M10

System overview of the M10 platform

Introduction

CBDC solutions and payment modernization software can be simple in concept but complex in the number of different modules needed to build an overall system. Evaluating functionality alone is not adequate and will have costly implications concerning maintenance, scalability, and extensibility unless the complete system is designed to work in harmony with existing banking and payment systems.

With feedback from banks, bank governors, and finance experts, M10 designed a turnkey solution that works with central banks and commercial financial institutions for CBDC and payment modernization solutions.

The following functional and technical requirements influence the design of the M10 platform:

- Control of M0 money supply by the central bank and M1 money by commercial banks.
- High transaction throughput to handle peak payment volumes
- Data privacy and protection
- Data Storage, onshoring
- End-to-end security
- Extensible platform to connect with external services (KYC/AML, ISO20022, etc.)
- Real-time payments & settlement of equities in seconds
- Audit Trail and Account Recovery
- Shared ledger access & connectivity between financial institutions

© 2020, M10 Networks, Inc. All rights reserved.

System Architecture

The M10 service is a cloud solution that scales linearly to process millions of payments per second. The ledgers are available 24x7, allowing payments to be settled instantly in the same currency or across currencies.

A trusted party hosts the ledger in multiple independent data centers where each data center validates its peers. A currency ledger may be hosted in-country to support onshoring requirements.

In addition to the ledgers, other shared services include Directory, FX Exchange, AML/CFT, sanctions screening, smart contracts, and more.

A transfer between two parties is performed on a shared ledger. Through a digitally signed instruction, the payer informs the shared infrastructure to transfer funds from her digital account to the payee's digital account.

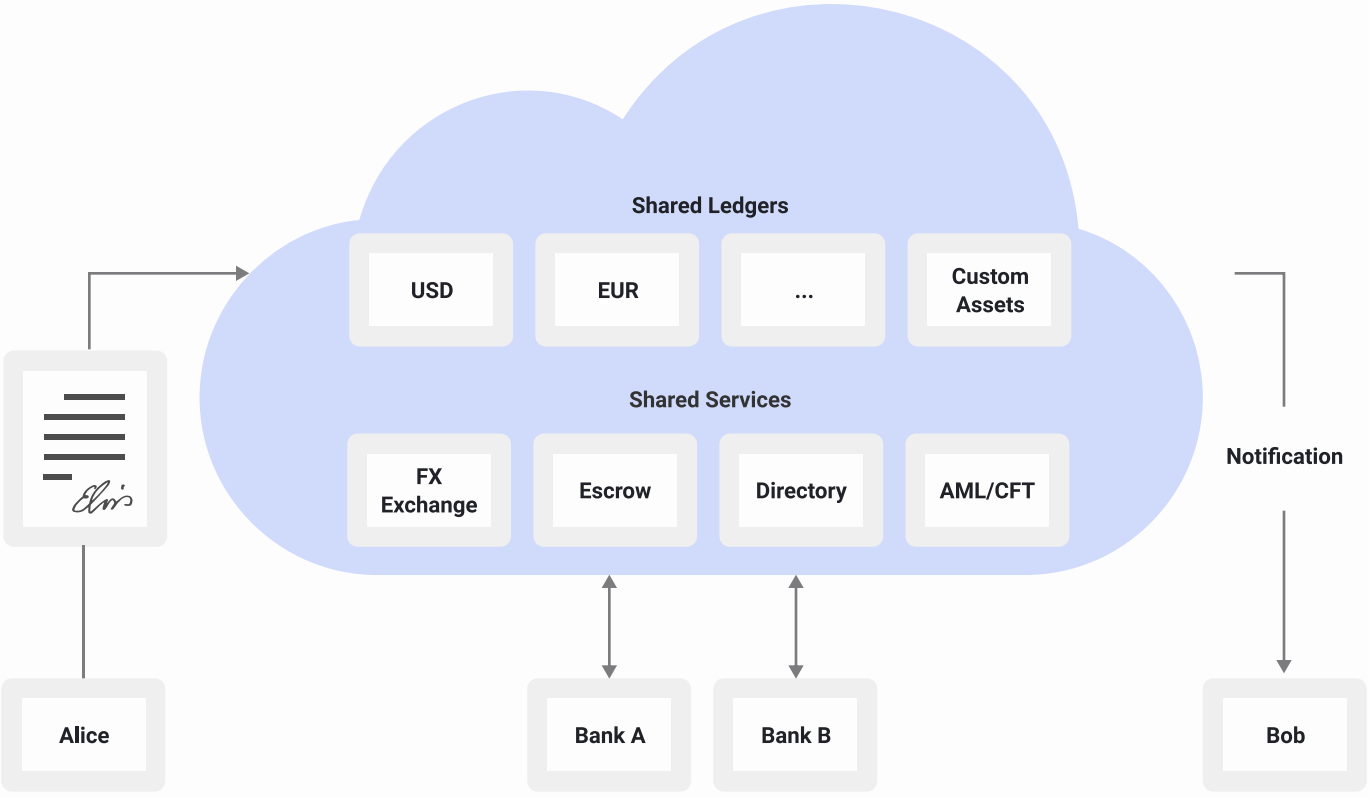


Figure 1: M10 cloud-based architecture

© 2020, M10 Networks, Inc. All rights reserved.

How does it work?

At the core of the platform is the shared hierarchical ledger, which preserves the two-tier monetary system used today while providing real-time payment capability. The shared nature of the ledgers allows participating banks to settle payments instantly.

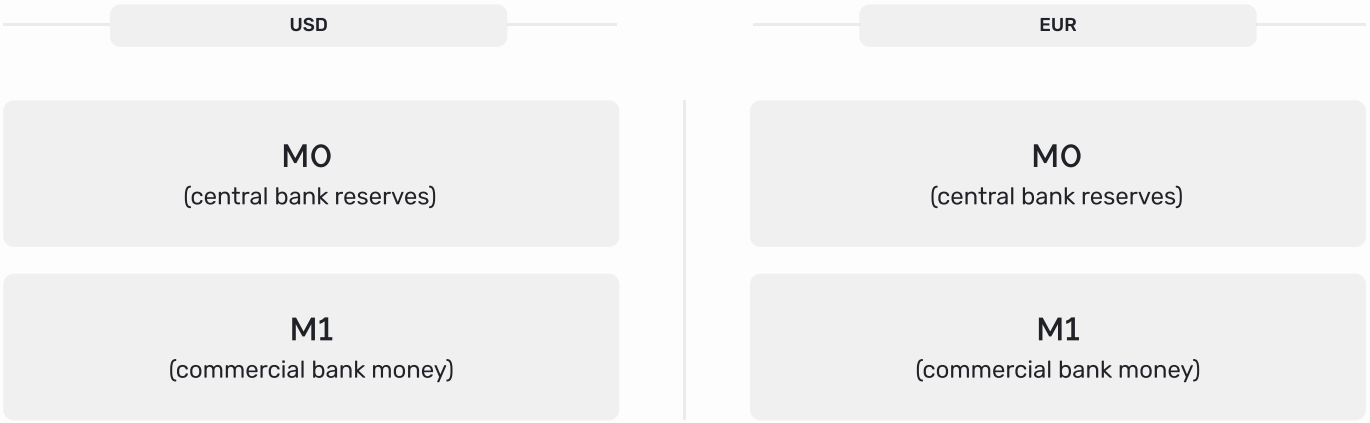


Figure 2: Shared hierarchical ledgers.

© 2020, M10 Networks, Inc. All rights reserved.

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 of 5 units of a currency between two customers at two different banks.

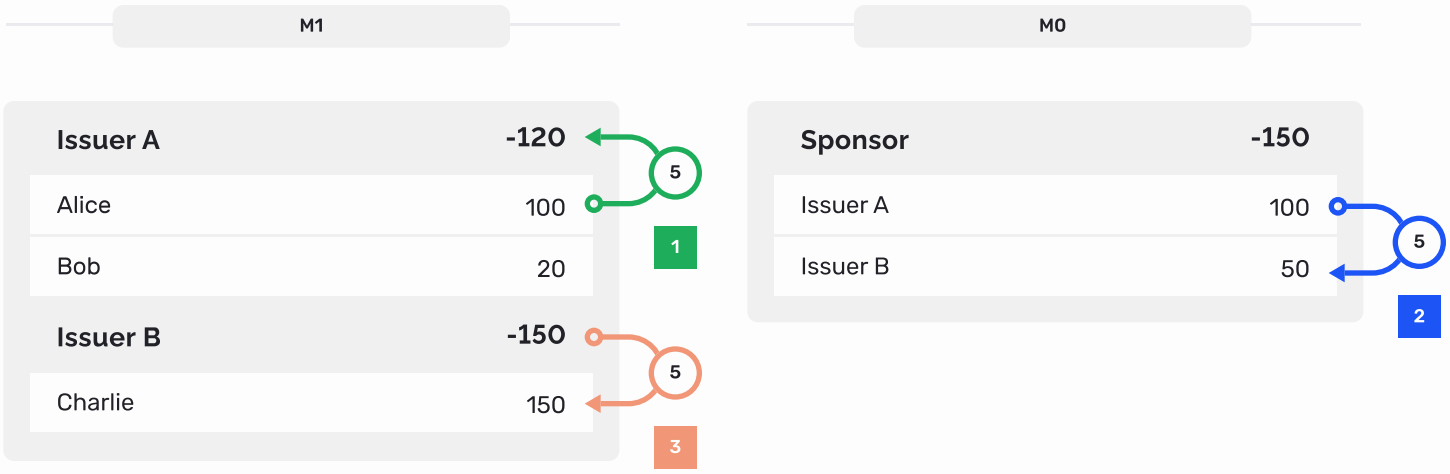


Figure 3: Intra-bank transfer.

