M10

Implementing a Regulated Liabilities Network

Authors: Marten Nelson, Richard Char, Chae An

Executive Summary

In June 2021, Citi released a paper entitled "The Regulated Internet of Value"[1] (the "Citi Paper"), authored by Tony McLaughlin, Head of Emerging Payments and Business Development at Citi's Treasury and Trade Solutions. In the Citi Paper, the author makes a case for networks of regulated liabilities and assets.

Regulated liabilities would include central bank money, commercial bank money, and electronic money, tokenized using distributed ledger technology and exchangeable on financial networks.

The Citi Paper is an essential contribution to the payments literature as it is the first articulation of a regulated liabilities network or "RLN." While the author states that "...creation of such networks may seem a pipe dream...", this paper is intended to be a companion to the Citi Paper and demonstrate how a seeming pipe dream can be realized today. If the Citi Paper describes the "What" of RLN, this paper attempts to explain our vision of the "How."

We begin by introducing the concept of a shared hierarchical ledger, which enables both central bank money and commercial bank money to be tokenized. Transactions can settle instantly because banks on the system are transacting using tokenized central bank balances on shared ledgers. The platform supports multiple regulated liabilities. There is one ledger per liability, and banks can have positions on multiple ledgers. The ability for a bank to debit a position on one ledger and credit the balance on a different ledger enables cross-border payments.

RLN simplifies regulatory compliance. Parties must be known to gain access to the network. All transactions are visible on an immutable, shared ledger rather than a proprietary siloed system within a bank. And the central bank or regulators can screen or filter transactions in real-time.

The RLN is not a theoretical construct. It is available today.

1 Tony McLaughlin. The Regulated Internet of Value. (June 2021), https://www.citibank.com/tts/insights/articles/article191.html

Summary of Citi's RLN vision

With the advent of blockchain technology, the Citi Paper foresees the creation of regulated, global, token-based, multi-asset networks far beyond the current form of digital money.

The Citi Paper explains that to maintain a stable economic environment with sound monetary policies, "safe digital money needs to be: (a) regulated, (b) redeemable at par value on demand, (c) denominated in national currency units and, (d) an unambiguous legal claim on the regulated issuer." Unlike the current cryptocurrencies such as Bitcoin, regulated liabilities include central bank money, commercial bank money, and electronic money since they all live on the balance sheet of the relevant regulated financial institution. By design, the transfer of money in a network of regulated liabilities will be in favor of verified legal persons, reducing the risk of financial crimes. By contrast, Bitcoin payments are conducted as a digital form of a bearer instrument.

The Citi Paper discusses the nature of regulated liabilities & sets forth desirable traits:

- "Regulated liabilities are denominated in national currency units and proceed from the sovereign right of nation-states to decide what counts as money within their territories
- The end-user has an unambiguous claim on a regulated institution, enforceable through the legal system
- The claim is redeemable at par value on demand in national currency units
- Institutions are regulated to ensure that they are able to meet those claims, e.g. capital rules for banks and collateral rules for E-money institutions
- The liabilities are fungible between regulated institutions, i.e. a dollar is a dollar irrespective of the regulated institution holding the liability
- Regulated liabilities are in favour of verified legal persons, they are not bearer instruments. This feature helps to combat financial crime
- Regulated liabilities are on one side of the balance sheet of institutions — on the other side of the balance sheet are assets deployed in an economy to stimulate economic growth. [2]

2 Tony McLaughlin. The Regulated Internet of Value. (June 2021) p2. https://www.citibank.com/tts/insights/articles/article191.html

The Citi Paper examines how a network would hold liabilities across various regulated entities and concludes:

- "A token in a central bank wallet is a liability of the central bank
- A token in a commercial bank wallet is a liability of the commercial bank
- A token in an E-money wallet is a liability of the E-money issuer

The legal meaning of the token is given by its location of the wallet in which it resides. When a token is at rest in a wallet controlled by an institution, then it is on the balance sheet of that institution as a liability in favour of the token holder."[3]

Payments on the RLN are conducted through the transfer of tokens. These are done through entries on a ledger, and not using bearer instruments.

