USBC

U.S. Bank Coin

Tokenized Deposits

Whitepaper — v1.0

October 2025

Overview

U.S. Bank Coin (“USBC”) is the world’s first retail tokenized deposit offering. Tokenized deposits can represent a superior digital dollar when compared with stablecoins, combining the benefits of blockchain with the safety and stability of the traditional banking system. While stablecoins are synthetic dollars, often issued by a fintech, USBC is an on-chain representation of real dollars and is issued by a U.S. bank. These digital U.S. dollars are designed to enable the underlying deposit to be eligible for FDIC insurance coverage through the issuing bank and Reg E protections.

Other tokenized deposit products exist, but USBC is the first to provide direct access to end users, made possible by its permissioned blockchain and risk management tech stack. USBC’s API-centric approach means that developers building on the platform can offer their customers digital U.S. dollars and their own U.S. bank deposit account worldwide.

Table of Contents

Executive Summary

In this paper, we introduce the U.S. Bank Coin ("USBC") Token, a U.S. dollar-denominated, identity-centric tokenized deposit powered by the USBC platform and recorded on the USBC Tokenized Deposit Network. The USBC Tokenized Deposit Network is a compliance-first, identity-enabled blockchain designed to support programmable and auditable financial transactions. Unlike stablecoins, USBC is not a newly issued digital asset backed by reserves. Instead, it is a tokenized representation of an existing U.S. bank[1] deposit held at a nationally)-chartered bank. Each tokenized deposit is an on-balance-sheet deposit recorded in the bank's general ledger, providing the same regulatory protections–including Federal Deposit Insurance Corporation (FDIC) insurance–as a traditional deposit with the added functionality of blockchain-based ownership and transfer. Tokenized deposits are issued on the USBC blockchain to represent ownership and transaction history, but no off-ledger reserves or synthetic mechanisms are used. All balances are fully reconciled with the issuing bank's general ledger, ensuring transparency, auditability, and regulatory compliance.

This model retains the advantages of blockchain-based money, such as speed, programmability, and accessibility [1], while operating fully within the U.S. commercial banking regulatory perimeters. It reflects a forward-looking approach that unites regulatory compliance, public trust, and financial inclusion with the innovation of distributed ledger technology.

Key differentiators of USBC include:

- **Identity As a Prerequisite For Use** - Every user must verify their identity before accessing the USBC ledger, which operates on the USBC Tokenized Deposit Network. Users create a unique personal or organizational identifier (a "name") in the system's namespace, serving as a directory entry for routing payments. Only identity-approved accounts can hold or transact tokenized deposits, ensuring that all participants are known to the bank (through direct or indirect relationships) and compliant with Know Your Customer ("KYC") standards.

- **Progressive Identity Levels and Access Tiers** - The model uses a risk-based approach and defines three identity trust levels–Bronze, Silver, and Gold–which reflect the strength of a user's verified identity based on submitted information. Silver and Gold are the equivalent of the minimum requirement for regular checking accounts with CPI compliance level of onboarding, while Bronze is a contemplated future product construct equivalent to an account type that does not require full CPI compliance. These levels only indicate identity assurance and are not dispositive of financial access or transaction limits.

---

[1] In this whitepaper, the term "bank" refers to U.S. insured depository institutions, including commercial banks, credit unions, and savings associations.

    - Bronze: Self-reported personal information and basic contact verification (e.g. phone or email).
    - Silver: Government-issued ID, selfie match, and proof of address.
    - Gold: Verification of an existing account with a regulated financial institution.

  Separately, each user is assigned a risk level of Low, Medium, High, or Very High, based on fraud indicators, sanctions and politically exposed person ("PEP") screening, geolocation confidence, device signals, and other contextual data. A user's actual permission, such as transaction limits, balance caps, and available features are governed by their assigned financial access tier (e.g. Base Tier, Tier 1, Tier 2, etc.). Financial access tiers are determined by combining the user's identity, trust level and risk rating. This layered structure keeps identity verification, risk classification, and financial access clearly separated but interoperable. It supports inclusive onboarding while ensuring that elevated financial privileges are granted only when both identity trust and risk posture meet appropriate standards, detailed within the Trust & Identity Management section of this whitepaper..

- **Privacy-Preserving Design** - The system is designed to protect users' personal data and transaction privacy. Personally Identifiable Information ("PII") provided for identity verification is kept confidential by the issuing bank in compliance with privacy laws (e.g. the Gramm-Leach-Bliley Act) and is not recorded on any public ledger. Transaction details on the blockchain are not publicly visible, preventing unwanted tracing of users' payment activity. Users retain control over what information to share and with whom, except as required by law for compliance. In practice, this means there is no public blockchain explorer revealing USBC transfers—only authorized participants and the bank can see necessary details, and even counterparties see only the information that has been consented to. This privacy-by-design approach enables open banking features without compromising personal data security.

- **Permissioned But Open-Access Blockchain Infrastructure** - The USBC ledger currently operates on a permissioned blockchain architecture, granting access solely to pre-approved participants [2]. Token custody and transaction initiation are limited to individuals and entities that have successfully cleared the bank's identity and eligibility screening. All transactional activity is governed by USBC's off-chain rules engine, which applies identity, risk, compliance, and financial controls before any transaction is approved. While the initial implementation uses a private blockchain to accelerate development, the long-term vision is chain-agnostic. The rules engine is designed to operate across both private and public chains, ensuring that core compliance logic is enforced consistently regardless of the underlying infrastructure. Importantly, even users at the entry-level access tier are subject to foundational screening and monitoring processes that exceed traditional standards for comparable financial instruments. This ensures that a baseline level of accountability is preserved across all user categories, reinforcing regulatory alignment without compromising scalability. The result is a secure, bank-supervised framework capable of evolving toward broader interoperability while maintaining strong compliance and user governance from the outset.

- **Robust Risk and Compliance Controls -** USBC is designed from the ground up to be safe, secure, and compliant, giving regulators and users confidence akin to traditional banking. Identity verification

and tier-based limits provide a strong foundation to prevent illicit use. All USBC transactions undergo risk-based monitoring before execution through interdictive rules and after execution in order to spot patterns of suspicious activity. This real-time oversight enables the bank to preemptively block or flag unauthorized transactions rather than only reporting them after the fact. In addition, the rules engine enforces objective limits to curtail risk. Standard bank-level controls such as capital requirements and liquidity management apply to the bank itself, not directly to the USBC token. However, the issuance and movement of USBC occur within the bank's regulated environment, benefiting from its broader risk management infrastructure.The initiative extends the full suite of bank risk management practices into the digital asset environment, addressing concerns that have plagued unregulated stablecoin systems.

- **Full Integration with Banking Protection and Regulation -** USBC is fully integrated into the existing banking system and governed by U.S. financial regulations. Each token in the user's Digital Wallet account represents an ownership interest in an underlying deposit liability held at a U.S. depository institution. A Digital Wallet is an application or interface that enables users to interact with their tokenized deposits by managing the cryptographic keys needed to authorize transactions, either through a custodial model managed by the bank or a non-custodial model managed by the user if supported, while also displaying balances, transaction history, and send/receive options.

- **Eligibility for FDIC insurance** - These underlying deposits are eligible for FDIC insurance, up to the applicable limits per depositor in the event of a bank failure, similar to funds held in a traditional checking or savings account. Funds backing USBC are held on the issuing bank's balance sheet, not in offshore trusts or segregated investment vehicles, and are managed under normal supervisory oversight. Rather than relying on omnibus For Benefit Of ("FBO") accounts or core banking systems, customer balances are recorded directly on the bank's general ledger and mirrored on-chain via tokenized representations. When a deposit is made, the corresponding token is issued to the user's wallet address, and the liability is simultaneously recorded in the general ledger. Withdrawals trigger a token burn and a matching debit from the general ledger–preventing the double-spend of money. This eliminates the need for shadow accounts or complex system synchronization, while maintaining full auditability and reconciliation between the blockchain and the bank's general ledger. USBC represents regulated bank money, not a new form of private currency. It avoids many of the financial stability and monetary control concerns associated with stablecoins that, while regulated, do not operate within the same framework as insured bank deposits. Unlike those models, USBC is designed to function as a compliant, insurable, and redeemable digital dollar that aligns fully with existing U.S. monetary policy and banking standards.

In summary, USBC offers a compliant bridge between traditional banking and digital assets. It delivers many of the benefits that crypto stablecoins promised—faster settlement, 24/7 availability, global reach, and programmability—but with the credibility and safeguards of the established banking framework. Users gain more inclusive access to dollar-based payments and innovation without sacrificing trust. Meanwhile, banks and regulators retain oversight of money flows, ensuring that controls around identity, fraud, and systemic risk remain intact. This whitepaper details the architecture, features, and governance of the USBC system, illustrating how it can enhance financial inclusion, preserve privacy, and future-proof the role of

banks in the digital economy. It also contrasts this approach with other digital money formats (e.g. stablecoins, traditional systems) to highlight why USBC represents an evolutionary middle ground, combining the advantages of both traditional banking and digital-asset approaches.

Introduction

Money has continually evolved over the ages, but it is traditionally defined by three primary functions: store of value, medium of exchange, and unit of account [3]. Modern fiat currency (e.g. the U.S. dollar) largely fulfills these functions domestically, whereas early cryptocurrencies (e.g. Bitcoin) introduced revolutionary new payment technology but failed to reliably serve as money due to extreme price volatility. This gap led to the rise of fiat-backed stablecoins in recent years as a "bridge" between traditional finance ("TradFi") and decentralized finance ("DeFi"). A stablecoin is a blockchain-based token designed to maintain parity with a national currency (usually 1:1 with U.S. dollars) by being fully backed with reserve assets [4]. U.S. dollar stablecoins have seen rapid growth—from virtually nothing a few years ago to a market of over $300 billion[2] in circulation [5]—and some projections saw the market approaching trillions of dollars within a few years [6]. These dollar tokens have demonstrated the demand for digital, always-on dollars and have showcased advantages in access, speed, and cost of payments, especially for tech-savvy users globally.

However, current implementations of fiat-backed stablecoins have shown both significant benefits and serious drawbacks [7, 8, 9]. On one hand, they offer the technical benefits of cryptographic transactions and global reach; on the other hand, most stablecoins operate outside of traditional banking regulations and compliance frameworks. Public stablecoin networks typically allow pseudonymous or anonymous activity, making it challenging to enforce anti-money laundering ("AML") rules, sanctions screening, and other financial crime controls on-chain. There is documented evidence of bad actors misusing permissionless stablecoins—from terrorist financiers to sanctioned regimes and drug cartels—precisely because those systems do not inherently require identity or provenance checks. Additionally, users transacting on open blockchain networks face a complex and less familiar user experience, often dealing with long cryptographic addresses and self-custody risks. These factors contribute to a trust deficit that limits stablecoins' adoption as a mainstream medium of exchange beyond the crypto niche. Policymakers worry about stablecoins undermining long-established safeguards in finance, and many consumers and enterprises are hesitant to transact in systems where neither parties' identities nor transaction legitimacy is assured.