1. Payer's M1 digital account is debited and the Issuer is credited (DR Alice / CR Issuer A).
2. Funds are debited and credited between the Issuers in M0 money (DR Issuer A / CR Issuer B).
3. Issuer B is debited, and the payee's M1 digital account is credited (DR Issuer B / CR Charlie).

© 2020, M10 Networks, Inc. All rights reserved.

Inter-bank settlement with FX

In M10, moving funds between different banks and currencies can be done in multiple ways.

Figure 6 shows a common method which includes five transactions. Presume Alice wants to send EUR 10 to Jacques, a client of the French bank, Bank C. (For this example we assume a EUR-USD exchange rate of 1.10).

(If desired, a bank can be the exclusive FX provider for its clients.)

1. M1 (USD): DR Alice / CR Bank A's FX account
2. M0 (USD): DR Issuer A / CR FX Service
3. M0 (EUR): DR FX Service / CR Issuer A
4. M0 (EUR): DR Issuer A / CR Issuer B
5. M1 (EUR): DR Issuer B / CR Jacque

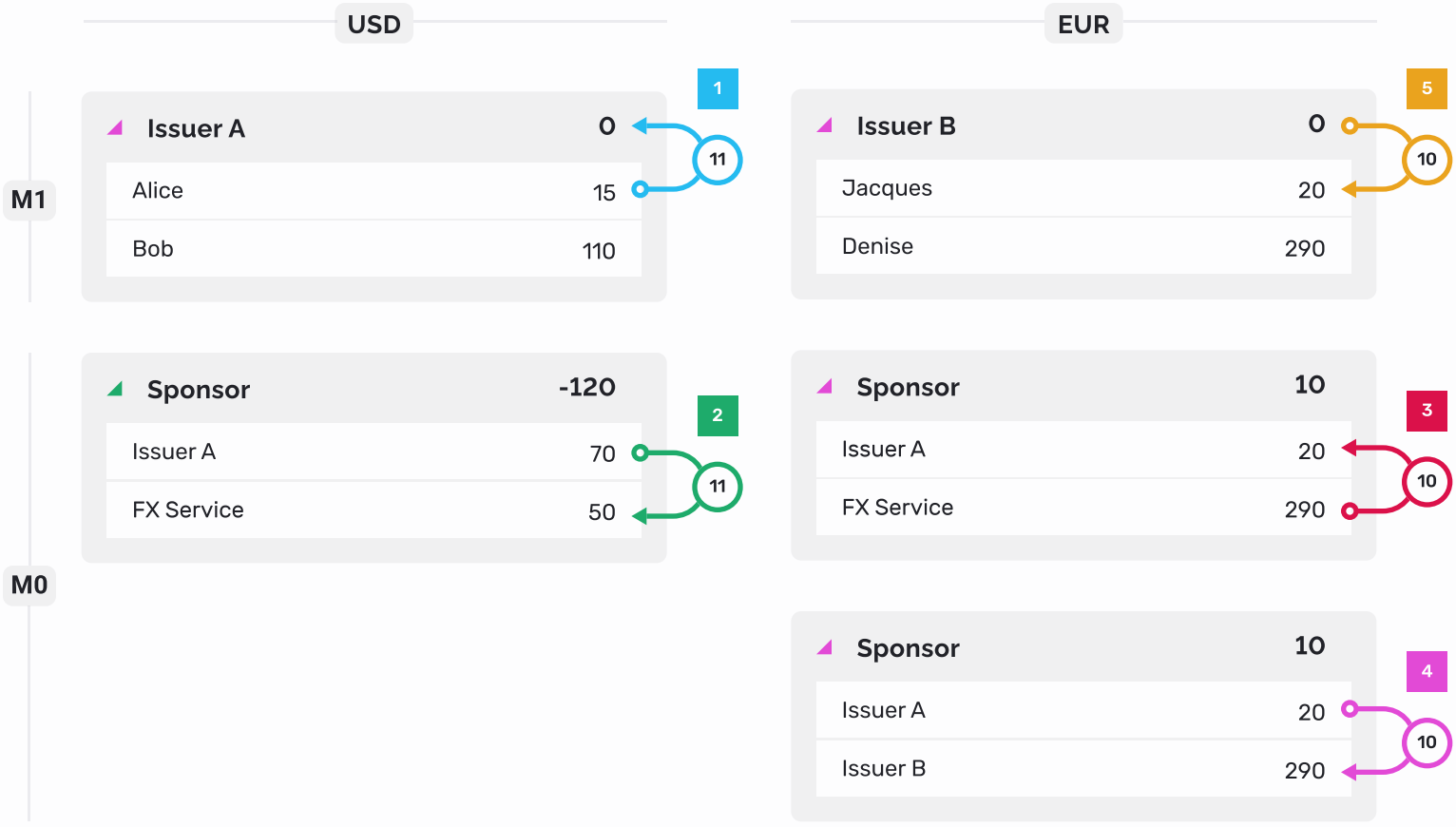


Figure 4: Moving funds to an account at a different bank in a different currency

© 2020, M10 Networks, Inc. All rights reserved.

Payment flows

Below are simplified diagrams to understand the interactions between users, banks, and the M10 platform. Details of the interworking of the M10 platform is discussed under the key components section (page 11).

1. Account Creation - M10 platform with Bank Integration
2. Account Loading from Bank
3. Account Unloading to Bank
4. Payment - Single Currency
5. Cross Border Payment - with FX

© 2020, M10 Networks, Inc. All rights reserved.