To achieve a global system, a constellation of interoperable RLNs is envisioned. Each network is "founded on national currencies and supervised by local regulators.[4]

Finally, the Citi Paper discusses central bank digital currencies ("CBDC"). It calls for a pivot beyond CBDC, making the argument that CBDCs are too limited and that a broader RLN paradigm that tokenizes all regulated liabilities can deliver benefits beyond CBDC.

The Citi Paper concludes with the warning that much of the innovation in distributed ledger technology is "taking place . . on the edges of the regulatory perimeter."[4] It also warns that if tokenization efforts by the **regulated** sector proceed in a fragmented manner, the result may be that "**unregulated** networks may gain in relative significance."[6]

Blockchain technology has the potential to express these liabilities on the same shared ledger, making money 'always on', instant and programmable, global in scope, but regulated by a sound banking system. The vision of a global network of regulated liabilities may seem like an impossibly ambitious dream, but we at M10 Networks are already working with central banks and commercial banks around the world to realize this 'ambitious dream.' The rest of the paper will discuss the technology and the approach that M10 Networks is providing to implement such a global regulated liability network.

3 Ibid. p 3
4 Ibid. p 5
5 Ibid. p 7
6 Ibid. p 7

Key considerations for an RLN system

An RLN should ultimately be able to tokenize and exchange all types of regulated liabilities: central bank money, commercial bank money, electronic money, and even stablecoins and cryptocurrencies (if and when regulated). However, for the purpose of this paper, we focus primarily on central bank money and commercial bank money, which we believe will be foundational to most RLNs. The functions of the M10 platform that we describe below apply to all regulated liabilities.

The shared hierarchical ledger

A key requirement for an RLN system is to enable the tokenization of both central bank money (issued to commercial banks) and commercial bank money (issued to bank customers). At M10, we implement this through the use of shared hierarchical ledgers. The central bank portion of the ledger is called M0 and the commercial bank portion of the ledger is called M1. M0 and M1 are distinct but joined in a hierarchical fashion.

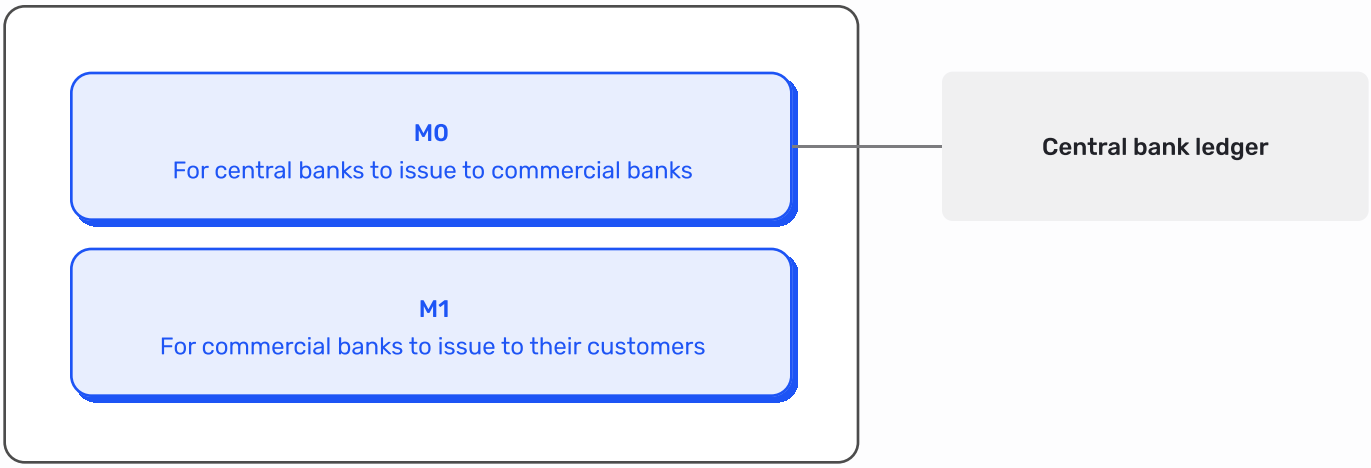

Figure 1: Hierarchical ledger.

This preserves the two-tier monetary system while providing real-time payment capabilities. The shared nature of the ledgers allows participating banks to settle payments instantly. The single source of truth replaces siloed ledgers across financial institutions.

