White Paper

File-Based Digital Assets for Financial Institutions

Knox Networks

April 2024

Executive Summary

Knox Networks is a software infrastructure platform that enables access to the global digital financial system through frictionless payments, auditable-yet-privacy-preserving records, and value-added services for financial institutions. We achieve these outcomes through file-based digital asset technology which improves upon scalability, interoperability, and privacy in payments.

The Knox Networks software platform can be used for authorizing, distributing, verifying, and transacting a variety of File-Based Digital Assets (FBDAs) for central banks, financial intermediaries (such as commercial banks and payment service providers), and retail users. FBDAs can take the form of, but are not limited to, cash and cash analogues (such as tokenized commercial bank deposits or central bank digital currencies), equities, treasuries, and other asset classes. This versatility stems from Knox Network's file-based architecture, allowing for many different asset classes to be digitized efficiently. FBDAs are utilized in a network to leverage cryptography and distributed systems techniques that can be easily deployed to the cloud and to custom environments by banks.

The focus of this white paper is to demonstrate the value of FBDAs when specialized as a digital banknote solution, thereby serving as a cash-like analogue (the example within this white paper will be that of central bank money, but private tokenized deposits are also possible). These digital banknotes serve as a fixed-value denomination (e.g., £1.00), light-weight file that includes a non-malleable cryptographic record of historical ownership. The Knox Networks software platform provides rich features that help drive innovation and improve efficiency while still preserving existing relationships, roles, and regulatory controls within the two-tier banking system.

Knox Networks aims to provide software services to support FBDAs along with identity management service interoperability. This white paper showcases the design goals, architectural design choices, and use cases of Knox Networks's FBDA solution to convey increased efficiency, interoperability, and security across the existing financial system for central banks, commercial banks, and customers.

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.

Table of Contents

Glossary

The Knox Networks solution introduces some specific terminology that is referred to in this white paper.

Term	Definition
Analytics Service	Provides historical time-series and static reporting of FBDAs at varying levels of observability.
Archival Service	Provides long-term storage compression of exhausted FBDAs for required queries.
Authority	Financial institution that runs the Authority Service, thereby authorizing permissions and distribution limits to Authorized Intermediaries within the network. In the case of a CBDC, the Authority would likely be a central bank. In the case of a commercial bank-issued coin or tokenized deposits, the Authority would likely be a division within the commercial bank.
Authority Service	1) Establishes distribution limits for Authorized Intermediaries; and 2) Issues newly minted FBDAs into circulation and provides the initial Authorization Signature on FBDAs.
Authorization Signature	The cryptographic signature from a trusted entity (likely the Authority Service or Transaction Validator Service) on an FBDA, proving the file has not been double spent and providing proof-of-settlement. A fully-settled FBDA must have both an Authorization Signature and a Transfer Signature.
Authorized Intermediary	Financial intermediary given permission within the system by the Authority to run a Distributor Service. Grants permission to distribute FBDAs into user wallets via the Distributor Service. In the case of a CBDC, generally a commercial bank or payment service provider. In the case of a commercial bank-issued coin, generally divisions or departments within the commercial bank.
Contract-Based Transactions	Transactions are built on top of the underlying asset layer via Contracts. Contracts help to create modular 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 FBDA and retail user information. Server side wallet solution in lieu of mobile wallet option hosted by the bank on behalf of the customer who opts in to do so.
Decentralized Identifier (DID)	W3C standard for identifying wallets via Public Key Infrastructure (PKI) in a privacy-preserving manner. No sensitive user data is stored. https://www.w3.org/TR/did-core/
Digital Wallet	Transacts and holds FBDAs and bank customer information, comes either via the Mobile Wallet Service or the server-side Custodial Wallet Service.
Distributor Service	1) Distributes and redeem FBDAs into and out of the system, under limits from the Authority; 2) Handles the distribution process of FBDAs to retail wallets; and 3) Replaces FBDAs in circulation once they reach a configurable size threshold.

Gateway Service	1) Provides bi-directional, end-to-end streaming connectivity; 2) Rate limiting and denial of service (DoS) preventions; and 3) Provides packet routing through networking network activity monitoring.
File-Based Digital Asset (FBDA)	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 a variety of asset classes, including but not limited to digital banknotes, equities, treasuries, and other asset classes.
Hashed Timelock Contract (HTLC)	Transaction methodology that reduces counterparty risk via use of hashlocks and timelocks to force acknowledgement of payment and or forfeit or payment, thereby allowing for atomicity in multi-step transactions/swaps.
Identity Bridge	Integrates with existing bank or government identity systems via OIDC/SAML or other traditional standards to bring into Knox and bridges to W3C standards-based DIDs and VCs for a seamless user experience that protects user privacy and maximizes interoperability.
Mobile Wallet Service	Transacts and holds FBDA and customer account information on customer's device. Built with Knox Networks mobile SDKs and sample apps.
Sanctions Service	1) Parses and indexes sanctions lists (e.g., OFAC or UN); 2) Provides search queries with provided personal identifiable information (PII); and 3) Batch file reports (e.g., suspicious activity reports) with regulatory bodies (e.g. US FinCen).
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)
Transaction Validator Service	The Transaction Validator Service processes transactions via two sub-services which perform complementary but distinct tasks: (1) **the Transaction Manager Sub-Service** reasons about the status of the transaction, and (2) **the Notary Sub-Service** carries out the transfer and signing of FBDAs.
Transfer Signature	The cryptographic signature from the previous owner of the FBDA proving transfer of ownership to the current bearer. This may be the signature of the Distributor Service when the FBDA was first authorized, or the previous owner of the FBDA for any later transaction.
Treasury Service	1) Remits FBDAs denominated in domestic and foreign currencies; 2) Handles residual change distributions; and 3) Holds FBDAs denominated in various currencies.
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

A Future with File-Based Digital Assets

As money becomes increasingly digital, financial institutions are looking for ways to transform their business from the legacy of yesterday's systems and reinvent themselves in the digital world. At the same time, banks are facing ever increasing costs, disintermediation, and revenues at risk. In fact, Accenture estimates that $280bn of commercial bank revenue will be lost to digital payment companies & nonbanks by 2025[1]. Knox Network's vision is to build a software platform that enhances financial institutions' access to the global digital financial system by focusing on improved scalability, interoperability, and privacy in payments.

The platform is built for frictionless payments, auditible-yet-privacy-preserving transactions, and value-added services (e.g. programmability, escrow transactions, cross border payments, identity verification, payment versus payment, and delivery versus payment). Knox Networks is aiming to support this journey to the digitized financial world by providing a robust software infrastructure platform leveraging Knox Network's File-Based Digital Asset (FBDA) technology.

The Knox Networks software platform enables high-speed transactions and settlements between central banks, commercial banks, and consumers through the movement of FBDAs. This system provides rich features that help drive innovation while preserving the existing relationships, roles, and regulatory controls that exist within the banking system.

FBDAs can take the form of, but are not limited to, cash and cash analogues (including tokenized commercial bank deposits and central bank digital currencies), equities, treasuries, and other asset classes. This versatility stems from Knox Network's file-based architecture, allowing for many different asset classes to be digitized efficiently (including securities, treasuries, repurchase agreements, etc). In addition to its flexibility, FBDAs allow for improved security, privacy, scalability, and interoperability with different identity and financial standards, currencies, assets and payment networks.

---

[1] *Source: Accenture: Banks Risk Losing US$280 Billion in Payments Revenue by 2025, According to Accenture Report.* https://newsroom.accenture.com/news/banks-risk-losing-us280-billion-in-payments-revenue-by-2025-according-to-accenture-report.htm

This white paper will focus on one implementation of FBDAs – as a flexible, non-account based, fixed-value "digital banknote" solution under a central bank as the Authority. **This paper will primarily refer to the implementation of a central bank digital currency (CBDC) - but private tokenized deposits run under the Authority of a commercial bank is also possible**. An FBDA is a fixed-value (e.g., ¥100 note) denomination file that includes a non-malleable cryptographic proof of historical ownership. Knox Networks provides software services and applications to authorize, issue, distribute, verify, sanction, transact, and report on FBDAs. FBDAs can be transferred over Knox Networks' Interbank Platform to provide real-time settlement and delivery to wholesale and retail participants, such as central banks, commercial banks or other financial institutions, and consumers.

Knox Networks has built a software platform that scales with both high throughput and low latency, preserves privacy protection via data ownership, and enables existing compliance, sanctions and anti-money laundering programs.