1. Account Creation - M10 platform with Bank Integration

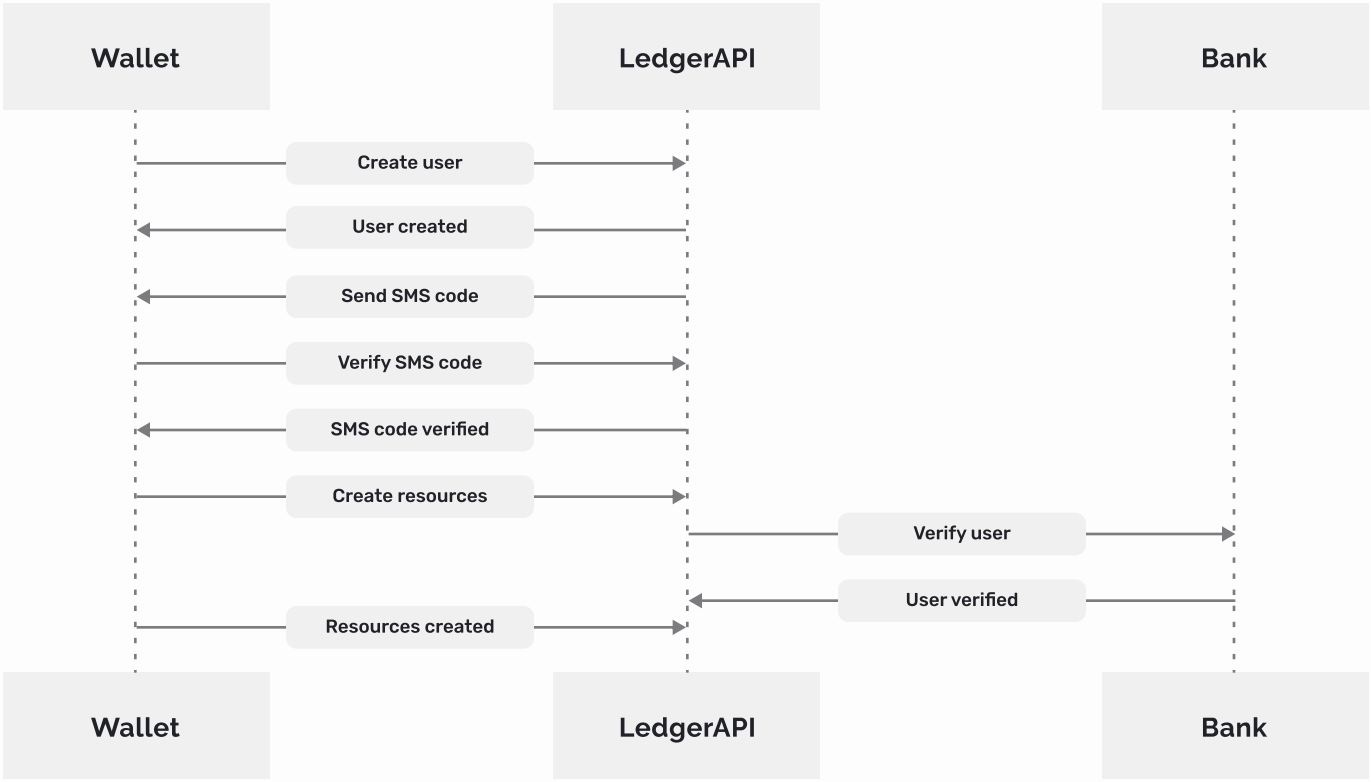


Figure 5: Account creation with Bank Integration

© 2020, M10 Networks, Inc. All rights reserved.

2. Account Loading from Bank

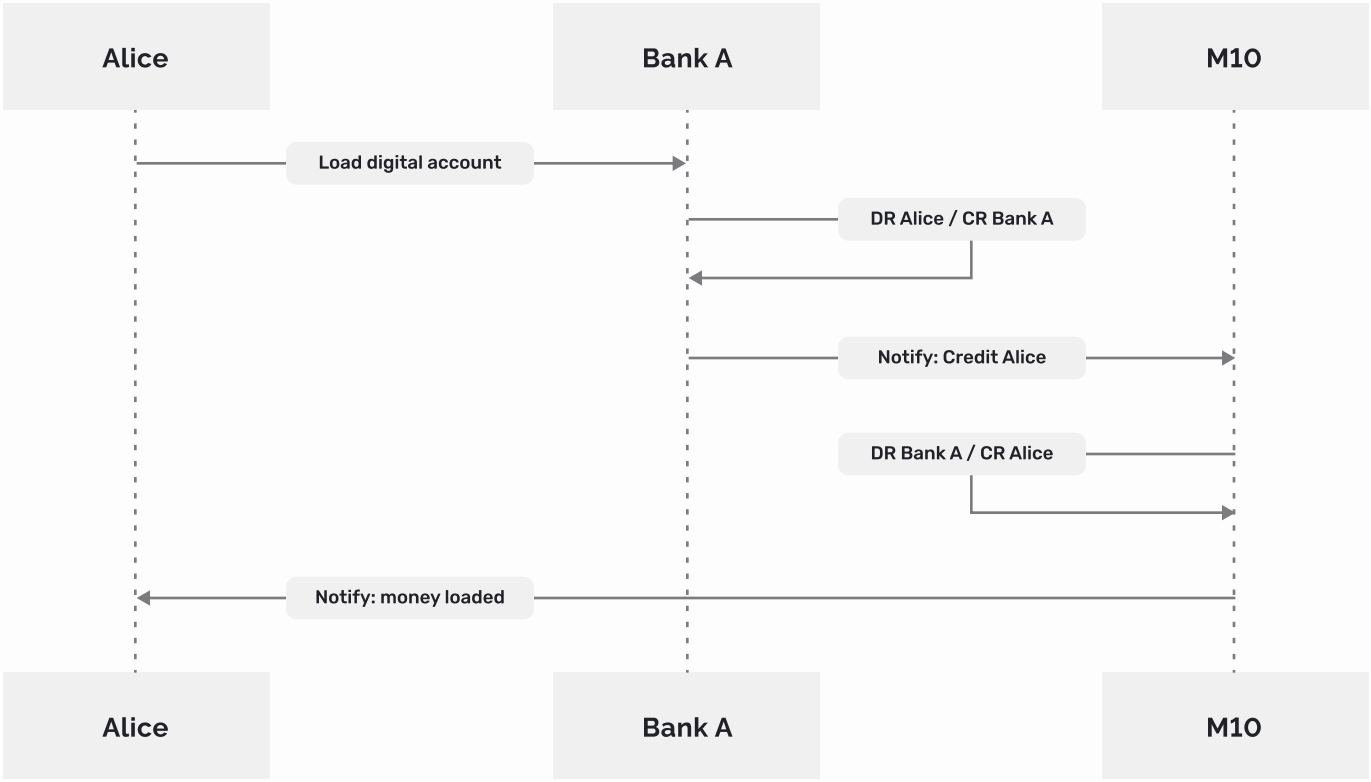


Figure 6: Account Loading from Bank

© 2020, M10 Networks, Inc. All rights reserved.

3. Account Unloading to Bank

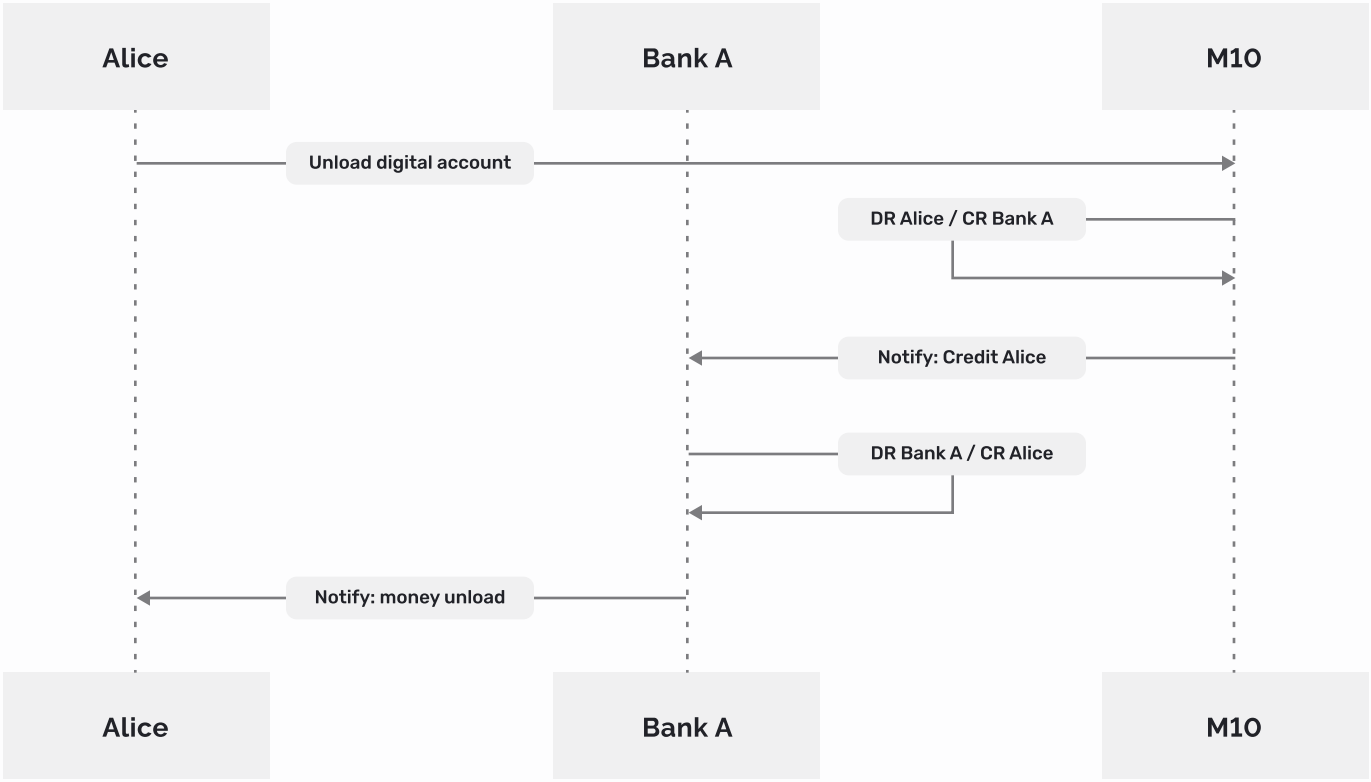


Figure 7: Account Unloading to Bank

© 2020, M10 Networks, Inc. All rights reserved.