To fund their digital M0 accounts, commercial banks transfer funds on the central bank ledger to a special "sponsor account," ideally established by the central bank in the fashion of an RTGS. For each amount placed in the sponsor account, the bank gets corresponding credit on the M0 ledger. In effect, the central bank is creating a stablecoin for participating commercial banks.

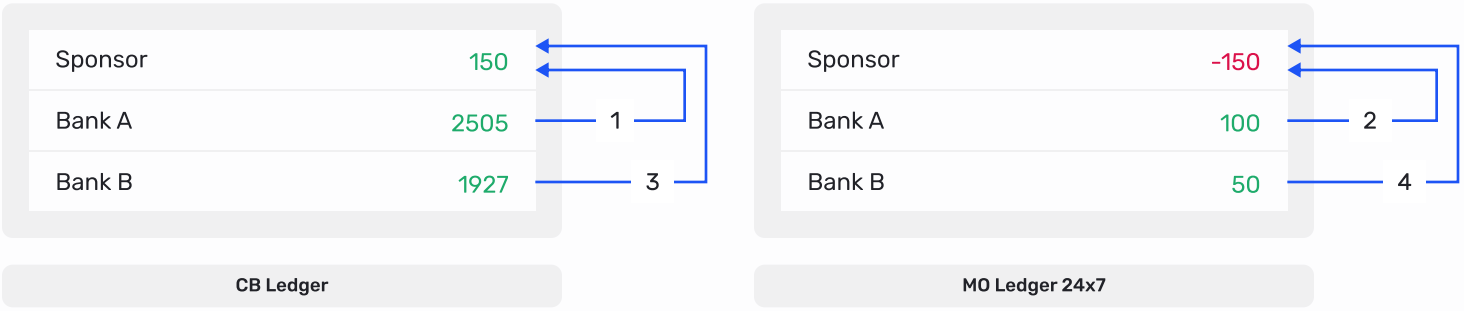

Figure 2: Funding the M0 ledger.

Commercial banks can then create accounts on the M1 ledger for their customers. To fund a customer account, money is debited from the customer's traditional bank account and credited to the customer's M1 account. Note that while a portion of the customer's assets has been converted from a traditional account to an M1 account, no new liabilities are created for the bank.

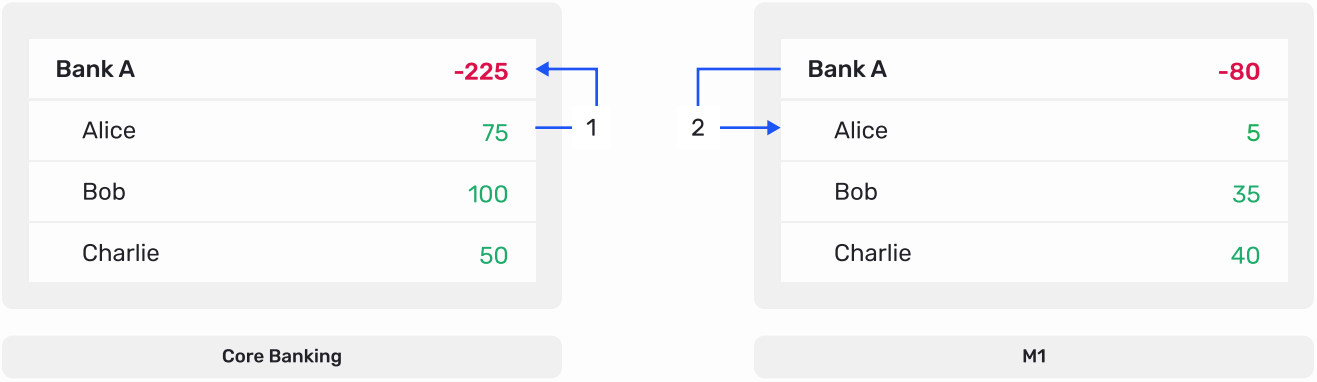

Figure 3: Funding the M1 ledger.

Like in the traditional system, balances in M1 accounts are not “backed” by the bank’s M0 account with the central bank, so there is no required ratio between M1 and M0. A bank’s required Liquidity Coverage Ratio (LCR) requirements can be addressed using M0, or other High-Quality Liquid Assets (HQLA).

