Hazel Network:
Unified Tokenized Bank Deposit and Stablecoin Token

Vantage Bank
Shawn Main
Jeff Sinnott

Custodia
Jesse Smith
Caitlin Long
Josh Marlow-Grell

June 2026

Most US dollars still settle on payment systems built in the 1970s that are closed nights, weekends, and holidays. Advances since then have been largely incremental, akin to the progression from dial-up internet to broadband using the same telephone lines. Tokenized bank deposits that programmatically convert to and from stablecoins via a unified token allow banks to safely and soundly upgrade payments from within the banking system, thereby helping to protect banks' customer relationships against disintermediation by fintechs. Hazel Network built its unified token to programmatically execute the embedded compliance and operational controls that banks require, making it clear Hazel Network was built by banks for banks.

Abstract. This paper describes the inevitable evolution of banking as new technology enables efficiencies and functionalities not previously possible. Traditional banking requires intermediaries and adds delays to payment settlement. Traditional payment systems do not offer the programmability and composability that customers and counterparties have come to expect from digital infrastructure. Every dollar that a customer moves from a bank to a stablecoin issuer leaves that bank and rarely comes back to it – until now. Hazel Network offers a new way forward, built on battle-tested infrastructure that does not require a new blockchain, cryptocurrency, or intermediary. A single, integrated smart contract issues a token that is a bank deposit when held within a consortium of banks, and a GENIUS Act-compliant stablecoin redeemable one-to-one for a US dollar when held by anyone else. Consortium member banks settle directly with one another in near real-time. Their customers' deposits can leave the network and – here's the secret sauce – programmatically settle back at the originating bank without the conversion friction or third-party intermediation inherent to third-party stablecoins. Hazel Network embeds compliance and reserve-requirement logic into transaction screening, and automatically enforces both at Hazel Network's protocol level. Hazel Network is bank-grade, institutionally operated, and live on Ethereum mainnet today.

Important Notice. *This white paper is provided for informational purposes only and does not constitute an offer to sell or a solicitation of an offer to buy any token, security, deposit, or other instrument. It is intended for institutional audiences. The full disclaimer at the end of this document applies to this white paper in its entirety.*

1. Introduction

Most of the dollars moving through the United States today still settle on payment rails built in the 1970s that operate only on weekday hours and end-of-day cycles. Hazel Network delivers 24/7/365 programmable settlement within the banking system, through customers' existing bank accounts, so that dollars move at the speed of global commerce. Newer payment rails such as FedNow and RTP have addressed parts of legacy payment systems' speed problem, but adoption has been gradual and combined volume on those newer rails remains a small fraction of legacy settlement traffic. Speed isn't the only limitation of existing infrastructure. The deeper constraint is that the rails were not designed for the features customers and counterparties have come to expect from any other piece of digital infrastructure: programmable conditions, composable interfaces, real-time auditability, and round-the-clock availability. A bank operating on existing rails can offer its customers a payment – but it cannot easily offer a payment that releases on a delivery confirmation or settles atomically against a tokenized asset.

When a customer moves a dollar from a bank into a stablecoin, the dollar usually leaves the banking system for T-bills or migrates to a deposit at a large-bank stablecoin custodian. It rarely settles back at the bank of origin.[1] The consequence is a disintermediation of banks' core deposits via a sustained outflow of deposits into a parallel financial system.

Hazel Network proposes a different path – one that brings bank customers the benefits of modern payment technologies while also preserving banks' core deposits from disintermediation by third-party stablecoins. Hazel provides bank-architected infrastructure without requiring banks to trust a new blockchain, a new token, or a new intermediary. A single smart contract, deployed on Ethereum mainnet, issues a token that is a bank deposit when held by a member bank in the network, and a fully-reserved, GENIUS Act-compliant stablecoin redeemable one-to-one for a US dollar when held by anyone else. Member banks settle directly with one another in near real-time. Customer deposits can leave the network *and* programmatically route back to the originating bank. Compliance is enforced at the protocol level, by code that screens every transfer and prevents the creation of unbacked external supply automatically.

The financial system has long treated the choice between regulated stability and on-chain composability as a forced one. The financial system has often treated stability and speed as opposites: the proverbial tortoise protects trust by moving cautiously, while the proverbial hare moves fast by cutting corners. Hazel rejects that framing, because the hare represents disciplined speed; velocity is achieved through design, not exemption.

Hazel Network enables banks to move quickly precisely because regulatory compliance, controls, and prudential safeguards are intentionally embedded directly into the rails rather than being bolted on afterwards. By baking these constraints in at the protocol level, Hazel allows banks to operate at software speed while remaining fully regulated and bank-grade.

Hazel Network is live. Mainnet operations are underway.

[1] Source: `https://www.jpmorganchase.com/institute/all-topics/financial-health-wealth-creation/dynamics-demographics-us-household-crypto-asset-cryptocurrency-use`.

The chapters that follow describe the consortium model that defines the Hazel Network's perimeter, the unified-token design that makes the closed loop possible, the economic model that aligns incentives across banks of any size, and the operational architecture that makes it work in practice.

2. The Financial Institution Consortium Model

Hazel Network is a consortium of financial institutions operating on a network that incorporates blockchain infrastructure integrated with a side-core. Membership is defined, bounded, and contractually established. Wallet-level flows in aggregate can be observed on-chain, but only onboarded participants can transact. Customer identities and account details remain off-chain at member banks, under the same confidentiality frameworks that apply to traditional deposits. Network-level transparency coexists with customer-level privacy. The boundary between members and non-members is the central organizing principle of the network's design.

