housed in central bank archives. MM authentication should not take longer than 400 milliseconds, however absurd data

---

5 The completion of payment initiation is defined as just following payer authorization to their provider, or just following confirmation by the payer’s provider that pre-authorization exists for a given payment.
received because of faulty communications can be refused without notification to central bank archives. EW logic to determine the difference between absurd data and MM validation failure needs government by central bank experts. However, discovery of revoked central bank signatures within MM always requires central bank review.

Circulating MM may circulate without review from issuers for many years. Properly stored MM may respond to central bank queries and conform to the broadcast government rules for a specific region. MM may move outside review of government and later redeemed if validated and not refused because of anonymous circulating events. Governments likely will legislate anonymity of transactions based on value; global acceptance and use of MM likely will occur based on anonymity capability. The dialectic between public need for anonymous transactions and government need for scrutiny of transactions cannot be resolved within the mechanics of the BOLMM. Governments control the functions of EW and depositories of MM, but the MM functions require the minimum logic necessary for validation within the prescribed 400 milliseconds.

S.3 (Payment finality); Payment is final after payee software validates MM within 400 milliseconds.

S.7 (Security controls); EW logic and payer choice controls security.

S.9 (End-user data protection); Payer and payee negotiate terms and context of payment prior to movement of MM. Payers and payees enact security procedures as they deem fit.

F.1 (Fast approval); 400 milliseconds.

F.5 (Prompt visibility of payment status). 400 milliseconds.

5. Clearing

Detail the process for the exchange of relevant payment information between a payer’s and a payee’s providers (depository institution or regulated non-bank account provider), including payment format (message) standards utilized, the necessary communication processes, and how long the clearing process will take from the point of completion of payment initiation. Also describe any security features associated with approval, including protecting sensitive information.

MM move based on payer and payee negotiations; the electronic negotiation between EW is the substitute for clearing operations. Since no authorization by FI is required, clearing functions become obsolete. Outside parties to a particular transaction may have access to negotiation details as configured by payers and payees, however MM move from the payer EW or FI to the payee EW or FI electronically propagated by sound waves or light waves depending on the users...
desired choice of transmission of MM. Payees may wish to validate MM before receipt and can request and receive confirmation by the issuing central bank (or its agent) of the authenticity of MM. Insurance companies likely will require authentication of proposed MM and its movement to payees or require increased premiums for coverage of MM value.

E.4 (Payment format standards); MM, BOLMM, FMM, and EW will have data formats standards conforming to ISO 20022 XML tags⁶.

S.7 (Security controls); Configurable based on payer and payee desire for anonymity or desire for mitigation of risk.

S.9 (End-user data protection); Configurable based on payer and payee desire for anonymity or desire for mitigation of risk.

F.2 (Fast clearing). Validation of MM by payers or nominated payees occurs from central bank points of presence. Insufficient bandwidth or processing capability offered to EW or FI affects the speed of pre-initiation events. Transactions will occur without validation of MM at the payee’s risk. Controls embedded in EW and MM provide off-line validation and therefore sufficient risk mediation for most small value transactions.

6. Receipt

Describe how the approach would enable availability of funds (and contextual data, as appropriate) to the payee and the time this will take from the completion of payment initiation. Detail when and how the approach will make the payment status visible to the payer and payee (for example, visibility to the payer and payee that the payment has been approved, visibility to the payer and payee that the funds have been received in the payee’s account for use, etc.). Describe any security features associated with approval, including protecting sensitive information and mechanisms to block funds availability if an unauthorized, fraudulent, or erroneous payment is reasonably identified by the payer’s provider (depository institution or regulated non-bank account provider) prior to payment finality.

After transmission time and 400 milliseconds validation time MM are immediately available to the payee. Prior to receipt payees may request additional authentication of proposed payment from a central bank or its agent from a point of presence in a specific location. Retailers or other payees accepting payment at various velocities may wish to pay a provider to give efficient and...
timely access to central bank point of presence for proposed MM validation. Data payees or payees require, apart from MM, may follow or precede MM as dictated by user requirements, however it is recommended strict data protocols conforming to XML tagged formats be propagated by central banks for the transmission, receipt, and storage of contextual data related to unique transaction identifiers embedded in FMM.

Payee EW likely will have configurations that allow transmission of confirmation of MM receipt, however such courtesies do not affect the immediate availability of MM received and validated by payee EW. Payees can create functional queues and immediately transfer any received payment to another EW or FI account or use as a payment to another payee.

EW providers will sell standard functions for EW users including showing payment history, aggregate value, errors, proposed payments, or contextual data related to specific MM. EW providers design how such data is transmitted to EW users however central banks propagate standards for transferring value and contextual data from EW to EW.

If received MM fail validation, then the payment is void and the receiving EW immediately transfers the MM to the central bank archive and may send a copy to insurance firms designated by the payer EW. The payee may send a message to the payer indicating the status of the failed payment, however the only requirement is the MM moves immediately as a failed MM to the issuing central bank archive. Central banks will develop policies for notifying payers on MM failing validation. However, if payers do not configure their EW to notify regulating agencies of user contact information associated with unique EW identifying numbers (EWID) notification only goes to the EW address without identifying the offending payer. Central banks may consider tracking consecutive failed validations from a single EW and revoking the seal resident within the EW forcing the user to go to a FI or an insurance agency to restore residual value on the offending EW.

Attackers will need to prevent test counterfeit MM from leaving a payee EW until they can determine acceptance by payee EW. One way to create a test for counterfeit MM transfer is to create an unauthorized EW. The attacker can use the receipt of counterfeit data to try to tamper further with MM resident in counterfeit EW. Such hacks include changing the EWID or FMM transaction IDs. Normally such tampering causes immediate revocation of MM seals but attackers will prevent this using evolving techniques. Central banks update BOLMM in real time which will frustrate attacker ability to stay current with evolving security procedures. Once central bank archives receive failed MM, analysis of the FMM may pinpoint the last legitimate user before revocation of the central bank seal. Although the trail may lead investigators to a false recipient, the last legitimate payer EW likely has the details of the payment to the properly identified EWID. Users may configure their EW to respond electronically to investigator electronic requests, or use registered EWID to talk with the last legitimate user personally. Insurance rates likely will drive investigator tools and capabilities however it is vital the
government have strong redundant capabilities to track and prevent attackers from creating counterfeit MM.

Circulating MM have a vulnerability to interception; the solution mitigates the risk of interception by using timing algorithms and predicting a time for EW receipt of MM. EW payees set expected time of receipt that begins when negotiation messages finish and an agreement exists between payer and payee. Timing algorithms calculate time of transport using geocodes and the type of transport medium (light or sound waves). These variables also are optional elements in FMM. Timing algorithms need to use current velocity of MM receipt and bandwidth of the EW to prevent false reports of intercepted MM. If expected wait time for transport expires, the receiving EW revokes the MM and reports the attack to the central bank. Insurance covers the lost value of the receiving EW.

Payers may prevent MM from transport until agreement exists between payer and payees. Law defines an agreement between payer and payee. After agreement EW must transport payer MM to payee MM. Prevention of movement revokes the currency. Central banks receive two revocation messages for the same MM (the proposed receiving EW and the sending EW). Such cases may cause civil or criminal investigation and the central bank archives contain evidence of the failed agreement. Central banks must provide all spent or revoked FMM to courts of competent jurisdiction. Researchers can use aggregate FMM for research. Otherwise spent or failed FMM must remain confidential to payers and payees.

U.1 (Accessibility); Payees have access to MM after expected transport time as modified by payer and payee conditions and 400 milliseconds of validation of currency.

U.2 (Usability); EW providers sell product to EW users and usability affects sales. Too many legal restrictions on EW will reduce innovation creating solutions to EW user usability requests.

U.3 (Predictability); MM issuance, circulation, and redemption occur in real time; gross real time payment systems originate payment to EW or to other traditional accounts based on value contained within FMM. Speed of payment and value of payment are predictable and based on known and published parameters.

U.6 (Applicability to multiple use cases); Solution applies to all use cases.

S.5 (Handling disputed payments); Payers and payees use active or spent FMM and its associated contextual data as evidence of their agreement and payment.

S.7 (Security controls); Configurable.

S.9 (End-user data protection); Configurable.
F.3 (Fast availability of good funds to payee); 400 milliseconds plus transport time.

F.5 (Prompt visibility of payment status). Configurable by EW providers.

7. Settlement

Describe the approach or model for funds settlement between the providers to the approach, and the time it takes from the completion of payment initiation to the settlement of the payment. Describe whether the settlement will take place in central bank money or commercial bank money. Detail how the solution will manage settlement risks that may arise from a lag between funds availability to the payee and settlement between providers, or from settlement in commercial bank money.

Settlement is the redemption of MM by users. Users present MM; after validation of the presented MM (400 milliseconds or less), FI immediately transfer the value contained within FMM to a redeemer account by using gross real time payment systems. The redeeming FI may push the redeemed FMM to a correspondent FI or to the regional central bank or reissue it to other MM users. Central bank policy controls the volume of redemption requests for its issued currency; redemption fees cause longer MM circulation; redemption discounts reduces MM in circulation.

S.4 (Settlement approach); Settlement is defined as the redemption of MM by a central bank. FI use gross real time payment systems to transfer funds to redeemer accounts. FI will settle MM value based on central bank policies. Central banks receive enhanced controls to govern circulating currency.

S.7 (Security controls); Redeeming FI validate the central bank signature resident in the MM. If the validation fails then the redeeming FI moves the MM immediately to the central bank archives and the activities described earlier in section A. 6. (Receipt) occur.

S.9 (End-user data protection); Users receive value contained within authentic MM immediately. FI cannot prevent redemption for any reason other than an invalid (revoked) central bank seal.

F.4 (Fast settlement among depository institutions and regulated non-bank account providers). Solution requires gross real time payment between users and FI, and FI and central banks.

8. Reconciliation

Describe the solution’s mechanisms to create and record information to facilitate post-transaction evaluation, the processes and timeframes for handling unauthorized, fraudulent, erroneous, or otherwise disputed payments, and the allocation of liability among, and substantive liability limits for, all parties involved in the payment. Describe how consumer
protections are built into the reconciliation processes. Also describe any security features associated with reconciliation, including protecting sensitive information.

Any and all users of MM including central banks, FI, payers, and payees use FMM to reconcile spent or unspent value. Each row of FMM data contains the past value, the transaction amount, and the current value. Users can retain copies of completely spent FMM before sending it to the central bank archives. If users did not opt for anonymous transactions, or elect to receive FMM with anonymous sections in the FMM, then all contextual data indexed to the unique FMM transaction ID can aid reconciliation efforts.

U.3 (Predictability); Values within FMM should always balance or the central bank seal is revoked.

E.7 (Exceptions and investigations process); Spent and active FMM become evidence in court proceedings.

S.5 (Handling disputed payments); Payment disputes become a matter for courts of competent jurisdiction.

S.6 (Fraud information sharing); All spent or invalid FMM move to the central bank archives. There are no exceptions to this fundamental concept. Courts will allow or disallow investigators access to specific central bank archived transactions.

S.7 (Security controls); Altering or attempting to alter FMM revokes the central bank seal and immediately moves the revoked MM to the central bank archives.

S.9 (End-user data protection). MM resident in EW remain the sole asset of the EW owner. Reconciliation occurs as required by the owner and as provided by EW firms. If FMM do not balance, then the EW revokes the seal and insurance companies replace the FMM value. Insurance firms will need access to revoked MM to validate and pay claims, and how they receive a true, valid, copy, of the FMM as a basis of a claim must be a matter of legislation.
Part A, Section 2: Use Case Description

In this section, the proposer should describe what the solution does at each stage of the end-to-end payments process for each use case that the solution supports (business to business; business to person; person to business and/or person to person, as indicated in the table “Supported use case coverage summary”, above). Proposers should include flow diagrams of the messaging and payment flows and the roles of stakeholders (end users, technology providers, processors, including the proposer(s) for the solution) through the eight stages of the end-to-end payment process of their solution. The description and diagrams should be specific to each supported use case and should highlight all processes and features that are unique to the use case being described. For example, the solution may be designed to enable contextual data capability for business-to-business payments, but not for person-to-person payments. The business-to-business use case description should, therefore, include all the additional processes and features related to enabling contextual data capability.

<table>
<thead>
<tr>
<th>Options for Initiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case</td>
</tr>
</tbody>
</table>
| Business to Business (B2B) | • Two Person control over payment configuration  
• Capability to increase security for values exceeding Ceilings  
• Unlimited Number of concurrent payments  
• Use of Foreign FMM for payment to payee residing in the same foreign location  
• Allowance for payment on receipt of invoice either immediately or after the elapse of time  
• Duplication of corporate treasury controls in the EW  
• Use of insurance modules to mitigate risk | Commercial firms will create EW modules to meet the specifications of businesses. Some of these modules such as insurance modules will be standard interfaces that will fit in the EW but not configurable by the businesses, however most modules will be configurable by the EW owner and provide great flexibility over the security, timing, and cost of payments. |
| Business to Person (B2P) | • Limits to value without executive level approval  
• Same abilities as B2B payments | Can originate payments from same EW as B2B |
| Person to Business (P2B) | • Initiation with same functions and options as B2B  
• Ability to allow Business to pull payments from EW | |
Options for Initiation

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Example Features</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Person to Person (P2P)  | • All functions and options previously described  
• Flexibility to add features demanded by payers and payees such as programmatically determining tax liability and submitting simultaneous tax payment and P2P payment  
• Low cost insurance makes Regulation E obsolete |                                                                      |

**B2B**

Businesses may authorize FI to create MM from corporate funds and deposit it to a payee FI account or an EW. Businesses may also move stored MM from corporate EW to a payee (regardless if the payee is a business, a person, or a government).

If businesses request their FI to handle payments, then diagram 1 shows the flow.

**Diagram 1: Origination of B2B payments outside of EW**

![Diagram of B2B payment flow](image)

Otherwise businesses become circulators as shown in diagram 2.
Diagram 2: Businesses Circulating Currency

**B2P**
Businesses have the same choices to pay persons or businesses. See diagrams 1 and 2.

**P2B**
Persons have the same options as businesses to move funds to businesses. See diagrams 1 and 2.

**P2P**
Persons likely will circulate small value transactions as depicted in Diagram 2; however, people can always authorize their FI to move funds to other people’s EW or FI account using MM and as depicted in Diagram 1.
Part A, Section 3: Use Case by Effectiveness Criteria

For each use case that the solution supports (business to business; business to person; person to business and/or person to person, as indicated in the table “Supported use case coverage summary”, above), complete the following table. For each criterion relevant to the lifecycle stage, enter a “Y” if the use case addresses the Effectiveness Criteria (at least to a “somewhat effective level”) or an “N” if it does not (blanks will be assumed as “N”). For example, the solution may be designed to enable contextual data capability for business-to-business payments (U.4, Contextual data capability criterion), but not for person-to-person payments. Proposers should enter a “Y” for any functionality that will be in place at the date of implementation or for which there is a credible plan to implement the enhancement at a future date (as described in Part B, sub-section 1 “Implementation Timeline”).

For solutions where lifecycle stages occur simultaneously, the proposer should enter a “Y” or an “N” based on the criterion listed (rather than focusing on the categorization by lifecycle stage). The table is intended to be a summary of the description in Part A, Section 2.

<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>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>
</tbody>
</table>

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<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&lt;sup&gt;7&lt;/sup&gt;</td>
<td>S.3</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>F.1</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>F.5</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Clearing&lt;sup&gt;8&lt;/sup&gt;</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></td>
<td>U.3</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>S.5</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.3</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>Settlement</td>
<td>S.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.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

<sup>7</sup> The payer provider does not have to approve payment. However, the currency meets all the effectiveness criteria as if the payer provider approved payment. Providers only refuse redemption of MM if the central bank seal is revoked.

<sup>8</sup> Clearing and settlement occur at the same time. Clearing may be equated to message exchanges leading to payer/payee agreement, however once the payer and payee agree, MM moves from the payer to the payee immediately and irrevocably except as provided by government regulation.
## 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>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

In this part, the proposer should describe important business considerations to demonstrate the feasibility for the solution. Proposers may detail their qualifications or past experience in implementing faster payments in the sub-sections below if they view it will support the description.

1. Implementation Timeline

Specify the projected timeline and explain the credible plan for developing, testing and achieving initial implementation of the solution, including all key milestones and project phases to reach ubiquity (as defined in the glossary). The level of detail in the credible plan and timeline will assist in demonstrating the feasibility of the solution. The description should clearly indicate the use cases, functionality (e.g., cross-border, domestic, contextual data capability, etc.), whether the solution will be newly built and/or interface/interoperate with existing solutions, and features that will be ready at initial implementation and those that will be added in subsequent phases. The description should also indicate key dependencies (e.g., stakeholders or other external factors) and possible risks to the projected timeline.

Central banks must agree to standards for MM and EW. Although these standards have a tagged format as defined in ISO 20022, new fields and precise definitions of all fields will be a constant activity. Central banks govern the time frames for the development of adequate standards. However, the Current ISO 20022 standard can govern the pilot issuance of MM by a central bank. For example, central banks can issue MM to a group or an agency that can use the currency with selected group members or firms. In this case development of the BOLMM, and deployment of central bank points of presence exists and since they govern the security for circulating currency must have expert payment and security consultants provide quality assurance for pilot MM issued by a central bank.

Pilots for MM circulation can be defined geological areas or a volunteer group of users willing to buy the currency from their FI. After review of pilot activity, the central bank issues MM to new locations or users, or modifies MM, or allows commercial firms to provide EW functionality. Diagram 3 shows the projected timeline.
U.1 (Accessibility); Central banks need to try to issue MM to as many firms and people that apply to use the currency in a pilot.

U.2 (Usability); Commercial firms developing EW functionality will provide functions for enhanced user satisfaction.

U.3 (Predictability); Rules for issuance, circulation, redemption, and revocation must be clearly published and software acting on those rules must be tested and certified by a central bank or its agents.

E.3 (Implementation timeline); 7 Months for development, 1 year for pilot and rollout.

E.5 (Comprehensiveness). Meets all user cases

2. Value Proposition and Competition
For each use case supported by the solution, describe the value proposition to each stakeholder in the solution (end users, technology providers, processors, the proposer(s) of the solution) through each of the eight stages of the payment lifecycle (as discussed in Part A). Consider why stakeholders will adopt the solution. NOTE: If the value proposition discussion includes fees in the system, describe the nature of what type of fees might be charged to and received by different stakeholders such as whether they are one-time, recurring, per item, ad valorem, any floors/caps, per item + ad valorem and provide any related system constraints. Do not provide any proprietary cost or pricing information.

FI move the currency electronically eliminating costs associated with cash, check processing, or payment card clearing and settlement. Payees do not have to pay to receive circulating currency but can negotiate a price from a payer that includes overhead costs such as insurance or EW security controls. Initial calls to government modules (present in geographical locations) govern all taxes related to transactions; payers and payees negotiate payment of all taxes; government rules determine the timing of payment of taxes. End users can prevent movement of mm to government for taxes, however such action may have consequences such as the revocation of the EW seal. FI redeeming MM may be forced to collect taxes and settle funds to conventional accounts for FMM value less collected taxes. Taxes removed from MM payments must move to the taxing agency immediately using either the MM method or by gross real time payments. The nature of consecutive payments to payees, their associated accounts, and government taxing agencies is configured as a default setting, updated with calls to government modules, and configured by EW users. Such controls increase time needed for pre-initiation of payment and negotiations between payer and payee.

There are no value ceilings in MM. Central banks may wish to issue very large value MM to their correspondent banks, which may in turn issue MM of varying values to their customers.

Describe how the solution will enable access to new entrants (competition) into the broader ecosystem of the proposed solution (e.g., to provide base-level features or value-added services).