A key insight this whitepaper highlights is that the benefits of digital tokenization can be paired with robust identity and compliance controls to create a form of digital money that innovates within the regulatory guardrails, rather than outside them. This approach was initially pioneered in the context of stablecoins-–envisioning an identity-driven stablecoin ecosystem-–but it has since evolved toward an even more bank-integrated model: tokenized deposits. By applying an identity and trust framework to tokenized bank liabilities, the approach achieves both sets of advantages-–the convenience and programmability of blockchain tokens and the safety and oversight of the traditional banking system. With USBC, bank money

[2] All amounts given in U.S. dollars unless otherwise indicated.

meets the blockchain. It transforms a standard demand deposit into a real-time, on-chain representation that moves within a distributed ledger environment while remaining fully-recorded within the bank's general ledger. The token and the deposit are a synchronized, dual-entry record of the same bank liability simultaneously recorded across two ledgers: the bank's general ledger and the USBC blockchain.

The tokenized deposit model addresses the shortcomings of prior stablecoins by keeping digital dollars entirely within the insured banking system. Participants are not anonymous internet users but verified individuals with direct or indirect relationships with a regulated U.S. depository institution, each subject to various levels of identity verification and ongoing compliance controls. Every transaction is associated with a known identity (though, as described below, personal details remain private between transacting parties), enabling real-time enforcement of financial crime safeguards and policy-based controls. At the same time, users gain the benefits typically associated with stablecoins, including instant settlement, 24/7 availability, and global reach, without assuming the structural risks of privately issued tokens. Crucially, tokenized deposits are not synthetic instruments or newly created private monies. They are merely digital representations of existing demand deposit liabilities recorded directly on the depository institution's general ledger. Unlike stablecoins that rely on segregated reserves, offshore trusts, or FBO account models, USBC balances are held as direct deposit obligations of the issuing depository institution and are eligible for FDIC insurance up to applicable limits. Redemption is not contingent on collateral sufficiency or off-chain processes; when a user exits the system, their wallet balance is debited and the corresponding amount is reflected as a debit to the user's deposit liability, settled through standard bank operations. This structure eliminates depegging risk and preserves one-to-one parity under all conditions.

Furthermore, tokenized deposits operate within the fractional reserve banking model, meaning deposited funds support lending and credit creation, which enhances economic utility without compromising individual liquidity. Consumer protections, including those provided under the Electronic Fund Transfer Act (known as the "EFTA" or "Regulation E"), apply fully to these accounts and offer users recourse in the event of unauthorized transactions or related disputes [10]. In addition, USBC may accrue interest where applicable, just as with any other insured deposit, allowing customers to benefit from yield while retaining digital utility. By recording deposit liabilities in the bank's general ledger and reflecting individual ownership and transaction history on the blockchain, the model creates a synchronized, dual-record system that supports innovation without fragmenting monetary control or destabilizing deposit bases. Unlike unbacked cryptocurrencies or prospective CBDCs that could disintermediate banks, tokenized deposits reinforce the existing structure of deposits, loans, and reserves. The only substantive change is the modernization of the payment infrastructure on which a customer can use his or her funds.

This whitepaper will explore the USBC system in detail. We will discuss the utility and use cases unlocked by tokenized deposits, the underlying technology and how it integrates identity and privacy, the issuance and redemption process, and how reserves, circulation, and risk are managed within a bank-regulated environment. We will also outline the governance and legal/licensing considerations, demonstrating that this model can be deployed under existing laws and oversight. Throughout, we contrast USBC with both stablecoins and traditional payment systems to highlight the unique advantages of each. Our goal is to show how USBC can enhance financial inclusion and efficiency while strengthening trust in the monetary system, ultimately emerging as a viable digital dollar paradigm for regulators, banks, enterprises, and end-users alike.

Utility and Use Cases

USBC's core value proposition is that it provides a safe, compliant, and versatile foundation for a variety of payment use cases and financial applications. By combining the real-time settlement and programmability of blockchain technology with the trust and familiarity of regulated bank money, this model unlocks opportunities that benefit both consumers and businesses. We expect third-party innovators building on the platform will discover and implement numerous impactful use cases beyond those already identified including:

- **Financial Inclusion and Open Access:** A core promise of this model is to extend access to regulated financial services for the unbanked and underbanked—using a *risk management*, not *risk avoidance*, approach. Much like how consumers today can purchase prepaid cards or money orders without forming a direct relationship with a bank, Bronze-level users can engage in limited transactions and receive USBC tokenized deposits through indirect banking relationships. However, unlike legacy payment instruments that offer complete anonymity, our model introduces meaningful compliance guardrails even at the most basic level. Bronze users are required to provide verified contact information, self-declared name and date of birth, and an associated IP address, delivering a significantly higher degree of traceability and accountability than traditional prepaid products, where funds still reside in a bank's treasury without any attached identity. Before onboarding users at even the bronze tier, we conduct a comprehensive risk assessment, evaluating phone, email, and IP fraud scores, as well as performing sanctions screening and negative news checks on the proposed bronze customer. Only users who meet these baseline thresholds are enabled to receive and hold limited tokenized deposits within our system. To further support financial inclusion within a compliance framework, we intend to offer payment cards with limited functionality to Bronze users. These tools allow us to monitor and assess transaction behavior within conservatively set limits. By observing spending and deposit patterns, we can begin to build a behavioral profile, even in the absence of full identity documents. As users provide more identity data and demonstrate consistent, predictable financial behavior, they become eligible to move up to higher identity trust levels (i.e. Silver and Gold), unlocking broader functionality and deeper integration with the formal financial system, subject to more additional review. This tiered, risk-based approach enables users without prior banking relationships to start building a verifiable financial footprint—something that is simply not possible with today's disconnected prepaid systems. It offers a seamless and compliant on-ramp into the regulated financial system within a limited and measurable risk framework, while maintaining strong oversight, identity controls, and the flexibility to adapt to individual user profiles over time.

- **Cross-Border Payments and Remittances:** International payments today are often slow and costly, passing through multiple correspondent banks and networks (e.g. SWIFT wires) with high fees and delays [11]. A tokenized deposit system presents an opportunity to disrupt the status quo of cross-border transfers by enabling direct, peer-to-peer value movement between individuals or companies with bank-verified identities. For instance, if two banks in different countries participate in an interoperable tokenized deposit network, a customer in the U.S. could send USBC to a recipient abroad instantly, with the recipient's local bank (or a partner entity) seamlessly converting it to local currency or, if the recipient holds an account with a U.S. bank, simply reflecting the

transfer as a ledger update. Even in the case of a single U.S. bank's system, an international remittance becomes simpler: an overseas user could onboard to receive a payment in tokenized U.S. dollars ("USD") and later cash out via an ATM or local bank partner. By removing intermediary steps, the cost of remittances and cross-border business payments can be drastically reduced, benefiting especially those sending smaller payments that currently incur disproportionate fees.

- **Hedge Against Local Currency Instability:** In regions plagued by high inflation or volatile local currencies, holding value in a stable currency like the U.S. dollar can be crucial for preserving wealth. Stablecoins have already been used this way by some [7], but tokenized deposits offer a more secure avenue. Non-U.S. persons (where permitted by regulation) could hold USBC, giving them the stability of the dollar without an exposure to a private stablecoin issuer's credit risk. Because these tokenized deposits are actual bank deposits, holders gain confidence from FDIC insurance and the bank's oversight. This use case essentially provides a digital dollar account to anyone globally who qualifies, helping people in unstable economies protect their savings by diversifying into a trusted currency.

- **24/7 Instant Payments:** USBC tokenized deposits settle in real time, around the clock. This means payments that traditionally might wait for batch Automated Clearing House ("ACH") processing or only move during banking hours can be completed instantly at any time, day or night. Businesses and individuals utilizing the USBC Tokenized Deposit Network could use this for just-in-time payments, emergency disbursements, or simply the convenience of not having to wait. For instance, an e-commerce marketplace could pay out sellers instantly after a sale (even on weekends and bank holidays), or an individual could pay a friend at 2 AM with instant settlement. Although newer real-time payment systems (e.g. RTP, FedNow in the U.S.) also aim to provide instant settlement, USBC offers interoperability with other blockchain-based services and potentially cross-border capability in one unified system. It delivers real-time gross settlement for retail payments, improving cash flow and reducing counterparty risk of pending payments.

- **Integrated and Programmable Payments:** In the future, once multi-chain asset management is implemented and support for public or semi-public chains is introduced, the tokenized deposit ledger will be able to integrate with other digital applications and support programmable money. This will allow companies to embed payment functions into their products via APIs or smart contracts without building an entire banking backend. For example, a rideshare app could use USBC to pay drivers instantly after each ride, splitting the fare between driver, company, and taxes automatically in a single transaction. Supply chain platforms could enable conditional payments triggered by delivery confirmations or internet of things ("IoT") data. These types of embedded, programmable payments become feasible when supported by a unified ledger and identity namespace, where user accounts can be mapped to human-readable identifiers (e.g. a username) instead of traditional routing and account numbers. Additionally, programmable logic could support features like escrow, subscription billing, or compliance-enforced conditions (e.g. only releasing funds when KYB credentials are verified on both sides). While these capabilities are not yet available on the current private, permissioned ledger, they are core to the USBC roadmap and will unlock powerful integrations as the platform evolves.

- **Enterprise Treasury and Settlement:** Businesses, especially those operating in digital asset markets or with global operations, can use USBC for treasury management. Instead of holding

large balances in physical accounts across numerous banks and dealing with cutoff times for wire transfers, a corporation could hold USBC and instantly move funds between internal departments, subsidiaries, or to suppliers on the network. Settlement of invoices could be accelerated, for example, a company could pay a vendor upon invoice approval, with the payment executing via smart contract that both parties' banks cosign, providing near-immediate settlement finality. Financial institutions themselves could use USBC for interbank settlement in a network.

- **Corporate Treasury, Tax, and Financial Reporting:** Multinational corporations face mounting complexity in managing liquidity, reconciling intercompany flows, and meeting increasingly stringent tax and audit obligations across jurisdictions. Traditional payment systems are reliant on wire transfers, batch netting, and FX conversions. As a result, they are slow, opaque, and poorly suited to real-time treasury operations or modern ERP integration. Stablecoins, though faster, introduce regulatory ambiguity, pseudonymity, and lack of yield, undermining their usefulness as working capital instruments. USBC addresses these challenges by functioning as a fully reserved, FDIC-insured, identity-layered digital dollar natively compatible with enterprise systems. Intercompany transfers can be executed instantly, with legal entity attribution, timestamped valuation, and built-in compliance logic for OECD Pillar Two and Country-by-Country reporting. Treasury teams can hold idle balances in interest-bearing custody, while tax and accounting teams benefit from a programmable audit trail that aligns with domestic and international accounting and reporting requirements. Whether supporting internal funding, global liquidity management, or reconciliation of intra-group flows, USBC introduces a new layer of operational efficiency and regulatory alignment that neither traditional cash nor crypto-native stablecoins can provide.