Traditional payments between banks must settle in central bank money, often using an RTGS. In the M10 system, the M0 part of the ledger serves as the RTGS. The M1 portion of the ledger is for intra-bank transfers. See the figure below for an example of a transfer between two customers at two different banks.

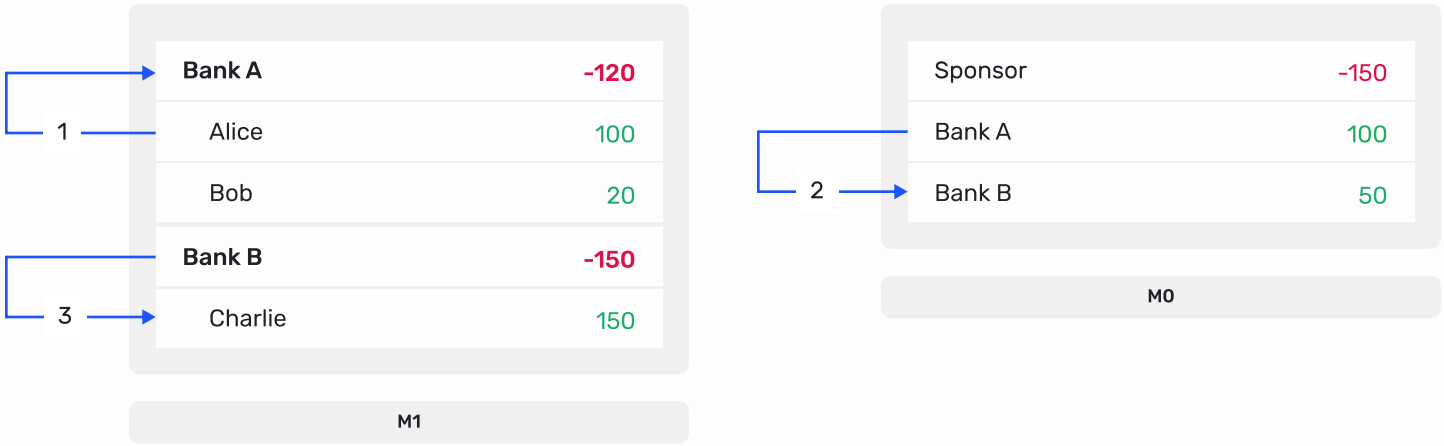

Figure 4: Transfer of funds between two banks.

M10’s shared hierarchical ledger can hold any “digital asset”. Digital assets are not to be confused with typical assets on a bank’s balance sheet. A digital asset is simply a digital representation of an asset such as money, gold, real estate, fine arts, etc.

Multiple digital assets

The Citi Paper envisions an “internet of value” that includes the tokenization of regulated liabilities and regulated assets. From a DLT perspective, both regulated liabilities and regulated assets are considered “digital assets”. Multiple digital assets can be supported with (1) a single multi-digital asset ledger or (2) multiple single-digital asset ledgers.

	Pros	Cons
Single multi-digital asset ledger	The exchange between assets is less complex as it’s done on a single ledger.	Difficult regulatory issue if different currencies are hosted on a single ledger. Central banks will want their currency hosted in-country.
Multiple single-digital asset ledgers	Enables each central bank to regulate its tokenized currency locally.	Requires some financial institutions with accounts on multiple ledgers to facilitate trading between the ledgers. Requires the local operator to host each ledger.

Table 1: Single-asset, vs. multi-asset ledgers.

In the M10 solution, we use separate local ledgers for each asset [6]. The ledgers are then logically connected through a cloud service. We assume financial institutions, particularly larger multinational banks will be allowed by regulators to have accounts on multiple ledgers. Banks that have M0 accounts on multiple ledgers are able to offer instant cross-border payments to their customers.