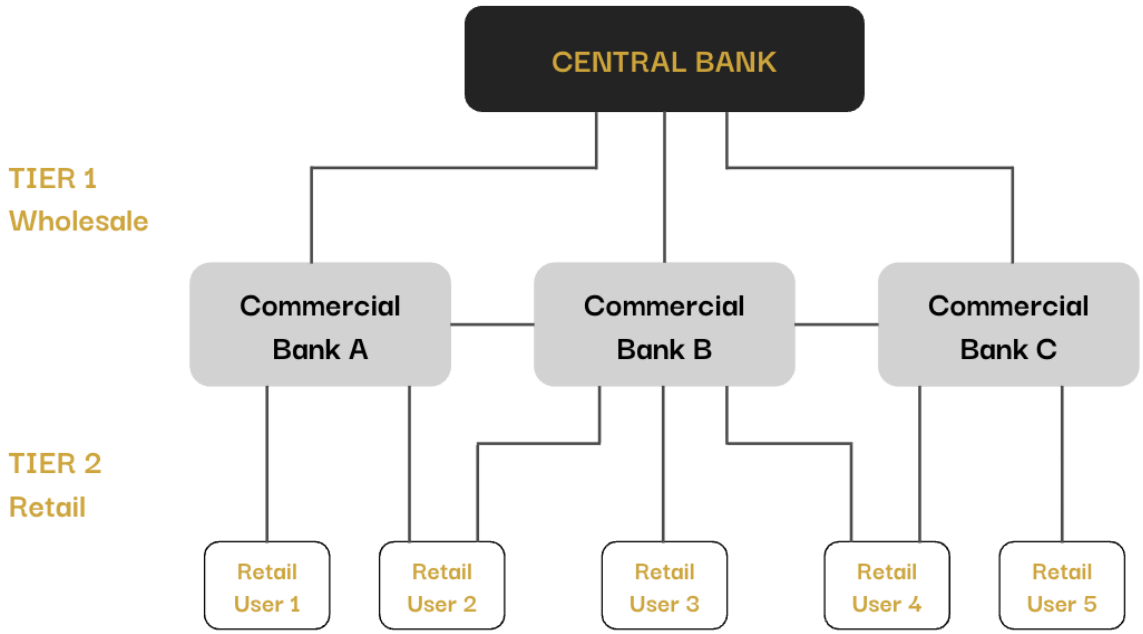

FIGURE A: Current Two-Tier Banking System

Knox Networks seeks to augment the abilities of all participants in the current two-tier banking system with the ability to enhance security, transparency, and auditability for financial institutions. Knox Networks recognizes the important role that banks play as intermediaries in the financial system both at the central bank and commercial bank level, and does not seek to disrupt the nature of the two-tier banking system. Instead, Knox Networks allows existing players to innovate to provide customers with new products and services while improving efficiency and lowering the cost of existing offerings.

To understand what Knox Networks's vision of the financial system might look like, it is crucial to understand how FBDAs work and exactly what makes them different from the existing payment architectures of today.

File-Based Digital Assets

A File for the Future of Money

The building block of the Knox Network system is the File-Based Digital Asset or FBDA, which is moved through the system and between stakeholders via the Interbank Platform. The FBDA provides the same benefits of physical banknotes with the added benefits of a digital-first technology.

FBDAs are authorized through the Authority Service as obligations against a particular Authority, and distributed into circulation by Authorized Intermediaries via the Distributor Service. In the case of a CBDC, generally a central bank will play the role of the Authority, and commercial banks or payment service providers will serve as Authorized Intermediaries. In the case of a commercial bank-issued coin, different divisions or departments within the commercial bank could represent both the Authority and the Authorized Intermediaries. More on this in the **Architecture** section.

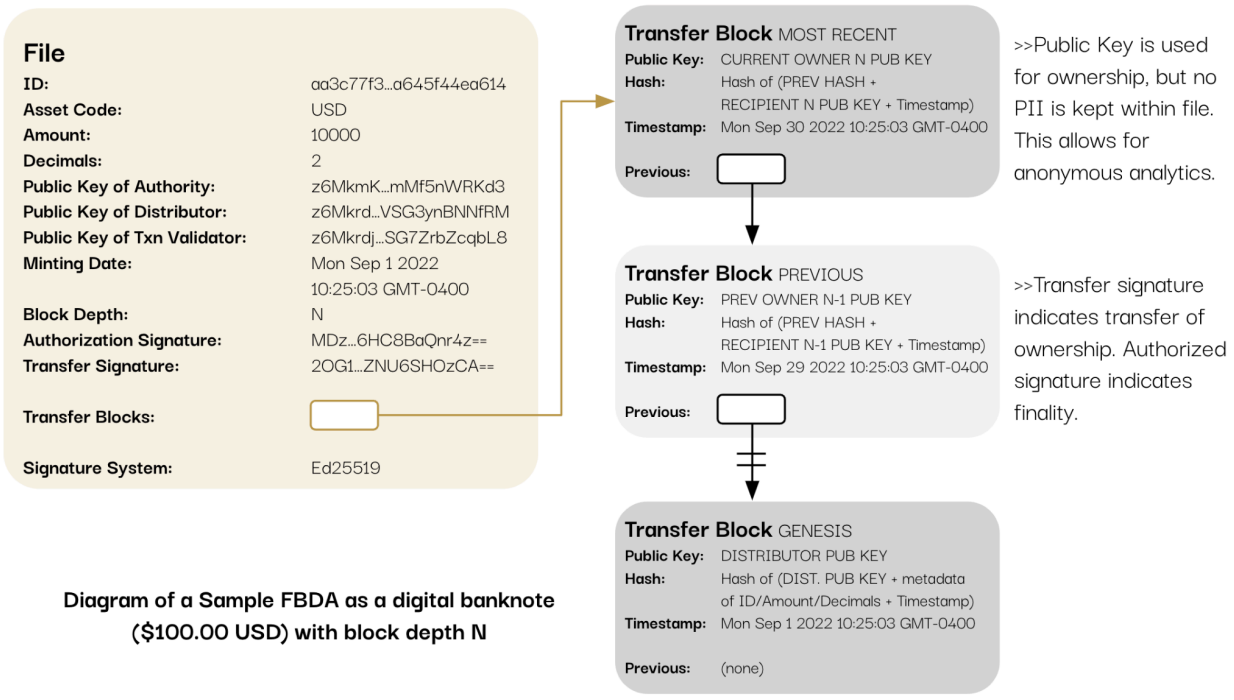

Diagram of a Sample FBDA as a digital banknote ($100.00 USD) with block depth N

FIGURE B: Diagram of a Sample $100.00 note FBDA with block depth N.
Suggested Maximum FBDA Size: ~6kb to keep FBDAs small.

As shown in **FIGURE B,** each FBDA comes with a number of properties inherent to the file itself, including (but not limited to) its cryptographic hash, amount and asset code (e.g., USD $100.00), and addresses for the Authority and Authorized Intermediary for that particular FBDA. The linked list grows from “size 1” to “size n” with each individual transaction adding a block to the chain.

How FBDAs Work

Rather than a distributed ledger-based system across the entire network, every FBDA builds its own individual linked hash-chain list, with the chain growing with each transaction (default max list size is 62 transactions, but this is configurable). The block depth of each FBDA grows as transfers occur through a two-part signature process.

Every FBDA in a transaction can be considered independent from one another, which allows for transactions themselves to be independent. This independence of FBDAs and transactions

allows for concurrent processing of transactions via sharding techniques, and enables the Knox Networks system to horizontally scale transaction validation within the system. This independence does not require a dependency of analyzing past payments (such as the case for UTXO models) nor of distributed consensus to authorize payments or assert the validity of a given FBDA. Since the integrity of the FBDA starts with the initial blocks signed by trusted entities (the Authority and the Authorized Intermediaries), any attempts to tamper with the FBDA are easily detectable. Also, an attempted compromise on an FBDA only renders that tampered individual the FBDA untranslatable, and not the entire network.

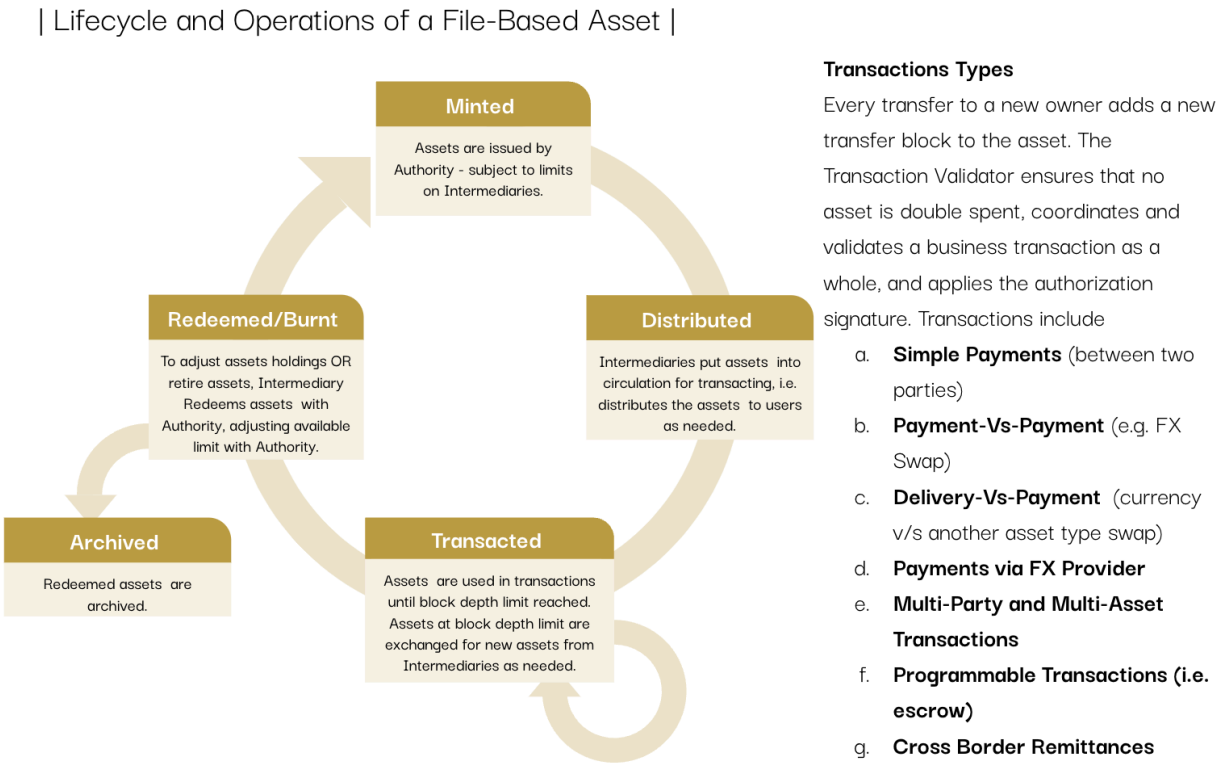

FIGURE C: Sample FBDA Lifecycle Diagram

Despite this power, FBDAs are designed to be compact. A fully transacted FBDA maxes out at 6kb under the Ed25519 signature system to remain small enough for storage on mobile devices or for embedding within other payment formats. After an FBDA hits the transaction block depth threshold, the FBDA is redeemed by the Authorized Intermediaries, retired to the **Analytics**

Service or Archival Service, and a new FBDA of equivalent value is re-distributed to go back into circulation, without interrupting the user experience. This threshold keeps FBDA file sizes small, and allows for renewal through the system of new versions of the FBDAs and historical pseudonymous analytics on transactions. **FIGURE C** showcases the entirety of the FBDA lifecycle.

