White Paper

Unified Ledger for Multi-Asset Businesses

Updated Product Developments

Knox Networks

January 2025

Executive Summary

Knox Networks infrastructure software aims to simplify all financial asset management by treating all assets as a “store a value” that can be stored, secured and transacted with uniformity and high efficiency.

Today, businesses are forced to manage various asset types across many disparate financial rails and systems. Introducing new asset types and systems often require changes to existing flows and add complexity. To streamline this process, Knox was designed to help businesses manage their complex financial networks today while preparing for the future of digital assets.

Knox targets problems with a unified way of managing/transacting across a variety of assets and systems. Knox augments the programmability, interoperability, scalability, and real-time monitoring between backend systems, allowing for:

- **Unified Asset View:** Gain a real-time, harmonized view of all assets and currencies, ensuring a single source of truth for accounts.
- **Scalable Streamlined Management:** Manage assets, wallets, and accounts through one ledger, adding asset types at scale without core system changes.
- **System Interoperability:** Integrate seamlessly with both traditional finance and digital asset systems, simplifying interactions with various custody and omnibus accounts and networks.
- **Seamless Privacy:** through open-source standards that protect identification data while also minimizing the need to rip and replace existing systems
- **Programmable Actions:** Execute all transaction types through configurable templates via APIs, including multi-party and multi-asset, using APIs and event-driven architecture.
- **Efficient Operations:** Achieve operational cost savings - e.g., netted settlements with a market maker, batched withdrawals, wallet rebalancing, sweeping, automation, trading, settlement, and more.

Knox was built to bridge the gap between managing traditional financial and digital assets.

Table of Contents

Disclaimer

DISCLAIMER: PLEASE READ THE ENTIRETY OF THIS "DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS, OR TAX ADVICE, AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER KNOX-NETWORKS, INC. (THE "**COMPANY**"), ANY OF ITS TEAM MEMBERS OR AFFILIATES AND THEIR TEAM MEMBERS (COLLECTIVELY, THE "**KNOX TEAM**") WHO HAVE WORKED ON THE KNOX NETWORKS SOFTWARE PLATFORM IN ANY WAY WHATSOEVER, NOR ANY SERVICE PROVIDER OR ADVISORY BOARD MEMBER SHALL BE LIABLE UNDER ANY THEORY FOR ANY DIRECT, INDIRECT OR OTHER LOSS, COST OR DAMAGE WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT HTTPS://WWW.KNOX-NETWORKS.COM (THE **WEBSITE**) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE COMPANY OR ITS AFFILIATES.

THE INFORMATION SHARED IN THIS WHITEPAPER IS NOT ALL-ENCOMPASSING OR COMPREHENSIVE AND DOES NOT IN ANY WAY INTEND TO CREATE OR PUT INTO IMPLICIT EFFECT ANY ELEMENTS OF A CONTRACTUAL RELATIONSHIP, WHICH COULD ONLY BE CREATED BY A WRITTEN AGREEMENT IN A FORM PROPOSED BY THE COMPANY. CERTAIN STATEMENTS, ESTIMATES, AND FINANCIAL INFORMATION FEATURED IN THIS WHITEPAPER ARE FORWARD-LOOKING STATEMENTS THAT ARE BASED ON AND TAKE INTO CONSIDERATION SOME KNOWN AND UNKNOWN CONTINGENCIES, RISKS, AND OTHER DEVELOPMENTS WHICH MAY CAUSE SUCH STATEMENTS TO DIFFER MATERIALLY AND SUBSTANTIALLY IN PRACTICE FROM THE FEATURED ESTIMATES, RESULTS AND/OR CONCLUSIONS PRESENTED OR IMPLIED OR EXPRESSED IN SUCH STATEMENTS.

Glossary

The Knox Networks solution introduces some specific terminology that is referred to in this White Paper.

Term	Definition
Atomic Transaction	A specific type of transaction in which either all legs of the transaction succeed or fail (i.e., it is impossible for only a portion of the transaction to succeed while the rest fails).
Authority Service	Issues newly minted FBDAs into circulation and provides the initial Authorization Signature on FBDAs.
Contract-Based Transactions	Transactions are built on top of the underlying asset layer of FBDAs via Contracts. Contracts help to create configurable transactions that cover a wide range of use cases, including atomic multi-party settlements (PvP, DvP), cross-border payments, escrow, etc., using industry-recognized techniques such as Hashed Timelock Contracts (HTLCs).
Custodial Wallet Service	Transacts and holds FBDAs and owner information. Each wallet can hold a variety of asset types.
Decentralized Identifier (DID)	W3C standard for identifying wallets via Public Key Infrastructure (PKI) in a privacy-preserving cryptographic manner. No sensitive user data is stored. https://www.w3.org/TR/did-core/
Encumbrance and Unencumbrance	**Encumbrance** - The process of locking an asset on an external system while on the Knox platform to ensure it cannot be double spent. **Unencumbrance** - The process of unlocking an asset on an external system while offboarding on the Knox platform.
File-Based Digital Assets (FBDAs)	FBDAs are fixed-value denominated files that include a non-malleable cryptographic proof of historical ownership. FBDAs are brought into circulation via the Distributor Service from Authorized Intermediaries. Can tokenize various asset classes, including but not limited to digital deposits, equities, treasuries, and other asset classes.
Gateway Service	Provides bi-directional, end-to-end streaming connectivity; manages the rate-limiting and denial of service (DoS) preventions; and provides packet routing through networking network activity monitoring.
Hashed Timelock Contract (HTLC)	Transaction methodology that reduces counterparty risk via hash locks and timelocks to force acknowledgment of payment and or forfeit or payment, thereby allowing for atomicity in multi-step transactions/swaps.
Identity Bridge - Credential Adapter Service	Transforms existing KYC/KYB information into VCs issued to the DID of a wallet that cryptographically attests to having a required credential (e.g., having an Account with the institution, being an accredited investor, etc.). The service integrates with the institution's existing KYC/KYB system using a standardized webhook interface but is designed to plug in custom integrations as required.
Identity Bridge - User Management Service	Enables frictionless integration of end-user wallets with financial institutions' existing identity systems using SAML/OIDC. Provides APIs for user discovery using aliases, e.g., Phone number to Wallet Address lookup.
Identity Bridge -	This service is a W3C-defined Verifiable Data Registry, which manages W3C DIDs and DID

Registry Management	Documents associated with each wallet, as well as a revocation list of VCs. Attributes of the financial institutions' DIDs themselves can be searched to identify further discovery services within financial institutions as well as trusted issuers of credentials.
Know Your Customer/ Business (KYC/KYB)	The process by which financial institutions undergo due diligence on customers and businesses for compliance purposes while also assessing the risk of doing business with them.
Payment vs Payment (PvP) and Delivery vs Payment (DvP)	A transaction that involves two parties atomically exchanging assets. Atomic transactions are those that either fully happen or do not happen at all (i.e., party A can only send over assets to party B if and only if party B sends over assets to party A). Examples include: **Payment-vs-Payment** - currency A exchanged atomically for currency B. **Delivery-vs-Payment** - currency A exchanged atomically for security B.
Signature Block	A recursive linked-list structure providing the public key, hash, timestamp and previous signature block. The hash within the most recent signature block is signed by the previous owner and the authorizer's keys, respectively, to create the authorization and transfer signatures. These signature blocks sit within each unique FBDA. **Genesis Signature Block** - the root signature block of an FBDA (n=0) **Transfer Signature Block** - subsequent signature blocks of an FBDA (n>0)
Supplementary Services	Services that are not core to the Knox base technology but can be added on top of the system. Examples include: **Analytics Service** for gaining insights from transactions; or **Reporting Service** for improving internal reporting processes; or **Exchange Service** for interacting with digital asset exchanges; or **Sanctions Service** for plugging in with sanctions/KYC service.
Tokenization	The process of digitally representing assets in a cryptographically protected and verifiable manner.
Transaction Validator Service	The Transaction Validator Service processes transactions via (1) reasoning about the status of the transaction and (2) carrying out the transfer and signing of FBDAs.
Treasury Service	Remits FBDAs denominated in domestic and foreign currencies and holds FBDAs denominated in various currencies for institutions.
Modified Unspent Transaction Output (UTXO)	A method that adopts Unspent Transaction Output (UTXO) principles to Knox's transaction process. Used during transactions to optimize denomination and numbers of FBDAs in circulation.
Verifiable Credential (VC)	W3C standard for digital credentials, representing information from physical credentials such as a bank card or government identification. Digitally signed, tamper-resistant, and instantaneously verifiable. https://www.w3.org/TR/vc-data-model/

Introduction

Knox Networks infrastructure software aims to simplify traditional and digital financial asset management. Today, businesses are forced to manage too many disparate and complex financial rails.

To streamline this process, Knox has created a system to help businesses manage their complex financial networks today while preparing for the future of digital assets.

This White Paper will walk through the Knox system, first focusing on the technical components of the system, followed by what the Knox system enables with these building blocks.

Technology Overview

Knox was created to be modular to fit a variety of different business and operational use cases, but all use cases focus on integrating different data sources to provide financial institutions with a universal source of truth.