The solution allows for a new generation of commercial firms to enhance payment experiences. Insurance firms will rate EW and user choices to determine premiums for circulating MM. EW providers will provide differing solutions demanded by different use cases. Accounting firms, law enforcement, and others can use FMM to determine past history of circulating MM if allowed by payers and payees. Central banks can change BOLMM allowing for security controls to confront current threats. Central banks fees or discounts influence the volume of circulating MM. Banks will use circulating MM as assets on their books with the distinct possibility that funds payed to banks for MM may never be redeemed or redeemed many years in the future after the value of FMM erodes due to inflationary pressures. New commercial firms will need to build.
and place points of presence for users receiving volume MM payments. These points of presences must immediately validate MM proposed for payment and thus have sufficient bandwidth to meet payee demands. Central banks must provide archival services for all spent or revoked FMM.

U.3 (Predictability); Movement and storage of funds remains consistent for MM and EW

E.1 (Enables competition); Many commercial firms will compete to provide security, insurance, and access to government modules and points of presence.

E.2 (Capability to enable value-added services). The EW provides firms ability to add countless value added services. Some may wish to add customer loyalty applications; others may wish to pay interest for short term use of idle MM. As the currency evolves, no doubt exotic value added service will also evolve.

3. Integration Effort

For each use case supported by the solution, describe the points of integration required for each stakeholder in the solution (end users, technology providers, processors, the proposer(s) of the solution) for each of the eight stages of the payment lifecycle (as discussed in Part A). Proposers should include flow diagrams of the points of integration and the business relationships between the various stakeholders. For each stakeholder, identify the effort required on a relative order of magnitude basis (e.g., either temporally – days, weeks or years – and/or as compared to other common integration experiences in the payments industry such as, connecting to a new EFT service or supporting a new ACH file type). Discuss any explicit on-going efforts to maintain integration to the system.

EW circulate MM by using data protocol standards propagated by central banks. Retail environments may wish to have points of presence for central bank validation of circulating MM. Insurance firms may wish to create standards for insurance of funds contained in EW circulating MM. Government must agree to standards for calls to download logic governing payment in their geographical regions. FI and central banks must create specialized EW and secure transmission pipes to issue and redeem large value MM. Central banks must create FMM archival services. At first solution providers will need months of lead time to allow for the development and consideration of new hardware and software governing circulating MM. As the solution matures these variations of methods will allow user specific choices for circulating their MM, receiving MM from FI, and, redeeming MM. However, MM can circulate among current devices such as electronic cash registers, phones, or other points of sale with limited processing power by changing the software to validate, store, and transmit MM. Timing for the release of these new applications resident in current device depends on the propagation of standards by central banks. The full roll-out of MM and associated equipment should take about the same time
as the roll out of electronic point of sale terminals in the early 1980s in the US or perhaps a feature such as guarantee of check payment or EDI functions. Since use of the currency will be a lot more efficient than most current options used in retailer environments today response to strong demand for the currency will result in demand for sophisticated EW functions wherever housed.

Integration points must consider the payer’s depository institution or non-bank account provider (for origination and receipt on behalf of end users), third-party service providers, merchants (e.g., PoS and eCommerce), billers, consumers, businesses, etc.

FI issue and redeem circulating MM. Users can redeem MM at any FI or non-FI offering the service. If FI issues MM to a user, another or the same user can redeem all or part of the FMM value from another unrelated FI. Redemptions always occur using gross real time payments from issuing FI networks.

For example, a retailer today has 12 lanes equipped with ECRs, payment card readers, check readers, etc. MM used by payers shopping at the store initiate movement of MM from their EW to the merchant POS. The merchant can develop a function on the POS to periodically move MM stored in their POS to their FI account. Movement to the FI occurs exactly as earlier described in Section A.1 however the POS may consolidate all the individual MMs submitted by payers into one MM for transmission to their FI. FI receive the MM as redemption type, validate the MM depending on their policies, and immediately provide funds to the merchant account using a gross real time payment system. The FI can then keep the MM in its own form of EW or submit it to the issuing FI or FIs by breaking out the individual values owed by issuing FI contained in the FMM.

U.1 (Accessibility); FI provide Funds related to FMM immediately. It is recommended that all FI allow user redemptions or issuance 24 hours/day, 7 days/week, and 365 days per year. However individual FI policy coupled with central bank and government regulation determine accessibility of MM and accessibility of redemption services.

U.3 (Predictability); Unless an MM contains a revoked central bank seal MM circulates only constrained by local government law.

E.1 (Enables competition); Central banks create a competitive atmosphere by creating standards and creating policies to increase or decrease circulating MM. Too many regulations will limit innovators developing EW functions. Too few regulations may cause vulnerabilities from sloppy applications resident in EW.
E.2 (Capability to enable value-added services): It will be common place for innovators to add value added services to EW. The deployment of these modules are regulated and resident EW software must conform to standards propagated by central banks.

E.6 (Scalability and adaptability). There are no theoretical limits to the volume, velocity, or acceleration of MM. In practical terms though movement of issuance, circulation, and redemption of MM count on the infrastructure and bandwidth of transmitting and receiving equipment and EW.
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

This section should be used by proposers to assess how the solution meets each of the criteria outlined in the Effectiveness Criteria (considering all use cases supported by the solution). Proposers should include in their self-assessment any functionality that will be in place at the date of implementation or for which there is a credible plan to implement the enhancement at a future date (as described in Part B, sub-section 1 “Implementation Timeline”). For example, the Effectiveness Criteria specifically acknowledges that proposers may not have cross-border functionality at implementation but may have a credible plan to implement it at a later date.

Proposers should use the tables below to indicate their self-assessed rating on the Effectiveness Scale outlined for each criterion, as well as a detailed discussion of why the rating is justified and how the solution meets each criterion (e.g., U.1, U.2, etc.), including each consideration (e.g., U.1.1, U.1.2, etc.). Proposers may use the far-right column (“Proposal Page Number”) in the tables to cross-reference the section/page number for the relevant description provided in Part A or Part B, above.

Proposers should note that a number of the criteria have been written in a way that provides flexibility for a range of different approaches to address the criteria or for the solution to determine how certain terms and parameters are defined. Proposers should ensure their justification of how the solution meets each criterion includes a clear explanation of the approach taken in the solution, and how solution-determined terms and parameters are defined. For example, S.2.3 (Payer authorization criterion) requires the solution to enable the payer to revoke any pre-authorization of payments easily and timely. The proposer’s justification for S.2 should include how the revocation is “easy” for the payer and the time it takes (i.e., number of minutes, hours, or days) for the revocation to take effect. Similarly, E.6.2 (Scalability and adaptability criterion) requires the solution to demonstrate the capacity to handle projected volumes and values (determined by the solution), including heightened transaction volumes and values during peak times or periods of stress. The proposer’s justification for E.6 should include its assumptions for determining the heightened volumes and values and how they relate to normal periods (e.g., heightened volumes are equal to twice the projected volumes during normal periods).

NOTE: VE = Very Effective  
E = Effective  
SE = Somewhat Effective  
NE = Not Effective

Proposers should refer to the Effectiveness Criteria for an explanation of what Very Effective, Effective, Somewhat Effective and Not Effective mean for each criterion.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
1. **Ubiquity**

   Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: accessibility, usability, predictability, contextual data capability, cross-border functionality, and applicability to multiple use cases.

   **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><strong>Criteria Name</strong></td>
<td><strong>#</strong></td>
<td><strong>Consideration Name</strong></td>
</tr>
<tr>
<td>Ubiquity U.1</td>
<td></td>
<td>Accessibility</td>
</tr>
<tr>
<td>Ubiquity U.2</td>
<td></td>
<td>Usability</td>
</tr>
<tr>
<td>Ubiquity U.3</td>
<td></td>
<td>Predictability</td>
</tr>
<tr>
<td>Ubiquity U.4</td>
<td></td>
<td>Contextual data capability</td>
</tr>
<tr>
<td>Ubiquity U.5</td>
<td></td>
<td>Cross-border functionality</td>
</tr>
<tr>
<td>Ubiquity U.6</td>
<td></td>
<td>Applicability to multiple use cases</td>
</tr>
</tbody>
</table>

   **Justification for U.1:**

   [Discuss self-assessment addressing considerations U.1.1 to U.1.6]

   Central banks issue MM; Any user, or FI, may initiate immediate transfer of MM to authorized devices. Peer to peer transport makes payment possible to any device supporting the protocol. Fiat currency type is an element of the FMM. Government may wish to consider giving barebones EW to unbanked payers and payees. FI can issue MM to customers or non-customers. Special firms may transport circulating MM to any payee. Providers of the MM; i.e. FI issuing MM to users, make discounted payments to central banks issuing the currency. FI compete to issue MM to customers. Retailers and other large volume payees do not have fees associated with clearing costs associated with payment cards. Current point of sale equipment contains sufficient capabilities for EW functionality. Government define the standards allowing MM free movements across jurisdictions. Conversion of currency is a function of redemption.

   **Justification for U.2:**

   [Discuss self-assessment addressing considerations U.2.1 to U.2.4]
EW storing, transmitting and receiving MM meet standards by can reside in almost any electronic device required by users. Some examples discuss payments from current devices such as electronic cash registers or cell phones. An EW initiates payment to a peer client established once negotiation of payment begins. MM circulation does not conform to time of day considerations. Payment is final after payee receives MM and validates central bank seal within 400 milliseconds. Users buy EW conforming to their requirements.

**Justification for U.3:**

[Discuss self-assessment addressing considerations U.3.1 to U.3.6]

The components of MM, EW, allow users to customize the core value contained within EW. The core components include receipt, transmission, and storage of MM, and the detection of central bank seal revocation, or revoking the central bank seal. Current laws govern the definition of finality although the solution describes liability for disputed funds transfer. Payers and payees negotiate payments prior to transport of MM to payee. The solution requires the propagation of data protocol standards by central banks. The solution gives baseline expectations for issuance, circulation, and redemption of MM. Money Modules (MM), electronic wallets (EW) Break-out Logic MM, Fundamental Money Modules, central bank points of presence for authorization, and downloaded government constraint logic are unique common terms for the currency.

**Justification for U.4:**

[Discuss self-assessment addressing considerations U.4.1 to U.4.3]

Users can associate any data relevant to a unique transaction ID as they see fit. Transmitting and receiving geocodes are part of the FMM. The central bank archives all spent and revoked MM and can deliver these to investigators or courts as required by law. Users determine the need for security controls and contextual data and firms providing EW functionality provide those functions to EW users.

**Justification for U.5:**

[Discuss self-assessment addressing considerations U.5.1 to U.5.5]

Governments and central banks create standards for receiving or transmission of foreign value FMM. Local government restriction on circulating MM govern cross-border capabilities. Review of proposed payment across jurisdiction becomes part of the negotiation messages between payer and payee. Conversion of currency only occurs when users redeem their FMM from issuing FI networks. A payee must redeem a euro denominated MM from FIs issuing MM in Euros.

**Justification for U.6:**

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
[Discuss self-assessment]
The solution addresses all use cases.

2. Efficiency
Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: enables competition, capability to enable value-added services, implementation timeline, payment format standards, comprehensiveness, scalability and adaptability, and exceptions and investigations process.

<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>Efficiency</td>
<td>E.1</td>
<td>Enables competition</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.2</td>
<td>Capability to enable value-added services</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.3</td>
<td>Implementation timeline</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.4</td>
<td>Payment format standards</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.5</td>
<td>Comprehensiveness</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.6</td>
<td>Scalability and adaptability</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.7</td>
<td>Exceptions and investigations process</td>
</tr>
</tbody>
</table>

Justification for E.1:
[Discuss self-assessment addressing considerations E.1.1 to E.1.4]
Firms compete to offer users EW functions, MM insurance, issuance and redemption transfers. Circulating MM belong to EW users, not FI or issuing elements. All negotiations during issuance, circulation, or redemption occur prior to transfer of MM. All such data exchanges occur using standards propagated by central banks and controlled by government modules resident in EW. Users select the functionality required for their EW and either purchase them a-la carte, or purchase them bundled by the EW provider. Government boards certify functions from standards published by central banks.
Justification for E.2:
[Discuss self-assessment addressing considerations E.2.1 to E.2.3]
The solution allows users to configure EW and use software on per individual user requirements. Providers are either issuing FI or non-FI circulating issued MM. Disclosures of value added service occur during payer and payee negotiations if allowed by user EWs.

Justification for E.3:
[Discuss self-assessment addressing consideration E.3.1]
Users purchase MM from issuing FI and non-FI firms circulating MM. Users purchase the security controls they need for validation of proposed payer MM and for MM resident in EW. Ubiquity is assured because timing and costs of payment will be substantially less than currency, check or payment card transactions.

Justification for E.4:
[Discuss self-assessment addressing considerations E.4.1 to E.4.5]
Central banks develop standard protocols based on ISO 20022 and use EMV security procedures to create and protect the central bank seal. Acceptance of the standards by differing governments create interoperability and allow cross border transactions. These standards allow equipment, EW, and MM providers with clear standards for implementation. Rules and regulations governing functions and accreditation of functions are propagated by central banks.

Justification for E.5:
[Discuss self-assessment addressing considerations E.5.1 to E.5.2]
The solution uses current FI endpoints for issuance and redemption. Customized EW functionality provides users with all current functions offered by current payment solutions. Risk and vulnerabilities are governed by central bank controls, insurance companies, and EW functions.

Justification for E.6:
[Discuss self-assessment addressing considerations E.6.1 to E.6.3]
The solution solves all use cases. The solution provides methods for allowing increased volumes and rates of flow of MM. MM is configurable and circulating MM receive updates to BOLMM as determined by the issuing central bank.

Justification for E.7:
[Discuss self-assessment addressing considerations E.7.1 to E.7.3]
The solution provides standards for data required by users. The central bank provides an archive for all revoked or spent FMM which can be used as evidence in court proceedings. Researchers will use aggregate spent and revoked FMM to determine patterns of money movement.
3. Safety and Security

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: risk management, payer authorization, payment finality, settlement approach, handling disputed payments, fraud information sharing, security controls, resiliency, end-user data protection, end-user/provider authentication, and participation requirements.

**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><strong>Criteria Name</strong></td>
<td><strong>Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Risk management</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Payer authorization</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Payment finality</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Settlement approach</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Handling disputed payments</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Fraud information sharing</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Security controls</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Resiliency</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>End-user data protection</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>End-user /provider authentication</td>
<td>✓</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Participation requirements</td>
<td>✓</td>
</tr>
</tbody>
</table>
**Justification for S.1:**

[Discuss self-assessment addressing considerations S.1.1 to S.1.6]

EW receive updated logic from government points of presence as versions change, as users move across jurisdictions, and on initiation of EW original set-up operations. Settlement occurs from redemption of MM across secure FI networks to accounts. Validation ensures circulating MM are legitimate. EW revoke MM that cannot be validated. Non-receipt of proposed MM after payer/payee agreements. Insurance firms replaced revoked FMM value. Revocation, central bank archives, and law mitigate fraud and other attacks on circulating MM. Insurers increase rates for payers and payees restricting various EW common validation methods. Central banks continually evaluate risks to MM and update BOLMM to mitigate new attack methods.

**Justification for S.2:**

[Discuss self-assessment addressing considerations S.2.1 to S.2.3]

Payers authorize MM movement from authorized controls sold to payers as EW functions. Circulating MM does not require FI approval for transport to a payee MM. Payer and payee use negotiation messages to reach an agreement. Once an agreement is made MM moves across a peer to peer connection immediately. Users can assemble MM for movement any time before finalization of the payer/payee agreement.

**Justification for S.3:**

[Discuss self-assessment addressing considerations S.3.1 to S.3.3]

Payment is final 400 milliseconds after receipt by payee EW. Redemption of MM requires gross real time payment to user FI account of choice. User EW receive logic from government points of presence that govern conformity to regional laws regarding money transfer. Central bank archives provide evidence of dispute. Insurance firms cover risks associated with payments.

**Justification for S.4:**

[Discuss self-assessment addressing considerations S.4.1 to S.4.3]

Redemptions occur immediately using gross real time payment systems. The solution provides clear controls for liquidity and credit risk. Strict measurement of expected transfer time requires revocation of currency not received in a timely manner.

**Justification for S.5:**

[Discuss self-assessment addressing considerations S.5.1 to S.5.5]

EW revoke the central bank seal of disputed transactions requiring replacement of value by insurers based on FMM history contained in the central bank archives. Consumer protection modules reside in EW and used by payers and payees as governed by law and government required modules. Insurers will provide restoration of disputed MM transactional values.
**Justification for S.6:**

[Discuss self-assessment addressing considerations S.6.1 to S.6.7]

The central bank archives and protects spent and revoked MM. BOLMM logic creates new MM from MM resident in EW and moves it for transport after updating the resident FMM value. EW provides aggregate value of MM contained in a EW. Central banks propagate standards for data exchanges based on ISO 20022. Users configure EW sharable data as dictated by user choice.

**Justification for S.7:**

[Discuss self-assessment addressing considerations S.7.1 to S.7.3]

MM uses asynchronous signatures and encryption to protect the integrity of the currency. Central banks propagate BOLMM immediately to circulating MM as threats change. Users control functions in resident EW to provide user authentication and prevent intrusion. Central banks can require EW to contain any security review as needed. The solution provide data retention and disposal controls, monitoring and incident responses, communications and network security. EW can conform to existing user or treasury controls. MM reside in EW available for all types electronic computing equipment. Central banks update of BOLMM keeps security controls current.

**Justification for S.8:**

[Discuss self-assessment addressing considerations S.8.1 to S.8.5]

Target availability metrics are clear. Insurance covers lost, stolen, or revoked MM due to a variety of causes. All functions residing in EW receive validation by government approval bodies requiring a 3 week maximum review time of the function. Central bank experts review BOLMM logic and disperse it to circulating currency in real time.

**Justification for S.9:**

[Discuss self-assessment addressing considerations S.9.1 to S.9.3]

The solution provides central banks robust controls over circulating MM. Users determine what information is contained in data segments indexed by unique MM transaction IDs. Central bank archives can receive contextual data if users wish to send it.

**Justification for S.10:**

[Discuss self-assessment addressing considerations S.10.1 to S.10.6]

Authentication of MM and EW uses standard asynchronous electronic signatures. Payment not received by EW causes revocation of the proposed MM constructed during negotiations. Government can require any EW function deemed appropriate. Various protocols ensure the requirements of authentication modules. The solution provides the EW with government logic to control payment initiation and receipt. The solution allows central banks to replace the BOLMM at any time.
Justification for S.11:
[Discuss self-assessment addressing considerations S.11.1 to S.11.3]
The EW loads regional legal logic on first use or change in legal jurisdictions. Central banks dictate reserve strengths for circulating MM. Central banks may query circulating MM on selected aggregate environmental concerns.

4. Speed (Fast)
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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Speed (Fast) F.1</td>
<td>Fast approval</td>
<td>✓</td>
</tr>
<tr>
<td>Speed (Fast) F.2</td>
<td>Fast clearing</td>
<td>✓</td>
</tr>
<tr>
<td>Speed (Fast) F.3</td>
<td>Fast availability of good funds to payee</td>
<td>✓</td>
</tr>
<tr>
<td>Speed (Fast) F.4</td>
<td>Fast settlement among depository institutions and regulated non-bank account providers</td>
<td>✓</td>
</tr>
<tr>
<td>Speed (Fast) F.5</td>
<td>Prompt visibility of payment status</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Justification for F.1:*
[Discuss self-assessment]
Approval comes from the payer after agreement between payer and payee. Approval and transmission of MM occur simultaneously.

*Justification for F.2:*
[Discuss self-assessment]
Clearing does not exist. MM becomes final within 400 milliseconds of EW receipt.
Contextual data becomes available as data indexed by MM unique transaction identifiers. The movement time, whether contextual data is pre or post MM transfer, are negotiated by payer and payee.

**Justification for F.3:**  
[Discuss self-assessment]  
Contextual data moves across the same peer to peer connection as MM and depending on the amount of data needed by payee should be available no later than 10 seconds after MM movement.