Table 1: *Operational roles in the Hazel Network and the entities currently filling them.*

Role	Function	Current implementation
Member Bank	Holds consortium positions on the unified token and issues tokenized deposits to its own customers	Vantage Bank and onboarded member banks
Settlement Bank	Acts as correspondent for member banks; holds the deposit accounts backing each member's network activity; operates the off-chain deposit ledger recording inter-member positions	Vantage Bank
Digital Asset Issuer	Issues the unified token in its stablecoin form; holds segregated reserves; stands as the obligor when tokens are held outside the consortium	Custodia
Technology Provider	Supplies the smart contracts, cryptographic key management, and deposit-ledger platform	Custodia (contracts, key management); Infinant (Interlace deposit-ledger platform)

A member of Hazel Network is a financial institution that has executed the network's operating agreements, completed Vantage's onboarding and compliance review, and established a deposit relationship with Vantage. The agreements bind the institution to the consortium's rules. The compliance review confirms the institution can operate alongside other regulated participants. The deposit relationship establishes the financial position behind the member's network activity. Once admitted, the member's on-chain addresses are provisioned by Custodia and added to a registry that the unified token consults on every transfer. Membership is governed by written agreement. Every member is a known, vetted and regulated entity.

When a member bank holds the unified token inside the consortium, that holding is a bank deposit. The settlement bank is Vantage; its obligor role is confined to inter-member settlement balances and does not extend to member banks' own customer deposits, which remain liabilities of each issuing member bank, or to the stablecoin form, which is Custodia's fully-reserved obligation. The relationship mirrors any correspondent banking arrangement: the balance sits on Vantage's balance sheet as a liability, and the member bank's claim carries the standard supervisory framework. When a member bank in turn issues tokenized deposits to its own customers, the customer's tokenized deposit is an obligation of the issuing member bank, just like any other customer deposit.[2] Obligor responsibility runs along the same chain of bank-customer relationships that correspondent banking has used for a century. Tokenization changes only how the record is kept.

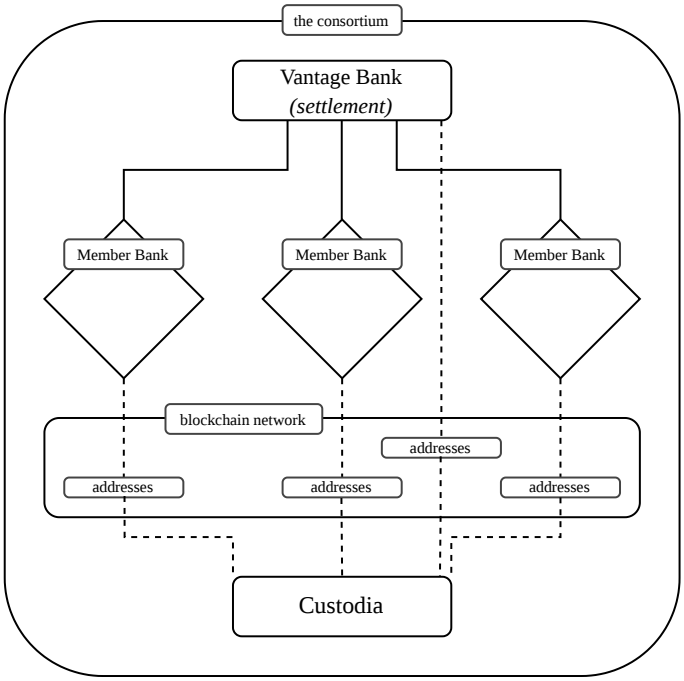

Figure 1: *Member banks hold deposit accounts at the settlement bank. Addresses within consortium managed by Custodia.*

Settlement across the consortium happens in three coordinated records. The unified token moves on-chain from one member's address to another, signed by Custodia's authorized operator. The Interlace deposit ledger, operated by Infinant on the settlement bank's behalf, records the corresponding shift in vostro positions. Vantage's general ledger reconciles at the end of day. All three must agree. The mechanism is structurally analogous to Fedwire: a central institution holds accounts for each participant, and inter-participant settlement happens by adjusting those accounts. What is new is the on-chain layer carrying an independently verifiable, immutable record of the same movement.

[2]The FDIC has clarified that the tokenization of a deposit liability does not alter its treatment as a deposit under the regulatory framework. *See* Travis Hill, Vice Chairman, FDIC, "Banking's Next Chapter? Remarks on Tokenization and Other Issues" (March 11, 2024), `https://www.fdic.gov/news/speeches/2024/spmar1124.html`.

The consortium's perimeter is also the boundary between two distinct legal regimes for the same, unified token. Inside the consortium, the token is a bank deposit, with the issuing member bank as obligor and with the protections and obligations that status implies. Outside the consortium, the same token is a fully-reserved stablecoin governed by the GENIUS Act, with Custodia as the obligor. The holding address determines which regime applies. The next section describes how the same token seamlessly switches obligors and legal character, as well as how Hazel Network programmatically maintains the distinction at the protocol level.

3. The Unified Token

The unified token is a single on-chain token whose legal character is defined by who holds it. This token is a tokenized bank deposit when held by a member bank in the consortium and a payment stablecoin when held by anyone else. The smart contract checks the consortium registry on every transfer and automatically applies the appropriate accounting and reserve treatment. There is no separate "deposit token" and "stablecoin token" – one token carries either one of two legal characters, depending on who holds it.

The design choice to ascribe to the token two legal characters that switch depending on whether the holder is inside or outside the consortium is unique.[3] Stablecoin issuers today operate single-character tokens, such as USDT and USDC, which exist as stablecoin tokens regardless of wallet or address. They rely on fiat redemption windows to move value between the on-chain and banking systems. Bank tokenization projects operate single-character tokens at the other end of the spectrum: they exist inside a single institution's closed network and never touch on-chain liquidity. Hazel's unified token is a hybrid that operates as a bank deposit when held inside a vetted consortium address and transforms into a regulated stablecoin when held anywhere else, with the legal characterization automatically changing at the consortium boundary rather than through a conversion or redemption transaction.

[3]The foundational token design is protected by US Patents 11,392,906, 12,450,578, 12,579,525 and others still pending, each entitled "Cryptographic Token with Separate Circulation Groups." Additional patents are pending on the unified-token model that extends this design to dual legal characterization at the consortium boundary and still other subject matter.