4. Payment - Single Currency

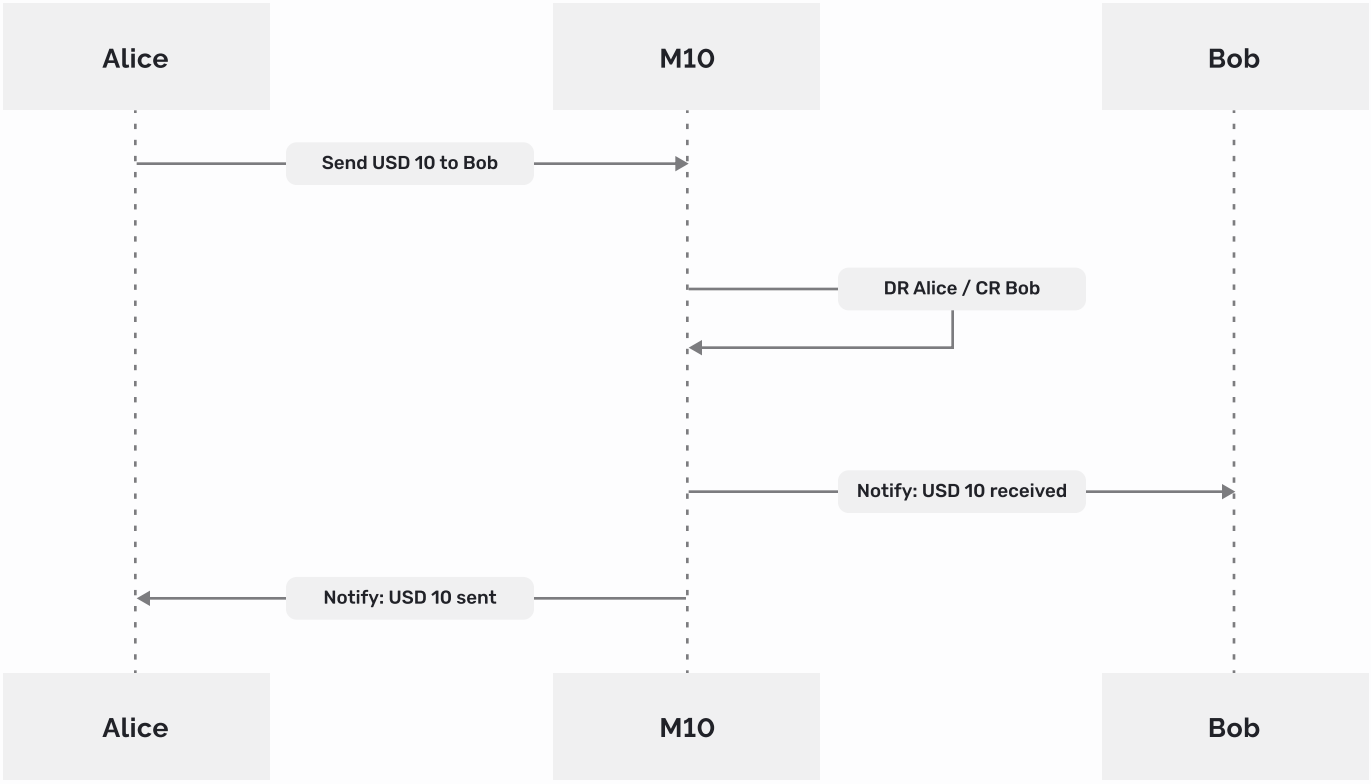


Figure 8: Payment - Single Currency

© 2020, M10 Networks, Inc. All rights reserved.

5. Cross-Border Payment - with FX

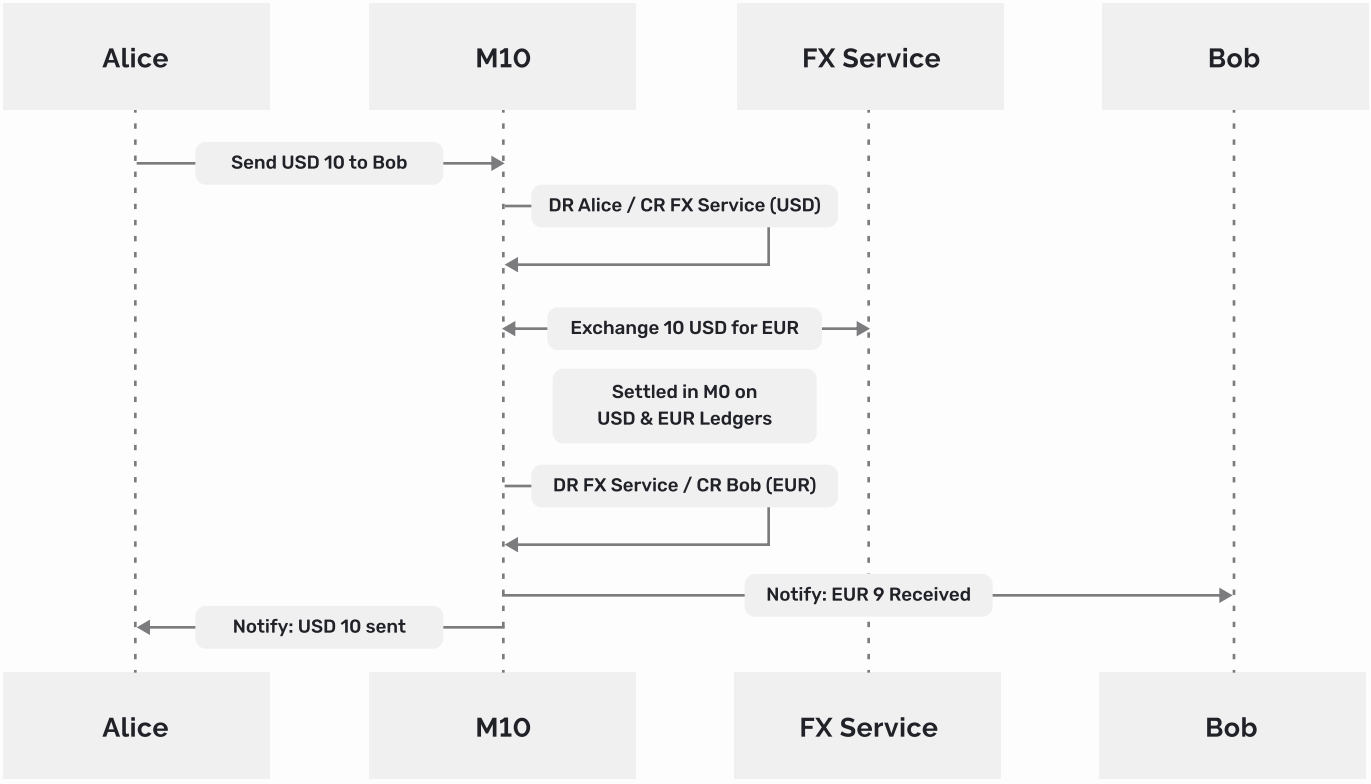


Figure 9: Payment - Multiple Currencies. (In this case the FX Service is the remitter)

© 2020, M10 Networks, Inc. All rights reserved.

Key components

For a turnkey system, M10 has developed the core system with six components needed to run a CBDC or modern payments system. Each of the components serves an essential function and is horizontally scalable based on load. In addition to high availability, state and transaction data is recoverable if a system outage or network failure.