**Justification for F.4:**  
[Discuss self-assessment addressing considerations F.4.1 to F.4.3]  
Circulating currency prevents low credit and liquidity risks because of fast finality of payment, and central bank controls over value transmitted within the FMM of MM. All interbank settlements use gross real time payment systems for redemptions including FI redemptions.

**Justification for F.5:**  
[Discuss self-assessment addressing considerations F.5.1 to F.5.2]  
EW use the BOLMM to change the value of resident MM immediately before transfer of value to payee accounts. EW report aggregate change in MM value instantly. The payee reports aggregate value of payee value 400 milliseconds after receipt of valid MM. EW will also show history and details of any transactions either proposed or completed as users required.

5. **Legal Framework**  
Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: legal framework, payment system rules, consumer protections, data privacy, and intellectual property.

**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># Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.1 Legal framework</td>
<td>✓</td>
</tr>
</tbody>
</table>
Legal Framework | L.2 | Payment system rules | √ | ES, 33
---|---|---|---|---
Legal Framework | L.3 | Consumer protections | √ | ES, 46
Legal Framework | L.4 | Data privacy | √ | 30
Legal Framework | L.5 | Intellectual property | √ | No changes in IP protection

**Justification for L.1:**

[Discuss self-assessment addressing considerations L.1.1 to L.1.5]
EW update legal logic on first use of EW in a new jurisdiction. EW will not operate without logic from local governments. Local governments control legal logic for EW. Payments, disputes, and finality have a basis in current laws. The legal module downloaded to EW provides all legal governance of circulating MM.

**Justification for L.2:**

[Discuss self-assessment addressing considerations L.2.1 to L.2.5]
Authentication occurs by inspection of central bank seals and approved controls embedded in EW. EW providers must certify their functions with government inspection committees. Payment sequences are fixed. Payments transmitted to payee EW are final 400 milliseconds after payee receipt unless the EW revokes the MM during validation. Central bank archives keep details on all revoked or spent MM and contextual data as submitted by payees and payers. The solution addresses timing. FMM provide transaction history. Central banks provide spent and revoked MM based on court orders. Central banks and governments provide operating rules for circulating MM. Common law and central bank archives provides evidence and legal frameworks governing disputes.

**Justification for L.3:**

[Discuss self-assessment addressing considerations L.3.1 to L.3.3]
Insurance firms replace value of revoked MM as provided by law. FMM provide MM ancestry and transaction details as required by law. The EW is configurable base on user requirements.

**Justification for L.4:**

[Discuss self-assessment addressing considerations L.4.1 to L.4.5]
Users define their own privacy controls. The solution provides robust security for stages of currency issuance, circulation, and redemption. The solution provides optional security.
measures configurable by users. Users control their sharing of contextual data based on individual payment negotiations or default EW settings. Data breaches of MM cause revocation of central bank seal. Security functions embedded in EW control the results of intrusion attempts or interception of MM in transit.

**Justification for L.5:**

[D Discuss self-assessment addressing consideration L.5.1]

MM does not change intellectual property law.

6. **Governance**

Provide a self-assessed rating in the table below and then describe how the solution meets criteria for: effective governance and inclusive governance.

<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:**

[D Discuss self-assessment addressing considerations G.1.1 to G.1.4]

Central banks and governments propagates standards, rules and regulations governing MM. All governance documents are available to the public. Current court procedures govern disputes using central bank archives as evidence. Appeals are handled by court rules. Inspectors and law enforcement officials may subpoena archived MM.

**Justification for G.2:**

[D Discuss self-assessment addressing considerations G.2.1 to G.2.5]

Central banks produce framework for certification agencies. Stakeholders may sit on government certification committees as voting members as governed by certification committee bylaws. The number of members in certification committees shall be placed in the bylaws along with clear causes for disallowing potential members. COI mitigating procedures for members in certification boards are placed in the framework for certification committees published by the central bank issuing the currency.
Introduction to TMC Response

Thought Matrix Consulting (TMC) prepared this document as a response to the McKinsey & Company (McK) assessment of the Money Module (MM) Design. My response addresses either a question or a comment from the preliminary assessment. The comment or question is quoted, footnoted, and numbered; the TMC response follows. For brevity, this is not a point-by-point rebuttal to the entire McK assessment, rather my response only endeavors to address those parts of the assessment requiring a more precise description of the solution.

I wish to thank the McK team for their review and remarkable insights which focused my attention to details of the MM solution. I am honored to work with the McK team.

TMC Response to Comments in “Areas for Improvement And Enhancement”

1. To be broadly effective, the solution must first win support from the central bank. The proposal does not outline a plan for gaining central bank support or for encouraging broad end-user adoption.1

TMC was not trying to sell a design, TMC was submitting a design. If TMC reviews a better design, then TMC will happily abandon the Money Module (MM) design for a better one. Later in the process, TMC hopes to work with the Faster Payment System Task Force (FPSTF) to discuss all designs and the merits and failings of each.

TMC believes that a currency will be used because it is a better form of payment than alternative payments. However, any cheaper, faster, and more secure payment methodologies fitting seamlessly with gross real time payment systems (GRTPS) are better than the card based token systems used for retail payments, or deferred netting payment systems regardless of the periodicity of the netting process.

2. Adoption has challenges unless the central bank issues a mandate to accept MM as legal tender since depository institutions would give up revenue associated with current payment systems, merchants would need to upgrade and develop new functionality in POS systems to accept MM, commercial firms would need to develop new EW functionality and products2

MM is legal tender because central banks issue it and state the value in terms of the number of lowest possible value units of central bank fiat currency. Mandating its acceptance however is difficult because it forces all economic participants to receive and send currency electronically,

---

1 McKinsey & Company; Faster Payments QIAT Preliminary Assessment, Proposer: Thought Matrix Consulting, LLC; P. 1; section entitled “Areas for improvement and enhancement”; 1st bullet.
2 IBID; section entitled “Areas for improvement and enhancement”; 2nd bullet.
which may not be technically feasible in environments ill-equipped with a modern infrastructure. It is possible to integrate MM into programmable POS systems recognizing that most of these devices use a version of VISA II at a low version of transit as shown in diagram 1.

Diagram 1: Typical Low Level Visa II data protocol

Payers today use various protocols such as swiping a magnetic card, inserting an EMV smartcard, or manually entering data uniquely identifying the payer to an authorizer. Most POS devices can also accept various disconnected forms of communication such as near field communication or proprietary protocols such as “Ipay” or “Samsung Pay”. Regardless of the method of entry used by a POS device or the size of the data stream entered by the user, some devices communicate to a point of presence (POP) with a version of VISA 2 protocol shown in Diagram 2. The actual data streaming from a POS device to a point of presence is unbounded by size and so can contain the MM data set within an ISO 20022 form regardless if the data is reformatted to an ISO 8583 data protocol standard. Thus with little change to POS devices, MM can use the current retailer payment infrastructure. The EMV protocol supports a digital currency because it supports independent data structures.

---

3 EMV: Integrated Circuit Card Specifications for Payment Systems Book 1 Application Independent ICC to Terminal Interface Requirements; Version 4.2; June 2008; See specifically definitions of “File Control Information” and “Application Definition Files” and the methodology for accommodating XML tagged structures.
- Solution relies on Central Banks to absorb the cost associated with maintenance, production and immediate distribution of BOLMM to all circulating MM. While the Solution notes that MM move based on Payer and Payee negotiations, there is not clarity on the consensus mechanism used to update the blockchain, the speed by which the blockchain can be updated\textsuperscript{4} through this consensus mechanism, and the governance for making updates to the blockchain.

The solution makes an assumption that central banks can fund the system on a cost basis just as the Federal Reserve charges fees to fund Fedwire. Before funding operations, central banks must estimate a cost, and determine a method of funding which accurately matches operational cost. TMC considered many options for funding but ultimately considered the funding mechanism as irrelevant to the design. However, I liked a formula used in the discount/fee mechanism that added remuneration fees to a rate formed from a central bank policy consensus.

The blockchain consists of the mandatory elements described in the design, and optional elements present by EW configuration. For example, say a payer and a payee verbally negotiate a price (as opposed to an EW setting that allows the payer to automatically accept the price provided by the payee) and the payer EW contains MM from more than one central bank. The

\textsuperscript{4} McKinsey; pps 1-2; “Areas for improvement and enhancement”; 3rd bullet.
EW may be configured by the payer and payees to select the denomination of the currency and their configurations do not allow the transaction to occur. In such a case, the payer and payee must negotiate a currency type outside electronic negotiation. Otherwise, payer and payee may have set a “do not care about currency type”, or a preference tree, which coupled with the preference tree of the participating wallet “agree” on currency type. Likewise, the EW of the participants in a transaction may have bit masks for contextual data allowed in the blockchain. The timing of electronic negotiations (depending on the user desire to manipulate the minutiae of transaction detail present in the blockchain) using a timing crystal allowing a CPU to determine the validity of electronic signature in 400 MS, provides a real time decision rapidly and not a consideration for parties conducting transactions.

- Security of the blockchain is a critical element for digital currency and the proposal needs to further elaborate on how security will be ensured particularly against around validation of the FMM and central bank seal to prevent manipulation of the BOLMM or the FMM outside of standard calls. In addition, the proposal states that security controls between the payer and payee are “configurable” and often “payers and payees enact security procedures as they deem fit” (page 32) leading to questions around what base level of security can be provided.

The security of the BOLMM, and the FMM are based on the encryption techniques using asynchronous encryption techniques such as elliptical curve cryptography or public key interchange. The EMV description of Combined DDA/Application Cryptogram Generation (CDA) sited in the solution is an adequate basis for the design. However, the actual method of encryption and electronic signature may be a dynamic structure determined at issuance and thus posing attackers the dilemma of determining what method protects the seal, making it hard to attack without causing a revocation event.

Access to EW is controlled by its owner, and if users do not wish to protect access, then there will be no protection to access. However, it is likely that the EW industry will set default access security for users just as most accounting software requires a password for access to data; not allowing users to create financial data without a minimum level of intrusion protection,

- Solution relies on critical “modules” including security, transmission, reception, legal controller, broadcast response, and of particular importance, insurance and consumer protection modules. More clarity is required on how these modules will be developed, how they will work, and what the end user experience will be for interacting with these modules.

---

5 IBID; p. 2
7 McKinsey; P.2
The design is the start of a work in progress and needs the enhancement of a team, not just a single architect. TMC agrees with the assessment.

- The Solution has not defined several elements of the faster payment solution, including: rules or a process for resolving disputes (rather, it relies on the court system for resolution); contextual data which a function of the EW but relies on relies on new development of actual tags created by a technical standards committee; fraud information-sharing capabilities; risk and legal framework; and governance model

TMC believes that law is an extremely good method for determining the outcome of disputes. TMC considers that data protocols made without consensus from a broad based pool of knowledgeable users are protocols doomed for failure. Part of the current problem with current small value payment systems comes from the use of proprietary protocols designed to protect profit, not to enhance the usability and lower the expense of a payment system.

Answers to Questions

Ubiquity

U.1.2: How can the Solution reach Payees without an existing Electronic Wallet?

There are many ways the solution can allow payers and payees to conduct transactions without using EW; market forces will enable firms to offer myriad solutions. However, the context of the question indicates concerns that unbanked or individuals with limited assets will not be able to participate in transactions. Worst yet, needs based systems such as the Supplemental Nutrition Assistance Program (SNAP (nee food stamps)) or the Special Supplemental Assistance Program for Women, Infants, and Children (WIC) now use card technology (or are in the process of converting to a card technology from paper based financial instruments) to issue benefits. FNS then controls purchases by using a network of authorized retailers to sell only items allowed by the programs. In order to fund these programs with MM, the United States Department of Agriculture (USDA), Food and Nutrition Services (FNS) need to issue MM with restricted use to unbanked individuals without funds for EW.

There are several solutions to the problem of the unbanked; the simplest solution is governments give an EW to individuals that cannot afford them or do not wish to use discretionary funds to buy one. This is not very different from government giving cellular phones to those that need one or giving EBT cards to individuals participating in FNS needs based programs. If governments need to restrict purchases, then they create modules in the issued EWs that restrict purchases based on the FNS blockchain history within the FMM. TMC envisions an electronic negotiation so that a food retailer POS requests a shopping list

8 IBID; p. 2
from the government issued EW (in the case of WIC) or determine if a product meets the requirements for purchase (in the case of SNAP) and then access the EW accordingly. The government issued EW must have the capability to receive unrestricted MM, a primary function common to all EW.

U.1.4: If pricing of security is left up to market forces, how will the unbanked and underserved (who often have less buying power) have access to a base level of transaction security?

All government issued EW will contain minimum access controls just as EBT cards now require a Personal Identification Number (PIN) to allow access to funds. Also, just as current EBT cards are not protected by Regulation E (Reg E), governments will not be required to protect needs based MM. However, unlike the EBT cards, users will be able to purchase insurance at the same rate as other similar non-government EW so governments issuing needs based EW may consider the costs of insurance versus the intrusion protection offered, so they keep insurance rates low for program participants.

U.1.5: What is the motivation for Providers and other entities (central banks, third party providers of modules) to participate and make the solution available to End Users?

Central Banks, correspondent banks, and retail financial institutions will base their wholesale purchases of MM based on discounts and other incentives offered by central banks. Thus profit is the motivation for the banking industry to issue MM to retail customers. The banking services industry currently processing card based transactions may receive increased profits by providing retailers contextual data about payment, and offer incentives to EW users to provide contextual data about payees. Insurance companies will use current methods to determine their risk and correspondent profits for an entirely new revenue stream.

U.2.1: How will the Solution ensure a base level of usability among Electronic Wallets?

The question arose for a “Somewhat Effective” rating for the U.2 Usability criteria. The assessment gave the following rationality for the rating:

"The EW can store, transmit, and receive MM via almost any electronic device and channel and is available 24/7/365 (U.2.1, U.2.3). However, the channels, devices and hours of accessibility are determined by the EW Providers – the requirements, guidelines, and guardrails that will shape the usability of the EW (minimum features required) are not stated (U.2.4). In addition, while the proposal mentions public and private keys, it is unclear how the Solution enables an Entity to initiate a payment with limited information such as a name, email address or phone number (U.2.2).”

EW providers may wish to add restrictions to payment and in some cases may be legally obligated to do so (restrictions for purchases for non-adult payers for example), however there is absolutely no requirement for EW providers to do so, and by restricting payer capabilities, they adversely affect the demand for their EW, and may inadvertently prevent the sale of increased security solutions. In some cases, for example large value

---

9 IBID; P. 3
corporate payments, the EW provider may offer a range of security considerations before allowing transfer of MM including determining if payment originates during impermissible times or suitability of transfer infrastructure, however there is no requirement for such conditions within the EW architecture. The EW provider enhances their profitability by reducing access choices so arbitrary decisions to reduce access reduces demand for their product, while simultaneously reducing opportunity to profit from user requirements.

An EW initiates payment to a registered EW number which may be an alias for a regular bank account. Users can configure their EW to make anonymous payments and so no reference to their actual demographic details become part of the FMM, however in many cases payers and payees (and their insurance companies) will want more identifying data to reside in the FMM.

Governments may want EW users to register truthful EW user demographic data at the time of activation of the device, however such intrusiveness may affect the ubiquity of the solution. At the time of initiation of payment, the EW will see all EW within the communication zone requesting payment of an amount. The payer may configure the device to require confirmation of the payee and the payee may configure their EW to send contextual and identifying data to the payer EW. Requiring specific software logic in all EW restricts opportunity for profits, unnecessarily slows transactions, and intrudes on user privacy. For example, a payer may configure an EW in an outdoor venue such as a State Fair, to always pay an EW requesting the same amount as expected without further consideration, however, prudent EW payers may want to see the payee name before transmitting value to an unidentified device. The payer then will see payment destinations such as “hot dog stand # 6” or “roller coaster operator” for the expected transaction. If the payee has not configured its EW to transmit the data to the payer, then the payee may not receive payment from payers demanding authentication of the payee EW. EW providers will create authentication of payee EW as profit drivers just as ID protection providers receive profit by protecting user identities. For example, some firms will sell services that allow EW users to register their devices with them so they can authenticate an EW number belongs to the registered entity, however there is no requirement for such a service.

U.2.2: What information about a Payee does Payer need to know in order to initiate a payment?

The payer needs its EW to receive an EW unique identifying number which may be an alias for a bank account. If the payee EW identifying number is an alias for a bank account, then funds only go one way; Payees have one EW alias to receive payment and one EW identifying number to initiate payment for a single FI account. FI and insurance companies likely will require its users using EW to initiate transfer of funds from an FI account to an EW account to use a minimum set of security features preventing “friendly
These closely coupled EW/FI account will by necessity be less private than the minimal knowledge needed by an uncoupled MM application, however such a product may prove to be useful for some payers and payees.

0U.3.1: In terms of baseline core features, "how do Payer and Payees negotiate payments prior to the transport of MM to Payee"?

Negotiations can be simple or complex. For example, a simple negotiation between a payer and payee is a verbal agreement of price swiftly followed by payment transmission. Payers and payees, however, may wish to select from a continually growing list of options which allow electronic negotiations to occur without human intervention. For example, a payer may have configured an EW as follows:

- Pay Euros first, then dollars, then yen
- Do not pay if location is a casino
- Get a second authorization if amount exceeds pre-set limit
- Do not pay for a used car
- Never pay for warranties over 5% of purchase price
- Do not pay sales tax
- Pay excise taxes except in the State of Georgia
- Do not pay if location is a bakery

A payee for the same transaction may have configured an EW as follows:

- Do not accept Euros
- I am an individual without other identity
- Accept any value of payment
- Do not accept payments from Olly Molly
- Pay all taxes for this jurisdiction as separate payments to each taxer
- Always categorize payments; interrupt user if payment has no category
- Do not accept anonymous payments
- Only ID x can make changes to acceptance rules

Since the language of the logic of each EW conforms to standards the negotiation takes only a few milliseconds per bulleted expression.

U.3.4: What is the baseline set of features provided to the end user? What does it mean to be configurable by the Payee? How will this be done? Please give an example using security, authorization or contextual data.

An EW can transmit and receive MM. An EW follows the logic of an EW using an infinite number of switches sold by EW providers and independent software providers which have applications approved for use.

---

10 Friendly fraud is when the owner of an account claims unauthorized use of funds that in actuality the user did authorize the use of funds.
For example, a protoplasm walking around in the universe determines it needs to buy an apple. However, it only wants to buy apples and it only wants to receive money from other protoplasm. Fortunately another protoplasm designed a MM for its fellows and once loaded into an EW it determines from electronic negotiation that the current purchase is indeed an apple an no funds are resident that did not come from other protoplasm. The sale succeeds.

U.4.1: Please explain how contextual data can be transferred or associated with the payment, what format is used, how it is standardized and customized, and what needs to be created by a technical standards committee

Contextual data will be placed in the FMM using tagged fields created by a standards body. For example, the tiddlywink association of outer Mongolia (OMTA) wants to ensure that purchasers know that they are purchasing genuine Outer Mongolian tiddlywinks and not allow the purchase to succeed if the seller is not a registered OMTA provider. The association writes and tests an application for OMTA members or its enthusiasts. OMTA gives the object code to the Outer Mongolian Economic Standards Committee (OMESC) which loads the MM into its testing EW. After insuring that the MM functions as advertised and does not interact inappropriately with other EW MM, the OMSC certifies the MM for all tenders using the Tugrik currency for purchases of Outer Mongolian tiddlywinks. As the demand for Mongolian tiddlywinks increases and international payers surface using currency other than the Tugrik, and as payer outrage from substandard tiddlywinks draws OMTA concern, the OMTA requests the Asian standards board to approve its MM for purchases in Yen or Yuan. The OMTA uses an xml tag “малтатас_good”. It is set if the registration number and location of the sale originate from a bono fide OMTA seller and the tag is checked if the payer attempts to purchase counterfeit Outer Mongolian tiddlywinks. The EW hypervisor (single threaded CPU logic resident in EW and approved for use by Standards committees) then checks the memory set by MM to determine if a MM prevents movement of MM from the current EW. In our case the purchase happily completes and the “Approved by the OMTA“ field is set in the FMM. The field “ABOMTA” becomes a registered trademark and the tag <ABOMTA>1</ABOMTA> can only be set in the FMM by a valid OMTA MM.