- **Cryptocurrency Traders:** Today, cryptocurrency traders rely heavily on stablecoins to move in and out of digital asset markets. However, bridging between blockchain-based assets and traditional bank accounts remains complex, expensive, and slow. On/off ramps often involve multiple intermediaries, manual withdrawals, high fees, and multi-day settlement times. Tokenized deposits like USBC offer a dramatically simplified alternative. Traders can move from digital assets directly into USBC, an FDIC-insured bank liability, without ever leaving the blockchain environment. Once in USBC, funds are immediately available as bank money, enabling same-day access to traditional financial infrastructure, including wire transfers, ACH payments, or spending via debit rails. There is no need to withdraw funds via an exchange (to "cash out") or convert to fiat currency through third-party services. This eliminates costly ramp fees, reduces counterparty risk, and streamlines post-trade fund management. For example, a trader who exits a cryptocurrency position into USBC can immediately use those funds to pay a vendor, initiate a treasury transfer, or hold them securely within a bank-regulated environment. Given that the vast majority of stablecoin volume today is driven by trading activity, capturing this use case could unlock substantial adoption by crypto-native users looking for a faster, safer way to bridge digital and traditional finance.

These use cases illustrate how USBC can permeate many aspects of finance and commerce. It's important to note that tokenized deposits do not necessarily replace existing systems overnight—rather, they augment and coexist with traditional payment rails. For end-users who need the advantages, the tokenized option becomes available, while those comfortable with legacy methods can continue as before. Over time, as trust and familiarity grow, we anticipate broader adoption. Ultimately, the utility of USBC will be determined by how seamlessly it integrates into everyday financial activities. By designing the system with

open APIs, an identity-driven directory, and support for standard token formats across different chains, we aim to make integration as straightforward as connecting to any modern fintech platform. This open approach will enable an ecosystem of innovative applications—from fintech startups building new payment solutions, to large technology companies embedding banking into their user experiences, to decentralized finance platforms that want to incorporate regulated, real-world assets. In all cases, USBC serves as a trusted digital cash layer that can integrate with various services without compromising on compliance or reliability.

CHAPTER 2 _ THE USBC TECH STACK

Technology

USBC is underpinned by a blockchain ledger that serves as the single source of truth for all tokenized deposit transactions. The current implementation runs on an Ethereum-based blockchain, augmented by the proprietary rule engine, which acts as a Layer 2 control layer. Layer 2 refers to a system built on top of the base blockchain (known as “Layer 1”) that provides additional features or controls. In this case, the Layer 2 control layer enforces mandatory compliance rules and connects directly to the banking system. This setup allows the bank to maintain regulatory oversight and operational control while still leveraging the transparency and immutability of the underlying blockchain. By leveraging Ethereum’s technology stack, including the widely-adopted ERC-20 token standard, the system benefits from mature tooling, broad developer support, and strong security infrastructure, all within a controlled environment. Support for additional blockchains is planned as part of the platform’s multi-chain roadmap. The ledger is permissioned, meaning that on USBC’s private chain, nodes are operated by USBC . On public chains, transactions occur through public nodes, but USBC’s rule engine enforces compliance and access controls. In all cases, only vetted users can hold and transfer USBC, ensuring that transactions are governed by identity, risk, and regulatory rules regardless of the underlying infrastructure. Unlike traditional blockchain networks where control is decentralized by design, the USBC model introduces a governance layer that ensures all transactions regardless of the underlying chain are subject to identity, compliance, and financial rules. Whether operating on a private or public blockchain, USBC’s rule engine enforces these controls, enabling the system to meet regulatory requirements while remaining flexible across multiple blockchain environments.

The bank’s general ledger is directly integrated with the blockchain ledger, eliminating the need for a traditional core banking system or intermediary reserve structures with respect to the tokenized deposits. When a customer’s deposit is tokenized, the total liability is recorded in the bank’s general ledger and simultaneously represented on the blockchain by issuing the equivalent number of USBC tokenized deposits to the customer’s wallet address. The general ledger serves as the centralized record of all incoming deposit liabilities, without associating them with specific customers. In contrast, the blockchain reflects individual ownership and transaction history by recording each customer’s tokenized deposit balance on-chain. In practice, the general ledger and blockchain together form a unified and auditable view of balances and activity. There is no synthetic token pool, no off-ledger reserve, and no discrepancy between systems.

While the blockchain itself is maintained by a permissioned set of node operators, the platform is designed to be openly accessible to developers. APIs and smart contract interfaces are fully exposed, allowing any external application, such as wallets, payment apps, or enterprise systems, to interact with USBC tokenized deposits. For example, a fintech app can integrate USBC functionality (e.g. displaying balances or initiating transfers) simply by calling public APIs or invoking smart contract methods. No node participation is required. The platform uses Ethereum-compatible accounts and RPC interfaces, enabling developers to work with familiar tools and infrastructure, and existing wallets with minimal adjustment. In addition to these standard interfaces, the system offers purpose-built APIs that extend functionality beyond what typical Ethereum tooling provides, supporting enterprise-grade capabilities for regulated use cases. Looking ahead, wallet applications may be encouraged or required to support multi-signature features to enhance transaction security and compliance, though this will not limit initial access. The long-term goal is to foster a robust ecosystem of decentralized applications ("dApps") built around USBC, such as programmable escrow, multi-signature treasury accounts, or cross-chain settlement bridges. The assumption being that all integrated developers or fintechs would be vetted to be in line with regulatory participation expectations.

At the heart of the ledger's compliance architecture is a rules engine that governs which transactions may proceed. Before any transaction is submitted to the blockchain, it must be reviewed and signed by this rules engine, which enforces a configurable set of policies tied to user identity level, regulatory obligations, and risk controls. For example, if a Bronze-level user attempts to initiate a transfer that exceeds their daily limit or targets a prohibited address, the rules engine will automatically reject the transaction and withhold its required signature. In the planned multi-signature model, every valid USBC transaction must include not only the user's signature but also a co-signature from the rules engine. The USBC smart contract verifies that both signatures are present and valid before processing the transfer. This ensures that all compliance checks are performed off-chain prior to submission and enforced on-chain through signature validation logic. The rulebase and metadata that drive the engine's decisions can be updated independently of the ledger, allowing compliance policies to evolve over time without modifying smart contracts or validator behavior. For example, if a new regulation requires additional information to accompany high-value transfers, that logic can be incorporated into the external engine without redeploying on-chain infrastructure. This decoupled design enables robust compliance enforcement while preserving blockchain performance, transparency, and flexibility.

Given that the platform handles real money and supports critical infrastructure, ensuring robust security is essential. The ledger benefits from Ethereum's strong cryptographic foundations. Transactions are signed using elliptic curve digital signatures, and blocks are tamper-evident. In a permissioned setup, the consensus algorithm can be optimized to achieve faster finality and higher throughput than public Ethereum, since trust is vested in a set of vetted validators. Validating nodes operate within secure, enterprise-grade environments and are not exposed directly to the internet; only RPC endpoints are externally accessible, and these are protected by DDoS mitigation layers and access controls. Key management is handled through software-based vaults such as Azure Key Vault and HashiCorp Vault, ensuring secure storage and restricted access to signing credentials. The system is designed with built-in redundancy so that if one node fails, others immediately take over to prevent downtime. Ledger state is inherently distributed across all participating nodes, ensuring that no single point of failure can compromise data integrity or continuity. From a cybersecurity standpoint, role-based access control and audit logging are enforced at every level. Each administrator action or system interaction is recorded for transparency and traceability. Smart contract logic is transparent and auditable by regulators and independent

assessors. By combining best practices from blockchain security and the bank's existing IT policies, the USBC platform is engineered to meet or exceed the security standards of traditional digital banking systems. In addition to internal safeguards, the platform's infrastructure, including its APIs, operational controls, and system architecture, will be subject to independent third-party audits. These audits are intended to confirm that the platform operates as intended, follows security and compliance best practices, and maintains the integrity of customer-facing systems. This external oversight is especially important given the platform's role in enabling programmatic access to tokenized deposits.

Early implementations of blockchain technology often faced throughput and latency limitations [1]. The USBC ledger, built on a private, permissioned blockchain network, achieves significantly improved performance over public chains while maintaining compatibility with widely adopted tooling. The platform is well-suited for a wide range of financial applications, including retail payments, without compromising decentralization or auditability. Since the ledger is intended for payments, which are relatively low-data transactions, blocks remain small and efficient. Additionally, because every user is verified, techniques like sharding or partitioning by identity groups can be explored if the user base grows significantly—for instance, multiple parallel ledgers or sidechains could be used for different regions or tiers, all interoperable via the main identity namespace and cross-ledger bridges. The USBC system is also designed with future interoperability in mind, enabling potential integration with external blockchains. Although bridging to public networks, such as allowing transfers to self-custodied wallets, remains a longer-term consideration, early evaluations of common interoperability mechanisms revealed limitations around speed and secure multi-signature support. As an alternative, the platform is exploring connector-based approaches for cross-chain asset management, with a proof of concept planned before finalizing the integration strategy. In the near term, scalability within the permissioned network is more than sufficient for anticipated volumes. Even the most widely used public stablecoins, serving global markets, typically process only tens of thousands of on-chain transactions per day. This is a level of throughput that the USBC ledger is well-positioned to match and exceed. Ongoing performance testing and architectural refinement are part of the platform's governance process to ensure long-term scalability and operational resilience.

In summary, the technology stack for USBC is a hybrid of traditional banking systems and blockchain components, carefully orchestrated to deliver the benefits of both. It uses the immutability and programmability of blockchain to provide new features like instantaneous transfers, global addressing via unique names, and smart contract-driven services. Developers and partners see a familiar blockchain environment to build upon, but one that is enriched with identity and compliance layers not found on public chains. Users experience the system through user-friendly banking apps or web interfaces that abstract away the blockchain complexity – the interface presents only a "digital dollars" account that can send or receive money instantly. Behind the scenes, every such transaction is recorded as a blockchain event on a ledger. Tokenized deposits are issued or redeemed based on real-time changes. Each on-chain transfer reflects a corresponding update in account ownership and transaction history. This fusion of technologies ensures that as the financial system continues integrating with blockchain infrastructure, banks and regulators have a platform they can audit, govern, and trust, future-proofing the bank's role within a blockchain-enabled financial ecosystem while maintaining full regulatory alignment.