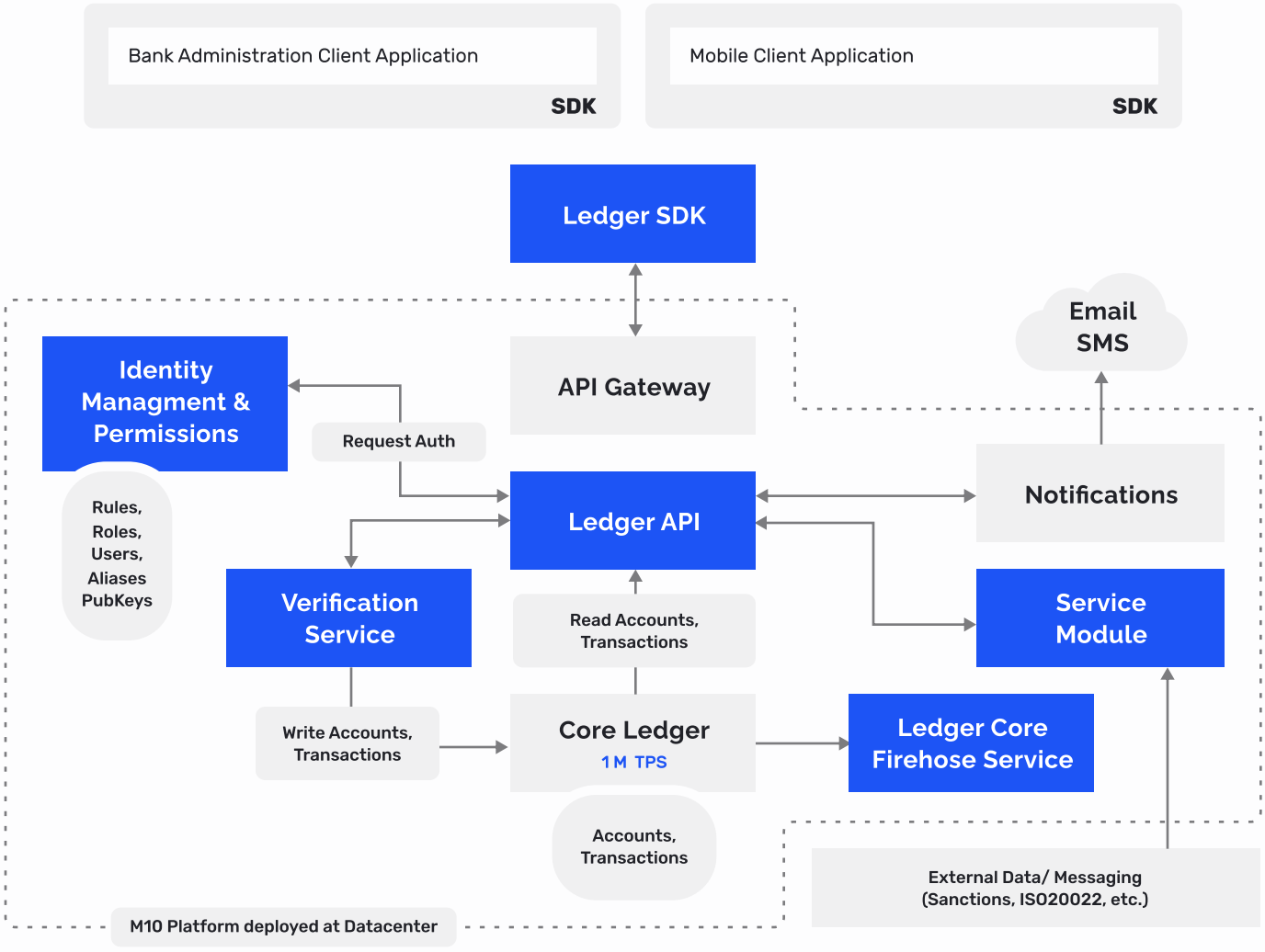


Figure 10: Higher level architecture

© 2020, M10 Networks, Inc. All rights reserved.

1. Core Ledger

The core ledger records the transactions and account balances between the banks and the users of the system. Its hierarchical nature allows it to be highly configurable to mimic how current banking relationships work today, but with the advantage of instant settlement for real-time payments via the shared ledger.

The core ledger addresses the challenges of:

- High transaction throughput to handle sustained peak payment volumes
- Control of M0 money supply by the central bank and M1 money by commercial banks.

pBFT Ledger

M10's ledger is a custom Practical Byzantine Fault Tolerant (pBFT) ledger, capable of processing 1M+ payment transactions per second and with the inherent property of being 1/3 fault-tolerant where 1/3 of the nodes can be faulty while the system is still being operational. A single currency ledger consists of three nodes: a proposer/voter and two voters who form a committee that finalizes endorsed blocks of transactions.

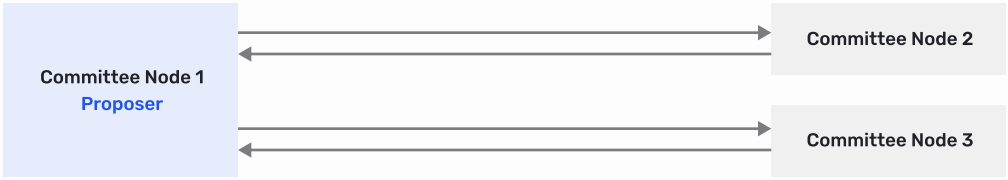
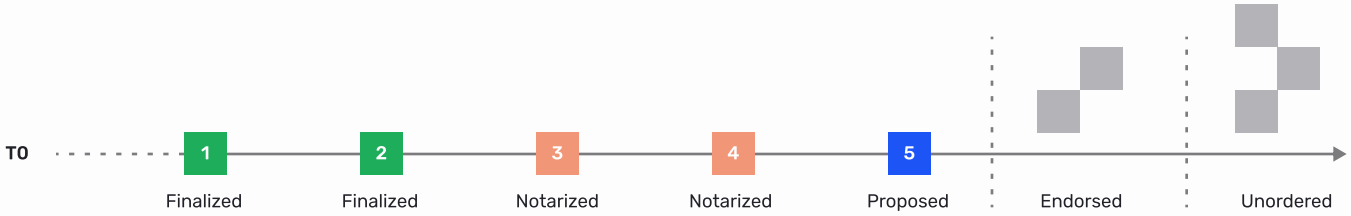


Figure 11: Committee Node1 proposes new blocks (transfers) to the other committee nodes to vote on.

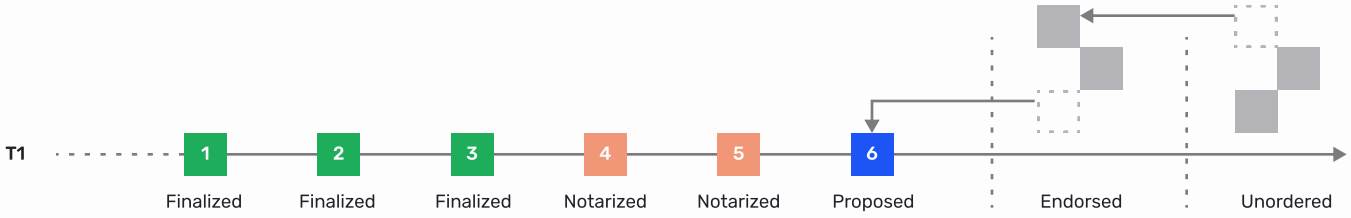
© 2020, M10 Networks, Inc. All rights reserved.

Transactions are batched into blocks for the committee nodes to process. This process consists of four steps:

1. Endorse block of transactions;
2. Proposer node proposes a block of transactions;
3. Voter nodes notarize the block of transactions;
4. The block of transactions is finalized to the chain



Linear view of the chain as transactions are added.



As the block's signature is verified, it moves into the "Endorsed" state then "Proposed" as it's processed.

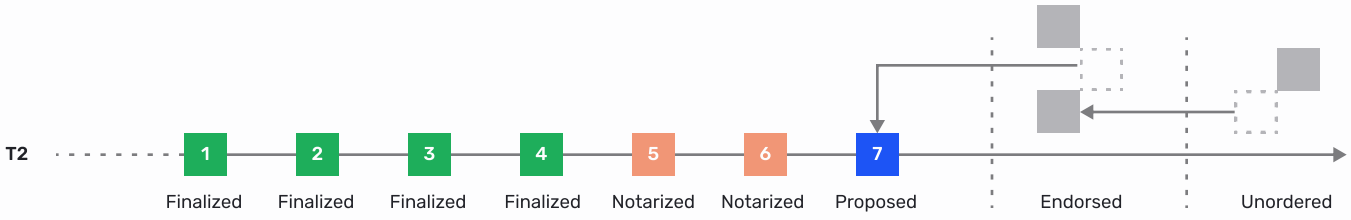


Figure 12: Sequence of processing new blocks (payment transfers) with the Committee nodes voting on the blocks.

© 2020, M10 Networks, Inc. All rights reserved.

Hierarchical ledger; M0 & M1 money representation

The hierarchical ledger requires a sponsor bank to manage a specific currency. The sponsor bank is responsible for the oversight of monetary policy and the issuing banks using its currency. This role of the sponsor bank would be ideally filled by the Central Bank or a bank operating on behalf of the Central Bank.

The sponsor bank controls M0 funds. An issuing bank with M0 funds may issue M1 funds to its customers. Depending on the issuing bank's legal framework, the issuing bank may implement fractional reserve banking.