Table 2: *The unified token compared with privately-issued stablecoins and traditional bank deposits.*

Property	Privately-Issued Stablecoin	Traditional Bank Deposit	Hazel Unified Token
Holder's claim is on	Single-issuer entity	The depository bank	Member bank (deposit form); Custodia (stablecoin form)
FDIC insurance eligible	No	Yes (up to limits)	Yes (deposit form)
Cash equivalent under accounting standards	Generally no (IAS 32 financial instrument)	Yes	Yes (deposit form); yes when GENIUS-compliant
Settles 24/7/365 on chain	Yes	No (banking-hours batch rails)	Yes
Programmable and composable on chain	Yes	No	Yes
Reserve or backing requirement	Off-chain issuer attestation	Bank fractional reserve under prudential oversight	On-chain cap (stablecoin form); deposit framework (deposit form)
Legal certainty as collateral under US law	Uncertain (UCC Article 12 gaps)	Yes (longstanding deposit law)	Yes (GENIUS Act for stablecoin form; deposit law for deposit form)
Single instrument across off-chain and on-chain contexts	N/A	N/A	Yes
Requires Exchange	Yes	N/A	No

When a bank customer sends funds from a member bank's wallet to a non-consortium wallet, the token remains the same technical instrument but its obligor and its legal status changes. When the token crosses the consortium perimeter, the smart contract automatically reclassifies the same balance as a stablecoin obligation backed by Custodia's reserves (and reserves programmatically move at the settlement bank accordingly). The same is true in reverse. When a stablecoin holder transfers tokens back to a member bank, the smart contract reclassifies the balance as a tokenized deposit and the receiving bank credits the customer's account (and reserves programmatically move). No token conversion transaction or crypto exchange involvement takes place. The legal character and reserves change at the perimeter, while the technical instrument does not.

The consequences of the unified design accrue to several distinct parties.

For the originating bank, the unified token is designed with a goal of preserving the primary banking relationship (and core deposits). Customer funds moving from a deposit account into a blockchain wallet do not represent a permanent migration of the bank's core deposits outside the bank, as is usually the case when customers move funds to incumbent stablecoins today. Within Hazel Network, when the token crosses the consortium boundary, the customer's claim shifts from a deposit at the originating bank to a stablecoin obligation of Custodia, backed by one-to-one reserves. An incoming transfer to the customer's original receiving address programmatically credits the deposit at the originating bank, thereby maximizing the preservation of the member bank's core deposits.

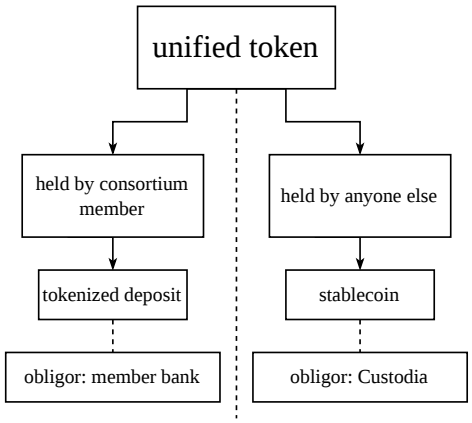

Figure 2: *Tokens held by consortium members are bank deposits, obligations of the issuing member bank. Tokens held anywhere else are GENIUS Act stablecoins, obligations of Custodia.*

This novel token design eliminates the conversion friction that currently defines the relationship between bank deposits and stablecoins. A dollar moving between the deposit form and the stablecoin form retains its dollar of value. Customers do not need a crypto exchange account to move balances between bank and blockchain contexts. Nor do they need to pay conversion fees or accept slippage. The same balance works natively as either a stablecoin or as a tokenized deposit. ***This property is the singleness of money.*** One dollar of value remains one dollar of value regardless of the legal character of the token.

For the consortium, each additional member bank increases the proportion of transactions that stay within the consortium, increasing the share of customer activity in which the primary banking relationship is preserved.

Both legal characters of the token stem from the same smart contract. This is the simplest possible architecture for the operation it performs, and it produces properties that a more elaborate design could not: balances cross the consortium boundary as transformations rather than conversions, the two characters share a single contract state and cannot diverge from each other, and the system has one surface to audit. The programmatic reserve state and the supply against it are visible in real time to every member bank and to any external party. Members do not have to 'take an issuer's word for it' to know whether the external supply is fully backed at every moment. That information is verifiable on-chain and is enforced at the protocol level as a condition of every out-of-consortium transfer.

One smart contract, one token, two legal profiles.

4. The Programmatic, Frictionless Path To and From the Originating Bank

When a customer moves a dollar from a bank to an incumbent stablecoin, the dollar typically does not land back at the bank of origin. The customer's funds settle at whichever bank holds the stablecoin issuer's reserves, and the vast majority of stablecoin reserves are then invested in T-bills. When those funds enter back into the banking system, they may land anywhere – at the same bank, at a different bank, or with a different issuer entirely. The deposit that began at the originating bank does not necessarily, as a matter of design, easily find its way back to its primary banking relationship at the originating bank. Friction created by fintechs is sometimes *designed* to disintermediate that primary banking relationship.

This is the structural problem at the center of the deposit-disintermediation concern. Banks lose customer relationships to stablecoin issuers because each conversion is usually one-way. The relationship leaves once and typically never comes back. Each conversion from bank deposit to stablecoin moves the customer's claim out of the originating bank's books, likely permanently. The friction of converting a stablecoin back to a bank deposit compounds the problem: even customers who want to move funds back to a bank face fees, settlement delays, debanking risk and conversion costs that act as a disincentive for most amounts. This friction is designed to minimize flows back into the banking system. The stablecoin economy treats deposit outflow as the default direction, while deposit inflow is incidental.

Hazel inverts this default one-way direction. Since the unified token is the same token inside and outside the consortium, the journey back to the originating bank uses the same path the token took to leave. When member bank tokens are sent to a non-consortium wallet, the tokens become a stablecoin. When those tokens move from any wallet back to the originating member bank's wallet, they programmatically become a tokenized deposit again, in the same account at the original bank. The token does not change; only the legal classification changes.