Knox is powered by **File-Based Digital Assets** and the **Multi-Asset Transaction Ledger**, which work together to create the technical backbone of Knox through the **Knox System Architecture**. These technologies enable:

- **Programmability through Contract-Based Transactions**,
- **Scalability through Knox's Horizontally Scalable Design**
- **Standards-based Digital Identity on the Knox System, and**
- **Interoperability with Ledger and Traditional Systems**

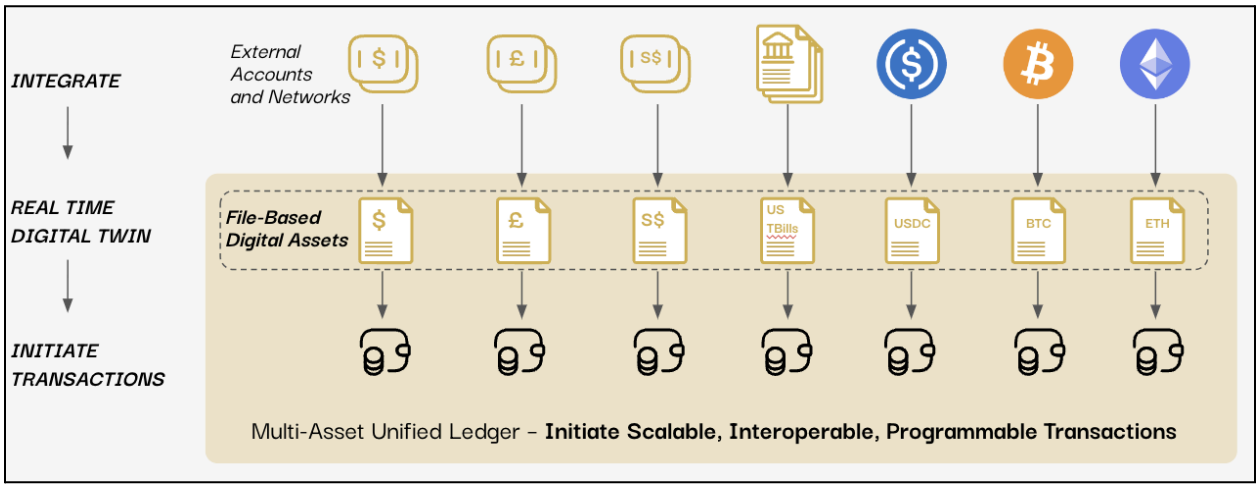
Taken together, these technologies are able to solve a variety of different business problems, which are highlighted under **What Knox Enables**. Following this, a sample unified ledger diagram is shown to showcase the power of the technology. This paper is not intended to be overly technical. Instead, it will refer to the **Developer Portal** for more information on how different technical components work together.

File-Based Digital Assets

The building block of the Knox Network system is the File-Based Digital Asset (FBDAs), which is moved through the system and between stakeholders via the Multi-Asset Transaction Ledger. FBDAs are not actually files but are instead just a conceptual shorthand to simplify their meaning and instead are a common data structure (a JSON Binary Large Object, or BLOB) stored in a traditional database.

FBDAs serve as a common building block on the platform, representing all forms of different assets - whether it be cash, deposits, crypto, securities, or any financial asset. Knox can represent these assets as FBDAs through a couple of different processes, depending on the use case. One process is known as “Digital Twinning” (see picture below), which is used for mirroring assets that exist on an external system. Another process is creating a “Digital Native,” which is used for the direct issuance and movement of assets on the Knox ledger.

This enables a standard digital format so businesses can store, transact, audit, secure, and manage all asset types in a unified manner. Asset provenance when interacting with external systems is guaranteed under **Asset Encumbrance**.



Digital Twinning Assets into FBDAs and bringing them onto the Knox Platform

FBDA Structure

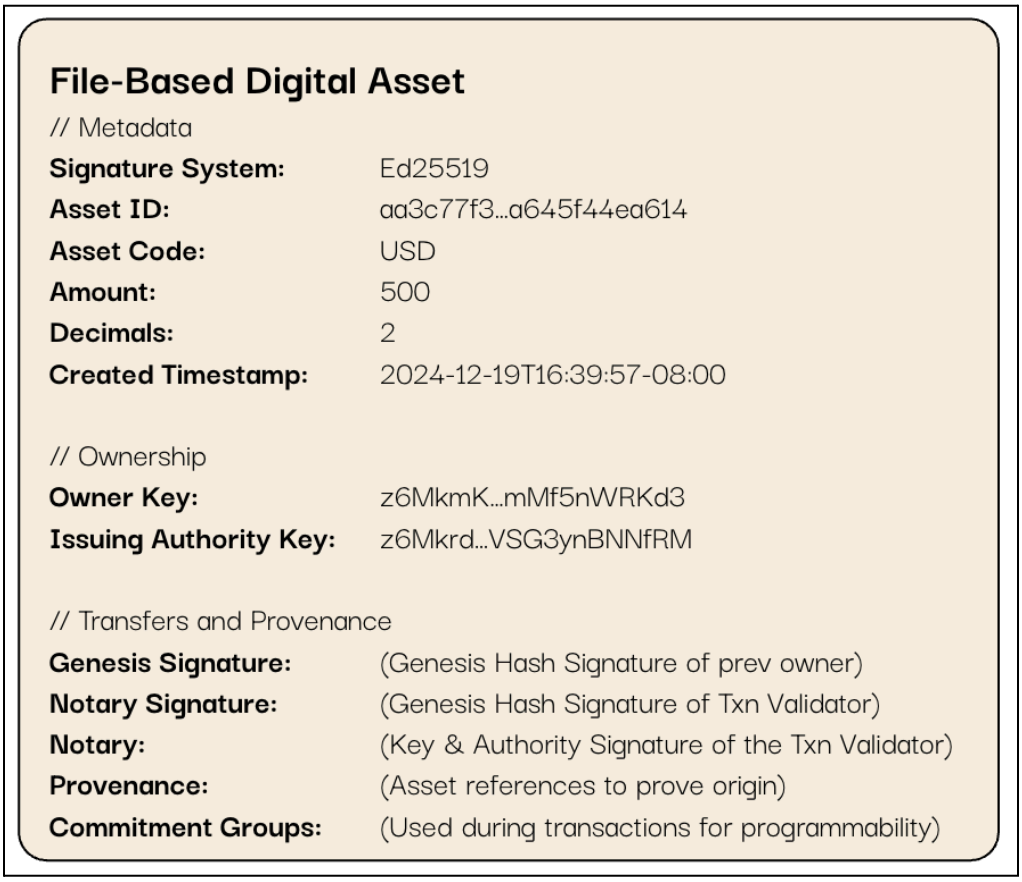


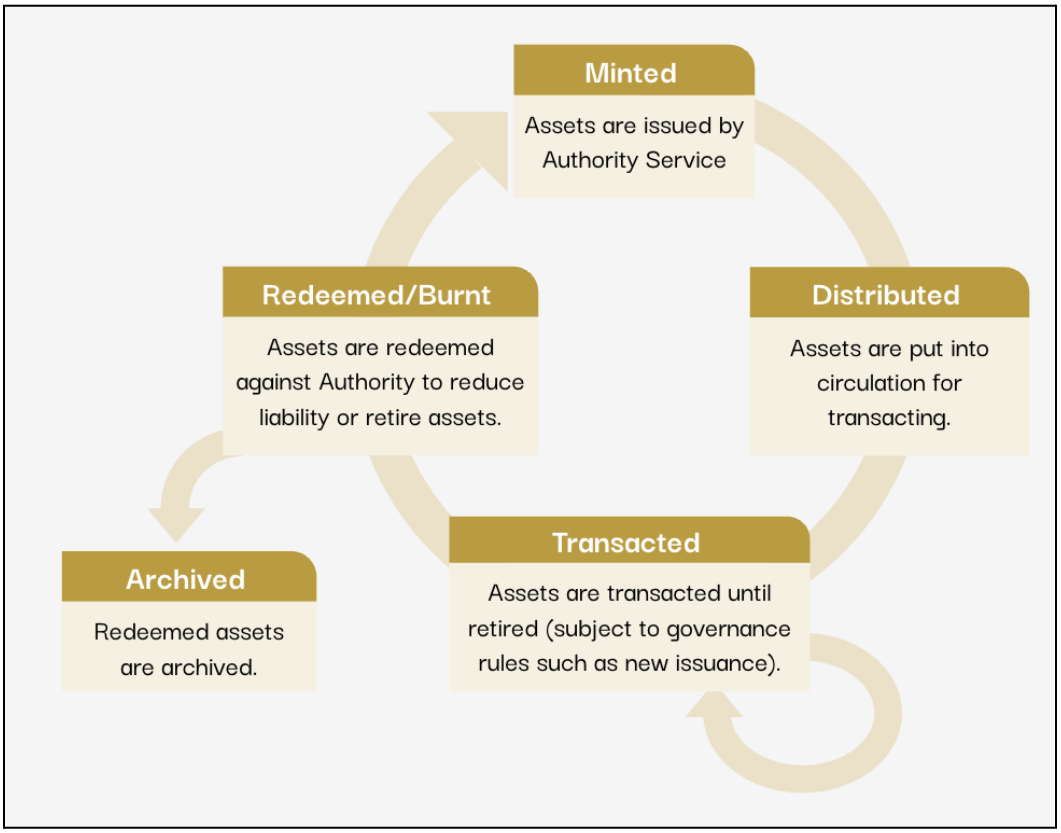
Diagram of File-Based Digital Asset (FBDA) "Digital Twinning" $5.00 USD

File-Based Digital Assets are designed to be flexible for different assets.