U.4.2: How will the Solution enable easy integration with interfacing business and personal finance systems?

It is possible to transmit using current POS if the EW can transmit a magnetic wave that conforms to a 3 track read of a magnetic stripe. ISO/IEC 7813:2006(en) allows 226 bytes of data available for a mag stripe reader. A 226 byte structure less controlling beginning and ending bytes; semaphores, and other data, say 200 bytes for MM, allows a brief FMM and the other mandatory requirements for a MM transmission. However, only freshly minted FMM without long circulation history will be less than 220 bytes. Therefore, to be usable, governments must allow truncation and collapse of FMM data for small value retail sales, say under 999,999,999 units of value.

U.5.1: Please explain how "review of proposed payment across jurisdiction becomes part of the negotiation messages between Payer and Payees" by providing a step by step description of how money would move cross border starting from initiation to settlement

Users configure their EW to accept or transmit all currency or some currency. Currently there are approximately 150 currencies recognized by the United Nations. Users can configure their EW with MM governing payment type. For example, a user may use a commercial MM to allow all currencies, some currencies, or only one specific currency. MM arrive in an
EW with a value of the number of smallest monetary units for a UN recognized currency. The EW will also contain MM that allow the EW to convert currency by transmitting the MM to the issuing central bank or its agent and requesting the equivalent value be transmitted to an EW or another account. Governments provide MM with logic to assess the legality of cross border payments so EW use its logic to conform to local law governing payment to payees outside of a geographical locale. EW users can override government MM but likely will lose insurance covering such payments. Anonymous transfer of value is not anonymous because elements of a transaction remain within an EW or payment archives. At a minimum, data elements within the blockchain of a FMM will contain the standard elements however a geocode of the payer and payee must also be present for cross border transactions. The currency type and the number of lowest value of currency units are already standard data elements; geocodes for payers and payees as elements of the FMM are optional but likely will be required by law, yet the games of smugglers and other black market participants will configure EW to violate law. Ubiquity of the currency relies on the payers and payees to remain anonymous regardless of laws requiring them to declare their activity. Forensic evidence exists; courts decide if the arguments from advisories about the forensic evidence from MM are relevant, or not.

The step by step solution to a cross border payment is the same as any other payment. The payer finds the payee EW and moves a MM to it. Users redeem MM from central banks or their agents. Cross border payments or strictly domestic payments do not change the mechanics of a monetary movement although law may require more information about the activity.

U.5.2: How can MM be interoperable with other faster payment solutions such as the UK Faster Payments Service?

UK payments require FI to be party to a transaction, whereas MM do not require FI to circulate. This fundamental difference makes the two methods of payment incompatible.

Efficiency

E.1.2: How are EWs created and are they linked to users or Providers? How would a user switch Providers and maintain their EW or do they need to switch and obtain a new EW from the new Provider?

Licensed firms create EW and use other licensed firms to add MM to EW. Once a person purchases or otherwise receives an EW it is their property and the MM within it are also that person’s property. People will obtain as many EW for the varied uses of specific types of payments as their activity requires. EW providers likely will create features for their product as marketing ploys, not unlike car manufacturers creating features to sell their products.

E.1.3: How will you ensure adequate levels of disclosure of to end users to ensure competition based on transparency and user choice?

Public laws govern competition and information provided to payers. The MM concept is public laws govern its use and the protection of payers and payees.

E.2.1: How will Providers integrate with the Solution? Please provide a step by step example

A customer buys an EW from a licensed provider and pays for the MM loaded into it from any source offering MM for EW. Providers do not participate in the circulation of MM.

E.2.1: Please provide more detail on what a "module" is, how it works, and a description of the end user experience with a module in the context of provision of a value-added service
Modules are the primary elements of the solution; some MM are required such as the FMM or the BOLMM, but many MM residing in an EW are present by consumer choice. MM allow members of society to codify their payment choices and let a device use the logic they want applied to a payment. My vision for the currency is as follows:

- Person buys an EW
- Person purchases MM
- Person spends MM
- Person buys more MM
- Person spends more MM
- Person has remorse from a payment and loads a new MM governing their payment choice. For example, person does not want to pay more than a specified amount for a specified purpose. Person constructs or buys MM limiting the amount for such a purpose and then adds other MM to further architect their payment choice.

E.3.1: Please provide more detail on the implementation plan, particularly for where new standards and builds are needed

As a payment system architect, I am a lousy implementer. My plans for implementation are simple, give the idea to a central bank and let the central bank implement the design. However, knowing that as an implementer I am a duck out of water, I would start using a local FI in a chosen geography with a good number of payers and payees that will want to use the currency. I then would monitor the pilot operation and have smart people write reports about its issuance, circulation, and redemption that would influence standards committees and governments to write controlling modules that would not limit payer choices or needlessly interfere with anonymous transactions but would increase the logic used by payers and payees to conduct transactions more intelligently than they can do currently.

E.4.1: How will the Solution’s message format be interoperable with existing payment format standards and with the ISO20022 message format? Please describe how the Solution “conforms to ISO20022 tagged structure.”

MM uses tagged fields.

E.4.4: What is the mechanism for updating the message format? Is it a consensus mechanism to update the blockchain?

Only the BOLMM updates the FMM and central banks create and replace the logic to update the blockchain (FMM) as needed. Central banks control revocation of currency and insurers use published protocols to pay customers for losses. Standard data elements in the blockchain will remain constant, however new tagged fields created by all in society will create a huge FMMs with elements consumers want as a record of transactions. Anonymity remains paramount for social acceptance, however, only if users want anonymity. It is the combination of government control and social manipulation that makes the currency acceptable.

E.6.2: What are the peak volumes and value you expect? How will you scale to accommodate this and ensure the level of security and response time required?

I expect that in the US we would see about 90% of M1 circulation, however the math the provides that projection is dubious at best. Security provided by asynchronous encryption and public and private signatures is not limited by the value or quantity of circulating MM.
E.7.1: What tools and protocols will be provided for addressing exceptions?

Any exception revokes the MM involved in a transaction. Insurers likely will immediately replace revoked MM and EW users may never know their insurer replace a MM for cause.

S.1.1: How will the government ensure all EW receive and adopt the updated logic?

BOLMM will go first to regions under attack, and roll out; logic works the same way as determining if encryption keys need to be changed or POS devices needs an upgrade, i.e. at time of use. Simultaneous update of all MM in circulation is not obtainable or desirable.

S.1: Please provide more detail on the sub-criteria, if and where available to address the above Question is too vague for response.

S.2: What does the proposal mean by “Payers configure their own authorization procedures using software hosted in the EW”? What are examples of how the authorization procedures may differ?

Users configure their wallets from their perception of payment risk. For example, A consumer may configure a simple EW to ask for a PW and a fingerprint before it presents a pay option or shows value. Corporate treasury EW may ask for more evidence of authorized payers including co-signers, or executive review before value moves.

S.3.3: What mechanisms and processes will be provided to protect or compensate Payers in cases of disputes? How Payers without the ability to purchase insurance modules be protected?

Disputes outside of a normal insurance company automatic payments for loss, will be addressed by the courts of competent jurisdiction. Insurance rates will be highly competitive since unauthorized movement of MM results in its revocation limiting actual losses.

S.4: While the solution transfers MM in real-time, the settlement process when redeeming MM needs further clarity (S.4.1). While the FI is required to settle via RTGS (real-time gross settlement) with the central bank for the redemption (S.4.3), what existing settlement mechanism is used, how frequently settlement occurs — e.g., next available window, next day, immediate, etc., and how the Solution will manage any credit or liquidity exposure are not described (S.4.1, S.4.2).

Central banks implement a redemption strategy, however, there is no reason why redemptions cannot occur 24 hours every day, for seven days a week, for all 365 days in a year. Validation of MM is electronic and only needs a validation portal to accept a redemption request, however movement of funds can only occur during bank operating hours. It is possible that third party redeemers may build an industry based on the payment of cash for MM immediately at any time for a percentage of the redemption amount; it also possible that such commercial operations will force to legislatures to enact laws to prevent abuses.

Credit risks occur only if central banks issue MM without its purchase. Liquidity risks occur because of treasury (private or public) operations and is no different than such operations occurring every day. Consider MM as cash and so the same vulnerabilities that exist with cash, exist with MM.

S.5.1, S.5.2: Which, if any, insurance and consumer protection modules are mandatory versus voluntary? How will these be developed?

EW have no requirements except for the ability to transfer and store standard MM. However, consumer demand will build requirements for specific MM security and other features. The original issuance of MM may have more strident requirements since its cycles will not be
well understood, yet in time, issuing central banks likely will reduce the rules governing each cycle.

S.5.3: What is the mechanisms for requesting prompt voluntary return of funds?

If a MM payee does not receive an expected transfer, then the payee EW revokes the MM; the revocation triggers the insurance module to replace the loss. The original MM become worthless and any attempt to redeem it will cause law enforcement reaction.

S.5.4, S.5.5: How would disputes be handled for non-insureders?

Existing laws governing theft, fraud, and other financial crimes also protect MM users.

S.6: Please share more information if available on fraud information sharing

Thought Matrix Consulting developed a proprietary method for detecting fraud named “Bad Ed”, (Behavior Detection, Evasion Detection). The methodology has the advantage of not producing false positive alerts although false negatives exist. The false negative/false positive ratio is critical for the detection of fraud and likely can be applied very successfully for monitoring EW activity.

All MM will eventually be archived and can be reviewed by authorities reviewing payer and payee behavior and claims of malfeasance can be substantiated by examination of the block chain contained in FMM.

S.7: Please provide more detail and examples, where possible, on how the Solution meets the subcriteria within Security Controls

The assessment criteria have the following goals:

“Security controls means that the Solution has layered and robust technical, access, operational, procedural, and managerial controls to address and foster security, including but not limited to the integrity and protection of confidential, private and sensitive Data.

S.7.1 The Solution should provide strong technical access components and controls, including –

• Identity verification and access management
• Data encryption in-transit and at-rest
• Data quality and integrity controls
• Data breach prevention and detection
• Layered security controls (e.g., The Open Systems Interconnect, OSI)
• Components and controls that leverage and are consistent with industry standards (e.g., NIST, ISO, ANSI).

S.7.2 The Solution should provide strong operational and procedural components and controls, including –

• Data retention and disposal controls

The solution uses the following methods as previously described:

• Identity verification an access management is configurable based on user perception of risk.
• The solution uses asynchronous keys to encrypt data and validate that the seals have not been compromised
• Data breach revokes the seal. There are other proprietary methods for other detection of highly probable attacks.
• Security controls are found in the seal, by encryption of data entering and exiting the FMM and from the use of detection and authentication methods users placed in their EW.
• The use of standards increase the acceptance of the currency and reduce costs for all parties.
• Users can keep electronic data and the contextual data from transactions as they see fit. The central bank archive houses all spent or revoked MM.

S.8: Please provide more detail, where possible, on how the Solution meets the subcriteria within Resiliency

The FTPTF developed the following criteria for resiliency:

“Resiliency means that the Solution has mechanisms and systems to ensure high levels of end-to-end availability and reliability under normal and stressed operating conditions. S.8.1 The Solution should define its target availability metrics and describe its approach to ensure those metrics can be achieved.
S.8.2 The Solution should have business continuity and disaster recovery plans to ensure timely recovery and resumption of critical services in the event of an outage or a cyber-attack.
S.8.3 The Solution should have mechanisms to minimize the chance that an adverse Solution-related event will cause other market participants to fail to meet their obligations (i.e., trigger systemic risk).
S.8.4 The Solution should demonstrate that sufficient resources are devoted to business continuity and resiliency.
S.8.5 The Solution should conduct regular contingency testing across all operators and providers of its end-to-end systems. “

Measurement of MM occurs by broadcast messages from the central bank to targeted circulating MM including all circulating MM or a subset of MM. Occasionally, because of user geographic location, individual MMs may not be available but the measures can be updated once the MM enter a communication zone. The broadcast messages are uniquely identified so MM know if it responded already on the specific query. FMM are also identified by unique identifiers so central banks know which MM have yet to respond to a query.

The design allows the central bank to swap out the BOLMM so identified cyber-attacks have available defense mechanism that will prevent affected MM from movement (revocation) or install an antidote against the attack. Revoked currency are replace by insurance companies and have the revoked currency replaced by central banks on forensic proof that it was compromised.

The immediate replacement of revoked currency prevents high systemic risk vulnerability.

Firms can create methods for generating insurance claims so replacement will be a function of time, amount, positive forensic evidence of MM compromise. Insurance companies will allow firms to reduce their exposure to attack by buying recommended MM governing security on EW.
Tests of all the functions of MM should be routine and systematic. If a central bank changes the MM architecture, then prudence requires a battery of tests including developing tested contingencies to determine if plans work with circulating currency.

S.9.1: What requirements are made of Providers (EWs, financial institutions, RNAPs) on protection of sensitive information?

The rules have yet to be developed.

S.9.2, S.9.3: What information is needed by the Payer and Payee to complete account setup, transaction setup, problem solution and to complete a payment? Do Payers need to know Payee account numbers?

Account setup will differ widely depending on the user requirements for security. All payees and payers will need the unique EW ID number with a pre-configured ID (not necessarily unique) able to give more human identification of the unique EW ID. For example, an EW ID may be 1020 (not a real world example way because it is way too short) but the payer configures it to broadcast “Ed’s bags of coins” which the payee knows to be valid for the transaction being conducted.

S.10.1: Please explain what it means to have end users “configure” authentication – “User controls function in resident EW to provide user authentication and prevent intrusion”

Users may not want their EW to authenticate them at all, however ill advised that course of action is. The scale of controls then can be nothing or on the other side you may have a Multi-national corporation storing MM in its payroll EW, which would have the controls adequate to protect such a large pool of MM.

S.10.1: What is the framework that operators and Providers (EWs, financial institutions, RNAPs) will use to authenticate providers and end users? What is the baseline level enforced by operating rules?

Electronic signatures ensure that EW and other elements of the solution are bona fide participants for their roles.

S.11: Please provide more detail, where possible, on how the Solution meets the subcriteria within Participation requirements

The assessment criteria present the following language defining the criteria:

“Participation requirements means that the Solution should establish and monitor compliance with transparent requisites that Providers must adhere to on an ongoing basis as appropriate to their roles in the Solution.

S.11.1 The Solution’s participation requirements should be adequate to ensure that all Providers adhere to the Solution’s rules and requirements relevant to their role, including those related to security, resiliency, anti-money laundering/know your customer, and Data privacy/integrity protocols. See also criteria S.5-S.10.

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
It is not possible to construct any systems as large as an MM system to have insiders obey all the rules. However, typical controls such as certification of software, licensing of providers, and periodic inspection of security postures will ensure a reasonable amount of compliance. The threat that non-compliance can disqualify a provider or less harsh penalties are available and will likely evolve over time.

The central bank will create compliance rules and reporting requirements for all participants providing equipment or services to differing areas of the MM solution.

Central banks create procedures to allow participants to show proof of taking all measures required of them.

Fast

F.1: How does MM move based on “payer and payee negotiation”? How long does it take? What is the consensus mechanism in the blockchain, if any, and how long does that negotiation take?

Question was answered see above.

F.2: Please explain what happens when Payers and Payees negotiate a payment and the expected time it will take (e.g., page 35: “EW payees set expected time of receipt that begins when negotiations messages finish and an agreement exists between payer and payee.” “Payers may prevent MM from transport until agreement exists between payer and payees.” “Payees have access to MM after expected transport time as modified by payer and payee conditions and 400 milliseconds of validation of currency.”

If payers and payees have long lists of criteria for valid transactions, then negotiations take longer. If the distance separating users is long, then the transaction will take longer. If the MM are traveling at the speed of light, then the transmission will be shorter than if the MM move over sound waves. For example, if the transaction is moving across a fiber cable at 181,000 miles per second, terrestrial travel time will be negligible.

F.4: When an end user redeems MM at a Financial Institution where he/she is not a customer, and receives physical cash in return, please explain step by step how the Financial Institution settles (move money) either with the end user’s Financial Institution or with the Central Bank

Consider cashing a demand deposit instrument at the issuing institution

FI or others can keep MM in circulation available to give to their customers as required. However, it behooves central banks to required redemptions under certain conditions such as FMM being too lengthy. If the central banks wish to remove MM from circulation, then costs to redeem them go down. If the central bank wishes to keep more MM in circulation, then costs for redemptions rise. FI must receive funds for redemptions immediately.

Legal

L.1: Please provide more detail, where possible, on how the Solution meets the subcriteria within Legal Framework
Central banks and governments ensure that MM and EW conform to all applicable laws. EW receive government MM governing payment in specific locations.

L.2: Please provide more detail, where possible, on how the Solution meets the subcriteria within Payment system rules

Since government provide legal logic for all transactions only those that risk turning off the government MM (perhaps not possible in some configurations) risk not complying with current law. Central banks may also provide some governing logic such as logic preventing risky behavior when detected.

L.3: Please provide more detail on the “consumer protection modules” and the “insurance modules” – who develops the modules, what functionality do the modules contain around consumer protection, where does the end-user obtains the modules, and a description of the user experience

Insurance companies (or their software providers) prepare the insurance modules. Technical committees test and license insurer MM. Consumer protection modules are those developed by firms committed to consumer protection. End users can receive these approved MM from those firms that built them, or their agents.

L.4: Please provide more detail, where possible, on how the Solution meets the subcriteria within Data privacy

There are strong controls preventing data transmission of any contextual field or other element that is not required in a transaction. Although bona fide government researchers likely will be able to identify payers and payees from their unique EW ID, those types of details will be restricted to court ordered actions.

L.5: Please provide more detail, where possible, on how the Solution meets the subcriteria within Intellectual property

MM providers can receive copyrights or patents protecting their proprietary designs.

Governance

G.1: Please provide more detail, where possible, on how the Solution meets the subcriteria within Effective governance

Rules for governance will be published and enforced by the root issuing FI. However, with luck central banks will set up procedures to include those that want effective and better governance of MM.

G.2: Please provide more detail, where possible, on how the Solution meets the subcriteria within Inclusive governance

The details of effective inclusive governance must be developed by the central banks and are outside the scope of this design. By providing a governance model the design usurps improperly the role of the central bank.
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: Thought Matrix Consulting, LLC

Summary Description of Solution:

Money Modules (MM) is a new electronic currency based on block chain technology. It comprises standardized software, data modules, and the electronic wallets (EWs) that host them. The fundamental Money Module (FMM) is a block chain, and each record within the chain contains the issuer, a unique transaction ID, the issuer’s public electronic signature, the date issued, the fiat currency type, and the amount. The central bank issues the FMM, which then moves from the central bank to commercial banks, then to retail banks, and then to users’ electronic wallets, where the currency is broken down into smaller amounts. The module’s ancestry is always shown in the block chain. Access to read and to write to the FMM is allowed by the security module, which transfers money and updates the block chain upon instruction from an authorized EW approved by the central bank. EW applications make a standard call to a security module called “Break-Out Logic” (BOL-MM) that is created by central banks. Break-Out Logic receives arguments as designated by a standards committee to select the FMM, create new FMM, transfer the requested value, and update the FMM with the residual value. Firms and individuals redeem MM by submitting MM values to financial institutions, which convert the values in EW to local fiat currency as cash or value in a stored-value account. Redemption removes FMM data from an EW and moves it to government archival storage units.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths
  – The central bank issues MM as fiat currency and is responsible for governing and approving Electronic Wallets, thus increasing the likelihood of public trust in the system.
  – As anyone can have and receive MM, MM EWs can become portable bank accounts for the unbanked. An MM account may be acquired at any bank or distributor and redeemed at any bank or non-bank. The proposal states that the government may consider giving basic EWs to unbanked payers and payees.
  – The Solution is customizable and configurable by providers and end-users, particularly for security.
  – The MM solution defines a new payment life cycle (issue, circulate, redeem).
  – The Solution offers fast validation of MM (400-millisecond speed) and immediate availability of good funds to the payee after validation of MM.