Signing and Transferring FBDAs

Each FBDA contains a public key of the Authority and of the Authorized Intermediaries that originally minted the file. The Authority Public Key identifies which authority has authorized the distribution of the FBDAs, and the Distributor Public Key identifies which Authorized Intermediary distributed the FBDA.

Each FBDA contains two signatures: a "Transfer Signature" and an "Authorization Signature."

The owner of each FBDA is identified by the public key in the latest signature block. The Transfer Signature indicates the transfer of ownership from the previous owner and the Authorization Signature indicates the legitimacy of the transfer.

When the FBDA owner transfers ownership to the next owner, a new signature block is appended that contains the next owner's public key, a timestamp, and a hash of the previous block hash + the next owner's public key + the timestamp. This hash is signed by the transferring owner's private key to produce the Transfer Signature, indicating the transfer to the next owner. This Transfer Signature denotes the FBDA has been transferred to the new owner and can be cryptographically proven that the previous owner had assigned ownership to the new owner via the most recent signature block.

For the FBDA to be settled and to ensure the sender of the FBDA did not double spend the banknote, an Authorization Signature is required. When the FBDA is created, the Authorization Signature on the Genesis Block is always the Authority. For subsequent signature blocks, the Authorization Signature is provided by the Transaction Validator Service, which is a highly-scalable service that is given permission to validate transactions by the Authority or the Authorized Intermediaries.

This double signature system helps to secure FBDAs, and also helps in providing value added services on top of transactions such as atomic settlement capabilities like **Payment versus Payment (PvP)** or **Delivery versus Payment (DvP)**.

By authorizing the distribution of FBDAs to Authorized Intermediaries and the transaction validation to Transaction Validators, it allows for an 1) increase in the scalability of processing FBDA transactions and 2) easier separation of Authorities (such as central banks) from KYC responsibilities and daily retail transactions. In the case of a CBDC, this helps to closely mirror the current two-tier banking system, while augmenting the banking toolkit. In the case of a commercial bank-issued coin, this can allow for easier segmentation of KYC responsibilities for different jurisdictions.

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

Knox Networks vs. Existing Payment Systems

Knox Network's file-based solution provides improvement over other approaches that are being investigated to improve the current financial system. In particular, Knox Network's file-based solution avoids many of the pitfalls and shortcomings of distributed ledger technologies (DLT) and account based systems.

Knox Network's file-based architecture ensures and maintains atomicity, consistency, isolation, and durability principles (ACID) within its systems. By contrast, account-based systems typically attempt to maintain multiple disjointed ledgers by trying to keep them synchronized over a messaging layer. This makes account-based systems slow and error-prone, forcing the use of two-phase commits in an individual system's ledgers. In addition, these systems are not designed to build out auditable trails for every transaction and interoperate with one another easily. Indeed, auditability and interoperability usually require building an add-on system that generally adds complexity, delay, and error to the overall operation.

While distributed ledger systems have many security and interoperability advantages over traditional account based systems, these systems also fall short of the Knox Network's file-based approach. For example, distributed ledger systems require time consuming consensus mechanisms and therefore take an enormous performance hit for security, as there becomes a bottleneck in the number of transactions that can move through the system at a given time. This solution ultimately does not scale from a throughput perspective (transactions per second) nor from a latency perspective. This is especially true when trying to reconcile transactions across different geographical regions.

File-based systems improve upon the shortcomings of both the account based and DLT systems. File-based systems can scale independently of the number of transactions because each FBDA contains its own individual ledger and can be processed concurrently. Specifically, file-based systems are tokenized at the individual asset level, which allows these assets to be independently transacted and processed. This design allows for horizontal scaling by ensuring that multiple files can be processed simultaneously (concurrently) with the addition of more compute power, avoiding the bottleneck issues seen in other systems. In addition, file-based systems can still interoperate with both account-based and DLT systems because the files (i.e. packets of data) can be added as a payload to those external systems if necessary.

File-based systems come with their challenges, however, such as the fact that the size of each file grows with the number of transactions. Knox Networks's solution mitigates these problems via retiring and re-distributing FBDAs once they get to a certain size (~6kb), which allows files to be archived for analytical and auditing purposes. This is analogous to the current practice of removing paper notes from circulation after a certain period of wear and tear.

Identity Bridge

Helping to Manage "Who's Who?"

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.

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.

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 in tandem with VCs to help ensure that cryptographic operations can occur without needing to expose sensitive user data. The Identity Bridge integrates into existing identity systems, providing SDKs and modules for backend services, websites, and mobile apps in various programming languages (see **Technical Implementation**).

As banks and government institutions already provide identity services for its 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 bank or government institution's existing KYC process for AML/Sanctions checks against financial regulations. VCs can also be used to simplify the process for originally onboarding users in a cryptographically secure manner.

For example, the wallet can be a part of the bank'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 bank on behalf of the customer. Access can remain the same with the bank username and password login and banks can simply use their existing websites and integrate with Knox Networks wallet services over backend SDKs and APIs.

As shown in **FIGURE D**, the Identity Bridge creates a powerful yet empowering solution to the ever present problem of identity management within the financial system.

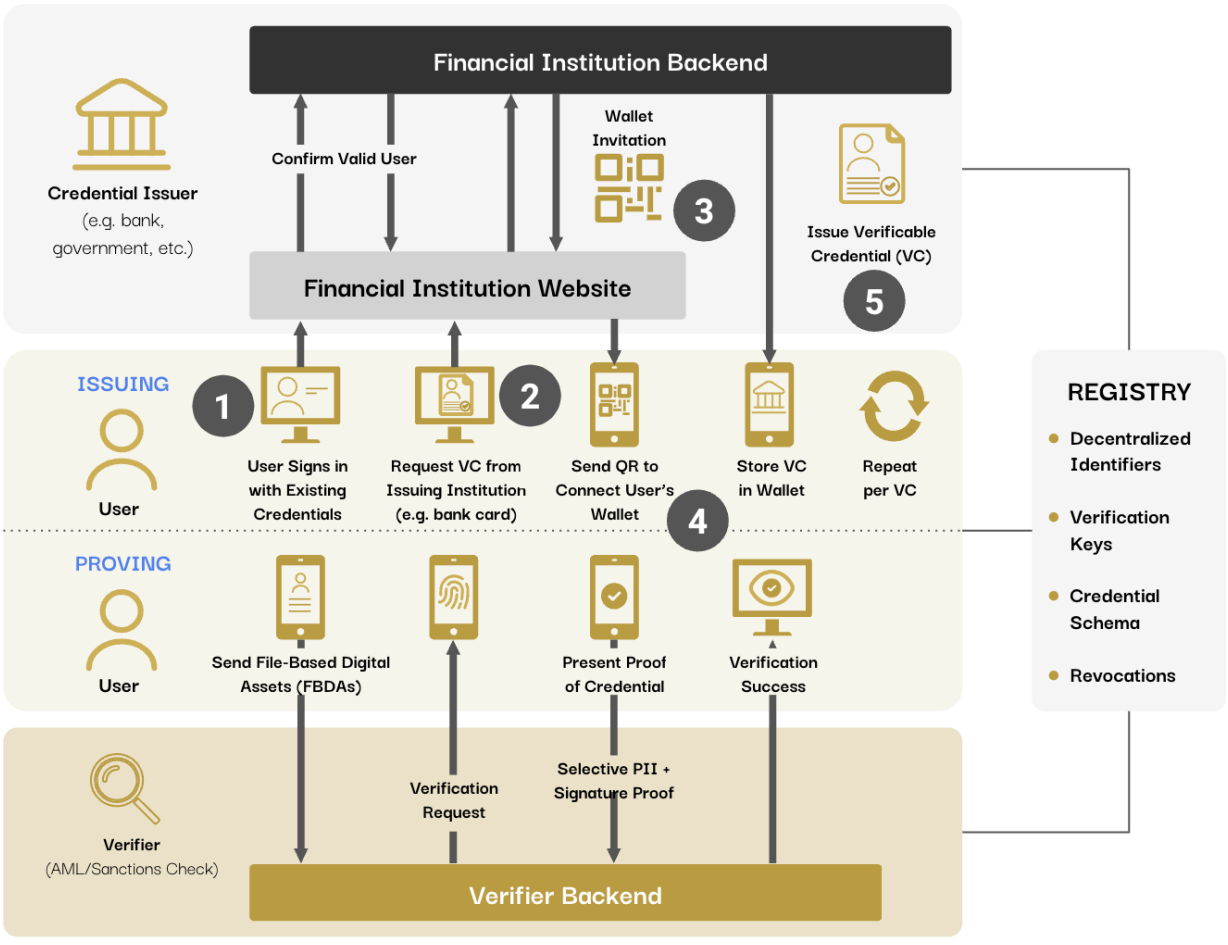

FIGURE D: Sample Identity Bridge Interaction Between Users and Banks

1. User is a customer of Bank A and logs in through the Identity Bridge using existing bank login credentials.
2. User is instructed by Bank A to register their wallet and requests a Verifiable Credential (VC) from the bank to capture the user's bank account details.
3. Bank 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 bank identifier as the credential issuer.
   NOTE: A bank hosted Custodial Wallet Service can also be used here.
5. The user now has this bank-issued VC held in the wallet. This data remains in the wallet and can be requested as needed for financial regulation.