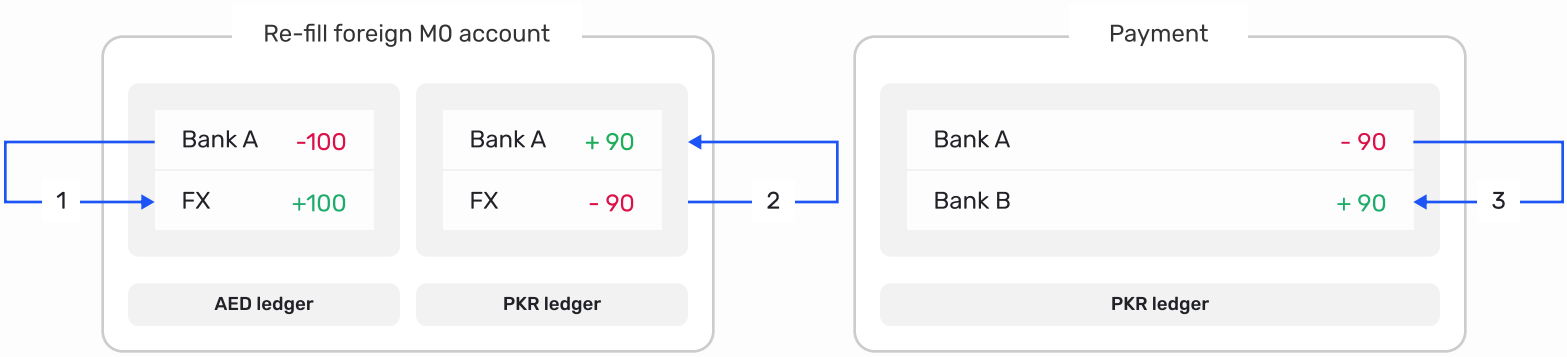

Figure 5: Cross-border payment

If the sender's bank doesn't have an M0 account on the foreign currency ledger, a third-party "delivery service" may be used. The delivery service is an entity (typically a bank) that does have M0 positions on the local currency ledger and the foreign currency ledger.

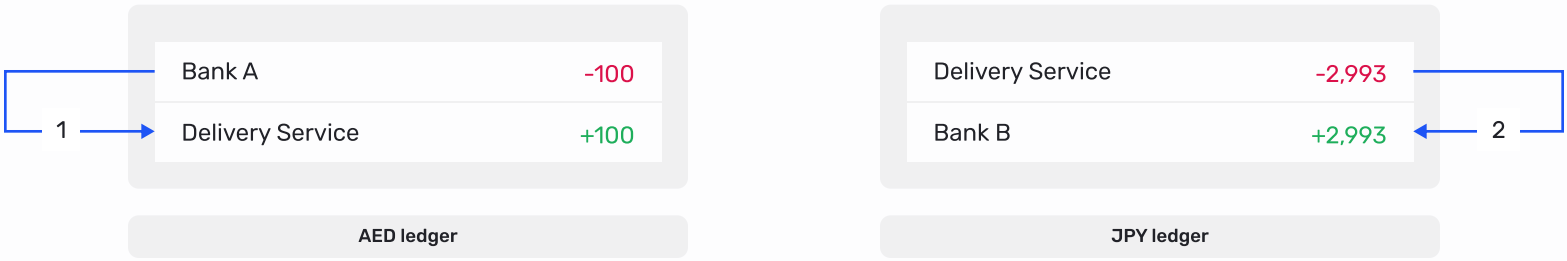

Figure 6: Cross-border payment with "delivery service"

7 Technically, M10's ledger supports multiple asset classes. However, each ledger is typically managed by a different sponsor and hosted and managed locally in-country (i.e., PKR in Pakistan, AED in UAE, EGP in Egypt) to meet legal requirements. Therefore, the standard implementation will be one ledger per asset.

One of the benefits of this approach is that a given ledger, say for tokenized Pakistan Rupee (PKR), can be supervised directly by the Pakistan central bank and operated by a trusted operator based in Pakistan. In the case of M10, the supervising bank would be the State Bank of Pakistan and the operator would be the National Institutional Facilitation Technologies (Pvt.) Ltd. ("NIFT"). The use of a clearing house as an operator is ideal since (1) it is trusted by the central bank and commercial banks in the country, (2) is connected to the commercial banks already, (3) has experience operating critical bank infrastructure, and (4) (as is the case with NIFT) is often owned and governed by some of the larger commercial banks in the country.