Trust & Identity Management

Trust is the cornerstone of USBC, and establishing trust begins with robust identity management. Unlike permissionless cryptocurrency systems where anyone can create an address and transact, this platform requires users to identify themselves and build a verified digital identity before they can access or transfer USBC. The identity framework has several key components:

Each participant in the system—whether an individual or an organization – is required to create a unique identifier (or name) within the platform's identity namespace. This works similarly to choosing a username or handle, but with the important rule that no two users can have the same name. The namespace is effectively a directory of all authorized users. For example, a user might register the name alice.smith or a business might register ABC_Corp. This human-readable name is linked to the user's blockchain address and, where applicable, may also reference traditional banking identifiers such as a routing number or account number. It serves as a user-friendly alias for facilitating payments, similar in function to how a domain name simplifies access to an IP address. While the system's namespace can operate like Domain Name System ("DNS") in certain implementations, its structure is flexible and can support purely blockchain-based identifiers without relying on traditional banking details.

By having a unique name for each user, the system avoids the confusion and risk of sending funds to the wrong cryptographic address; transactions can be addressed to alice.smith which the system knows corresponds to that user's current tokenized deposit ledger address. The namespace is maintained by the bank as an authoritative registry of who is who on the network. This not only improves usability but also inherently ties every account to an identity record, reinforcing that there are no anonymous accounts.

To register a name and open a USBC account, a user must go through an onboarding process that collects identity information and credentials. The platform supports a credential-based identity verification approach, meaning users provide verifiable credentials (e.g. information, documents or attestations) that prove aspects of their identity (e.g. phone number, email, geolocation, a government ID number, selfie and photo ID match, etc.). These credentials can be issued or validated by trusted third parties—for instance, an integrated KYC service might verify a driver's license and mark that credential as verified for the user. The system is designed so that credentials are user-controlled and privacy-protected: rather than the bank sharing the actual documents, it may store a hash or confirmation that the credential was verified. Users can accumulate multiple credentials in their profile, which together form a rich picture of their identity and reputation on the platform. The philosophy is that identity is not a one-time check but an ongoing, progressive process.

The model enables three primary identity trust levels for users: Bronze, Silver, and Gold, to categorize users based on the strength of their verified identity. These levels reflect how much information a user has provided and how confident the system can be in their identity. However, identity trust level alone does not determine financial access. Instead, the platform uses a combined framework: a user's identity trust level plus their risk level (e.g., low, medium, high, very high). Before any risk level is assigned, users are subject to extensive fraud and risk checks, including phone trust score, email trust score, geolocation confidence scoring, sanctions screening (based on name and geography), PEP screening, negative news screening, and other contextual risk signals. Identity trust level and risk level together determine what financial access

tier (e.g. Base Tier, Tier 1, Tier 2, etc.) they are assigned. Silver and Gold are the equivalent of the minimum requirement for regular checking accounts with CPI compliance level of onboarding, while Bronze is a contemplated future product construct equivalent to an account type that does not require full CPI compliance.

- **Bronze Level:** This is the entry-level identity trust level, requiring only self-reported information with basic verification. The goal is to keep barriers lower so that nearly anyone can begin interacting with the platform in a limited, but compliant way. Bronze-level users are permitted to open USBC Digital Wallet accounts and access limited platform functionality, subject to strict transaction caps that reflect the lower level of identity assurance.

- **Silver Level:** Silver represents a high identity trust level, generally aligned with the verification requirements of traditional bank onboarding. To reach this level, users must provide government-issued identification, a selfie match, and potentially additional supporting information. A Silver identity trust level indicates that the bank has a stronger degree of confidence in the user's verified identity—but this alone does not determine financial access. A user's actual permissions are governed by their assigned Financial Access Tier, which is based on the combination of identity trust level and risk rating. A Silver user with a Low or Medium risk rating may qualify for broader access, while a higher-risk Silver user may remain in a more restricted access tier. Financial flexibility is unlocked only when both identity and risk thresholds are met.

- **Gold Level:** Gold represents the even stronger identity trust level. At this level, the user is able to demonstrate that they already maintain an account with another regulated financial institution and have successfully completed that institution's KYC process. Gold-level users are generally eligible for the significantly higher levels of financial access, but again, this depends on the accompanying risk profile. A user with a Gold identity trust level and a Low risk rating may be assigned to a top Financial Access Tier with broad permissions, while a user with a similarly strong identity profile but a High or Very High risk rating may be restricted to a lower access tier with limited functionality. Each user's actual financial permissions, including maximum balance, transaction limits, and available features, are determined by the combination of their identity, trust level and risk rating, not by either factor alone. This layered model supports a risk-based approach consistent with global regulatory guidance, such as FATF's progressive Customer Due Diligence framework [13]. It also enables broader access to financial services for individuals with limited documentation or thin credit files, while maintaining strong safeguards against illicit activity.

One of the strengths of this progressive model is that a user's status is not static. Users are expected to advance through identity trust levels over time as they provide additional verified information. For example, an individual who initially onboards at the Bronze identity trust level, may later qualify for Silver by submitting a government issued identification. Over time, they could also reach Gold if they demonstrate a strong, verifiable presence within the formal financial system. Throughout this process, users retain control over their verified credentials. These credentials are not publicly exposed, and users can choose whether and when to share specific information with counterparties or services. As a user's identity trust level increases, their Financial Access Tier may also be reassessed, depending on their risk rating, which can enable access to additional features or higher transaction limits.

The platform employs a credential wallet or vault for each user. This secure vault stores verifiable credentials and personal data in encrypted form. The user, via their preferred application, can see which credentials they have provided (e.g., “Email verified”, “Phone verified”, “Passport verified by KYC provider X on 2025-01-10”, etc.). Over time, additional metadata (e.g. “trusted transaction history”, reputation scores) could be added—for instance, if the user has been active for a year with no suspicious flags, that could serve as a credential improving their standing. The system might also collect device identity and behavioral patterns, which augment identity indirectly. All this information builds a multi-dimensional identity profile that far exceeds the static snapshot of onboarding documents. It creates trust through context—when alice.smith sends a payment, the system knows she is a Gold identity trust level with a verified U.S. ID, has been a customer for two years, usually transacts domestically, etc. This makes unusual activity easier to spot and fosters trust among participants that bad actors are unlikely to go unnoticed.

Beyond compliance, the identity system plays a practical role in payment routing and user experience. Since every user has a unique name and is verified, the platform can offer a global “address book,”while preserving privacy. A user can search for a payee by name or alias—for example, a freelance worker could find the profile of a company to request payment, or a person could confirm their friend’s identifier before sending money. The directory might show minimal public info but no sensitive PII unless explicitly shared. This is similar to how one might find a contact by username in a messaging app. It simplifies the payment experience by allowing users to send funds using a recognizable, human-readable handle rather than requesting routing numbers, blockchain addresses, or other technical identifiers. This creates a user experience that is intuitive and familiar, helping to fulfill one of the core promises of digital currency: improving on the complexity of legacy payment systems. Over time, this directory model could also enable interoperability across financial institutions by providing a consistent identity layer that supports cross-bank transactions without added friction. This would function similarly to how email providers use the DNS system to discover recipient mail servers through Mail Exchange (“MX”) records, enabling seamless communication across different domains.

Selective disclosure is an optional feature of certain cryptographic methods used to exchange verifiable credentials. When supported by client applications or identity providers integrated with the USBC system, users can selectively prove specific attributes without revealing the full underlying data. For example, using techniques such as zero-knowledge proofs (“ZKPs”) or tokenized credentials, a user like Alice could demonstrate “I am verified at the Gold identity trust level” or “I am over 18 and a U.S. resident” without disclosing her exact birthdate, address, or original documents. These capabilities align with emerging decentralized identity standards and can be implemented in a centralized but user-consented framework. While selective disclosure is not inherent to all credential sharing, it can enhance privacy when used. The USBC platform itself does not natively implement these features, but compatible third-party providers may offer them. In all cases, the bank retains the complete verified identity information for regulatory purposes, while end users can manage how much is shared in day-to-day interactions.

The trust and identity management layer of the USBC system transforms what could have been an anonymous network into a web of trust where every account is anchored to a real-world identity that has been vetted to some degree. This significantly deters malicious actors—a bad actor cannot simply spin up hundreds of fraudulent accounts without providing verifiable credentials, and even if they attempted to use stolen identities, the multi-factor and ongoing monitoring would likely catch inconsistencies. Meanwhile, honest users benefit from a reputation-backed system: if a user has built up a Gold-level identity, others

can trust that interacting with you is lower risk, much as they trust a reputable bank or a long-established merchant. By combining blockchain technology with an identity framework inspired by digital identity best practices (e.g. the FATF guidance on digital ID, NIST digital identity standards), this model provides a foundation for a safe expansion of financial services. It assures regulators that despite the new form factor, the fundamental principle of "no anonymous value transfer" is preserved—every USBC tokenized deposit can be traced to a responsible owner when needed. It also assures users that who they transact with is known, reducing chances of fraud. Trust, therefore, is embedded into the core design of the ledger, which is a distinguishing factor setting USBC apart from generic digital currencies.

Privacy

A critical design goal of USBC is to protect user privacy while still enforcing the necessary transparency for compliance. The solution lies in data segmentation and controlled disclosure: ensuring that personal identity information is kept separate from transaction records on a public level, and giving users control over who sees their sensitive data. Only authorized participants—such as the issuing bank and designated counterparties like auditors or regulated financial institutions—have access to the full contents of the ledger. External parties and general observers cannot query the blockchain to view transaction flows. Even within the network, regular users can only view their own account activity and limited details related to transactions they are directly involved in; they cannot arbitrarily inspect other users' payments. This architecture ensures that personal financial data is protected from data miners, competitors, or malicious actors. Although today's design prioritizes privacy and regulatory oversight, the framework is built to support future interoperability with public or hybrid blockchain environments as policy, technology, and compliance standards evolve.

On the blockchain ledger itself, users are represented by their blockchain addresses or identifiers, not by their real names or PII. So, when the ledger records that 0xABC123... sent $500 to 0xDEF456..., the underlying system knows this corresponds to, say, Alice Smith paying Bob Jones, but those names are not recorded in the transaction record—only the pseudonymous addresses and the associated namespace aliases, which could even be hashed or obscured on-chain, are recorded. This approach is similar to how bank account numbers work: internal bank systems map an account number to a customer profile with PII, but statements and interbank messages use account numbers, not full identities, except where legally required. The difference here is that the mapping from pseudonymous address to identity is held by the bank in a secure KYC database (off-chain or in a permissioned identity contract), and not visible to other users by default. In effect, on-chain data might show "AliceName paid BobName $500" if those names are used, but those names themselves could be aliases. If greater secrecy is needed, even the human-readable names might be omitted from the transaction payload, leaving only internal IDs and cryptographic proofs.

Personal data provided by users (addresses, DOB, documents, etc.) is stored in secure systems and not on the blockchain in plain text. The blockchain might contain references or hashes of credentials (to prove that a verification was done), but not the actual documents. For example, when Alice's driver's license is verified, the system might store a hash of "License#12345 verified by KYCProvider on date" either off-chain associated with Alice's profile or on-chain in an encrypted credential contract accessible only to Alice and the bank. If it's on-chain, it would be encrypted such that only those with permission (like the bank or Alice)

can decrypt it. The idea is to minimize the exposure of PII. The bank's internal systems, which are subject to GLBA and other privacy laws, keep the raw PII safe, similarly to how traditional banks secure customer data.