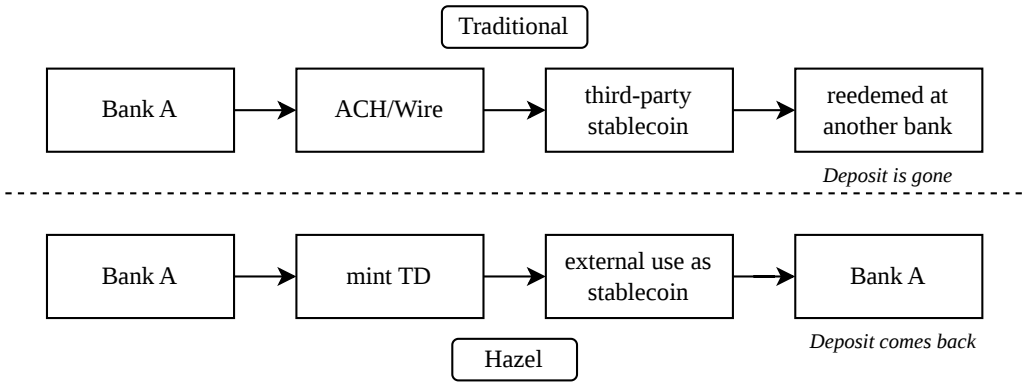

Figure 3: *Traditional stablecoin flows typically result in the loss of the primary banking relationship. Hazel allows this relationship to be easily maintained with a frictionless path back to the originating bank.*

This property produces two consequences that the existing stablecoin model does not.

The first is that the originating bank retains the primary banking relationship across the consortium boundary. A customer who holds the unified token in stablecoin form is still, in a connectivity sense, the originating bank's customer. The bank maintains a customer-wallet mapping. When tokens are sent back to the customer's account address, the corresponding customer's account is credited. The primary banking relationship persists even when the funds leave the bank's perimeter.

The second consequence is that banks become the on-ramp into the on-chain economy. The disintermediation problem is usually framed in one direction: customers leaving banks for stablecoins. The less-discussed direction is that banks have no native way for their customers to enter the on-chain economy without leaving the bank. A customer who wants to hold a stablecoin balance must wire or ACH funds to a crypto exchange or stablecoin issuer. With Hazel, the customer's bank *is* the entry point. A tokenized deposit at a member bank is already on-chain and can move directly to a non-consortium wallet without a crypto exchange or stablecoin issuer in the path. The bank captures the on-ramp economics that normally flow to fintechs.

The closed-loop property distinguishes Hazel from other approaches attempting to address similar problems. (a) Internal bank settlement networks – the private systems several large banks have built for their own customers and counterparties – retain deposits because the asset never leaves the bank's perimeter. They solve deposit retention but prevent the asset from participating in the broader on-chain economy. (b) Clearing-layer approaches connect existing stablecoin issuers to banks for par-value redemption. They reduce off-ramp friction but do not preserve the originating bank's relationship across the on-chain boundary. Redemption routes to whichever bank the customer happens to use. Hazel addresses a different question: how does a bank preserve the primary banking relationship both when the asset leaves the consortium perimeter and re-enters? The unified token is the answer.

Table 3: *How Hazel preserves the customer-bank relationship across the on-chain boundary, compared with alternative architectures.*

Property	Permissioned Tokenized Deposit Network	Stablecoin Clearing Network	Hazel Network
Token can leave the network for the broader on-chain economy	No (closed perimeter, whitelisted wallets)	Stablecoins already live on permissionless chains	Yes
Token comes back to the originating bank after leaving	Cannot leave	No originating-bank concept	Yes, by design
Originating bank retains the customer relationship across the on-chain boundary	Customer cannot leave the perimeter	No (redemption routes to whichever bank the customer uses)	Yes
Customer's bank is the on-chain entry point	Only within the bank's closed network	No (entry via exchanges or issuers)	Yes (direct on-ramp at member bank)
Bank's role	Participating bank holds the underlying deposit	Receiving institution acts as agent collecting redemption	Member bank is the principal obligor
Settlement venue	Permissioned blockchain	Off-chain clearing platform; stablecoins live on various chains	Ethereum mainnet
Live in production today	Planned	Pilot stage	Yes, mainnet since March 2026

5. Reserve Architecture

The unified token is backed differently inside and outside the consortium. Inside, it is a bank deposit. The legal and supervisory structure that governs ordinary bank deposits applies in full. There is no separate reserve mechanism inside the consortium because the standard deposit framework applies.

Outside the consortium, the reserve framework shifts to the GENIUS Act. Stablecoins issued under the GENIUS Act must be one-to-one backed by cash or cash-equivalent assets held in segregated reserves. Custodia is the issuer of the unified token in stablecoin form and holds such reserves required by the GENIUS Act. The GENIUS Act specifies a narrow set of permitted reserve assets, limited to cash and short-duration Treasury-backed instruments.

The architectural feature that distinguishes Hazel from other stablecoin protocols is that the stablecoin's reserve cap is programmatically enforced at the protocol level. Hazel Network's stablecoin smart contracts track token supply on-chain. Custodia role-gates the reserve function. The programmatic reserve balance is the on-chain floor against which the smart contract enforces external stablecoin supply. Actual segregated reserves equal or exceed the programmatic reserve balance at all times. Every out-of-consortium transfer triggers an automatic transaction screen: the resulting external supply must not exceed the programmatic reserve. If a transfer would breach the cap, the smart contract automatically rejects it before settlement, and no tokens move. The cap is a condition the smart contract requires before settlement, not an operational guideline. Incumbent stablecoins are often "trust me bro," but Hazel Network's reserve requirement is enforced on-chain.

Custodia's automated systems monitor the off-chain reserve account and push an on-chain update whenever the account balance changes. The smart contract automatically enforces the reserve cap against this declared balance on every out-of-consortium transfer. The integrity of the balance itself rests on off-chain controls and the monthly attestation. A role-gated signing process produces each update under institutional controls, after compliance checks pass and the corresponding fiat funds have settled in the reserve account. A one-to-one mapping between fiat settlements and on-chain updates ensures that no single fiat movement backs more than one declaration.