- The **Asset ID** serves as a method of uniquely identifying the FBDA in the system.
- The **Signature System** field is for identifying the cryptographic signature system in use.
- **Asset ID**, **Amount**, and **Decimals** are for specifying the value and type of asset being twinned (e.g., $100 USD),
- The Created Timestamp is to signify when the FBDA was first created.

For ownership, the **Owner Key** field and the **Authority Key** fields are used to determine the current holder and the original issuer of the asset, respectively. In summary, FBDAs provide Knox with a lingua franca for interacting with different assets on the platform.

FBDA Lifecycle



Sample FBDA Lifecycle

FBDAs are first allowed to be minted via limits set by the Authority Service, which sets governance rules for all assets it manages. Following this, assets are distributed via interacting with the Authority Service, which can then be used to transact different assets.

After a specified number of transactions, FBDAs can be redeemed against the Authority, resetting the value against the specified minting limits. Retired FBDAs can now optionally be Archived and moved into long-term storage.

Transaction Processing with UTXO

FBDAs are given a fixed value at the time of issuance (say $5.00 USD) but may be asked to fulfill situations where this is not possible (e.g., trying to pay $4). Knox utilizes a Modified UTXO approach to file denominations, allowing for changing files into different denominations as required.

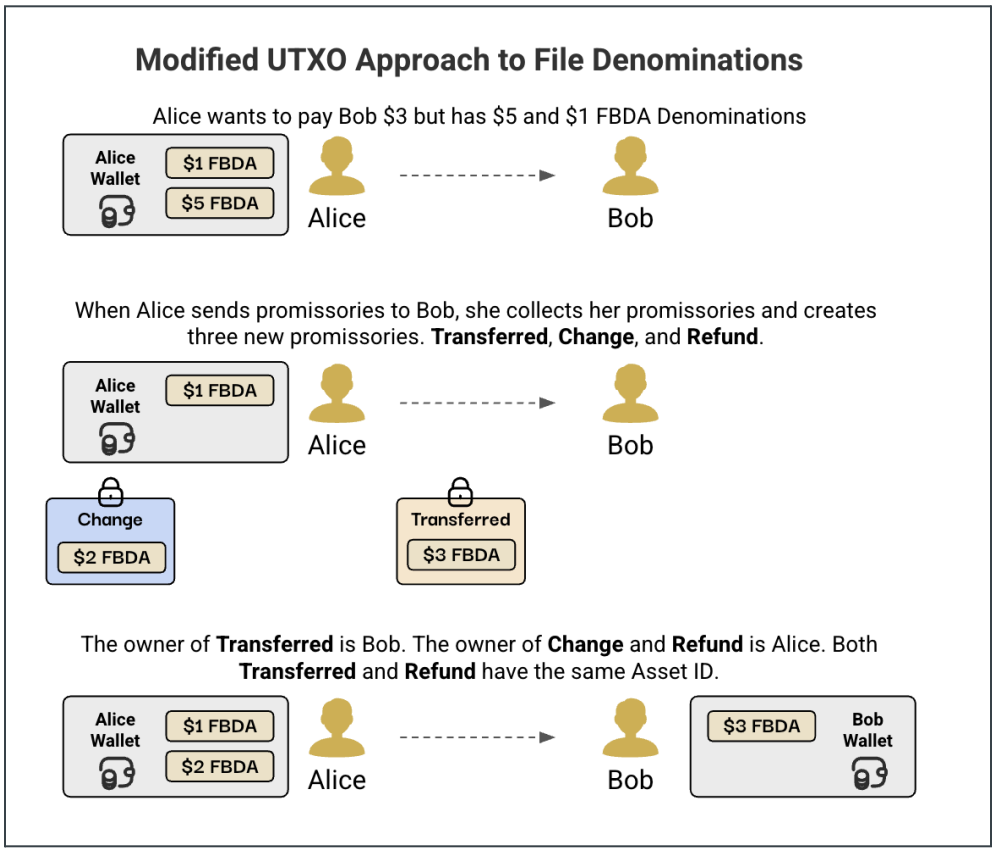
When Alice sends payments to Bob, she collects her FBDAs and creates three new FBDAs: **transferred**, **change**, and **refund**.

- The owner of **transferred** is Bob
- The owner of **change** is Alice
- The owner of **refund** is Alice
- Both **transferred** and **refund** have the same Asset ID. These FBDAs are mutually exclusive - i.e., only one group is created in a given transaction.

When these FBDAs are locked in, the Transaction Validator authorizes the unspent immediately and returns it. This allows Alice to use this in a new transaction while the previous transaction is still in progress.

As for transferred and refund FBDAs, depending on how the logic in the contract plays out, the Transaction Validator will authorize either "**transferred**" or "**refund**" FBDAs, but will not do both. The Transaction Validator signs and verifies FBDAs during a transaction to confirm this.

A sample UTXO transaction is demonstrated below:



Sample UTXO Transaction

Knox's Modified UTXO solution allows for independent transaction processing, leading to horizontal scalability. For more information on this, refer to **Scalability**.

This discussion focuses on signing and transferring FBDAs directly on the Knox system, but FBDAs can be transferred under various schemas. Relevant messaging standards (e.g., ISO 20022) can incorporate FBDA information directly as part of a message payload, for example.

Privacy and Security with FBDAs

FBDAs are pseudonymous, leveraging private/public key cryptography (e.g., FIPS 186-5 compliant Ed25519 by default for high performance, security, and efficiency but extensible to other cryptographic systems such as Secp256k1 or quantum-resistant algorithms such as Dilithium, Isogeny-based, etc.). This cryptographic scheme creates an immutable chain for each FBDA, which, when coupled with the two-phase signature process for a transfer of FBDAs, makes attempts at double-spending untenable. Sensitive data and keys can be stored in vaults/hardware security modules (HSMs), and only the minimal amount of data required to meet financial regulations will be granted by retail users as required.

The pseudonymity of a file holder's personal data leads to preserving privacy rights, yet financial institutions can access information needed for their compliance programs. The FBDA contains its own proof of ownership and authorized transfer and does not disclose any more of its provenance to transacting parties other than the transfer itself. It does not need to be published to any external chain (or public ledger) where non-transacting parties may view it. This makes data in the FBDA system auditable and transparent for Authorized Intermediaries but not publicly viewable.

Rust, a highly performant programming language with memory safety, is used throughout the Knox system for security. Rust can communicate over gRPC/HTTP2 for binary transport and multiplexing to enable high throughput and low latency.

Multi-Asset Transaction Ledger

The core of Knox's system is the Multi-Asset Transaction Ledger. The Multi-Asset Transaction Ledger serves as the backbone of the system, and coordinates with the components and services of the system.

- **File-Based Digital Assets** exist as building blocks in the system, each representing "digital twin" assets in a common format for processing
- **Wallets** exist to store these assets, as well as Identity Bridge credentials, and to implement local programmability
- **Contract-Based Transactions** serve as the logic operators of the system, handling programmability and transactions for the FBDAs stored in wallets.
- **Interoperability Connectors** help to connect the ledger to external systems, including both DLT and legacy systems.

System Architecture

Knox's system architecture was designed to be both powerful and robust to support a variety of different use cases. Written in a microservice architecture to allow for flexible deployment in Kubernetes and accommodate horizontal auto-scaling.

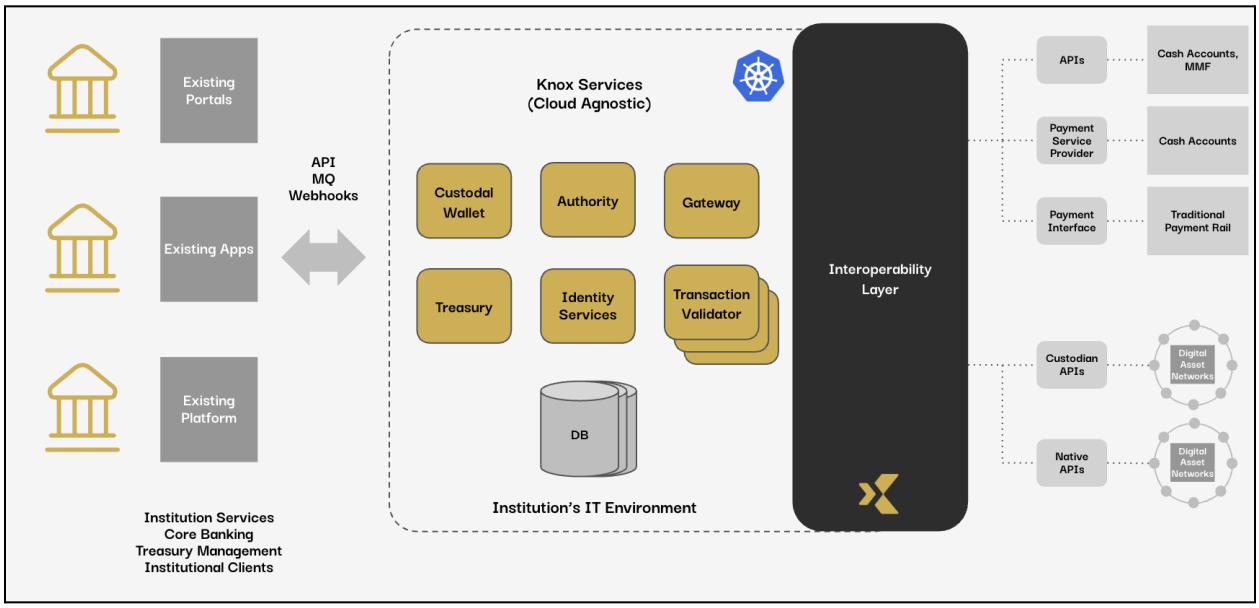
Services

Services in the Knox system include:

Term	Definition
Authority Service	Issues newly minted FBDAs into circulation and provides the initial Authorization Signature on FBDAs.
Custodial Wallet Service	Transacts and holds FBDAs and owner information. Each wallet can hold a variety of asset types.
Gateway Service	Provides bi-directional, end-to-end streaming connectivity; manages the rate-limiting and denial of service (DoS) preventions; and provides packet routing through networking network activity monitoring.
Identity Bridge - Credential Adapter Service	Transforms existing KYC/KYB information into VCs issued to the DID of a wallet that cryptographically attests to having a required credential (e.g., having an Account with the institution, being an accredited investor, etc.). The service integrates with the institution's existing KYC/KYB system using a standardized webhook interface but is designed to plug in custom integrations as required.
Identity Bridge - User Management Service	Enables frictionless integration of end-user wallets with financial institutions' existing identity systems using SAML/OIDC. Provides APIs for user discovery using aliases, e.g., Phone number to Wallet Address lookup.
Identity Bridge - Registry Management	This service is a W3C-defined Verifiable Data Registry, which manages W3C DIDs and DID Documents associated with each wallet, as well as a revocation list of VCs. Attributes of the financial institutions' DIDs themselves can be searched to identify further

	discovery services within financial institutions as well as trusted issuers of credentials.
Supplementary Services	Services that are not core to the Knox base technology but can be added on top of the system. Examples include: **Analytics Service** for gaining insights from transactions; or **Reporting Service** for improving internal reporting processes; or **Exchange Service** for interacting with digital asset exchanges; or **Sanctions Service** for plugging in with sanctions/KYC service.
Transaction Validator Service	The Transaction Validator Service processes transactions via (1) reasoning about the status of the transaction and (2) carrying out the transfer and signing of FBDAs.
Treasury Service	Remits FBDAs denominated in domestic and foreign currencies and holds FBDAs denominated in various currencies for institutions.

Below is a sample architecture that accommodates Knox services within an institution:



Sample Architecture In an Institution's IT Environment

For more detail, check out [Knox's Developer Portal](#).

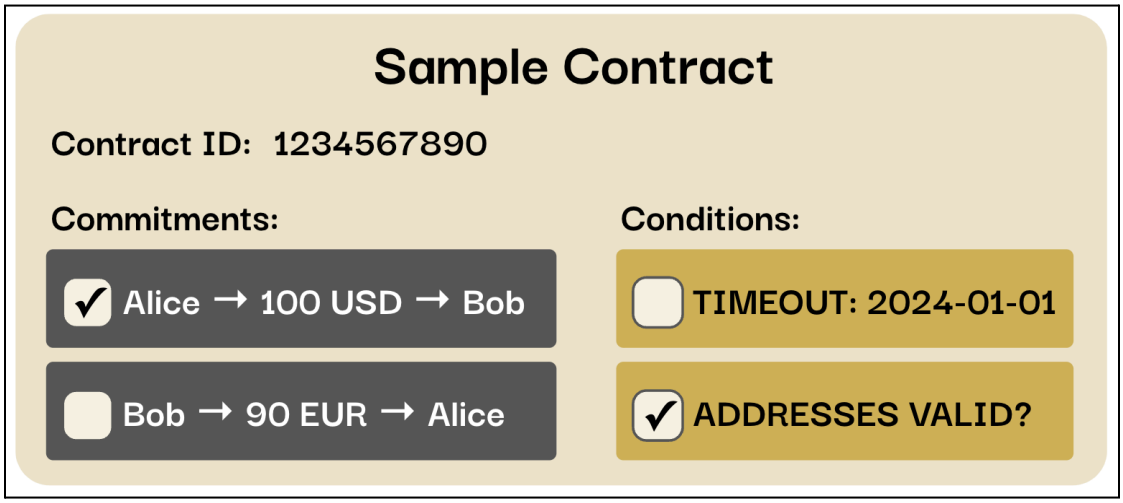
Programmability with Contract-Based Transactions

Knox Networks has implemented a system that separates the *programmability layer* (Contract negotiation) from the *asset transfer layer* (Contract fulfillment). A **Contract-Based Transaction** fulfills a transfer of assets stipulated in a successfully negotiated **Contract**.

Contracts help to create modular transactions that cover a wide range of use cases, including:

- Atomic multi-party and multi-asset settlements (such as PvP, DvP)
- Cross-border payments
- Escrow
- Exchange trades
- Netted settlements
- Treasury management and wallet rebalancing

Contract-Based Transactions reduce costly errors, improve revenue opportunities, limit exposure to counterparty failures, and enforce compliance by allowing institutions to stipulate regulatory requirements before any transfer of assets takes place. All assets are transferred atomically: if any participant fails to deliver on any of their commitments, then all assets will be retained by their original owner. **FIGURE E** shows a simplified view of a sample contract between two parties, Alice and Bob, in an FX transaction.



Simplified View of a Sample Two-Party Foreign Exchange (FX) Contract

Contract Structure

Knox **Contracts** stipulate a series of **Commitments** and **Conditions** to be fulfilled by **Participants**. Here is a sample **Contract** flow:

1. A Contract **Originator** proposes a **Contract** to all other **Participants.** Any participant can decide to accept or reject a proposed **Contract** based upon their own criteria.
    a. If a **Contract** is rejected, a newly proposed Contract can be created by any party.
2. All **Participants** sign the **Contract** as proof of agreement and acceptance.
3. Once a **Contract** is in place, each **Participant** submits the required assets corresponding to their **Commitments,** which are then locked (so the assets cannot be double spent).

4. When all **Commitments** are in place (committing the respective assets to the new owner) and all **Conditions** are met, the **Transaction Manager** atomically completes the transfer of all assets. If **Participants** do not submit their assets by the timeout **Condition** specified in the contract, the system atomically reverts ownership of previously locked assets to the original owners.
    a. Examples of other **Conditions** besides timeouts include AML/CFT/Sanctions checks, valid address checks, etc.

The above figure showcases a simplified Contract-Based Transaction execution for a simple atomic swap between multiple parties.

Sample Contract-Based Transaction Execution Flow

Sample Contract Template

The template itself is in RDF format, a W3C machine-readable standard schema designed to describe various parties, their relationships, and transaction parameters. This structure allows us to configure an unlimited number of participants, define the asset types they are transacting, and set specific conditions governing these transactions. Because of this flexibility, the Knox system enables highly customizable transactions by simply calling an API with these configurable templates; users can seamlessly send and receive funds, withdraw assets, execute

trades, settle payments, place limit orders, and perform a wide range of other financial operations. This dynamic approach ensures adaptability to different use cases, making transactions more efficient and tailored to specific needs.

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/> a
<https://knoxnetworks.io/contract/commitment/group>;
  <https://knoxnetworks.io/contract/commitment/group/expiration> "2024-10-10T20:14:27.249Z".

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/A1> a <https://knoxnetworks.io/contract/commitment>;
  <https://knoxnetworks.io/contract/commitment/amount> "100.00-KRW";
  <https://knoxnetworks.io/contract/commitment/recipient>
<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#respondent>;
  <https://knoxnetworks.io/contract/commitment/sender>
<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#originator>.

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/A2> a <https://knoxnetworks.io/contract/commitment>;
  <https://knoxnetworks.io/contract/commitment/amount> "100.00-CAD";
  <https://knoxnetworks.io/contract/commitment/recipient>
<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#originator>;
  <https://knoxnetworks.io/contract/commitment/sender>
<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#respondent>.

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#contract> a <https://knoxnetworks.io/contract>;
  <https://knoxnetworks.io/contract/memo> "";
  <https://knoxnetworks.io/contract/start> "2024-10-10T19:44:27.249Z";
  <https://knoxnetworks.io/contract/uetr> <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326>.

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#finalizer> a
<https://knoxnetworks.io/contract/finalizer>.

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#metadata> a <https://knoxnetworks.io/contract/metadata>.

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#originator> a
<https://knoxnetworks.io/contract/participant>;
  <https://knoxnetworks.io/contract/participant/publicKey>
"z6MksRdKE49ipfc9EduuDhm44njBJjKn3cYMHzqcso62HJMn".

<urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#respondent> a
<https://knoxnetworks.io/contract/participant>;
  <https://knoxnetworks.io/contract/participant/publicKey>
"z6Mkn4gsQ1K4gGs7KUb3NmwNwBS43FqYp2Fw6EYSGfF5sdjw".

GRAPH <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#finalizer> {
  []
    rdf:first true;
    rdf:rest (
        true
      );
    <https://knoxnetworks.io/action/finalize> <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/A1>,
      <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/A2>.

  [] a <https://knoxnetworks.io/expression/match/value>;
    rdf:first <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/A1>;
    rdf:rest (
        <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#G1/A2>
      ).
}

GRAPH <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#metadata> {
  <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#originator>
    <https://knoxnetworks.io/contract/participant/signature>
<signature:base64:/U7NIdeO6aFyn/BCKz7tBn7GMnoO+rCglozCx2PV574Q8rydYiGoPa1XfqBLCoTZsq1IX4AqpZSiQWyhnnkhD
w==>.

  <urn:uuid:0088b7ba-8172-4638-bb5e-9dd39775e326#respondent>
    <https://knoxnetworks.io/contract/participant/signature>
<signature:base64:QRWhBN0zrgCeXQ1GWMqxm8ntTHZ9MXbLzDatDsQQZqVQGS+wzRpeaATsbyb8FaAPt13vKZDrUFS1QaBLOdoWB
w==>.
}
```

Sample RDF Contract Format

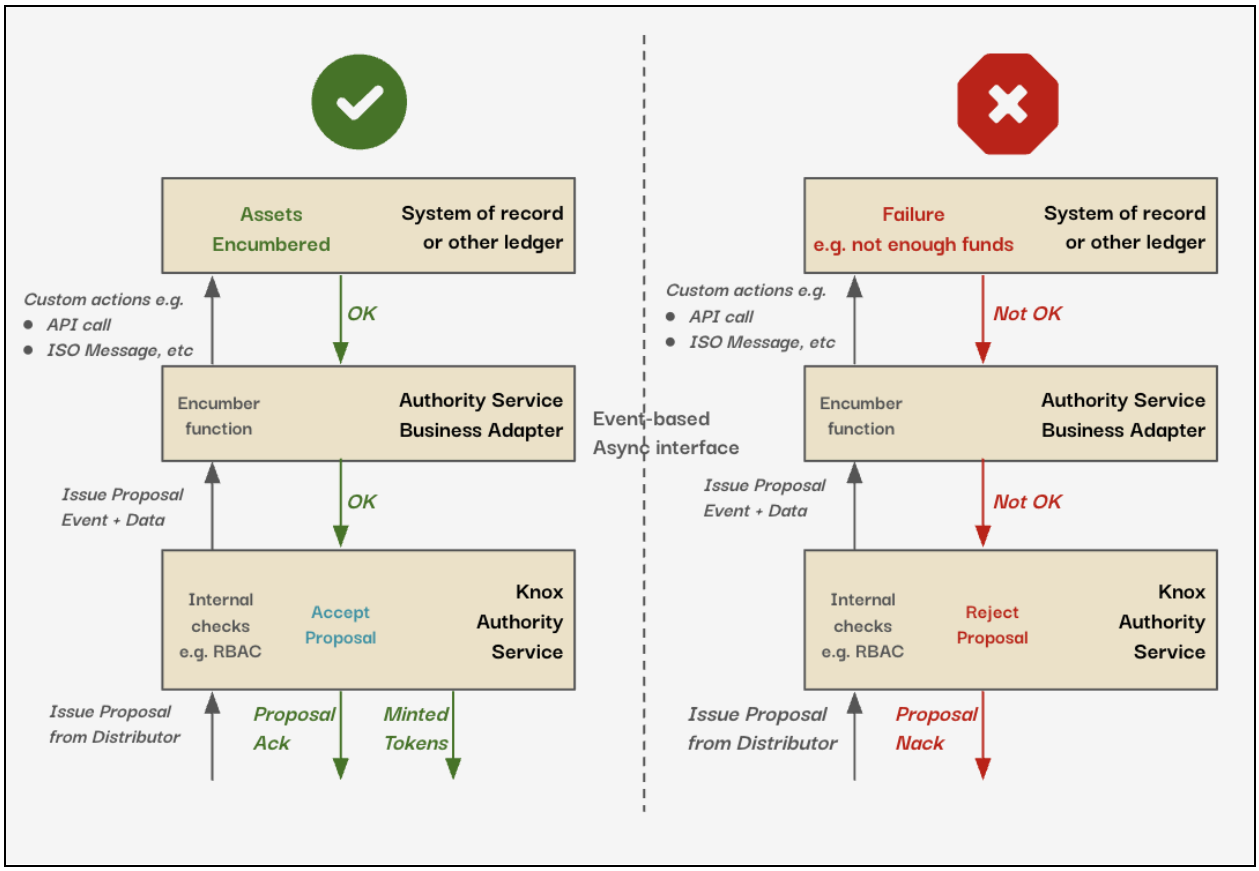
Contract-Based Transactions can also carry messages in any format (e.g., ISO 20022, NACHA) in line with the overall transaction. Knox eliminates the traditional separation between messaging and asset transfers, and messaging is available in line with the transaction.

Participants in the Knox system utilize Contract-Based Transactions via APIs to accomplish secure and complex transactions between multiple parties. Contract-Based Transactions are based on an event-driven architecture, and at every stage in the transaction lifecycle, various events are generated with their respective details. In addition to integrating DLTs over techniques such as HTLC mentioned above, this also allows easy integration with any traditional messaging interfaces and various systems expected in a modern institutional environment, using popular techniques such as MQ or Webhooks. Based on the events, flexible business, and regulatory logic can be inserted into the Contract to allow for complex and conditional execution of transactions. Knox Contract-Based Transactions are executed by state machines (rather than EVMs or equivalent smart contracting evaluators). There is no need to "encode" conditional statements or loops. Failure of transactions does not require complex steps to retrieve assets committed to the failed transaction. These are automatically reinstated to the last owner.

Knox Network's Contract-Based Transactions allow for institution-specific adapters to be easily plugged in (e.g., an adapter that maps fields from Knox transactions to fields in an ISO 20022, MT, or a FIX message for on-ramps/offramps to other systems). This maximizes the potential for programmability because any ecosystems that arise, whether DLT or traditional, can easily plug into using Knox Network's FBDAs as a method of payment.

Asset Encumbrance with Contract-Based Transactions

A critical challenge in asset tokenization is ensuring that the tokenized representation of an asset cannot be simultaneously spent or utilized through its original, non-tokenized form. This lack of assurance creates risks related to double spending and financial integrity. Additionally, ambiguity surrounding asset ownership, transfer rights, and associated limitations further complicates regulatory compliance and operational transparency. Without a clear mechanism to enforce asset constraints across systems, organizations face inefficiencies and potential legal and financial exposure.



Sample Asset Encumbrance

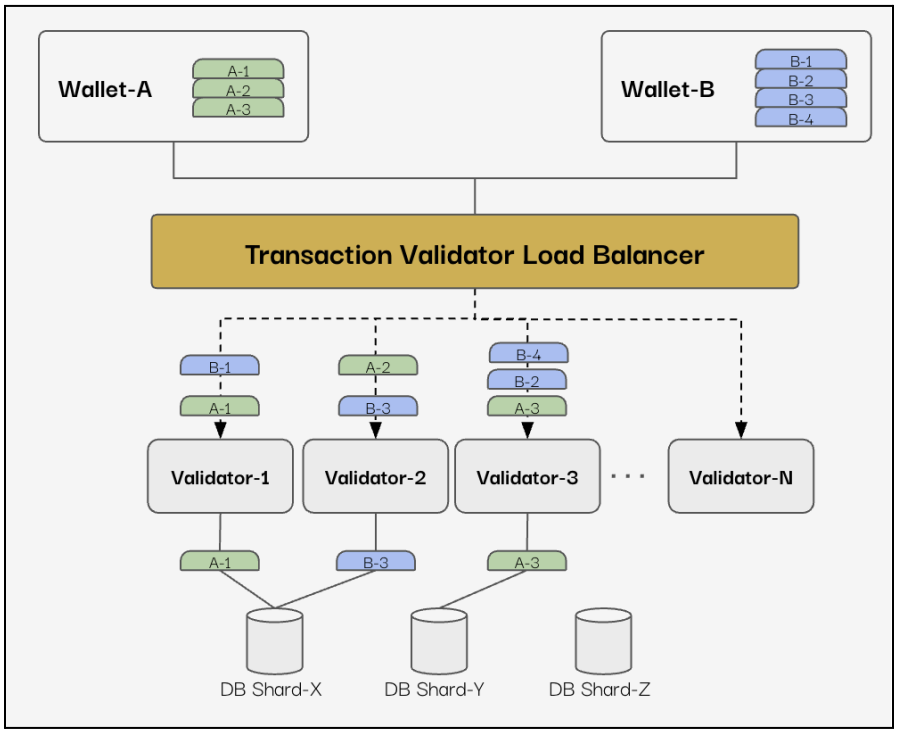
To address these issues, **Contract-Based Transactions** atomically encumber assets upon issuance and release them upon redemption. This flexible, event-driven design enables seamless interoperability with any backend system at any stage of the transaction, ensuring that assets are properly locked, unlocked, and managed across both traditional systems and distributed ledger technologies (DLTs). The framework accommodates complex asset interactions, such as minting or burning triggered by actions on other asset types, while streamlining workflows for issuance and redemption. Additionally, it supports customizable backend actions, including automated asset movements between accounts and real-time API interactions with external financial systems such as Real-Time Gross Settlement (RTGS) networks, custody services, omnibus FBO accounts, etc.

Scalability

Scalability has proven to be an issue for several payment and asset systems that have tried to revamp aspects of the financial system. This ultimately stems from the need to pass every

transaction through a singular point of entry, which creates a bottleneck in the system that prevents the system from scaling efficiently as the number of transactions grows. Due to fragmented back-office functions, intermediaries, and settlement times, traditional systems are not as scalable, especially at the retail level.