■ Areas for improvement and enhancement
  – To be broadly effective, the Solution must first win support from the central bank. The proposal does not outline a plan for gaining central bank support or for encouraging broad end-user adoption.
  – Unless the central bank issues a mandate to accept MM as legal tender, adoption could prove challenging, since depository institutions would have to forfeit the revenue associated with current payment systems, and commercial firms would need to develop new EW functionality and products.
  – Another potential hindrance to adoption is the assumption that a central bank (e.g., the Federal Reserve) will fund the costs associated with maintenance, production, and immediate
distribution of BOLMM to all circulating MM on a cost basis (similar to the way the Federal Reserve charges for FedWire). While the proposal notes that MM move based on payer and payee negotiations, the consensus mechanism used to update the block chain, the speed by which the block chain can be updated through this consensus mechanism, and the governance for updating the block chain are not clearly explained.

- The proposal states that security controls between the payer and payee are “configurable” and that often “payers and payees enact security procedures as they deem fit” (page 32), potentially allowing transactions to be made with only the most basic security.

- The Solution relies on critical “modules,” including security, transmission, reception, legal controller, broadcast response, and—particularly important—insurance and consumer protection modules. More clarity is needed as to how these modules will be developed, how they will work, and how the end-user will interact with them.

- The Solution has not defined several important elements of the faster payment solution, including: rules or a process for resolving disputes (rather, it relies largely on the court system for resolution), fraud information-sharing capabilities, risk and legal frameworks, and a governance model. The proposer states that the provision of contextual data depends on the development of actual tags by a technical standards committee, which is best done through consensus among a broad group of users.

- **Use cases addressed**

- **Proposer’s overall ability to deliver proposed solution**
  - The Solution is innovative and conceptual, as the FMM, EW, BOLMM and other modules are not yet developed or implemented.

  - The implementation plan provided is high-level. A more detailed plan is needed that includes the approach, timeline, hurdles, and requirements for all of the Solution’s dependencies, including: a technical standards committees to develop a tagged structure; creation of a permanent, secure payment data archive of all spent and redeemed FMM; a committee to approve electronic wallets; independent bodies to certify authentication solutions using new frameworks developed by the central bank; and rules for issuance, circulation, redemption, and revocation, along with software developed to act on those rules.
Ubiquity

U.1 Accessibility

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The proposed Solution is a digital currency issued and regulated by the Central Bank that can be redeemed for physical cash. The EW account enables anyone to send and receive payments from any account through depository institutions and regulated non-bank account providers (U.1.1). Governments could provide basic EWs to unbanked payers and payees, making the EW a portable bank account for the unbanked (U.1.4). As long as central banks adopt the solution, multi-currency payments are supported (U.1.3).

The Solution could be strengthened by developing a way for entities to reach payees without an existing electronic wallet; however, the proposer does suggest a potential work-around for solving the unbanked challenge: a free, government-issued EW (U.1.2). Further, while the Solution is theoretically accessible to all end-users, it relies on market forces for features such as security, which could leave smaller firms and the unbanked/underserved with limited access to the Solution (U.1.4). In addition, to achieve widespread adoption, central banks, providers, and third parties must adopt the Solution and make it available to end-users. According to the proposal, revenue generation is the motivating factor for adopting the Solution, as it provides retailers with contextual data about payment and offers incentives to EW users to provide contextual data about payees (U.1.5).

U.2 Usability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The EW can store, transmit, and receive MM via almost any electronic device and channel and is available 24x7x365 (U.2.1, U.2.3). However, EW providers determine the channels, devices, and hours of accessibility; the requirements, guidelines, and guardrails that will shape the EW’s usability (the minimum features required) are not stated (U.2.4). The proposer suggests that market forces will dictate which features become baseline features, but the proposal could be strengthened by suggesting which features and functionalities should be part of this baseline.

The Solution enables an entity to initiate a payment with limited information such as a name, email address, or phone number, but requires separate EW identifying numbers for both initiating and receiving a payment (U.2.2).

The Solution is consciously designed with a trade-off, as it prioritizes flexibility and adaptability over consistency in user experience.

U.3 Predictability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The Solution’s design ensures a baseline experience for issuance, circulation, and redemption of MM across channels, devices, and providers (U.3.1, U.3.4). While the end-user can configure
the EW to enable a personal customer experience, the solution uses communication and messaging protocols for functions such as the calls between EW and other modules (e.g., BOLMM and FMM) (U.3.3).

As discussed in U.2, the proposer’s vision for the Solution is rooted in flexibility and end-user customization; consequently, there is a risk that each payment and payee/payer will present a unique use case. As such, the predictability of each transaction may be questionable.

To strengthen the proposal, the proposer can: (1) clearly articulate the baseline experience; (2) develop operating rules to frame and communicate a common, core set of features and functionality, by device and channel; and (3) clearly explain how baseline features will be communicated to end-users (U.3.2). Further, while the proposal maintains that the Solution’s technical ability minimizes errors and states that a governing body will address error resolution, it would be beneficial to describe an error resolution process (U.3.5).

**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 relies on EW providers to sell standard functions for EW users, including security controls and contextual data (U.4.1). EW providers will design the data transmission to EW users, although central banks will propagate standards for transferring value and contextual data from EW to EW (U.4.3). To include contextual data in the FMM, the Solution leverages XML-tagged fields created by a standards body.

While still conceptual in nature, the design and proposal can be strengthened by providing details of the actual capabilities of the contextual data, including how it will be included with the payment, what message format will be used, and how the contextual data can be customized (U.4.1). (The Solution has ISO20022-tagged structure, but these tags must be created by a technical standards committee.) The proposal should also address how the Solution will interface with business or personal finance systems (U.4.2).

**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 enables cross-border payment if—and only if—governments and central banks create standards for receiving and transmitting FMM across borders, and EW providers offer cross-border functionality to end-users (U.5.1). Currency conversion only occurs when users redeem their FMM from issuing FI networks (U.5.4).

The Solution will support cross-border functionality at launch, as it can be configured to accept or transmit any or all of the approximately 150 currencies recognized by the United Nations. But it is not likely to be broadly adopted quickly, as central banks and governments must first create the standards necessary for receiving or transmitting foreign-value FMM in a cross-border setting. The proposal could be enhanced by detailing a plan for securing central banks’ and governments’ commitment to accept the Solution and persuading them to create the appropriate standards (U.5.5).
Additionally, detailing how the Solution allows for interoperability with other faster payment solutions in other countries (U.5.2) without requiring them to use Money Modules would be beneficial, as this information would shed light on the likelihood of, and potential challenges to, cross-border adoption. (As an illustration, the proposer maintains that requiring an FI to be a party to a transaction in the UK would be incompatible with the Solution, as MM do not require FIs to circulate.) Additionally, developing operational rules that formally require providers to disclose costs, timing, and risks in advance to the payer would add clarity to the proposal (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 provides the necessary features and functionality to meet the needs of the four major use cases (P2P, P2B, B2P, and B2B).

### 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 relies on the development of value-added services such as EW applications and modules from numerous service providers (E.1.1, E.1.4). It leaves pricing, features, and services completely up to providers and individuals based on market demand. Since providers do not have to be FIs, competition can be broad and based on value-added services, not just on price.

Once someone purchases or receives an EW, it is his/her property, and s/he can obtain as many EW as s/he needs for various, specific uses. The proposer expects EW providers to develop features for the products, further supporting the market-based nature of the Solution’s design. The proposal suggests that public law will govern the use of MM and the protection of its payers and payees (E.1.3).

The Solution’s dependence on the market for so much of its infrastructure is a slight concern. Without the provision of minimum features and/or preconfigured ways to access the Solution, smaller providers may not be able to compete as effectively (E.1.4).

#### 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:**
Value-added services will serve as the main differentiator among providers of various sizes and incumencies (E.2.2). Users will purchase these services (including security) based on their needs. Disclosure that value-added services are optional will occur during payer and payee negotiations, if allowed by the user's EW (E.2.3).
Because the Solution is a digital currency, providers do not participate in the circulation of MM. The proposal could be strengthened by articulating how an EW provider can “integrate” with the Fundamental Money Module (E.2.1). Further, because the Solution’s design affords an almost limitless capability to develop and offer value-added services, the proposal can be bolstered by laying out a clear process (e.g., use of open APIs, etc.) for enabling these services, with specifics about the ease or difficulty of doing so.

The Solution relies on third-party firms to develop “modules” such as transmission, reception, legal controller, insurance, consumer protection modules; there are even government modules that govern all taxes related to transactions. It would be helpful to understand how these modules work and how end-users interact with them.

### 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 implementation timeline is seven months for development and one year for pilot and rollout, which is scheduled for 2017. Critical to the timeline, however, is central banks’ agreement to: (1) adopt the solution, (2) potentially agree to distribute free EWs to unbanked/underbanked users, and (3) commit to significant new builds that are needed such as standards, specialized EW and secure transmission pipes, security layers, and equipment upgrades to enable acceptance of MM.

The proposal could be strengthened by adding more detail to its high-level implementation plan. Details might include the full timeline for new builds, initial adoption, and the path to ubiquity; funding plans; implementation and ubiquity hurdles, with plans to overcome them; and projected growth estimates (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 payment format standards are rooted in the ISO20022 XML-tagged structure; however, a technical standards committee must create the actual tags (E.4.5).

The proposal states, “Only the BOLMM updates the FMM, and central banks create and replace the logic to update the block chain (FMM) as needed.” The proposal could be strengthened by outlining how the new standards will interface with existing payment format standards.

### 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 MM solution defines a new payment life cycle (issuance, circulation, redemption) that covers all stages of the process (E.5.1). Its technical design supports all of its features (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:**

The Solution’s technical design as described supports projected use cases and is adaptable (E.6.1, E.6.3) based on updates to BOLMM by the central bank. Essentially, the central bank determines how the Solution’s technical design must be changed to adapt to ongoing developments and then distributes those changes through software updates.

The proposal describes ways to accommodate increased transaction volumes and flow rates, but it does not substantiate this purported scalability with specific projections and timelines beyond anticipating we would see roughly 90% of M1 circulation (E.6.2).

The proposal could be improved by discussing plans for accommodating the level of central bank capacity and security required to handle peak transaction volume (E.6.2); the Proposer suggests that the security provided by public and private signatures does not depend on the value or quantity of MM in the marketplace.

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 expects the central bank to provide an archive for all revoked or spent FMM. The archive can be used in court proceedings in case of dispute (E.7.2). While the Solution calls for the MM involved in an exception to be revoked immediately and replaced by an insurer, the proposal can be strengthened by discussing what happens if an exception is created and the issuing party does not have insurance.

The Solution’s design can be made more robust by including plans and requirements for tools, messages, alerts, notifications, and related protocols to support exception-handling (E.7.1). Additionally, the Solution should aggregate exceptions data to spot patterns not visible at the individual-participant level (E.7.3). In addition, while it may be a nice configuration option, the user’s ability to “turn off” transaction visibility to the central bank means that some data cannot be used to support the exceptions and investigations process (E.7.1, E.7.3).

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:**

The Solution’s design focuses on minimizing risk through security measures that confirm that MM are legitimate. With software version changes distributed by the government, the EW receives updated logic that addresses unexpected applications of laws and regulations (S.1.1). The validation process is meant to ensure that circulating MM are legitimate (S.1.4). The design of the system is such that any MM involved in an exceptions transaction will be immediately revoked and taken out of circulation; it is expected that insurers would
immediately replace the revoked MM. The government will ensure that EWs receive and adopt updated security logic by first going to specific regions under attack and beginning the roll-out there.

The proposal can be strengthened by addressing the operational risks related to deficiencies in information systems or internal processes (S.1.3). Additionally, to help prevent fraudulent payments, the proposal should articulate any baseline level of authentication security required of EW providers (i.e., delineate what is required in a commercial firm’s authentication module versus what is configurable by payers). The proposal can be improved further by clearly describing the Solution’s incentives to providers and operators to address and contain the risks they may pose to other participants, as well as by explaining how the periodic review and update of the risk management framework is expected to work (S.1.5-6).

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:**

The solution includes pre-authorization capability; the proposal states, “Payers can select the timeframe for payment or allow payees to control debits from payer EW. Payers revoke payment on demand until the payment moves to payees. All payer parameters may be changed prior to payment” (page 30) (S.2.2-3).

A significant amount of flexibility is built into the Solution; for example, a user may configure his/her wallet to ask for a password and fingerprint before presenting a payment option or showing value, corporate treasurers may ask for additional evidence of authorized payers, etc.

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:**

As a digital cash solution, the Solution does not require FIs’ approval of transactions (S.3.1). The payment is final when an EW or FI receives MM from an authorized source and confirms the authenticity of value (page 31). This confirmation (MM authentication) is expected to take no longer than 400 milliseconds after receipt by the EW (S.3.2). The courts will address disputes that go beyond automatic reimbursement by insurance companies.

The Solution does not specifically provide mechanisms and processes to protect or compensate the payer in cases of disputes, but rather depends on: (1) market forces to provide insurance modules that payers will purchase to cover any losses, and (2) the central bank’s archives of redeemed and revoked MM to provide evidence to courts in cases of disputes (S.3.3). The proposal can be strengthened by detailing how the insurance modules work, whether or not they are required to be included in an EW, and how disputes are handled when the payer lacks insurance.
S.4 Settlement approach

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
Transactions conducted within the Solution are settled immediately (S.4.1-2). When redeeming MM for collateralized fiat currency, there is a concern about the amount of cash needed exceeding the amount of cash on hand; the proposal can be strengthened by clearly articulating the process for converting MMIs to collateralized fiat currency.

S.5 Handling disputed payments

**Very Effective**  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
Disputes are handled by revoking the MM involved in the disputed transaction, and insurers are likely to replace the revoked MM in the system. Disputes that go beyond insurance companies’ automatic payments for loss will be handled through “court proceedings” (pp. 37, 54) (S.5.1), which would likely be a lengthy, expensive process. The Solution relies on the EW provider to develop consumer protection models that comply with laws and to offer insurance products to cover losses from disputes (S.5.2). Additionally, it relies on end-users to decide whether or not to adopt these modules.

The proposal should describe the process for requesting the return of a payment (S.5.3). It should also detail an approach for delineating roles, responsibilities, and liability allocation to responsibly protect business, government, and consumer payers (S.5.4-5). As stated in previous Criteria, the proposal should clearly outline what happens if the dispute involves a non-insured payer.

S.6 Fraud information-sharing

**Very Effective**  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
The Solution allows users to configure sharable data from the EW and does not require the sharing of information to facilitate managing and monitoring fraud (S.6.1). The solution does not aggregate, manage, or protect data owned by entities other than providers or operators (S.6.2). It only records spent and revoked MM; it thus shares real-time information only when a payment is revoked (S.6.3). All MM will eventually be archived and can be reviewed by anyone reviewing payer or payee behavior. The solution allows for post-fraud analysis, but not for pattern recognition (S.6.7). Sub-criteria S.6.4, S.6.5, and S.6.6 are not addressed in the proposal, although the Solution does require the creation of a central bank archive of transactions (S.6.1, S.6.6).

The proposal can be strengthened in a number of ways related to fraud information-sharing: (1) by requiring that specific data be shared at the Solution-level across providers, (2) by leveraging data to conduct post-transaction analysis to spot fraud patterns, and (3) by defining the types of data that will be shared.
The Solution does have a proprietary component and method for detecting fraud based on behavior and evasion detection.

### 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:**

The proposal addresses security controls related to technical access components and controls, such as asynchronous signatures and encryption used by MM to protect the currency’s integrity and the security seal’s validity (S.7.1). A data breach causes revocation of the security seal. Additional security controls are found in the seal. Data is encrypted both entering and exiting the FMM.

The proposal can be strengthened by detailing the security controls related to operational or procedural components (S.7.2), managerial policies, and oversight (S.7.3). Examples of the additional detail could include: (1) the data retention and disposal controls in place, (2) physical controls, (3) operational controls, (4) communication and network security examples, and (5) how the solution integrates with existing risk management processes and adapts to enterprise-level security architectures.

### 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 design for resiliency is based on replacing compromised MM immediately to protect against systematic risk. The design also allows for the central bank to swap out the BOLMM in the event of a cyber-attack to prevent affected MM from moving in the system. Insurance companies replace the revoked currency; the replacement currency comes from the central bank after forensic proof has established that it was compromised.

The proposal can be strengthened by directly addressing: (1) target availability metrics (S.8.1), (2) the approach to achieving those metrics, (3) the plan for business continuity (BC) or disaster recovery (DR) (S.8.2), (4) the resources devoted to BC and DR (S.8.4), (5) mechanisms to minimize the chance of triggering systemic risk (S.8.3), and, (6) contingency testing of the Solution (S.8.5).

### 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:**

The Solution is designed to promote flexibility and choice. Identity verification and access management are configurable based on the end-user’s perception of risk. The Solution does encrypt data (S.9.2-3), but the proposal could be improved by addressing the requirements of all parties—including EWs and financial institutions—to provide controls and mechanisms to protect sensitive information throughout the entire payments process (S.9.1). Additionally, the
Solution’s design could be enhanced by requiring a minimum level of security controls, which would allow the design to retain its flexibility while ensuring basic, essential security in the Solution (S.9.2-3).

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:**

The Solution allows the central bank to replace the BOLMM at any time and uses various protocols to ensure that authentication module requirements are met. Essentially, it relies on the central bank for updates when new authentication modules are adopted and old ones are decommissioned (S.10.6).

However, the Solution ultimately holds end-users responsible and in control of their own security in the payment process, including authentication. The proposal states that authentication is “configurable” without any baseline level of authentication described (S.10.1, S.10.4). In addition to establishing a baseline level of authentication, the proposal could be strengthened by discussing the potential for risk-weighted authentication as a means of further enhancing security features (S.10.4, S.10.5).

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:**

Participation requirements have not yet been developed, but the proposer does suggest that the rules will include controls such as certification software, licensing of providers, and periodic inspection of security controls (S.11.1). The proposal indicates that the central bank will create compliance rules and reporting requirements for all participants that provide equipment or services to any part of the MM solution.

The proposal can be strengthened by providing details of the participation requirements and a timeline for creation of the rules. The requirements should outline the process to monitor and ensure compliance by all providers against the 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:**

Based on the digital fiat currency concept and the Solution’s good-funds model, approval occurs in a fraction of a second. Approval and transmission of MM occur simultaneously.
F.2 Fast clearing

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
Based on the digital fiat currency concept and the Solution’s good-funds model, the electronic negotiation between EWs is essentially a substitute for clearing operations. Payers or nominated payees validate the MM via central bank points-of-presence. MM validation takes less than 400 milliseconds; however: if payers and payees have long lists of criteria for valid transactions, then the “negotiations” may take longer.

F.3 Fast availability of good funds to payee

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
Payees have access to MM after the expected transport time, as determined by the payer’s and payee’s conditions and 400 milliseconds of currency validation.

The availability of funds to a payee could be slightly delayed (by no more than 10 seconds), however, depending on the amount of contextual data required by the payee and the fact that the contextual data moves across the same connection as the MM, potentially slowing the process.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale
MM is settled immediately when an EW receives it (F.4.1, F.4.3). When redeeming MM for collateralized fiat currency, however, there is a concern about the amount of cash needed exceeding the amount of the cash on hand. The proposal could be strengthened by clearly articulating the process for converting MMs to collateralized fiat currency.

F.5 Prompt visibility of payment status

| Very Effective | Effective | Somewhat Effective | Not Effective |

Rationale:
Immediate notifications of payment status are available in the EW to both payee and payer.
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 proposer assumes that the central bank will ensure that MM and EW conform to all applicable laws. The Solution relies on the EW and government control of EW functionality and logic to support compliance and legal provisions (L.1.4, L.1.5). The EW updates the legal logic when the Solution is first used in a new jurisdiction, although how the EW obtains that information is not described (L.1.1).