Digital assets on the ledger are not limited to tokenized fiat currencies. The M10 system can also be used to tokenize other asset classes, such as treasury bills, bonds, and other regulated assets and liabilities. This enables instant, 24x7 trading and conversion from one asset into another.

However, all of the digital assets should be regulated. This is a key point of differentiation from stablecoins, which are issued by private parties without regulation. They rely on the use of private reserves to provide confidence in the stablecoin. Recently, rating agency Fitch warned that stablecoins could trigger credit market contagion if there is a stampede to convert stablecoins into traditional money.[8]

Finality

In an RLN, transactions should settle instantly and with finality. The M10's permissioned blockchain is immutable and provides finality at the ledger level. Transactions can not be reversed.

Fungibility, exchangeable and interoperable

RLN liabilities should be fungible between regulated financial institutions. In the M10 system, all banks are on a commonly shared set of ledgers to ensure fungibility. A tokenized euro issued by Bank A will be the same as a tokenized euro issued by Bank B, or a tokenized euro issued by Electronic Money Institution C.
As noted above, the use of banks with accounts on multiple ledgers provides that all the system participants can transact between the ledgers. This ensures exchangeability and interoperability within the M10 ecosystem.
Interoperability is also possible outside the M10 system, using gateway banks that have membership on M10 and the third party system (for example, the tokenized Chinese yuan or the European SEPA payment system).

8 "Stablecoins could trigger credit market contagion, warns Fitch", Financial Times. July 1, 2021, https://www.ft.com/content/b734b2e8-db37-46fe-93b1-d47a59f74068

Regulatory compliance

In the Citi Paper, the author posits that regulated liabilities must be in favor of verified legal persons or businesses, and not bearer instruments. This helps combat financial crimes. The M10 system is an account-based system where the identity of all transacting parties is known to the parties, the issuers, the system operator, and the regulator. Issuing financial institutions are responsible for KYC, AML/CFT, and sanction screening - just as they are today. The M10 system includes modules for AML/CFT and sanctions screening that can be used by participating Issuers to augment their own screening. Issuers can configure their own set of rules and define blacklists and whitelists. Issuers receive a stream of the transactions, including all metadata, to do the screening using existing tools and processes.

Having all Issuers on the same immutable ledger and the use of standard APIs makes compliance easier and less costly for the Issuers. Banks are no longer in silos trying to provide compliance in isolation.

Of greater significance, regulators now have real-time access to transactions. Using filtering and screening tools, they can identify (and stop) suspicious transactions which merit additional scrutiny and analysis. This is vastly superior to the status quo, where regulators rely on banks to provide reports on suspicious transactions, often hours or even days after the transaction has been completed.

Security and Trustability

To prevent malicious attacks, a payment system should require all interactions to be digitally signed using public-key cryptography. Systems based on shared secrets (such as passwords) are insecure and should be avoided. Imagine 3 computers running the same software in parallel. An instruction to move an asset is only issued if ⅔ (2 of the 3) of the computers agree to issue that transfer. This is enforced at each ledger: 2 of 3 computers must digitally sign a transaction in order for it to execute. As a result, 2 of the 3 computers would need to be compromised to manipulate a ledger. The ⅔ ratio scales up with more computers.

The M10 system contains a number of advanced security features including the use of a Byzantine Fault Tolerant (BFT) consensus mechanism to prevent double-spend, use of trusted execution environments (Intel SGX and AWS Nitro Enclaves), use of role-based access control to control user access to accounts, use of Rust programming language for improved memory safety, and various other techniques to defend against malicious developers. For a more detailed description of these security features, see the M10 security paper.[9]

9 M10 Security, (June 2021), https://tinyurl.com/3rcpkzrt

Privacy

In the context of CBDC, anonymous transactions are often mentioned as a requirement. This comes from the desire that a retail CBDC should have cash-like properties. This means that during a transaction, the counterparties shouldn't know the identity of each other.

Anonymity should be configurable by the counterparties. In M10 this can be set as default for all transactions, or per transaction basis. Given the different payment use cases supported by the M10 platform, the possibility for anonymous transactions varies.