Contract-Based Transactions

Multi-Asset, Multi-Party Atomic Transactions with Programmability

Knox Networks has implemented a system that separates the *programmability layer* (Contract negotiation) from the *asset transfer layer* (Contract fulfillment) that lives within the **Transaction Validator Service**. A **Contract-Based Transaction** fulfills a transfer of assets that is 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 (PvP, DvP), cross border payments, escrow, etc., and support industry recognized techniques such as Hashed Timelock Contracts (HTLCs).

Contract-Based Transactions reduce costly errors, 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 retain their original owner. **FIGURE E** shows a simplified view of a sample contract between two parties, Alice and Bob, in an FX transaction.

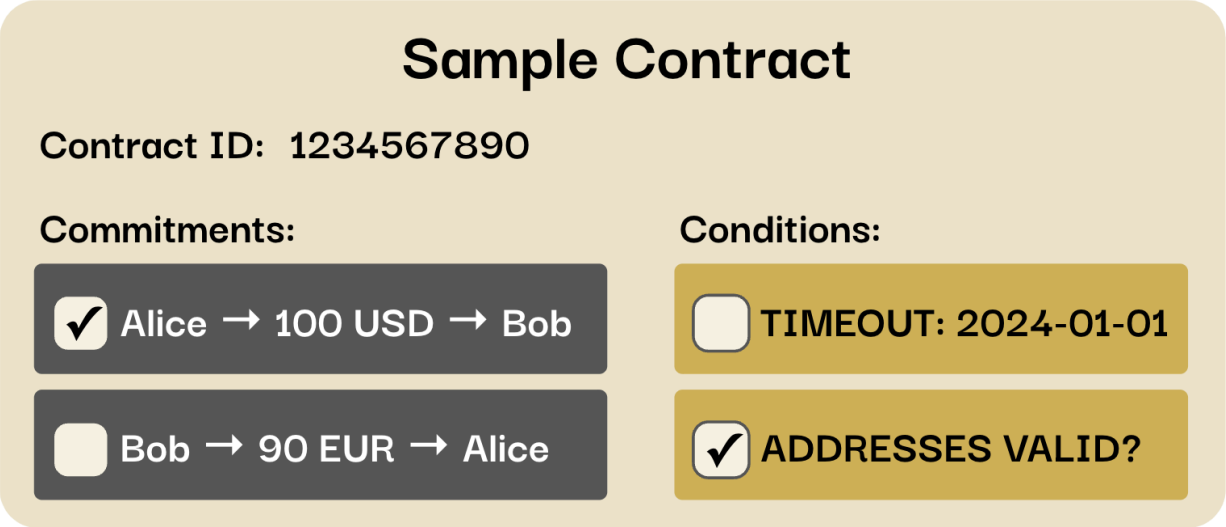

FIGURE E: Simplified View of a Sample Two-Party Foreign Exchange (FX) Contract

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 same 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..

FIGURE F showcases a simplified Contract-Based Transaction execution for a simple atomic swap between multiple-parties.

FIGURE F: Sample Contract-Based Transaction Execution Flow

Contract-Based Transactions are also able to carry messages in any format (e.g., ISO 20022, NACHA) inline with the overall transaction. With Knox, the traditional separation between messaging and asset transfers is eliminated and messaging is available inline with the transaction itself.

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 being able to integrate to DLTs over techniques such as HTLC mentioned above, this also allows easy integration with any traditional messaging interfaces and any variety of systems expected in a banking 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 other 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 bank 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.

System Design Goals

While existing payment innovations have offered improvements to previous models, today's global payments system still involves significant costs, delays, and risks. These frictions have ripple effects across the entire payments value chain, affecting government entities, commercial banks, and consumers alike. As a result of these pain points, Knox Networks was designed with the goals of solving for scalability, interoperability and programmability, and privacy and security, while preserving the two-tier banking system.

Scalability

Scalability has proven to be an issue for several payment 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 reconciliation, which creates a bottleneck in the system to scaling

efficiently as the number of transactions grows. Current traditional systems are not as scalable, especially at the retail level, due to fragmented back office functions, intermediaries, and settlement times.

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 all around the world, and thus designed a system that could rise to meet those requirements via high reliability, high throughput, and low latency.

Understanding the bottlenecks that exist in developing many centralized digital asset systems, Knox Network's FBDA solution was designed to horizontally scale. This horizontal scaling is possible because each FBDA, and thus each transaction, can be processed independently. This allows for FBDAs to be cryptographically signed and verified concurrently, removing the need for batching and an expensive consensus algorithm. While each **Transaction Validator Service** might have a limit of FBDAs they can process at a given time, each FBDA is not limited to exclusively one Transaction Validator Service to process a transaction. 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 taken out of circulation and re-distributed for scalable analytics once each FBDA has hit a transaction threshold (refer back to the **File-Based Digital Assets** section for more details).

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 Other Blockchains and Tokenization Platforms.

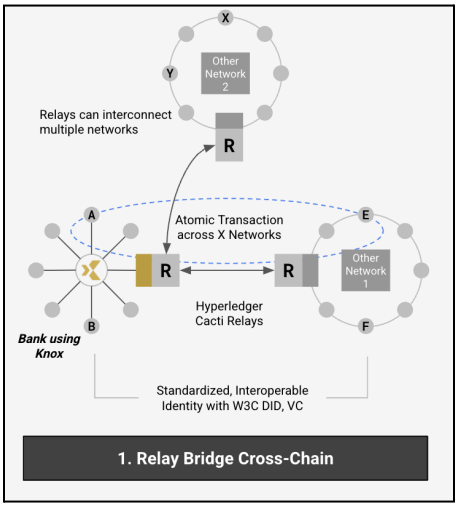

FIGURE G: Interoperability using Relay Bridge for Cross-Chain Communications

#1 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.

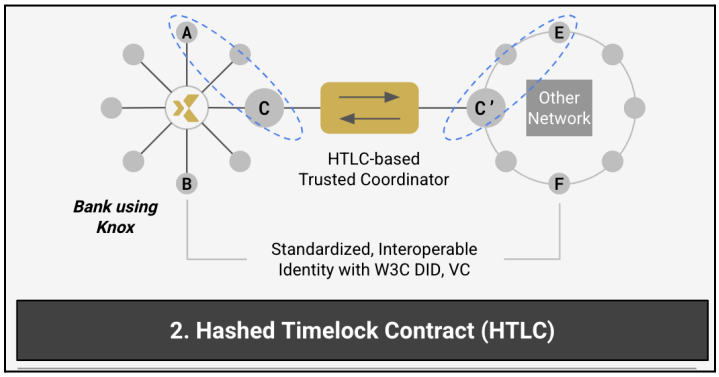

FIGURE H: Interoperability using HTLCs for Cross-Chain Communications

#2 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.

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

#3 Interoperability with Traditional Payment Systems

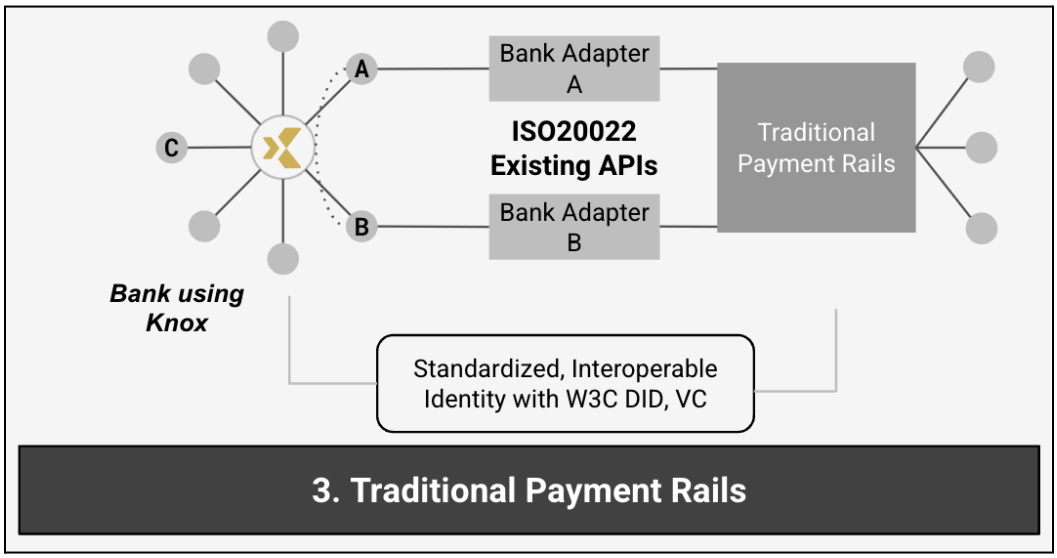

FIGURE I: Interoperability using HTLCs for Cross-Chain Communications

Knox allows 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 interfaces products in use at banks, 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.