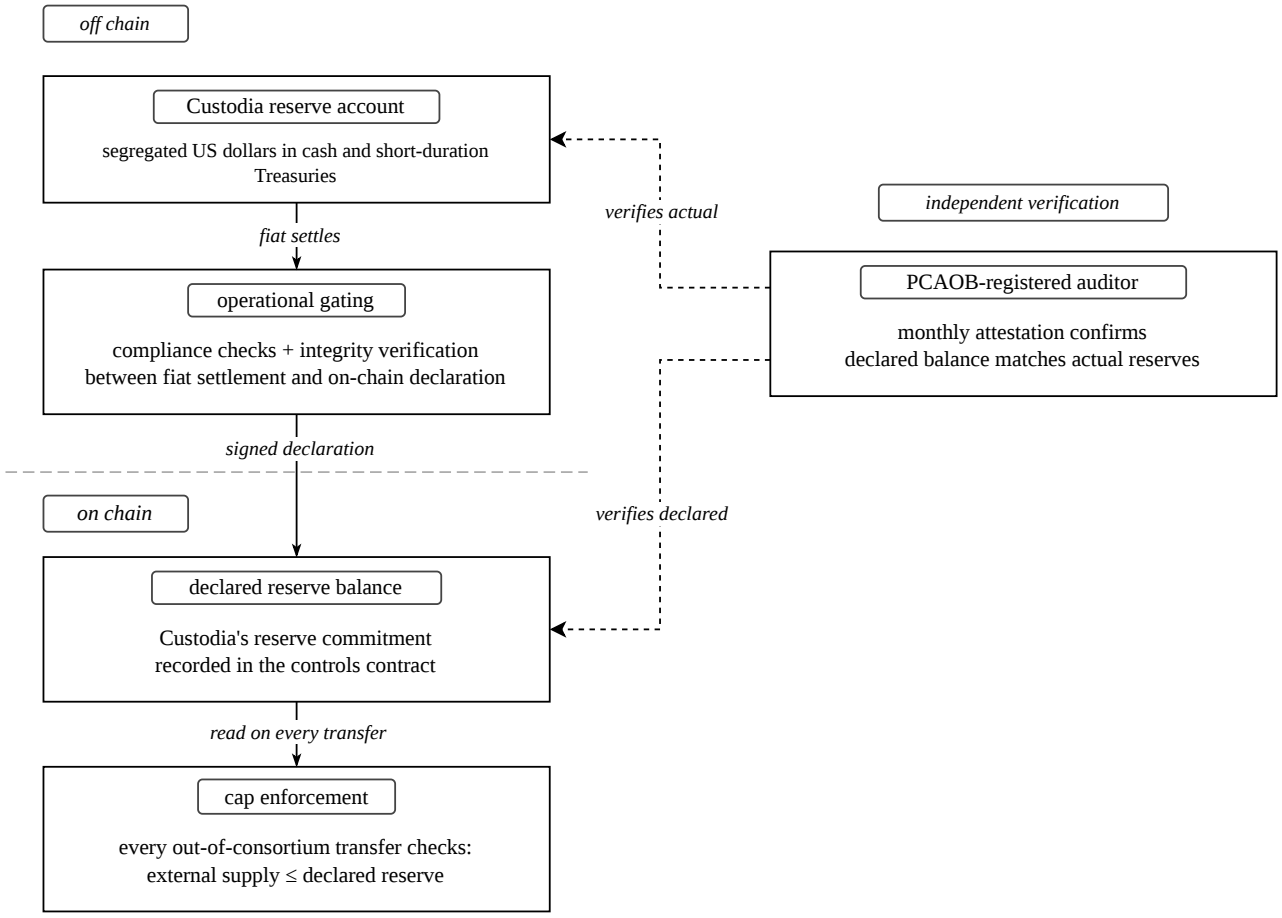

Figure 4: *Off-chain settlement gates the on-chain declaration that caps external token supply and ensures 1:1 backing.*

Protocol-level enforcement and external reserve attestation are complementary. The protocol-level cap prevents over-issuance from occurring in the first place. Additionally, monthly attestation by an independent accounting firm registered with the Public Company Accounting Oversight Board confirms that the declared reserve upon which the smart contract relies matches or exceeds the actual segregated reserves (noting there may be temporary timing differences between the accrual and payment of interest). The smart contract enforces the constraint continuously. The attestation anchors the constraint to actual reserves.

The architecture supports real-time visibility into the system's reserve state. Total token supply, externally-held supply, and the smart contract's current cap utilization are all observable on-chain.

The result is a reserve architecture that operates on three independent layers. The smart contract enforces the cap on every out-of-consortium transfer. Each reserve declaration follows corresponding fiat settlement and compliance verification. The attestation validates the actual reserves supporting the declared reserve balances.

6. Compliance by Construction

Hazel Network's compliance architecture covers automated OFAC sanctions screening, transaction monitoring, reserve enforcement, freeze and seize capabilities, and audit trail generation. Regulated banks own and operate these controls at every stage: Vantage vets member institutions and screens every transaction at the fiat layer, member banks handle customer-level compliance, and Hazel's protocol enforces sanctions and reserve checks automatically on every transfer. Hazel runs bank-grade compliance programmatically, at every stage and on every transaction.

The screening pipeline operates in three independent layers before on-chain settlement is programmatically permitted to occur. **Layer one** performs fiat-side compliance checks: sanctions screening, anti-money-laundering analysis, fraud signals, and adverse-media screening on every transaction at initiation. A transaction that fails any of these checks is automatically halted by the Hazel platform before it reaches the chain. **Layer two** performs analytics on the wallet addresses involved in the transaction, identifying associations with illicit actors, mixing services, or sanctioned entities through the analytics infrastructure that has matured around on-chain settlement. **Layer three** is on-chain: the smart contract checks both sender and recipient against the Chainalysis sanctions oracle on every transfer. If either address appears on the oracle's list, the smart contract rejects the transaction before settlement and no tokens move. The three layers are path-dependent. A transaction that passes layer one but fails layer two does not settle. If a transaction fails layer three, the smart contract automatically halts it at the protocol level.