The platform embraces principles of open banking and customer data rights, including those outlined in Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"), which gives consumers the right to access and share their financial data [14]. It also aligns with global privacy standards, such as the General Data Protection Regulation ("GDPR"), which require that users be informed about who is accessing their data and for what purpose [12].

In practice, this means users can authorize third parties to access their account information or initiate payments on their behalf, without the bank disclosing credentials or data without consent. For example, Alice might use a budgeting app that needs to view her transaction history. She can grant that app permission to retrieve her data securely—similar to how she might interact with current open banking APIs. In the USBC context, Alice could also choose to authorize a third-party smart contract with limited access to her wallet address or transaction metadata. All such access is explicitly opt-in. The bank will not share Alice's data or enable third-party access unless she provides consent or there is a valid legal mandate. This approach reflects modern privacy expectations and ensures that users retain full control over who sees their personal and financial information, and under what terms.

Consider a payment scenario: Alice pays Bob. One might ask what Bob learns about Alice in this case. In traditional banks, if Alice wires Bob money, Bob will see some details (her name on his statement). If Alice writes Bob a check, he sees her name and possibly address. The USBC system can give more privacy than those traditional methods, while still satisfying necessary requirements. Bob might see that a payment came from "AliceSmith#123" (Alice's namespace handle) with maybe a reference note. If Alice and Bob are strangers, Bob does not automatically receive Alice's contact information or personal details – just as if it were a cash payment, he might only know what Alice chose to tell him. On the other hand, if Bob requires proof of certain things (e.g. if Bob is a merchant who needs to record customer info for regulatory reasons), the system can facilitate that with Alice's consent. Alice could approve sharing her full name and shipping address as part of the payment (as e-commerce platforms do). The system could have an invoice feature where Bob requests specific info and Alice agrees to provide it. By not automatically exposing everything, the system adheres to a principle of least disclosure—only revealing what is necessary for the transaction or what the user agrees to. This also has security benefits: if one user's account is compromised, the attacker cannot scrape a global list of others' personal info from the blockchain, because that information is not present.

Privacy in a regulated financial system has limits: the bank must be able to provide information to regulators, law enforcement, or other banks as required by law. The system is designed to facilitate such lawful access when needed. Because every tokenized deposit ledger address is linked to a verified identity in the bank's records, if suspicious activity is detected or a court order is received, the bank could retrieve the PII of the involved addresses and share it with authorized authorities just as they would with any bank account. This is a crucial point: privacy for users does not equal opacity to regulators. The bank remains capable of tracing and reporting transactions. What the design avoids is unnecessary exposure of data, especially to unauthorized parties. So, from a regulator's viewpoint, the system can actually be more transparent than cash or some bank transactions, because the bank's digital ledger is very detailed and readily queryable internally—every movement is recorded and tied to an identity, easing audits and

compliance.

The platform can employ advanced cryptographic techniques for additional privacy where suitable. For instance, ZKPs could be used in future iterations to allow validation of certain conditions without revealing underlying data. A practical example illustrates this: Alice needs to prove to a decentralized application that she has a Gold level status (or is over 21 for a certain transaction) without revealing her name or ID documents. A ZKP could be generated by the bank's system to attest "Alice's account meets X criteria" which Alice can present, and the verifier can confirm true or false without seeing any other details. Another use might be proving that total tokenized deposits outstanding equal total deposits on the bank's general ledger (for public trust reasons) without revealing individual account holdings—a ZKP or cryptographic accumulator could demonstrate that the sums match. These techniques are emerging, and while not necessary for initial deployment, incorporating them could further enhance privacy and trust over time, especially if aspects of the system become more decentralized or involve external validators.

The bank will make its privacy policies transparent to users. Customers will be clearly informed about what data is collected, how it is used, and how their transactional privacy is protected from public exposure. Within the app, users will have access to privacy settings that allow them to control their visibility in directory searches, determine what information is shared when someone views their profile, and manage consents granted to third parties. These controls are designed to give users meaningful control over their data footprint.

If a user chooses to leave the platform, the bank will retain their personal data as required by applicable laws and regulations (for example, KYC records must typically be retained for five years after an account is closed). The user's name would be deactivated in the namespace, and any previously authorized third-party access would be revoked. However, any on-chain transactional data that was recorded during the user's activity are permanent and will remain visible on the ledger, as blockchain entries cannot be deleted. This data does not include personally identifiable information but may reflect historical transaction flows. While the bank maintains full off-chain records and internal mappings as required for compliance, users can be confident that they are not permanently exposing their personal data to third parties by joining the system and may disconnect authorized access at any time.

In summary, the USBC model strives to balance transparency and privacy. While financial activity is recorded on-chain and viewable by anyone, these transactions are tied to wallet addresses, not real-world identities. Personal details are never stored on-chain, and other users cannot determine who owns a given wallet address unless the user has chosen to associate their real name with it through a public namespace. This design ensures transparency for auditing and oversight, while preserving user privacy unless the user explicitly links their identity. It offers improvements over conventional crypto by eliminating public traceability, and it can even improve on some traditional bank privacy aspects by giving users direct control over data sharing, whereas traditionally a lot of that happens behind the scenes with credit bureaus, etc. This user-centric privacy approach is not merely an optional feature; it is crucial for adoption. People and businesses are more likely to use a new financial network if they trust that their sensitive information is safe and that transactions remain confidential except to those they choose to involve. By building privacy into the design, the USBC system aims to meet regulatory requirements without becoming a surveillance tool beyond what banking already necessitates, thereby respecting individual privacy rights and expectations in the digital age.

How Deposits Become USBC

In a traditional stablecoin model, issuance and redemption typically involve exchanging fiat for on-chain tokens held against an off-chain reserve, and destroying those tokens when users cash out. In the USBC model, tokenized deposits represent a seamless fusion of traditional banking infrastructure and blockchain technology. The Bank's general ledger acts as the recording layer for all on-chain tokenized deposits. Meanwhile, the USBC blockchain serves as the ledger for ownership, transaction history, and real-time balance management.

When a user deposits fiat funds in the bank, the liability is registered on-chain by issuing the amount of tokenized deposits to the user's wallet and money is credited to the depository institution's general ledger. Conversely, withdrawals trigger a cancellation of on-chain tokenized deposits and a debit from the general ledger. This eliminates the need for a core banking system and for individual shadow accounts while maintaining full auditability; both the blockchain and the general ledger provide reconciliation reports, ensuring transparency for regulators and auditors.

The process can be broken down as follows:

When a customer brings U.S. dollars to the bank, via ACH, wire or other supported rails, and those funds are credited to their Digital Wallet account, that event triggers the issuance of USBC. For customers onboarded to the USBC system, this process involves issuing USBC to their Digital Wallet account in direct synchronization with the corresponding credit to the bank's general ledger that tracks fiat. Suppose Alice deposits $1,000 into her USBC-enabled account. The bank credits $1,000 to the general ledger and simultaneously issues 1,000 USBC to Alice's blockchain address, which is tied to her verified identity.

There is no separate account structure or omnibus FBO ledger. USBC tokenized deposits reflect real, on-balance-sheet liabilities recorded in the general ledger. If Alice already holds funds elsewhere in the bank and opts into the tokenized system, the bank can reassign those funds to her USBC wallet by debiting her conventional balance, updating the general ledger, and issuing the appropriate amount of

USBC.

From the user's perspective, this transition is seamless: their wallet reflects their tokenized balance, which is fully reconciled with the general ledger. Importantly, users cannot double-spend across systems. Holding 1,000 USBC in a wallet means that $1,000 has already been accounted for in tokenized form. It cannot simultaneously be spent via another deposit account.

Users do not buy USBC from the bank. There is no premium, speculative market, or third-party issuance involved. USBC is not a separate asset, it is simply the on-chain representation of a known customer's bank deposit. Finally, USBC can only be held by fully onboarded, KYC-verified customers. Unlike public stablecoins that can be acquired pseudonymously, every tokenized deposit ledger address is tied to a verified identity, ensuring compliance from the point of issuance.

Below is an outline of the basic user lifecycle:

- **Deposit:** When a user funds their account, the deposit is recorded in the bank's general ledger. If enrolled in the tokenized platform, an equivalent amount of USBC is issued to the user's verified Digital Wallet address. This on-chain tokenized deposit reflects the same FDIC-insured liability recorded in the bank's systems.

- **Hold:** Users can hold their funds in USBC within their Digital Wallet account. These balances are fully insured up to applicable FDIC limits, and if the deposit product is interest-bearing may earn interest just like any other demand deposit. This stands in contrast to most stablecoins, which are unlikely to accrue interest payable to the stablecoin holder. Holding USBC is operationally equivalent to holding a checking or savings balance; the key difference is that the user's balance is also reflected on a blockchain ledger, enabling programmability and real-time transparency. Balances update instantly as transactions occur and can be viewed anytime through the bank's user interface.

- **Send (Transfer to Others):** Users can send USBC to other participants in the USBC ecosystem instantly. For example, when Alice sends 100 USBC to Bob, the external rules engine pre-approves the transaction based on identity level, compliance status, and risk policy. If approved, the blockchain ledger reflects the transfer by debiting 100 USBC from Alice's wallet and crediting 100 USBC to Bob's. From the general ledger's perspective, this is a movement of a $100 liability from one user's deposit account to another's, there is no external funds movement. The overall USBC supply remains unchanged; only the ownership of the underlying deposit has shifted. Users experience this like any peer-to-peer transfer: Alice selects Bob from her contact list and taps "Send." The transaction settles within seconds.

- **Receive:** To receive USBC, a user must have an active, verified account and share their wallet identifier with the sender. Once the transaction is approved and processed, the recipient's USBC balance updates in real time, and the corresponding general ledger entry reflects the new ownership of the deposit. There is no need to "claim" or "redeem" the funds. They are already fully integrated into the recipient's account. USBC held in the wallet is not a pending or speculative

balance; it is a live, FDIC-insured deposit in tokenized deposit form, ready to be used for additional transfers or withdrawal through traditional rails.

- **Withdraw:** If a user wants to withdraw funds from their USBC wallet to make an external payment or cash out, they initiate a redemption. For example, if Alice has 200 USBC and wants to pay her rent via ACH, she simply requests a withdrawal. The bank burns the 200 USBC from Alice's wallet and debits the same amount from the general ledger, initiating either (a) a credit to Alice's traditional deposit interface for ACH processing, or (b) a direct outbound payment to her landlord via ACH or wire. The total supply of USBC decreases by the amount redeemed, and the funds are no longer represented on the blockchain. This process is seamless to the user but ensures full traceability, regulatory compliance, and balance integrity across both the general ledger and the blockchain.