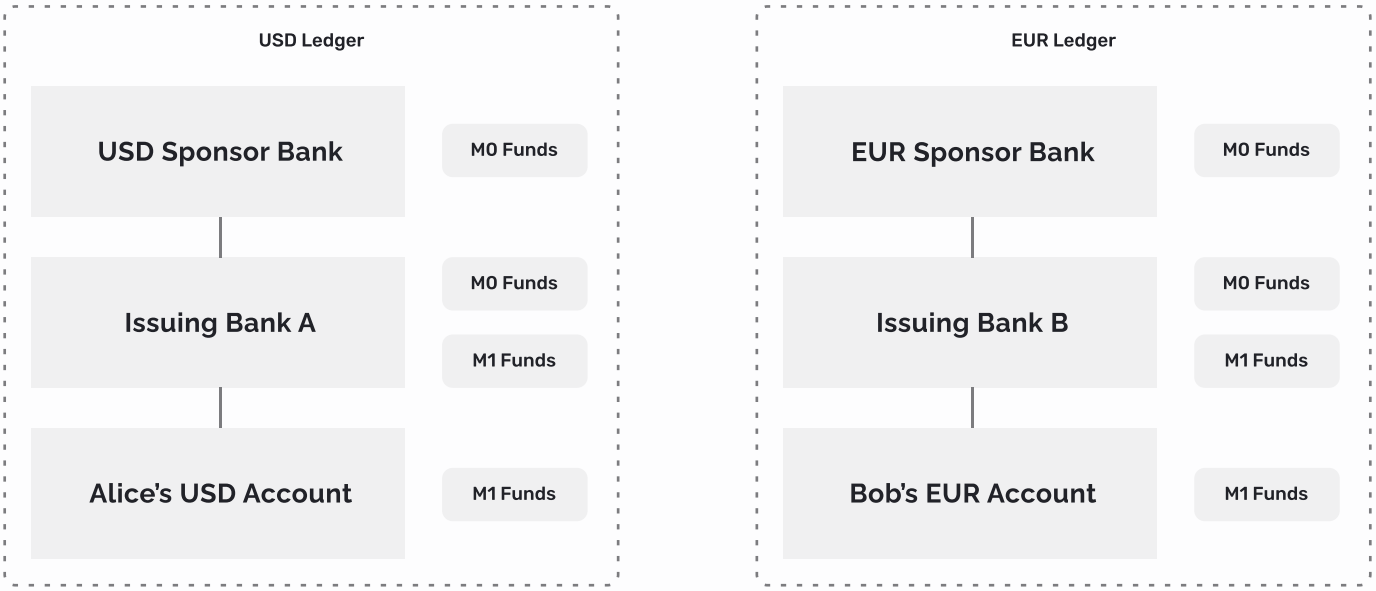


Figure 13: Account relationship within a ledger.

© 2020, M10 Networks, Inc. All rights reserved.

Portfolio / Account relationship

While each currency ledger represents accounts that banks and users have for a single currency, there's a need for a portfolio hierarchy to manage multiple accounts and financial instruments (digital money, equities, bonds, etc.). For banks and users, the portfolio object is created as a collection of "personal accounts" with underlying ledger accounts for various instruments.

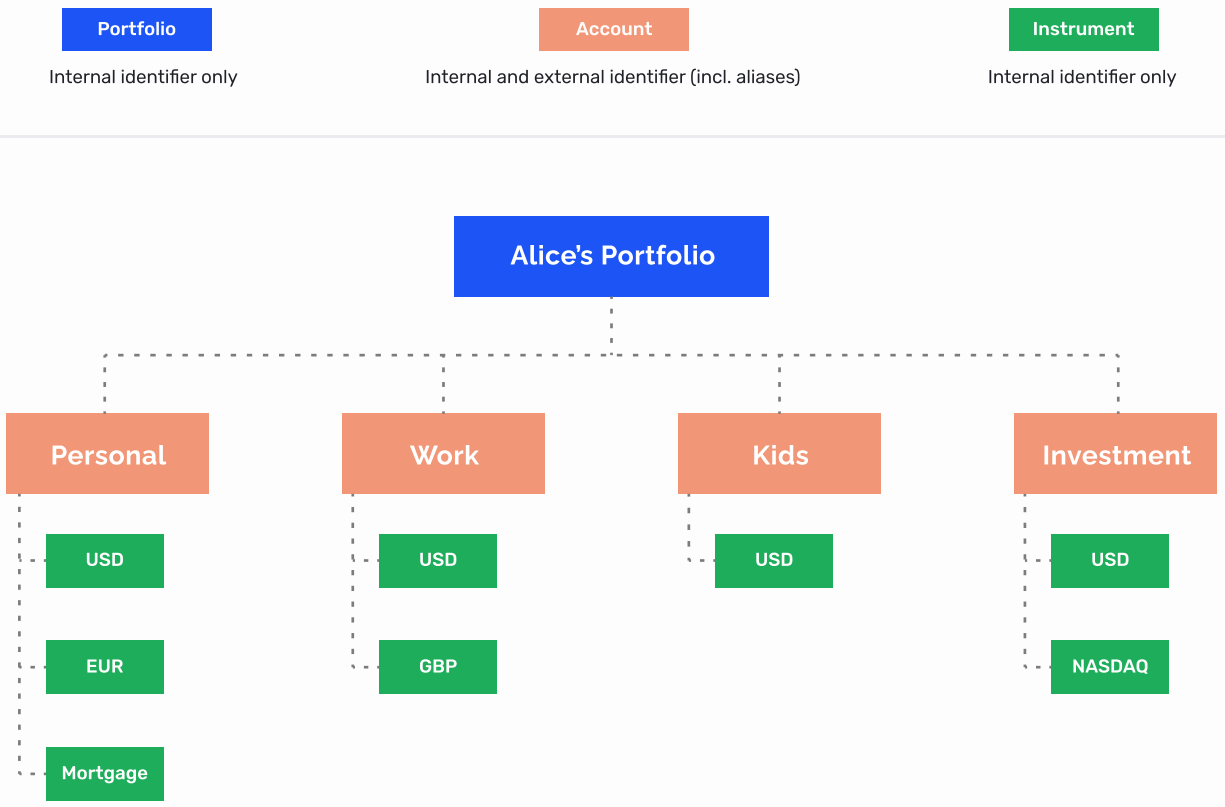


Figure 14: Relationship between Portfolio, Personal Accounts and Instruments.

© 2020, M10 Networks, Inc. All rights reserved.

2. Identity Management & Permissions System (RBAC) - Security

Identity Management and Permissions Systems are an integral part of how accounts are resolved and accessed. The systems need to have fast global access while also providing the security to prevent attacks that rewrite access to user accounts. M10's identity and permissions system addresses:

- Authentication
- Data privacy
- End-to-end security
- Access & delegation
- Directory services

Authentication

Participants in the M10 ecosystem are authenticated with digital signatures generated with a private key and verified with a public key. Aliases resolve an account's public key while email addresses and phone numbers verify account information.

Mock data set for a customer

Public Key	Alias
Name	Portfolio
Email	→ Accounts
Phone	→ → Instruments

By leveraging public / private key access to accounts, it eliminates passwords and provides the best security solution available today. The public key, account holder details, and the alias are stored in a data structure that can be expanded if there's a need to keep other customer and account-level information.

© 2020, M10 Networks, Inc. All rights reserved.

Data privacy

With the requirements of GDPR, customer data privacy is a crucial consideration when deciding on what data is collected, stored, and managed on the platform. Only information deemed necessary to identify and verify a customer and account ownership is stored. The system does not store data that can be retrieved from other systems (e.g., a bank's directory). For security and compliance purposes, the M10 system will persist the minimum amount of information needed to identify a user and their portfolio.

End-to-end security

Account and transaction data are stored on the currency ledger while user information is stored on the global directory ledger. Data at rest or on the ledger is encrypted and can only be accessible by those who have permission to the account. For a typical end-user account, the user and the onboarding bank are the only ones that can access the encrypted data.

Whether from an internal or external interface, data in transit is protected via TLS encryption to protect the data from being exposed. All messages are digitally signed and verified by the verification service. Added security can be provided by using the user's public key to encrypt the account data when in transit.

Access & delegation

Private/public keys to access the M10 account are created during the account creation process. An account holder can delegate different levels of access to her account.

© 2020, M10 Networks, Inc. All rights reserved.

Directory services

The directory service is a global system that provides alias/account resolution. On average, to process a payment requires four queries (resolve payer and payee, payer's bank, and payee's bank account details).

M10 uses a distributed ledger for the directory data. Since the directory can be used for global deployment and lookups between institutions, ledger properties that guarantee immutability is desirable to prevent attacks and account takeover scenarios.