Knox Networks designed a non-account-based system that could scale to fit within an institution's regulatory and financial requirements. Knox Networks understands that large financial institutions could be processing hundreds of thousands of transactions per second (TPS) for millions of customers worldwide and thus designed a system that could meet those requirements via high reliability, high throughput, and low latency.



Transaction Validators Performing Load Balancing for Horizontal Scaling

Transaction validation is distributed across horizontally scaled Transaction Validators, ensuring high concurrency and efficiency. The sequencing of FBDAs is not important, allowing for greater flexibility in processing. The transaction validators are specifically designed for high concurrency, with non-blocking database calls that enhance performance. When validating a file, only the corresponding row is locked, preventing contention between files and enabling seamless parallel processing. Additionally, the use of a sharded database architecture allows for horizontal scalability, further distributing the write load across multiple shards to enhance overall system throughput and reliability.

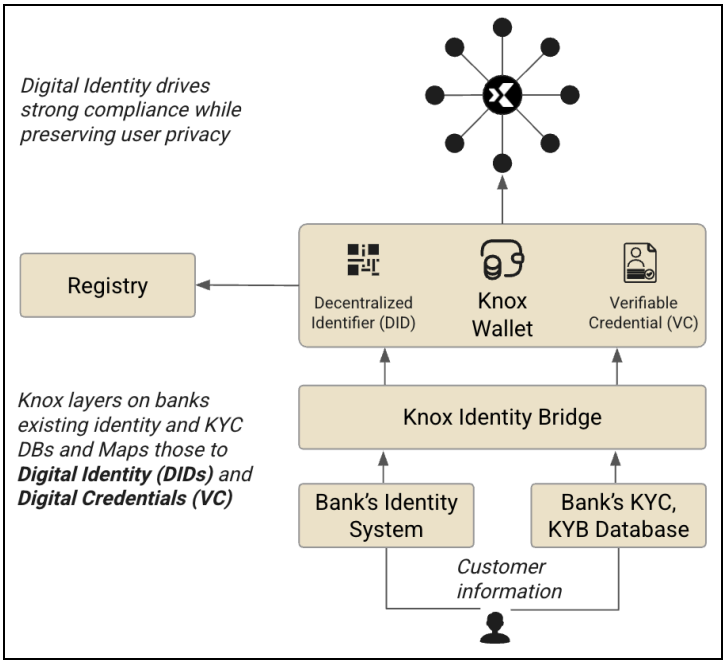
Understanding the bottlenecks in developing many centralized digital asset systems, Knox Network's FBDA solution was designed to scale horizontally. This horizontal scaling is possible because each FBDA, and thus each transaction, can be processed independently. This allows FBDAs to be cryptographically signed and verified concurrently, removing the need for batching and an expensive consensus algorithm. Increasing the throughput in the system can be achieved by increasing the number of transaction authorizers in the network as needed.

In addition, each FBDA is both a fixed value and is non-expiry, meaning that FBDAs can be held indefinitely, removing the risk of lost "expired" transactions when network connectivity goes down. At the same time, Knox Network's design allows for FBDAs to be archived and/or taken out of circulation and re-distributed as required to reflect updated schema formats.

Identity Bridge

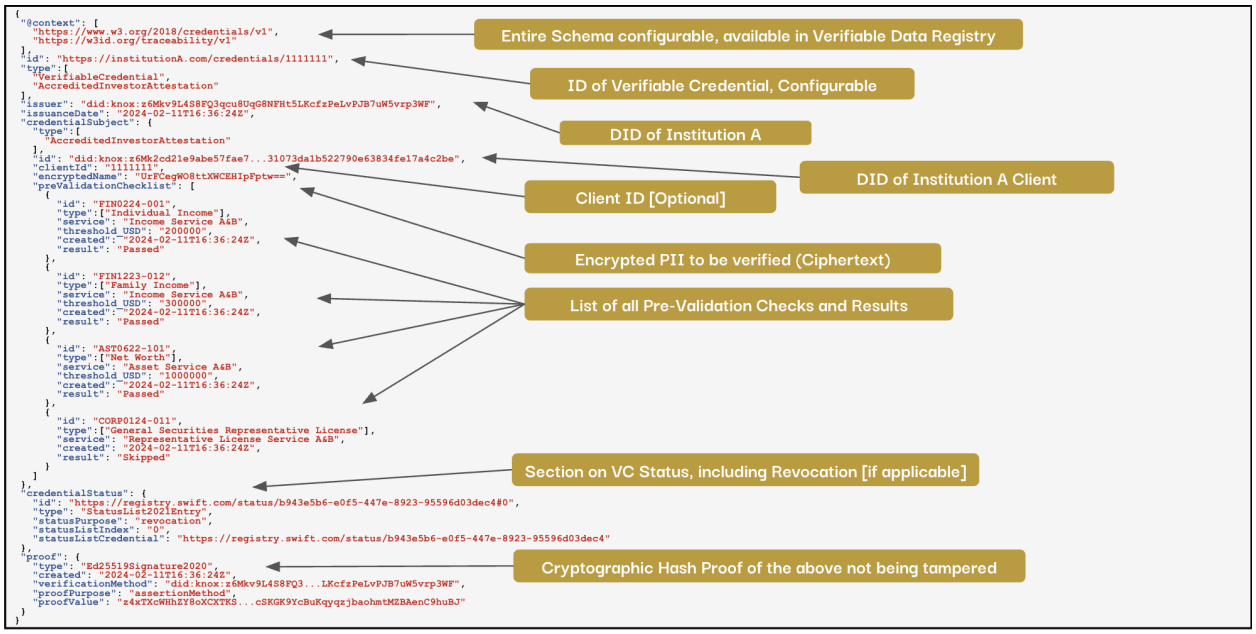
Identity is often proven today via either physical ownership of credentials (e.g., a driver's license or passport) or online via a list of usernames and passwords on centralized services over the internet. These solutions lack privacy, with both methods exposing more data than is necessary to parties in a transaction. For example, age verification might require the showing of a driver's license, which includes additional personal information like date of birth, address, and name. In reality, the only thing that must be proven is a verifiable way of knowing the answer to the binary question, "Is this user over 21?" While showing whole credentials may be acceptable to a person who may not remember, this exposure is not a best practice over the internet. With traditional identity systems, users store usernames and passwords on external centralized servers that are easy to forget and get reused in dozens of systems such that a single security breach exposes access to the rest of the victim's associated systems.

Knox Networks provides a secure white-labeled identity solution that integrates with financial and government institutions' existing identity solutions to work with FBDAs. The pseudonymity of this system preserves privacy of the users, while still making sender and recipient information available when required for financial regulatory compliance.



Digital Identity via Knox Using Verifiable Credentials and Decentralized Identifiers

The Identity Bridge ensures sensitive data stays in the user's secure storage, authenticating and interacting with cryptographic proofs of identity data instead of usernames and passwords via a system called **Verifiable Credentials (VCs)**. **Decentralized Identifiers (DIDs)** work with VCs to help ensure that cryptographic operations can occur without exposing sensitive user data.



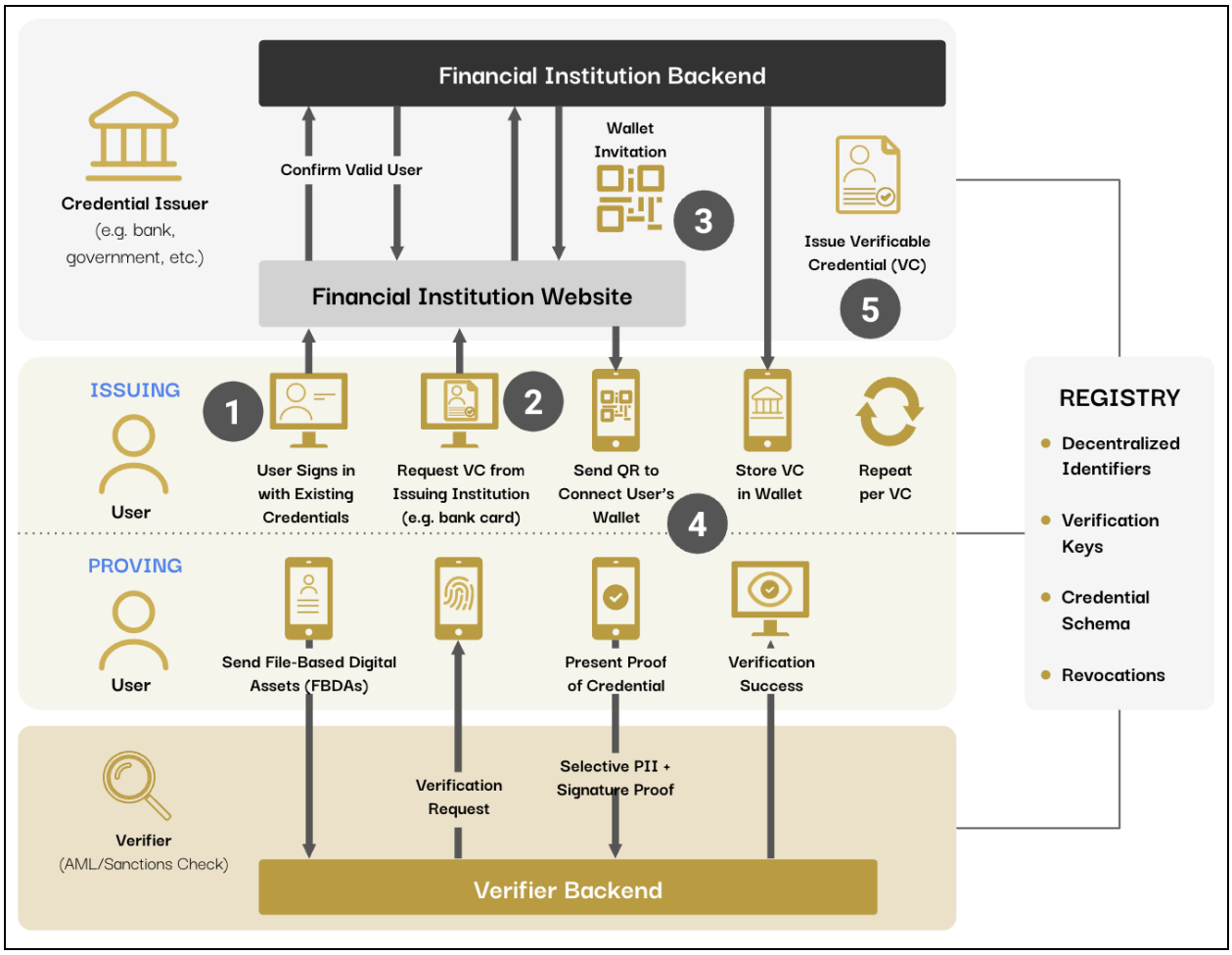
Sample Verifiable Credential for an Accredited Investor Check

The Identity Bridge integrates into existing identity systems, providing SDKs and modules for backend services, websites, and mobile apps in various programming languages.

As financial and government institutions already provide identity services for their customers, the Identity Bridge can easily integrate into the existing identity systems over standards such as OpenID Connect (OIDC)/Security Assertion Markup Language (SAML), or any other integration methods in order to set up the customers' wallets. After this one-time setup process, users can transact FBDAs via VCs while still leveraging the financial institution or government institution's existing KYC process for AML/Sanctions checks against financial regulations. VCs can also be used to simplify the process of initially onboarding users in a cryptographically secure manner.

For example, the wallet can be a part of the financial institution's mobile app, leveraging the SDKs and an example app provided by Knox Networks. With the mobile wallet, users can simply authenticate to the phone app locally through biometrics or password (data does not leave the device) and then simply scan QR codes to process the verification, authorization, storage, and transaction of the FBDAs in the system. Additionally, Knox Networks provides the server-side Custodial Wallet Service to be hosted by the financial institution on behalf of the customer. Access can remain the same with the financial institution username and password login and financial institutions can simply use their existing websites and integrate with Knox Networks wallet services over backend SDKs and APIs.