Privacy and Security

The existing privacy and security landscape across the financial system is insufficient and is a legacy of older fragmented systems within the banking sector. Right now, large scale data breaches put potentially millions of users' data in jeopardy. In addition, there is also concern that central bank digital currencies (CBDCs) under some architectural designs may expose user data to central banks (and by proxy, the government), thereby eroding the current two-tier banking system and potentially user privacy.

Knox Networks implements a secure system that would enhance privacy over the current system and allow for integration across multiple identity schemas, including ones that would be accessible to those without a bank account. Refer back to the **Identity Bridge** section to review how Verifiable Credentials and Decentralized Identifiers can enhance user privacy. In addition, the decoupling provided by the separation of operations from the Authority Service and the Distributor Service allows for separation between the Authority and retail transactions.

FBDAs are pseudonymous, leveraging private/public key cryptography (e.g., Ed25519 by default but extensible to other cryptographic systems such as Secp256k1). 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 spends 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 preservation of privacy rights, yet banks 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, nor does it 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.

Preserving the Two-Tier Banking System

Preserving the two-tier banking system is crucial for the global economy, particularly in how large banks, especially global systemically important banks (GSIBs), serve as the basis of global trade and economic stability. Central banks do not currently provide large scale retail banking operations in most developed economies, and would largely be both reluctant and unprepared to take on the responsibility of large scale KYC for retail financial services. And as mentioned prior, there is also concern of allowing central banks the ability to view transactional data.

The platform's architecture (as described in the next section) was created to rely on the strengths and robustness of the existing financial system, protect user privacy by decoupling it from direct interaction with Authorities, and help financial institutions manage the transition to a tokenization of their assets for both currencies and for securities. This software architecture allows financial institutions to improve upon the challenges within current financial services and operate within a broader ecosystem of digital assets.

Architecture

Building a Forward-thinking Architecture

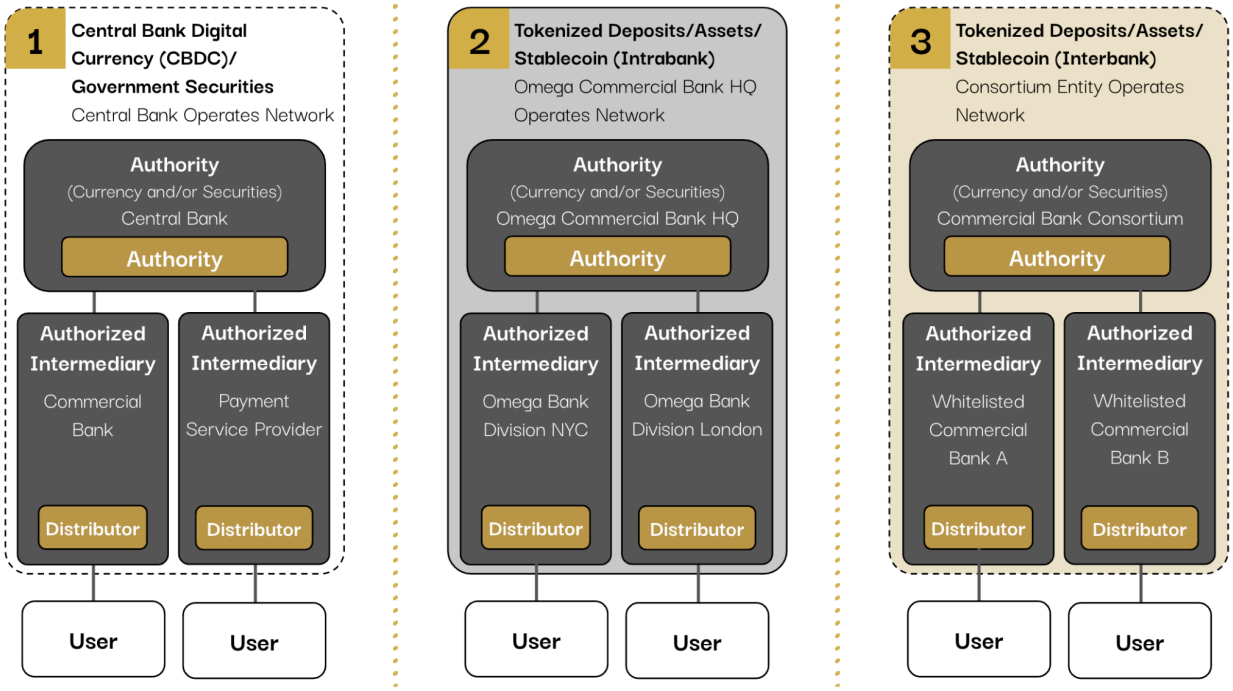

FIGURE J: Knox Networks Major Designs

Knox Networks seeks to improve upon the strengths of the two-tier banking system. It is important to note that this is a base configuration of the Knox Networks system, and can be customized to fit individual client needs. **FIGURE F** showcases the major (simplified) architectural models that Knox can fit. The focus of this section is to dive deeper into Model (1) as shown above for the sake of brevity and simplicity, since Models (2) and (3) are much more customizable to individual institutions, but are touched upon later at the end of this paper.

FIGURE G shows the potential architecture of the Knox Networks system for a CBDC, with the three tiers of users identified as Authorities, Authorized Intermediaries, and Retail Users which interact with each other via a variety of different services as described below. The **Use Case Examples** section showcases other sample network architectures, such as that of a commercial bank-issued coin.

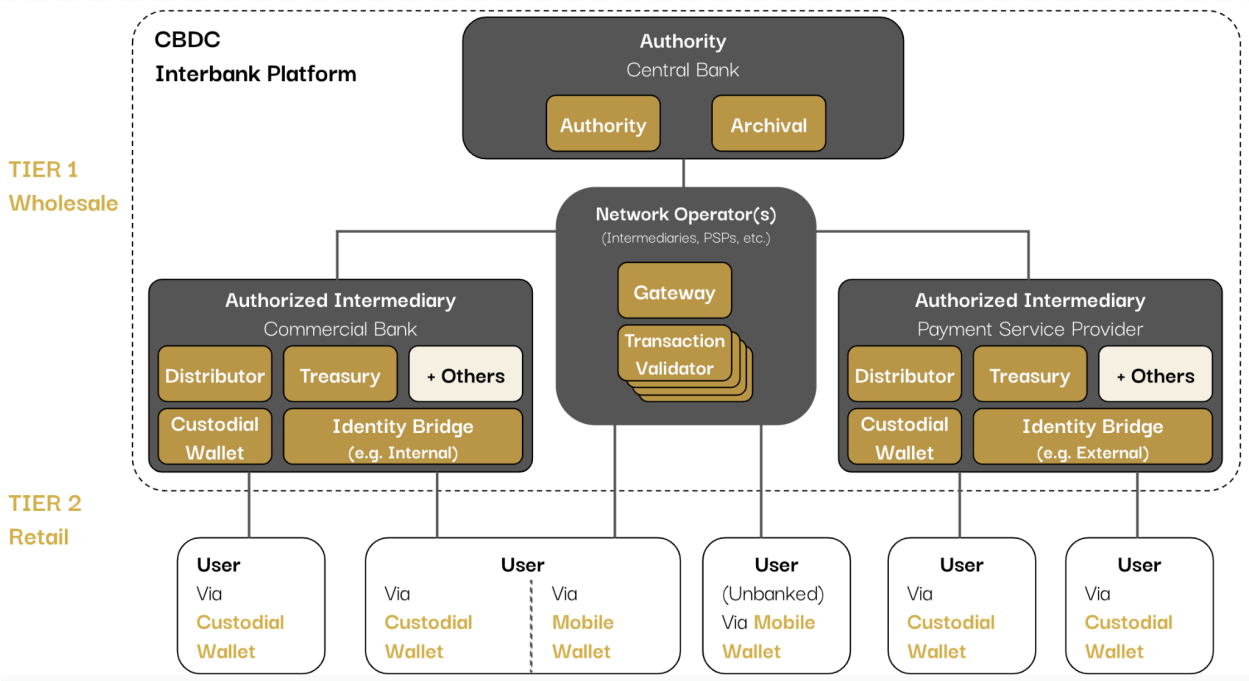

FIGURE K: Knox Networks Sample System Map for a Central Bank Digital Currency (CBDC)

Interbank Platform

The Interbank Platform serves as the underlying backbone of the Knox Networks system, connecting all the different institutional users and services within the network.

Authority

The Authority serves as the top level of the Knox Networks system, and through the **Authority Service** authorizes the issuance, management, and redemption of FBDAs in the system. In the case of a CBDC, the Authority would likely be a nation's central bank. In the case of a bank-issued coin or tokenized commercial deposits, the Authority would likely be a division within the bank, potentially within the Treasury Department. Authorities remain the arbiter over their financial systems' rules, and can authorize out permissions to other parties within the system in addition to authorizing permissions to themselves.