This seamless interoperability between USBC balances and traditional banking channels means users are not locked in to the new system. They can always convert back to regular money in their hand or in another bank. It eliminates the liquidity concerns often associated with stablecoins, where users might worry if they can redeem their tokenized deposits for real USD in a pinch. Here, redemption is just a standard banking service.

This raises the question of how a bank operating on fractional reserves guarantees redemption of USBC. The answer: exactly as banks always do—through liquidity management, not by having a one-to-one reserve for each tokenized deposit. The issuing institution treats tokenized deposits like any demand deposit: it keeps enough cash and reserves on hand to meet withdrawal demands under normal and stress conditions, and beyond that, it may invest or lend out the deposits. In practical terms, if many tokenized deposit holders suddenly withdrew to external accounts, the bank might have to use its cash or borrow from the Fed, but that is a normal banking function. The key is that redemption does not depend on selling off some reserve fund, as stablecoin issuers must do; it's backed by the depository institution's full balance sheet and access to central bank liquidity, which is a far stronger guarantee.

In the stablecoin world, large redemptions often involve sending tokens back to the issuer who then wires money out, or users selling on exchanges to someone who wants in. Here, there is no need for a secondary trading market for USBC because USBC is by definition a dollar at the issuing bank. If someone wants to acquire USBC, they can simply deposit dollars or have someone pay them. If someone does not want their USBC, they can simply withdraw or have someone with a regular account paid. The parity is built-in; USBC doesn't float in value against USD—they represent USD in a specific bank. This eliminates scenarios of USBC trading below par, which can happen with stablecoins if confidence wavers. One USBC equals one U.S. dollar in a U.S. federally insured bank account, always.

Reserve Management

One of the most fundamental differences between a stablecoin and USBC is how the backing funds (or "reserves") are managed and how that interacts with the broader financial system. Stablecoins are typically fully reserved: for every token issued, there is an equivalent value of cash or cash-like assets held in reserve by the issuer, often in a trust or custodial arrangement. These reserves might be held in the form of

bank deposits or money market instruments such as U.S. Treasury bills, repurchase agreements, commercial paper, certificates of deposit, and short-term agency securities. The stablecoin issuer does not lend out or invest those reserves in illiquid or risky assets; they are kept to ensure redemption at par. This model resembles money market funds or the historical gold standard—it creates a one-to-one backing but at the cost of removing that money from the traditional credit ecosystem; it just sits in a vault or short-term assets.

In contrast, USBC is part of the fractional reserve banking system. When a customer deposits $100 in a bank, the bank is typically required to hold only a fraction of that as reserves, either as vault cash or on deposit with the central bank—say 10%—and can use the rest to make loans or purchase other assets. The bank's obligation is to always be able to meet withdrawals by managing liquidity and capital, not by backing every dollar with cash at all times. This fundamental difference has several implications:

- **Economic Impact and Money Supply:** Stablecoins that are fully reserved do not multiply money; $1 in creates 1 token and that $1 sits idle or in very safe assets. USBC, as bank money, contributes to the normal money multiplier effect in the economy—banks take deposits and extend credit, which in turn creates more deposits, etc. From a monetary policy perspective, USBC behaves like any demand deposit. They are part of the M1/M2 money supply measures. If USBC grows significantly, it is essentially the same as deposits growing, which central banks understand and can manage via existing tools like reserve requirements or interest on reserves. In contrast, if stablecoins outside banks grow, they could circumvent some traditional controls and potentially contribute to an inelastic money supply scenario or create parallel flows that are harder for central banks to influence. In simpler terms, USBC ensures that innovations in payments do not come at the cost of siphoning money out of the regulated banking sector. Funds in tokenized form still fuel lending and investment. This alignment means the model is complementary to economic growth and credit provision.

- **Interest for Holders:** Since USBC consists of actual deposits, banks can pay interest on them just as they might on a typical interest-bearing checking or savings account. Stablecoins, as noted, generally do not pay interest directly to holders—any yield from reserves goes to the issuer, or to maintain the peg. In fact, regulators have suggested prohibiting interest on stablecoins to prevent them from out-competing deposits and possibly to avoid them becoming investment products. In our model, holders of USBC can earn interest, making it more attractive to keep funds in this form long-term. This could be structured as a baseline interest rate for all USBC balances, or tiered by user type, or even as rewards.

- **Run Risk and Liquidity:** A concern with stablecoins is that if users lose confidence, they might all rush to redeem, and even a fully reserved issuer can face operational challenges meeting redemption requests quickly. This is a run dynamic. Banks are familiar with run risk too—that's why deposit insurance was created and central bank lender-of-last-resort facilities implemented to reassure depositors. USBC benefits from these protections. If panic occurs, the FDIC insurance up to $250,000 means small users are assured safety, and the Federal Reserve's discount window or other facilities stand behind the bank for liquidity if needed. Additionally, because not all data is public, there may be less spark for a panic based on watching on-chain movements. For stablecoins, anyone can see large outflows on the blockchain and potentially panic, whereas in a private network that information is not public; communications about stress would come through

official channels. This opaqueness to the public can actually mitigate herd behavior, while regulators still retain insight through supervision.

- **Asset-Liability Management:** The bank will manage USBC within its broader asset-liability management ("ALM") framework. One nuance: this relates to liquidity risk, not because USBC is a volatile asset, but because it enables 24/7 access to funds. This increases the speed at which deposits could be withdrawn in the event of a run. However, since the underlying deposits supporting USBC are demand deposits, the bank likely already assumes they could be withdrawn anytime. The difference is that outflows are no longer limited to business hours. The bank might hold a bit more liquidity to cover weekend or nighttime outflows, or set up access to facilities such as the Federal Reserve's 24x7 liquidity program or other contingent funding lines. Over time, withdrawal patterns will become more predictable, allowing the bank to forecast needs and maintain appropriate liquidity buffers. It is worth noting that in stable, normal conditions, USBC balances might actually remain with the bank longer than traditional deposits for some users, because they have more utility.

- **Transparency and Reporting:** Regulators will likely require transparency on how USBC liabilities are growing and how they're backed. The bank will report USBC totals as part of its overall deposit base on balance sheets. Internally, it can segment them to monitor usage. There may also be public transparency provided—e.g., the bank could publish periodic attestation of the total USBC and confirm they equal a subset of total deposits on books, maybe even providing high-level breakdown of the asset reserves against them. The bank's existing regulatory filings could incorporate USBC under the appropriate category. This gives regulators full transparency and assures the public that no off-balance-sheet risks or undisclosed exposures exist.

In sum, reserve management for USBC follows the longstanding practices of regulated banking. The public and users can be confident that each tokenized deposit is backed by the full faith and credit of a regulated bank, plus insurance safety nets—not just a pool of assets sitting in an account. This fosters stability: even in extreme scenarios like a financial crisis, measures like deposit insurance and central bank support would directly protect tokenized deposit holders, whereas stablecoin holders might be in uncharted territory if, say, markets for their backing assets froze. Additionally, by keeping funds within banks, USBC ensures that innovations do not inadvertently hollow out the banking sector. This is a noted concern among regulators. This model demonstrates how to innovate through banks rather than around them, aligning incentives. Banks get to maintain deposit bases, even grow them if they attract new customers via this technology offering, and the economy benefits from those deposits being used productively.

Finally, it is worth noting an optional approach: banks could choose to hold a higher liquidity buffer specifically against USBC if they observe these balances are more volatile. That is a business decision—some might initially treat USBC with caution and keep, say, 50% in cash for them until patterns stabilize. Over time, as confidence builds, they might normalize ALM for these like any deposits. This conservative initial approach could be communicated to regulators to show prudence. But eventually, USBC management should blend into general balance sheet management, making the distinction mostly about technology, not fundamentally different financial treatment.

Circulation

Circulation refers to how USBC flows within the ecosystem, how widely they can be used, and what mechanisms exist for moving them between different environments. The model is deliberately more restrictive than an open cryptocurrency in order to maintain compliance, but is designed to expand reach through potential cross-platform interoperability.

Initially, USBC circulates only among customers of the issuing bank. If Bank ABC issues USBC, then any sender or receiver must be an onboarded user of Bank ABC's platform. This means that if Alice is a customer of Bank ABC and Bob is not, Alice cannot directly send Bob USBC unless Bob also joins. This closed user group ensures that all USBC holders are known and KYC'd by the bank. Although it limits reach at first, it still covers a potentially large user base if the bank has many customers. Additionally, Bank ABC could open its network to certain trusted partners without them being full retail customers—for instance, perhaps merchants or fintechs can receive USBC via a custodial arrangement even if they do not have a traditional account, by doing a lightweight onboarding for the USBC platform. In all cases, the guiding rule is no unknown wallets on the ledger.

Transfers are peer-to-peer among allowed participants. The circulation is tracked on the blockchain ledger in real time. Unlike traditional bank ledgers where an internal transfer might just be a database entry, here it is a blockchain transaction, which is secure and final. The speed of circulation is essentially instantaneous settlement. If a million users are on the platform, they can all send funds to each other 24/7 with immediate finality. This creates a network effect: the more users or businesses join, the more useful the tokenized deposit becomes, similar to how email became more valuable as more people adopted it.

Although tokenized deposits circulate primarily on their native ledger, they are not isolated from the broader financial system because any user can convert to traditional payments when needed. If Alice needs to pay someone who's not on the network, she can redeem and do an ACH or wire. Likewise, if someone outside wants to pay Alice, they can still send a normal transfer to her bank which then tokenizes on receipt if Alice wants. This means USBC co-circulate with non-tokenized deposits in the economy. Money can flow in and out of the USBC ledger seamlessly through the bank's integration.

Even within the network, the bank has ultimate control to freeze or seize USBC in line with regulations, like how banks can freeze accounts or comply with court orders. Smart contracts could include freeze functions tied to the bank's authority. These would be rarely used, only for legal and compliance matters, but are a necessary backstop. This is another way circulation is controlled as opposed to open cryptocurrency—there is governance control to intervene when required by law or security.

As mentioned, based on identity levels, the circulation for certain users will be throttled. This ensures that even though USBC can technically hop around instantly, a malicious user cannot rapidly circulate huge sums through many accounts without hitting compliance checkpoints. This functions analogously as circuit breakers in the system to manage risk.

Within the bank, every movement is recorded. The bank has the ability to analyze how USBC circulates (e.g. patterns of payments, velocity, network graph of transfers). This can feed into risk scoring. But externally, as previously emphasized, this is not visible, preserving privacy to others.

Circulation also covers usage in commerce or other services. For example, consider a retail scenario. If the merchant has an account, yes. If not, perhaps via a card link—e.g. the bank could issue a debit card that draws from the USBC account, converting on the fly to a card network transaction. Conversely, an online platform could integrate the bank's API to accept USBC for checkout. These expansions effectively make USBC a payment method in various contexts, expanding their circulation beyond just P2P.