The proposal could be strengthened by providing detail on the legal framework, including assessment of gaps (L.1.2), how the participants are legally bound (L.1.3), compliance with current laws (L.1.4), and unique provisions needed (L.1.5).

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 considers many governing bodies to direct and certify the work of EW providers, but the payment system rules have yet to be defined (L.2.1, L.2.4). It is assumed that the governing body(ies) will prove effective and develop the appropriate set of operational rules (L.2.2). The proposal could be enhanced by suggesting which governing body is likely to be the chosen body for the Solution. It can further be improved by requiring the rules to pay particular attention to the remediation process (L.2.5).

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 Solution includes options for end-users to establish additional consumer protections through “consumer protection modules” (L.3.3). The proposal suggests that insurance companies have responsibility for creating the insurance modules, that technical committees will test and license the insurer MM, that firms committed to consumer protection will develop consumer protection modules, etc.

The proposal could be strengthened by detailing the types of protections that would serve as a minimum standard set of protections and by describing which of these is/are configurable (L.3.1 and 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 solution states that users will define their own data privacy controls (L.4.1), users will control their sharing of contextual data based on individual payment negotiations or default EW settings (L.4.4), and that security functions embedded in the EW will block any intrusion attempts or interceptions of MM in transit (L.4.2).

The proposal can be made more robust by outlining an approach to data privacy and links to relevant legal requirements (L.4.1, L.4.2). Further, it should indicate whether/how users are informed of the data being collected on them (if any is collected) and describe the steps taken when data breaches occur (beyond revocation—are there notifications, etc.? ) (L.4.5).

### 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 proposal states that the MM solution does not violate intellectual property law. The proposal can be strengthened by including a proposed approach to managing risk from third-party intellectual property rights (L.5.1).

### 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 issuing FI will publish and enforce the rules for the Solution’s governance, but central banks and governments could possibly take control of this governance (G.1.1). According to the proposal (page 61), all governance documents will be made available to the public (G.1.2).

The proposal could be enhanced by addressing the process whereby appeals of specific decisions are handled (G.1.3). It should also describe how compliance would be independently validated (G.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 proposed governance includes input from stakeholders through government certification committees (G.2.2, G.2.3) and will take into account mitigating procedures for conflicts of interest (G.2.5).

While the proposal discusses the Solution’s governance model at a high level, further information is needed about the model’s composition and dynamics concerning public interests (G.2.1), obtaining input from stakeholders (G.2.2-3), proportionally influencing outcomes (G.2.4), and managing real and perceived conflicts of interest (G.2.5). The proposer suggests that the details of effective inclusive governance must be developed by the central bank and are outside the design scope.
### APPENDIX A: ASSESSMENT SUMMARY

**= QIAT Assessment  ○ = Proposer Self-Assessment

#### UBIQUITY

<table>
<thead>
<tr>
<th>U.1: Accessibility</th>
<th>Very Effect</th>
<th>Effective</th>
<th>Somewhat Effect</th>
<th>Not Effect</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
</tbody>
</table>

#### EFFICIENCY

<table>
<thead>
<tr>
<th>E.1: Enables competition</th>
<th>Very Effect</th>
<th>Effective</th>
<th>Somewhat Effect</th>
<th>Not Effect</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
</tbody>
</table>

#### SAFETY AND SECURITY

<table>
<thead>
<tr>
<th>S.1: Risk management</th>
<th>Very Effect</th>
<th>Effective</th>
<th>Somewhat Effect</th>
<th>Not Effect</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<td>SAFETY AND SECURITY (cont’d)</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.8: Resiliency</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>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPEED (FAST)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.1: Fast approval</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGAL</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1: Legal framework</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1: Effective governance</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

Thought Matrix did not submit further comment.
THOUGHT MATRIX PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

Please share your concerns about this proposal’s assessment against the Effectiveness Criteria.

The solution requires a central bank role; there is no guarantee that a central bank will agree to issue such a fundamental component of the solution. Therefore, I do not believe that the solution is viable, and it should not be assessed against the effectiveness criteria. If we must rate it, I suggest that it be characterized as an academic exercise.

This proposal appeared to have suggestions, not fully thought out solutions. In addition, this proposal does not address B2B, a key requirement for any solution. Stress was placed on "privacy" which hampers KYC requirements. In addition, this solution does not appear to integrate with other solutions and appears to rely on virtual currency.

One of the main shortcomings of this proposal is its brevity. In many instances, the QIAT downgrades the solution because the proposal does not outline the plan for realizing a criterion.

The strength of the system is in its high-speed payment transmission.

The QIAT criticized the system for its lack of consumer protections. The system contemplates a system of payment insurance. Presumably, some entity or entities would pay the premiums to support that system.

U.1 Accessibility should be not very effective, but effective. The system can be appended to allow governments to issue Electronic Wallets, but on its own, the system cannot provide a solution for unbanked consumers. The system is dependent upon government. It is not safe to assume that either the federal government or all state governments would take on this initiative.

U.5: Should be effective, not somewhat effective. The system does support all currencies and will serve all types of use cases provided that there is foreign government assent to supporting B2B.

E.3. Implementation Timeline: Should be very effective, not somewhat effective. The solution can be adapted as soon as a central bank adopts its function. The solution is fast.

S.3. Payment Finality should be not effective, instead of effective. The system is obviously riskier because it offers push (so that the receiver would not have to verify). It does not have a solution process for contested charges. It assumes that insurance will substitute for enforcement.

S.5: Handling disputed payments. This should be not effective, instead of somewhat effective. See above.

L.3: Consumer protections: Should be read as not effective, instead of somewhat effective. In effect, this system substitutes insurance for a legal regime of enforcement of rules. In this system, insurers create
modules; governance bodies regulate the insurers, and consumer groups weigh in on best practices for protections.

U2 Usability: SE rating. The assessment rates usability on its initial state and not after it has been configured by the user. This is akin to rating a modern car as unusable because it has not been configured to a customer’s requirements.

U3 Predictability: SE rating. A flexible application does not make such unpredictable. The rating is absurd on its face.

U5 Cross-Border Functionality: SE Rating. The rating was strictly based on the subjective criteria of likelihood of adoption which is an irrational approach to evaluating its merits. The solution provides cross-border functionality which fits seamlessly into the solution, a fact ignored by the assessment team.

E3 Implementation Time-Line: SE Rating. The assessment bases its time line against its potential political success which has no bearing on the time line. If the assumption is that an implementer accepted the design and created standards then the schedule is realistic.

E6 Scalability and adaptability. A central bank region can issue the currency to its correspondent banks for values demanded by the public. All central banks’ regions can scale issuance operations based on public demand. Repeating digital data as required does not seem to be an over burdensome activity and can be easily accommodated by a modern central bank. The rating is absurd and without merit.

E.7 Exceptions and investigations process. Central banks do not need to operate an archive of spent or revoked MM; however, we believe central banks are a natural resource for such operations because of the expertise associated with central bank operations. The critique seems to evaluate storage as storage of physical items and not data. Thought Matrix Consulting developed a suite of analytical tools based on aggregate data of financial data. These trademarked tools named "Bad Ed" (an acronym for Behavior detection, Evasion detection) are proprietary and thus were not discussed in a public document. The major advantage to the suite of Bad Ed tools is that there are few to no false positive results. The suite will work extremely well with digital currency such as MM. The reviewers seem to think that providing specific approaches to fraud detection affect the efficacy of the solution, which is a horrendous assumption.

S.1 Risk management. Risk management is an evolution process; a dialectic series of attacks and responses which cannot remain static. The assessors seem to think currency design can prevent fraud whereas in reality a new currency creates new and unforeseen attacks and its operational risks cannot be defined until the currency actually circulates in the economy. Since the currency represents value it is assured it will be used in fraudulent schemes, and no convoluted design will prevent it use for fraudulent purposes, as the assessment team knows very well.

S.5 Handling disputed payments. A currency design does not negate the logic of Caveat emptor. A currency does not need to create institutions for handling disputes; society has developed its own
institutions and honed them for many millennia, and those will be quite effective for handling the inevitable disputes arising from human financial transactions using digital values.

S.6 Fraud information-sharing. I did not wish to discuss my trademarked processes for fraud detection. If the Bad Ed suite of fraud detection tools is used in a real-time basis on data entering the archive, would show fraud as it occurred without false positives.

S.7 Security controls. Security controls were described in detail. Operators have the capability of configuring the currency as they see fit and as risks develop. The assessors seem to think a general design needs precise configuration details, which is impossible without a planned implementation. The comments are completely irrelevant.

There is not enough space in this forum to adequately address all the prejudicial and unreasonable opinions of the assessors. Needless to say, TMC believes the paper received biased views.

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 define rules or a process for resolving disputes (it relies largely on the courts); for fraud information and sharing capabilities; for risk, legal and governance frameworks. The solution does not encrypt data.

Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

The QIAT was fairly critical of the proposal, which I my opinion was absolutely fair.

This proposal is another “thought experiment.” It has not been built, is not funded, has not addressed serious technical issues and has no track record. It is also built on the assumption of the involvement of the central bank.

Agree as assessed. Solution proposal is very light on details of key criteria elements.
The proposal heavily relies on central banks and insurance companies to create a coherent framework for making MM accessible. The burden should not be placed on end-users, especially vulnerable consumers, to figure out how to "configure" settings to ensure appropriate levels of security. Dispute handling, likewise, should not rely on consumers and other end-users navigating the court system to get their money back in case of fraud.

Lacking in security criteria as noted by QIAT.

Truly an aspirational submission for adoption by U.S. players.

Proposal does not demonstrate how widespread adoption will be achieved. Legal Framework and Governance are not described.

(1) Speed (2) addresses unbanked/underbanked segment (3) customizable for security features and end-user experience (4) device and channel agnostic.

Heavy dependence upon the FED to issue the currency, other government agencies to regulate the wallets. Concept of moving from push & pull payments to pure issuance, circulation and redemption. Very fast—400 milliseconds. Concerned about how to deploy the configurable security controls between the payer and payee—is there a clean fit? Unclear on critical modules—security, transmission, reception, legal controls. Default to resolve disputes to court systems. Operational risk—many components yet to be developed.

Interesting concept to suggest that the participants purchase insurance to cover payment loss due to fraud, inability to resolve disputes, etc.

Model based on block chain electronic currency/wallet based on modules. Although MM could eventually replace the current US payments systems, there are still a lot of challenges tied to overall adoption of the modules, jurisdiction and adoption throughout use cases. The US Central Bank might be more open to this solution vs. other countries where Central Banks are more restrictive, and, cross-border still remains a challenge for electronic wallets.

For this solution to be effective the Central Bank must embrace it through a mandate so it can be broadly adopted. Overall very challenging to adopt and to implement as a faster payment solution.

Electronic Currency/Electronic Wallets (EW) based on various “Fundamental Money Module (FMM)”—or “Money Modules (MM),” some realistic and others more challenging. Model based on Central Bank issuing the currency and Blockchain being embedded with through the transaction amount Commercial and Retail Banks.

Accessibility is rated too highly, as the proposal does not demonstrate how the solution allows users to reach any and all payees, nor how widespread adoption will be achieved (i.e., true ubiquity). Contextual data capability is rated too highly as the solution does not describe how data elements will be known by all parties sending and receiving information that would flow with a payment. Rules and governance areas are rated too highly as specifics are not provided.
In my agreement I echo statements from the assessment: "To be broadly effective, the Solution must first win support from the central bank. The proposal does not outline a plan for gaining central bank support ..." and “The Solution is innovative and conceptual, as the FMM, EW, BOLMM and other modules are not yet developed or implemented."

New currency based on DLT, issued by central bank. Serves the underbanked. Requires funding and adoption by central bank. Missing guidelines. Does not appear to be a complete solution.

Taken at face value, I believe the proposal was assessed fairly. The reliance on the central bank for the implementation of the solution will be challenging. Similar to other proposals I am not sure that this proposal will be rapidly adopted by core banking providers and their client institutions.

**TASK FORCE SOLUTION-ENRICHING COMMENTS**

**Ubiquity**

Thank you for your submission. I found this concept unique and thoughtful, allowing payment options for the unbanked and moving us closer to a digital currency concept.

While your solution has its strengths, I'm just not sure the greater body of consumers in the U.S. will be open to electronic currency (especially when we continue to struggle to achieve 100% adoption of debit cards).

It appears the solution is overly reliant upon the FED. The proposal could be enhanced if there are mechanisms that the solution could be rolled out without extensive assistance from the FED.

While the proposal provides for anyone to have and receive Money Modules (MM), the solution could be enriched if a strategic plan was included that detailed how/if our Central Bank would entertain the issuance of a new payment currency (digital currency) and a new payment rail built on block chain technology.

Describe more specifically what capabilities of the solution would enable the ability to have surety in reaching any other individual in the US.

Built on central bank concept which means only FIs could ever participate, leaving processor to work through FIs, potentially disenfranchising unbanked consumers.

This proposal was unique in its thoughts about the Electronic Wallet, EW, and how it would be utilized by consumers. The proposal did state that the government might consider giving a bare bones EW to the unbanked and this system could be used as a portable bank account for many users. However what is the value proposition for consumers? Why would they transition to using such a system? The proposal made the case as to why Central Banks might be interested but did not explain how to drive consumer adoption. Why would I as a government end-user accept this? How would I make payments
to other municipalities and school districts? Unless forced to take this currency, they would still want dollars as they know they can spend it and it doesn't have to be converted.

End-user providers get to select which device and channels it is available on.

Cross-border works only if central banks between countries create standards to receive and transmit.

Since central bank involved, could hinder rapid adoption due to needing to set up infrastructure, etc. Also, debit brands and networks would be very resistant.

The proposed solution leaves too much flexibility in the hands of the providers, leaving no consistent expectation around the end-user experience. This could result in extreme complexity within the solution and create additional adoption barriers. I agree that a baseline should be established.

**Efficiency**

The solution could be enriched by providing a description of the expected end-user’s experience when using the system's core set of features, given the flexibility of the proposed solution.

Conceptual.

Requires central bank.

Who funds the costs of setting up and maintaining the system?

Timeline to implement does not seem realistic given central bank approval and involvement is necessary.

Scalability and adaptability criteria not effectively addressed.

Overall, the proposal is big on generalities and lacks in critical specifics, such as how to address central bank acceptance and how to build a robust exceptions and investigations capability if the end-user has the ability to "turn off" transaction visibility. This last example appears to set up a classic adverse selection scenario which could undermine a significant portion of the offering.

I don't understand who is going to build the Money Modules and would it be possible for them to connect with other potential systems?

**Safety and Security**

Describe further the role that the government is envisioned to take on in security – how is money removed from circulation in the case of fraud (or suspected fraud) and how are parties informed of such?
Who is developing the underlying "module" that will be configurable by the users? It is not clear how this process would work and who would maintain it.

Does not require the sharing of fraud data.

Disputes handled through court proceedings.

End-user data protection based on end-users’ perception of risk.

Proposal would be strengthened with establishment of some baselines for security

In the proposal and through the in-person presentation, recourse options appear to the "the courts" and "insurance", both options the sole responsibility of the end-user to undertake. This again would appear to be a critical hindrance to end-user adoption. More thought in general to security standards, tools, and accountabilities across all parties in the solution is needed.

**Speed (Fast)**

The solution definitely achieves stated objectives for real-time payments.

**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 to include a core set of Rules associated with the Fundamental Money Module (FMM) block chain technology that includes operating rules based on device and channel of the end-user.

Describe more specifically what rules would be needed and their impact on the various players in the payments ecosystem.

Similar to the security facet, more detailed legal framework, system rules and consumer protection recommendations that align all parties’ interests in operating and functioning under a robust payments system of this type is needed.

**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 to include error resolution process and a governance model for the solution. In addition, the solution could be further enriched to provide an overall strategic plan for
cross-border payment governance, given the requirement within the proposal that governments and central banks need to create standards for receiving/transmitting FMM across borders.

Governance would be more effective if all stakeholders had voting rights when specifications are being changed or enhanced.

Provide more details on governance – and any governance role of the private sector vs. expectations of government. Clarify – does the court govern all disputes between all parties?

The governance structure needs to be worked out. Details were scarce and with heavy Central Bank involvement necessary for this to succeed this will be a work in process for a while. I will however add that without involvement of end-users in the governance structure this proposal will be missing critical voices that provide a unique perspective.

Solution relies heavily on government involvement to govern. Unsure if that is palatable, but we believe the idea of government agencies, such as the FED, to own, operate and govern the system would be effective.

G.1 Effective governance & G.2 Inclusive governance – SOMEWHAT EFFECTIVE. Challenging to set up this type of governance model: Left to “independent governance of payment flows by skilled payment system professionals that understand the public policy of policy implementation.”