There are two key structural differences between Hazel Network and existing stablecoin compliance arrangements. In a traditional stablecoin setting, sanctions screening, wallet screening and transaction monitoring are activities that an institution commits to performing on its transactions. The traditional control depends on the legacy stablecoin issuer maintaining and executing on its commitment.

In Hazel Network, by stark contrast, we baked the controls into the protocol's code: the third layer – sanctions screening – is built into the smart contract, and the second layer – wallet screening – is automated within Hazel Network's platform, preventing high-risk transactions from even initiating an on-chain token transfer until the compliance department has cleared the compliance alerts. The check is not a commitment Custodia makes, but rather an execution built into the protocol's code. The on-chain check is independent of Hazel Network's off-chain systems, so a sanctioned transaction cannot settle even if upstream screening were to miss it. Layers two and three use different vendors by design, so a miss by one vendor does not compromise the chain of screening.

For incoming on-chain transactions, the Hazel Network platform adds additional transaction screening at layer two (which is not applicable to outgoing transactions).

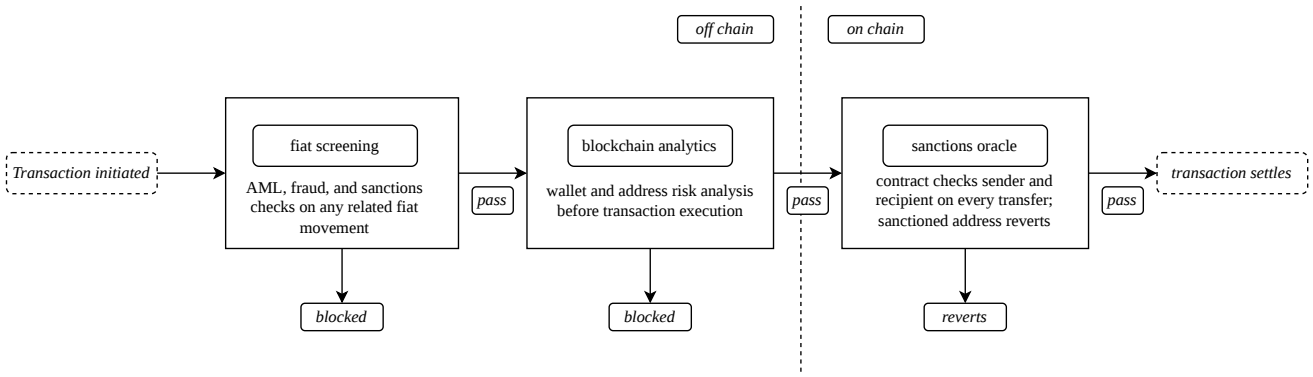

Figure 5: *Compliance is fully automated and gates every transaction across three layers, two off-chain and one on-chain.*

The compliance architecture described above also produces audit trails visible at the wallet and transaction levels in real time and on-chain. Every mint, burn, transfer, and freeze is a discrete timestamped event. Total token supply, externally-held supply, reserve cap utilization, and wallet balances are all observable. A supervisory examiner does not need to request an extract from Hazel Network to verify the system's state.

Beyond automatic enforcement, the smart contract supports three operational controls that allow authorized parties to act on specific accounts and transactions. **Freeze**, applied by an authorized compliance role, blocks transfers to and from a specified address pending review. **Seize** moves tokens from a frozen address to a designated holding wallet, exercisable when a freeze is supported by formal legal process. **Pause** halts every mint, burn, and transfer on the smart contract. It is reserved for incidents where continuing to operate the network is less preferable than halting it: to thwart an attack pattern on the smart contract, an unexpected operational incident requiring full review, or a network-level compliance directive. Each control is role-gated and logged on-chain. The capability to freeze and seize extends to all unified tokens, including tokens held outside the consortium because all tokens remain associated with the unified smart contract at all times. A token that has left a member bank and entered a non-consortium wallet remains subject to the same control surface as a token held inside the consortium.

Table 4: *Operational compliance controls available in the unified token smart contract.*

Control	Effect on the contract	Conditions for invocation	Authority required
Freeze	Blocks transfers to and from a specified address	Valid legal request from law enforcement, or internal monitoring identifying criminal association with sufficient evidence to act	Custodia Compliance, quorum-approved
Seize	Moves tokens from a frozen address to a designated holding wallet	Freeze supported by formal legal process	Custodia Compliance, quorum-approved
Pause	Halts every mint, burn, and transfer on the contract globally	Reserved for contract-level incidents requiring global intervention, identified through internal monitoring or supervisory direction	Custodia Compliance, quorum-approved

Custodia's policy for invoking these controls reflects deliberate posture. Authority and willingness to act follow defined conditions. The freeze authority is exercised in two situations: when Custodia receives a valid legal request from law enforcement, and when internal monitoring identifies a strong association between an address and criminal activity, supported by sufficient evidence to act. Seizure follows formal legal process. Custodia acts on law enforcement requests and on verifiable evidence of criminal association.

The result is a compliance posture with the operational reach that a regulated environment requires without unbounded discretionary authority. The screening pipeline catches illicit activity. The on-chain enforcement automatically rejects sanctioned transactions. The operational controls allow action when action is warranted. The visibility allows verification by anyone who needs to verify.

7. Three Implementation Models

A bank joining Hazel Network chooses how it integrates the Network into its operations. Three integration models exist, designed to meet the needs of banks of all sizes. Each model uses the same smart contracts, settlement infrastructure, and compliance procedures embedded into Network workflows. The three models vary based on how each bank's existing systems connect to that infrastructure.

Underneath the three models lies the correspondent banking relationship. The member bank's account at the settlement bank is a 'Due From' asset on its balance sheet, identical in character to any other correspondent relationship. The integration models differ only in how the bank's systems interact with that position.