In summary, circulation of USBC starts controlled and bank-internal but is poised to widen through partnerships with approved entities such as merchants, fintechs, or platform integrations. Circulation management ensures that USBC flows freely for legitimate use while remaining fully within the bank's regulated perimeter. This approach maintains a careful balance of openness and control: access is available to verified participants who meet the bank's compliance standards, while remaining closed to unknown or unverified parties. As adoption grows, the network may expand through additional use cases and trusted integrations, without compromising regulatory oversight or identity assurance.

The ethos is similar to how the internet grew: at first, intranets (i.e. closed networks) provided value, then they interconnected to form the internet with standard protocols. USBC could circulate as easily as email, but with verified senders and recipients at each node.

CHAPTER 4 _ RISK MANAGEMENT AND GOVERNANCE

Risk Management

As repeatedly emphasized, the identity-first design is the primary mitigant against illicit finance risk. Every user is verified, and every transaction is linked to a known identity. This means that Bank Secrecy Act ("BSA") compliance is embedded into the system, the bank knows who is transacting and can monitor activity patterns. The platform employs automated transaction monitoring systems similar to those used for bank accounts, but even more granular since all transactions are digital and in real-time. Suspicious patterns will trigger alerts. The depository institution's compliance team can then investigate and, if needed, freeze accounts or block transactions pending review. Sanctions screening is integrated at the transaction level; for instance, if a tokenized deposit ledger address is found to be associated, or if a name matches, with a sanctioned individual/entity, the system will prevent USBC from being sent to or from that tokenized deposit ledger address and flag it. Since transactions require a degree of bank validation, the bank can essentially stop prohibited transactions before they go through, rather than just reporting them later. This is a powerful advantage over open systems and is analogous to the bank being able to intercept a wire transfer in transit if it saw an issue.

Moreover, the bank retains logs and has the ability to generate Suspicious Activity Reports ("SARs") to regulators if any activity looks like money laundering, fraud, or other criminal use. Due to the fact that USBC transfers are internal, the bank arguably has better oversight than in normal banking, where cash withdrawals or external crypto movements could obscure flow. Here, if Alice tried to use the USBC system to launder money by obfuscating the source of illegally derived funds through sending to many accounts, all those accounts are within one view and can be traced, unlike if she sent money out to external banks. So ironically, while a layperson might think tokenized deposits increase risk, within this framework they actually enhance traceability for law enforcement, since all transactions are recorded immutably and tied to

identity.

In traditional banking, fraud like account takeovers, phishing, scams, is a big risk. In the USBC system, because transactions are irreversible on the ledger, protecting users from fraudulent losses is critical. The bank implements strong user authentication so it is difficult for a fraudster to commandeer someone's account. If despite these measures a user is scammed into sending money, the bank has policies similar to how they handle fraud in other channels: for outright unauthorized transactions, the bank would make the customer whole under Regulation E or its own guarantee and pursue the investigation; the advantage here is if the funds are still on the ledger and went to another account, the bank can potentially freeze/recover them, which is easier than recovering a wire. For authorized-but-scammed customers, banks traditionally have limited liability, but as a matter of trust, the bank could choose to implement certain consumer protection rules even on this platform Since identity is known, if Alice is scammed by Bob into sending money, the bank can approach Bob directly and law enforcement can take action – this deters many would-be fraudsters because they cannot hide behind anonymity.

Governance

Effective governance is critical to the long-term success and integrity of the USBC system. Governance spans the technical, operational, and policy dimensions of the platform, ensuring that it remains secure, compliant with regulations, and aligned with the interests of all stakeholders. The governance structure and principles are as follows:

- **Operational Governance (Internal):** The issuing bank maintains ultimate control and responsibility for the USBC platform. Its duties include reviewing performance and risk reports, approving system upgrades or rule changes, and ensuring adequate resources for the platform. All major decisions are documented and auditable, providing a clear governance trail. Day-to-day operations—such as customer onboarding approvals, identity verification, and transaction monitoring escalations—are handled by designated operational teams within the bank, following the policies set by the governance committee.

- **Technical Governance and Upgrades:** The USBC ledger runs on software that is expected to evolve over time. To manage changes, a governance process for software updates is in place. This process mirrors best practices from enterprise IT and blockchain governance. For instance, any code change is first tested in a sandbox environment, undergoes security audit, and then is proposed to the governance committee. Only upon formal approval can it be deployed to production. Certain critical smart contracts may have upgradeable proxies controlled by a multi-signature key held by trusted executives or a governance contract. This means updates can be applied when authorized by, say, 3-of-5 key holders representing different departments, preventing unilateral action. In emergency situations, an expedited governance path allows for swift patching, but even then a post-change review is required. The guiding principle is safeguarded agility—the platform can improve and respond to new requirements, but always under strict oversight.

- **Regulatory Oversight and Compliance Governance:** Regulators (e.g. the OCC) maintain oversight

of the bank's activities, including the USBC program. From a governance perspective, the bank has committed to transparency with regulators. Regulators are kept informed about the platform's design, major updates, and risk metrics. The bank may provide regulators with regular reports specific to tokenized deposits—for example, total tokenized deposit balances, number of active users, any significant compliance incidents, and how they were resolved. By treating regulators as key stakeholders in governance, the bank builds trust and ensures that the platform's evolution remains within acceptable bounds.

- **Accountability and Transparency:** Good governance requires accountability. The issuing institution commits to clear and transparent rules for the USBC program. Customers will be informed of the terms and conditions of using USBC, including their rights and the bank's rights. Changes in terms or policies are communicated proactively. Internally, any breach of governance procedures triggers a post-mortem and remedial actions, reinforcing that governance processes must be followed.

- **Independent Third-Party Reviews:** In addition to governance conducted by the participating bank, the USBC network will undergo regular third-party audits and reviews, similar to those performed on traditional core banking systems. These independent assessments will cover system integrity, security controls, operational reliability, and compliance alignment. Full audit reports will be made available to network participants and regulators to ensure transparency and trust across the ecosystem.

- **Alignment with Existing Bank Governance:** The USBC program is integrated into the bank's overall corporate governance structure. It is subject to the same audit and risk committees that oversee bank operations. The bank's Board of Directors is briefed on the initiative and provides high-level guidance. This ensures that the highest level of the organization is aware of and accountable for the program, which is crucial given the innovation's strategic importance and potential impact on the bank's risk profile and reputation.

In conclusion, the governance model for USBC is enterprise ready, multi-layered, and adaptive. It leverages the bank's existing governance strengths—clear lines of authority, regulatory compliance, and risk oversight—and augments them to handle the nuances of a blockchain-based system. The tone of governance is one of careful innovation: the bank is forward-looking and willing to push boundaries to realize the benefits of tokenization, but it will do so in a controlled, transparent manner that maintains the confidence of regulators and customers alike. This governance ethos will help ensure that as the USBC platform grows, it remains stable, trustworthy, and aligned with the public interest.

Licensing and Legal

The USBC model has been carefully designed to operate within the existing legal and regulatory framework for U.S. banking, avoiding the uncertainties that surround non-bank stablecoins or novel fintech charters. The following outlines the licensing, regulatory, and legal considerations and how the model addresses each:

- **Banking License and Regulatory Perimeter:** USBC is issued by a U.S. insured depository institution ("IDI") that holds a standard bank charter and is a member of the FDIC. No new special-purpose charter is needed; the bank's authority to accept deposits is the only authorization required to issue USBC. By anchoring the model to a regulated bank, USBC remains within the established commercial banking framework. All legal obligations that apply to deposit-taking institutions also apply to USBC where relevant. All laws and regulations that apply to deposits and banks in general would also apply to USBC. A bank would include USBC balances on its balance sheet and regulatory reports, ensuring full transparency to regulators.

- **FDIC Insurance and Customer Protection:** Each USBC account is an insured deposit account of the bank, covered by FDIC deposit insurance up to the standard limit, which is currently $250,000 per depositor, per bank, per deposit category. This means that customers holding tokenized deposits have the same protections against bank failures as if they held a checking or savings account directly at the bank. In the unlikely event of the bank's failure, the FDIC would insure the balances, and any uninsured portion would have the same priority as other deposits in receivership. By contrast, holders of stablecoins issued by non-banks have no such statutory insurance—they are exposed to the issuer's credit risk. With USBC, legal ownership of funds remains with the customer as a depositor of the bank, not as a creditor to a separate stablecoin trust. Customers receive regular statements and disclosures as required for bank accounts, and their rights are governed by established banking law.

- **Securities and Commodity Laws:** USBC is not a security or investment contract—it is simply a deposit liability, which is explicitly exempt from securities laws. Therefore, issuing USBC does not require registration with the SEC, nor does the platform create a tradable security.

- **Money Transmission Laws:** Insured depository institutions in the U.S. generally have an exemption from state money transmitter licensing when conducting bank activities. Due to the fact that USBC is a bank deposit product, the bank does not need separate money transmitter licenses in each state to allow users to transfer tokenized deposits. The activity is covered under the bank's powers to move deposits and facilitate payments. If the bank partners with non-bank entities for distribution, that fintech would rely on the bank's regulatory umbrella to avoid needing its own licenses. In essence, the regulatory compliance burden is centralized at the bank, which is accustomed to it, rather than distributed to potentially lightly regulated entities.

- **BSA/AML Compliance:** The bank, as a regulated financial institution, is already subject to the BSA and implements a full AML program. All USBC activities fall under that same program.

- **Data Privacy and Consumer Protection Laws:** Since tokenized deposits are bank accounts, they are subject to privacy rules like the Gramm-Leach-Bliley Act which governs how banks handle customer non-public information. The bank provides customers with GLBA privacy notices, explaining what data is collected and how it may be shared. As described in the Privacy section, the platform was built to meet and exceed these requirements by giving customers fine-tuned control of their personal data. Additionally, consumer protection regulations such as Regulation E would apply to USBC transactions. This means consumers have error resolution rights—for instance, if a consumer identifies an unauthorized USBC transfer, they can notify the bank and have it investigated and possibly reimbursed under Regulation E's protections, which is a

significant advantage over holding cryptocurrency, where there is typically no recourse for unauthorized transactions.

- **Contractual Framework:** Each user agrees to a deposit agreement and digital services terms when enrolling. This legal contract spells out that USBC represents a deposit obligation of the bank, that the user must abide by the platform's rules, and the bank's rights. It also covers how disputes or errors are handled, and includes disclaimers typical for online banking services. From a legal perspective, the ownership of funds is clearly in the user's name as a depositor, and the blockchain ledger is just a record of transactions, not the legal title. In case of any conflict between what the blockchain shows and the bank's general ledger, the bank's general ledger is authoritative—but in practice they are kept in sync.

In summary, the legal and licensing framework for USBC leverages the existing bank regulatory regime, which is one of the strongest and most protective in the world. The bank's approach is to translate new technology into familiar legal terms: a blockchain transaction is legally an electronic funds transfer; USBC is legally a deposit liability; the ledger is legally part of the bank's records. By doing so, the model avoids the pitfalls that have plagued other digital currency efforts and provides confidence to all parties that the rule of law and decades of banking precedent fully apply. Customers, therefore, enjoy both the novel functionality and the legal protections of traditional banking—novel functionality with the legal protections of traditional banking—and regulators can encourage innovation without fearing a step into the unknown.