Function	Can be anonymous	Example
Send	Yes	Payer: "You sent $10 to Bob" Payee: "You've received $10"
Send based on Request	No	Payee: "You've requested $10 from Alice" Payer: "You sent $10 to Bob" Payee: "You've received $10 from Alice"
Request w/ QR (P2P in-person. Like cash payment)	Yes	Payee: "You've requested $10" Payer: "You sent $10 to Bob" Payee: "You've received $10"
POS w/ QR (Like cash payment)	Yes	Payer: "You sent $10 to Starbucks" Payee: "You've received $10"
Pre-authorized push	No	Payer: "You sent $10 to Amazon" Payee: "You've received $10 from Alice"

Table 2: Privacy options.

The regulator should be able to allow/disallow transaction anonymity for all transactions on the ledgers in its jurisdiction and indicate whether it can be overridden by the payer or not.

Smart contracts for programmability

General-purpose blockchains make programmability a key feature. However, this comes with a heavy price. The throughput of the DLT suffers significantly.

M10 takes a different approach: instead of running the smart contract as part of a blockchain, a smart contract is run as an external trusted program.[10] The smart contract can be a client of multiple M10 ledgers and the counterparties deposit assets to M1 accounts held by the contract. The smart contract can include any digital asset supported by the M10 system and conditions are created through a GUI or API.

For example, if there are two counterparties, each holding a different asset on a different blockchain, the contract could do an atomic swap of their assets and the counterparties do not have to trust each other.

10 General purpose DLTs typically include a fully Turing complete system to enable programmability of transaction behavior. In contrast, at M10 we provide a select set of limited programming primitives that external services can leverage to achieve the same behaviors without the weight of a fully Turing complete system.

Example use cases

An RLN can serve most payment use cases. In this section, we'll describe three common applications of RLN: domestic instant payments, cross-border instant payments, and programmable payments.

Domestic instant payments

The shared hierarchical ledger enables instant settlement between banks and their customers on the network. This includes payments between individuals (P2P), between businesses (B2B), and from individuals to businesses (C2B). The directory service enables the lookup of individuals and businesses by name, email, and phone number. Payments are always "push payments" (credit transfers) and can be pre-authorized to create pull-like (debit transfer) payments.

Cross-border instant payments

Cross-border payments often take a long time (up to 5 days) to settle and can be expensive. The reason for this is the use of the correspondent banking model. While this model has served the international payments industry well for decades, in light of modern technologies, the correspondent banking model is outdated and inefficient.

Instead of routing payments through a number of intermediaries (correspondent banks), point-to-point transactions between banks are instant and low cost. In the M10 system, currency ledgers are interconnected through an FX service. The FX service has accounts on the source and destination ledgers of a transaction and provides liquidity to the transacting counterparties. The shared hierarchical ledgers also enable instant settlement of cross-border payments.

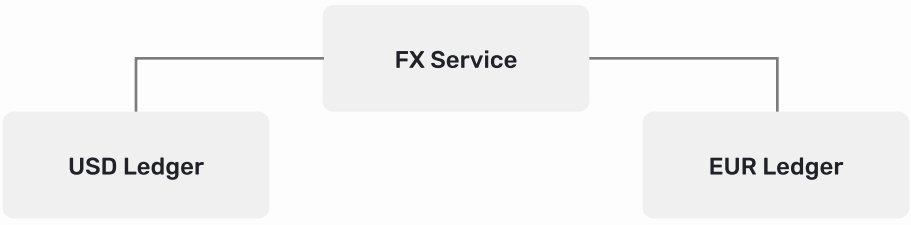

Figure 7: FX service with multiple currency ledgers.

Programmable payments

Through the use of smart contracts, advanced payments use cases can be programmed and executed. FX swaps and repurchase agreements (repo) are some examples.

Consider an FX swap where Bank-X deposits 100M of currency A into a contract and Bank-Y deposits the corresponding amount of currency B into the same contract. The contract pays out currency B to Bank-X and holds currency A. When Bank-X returns the correct amount of currency B into the contract, the contract returns currency A to Bank-X and currency B to Bank-Y (less any fees).