As shown in the figure below, the Identity Bridge creates a powerful yet empowering solution to the ever-present problem of identity management within the financial and digital asset ecosystem.



Sample Identity Bridge Interaction Between Users and Financial Institutions

1. User is a customer of Financial Institution A and logs in through the Identity Bridge using existing institutional login credentials.
2. User is instructed by Financial Institution A to register their wallet and requests a Verifiable Credential (VC) from the financial institutional to capture the user's institutional account details.
3. Financial Institution A verifies the request and prepares an invitation for the user to register the wallet and download the VC.
4. The invitation is shared with the user, who scans the QR code via the mobile wallet app. The identifier from the wallet is cryptographically verified, and the VC is specifically issued to the user as the subject and the institutional identifier as the credential issuer.
   NOTE: An institutionally-hosted Custodial Wallet Service can also be used here.
5. The user now has this institutionally-issued VC held in the wallet. This data remains in the wallet and can be requested as needed for financial regulation.

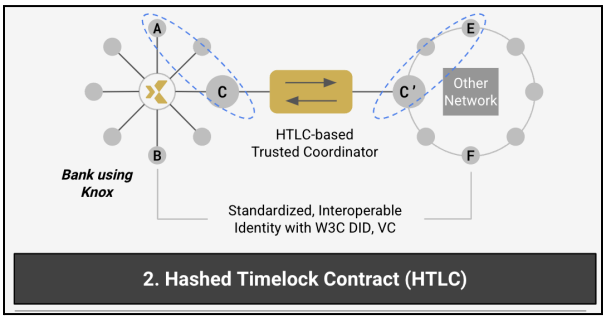
Interoperability

The financial services ecosystem consists of a variety of established and competing technological standards, which challenges the possibility of “one-size-fits-all” solutions for legacy and digital assets. Data formatting and standards can vary greatly across different networks and ledgers, which makes reconciliation of complex multi-party, multi-asset transactions across systems difficult.

In response, Knox Networks designed a flexible and future-proofed system that could interoperate with versatile programmable ecosystems in the digital assets space and traditional legacy systems. Knox has developed interoperability methods for interacting with tokenization platforms, blockchains, DLTs, and traditional payment rails.

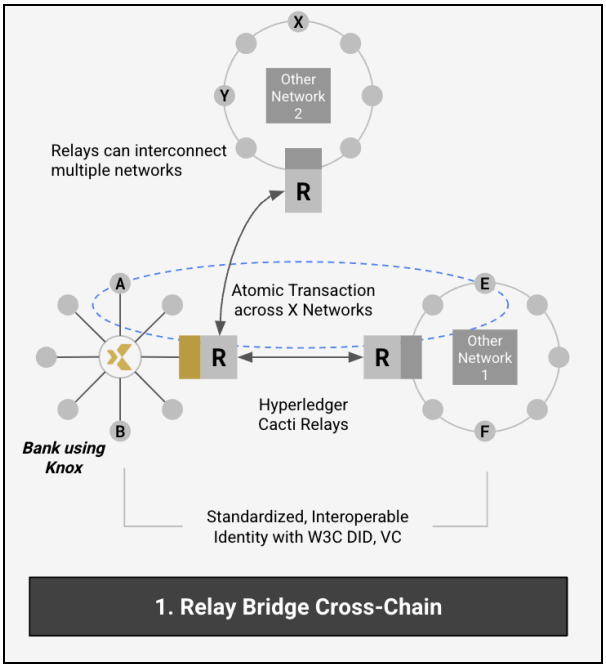
#1, #2 - Interoperability with Blockchains and Tokenization Platforms

Both the below techniques enable coordinated asset transfers and exchanges across Knox and the other ledger.



Interoperability using HTLCs for Cross-Chain Communications

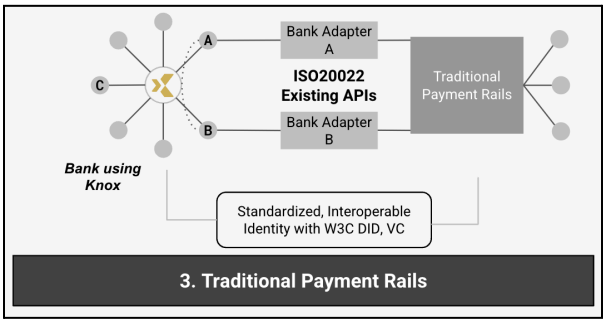
#1 Hashed Timelock Contracts - Knox supports protocols such as HTLC to bridge transactions with other ledger technologies that support HTLC, e.g., any EVM Chain, Hyperledger Fabric, Firefly, R3 Corda, DAML, as well as interaction with the ERC-20 token standard (among other standards).



Interoperability using Relay Bridge for Cross-Chain Communications

#2 Relay Bridges Cross-Chain - Knox supports relay bridges based on open-source standards such as Hyperledger Cacti, which enables interoperability with other ledgers that support the same relay mechanism.

#3 - Interoperability with Traditional Payment Systems



Rest APIs for Traditional Payment Rails

#3 Traditional APIs - Knox also supports Rest APIs for interacting with traditional systems.

Knox allows the transporting of messaging information in any standard alongside a Knox transaction. For example, ISO 20022 or SWIFT MT equivalents can be carried along with the Knox transaction.

Knox's event-driven architecture supports writing adapters that can translate back and forth from standards such as ISO 20022, SWIFT MT, FIX, and can integrate with any messaging standards. All fields from the Knox transaction are available for mapping to fields within these

standards. Internally, Knox uses standards such as UETRs (UUIDV4), ISO Dates, and ISO currency standards for ease of mapping to the same fields in ISO 20022 and MT messages.

These adapters can form on-ramps/off-ramps with existing messaging interface products in use at financial institutions over protocols such as MQ, file-based adapters, or REST APIs.

The file-based ownership structure of the system means that FBDAs can be embedded across other payment networks (e.g., traditional bank account systems or DLT-based platforms like Ethereum), including stakeholders that are not using Knox Networks and stakeholders that are required to use various financial standards (e.g., ISO 20022, SWIFT). FBDAs allow interoperability across virtually all major ecosystems because it just requires the system to have the ability to transfer small packages of data. For example, FBDAs could be embedded within an ISO 20022 message to transfer to another party. This means the Knox Networks software platform can support multiple regulatory and currency regime requirements.

What Knox Enables

The Unified Ledger

Businesses have to deal with multiple asset classes across many systems, making it difficult to get a harmonized view of the big picture. As a result, operational complexity increases, and costs and settlement efficiency are all negatively impacted.