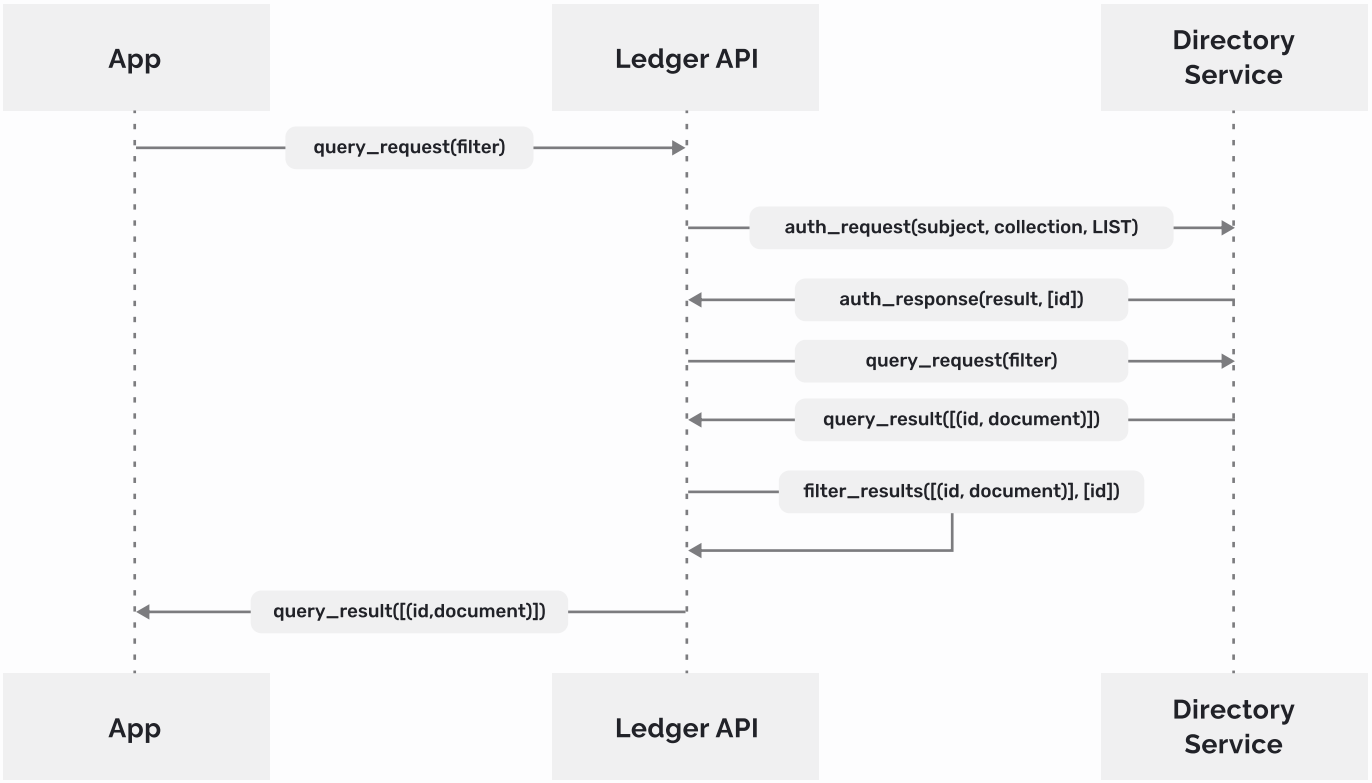


Figure 15: Querying the directory service for account-related information.

© 2020, M10 Networks, Inc. All rights reserved.

3. Verification Service

To prevent malicious attacks, the system only accepts digitally signed requests. The role of the verification service is to verify signatures before recording requests on the ledger.

The verification service processes requests in batches. Each request signature and part of the associated content is verified before submitting a single signed payload to the ledger.

The verification service is a critical component, so the system's operator must store the private key safely. A leaked private key could potentially provide a malicious actor the ability to bypass signature verification.

Signature verification is an expensive operation. By separating signature verification from the ledger itself, we achieve significant performance gains.

The system uses SGX acceleration to optimize the throughput of signature verification further. SGX also ensures the verification code isn't tampered with and safeguards the private key.

© 2020, M10 Networks, Inc. All rights reserved.

4. Ledger API & Ledger SDK

Ledger API

The Ledger API, from an external view, is a gRPC protocol API that provides functionality to create, fetch, query account, and transaction information.

The Ledger API, as an internal service, provides:

- Message routing
- Interaction within the platform
- Subscriptions (for notifications)
- API signing (for verification)

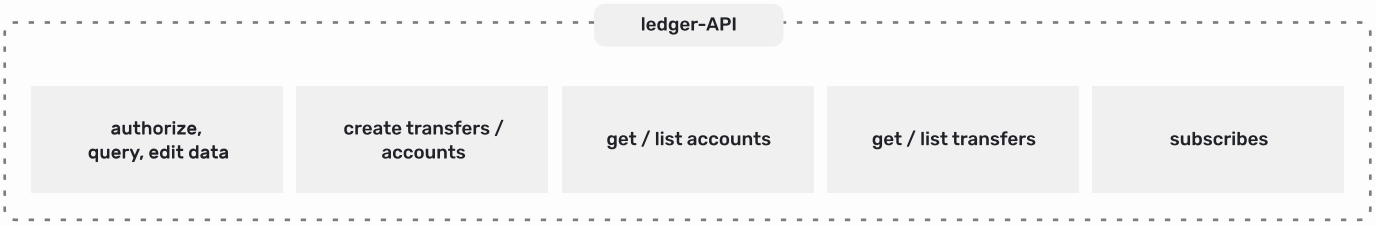
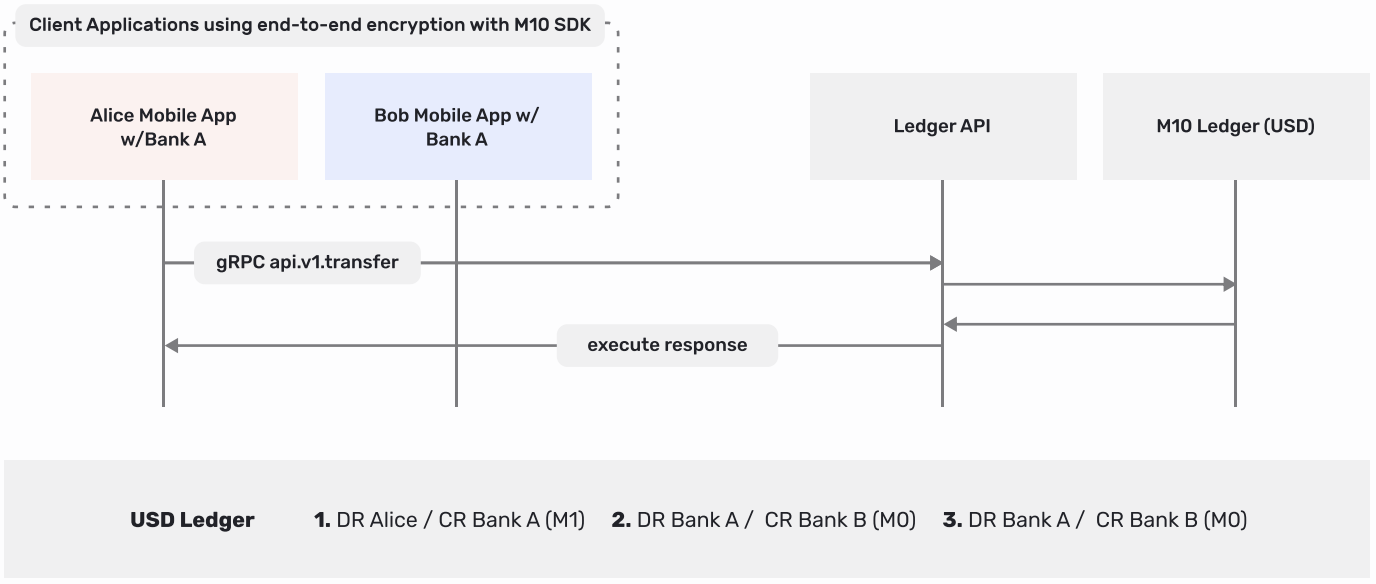


Figure 16: Ledger API capabilities



USD Ledger **1.** DR Alice / CR Bank A (M1) **2.** DR Bank A / CR Bank B (M0) **3.** DR Bank A / CR Bank B (M0)

Figure 17: gRPC call to transfer $200 USD between Alice at Bank A to Bob at Bank B.

© 2020, M10 Networks, Inc. All rights reserved.

Ledger SDK

To simplify the usage of the Ledger API and the signing of the request for the M10 platform, the Ledger SDK abstracts out the complexities of signing and verifying messages.