Regulated Liabilities Network benefits

An Regulated Liabilities Network provides a number of benefits:

- Payment modernization can be achieved without upsetting the two-tier monetary system.
- No change in the roles of central banks or commercial banks. Businesses and customers are better served by commercial banks that have the experience and motivation to provide customer service, education, reporting, and innovation.
- No change to national laws required. Banks are already regulated entities. Using the RLN enables them to do things more efficiently but from a regulatory perspective, the banks are doing what they already do today: accept deposits, provide loans, enable payments, provide trade financing, disbursements, remittances, and merchant payment processing.
- An RLN can be highly cost-effective. In the RLN we have described, commercial banks connect their core banking systems to a cloud service. Because of the shared ledgers and platform, there are economies of scale. The reduced reliance on correspondent banking provides additional savings. As does the ability to lower liquidity requirements, since banks can move assets instantly to where they are needed.
- The RLN can be made to be highly secure. As we described, a modern RLN can use state-of-the-art authentication, tokenization, access management, and other tools which are generally not available to your average commercial bank.
- Payment modernization can be realized in a matter of weeks or months. Not in 5-10 years. This is critical in order to respond to the threat of unregulated internet of value.

Regulated Liabilities Network - a stepping stone to CBDC

The Citi Paper sets up RLN as an alternative to CBDC, or perhaps a more universal solution that includes a CBDC as a component of the larger network. While the M10 platform can be used for CBDC from the start, we believe that an RLN that addresses payment modernization is a better starting approach. CBDC can easily be added at a later point in time. Starting with the RLN for payment modernization has a number of benefits:

- **Faster time to market.** The private sector innovates faster than governmental entities. Commercial banks will spend on infrastructure with positive ROI more easily than a central bank which depends on a governmental (and perhaps political) budgeting process.

- **The commercial RLN can be implemented without the need for legal changes.** If a CBDC is later desired, the infrastructure is in place (M0 and M1), and the central bank can request the legal changes necessary to enable it to issue central bank digital money on M0.

- **An RLN as proposed by M10 preserves the two-tier monetary system.** Some types of CBDC, specifically a retail direct CBDC, have the central bank issuing digital currency directly to businesses and consumers, thereby competing with (and potentially marginalizing) the commercial banks. By starting with payment modernization, it is more likely any eventual CBDC will be a hybrid or synthetic CBDC in which the commercial banks continue to maintain their role vis-a-vis businesses and customers.

Build a Regulated Liabilities Network now

Central banks should protect their country's residents and businesses from the risks of unregulated liabilities. Rather than outlawing unregulated liabilities, which would become a game of whack-a-mole, central banks should encourage and support providers of regulated liabilities to join forces in a network that delivers attractive customer experiences and reduces the demand for unregulated liabilities.

Implementation of an RLN with all its stated benefits is feasible now. The turnkey solution is available from M10 today.

About the authors

Marten Nelson, Co-founder and COO at M10

Marten Nelson is the co-founder and COO of M10 Networks, developer of digital money technology for banks and central banks. Before starting M10, Marten co-founded Token, the industry leader in API platform solutions for banks and developers and served as its CMO. He is a member of ITU's Global Digital Currency Initiative and was a member of the Federal Reserve's Faster Payments Task Force and is a frequent contributor to reports and discussions on CBDC and other digital currency forms. Marten has a track record of creating new markets with ground-breaking technologies in email security, open banking and edtech.

Richard Char, SVP Business Development and General Counsel at M10

Richard Char is the head of business development and general counsel at M10. He has been a legal adviser and senior business development executive with leading financial technology companies for over 30 years. Prior to joining M10, Richard was most recently global head of business development at Verifone where he established Verifone's partnerships with companies such as Visa and Mastercard, First Data and Vantiv, Apple, Google and Samsung, Richard was Managing Director at Citibank's Global Enterprise Payments group, where he helped to launch Citi's first consumer digital wallet and personalized digital offer platform.

Chae An, CTO at M10

Chae recently joined M10 Networks as CTO after various roles at IBM for over 30 years in technology research and development in the financial services industry as well as the manufacturing industry. Most recently at IBM, he was the global CTO for IBM's financial services business, leading the innovations and technical strategy work with banks around the world, including core transformation, open-banking, blockchain, and other technology and business innovations. Chae led the creation of payments solutions business at IBM and he and his team deployed the enterprise payments solutions at many large banks and national infrastructures around the world.

Your Questions

M10 will gladly answer any questions you may have to further deepen your knowledge about M10. Please contact us at info@M10.io.