Authorized Intermediaries

Authorized Intermediaries serve as the middle layer within the Knox Networks architecture. Authorized Intermediaries can engage in the Knox Networks system through the system as permitted by the relevant Authority. In the case of a CBDC, Authorized Intermediaries would likely be commercial banks or payment service providers. In the case of a bank-issued coin or tokenized commercial deposits, Authorized Intermediaries may be divisions or departments within the bank. Authorized Intermediaries can be under multiple monetary and asset schemes, and thus can have different Authorities for different jurisdictions. For example, in an international CBDC scenario, Bank A could operate under the governance of Central Bank 1 in country 1 and under Central Bank 2 in country 2. Authorized Intermediaries primarily utilize the **Distributor Service** for distributing, managing, and redeeming FBDAs under the distribution limits set by the Authority.

Retail Users

Retail users interact with the Knox Networks system via Digital Wallets. Digital Wallets can either be provided server-side via the Custodial Wallet Service or via Mobile Wallets on user devices. Wallets are designed to integrate with identity management solutions both provided directly from the commercial bank, government institutions, and/or to individual sovereign data identity management solutions (see **Identity Bridge**). Commercial banks and other vendors may utilize the Knox Networks SDKs along with sample mobile apps to natively integrate the Knox Networks wallets into their own applications such as mobile banking, payment systems, or granular consumer analytics.

The Mobile Wallet allows for FBDAs to be directly transferred to mobile accounts and transacted offline (see **Use Case Examples**).

Unbanked Users

Knox Networks understands that not all potential end users of a retail digital wallet may have access to a bank account, particularly for CBDC applications. With permission from the Authority, a bankless Mobile Wallet can still be used within the system, with or without an identity

system (similar to how a debit card works today). To minimize potential fraud, the Authority could place relevant limits on these wallets (e.g., capping the amount of value that can exist in an unlinked wallet).

Main Services

Authority Service

Authorities utilize the Authority Service to:

1. Establishes distribution limits for the Authorized Intermediaries;
2. Provides the initial Authorization Signature on FBDAs; and
3. Authorizes newly minted FBDAs into circulation via the Distributor Service.

NOTE: Authorities can enact all the powers listed below on themselves, but for the purposes of this paper, it is assumed that the Authority (central bank in the case of a CBDC) will not be providing retail banking services, and will instead just authorize all services directly to the Authorized Intermediaries, i.e. retail commercial banks or payment service providers.

Distributor Service

The Distributor Service is run by Authorized Intermediaries and oversees the distribution of FBDAs into circulation. Through the Distributor Service, Authorized Intermediaries can:

1. Distribute and redeem FBDAs into and out of the system, under limits from the Authority;
2. Handles the distribution process of FBDAs to retail wallets; and
3. Replaces FBDAs in circulation once they reach a configurable size threshold.

Transaction Validator Service

The Transaction Validator Service processes transactions via two sub-services which perform complementary but distinct tasks: (1) the **Transaction Manager Sub-Service** coordinates and reasons about the status of the transaction, and (2) the **Notary Sub-Service** carries out the instruction of transactions.

The Transaction Manager Sub-Service is a robust solution for allowing programmability into the Knox system via overseeing the management Contract-Based Transaction. Utilizing the Transaction Manager Service for **Contract-Based Transactions** allows for more complex

transaction types to be built out, including atomic transactions such as **Delivery vs. Payment** and **Payment vs. Payment**. The Transaction Manager Sub-Service sends over authorization or rollback instructions to the Notary Sub-Service depending on fulfillment or violation of commitments.

The Notary Sub-Service is a highly-scalable method for validating transactions under jurisdiction from either the Authority or from an Authorized Intermediary. This horizontal scaling is possible because each FBDA is an independent proof-of-ownership, allowing for transactions of FBDAs to occur independently of one another (and therefore concurrently). The Notary Sub-Service can provide Authorization Signatures on FBDAs upon transfer.

Gateway Service

The Gateway Service can serve as a way for Authorities and Authorized Intermediaries to both monitor network health and guard against cyber attacks in the Knox Networks system. The Gateway Service can be run by a network operator that may be the Authority directly, a third party, or delegated to particularly important Authorized Intermediaries (e.g. GSIBs or commercial bank divisions).

Custodial Wallet Service

The Custodial Wallet Service transacts and holds FBDAs and bank customer information. This is the server-side version of the Digital Wallet that is hosted by the bank on behalf of customers. This wallet can provide bank customers with custodial accounts and interoperability with existing account-based systems. This system can allow for the storage of active FBDAs that belong to particular accounts, and for managing the transferring of FBDAs between accounts as necessary.

Mobile Wallet Service

The Mobile Wallet Service similarly transacts and holds FBDAs and bank customer information. This is the client-side version of the Digital Wallet that is hosted by retail users on their mobile devices, and allows for **Offline Transactions**. This wallet can provide privacy-preserving identity

services for users. This system can allow for the storage of active FBDAs that belong to particular users, and for managing the transferring of FBDAs between accounts as necessary.

Treasury Service

The Treasury Service oversees the management of holding multiple currencies, remittances, and other assets. Through the Treasury Service**,** central or commercial banks can:

1. Remits FBDAs denominated in domestic and foreign currencies;
2. Handles residual change distributions; and
3. Holds FBDAs denominated in various currencies.

Archival Service

For longer term storage, the Archival Service can be used by Authorized Intermediaries and Authorities to take FBDAs and provide space efficient, long-term storage compression for ad hoc queries of archived FBDAs (similar to a cold data solution in cloud environments).

Supplementary Services

The services outlined above are part of the core Knox Networks system. One of the benefits of a file-based architecture is that it allows for extensibility, thereby allowing for supplementary services (both internally and externally) to be built out as value add-ons. Here are two examples of what supplementary services might look like.

Sanctions Service

The Sanctions Service oversees the management of know your customers (KYC)/anti-money laundering (AML) compliance. Through the Sanctions Service, central or commercial banks can**:**

1. Parse and index sanctions lists (e.g., OFAC or UN)
2. Provide search queries with provided PII from zero-knowledge proofs
3. Batch banknote reports (e.g., suspicious activity) with regulatory bodies (e.g., FinCEN)
4. Regulators can define dynamic AML (including KYC) requirements for every movement of FBDAs according to amount, source, and destination

5. FBDAs also help address the Travel Rule since everyone in the network is known or if money is sent to someone out of network, they will not be able to collect it until they have provided the required KYC/AML information

Analytics Service

The Analytics Service can then take these retired FBDAs and provide time-series and static reporting of banknote files at varying levels of observability. This allows for Authorities and Authorized Intermediaries to perform historical analytics on these banknotes to better understand the flow of FBDAs throughout an economy, all while not providing access to user data through the disaggregation of transactional and personal data. Analytics providers can query an analytics API to obtain aggregate, pseudonymous historical transaction data for archived FBDAs.

Use Case Examples

Knox Networks In Action

There are two tiers of use cases that FBDAs fulfill. The first tier includes all basic functionality such as the distribution, redemption, transfer of FBDAs, and the management of distribution limits. The second tier builds on top of the basic flows and targets many of the pain points we see in the financial system today. These second tier use cases are explained below.

National CBDC Network

Perhaps the most obvious use case for the Knox Networks system is that of a national (or international) CBDC network. In this scenario, Knox Networks would be able to provide a country/currency union a fully integrated interbank and identity solution that supports all the flows of an economy, from currency distribution to management of financial institutions to transfers at both the retail and wholesale level. For example, the **Treasury Service** can be used for making cross-border payments at both the central and commercial bank levels.

FIGURE E in the **Architecture** section showcases a sample CBDC architecture under Knox.

Tokenized Deposits/Bank-issued Coin

While CBDCs have been in the public eye for some time, private money in the form of tokenized commercial bank deposits have also emerged as an attractive offering for commercial banks. Knox can handle both public and private forms of tokenized digital currency, and can help commercial banks with their management of assets both domestically and internationally. **FIGURE H** shows a sample Knox architecture for a large commercial bank that operates in multiple different jurisdictions and currencies. Combining this with a flexible tokenization scheme to represent securities as shown in **"Tokenizing" Other Asset Classes Into Files** would allow commercial banks even more extensibility within the system.