Knox's Unified Ledger is a product that helps multi-asset businesses to transact and interoperate with any external accounts or their own operating entities (traditional cash and custodial accounts, FBO/omnibus accounts, digital asset+stablecoin wallets) and provides a real-time, unified ledger to manage all forms of cash and assets via a single source of truth. This B2B software is API/SDK based and gives clients the ability to plug into any new asset ecosystem easily while managing it alongside their existing business.

Businesses holding diverse assets spread across several custody accounts on behalf of their customers and/or their own operating entities. Traditionally ,these are then managed by separate siloed systems (spreadsheets, data stores, and workflows spanning discrete systems), leading to problems and sub-optimal operations.

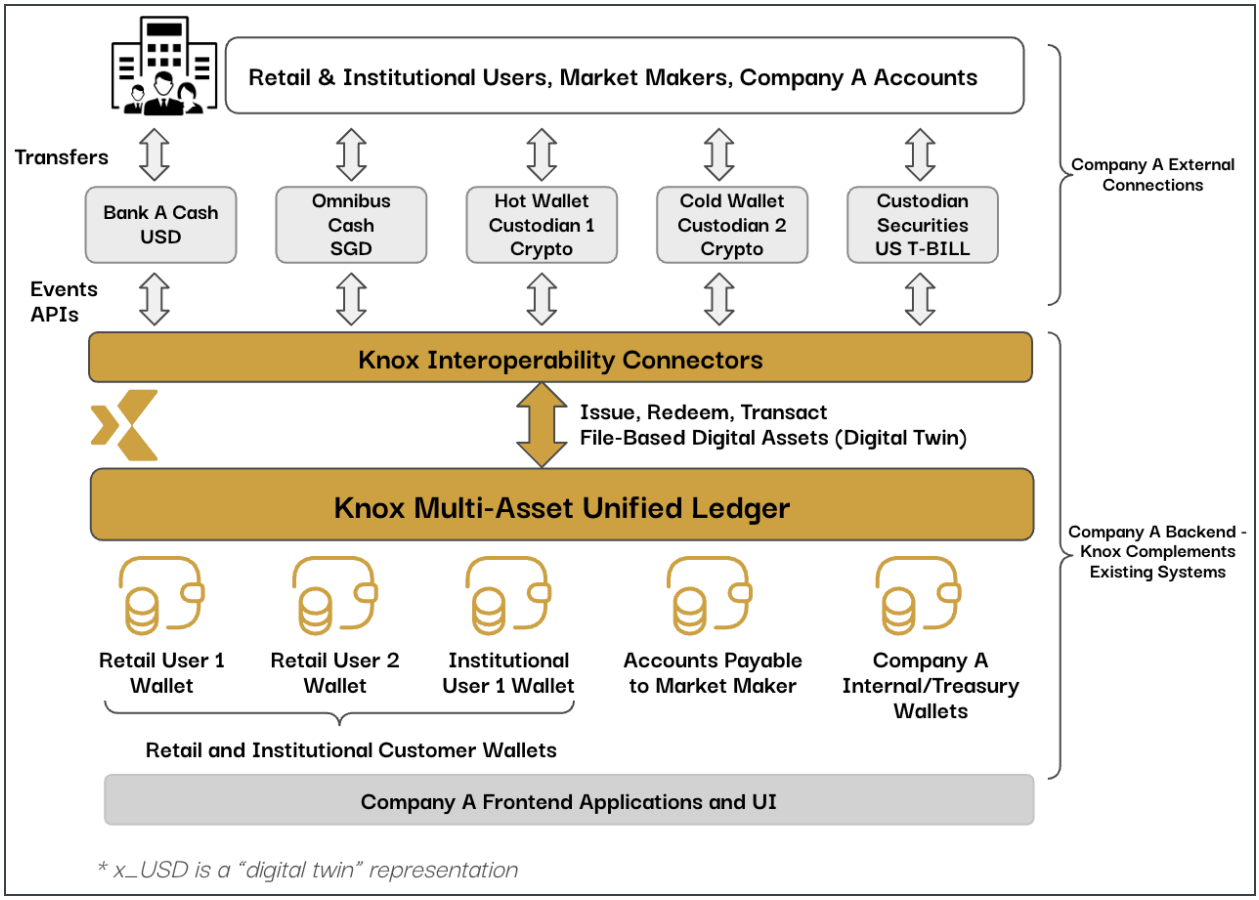
As firms invest in digital assets and stablecoins, these problems only get worse since on-chain assets and their interfaces have their own complex flows, and businesses have to manage a diversity of networks, wallet providers, on-chain fees, on/off-ramp flows, etc.

The unified ledger is built to complement existing back-end systems, without requiring a rip and replace of current systems.

- **Integration**: Connect seamlessly with traditional and digital asset custody accounts.
- **Digital Twin**: Create a real-time digital twin of assets held in custody accounts via the Knox multi-asset shared ledger, synchronized with the underlying accounts.
- **Transaction Management**: Initiate transactions through the Knox ledger, acting as a proxy for underlying accounts, and configure efficient settlement processes.
- **Scalability**: The ledger is highly scalable, supporting multi-party, multi-asset transactions.
- **Interoperability**: Connectors simplify edge integrations without impacting the core system.

Knox's Unified Ledger targets problems with scaling transactions, settlement efficiency, lack of interoperability, and real-time monitoring between backend systems. The Unified Ledger provides continuous verification of assets and liabilities, allowing for tangible outcomes:

- **Unified Asset View**: Gain a real-time, harmonized view of all assets and currencies, ensuring a single source of truth for accounts.
- **Streamlined Management**: Manage assets and money through one ledger, scaling asset types without core system changes.
- **System Interoperability**: Integrate seamlessly with both traditional finance and digital asset systems, simplifying interactions with various custody accounts and networks.
- **Programmable Actions**: Execute all transaction types, including multi-party and multi-asset, using APIs and event-driven architecture.
- **Efficient Settlements**: Achieve cost savings through internal netting, batched withdrawals, reconciliation, wallet rebalancing, sweeping, and automation.
- **Fee Tracking**: Monitor transaction fees and accruals directly on the Knox ledger.



Sample Unified Ledger

The Unified Ledger enables real-time transparency across all assets and owners, facilitating seamless bridging and transactions between off-chain and on-chain assets. It enhances the efficient use of cash and assets by streamlining transactions within a single, integrated system.

Tokenized Assets for Multi-Institutional Use

The financial industry faces fragmentation across multiple payment rails and different classes. Legacy systems struggle with inefficiencies, high costs, and slow settlement times for multi-party, multi-asset transactions domestically and cross-border. While individual institutions can tokenize their own assets, a combined tokenized asset platform across multiple institutions creates a revolutionary infrastructure for regulated, real-time settlement networks.

Knox's solution for Multi-Institutional Tokenized Assets addresses inefficiencies in reconciliation, settlement, and regulatory compliance by unifying tokenized assets across institutions into a single network. Features include:

- **Real-time settlements:** Instantaneous finality for inter-institutional transactions, reducing settlement risk.
- **Interoperable infrastructure:** Seamlessly integrate different assets across domestic and international systems.
- **Enhanced liquidity management:** Centralized insights into tokenized and traditional assets to optimize liquidity.
- **Programmable compliance:** Automate regulatory reporting, reserve requirements, and settlement conditions through smart contracts.
- **Cost efficiency:** Streamlined operations reduce reconciliation costs and reliance on intermediary systems.
- **Scalability and future readiness:** Easily adapt to emerging payment systems and regulatory changes.

Read through pages 33-40 from **Knox White Paper - April 2024 for more information**.

Conclusion

Knox is designed to bridge the gap between traditional finance and digital assets for businesses today. Knox's technology suite is designed to bring the best of digital assets to traditional finance, and is supported by a technology suite to simplify the complexities of dealing with modern financial rails.

By applying cutting-edge technology to leading business problems, Knox is able to help financial firms save on costs, automate processes, interoperate with different systems, and unlock new efficiencies with assets.