The “Rules for governance will be published and enforced by the root issuing FI.” Inclusive governance “must be developed by Central Bank “ and accessibility & legal must be given by Central Banks and Governments, with the usability governed by providers’ EW.”
<table>
<thead>
<tr>
<th>Comment</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>The solution requires a central bank role; there is no guarantee that a central bank will agree to issue such a fundamental component of the solution. Therefore, I do not believe that the solution is viable, and it should not be assessed against the effectiveness criteria. If we must rate it, I suggest that it be characterized as an academic exercise.</td>
<td>TMC strongly believes that the central bank role is a critical element to the design for several reasons including new capability to implement fiscal policy and encouraging public trust. Many critics of the design state that a design needs to be a sales pitch and they are mistaken. The only way to determine if the system is not viable is to pilot it and make tweaks based on user experiences. Many of the critics also do not have direct hands-on experience implementing payment systems and so have no really good yardstick to measure its viability other than the effectiveness criteria, which are an abstraction of facets needed for implementation and really only known after an implementation.</td>
</tr>
<tr>
<td>The QIAT was fairly critical of the proposal, which in my opinion was absolutely fair. This proposal is another &quot;thought experiment&quot;. It has not been built, is not funded, has not addressed serious technical issues and has no track record. It is also built on the assumption of the involvement of the central bank.</td>
<td>A design does not need an implementation, in fact implementations typically occur after designs. The reviewer seems to believe that thought has no place in designs, however they do have a place critical to the design process (and also quite useful for reviewing designs).</td>
</tr>
<tr>
<td>Agree as assessed. Solution proposal is very light on details of key criteria elements</td>
<td>It is too early in the design process to make very specific implementation choices. However TMC looks forward to fully defining implementation parameters for various scaled prototypes.</td>
</tr>
<tr>
<td>The proposal heavily relies on central banks and insurance companies to create a coherent framework for making MM accessible. The burden should not be placed on end-users, especially vulnerable consumers, to figure out how to &quot;configure&quot; settings to ensure appropriate levels of security. Dispute handling, likewise, should not rely on consumers and other end-users navigating the court system to get their money back in case of fraud</td>
<td>TMC envisions that most EW will be have their wallets configured to a standard format and most EW used by private persons for routine purchases will not need special configurations. However, people likely will want to select their own password and otherwise make selections governing the security of the MM resident in the EW. Claiming fraud is common place; proving it in a court of competent jurisdiction regardless if the currency is digital or paper.</td>
</tr>
<tr>
<td>Lacking in security criteria as noted by QIAT</td>
<td>Security is configurable and can be extremely hard to attack for large value MM EW.</td>
</tr>
<tr>
<td>Truly an aspirational submission for adoption by U.S. players.</td>
<td>The design was fairly easy to make; the sales work needs more effort.</td>
</tr>
<tr>
<td>Comment</td>
<td>Response</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Proposal does not demonstrate how widespread adoption will be achieved. Legal Framework and Governance are not described.</td>
<td>Widespread adoption will occur from demand. Retailers sick of paying exorbitant fees for payment acceptance will stop accepting card payments because a sensible alternative exists. Legal framework already exists and does not change. Governance will evolve formed from decisions needed for implementation.</td>
</tr>
<tr>
<td>(1) Speed (2) addresses unbanked/underbanked segment (3) customizable for security features and end user experience (4) device and channel agnostic</td>
<td>I agree.</td>
</tr>
<tr>
<td>Heavy dependence upon the FED to issue the currency, other government agencies to regulate the wallets. Concept of moving from push &amp; pull payments to pure issuance, circulation and redemption. Very fast - 400 milliseconds. Concerned about how to deploy the configurable security controls between the payer and payee - is there a clean fit? Unclear on critical modules - security, transmission, reception, legal controls. Default to resolve disputes to court systems. Operational risk - many components yet to be developed. Interesting concept to suggest that the participants purchase insurance to cover payment loss due to fraud, inability to resolve disputes, etc.</td>
<td>I expect that EW providers for regular payers will use a password to access MM. However some people may want more security than that such as a physical token placed near the EW. Corporate EW containing large values likely will increase their security using common techniques such as requiring two people with separate codes to gain access to MM. It is likely that payees will have no restrictions for receipt of MM. Transmission occurs from available means, likely in most cases to be radio waves at an assigned frequency, however there MM can also travel using fiber optics.</td>
</tr>
<tr>
<td>This proposal appeared to have suggestions, not fully thought out solutions. In addition, this proposal does not address B2B, a key requirement for any solution. Stress was placed on &quot;privacy&quot; which hampers KYC requirements. In addition, this solution does not appear to integrate with other solutions and appears to rely on virtual currency.</td>
<td>The solution is a design; implementation poses different challenges. Banks issuing the currency to consumers likely will know their customer in the same manner required currently. Others issuing the currency may also need to comply to laws affecting issuance. However, most people will likely choose to insure their MM and the insurance companies will know who they insured and their exposure to risk. People not choosing to insure their MM will be fairly anonymous however not completely. For example, a person selling contraband may need to accept insured currency because the payer uses the currency for legal purchases. People can buy the currency with all the methods for payment available today. Businesses can conduct transactions using MM and the proposal explicitly states such.</td>
</tr>
<tr>
<td>Comment</td>
<td>Response</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>Model based on block chain electronic currency/wallet based on modules. Although MM could eventually replace the current US payments systems, there are still a lot of challenges tied to overall adoption of the modules, jurisdiction and adoption throughout use cases. The US Central Bank might be more open to this solution vs. other countries where Central Banks are more restrictive, and, cross-border still remains a challenge for electronic wallets. For this solution to be effective the Central Bank must embrace it through a mandate so it can be broadly adopted. Overall very challenging to adopt and to implement as a faster payment solution. Electronic Currency / Electronic Wallets (EW) based on various “Fundamental Money Module (FMM)”—or “Money Modules (MM)” some realistic and others more challenging. Model based on Central Bank issuing the currency and Blockchain being embedded with through the transaction amount Commercial and Retail Banks.</td>
<td>I agree.</td>
</tr>
<tr>
<td>Accessibility is rated too highly, as the proposal does not demonstrate how the solution allows users to reach any and all payees, nor how widespread adoption will be achieved (i.e., true ubiquity). Contextual data capability is rated too highly as the solution does not describe how data elements will be known by all parties sending and receiving information that would flow with a payment. Rules and governance areas are rated too highly as specifics are not provided.</td>
<td>Users can pay anyone with an EW or bank account. Widespread adoption occurs from user demand especially those paying extravagant fees for the privilege of accepting card payments. Contextual data is provided from XML tags as described in the ISO 20022 protocol. The rules and governance have a deliberately loose framework because they are implementation details</td>
</tr>
<tr>
<td>In my agreement I echo statements from the assessment: &quot;To be broadly effective, the Solution must first win support from the central bank. The proposal does not outline a plan for gaining central bank support ... &quot; and &quot;The Solution is innovative and conceptual, as the FMM, EW, BOLMM and other modules are not yet developed or implemented.&quot;</td>
<td>A design is not a marketing brochure. The issuance of currency (digital or otherwise) is a natural government function because the cost charged by private companies to move transactions is much higher; and the speed of movement is dangerously slow. We see the same dialectic around single payer health care and the fight to preserve health care profits regardless of the consequences to the well-being of the nation.</td>
</tr>
<tr>
<td>New currency based on DLT, issued by central bank. Serves the underbanked. Requires funding and adoption by central bank. Missing guidelines. Does not appear to be a complete solution</td>
<td>Comment needs to be more specific; what more is required for the reviewer to consider the solution complete?</td>
</tr>
</tbody>
</table>
One of the main shortcomings of this proposal is its brevity. In many instances, the QIAT downgrades the solution because the proposal does not outline the plan for realizing a criterion. The strength of the system is in its high-speed payment transmission. The QIAT criticized the system for its lack of consumer protections. The system contemplates a system of payment insurance. Presumably, some entity or entities would pay the premiums to support that system.

U.1 Accessibility should be not very effective, but effective. The system can be appended to allow governments to issue Electronic Wallets, but on its own, the system cannot provide a solution for unbanked consumers. The system is dependent upon government. It is not safe to assume that either the federal government or all state governments would take on this initiative.

U.5: Should be effective, not somewhat effective. The system does support all currencies and will serve all types of use cases provided that there is foreign government assent to supporting B2B.

E.3. Implementation Timeline: Should be very effective, not somewhat effective. The solution can be adapted as soon as a central bank adopts its function. The solution is fast.

s.3. Payment Finality should be not effective, instead of effective. They system is obviously riskier because it offers push (so that the receiver would not have to verify). It does not have a solution process for contested charges. It assumes that insurance will substitute for enforcement.

S.5: Handling disputed payments. This should be Not effective, instead of somewhat effective. See above.

L.3: Consumer protections: Should be read as not effective, instead of somewhat effective. In effect, this system substitutes insurance for a legal regime of enforcement of rules. In this system, insurers create modules; governance bodies regulate the insurers, and consumer groups weigh in on best practices for protections.

Payees can pull and payers can push depending on the circumstances of a specific transaction. Review of validity of the MM requires 400 milliseconds that determines if the seal is valid, the amount correct, etc. If the currency is not valid then payment is rejected and there may be legal consequences for attempting a transaction with invalid MM.
<table>
<thead>
<tr>
<th>Comment</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taken at face value, I believe the proposal was assessed fairly. The reliance on the central bank for the implementation of the solution will be challenging. Similar to other proposals I am not sure that this proposal will be rapidly adopted by core banking providers and their client institutions.</td>
<td>The proposal must be a mandate as its existence will force financial institutions to replace profits currently provided by payment cards.</td>
</tr>
<tr>
<td>Model based on block chain electronic currency/wallet based on modules. Although MM could eventually replace the current US payments systems, there are still a lot of challenges tied to overall adoption of the modules, jurisdiction and adoption throughout use cases. The US Central Bank might be more open to this solution vs. other countries where Central Banks are more restrictive, and, cross-border still remains a challenge for electronic wallets.</td>
<td>I agree.</td>
</tr>
<tr>
<td>For this solution to be effective the Central Bank must embrace it through a mandate so it can be broadly adopted. Overall very challenging to adopt and to implement as a faster payment solution.</td>
<td></td>
</tr>
<tr>
<td>Electronic Currency / Electronic Wallets (EW) based on various &quot;Fundamental Money Module (FMM)&quot;—or “Money Modules (MM)” some realistic and others more challenging. Model based on Central Bank issuing the currency and Blockchain being embedded with through the transaction amount Commercial and Retail Banks.</td>
<td></td>
</tr>
</tbody>
</table>
Response to General comments

<table>
<thead>
<tr>
<th>U2 Usability: SE rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>The assessment rates usability on its initial state and not after it has been configured by the user. This is akin to rating a modern car as unusable because it has not been configured to a customer's requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U3 Predictability: SE rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>A flexible application does not make such unpredictable. The rating is absurd on its face.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U5 Cross-Border Functionality: SE Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>The rating was strictly based on the subjective criteria of likelihood of adoption which is an irrational approach to evaluating its merits. The solution provides cross-border functionality which fits seamlessly into the solution, a fact ignored by the assessment team.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E3 Implementation Time-Line: SE Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>The assessment bases its time line against its potential political success which has no bearing on the time line. If the assumption is that an implementer accepted the design and created standards then the schedule is realistic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E6 Scalability and adaptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A central bank region can issue the currency to its correspondent banks for values demanded by the public. All central banks regions can scale issuance operations based on public demand. Repeating digital data as required does not seem to be an over burdensome activity and can be easily accommodated by a modern central bank. The rating is absurd and without merit.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E.7 Exceptions and investigations process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central banks do not need to operate an archive of spent or revoked MM, however, we believe central banks are a natural resource for such operations because of the expertise associated with central bank operations. The critique seems to evaluate storage as storage of physical items and not data. Thought Matrix Consulting developed a suite of analytical tools based on aggregate data of financial data. These trademarked tools named &quot;Bad Ed&quot; (an acronym for Behavior detection, Evasion detection) are proprietary and thus were not discussed in a public document. The major advantage to the suite of Bad Ed tools is that there are few to no false positive results. The suite will work extremely well with digital currency such as MM. The reviewers seem to think that providing specific approaches to fraud detection affect the efficacy of the solution, which is a horrendous assumption.</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S.1 Risk management</td>
</tr>
<tr>
<td>S.5 Handling disputed payments</td>
</tr>
<tr>
<td>S.6 Fraud information-sharing</td>
</tr>
<tr>
<td>S.7 Security controls</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>The proposal is not in conformance with the requirements of a full solution proposal.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>This proposal does not meet the requirements.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a &quot;detailed discussion of why the rating is justified and how the solution meets each criterion&quot; (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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>A few of the reasons why the proposal did not meet the requirements are as follows:</td>
</tr>
<tr>
<td><strong>The Solution does not defined rules or a process for resolving disputes (it relies largely on the courts); for fraud information and sharing capabilities; for risk, legal and governance frameworks.</strong> The solution does not encrypt data.</td>
</tr>
<tr>
<td>Thank you for your submission. I found this concept unique and thoughtful, allowing payment options for the unbanked and moving us closer to a digital currency concept</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>While your solution has its strengths, I'm just not sure the greater body of consumers in the U.S. will be open to electronic currency (especially when we continue to struggle to achieve 100% adoption of debit cards).</td>
</tr>
<tr>
<td>It appears the solution is overly reliant upon the FED, the proposal could be enhanced if there are mechanisms that the solution could be rolled out without extensive assistance from the FED.</td>
</tr>
<tr>
<td>I would have liked to see some suggested implementations for a legal framework, particularly in light of the need to ensure that all financial institution's have equal access to a faster payments systems.</td>
</tr>
<tr>
<td>While the proposal provides for anyone to have and receive Money Modules (MM), the solution could be enriched if a strategic plan was included that detailed how/if our Central Bank would entertain the issuance of a new payment currency (digital currency) and a new payment rail built on block chain technology. The solution could be enriched by providing a description of the expected end-users experience when using the system's core set of features, given the flexibility of the proposed solution.</td>
</tr>
<tr>
<td>Governance would be more effective if all stakeholders had voting rights when specification are being changed or enhanced.</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Describe more specifically what capabilities of the solution would enable the ability to have surety in reaching any other individual in the US</td>
</tr>
<tr>
<td>It would be helpful to describe what contextual data needs to be supported by all parties in order to consistently send and receive the data that flows with the payment itself. Describe more fully how the modules of the solution interface with other internal bank systems.</td>
</tr>
<tr>
<td>Describe further the role that the government is envisioned to take on in security – how is money removed from circulation in the case of fraud (or suspected fraud) and how are parties informed of such.</td>
</tr>
<tr>
<td>Built on central bank concept which means only FIs could ever participate leaving processor to work through FIs, potentially disenfranchising unbanked consumers.</td>
</tr>
<tr>
<td>The solution definitely achieves stated objectives for real-time payments.</td>
</tr>
<tr>
<td>Who is developing the underlying &quot;module&quot; that will be configurable by the users? It is not clear how this process would work and who would maintain it.</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>This proposal was unique in its thoughts about the Electronic Wallet, EW, and how it would be utilized by consumers. The proposal did state that the government might consider giving a bare bones EW to the unbanked and this system could be used as a portable bank account for many users. However what is the value proposition for consumers? Why would they transition to using such a system? The proposal made the case as to why Central Banks might be interested but did not explain how to drive consumer adoption. Why would I as a government end user accept this? How would I make payments to other municipalities and school districts? Unless forced to take this currency, they would still want dollars as they know they can spend it and it doesn't have to be converted. The governance structure needs to worked out. Details were scarce and with heavy Central Bank involvement necessary for this to succeed this will be a work in process for a while. I will however add that without involvement of end users in the governance structure this proposal will be missing critical voices that provide a unique perspective.</td>
</tr>
<tr>
<td>end user providers get to select which device and channels it is available on cross border works only if central banks between countries create standards to receive and transmit Since central bank involved, could hinder rapid adoption due to needing to set up infrastructure, etc. Also, debit brands and networks would be very resistant</td>
</tr>
<tr>
<td>Conceptual requires central bank who funds the costs of setting up and maintaining the system timeline to implement does not seem realistic given central bank approval and involvement is necessary scalability and adaptability criteria not effectively addressed does not require the sharing of fraud data disputes handled through court proceedings end user data protection based on end users' perception of risk</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>proposal would be strengthened with establishment of some baselines for security</td>
</tr>
<tr>
<td>Solution relies heavily on government involvement to govern. Unsure if that is palatable, but we believe the idea of government agencies, such as the FED, to own, operate and govern the system would be effective.</td>
</tr>
<tr>
<td>The proposed solution leaves too much flexibility in the hands of the providers, leaving no consistent expectation around the end-user experience. This could result in extreme complexity within the solution and create additional adoption barriers. I agree that a baseline should be established. Overall, the proposal is big on generalities and lacks in critical specifics, such as how to address central bank acceptance and how to build a robust exceptions and investigations capability if the end-user has the ability to &quot;turn off&quot; transaction visibility. This last example appears to set up a classic adverse selection scenario which could undermine a significant portion of the offering.. In the proposal and through the in-person presentation, recourse options appear to the &quot;the courts&quot; and &quot;insurance&quot;, both options the sole responsibility of the end-user to undertake. This again would appear to be a critical hinderance to end-user adoption. More thought in general to security standards, tool, and accountabilities across all parties in the solution is needed. Similar to the security facet, more detailed legal framework, system rules and consumer protection recommendations that align all parties interests in operating and functioning under a robust payments system of this type is needed.</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>I don't understand who is going to build the Money Modules and would it be possible for them to connect with other potential systems?</td>
</tr>
</tbody>
</table>

**GOVERNANCE**

G.1 Effective governance & G.2 Inclusive governance – SOMEWHA EFFECTIVE. Challenging to set up this type of governance model: Left to “independent governance of payment flows by skilled payment system professionals that understand the public policy of policy implementation”.

The “Rules for governance will be published and enforced by the root issuing FI.” Inclusive governance “must be developed by Central Bank “ And accessibility & legal must be given by Central Banks and Governments, with the usability governed by providers EW.

Comments are factual and so there is no need for a response.
Faster Payments QIAT

FINAL 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

FINAL ASSESSMENT

Proposer: Thought Matrix Consulting, LLC

Summary Description of Solution:

Money Modules (MM) is a new electronic currency based on block chain technology. It comprises standardized software, data modules, and the electronic wallets (EWs) that host them. The fundamental Money Module (FMM) is a block chain, and each record within the chain contains the issuer, a unique transaction ID, the issuer’s public electronic signature, the date issued, the fiat currency type, and the amount. The central bank issues the FMM, which then moves from the central bank to commercial banks, then to retail banks, and then to users’ electronic wallets, where the currency is broken down into smaller amounts. The module’s ancestry is always shown in the block chain. Access to read and to write to the FMM is allowed by the security module, which transfers money and updates the block chain upon instruction from an authorized EW approved by the central bank. EW applications make a standard call to a security module called “Break-Out Logic” (BOLMM) that is created by central banks. Break-Out Logic receives arguments as designated by a standards committee to select the FMM, create new FMM, transfer the requested value, and update the FMM with the residual value. Firms and individuals redeem MM by submitting MM values to financial institutions, which convert the values in EW to local fiat currency as cash or value in a stored-value account. Redemption removes FMM data from an EW and moves it to government archival storage units.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths
  – The central bank issues MM as fiat currency and is responsible for governing and approving Electronic Wallets, thus increasing the likelihood of public trust in the system.
  – As anyone can have and receive MM, MM EWs can become portable bank accounts for the unbanked. An MM account may be acquired at any bank or distributor and redeemed at any bank or non-bank. The proposal states that the government may consider giving basic EWs to unbanked payers and payees.
  – The Solution is customizable and configurable by providers and end-users, particularly for security.
  – The MM solution defines a new payment life cycle (issue, circulate, redeem).
  – The Solution offers fast validation of MM (400-millisecond speed) and immediate availability of good funds to the payee after validation of MM.

■ Areas for improvement and enhancement
  – To be broadly effective, the Solution must first win support from the central bank. The proposal does not outline a plan for gaining central bank support or for encouraging broad end-user adoption.
  – Unless the central bank issues a mandate to accept MM as legal tender, adoption could prove challenging, since depository institutions would have to forfeit the revenue associated with current payment systems, and commercial firms would need to develop new EW functionality and products.
  – Another potential hindrance to adoption is the assumption that a central bank (e.g., the Federal Reserve) will fund the costs associated with maintenance, production, and immediate
distribution of BOLMM to all circulating MM on a cost basis (similar to the way the Federal Reserve charges for FedWire). While the proposal notes that MM move based on payer and payee negotiations, the consensus mechanism used to update the block chain, the speed by which the block chain can be updated through this consensus mechanism, and the governance for updating the block chain are not clearly explained.

– The proposal states that security controls between the payer and payee are “configurable” and that often “payers and payees enact security procedures as they deem fit” (page 32), potentially allowing transactions to be made with only the most basic security.

– The Solution relies on critical “modules,” including security, transmission, reception, legal controller, broadcast response, and—particularly important—insurance and consumer protection modules. More clarity is needed as to how these modules will be developed, how they will work, and how the end-user will interact with them.

– The Solution has not defined several important elements of the faster payment solution, including: rules or a process for resolving disputes (rather, it relies largely on the court system for resolution), fraud information-sharing capabilities, risk and legal frameworks, and a governance model. The proposer states that the provision of contextual data depends on the development of actual tags by a technical standards committee, which is best done through consensus among a broad group of users.

■ Use cases addressed


■ Proposer’s overall ability to deliver proposed solution

– The Solution is innovative and conceptual, as the FMM, EW, BOLMM and other modules are not yet developed or implemented.

– The implementation plan provided is high-level. A more detailed plan is needed that includes the approach, timeline, hurdles, and requirements for all of the Solution’s dependencies, including: a technical standards committees to develop a tagged structure; creation of a permanent, secure payment data archive of all spent and redeemed FMM; a committee to approve electronic wallets; independent bodies to certify authentication solutions using new frameworks developed by the central bank; and rules for issuance, circulation, redemption, and revocation, along with software developed to act on those rules.
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 proposed Solution is a digital currency issued and regulated by the Central Bank that can be redeemed for physical cash. The EW account enables anyone to send and receive payments from any account through depository institutions and regulated non-bank account providers (U.1.1). Governments could provide basic EWs to unbanked payers and payees, making the EW a portable bank account for the unbanked (U.1.4). As long as central banks adopt the solution, multi-currency payments are supported (U.1.3).

The Solution could be strengthened by developing a way for entities to reach payees without an existing electronic wallet; however, the proposer does suggest a potential work-around for solving the unbanked challenge: a free, government-issued EW (U.1.2). Further, while the Solution is theoretically accessible to all end-users, it relies on market forces for features such as security, which could leave smaller firms and the unbanked/underserved with limited access to the Solution (U.1.4). In addition, to achieve widespread adoption, central banks, providers, and third parties must adopt the Solution and make it available to end-users. According to the proposal, revenue generation is the motivating factor for adopting the Solution, as it provides retailers with contextual data about payment and offers incentives to EW users to provide contextual data about payees (U.1.5).