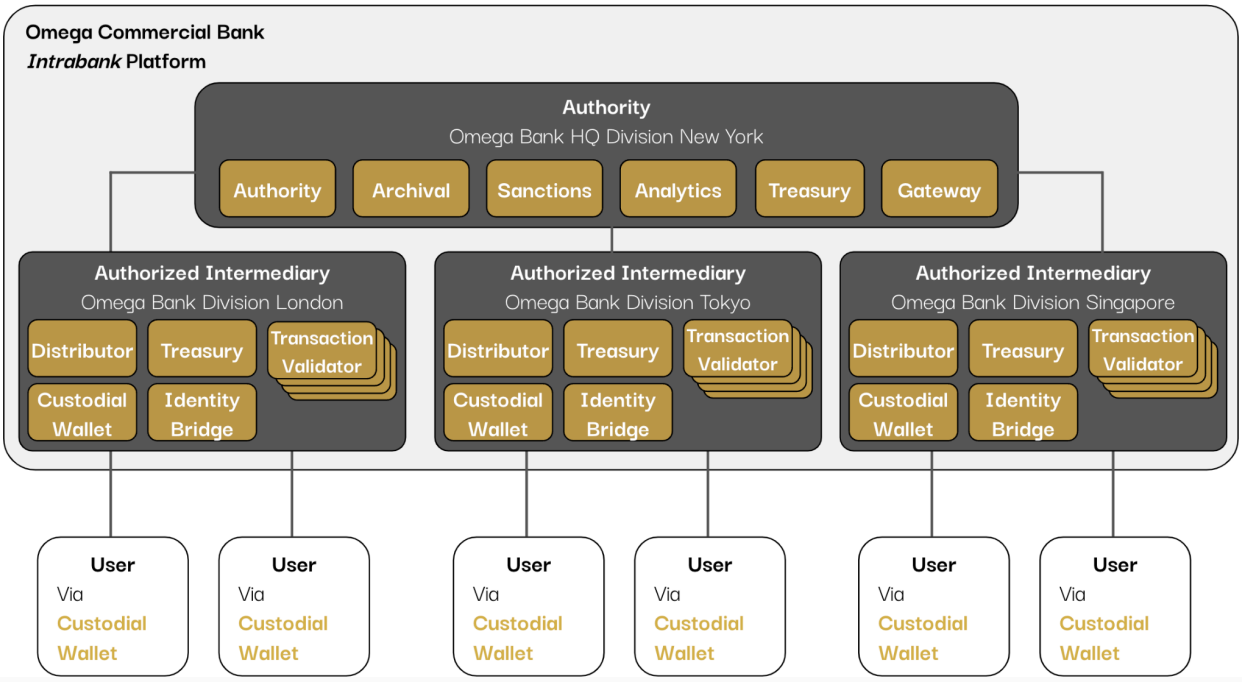

FIGURE L: Knox Networks Sample System Map for Tokenized Bank Deposits

NOTE: Bank-issued or other financial institution-issued stablecoins are technologically very similar to tokenized commercial bank deposits under the Knox system, but have non-insignificant differences with regard to regulatory requirements and broader KYC impacts. Both are supported by the Knox system, but "tokenized deposits" is the default scenario assumed for commercial banks.

Payment versus Payment (PvP)

Payment versus Payment (PvP) services, as highlighted in **FIGURE I**, are possible under the Knox Networks solution via the Transaction Manager Service. The Transaction Manager is used to create an atomic swap, which minimizes counterparty risk in foreign exchange transactions. By utilizing Hashed Timelock Contracts (HTLCs), the first half of a payment transaction can be committed through the local signature transfer of the relevant FBDAs, but the second half of the transaction is not to be signed and initial payment not released until after delivery of payment. If the other party provides delivery of services within a specified amount of time, the second phase of the transfer occurs, and the authorization signature is applied. This is an atomic settlement: either both legs of the transaction go through, or neither does. In the event that delivery of services is not applied within the timeframe, the transaction can then be abandoned, with no counterparty risk.

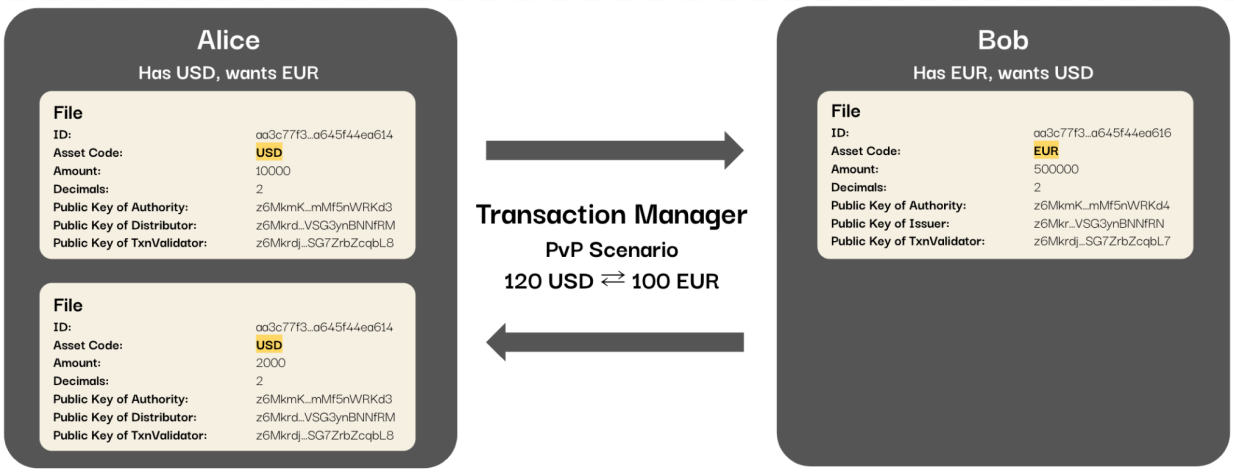

FIGURE M: Simplified Example of a PvP Transaction utilizing FBDAs in the Knox Architecture, Showing Foreign Exchange Transaction of USD for EUR

NOTE: Asset Codes highlighted for clarity

Delivery versus Payment (DvP)

Delivery versus Payment (DvP) services, as shown below in **FIGURE J** and **FIGURE K**, are also possible under the Knox Networks solution via the Transaction Manager Service. Similar to PvP

transactions, this atomic settlement capability helps to minimize the counterparty risk involved in a securities transaction. The only major difference between the two is that one party in the DvP transaction has an FBDA that represents a security of some type. Examples of securities that could be represented using FBDAs can be found in the **"Tokenizing" Other Asset Classes Into Files** section.

FIGURE N: Simplified Example of a DvP Transaction utilizing FBDAs in the Knox Architecture, Showing the Purchase of a Treasury Bill for USD

NOTE: Asset Codes highlighted for clarity

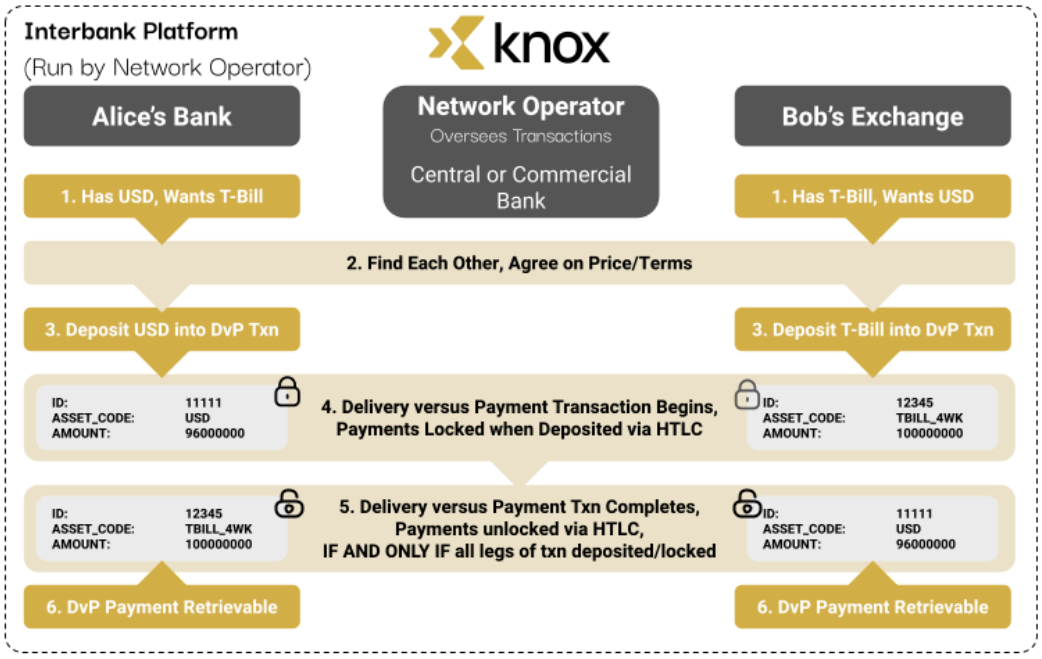

FIGURE O: Detailed Example of a DvP Transaction utilizing FBDAs in the Knox Architecture, Showing the Purchase of a US Treasury Bill for USD utilizing Contract-Based Transactions

Consortium Commercial Bank Network

A regional cross-border payments network could also be enacted without the overlying authority of a central bank to enact payments (though still subject to relevant central bank regulation). A consortium of banks could operate their own Knox Networks system using FBDAs to represent reserves that banks have with one another or with other types of assets. An Authority can represent the consortium, and authorize white-listed commercial banks as Authorized Intermediaries to distribute and transact FBDAs based on the reserves the bank currently holds across the Interbank Platform. Coupling this with PvP/DvP services, commercial banks could engage in more efficient transactions between one another with greater flexibility and transparency. This use case is illustrated in **FIGURE L.**