The first model is **Basic**. A member bank participates in the network through the Hazel Platform and Bank Console, with compliance screening performed by Vantage and Custodia. No integration on the bank's side is required, and no change to the bank's core is needed. The Basic model is intended for banks that want to participate in the network using the standard platform and console.

The second model is **Advanced**. Hazel delivers three scheduled artifacts to the member bank on a cadence of the bank's choosing: a posting file with that cycle's tokenized deposit activity, a compliance file with the associated transactions across all customers, and an online banking Software Development Kit ("SDK")/widget for installation into their online banking platform of choice. The bank ingests these files into its core and its compliance systems. With its own systems updated from the file feed, the bank can present tokenized activity to customers and reflect it in its general ledger through familiar batch processes. The Advanced model is intended for banks that have a defined integration path and prefer the rhythm of scheduled deliveries.

The third model is **Enterprise**. A member bank integrates with Hazel via APIs. Activity is delivered to the bank's core systems as it occurs with real-time debits and credits, and the bank initiates transactions programmatically. The Enterprise model removes latency windows that the batch-file pattern introduces and lets member banks build programmable products on top of the consortium's settlement layer.

The three models are operational variants. A token issued by a member bank using Basic is the same technical instrument as a token issued by a member bank using Enterprise. A transfer initiated in one model can be received by a bank operating in any other. The integration choice determines how the bank's systems interact with the network.

8. First Reference Implementation: Ethereum

While Hazel Network's design is blockchain-agnostic, the initial reference implementation runs on Ethereum mainnet. Any EVM ("Ethereum Virtual Machine") capable blockchain could host the smart contracts; Hazel chose Ethereum as our first implementation because of the supporting ecosystem of operational and IT security maturity, audit firms, analytics infrastructure and regulator familiarity. In this reference implementation, the smart contracts are named AvitToken and AvitControls, and the token's symbol on Ethereum is Avit (rhymes with "have it"). When this token is held by an address within the consortium boundary, it is a tokenized deposit and is not an Avit stablecoin. Other deployments under the same smart contracts may use white-label branding.

8.1 Why Deploy on Ethereum First

Ethereum has operated continuously since 2015. In that decade it has accumulated the deepest audit and forensics ecosystem of any smart-contract platform. The firms that audit Solidity contracts have established practices for the patterns Hazel Network uses, including the OpenZeppelin[4] AccessControl, UUPS proxy, Pausable, and ReentrancyGuard implementations that the AvitToken contract inherits.

The Chainalysis sanctions oracle[5] that AvitToken automatically reads prior to every token transfer is widely deployed on Ethereum. The same is true for the commercial blockchain-analytics providers, which Hazel Network member banks consult in their compliance workflows. The on-chain compliance signals upon which Hazel relies are native to Ethereum, a fact that should bring significant comfort to the member banks' risk and compliance officers.

Federal and state regulators in the United States have reviewed Ethereum-based financial instruments across multiple supervisory cycles. The novelty cost of explaining Ethereum to an examiner is low. Less-established platforms require considerably more groundwork.

The Ethereum base layer continues to evolve through the Ethereum Improvement Proposal ("EIP") process, and smart contracts inherit improvements without redeployment. The client diversity of the network, with Geth, Nethermind, Besu, Erigon, and Reth implementing the protocol independently, protects deployed smart contracts from single-client failure modes.

Hazel's implementation is conservative within Ethereum, using widely-vetted OpenZeppelin smart contract patterns and the ERC-20[6] standard.

8.2 Deployment

Hazel Network's production deployment has been live on Ethereum mainnet since March 2026. Multiple parallel deployments on the Sepolia testnet provide test environments for staging and integration validation.

---

[4] OpenZeppelin Contracts, smart contract library for Ethereum. `https://docs.openzeppelin.com/contracts`.

[5] *See* Chainalysis sanctions screening oracle documentation: `https://go.chainalysis.com/chainalysis-oracle-docs.html`.

[6] Ethereum Improvement Proposal 20, ERC-20 Token Standard. `https://eips.ethereum.org/EIPS/eip-20`.

All smart contracts deploy as ERC-1967 proxies[7] under the Universal Upgradeable Proxy Standard ("UUPS") pattern.[8] The proxy address is the permanent, externally-facing identity of the smart contract. Users and integrators interact with the proxy while the proxy delegates execution to the current implementation. When a smart contract is upgraded, the implementation address changes while the proxy address does not. This pattern provides an upgrade path for future feature additions without disrupting deployed positions or requiring counterparties to re-integrate.

The upgrade authority is role-gated. An upgrade transaction can be initiated only by a key holding the upgrader role, and that key is held under institutional controls that require multi-party authorization for any smart contract upgrade or configuration operation.

The production smart contract addresses on Ethereum mainnet are:

- AvitToken (proxy): `0xCcdc193AcF86160dDC79E20F7e471e53f2AF8Ecb`
- AvitControls (proxy): `0xCB90a6270cfac7aAeC36a2d17171D46A2137049a`
- Chainalysis Sanctions Oracle: `0x40C57923924B5c5c5455c48D93317139ADDaC8fb`

The Sepolia testnet deployments are:

- AvitToken (proxy): `0x4F7aeEcBfe25e5d6dc5150D69C76AA9ED52a6438`
- AvitControls (proxy): `0xFcA0b018E1eF2742493Fe91Ff6fdB5Dd72C75e3B`
- Sanctions oracle (test): `0x2C095A4e6550DD26D321314DC29A740A942776fd`

Block explorers render the current implementation behind each proxy, the historical implementations, every transaction, every event and every role assignment.

8.3 On-Chain Components

Hazel's on-chain surface comprises three smart contracts. Two are maintained by Custodia: AvitToken and AvitControls. The third is the Chainalysis sanctions oracle, maintained by Chainalysis and queried by AvitToken prior to every transfer.