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 EW can store, transmit, and receive MM via almost any electronic device and channel and is available 24x7x365 (U.2.1, U.2.3). However, EW providers determine the channels, devices, and hours of accessibility; the requirements, guidelines, and guardrails that will shape the EW’s usability (the minimum features required) are not stated (U.2.4). The proposer suggests that market forces will dictate which features become baseline features, but the proposal could be strengthened by suggesting which features and functionalities should be part of this baseline.

The Solution enables an entity to initiate a payment with limited information such as a name, email address, or phone number, but requires separate EW identifying numbers for both initiating and receiving a payment (U.2.2).

The Solution is consciously designed with a trade-off, as it prioritizes flexibility and adaptability over consistency in user experience.

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’s design ensures a baseline experience for issuance, circulation, and redemption of MM across channels, devices, and providers (U.3.1, U.3.4). While the end-user can configure
the EW to enable a personal customer experience, the solution uses communication and messaging protocols for functions such as the calls between EW and other modules (e.g., BOLMM and FMM) (U.3.3).

As discussed in U.2, the proposer’s vision for the Solution is rooted in flexibility and end-user customization; consequently, there is a risk that each payment and payee/payer will present a unique use case. As such, the predictability of each transaction may be questionable.

To strengthen the proposal, the proposer can: (1) clearly articulate the baseline experience; (2) develop operating rules to frame and communicate a common, core set of features and functionality, by device and channel; and (3) clearly explain how baseline features will be communicated to end-users (U.3.2). Further, while the proposal maintains that the Solution’s technical ability minimizes errors and states that a governing body will address error resolution, it would be beneficial to describe an error resolution process (U.3.5).

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 relies on EW providers to sell standard functions for EW users, including security controls and contextual data (U.4.1). EW providers will design the data transmission to EW users, although central banks will propagate standards for transferring value and contextual data from EW to EW (U.4.3). To include contextual data in the FMM, the Solution leverages XML-tagged fields created by a standards body.

While still conceptual in nature, the design and proposal can be strengthened by providing details of the actual capabilities of the contextual data, including how it will be included with the payment, what message format will be used, and how the contextual data can be customized (U.4.1). (The Solution has ISO20022-tagged structure, but these tags must be created by a technical standards committee.) The proposal should also address how the Solution will interface with business or personal finance systems (U.4.2).

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 enables cross-border payment if—and only if—governments and central banks create standards for receiving and transmitting FMM across borders, and EW providers offer cross-border functionality to end-users (U.5.1). Currency conversion only occurs when users redeem their FMM from issuing FI networks (U.5.4).

The Solution will support cross-border functionality at launch, as it can be configured to accept or transmit any or all of the approximately 150 currencies recognized by the United Nations. But it is not likely to be broadly adopted quickly, as central banks and governments must first create the standards necessary for receiving or transmitting foreign-value FMM in a cross-border setting. The proposal could be enhanced by detailing a plan for securing central banks’ and governments’ commitment to accept the Solution and persuading them to create the appropriate standards (U.5.5).
Additionally, detailing how the Solution allows for interoperability with other faster payment solutions in other countries (U.5.2) without requiring them to use Money Modules would be beneficial, as this information would shed light on the likelihood of, and potential challenges to, cross-border adoption. (As an illustration, the proposer maintains that requiring an FI to be a party to a transaction in the UK would be incompatible with the Solution, as MM do not require FIs to circulate.) Additionally, developing operational rules that formally require providers to disclose costs, timing, and risks in advance to the payer would add clarity to the proposal (U.5.3).

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 provides the necessary features and functionality to meet the needs of the four major use cases (P2P, P2B, B2P, and B2B).

**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 relies on the development of value-added services such as EW applications and modules from numerous service providers (E.1.1, E.1.4). It leaves pricing, features, and services completely up to providers and individuals based on market demand. Since providers do not have to be FIs, competition can be broad and based on value-added services, not just on price. Once someone purchases or receives an EW, it is his/her property, and s/he can obtain as many EW as s/he needs for various, specific uses. The proposer expects EW providers to develop features for the products, further supporting the market-based nature of the Solution’s design. The proposal suggests that public law will govern the use of MM and the protection of its payers and payees (E.1.3).

The Solution’s dependence on the market for so much of its infrastructure is a slight concern. Without the provision of minimum features and/or preconfigured ways to access the Solution, smaller providers may not be able to compete as effectively (E.1.4).

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:**
Value-added services will serve as the main differentiator among providers of various sizes and incumbencies (E.2.2). Users will purchase these services (including security) based on their needs. Disclosure that value-added services are optional will occur during payer and payee negotiations, if allowed by the user's EW (E.2.3).
Because the Solution is a digital currency, providers do not participate in the circulation of MM. The proposal could be strengthened by articulating how an EW provider can “integrate” with the Fundamental Money Module (E.2.1). Further, because the Solution’s design affords an almost limitless capability to develop and offer value-added services, the proposal can be bolstered by laying out a clear process (e.g., use of open APIs, etc.) for enabling these services, with specifics about the ease or difficulty of doing so.

The Solution relies on third-party firms to develop “modules” such as transmission, reception, legal controller, insurance, consumer protection modules; there are even government modules that govern all taxes related to transactions. It would be helpful to understand how these modules work and how end-users interact with them.

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 implementation timeline is seven months for development and one year for pilot and rollout, which is scheduled for 2017. Critical to the timeline, however, is central banks’ agreement to: (1) adopt the solution, (2) potentially agree to distribute free EWs to unbanked/underbanked users, and (3) commit to significant new builds that are needed such as standards, specialized EW and secure transmission pipes, security layers, and equipment upgrades to enable acceptance of MM.

The proposal could be strengthened by adding more detail to its high-level implementation plan. Details might include the full timeline for new builds, initial adoption, and the path to ubiquity; funding plans; implementation and ubiquity hurdles, with plans to overcome them; and projected growth estimates (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 payment format standards are rooted in the ISO20022 XML-tagged structure; however, a technical standards committee must create the actual tags (E.4.5).

The proposal states, “Only the BOLMM updates the FMM, and central banks create and replace the logic to update the block chain (FMM) as needed.” The proposal could be strengthened by outlining how the new standards will interface with existing payment format standards.

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 MM solution defines a new payment life cycle (issuance, circulation, redemption) that covers all stages of the process (E.5.1). Its technical design supports all of its features (E.5.2).
E.6 Scalability and adaptability

Very Effective  Effective  **Somewhat Effective**  Not Effective

**Rationale:**

The Solution’s technical design as described supports projected use cases and is adaptable (E.6.1, E.6.3) based on updates to BOLMM by the central bank. Essentially, the central bank determines how the Solution’s technical design must be changed to adapt to ongoing developments and then distributes those changes through software updates.

The proposal describes ways to accommodate increased transaction volumes and flow rates, but it does not substantiate this purported scalability with specific projections and timelines beyond anticipating we would see roughly 90% of M1 circulation (E.6.2).

The proposal could be improved by discussing plans for accommodating the level of central bank capacity and security required to handle peak transaction volume (E.6.2); the Proposer suggests that the security provided by public and private signatures does not depend on the value or quantity of MM in the marketplace.

E.7 Exceptions and investigations process

Very Effective  Effective  **Somewhat Effective**  Not Effective

**Rationale:**

The Solution expects the central bank to provide an archive for all revoked or spent FMM. The archive can be used in court proceedings in case of dispute (E.7.2). While the Solution calls for the MM involved in an exception to be revoked immediately and replaced by an insurer, the proposal can be strengthened by discussing what happens if an exception is created and the issuing party does not have insurance.

The Solution’s design can be made more robust by including plans and requirements for tools, messages, alerts, notifications, and related protocols to support exception-handling (E.7.1). Additionally, the Solution should aggregate exceptions data to spot patterns not visible at the individual-participant level (E.7.3). In addition, while it may be a nice configuration option, the user’s ability to “turn off” transaction visibility to the central bank means that some data cannot be used to support the exceptions and investigations process (E.7.1, E.7.3).

Safety and Security

S.1 Risk management

Very Effective  Effective  **Somewhat Effective**  Not Effective

**Rationale:**

The Solution’s design focuses on minimizing risk through security measures that confirm that MM are legitimate. With software version changes distributed by the government, the EW receives updated logic that addresses unexpected applications of laws and regulations (S.1.1). The validation process is meant to ensure that circulating MM are legitimate (S.1.4). The design of the system is such that any MM involved in an exceptions transaction will be immediately revoked and taken out of circulation; it is expected that insurers would
immediately replace the revoked MM. The government will ensure that EWs receive and adopt updated security logic by first going to specific regions under attack and beginning the roll-out there.

The proposal can be strengthened by addressing the operational risks related to deficiencies in information systems or internal processes (S.1.3). Additionally, to help prevent fraudulent payments, the proposal should articulate any baseline level of authentication security required of EW providers (i.e., delineate what is required in a commercial firm’s authentication module versus what is configurable by payers). The proposal can be improved further by clearly describing the Solution’s incentives to providers and operators to address and contain the risks they may pose to other participants, as well as by explaining how the periodic review and update of the risk management framework is expected to work (S.1.5-6).

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:
The solution includes pre-authorization capability; the proposal states, “Payers can select the timeframe for payment or allow payees to control debits from payer EW. Payers revoke payment on demand until the payment moves to payees. All payer parameters may be changed prior to payment” (page 30) (S.2.2-3).

A significant amount of flexibility is built into the Solution; for example, a user may configure his/her wallet to ask for a password and fingerprint before presenting a payment option or showing value, corporate treasurers may ask for additional evidence of authorized payers, etc.

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:
As a digital cash solution, the Solution does not require FIs’ approval of transactions (S.3.1). The payment is final when an EW or FI receives MM from an authorized source and confirms the authenticity of value (page 31). This confirmation (MM authentication) is expected to take no longer than 400 milliseconds after receipt by the EW (S.3.2). The courts will address disputes that go beyond automatic reimbursement by insurance companies.

The Solution does not specifically provide mechanisms and processes to protect or compensate the payer in cases of disputes, but rather depends on: (1) market forces to provide insurance modules that payers will purchase to cover any losses, and (2) the central bank’s archives of redeemed and revoked MM to provide evidence to courts in cases of disputes (S.3.3). The proposal can be strengthened by detailing how the insurance modules work, whether or not they are required to be included in an EW, and how disputes are handled when the payer lacks insurance.
S.4 Settlement approach

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
Transactions conducted within the Solution are settled immediately (S.4.1-2). When redeeming MM for collateralized fiat currency, there is a concern about the amount of cash needed exceeding the amount of cash on hand; the proposal can be strengthened by clearly articulating the process for converting MMIs to collateralized fiat currency.

S.5 Handling disputed payments

**Effective**  **Somewhat Effective**  Not Effective

**Rationale:**
Disputes are handled by revoking the MM involved in the disputed transaction, and insurers are likely to replace the revoked MM in the system. Disputes that go beyond insurance companies’ automatic payments for loss will be handled through “court proceedings” (pp. 37, 54) (S.5.1), which would likely be a lengthy, expensive process. The Solution relies on the EW provider to develop consumer protection models that comply with laws and to offer insurance products to cover losses from disputes (S.5.2). Additionally, it relies on end-users to decide whether or not to adopt these modules.

The proposal should describe the process for requesting the return of a payment (S.5.3). It should also detail an approach for delineating roles, responsibilities, and liability allocation to responsibly protect business, government, and consumer payers (S.5.4-5). As stated in previous Criteria, the proposal should clearly outline what happens if the dispute involves a non-insured payer.

S.6 Fraud information-sharing

**Very Effective**  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
The Solution allows users to configure sharable data from the EW and does not require the sharing of information to facilitate managing and monitoring fraud (S.6.1). The solution does not aggregate, manage, or protect data owned by entities other than providers or operators (S.6.2). It only records spent and revoked MM; it thus shares real-time information only when a payment is revoked (S.6.3). All MM will eventually be archived and can be reviewed by anyone reviewing payer or payee behavior. The solution allows for post-fraud analysis, but not for pattern recognition (S.6.7). Sub-criteria S.6.4, S.6.5, and S.6.6 are not addressed in the proposal, although the Solution does require the creation of a central bank archive of transactions (S.6.1, S.6.6).

The proposal can be strengthened in a number of ways related to fraud information-sharing: (1) by requiring that specific data be shared at the Solution-level across providers, (2) by leveraging data to conduct post-transaction analysis to spot fraud patterns, and (3) by defining the types of data that will be shared.
The Solution does have a proprietary component and method for detecting fraud based on behavior and evasion detection.

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:**

The proposal addresses security controls related to technical access components and controls, such as asynchronous signatures and encryption used by MM to protect the currency’s integrity and the security seal’s validity (S.7.1). A data breach causes revocation of the security seal. Additional security controls are found in the seal. Data is encrypted both entering and exiting the FMM.

The proposal can be strengthened by detailing the security controls related to operational or procedural components (S.7.2), managerial policies, and oversight (S.7.3). Examples of the additional detail could include: (1) the data retention and disposal controls in place, (2) physical controls, (3) operational controls, (4) communication and network security examples, and (5) how the solution integrates with existing risk management processes and adapts to enterprise-level security architectures.

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 design for resiliency is based on replacing compromised MM immediately to protect against systematic risk. The design also allows for the central bank to swap out the BOLMM in the event of a cyber-attack to prevent affected MM from moving in the system. Insurance companies replace the revoked currency; the replacement currency comes from the central bank after forensic proof has established that it was compromised.

The proposal can be strengthened by directly addressing: (1) target availability metrics (S.8.1), (2) the approach to achieving those metrics, (3) the plan for business continuity (BC) or disaster recovery (DR) (S.8.2), (4) the resources devoted to BC and DR (S.8.4), (5) mechanisms to minimize the chance of triggering systemic risk (S.8.3), and, (6) contingency testing of the Solution (S.8.5).

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:**

The Solution is designed to promote flexibility and choice. Identity verification and access management are configurable based on the end-user’s perception of risk. The Solution does encrypt data (S.9.2-3), but the proposal could be improved by addressing the requirements of all parties—including EWs and financial institutions—to provide controls and mechanisms to protect sensitive information throughout the entire payments process (S.9.1). Additionally, the
Solution’s design could be enhanced by requiring a minimum level of security controls, which would allow the design to retain its flexibility while ensuring basic, essential security in the Solution (S.9.2-3).

S.10 End-user/provider authentication

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th><strong>Somewhat Effective</strong></th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Solution allows the central bank to replace the BOLMM at any time and uses various protocols to ensure that authentication module requirements are met. Essentially, it relies on the central bank for updates when new authentication modules are adopted and old ones are decommissioned (S.10.6).

However, the Solution ultimately holds end-users responsible and in control of their own security in the payment process, including authentication. The proposal states that authentication is “configurable” without any baseline level of authentication described (S.10.1, S.10.4). In addition to establishing a baseline level of authentication, the proposal could be strengthened by discussing the potential for risk-weighted authentication as a means of further enhancing security features (S.10.4, S.10.5).

S.11 Participation requirements

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th><strong>Somewhat Effective</strong></th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Participation requirements have not yet been developed, but the proposer does suggest that the rules will include controls such as certification software, licensing of providers, and periodic inspection of security controls (S.11.1). The proposal indicates that the central bank will create compliance rules and reporting requirements for all participants that provide equipment or services to any part of the MM solution.

The proposal can be strengthened by providing details of the participation requirements and a timeline for creation of the rules. The requirements should outline the process to monitor and ensure compliance by all providers against the 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:**
Based on the digital fiat currency concept and the Solution’s good-funds model, approval occurs in a fraction of a second. Approval and transmission of MM occur simultaneously.
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:

Based on the digital fiat currency concept and the Solution’s good-funds model, the electronic negotiation between EWs is essentially a substitute for clearing operations. Payers or nominated payees validate the MM via central bank points-of-presence. MM validation takes less than 400 milliseconds; however: if payers and payees have long lists of criteria for valid transactions, then the “negotiations” may take longer.

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:

Payees have access to MM after the expected transport time, as determined by the payer’s and payee’s conditions and 400 milliseconds of currency validation.

The availability of funds to a payee could be slightly delayed (by no more than 10 seconds), however, depending on the amount of contextual data required by the payee and the fact that the contextual data moves across the same connection as the MM, potentially slowing the process.

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

MM is settled immediately when an EW receives it (F.4.1, F.4.3). When redeeming MM for collateralized fiat currency, however, there is a concern about the amount of cash needed exceeding the amount of the cash on hand. The proposal could be strengthened by clearly articulating the process for converting MMs to collateralized fiat currency.

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:

Immediate notifications of payment status are available in the EW to both payee and payer.
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 proposer assumes that the central bank will ensure that MM and EW conform to all applicable laws. The Solution relies on the EW and government control of EW functionality and logic to support compliance and legal provisions (L.1.4, L.1.5). The EW updates the legal logic when the Solution is first used in a new jurisdiction, although how the EW obtains that information is not described (L.1.1).

The proposal could be strengthened by providing detail on the legal framework, including assessment of gaps (L.1.2), how the participants are legally bound (L.1.3), compliance with current laws (L.1.4), and unique provisions needed (L.1.5).

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 considers many governing bodies to direct and certify the work of EW providers, but the payment system rules have yet to be defined (L.2.1, L.2.4). It is assumed that the governing body(ies) will prove effective and develop the appropriate set of operational rules (L.2.2). The proposal could be enhanced by suggesting which governing body is likely to be the chosen body for the Solution. It can further be improved by requiring the rules to pay particular attention to the remediation process (L.2.5).

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 Solution includes options for end-users to establish additional consumer protections through “consumer protection modules” (L.3.3). The proposal suggests that insurance companies have responsibility for creating the insurance modules, that technical committees will test and license the insurer MM, that firms committed to consumer protection will develop consumer protection modules, etc.

The proposal could be strengthened by detailing the types of protections that would serve as a minimum standard set of protections and by describing which of these is/are configurable (L.3.1 and L.3.3).
L.4  Data privacy

Very Effective          Effective          Somewhat Effective          Not Effective

Rationale:
The solution states that users will define their own data privacy controls (L.4.1), users will control their sharing of contextual data based on individual payment negotiations or default EW settings (L.4.4), and that security functions embedded in the EW will block any intrusion attempts or interceptions of MM in transit (L.4.2).
The proposal can be made more robust by outlining an approach to data privacy and links to relevant legal requirements (L.4.1, L.4.2). Further, it should indicate whether/how users are informed of the data being collected on them (if any is collected) and describe the steps taken when data breaches occur (beyond revocation—are there notifications, etc.? ) (L.4.5).

L.5  Intellectual property

Very Effective          Effective          Somewhat Effective          Not Effective

Rationale:
The proposal states that the MM solution does not violate intellectual property law. The proposal can be strengthened by including a proposed approach to managing risk from third-party intellectual property rights (L.5.1).

Governance

G.1  Effective governance

Very Effective          Effective          Somewhat Effective          Not Effective

Rationale:
The issuing FI will publish and enforce the rules for the Solution’s governance, but central banks and governments could possibly take control of this governance (G.1.1). According to the proposal (page 61), all governance documents will be made available to the public (G.1.2).
The proposal could be enhanced by addressing the process whereby appeals of specific decisions are handled (G.1.3). It should also describe how compliance would be independently validated (G.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 proposed governance includes input from stakeholders through government certification committees (G.2.2, G.2.3) and will take into account mitigating procedures for conflicts of interest (G.2.5).

While the proposal discusses the Solution’s governance model at a high level, further information is needed about the model’s composition and dynamics concerning public interests (G.2.1), obtaining input from stakeholders (G.2.2-3), proportionally influencing outcomes (G.2.4), and managing real and perceived conflicts of interest (G.2.5). The proposer suggests that the details of effective inclusive governance must be developed by the central bank and are outside the design scope.