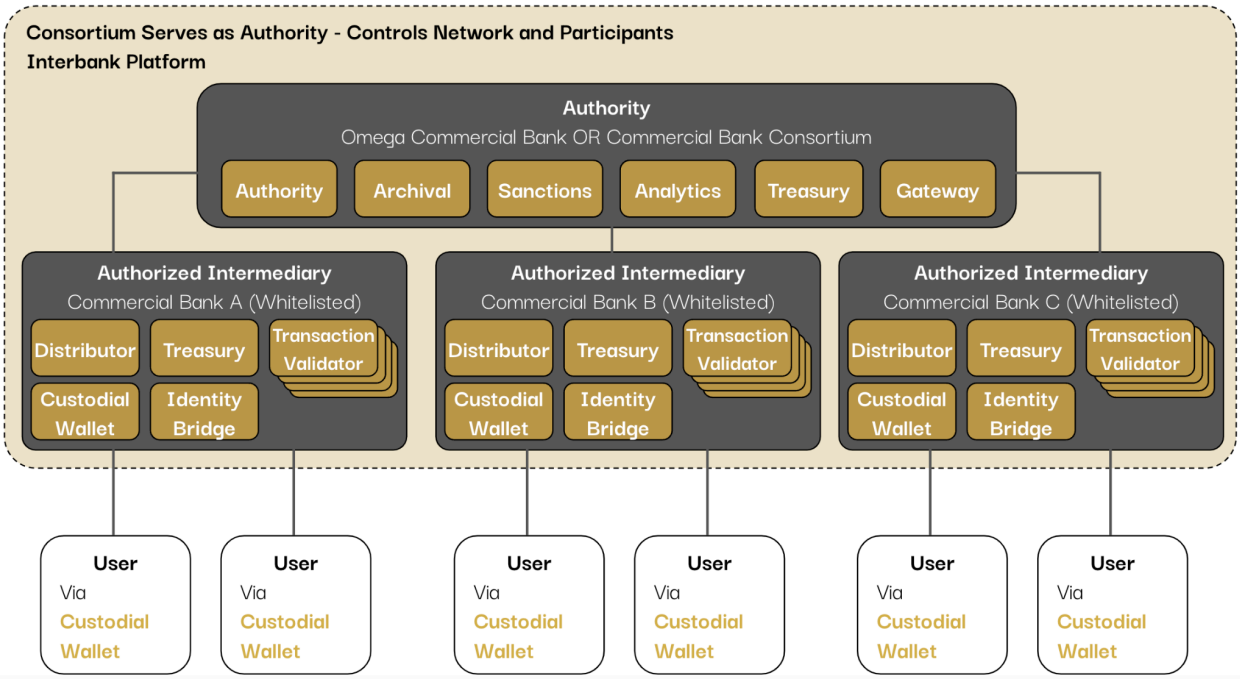

FIGURE P: Consortium Commercial Bank Network, with Commercial Bank Consortium running the Authority Role and White-listed Commercial Banks as Authorized Intermediaries

Economic Health Management

Through the **Gateway Service** and **Analytics Service**, Authorities and Authorized Intermediaries can monitor the health and status of the economic rails of the network. This would allow for a view into the underlying fundamentals of an economy at both the macroeconomic (for central banks) and microeconomic (for commercial banks and payment service providers) levels. For example, a better understanding of transaction flows could also enable governments to more closely monitor and mediate money velocity and supply, liquidity risks, and other macroeconomic risks.

Services for Business Logic Implementation

The Knox Networks system also provides the functionality for the creation of a transaction layer that can apply business level logic, simplifying many different business processes with an underlying payment API. Coupling this with the **Identity Bridge** solution, pre-validation of counterparty identity could be used to make transactions that ensure parties within a transaction really exist and are who they say they are. This feature of conditional transactions is also able to support processing of fees and change, while automatically creating a paper trail of receipts via the updated FBDAs.

Store-and-Forward

In the event a client cannot connect to the network, it is still possible to review FBDA balances and sign transactions. If the payee's device is able to be connected over standards such as USB, WiFi Direct, or Near Field Communication (NFC) the FBDA may be transferred peer-to-peer without an external network or third party service processing the transaction for one transaction "hop."

Each client may establish a direct connection to the bi-directional streaming networking layer using SDKs. The SDKs provide built-in message buffering, store-and-forward messaging when networks are unavailable, reconnection logic on transient network outages and allow packet routing between multiple networking services (see **Technical Implementation**).

Gateway Services can route packets to other Gateway Services to provide routing resilience when an end recipient cannot be found in the local network connections. For additional durability, the gateway service provides store-and-forward packets for configurable duration and size limit for connections that cannot be found.

Offline Transactions

FBDAs are designed to enable either the Transaction Validator Service to provide an Authorization Signature. By default, the Transaction Validator Service provides an Authorization Signature, enabling the horizontal scaling of cryptographic verification and signing, and providing a fault tolerance by reverting to the Authority to handle FBDA Authorization Signature in a last resort effort.

When the Transaction Validator is available by a retail user, possibly due to loss of local connectivity, end users can transact FBDAs on their mobile wallets peer-to-peer offline. This is especially important in areas where access to the internet may be scarce, such as where natural disasters may be prevalent. Low bandwidth technologies can be explored for an environment where connectivity is poor but still existent, to help authorize payments that were previously done offline.

FBDAs held locally can be queried for the wallet balances without internet connectivity. Clients are able to connect to multiple gateways and gateways are able to be networked to provide resilience in case one gateway goes offline due to a regional data center outage or other condition.

FBDAs are designed to allow for intermittent offline capabilities – i.e. one transaction “hop” in an offline environment. The system can be configured by an Authority to allow for subsequent offline transactions without resyncing to a network, but it is noted that this increases the risk of fraud via double spend attacks and replication attacks. To guard against these attacks for offline transactions, specific rules can be enacted to minimize fraud potential. For example, a provision could be enacted to cap the limit of offline transactions (e.g., a $10 billion contract between banks should be verified immediately online versus allowing offline transactions of $20 between end users and retail institutions). In addition, analytics and monitoring alerts can be

used to help identify suspicious activity within the network, which allows issues to be raised and prosecuted for participants that are trying to engage in fraudulent transactions.

"Tokenizing" Other Asset Classes Into Files

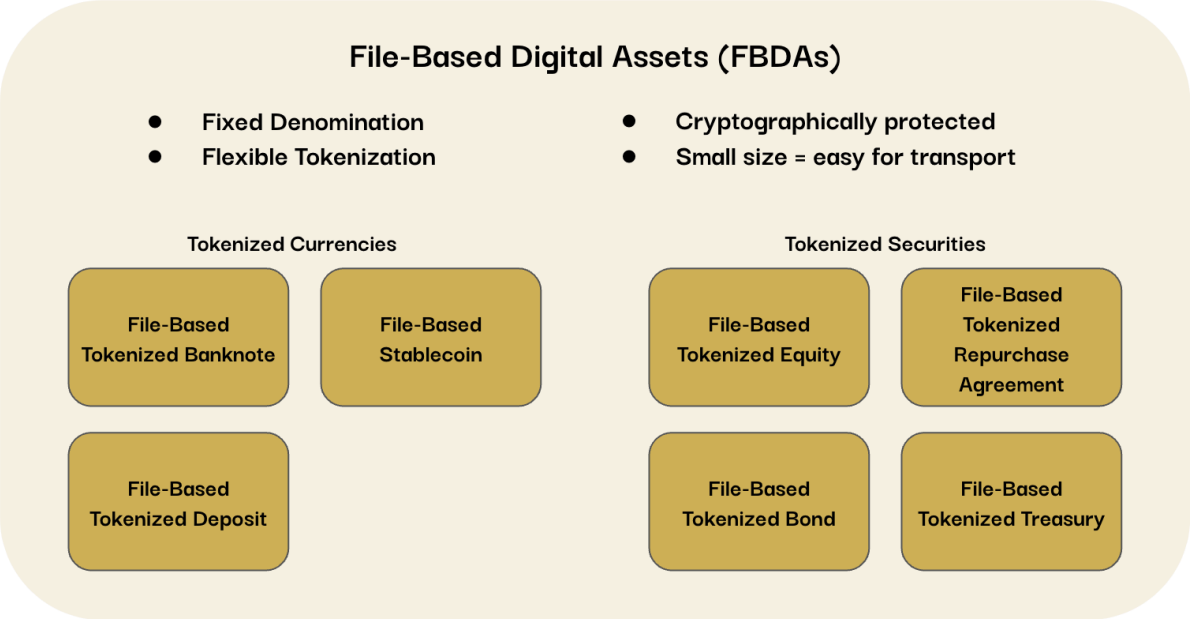

FIGURE Q: The Tokenization Flexibility of File-Based Digital Assets

As mentioned earlier, this white paper has outlined the ways in which FBDAs could be used to transform existing banknotes in the financial society, but this is only a small part of how FBDAs could transform many more asset classes by "tokenizing" them via FBDAs.

Non-banknote asset classes could be "tokenized" via FBDA technology to similarly track the ownership, management, and transfer of different digital asset classes in a manner similar to what has been shown with FBDAs. These different asset classes could include assets like securities, treasuries, and repurchase agreements as shown in **FIGURE M**, and are applicable to be used both by central banks (such as distributing treasuries or other government securities) and by commercial banks (such as corporate bonds or other securities).

Technical Implementation

Engineered to be Robust

Knox Networks' technical backend utilizes the industry-standard container management system for deployment. This allows for easier maintenance and monitoring of deployments, which is critical in large-scale infrastructure projects. The Knox Networks software platform fits within a variety of different cloud and database options, relevant to both client needs and to relevant regulatory requirements.

Knox Networks is developing an API that is designed to work across languages and platforms to allow for clients to realize the full potential of Knox Networks' network interoperability. Knox Networks also provides web and mobile SDKs that can be utilized for a variety of applications from native integration into client applications, to plug-and-use applications that could be utilized by third party platforms.

Check out the **Developer Portal** for the most up-to-date information on Knox Networks's technology.

Conclusion

Knox Networks: Scalable, Interoperable, Secure

Knox Networks has designed a software solution that builds on the current two-tier banking system while also augmenting the abilities of large financial institutions within existing regulatory requirements. Knox Network's architecture and novel file-based technology (i.e. File-Based Digital Assets) enables improved access to the global financial system and frictionless payments by focusing on privacy, scalability, and interoperability between different financial standards and payment networks. This extensible software can be leveraged for several use cases within the financial industry.