Each call into the SDK is broken down into four main steps:

1. Composition and serialization of the request payload
2. The signing of the (serialized) request
3. Composition of the gRPC Protobuf message
4. gRPC call to Ledger API Service for transmission

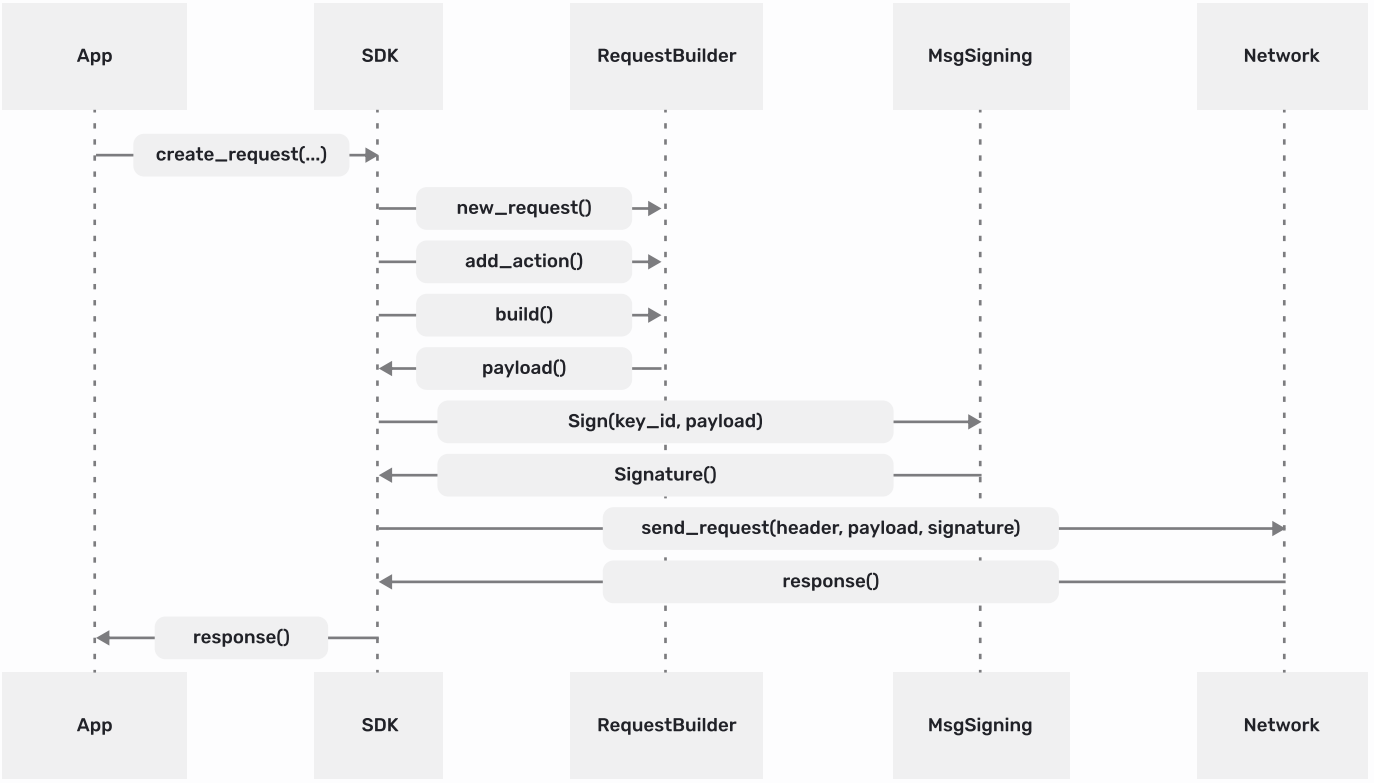


Figure 18: SDK preparing a request (payload & signing) to be sent.

© 2020, M10 Networks, Inc. All rights reserved.

Example SDK calls

Create User with Alias

```
Future<List<int>> createUserWithAliases({
  @required String name,
  @required User_UserCreationType userCreationType,
  String handle,
  String email,
  String phoneNumber,
  String defaultInstrument,
  String roles,
  List<User_SearchableAlias> searchableAliases,
})
```

Create User Portfolio

```
Future<List<int>> createPortfolio({
    List<int> portfolioId,
    @required List<int> userId,
    @required String name,
    @required List<int> bankId,
    Portfolio_PaymentType paymentType,
    int limit,
    Portfolio_PortfolioStatus status,
    List<List<int>> accounts,
    List<int> owner,
  })
```

Create a payment to target account (receiver)

```
Future<Transaction> createTransaction({
    @required List<int> account,
    @required List<int> targetAccount,
    @required String amount,
    String memo = "",
    List<int> targetLedgerId,
  })
```

© 2020, M10 Networks, Inc. All rights reserved.

5. Transaction Data & Firehose Events

The firehose service delivers transaction logging to participating banks. The banks subscribe to the service and receive events as the ledger processes payments. The banks use the service to synchronize events on the M10 ledgers with their in-house systems in real-time.

1. High speed & low latency logging of events
2. Data storage / logging & onshoring
3. Real-time data to be used by banks for screening, monitoring, compliance

Each currency ledger is typically deployed within the country or region of the respective currency. This is to satisfies data onshoring requirements.

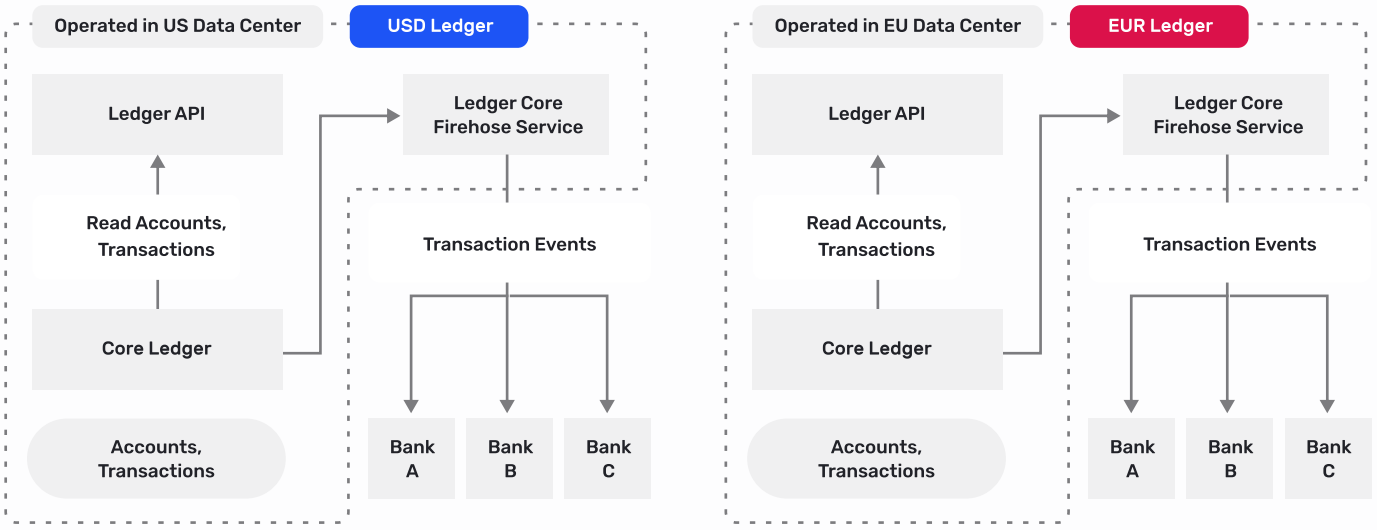


Figure 19: Banks receiving events from Firehose service in respective geographies.

© 2020, M10 Networks, Inc. All rights reserved.

6. Shared Service Modules

The ability to extend the overall system is critical. External services can be integrated directly via the Ledger API (gRPC) or through the Ledger SDK.

External services that can connect to the Service Module:

- Sanctions / AML screening
- ISO20022 messaging
- Exchange software
- Smart Contracts

The Service Module component addresses:

- External data & handling
- Logic & rules for executing transfers

Example:
Sanctions screening can be added as part of the payment flow, validating authorized senders and receivers. ISO20022 handler/parser mapping between M10's APIs and ISO20022 XML syntax.

© 2020, M10 Networks, Inc. All rights reserved.

Regulatory compliance

M10 is a network that banks join as Issuers. The liability for regulatory compliance resides with the Issuers. Individuals and businesses participating in the M10 ecosystem have been on-boarded by their Issuer, who is responsible for KYC.

The M10 system includes modules for AML/CFT and sanctions screening that can be used by participating Issuers as a further check on 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.

© 2020, M10 Networks, Inc. All rights reserved.

Conclusion

The M10 platform is a complete payment modernization system. The advantage is its completeness as an "out of the box" solution for central banks and commercial banks. The M10 platform can be deployed in either a public or private cloud infrastructure and realizes the benefits of real-time payments without any extensive integration effort. The system is suitable for both wholesale and retail payments.

Key benefits of the M10 solution:

- Control of M0 money supply by the central bank and M1 money by commercial banks
- High transaction throughput (1M+ tps) to handle sustained peak payment volumes
- Real-time payments & settlement of equities in milliseconds
- Shared ledger access & connectivity between financial institutions
- Data privacy and protection
- End-to-end security
- Extensible platform to connect with external services (KYC/AML, ISO20022, etc.)

© 2020, M10 Networks, Inc. All rights reserved.