CHAPTER 5 _ CONCLUSION

Conclusion

The offering of tokenized deposits marks a pivotal step toward a more secure, inclusive, and resilient financial system. USBC leverages the strengths of blockchain technology while remaining fully anchored within the U.S. regulatory framework, combining the innovation of programmable money with the trust and safeguards of traditional banking. By representing actual, FDIC-insured deposits on a blockchain ledger, USBC eliminates the opacity, reserve risks, and regulatory ambiguity associated with stablecoins.

Looking ahead, USBC envisions a future where self-custody wallets function as fully regulated bank accounts. With compliance and identity at its core, the USBC model lays the groundwork for broad, equitable access to digital financial services, without compromising the safety and stability of the banking system. This is not just a technical evolution; it's a systemic upgrade to how money can move, scale, and serve everyone.

Definitions/Glossary

Bank Reserves: Funds that a commercial bank holds in cash or on deposit with the Federal Reserve or central bank to meet regulatory requirements and customer withdrawal demands. In a fractional reserve system, banks keep a portion of deposits as reserves and lend out the rest.

Bronze, Silver, Gold Levels: Levels of identity verification and access privilege in a progressive KYC system. Bronze indicates a basic, entry-level verified account with minimal credentials provided (and thus low transaction limits). Silver is a mid-level status with standard identity documents verified, allowing higher limits and more features. Gold is the highest level, where the user's identity is thoroughly verified (comparable to a fully KYC'd bank customer).

Central Bank Digital Currency ("CBDC"): A digital form of a country's fiat currency issued directly by the central bank. A retail CBDC would be held by the public as a digital equivalent of cash (a central bank liability), whereas a wholesale CBDC is for banks to settle interbank transfers. Tokenized deposits differ in that they are liabilities of private banks, not the central bank.

Digital Asset: A broad term for any asset issued or transferred using distributed ledger or blockchain technology. This includes cryptocurrencies (e.g. Bitcoin), stablecoins, tokenized deposits, NFTs, etc. A tokenized deposit is a type of digital asset representing a bank deposit.

Distributed Ledger: A database that is shared and synchronized across multiple computers or nodes, allowing transactions to have multiple witnesses and creating a tamper-evident history. Blockchain is one type of distributed ledger technology ("DLT"). The tokenized deposit platform uses a permissioned distributed ledger to record transactions.

Financial Action Task Force ("FATF"): An intergovernmental body that sets international standards for combating money laundering, terrorist financing, and other threats to the financial system. FATF issues guidance that shapes national AML and KYC regulations. The USBC platform is designed to support compliance with FATF recommendations, especially those related to digital assets and identity.

FDIC Insurance: The protection provided by the Federal Deposit Insurance Corporation (a U.S. government agency) that guarantees deposits at member banks up to a certain limit (currently $250,000 per depositor, per bank) in the event of a bank failure. Tokenized deposits at an FDIC-insured bank benefit from this insurance just like traditional deposits do.

Fractional Reserve Banking: The banking system in which banks are required to keep only a fraction of their depositors' funds in reserve, lending out the remainder. This allows banks to create credit and expand the money supply while still meeting withdrawal demands under normal conditions. Tokenized deposits operate within this framework, unlike fully reserved stablecoins.

Know Your Customer ("KYC"): A set of procedures that financial institutions follow to verify the identity of their clients and assess potential risks of illegal intentions (like money laundering or terrorist financing). This typically involves collecting and verifying personal information and documents. In this platform, KYC is integral and leveled (progressive KYC through Bronze/Silver/Gold).

Open Banking: The practice of banks securely sharing financial data with third-party providers (with customer consent) to enable new financial services. This is often via APIs and is mandated or encouraged by regulations in some jurisdictions. The tokenized deposit platform embraces open banking by allowing customers to grant trusted third parties access to their accounts or data, pursuant to Section 1033 of Dodd-Frank in the U.S.

Permissioned Blockchain: A blockchain or distributed ledger that is not open to the general public; participants (nodes and users) must be granted permission by an authority. This contrasts with permissionless (public) blockchains like Bitcoin or Ethereum. The tokenized deposit ledger is permissioned, meaning only KYC'd customers can transact – but it uses technology similar to public blockchains under the hood.

Progressive Identity: An approach to digital identity verification where users can gradually build up their verified identity over time, unlocking greater permissions as more credentials are added. It acknowledges that not all users can immediately provide a full suite of documents and that trust can be established incrementally. The Bronze/Silver/Gold level system is an implementation of progressive identity.

Remote Procedure Call ("RPC"): A technical protocol that allows one piece of software (such as a user's wallet or a bank system) to request data or actions from another system (such as a blockchain node) over a network. RPCs are the main way external applications communicate with the blockchain, such as to retrieve balances, submit transactions, or check status.

Smart Contract: Self-executing code on a blockchain that automatically enforces rules and actions when predetermined conditions are met.

Stablecoin: A digital token designed to maintain a stable value by being pegged to a reference asset, often a fiat currency like the U.S. dollar. Stablecoins are typically fully backed by reserves of assets. Examples include USDC or USDT (pegged to USD). In this paper we distinguish stablecoins (issued by non-banks, outside the banking system) from tokenized deposits (issued by banks as regulated deposits).

Tokenized Deposit: A bank deposit represented as a digital token on a blockchain ledger. Each tokenized deposit is a direct claim on the issuing bank, equivalent to traditional deposits in value and legal status, but transferable on a blockchain platform. Tokenized deposits combine the trust of bank money with the programmability of digital tokens, and are not a separate cryptocurrency or stablecoin—they are the same dollars customers hold at the bank, in tokenized deposit form.

Transaction Finality: The point at which a transaction is irrevocably settled and recorded. In blockchain systems, finality can be probabilistic (in public chains) or deterministic (often in permissioned chains). In the tokenized deposit ledger, once a transaction is confirmed by the bank's node(s) and meets all rule checks, it is final – the ledger provides immediate settlement finality, much like a core banking system posting.

USBC Tokenized Deposit Network: The blockchain infrastructure used to record ownership and transaction history for USBC. It is a permissioned, compliance-first distributed ledger that supports identity-aware financial transactions. Only KYC'd users can transact, ensuring transparency, auditability, and regulatory alignment.

Verifiable Credentials: Digital credentials (e.g., identity attributes, attestations of documents) that can be cryptographically verified as authentic. These might include things like "Passport verified by Authority X" or "Income verified by Employer Y." In the identity system, users collect verifiable credentials which the system checks (often via third-party verification) to increase their identity level. These credentials are stored securely and used to prove identity or other attributes without repeatedly exposing original documents.

Wallet (Digital Wallet): An application or interface that allows a user to interact with their digital assets – in this case, their tokenized deposits. The wallet holds the cryptographic keys needed to authorize transactions. It may be custodial (managed by the bank on the user's behalf, accessible via the banking app) or non-custodial (managed by the user, if supported in the future). The wallet shows the user's balance, transaction history, and provides options to send/receive tokenized funds.

References

[1] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of blockchain technology applications for financial services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations,* vol. 2, no. 3, p. 100073, 2022, doi: 10.1016/j.tbench.2022.100073.

[2] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express,* vol. 7, no. 2, pp. 229-233, 2021, doi: 10.1016/j.icte.2020.09.002.

[3] L. Levulytė and A. Šapkauskienė, "Cryptocurrency in context of fiat money functions," *The Quarterly Review of Economics and Finance,* vol. 82, pp. 44-54, 2021, doi: 10.1016/j.qref.2021.07.003.

[4] J. Spira and D. Wessel. (2025, June 6) What are stablecoins, and how are they regulated? *Brookings*. Available: https://www.brookings.edu/articles/what-are-stablecoins-and-how-are-they-regulated/

[5] (2025, June 9) Top USD stablecoin coins today by market cap. *Forbes*. Available: https://www.forbes.com/digital-assets/categories/usd-stablecoin/?sh=2e66ae607ddf

[6] S. A. Maex and S. Slavov, "Initial evidence on the content and market implications of stablecoin reserve reporting," *Journal of Accounting and Public Policy,* vol. 51, p. 107309, 2025, doi: 10.1016/j.jaccpubpol.2025.107309.

[7] D. Arner, R. Auer, and J. Frost, "Stablecoins: Risks, potential and regulation," Bank for International Settlements, 2020.

[8] A. Briola, D. Vidal-Tomás, Y. Wang, and T. Aste, "Anatomy of a Stablecoin's failure: The Terra-Luna case," *Finance Research Letters,* vol. 51, p. 103358, 2023, doi: 10.1016/j.frl.2022.103358.

[9] P. O. Diop, J. Chevallier, and B. Sanhaji, "Collapse of Silicon Valley Bank and USDC depegging: A machine learning experiment," *FinTech,* vol. 3, no. 4, pp. 569-590, 2024.

[10] 12 CFR Part 1005 - Electronic Fund Transfers (Regulation E), https://www.consumerfinance.gov/rules-policy/regulations/1005/.

[11] K.-F. Israel, "The fiat money illusion: On the cost-efficiency of modern central banking," *The World Economy,* vol. 44, no. 6, pp. 1701-1719, 2021, doi: 10.1111/twec.13028.

[12] B. Oude Roelink, M. El-Hajj, and D. Sarmah, "Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication," *Security and Privacy,* vol. 7, no. 5, p. e401, 2024, doi: 10.1002/spy2.401.

[13] Financial Action Task Force (FATF), “Guidance on digital identity,” Mar. 2020. Available: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

[14] Consumer Financial Protection Bureau (CFPB), “Request for information regarding consumer access to financial records (Dodd-Frank Act Section 1033).” Available: https://www.consumerfinance.gov/rules-policy/notice-opportunities-comment/archive-closed/dodd-frank-act-section-1033-consumer-access-to-financial-records/

[15] Federal Reserve Board, “The liquidity coverage ratio and corporate liquidity management,” Aug. 13, 2021. Available: https://www.federalreserve.gov/econres/notes/feds-notes/the-liquidity-coverage-ratio-and-corporate-liquidity-manag

Authors & Contributors

Greg Kidd - Chairman & CEO, USBC

Izzet Can Akkus - Chief Strategy Officer, USBC

Erik Westra - Senior Advisor - Architect, USBC

Tom Gentle - Management Consultant, FS Vector

Kirk Chapman - COO, USBC

Robin Huiser - Chief Blockchain Architect, USBC

Sree Charran - Chief Blockchain Technology Officer, USBC

Norman Rountree - Chief Information Security Officer, USBC

Mitja Simcic - CTO, USBC

Vadim Slavin - Director of Front End Product, USBC

Alec Liu - Chief Marketing Officer, USBC

Thomas Milkey - Strategy Associate, USBC

Liz Sweigart - PhD, Advisor - Rewards Token, USBC