AvitToken is Hazel Network's unified token smart contract for both tokenized deposits and stablecoins. It implements the ERC-20 standard interface for balance queries, transfers, allowances, and the corresponding events. Beyond the standard interface, the smart contract carries the operational logic for the network: consortium membership checks, reserve-cap enforcement, sanctions screening, and the operational controls for freeze, seize, and pause.

Every transfer through AvitToken is subject to three independent checks before settlement.

[7] Ethereum Improvement Proposal 1967, Proxy Storage Slots. `https://eips.ethereum.org/EIPS/eip-1967`.

[8] OpenZeppelin documentation, UUPSUpgradeable. `https://docs.openzeppelin.com/contracts/4.x/api/proxy`.

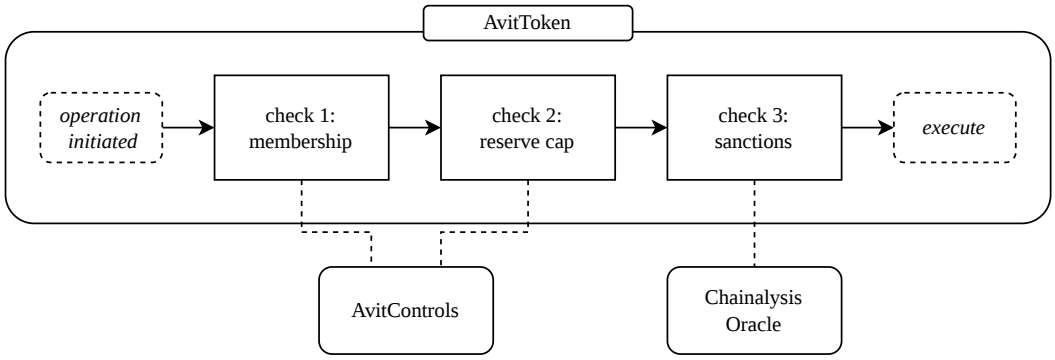

Figure 6: *AvitToken applies three independent checks to every transfer. All three must pass for the transfer to execute; any failed check reverts the transaction.*

The first check verifies consortium membership of sender and recipient. AvitToken queries AvitControls for each address and classifies the transfer into one of four cases (see Table 5). This classification determines whether the smart contract treats the resulting balance as a tokenized deposit or a stablecoin.

Table 5: *Transfer classification under the four consortium-membership cases.*

Transfer Type	Reserve Cap Check	External Supply Impact	Resulting Character
Consortium-to-consortium	Not applicable to Tokenized deposits	None	Tokenized deposit
Consortium-to-external	Applied	Increases	Stablecoin
External-to-consortium	No minting authority, therefore not applicable	Decreases	Tokenized deposit
External-to-external	No minting authority, therefore not applicable	None	Stablecoin

The reserve cap is the second check. For any transfer that would increase external supply, the smart contract automatically compares the resulting external supply against the programmatic reserve balance held in AvitControls. If the resulting external supply would exceed the reserve, the transfer reverts (a technical term: the smart contract automatically halts the transfer, so no tokens move). The AvitToken itself proactively ensures that it cannot become a liability without sufficient reserves for redemption. It also automates this Hazel Network operational control at the protocol level (a control that we had already implemented in our system prior to the infamous failure of internal controls by an incumbent stablecoin issuer in October 2025, which resulted in its unintentional minting of $300 trillion in unbacked stablecoins[9]. Again, this is no accident; Hazel Network's protocol is built by banks for banks, to actual standards required by banks).

Sanctions screening is the third check, performed against the Chainalysis sanctions oracle. AvitToken queries the oracle for both sender and recipient on every transfer. If either address appears on the oracle's list, the transfer reverts.

[9] *See* Paxos Accidentally Mints $300 Trillion, `https://finance.yahoo.com/news/paxos-accidentally-mints-300-trillion-223852659.html`.

Beyond transfers, the AvitToken smart contract supports mint, burn, sweep (consortium-to-consortium movement of tokens between member-bank addresses), freeze, seize, and pause. Each function is gated to a specific on-chain role (see Table 6). Each role is held by a Custodia-controlled private key under institutional controls. Every action is logged on-chain as a discrete, timestamped event.

Table 6: *On-chain roles in the AvitToken and AvitControls contracts.*

Role	Contract	Function
`UPGRADER_ROLE`	Both	Authorize contract upgrades
`MINTER_ROLE`	AvitToken	Mint tokens
`BURNER_ROLE`	AvitToken	Burn tokens
`SWEEPER_ROLE`	AvitToken	Move tokens between consortium addresses
`PROTECTOR_ROLE`	AvitToken	Freeze and seize addresses
`PAUSER_ROLE`	AvitToken	Pause and unpause the contract
`CONSORTIUM_MANAGER_ROLE`	AvitControls	Add and remove consortium members
`RESERVE_UPDATER_ROLE`	AvitControls	Update the declared reserve balance

AvitControls is the registry and reserve oracle that AvitToken consults on every transfer. It maintains two pieces of state: the consortium membership registry and the Custodia reserve balance.

The consortium membership registry is the list of on-chain addresses that the unified token treats as inside the consortium. It is updated through a role-gated function controlled by Custodia under Hazel Network's onboarding procedures. The registry is queried by AvitToken on every transfer.

The Custodia programmatic reserve balance is the declared value against which the token contract enforces out-of-consortium transfers. It is updated through a separate role-gated function. The smart contract trusts the declared value. The off-chain process that produces the declaration is gated by institutional controls and ties each declaration to a corresponding fiat settlement in the segregated reserve account.

AvitControls is UUPS-upgradeable under the same pattern as AvitToken.

The Chainalysis sanctions oracle is maintained by Chainalysis. Its address is set at AvitToken initialization and can be updated through a role-gated function if Chainalysis migrates in the future to a new address or if Hazel Network decides to adopt a replacement oracle down the road.

The three smart contracts together execute Hazel's reserve discipline, operational controls and compliance posture *at the protocol level*. AvitControls supplies the state and AvitToken applies the rules on every transfer, with the Chainalysis oracle providing the final sanctions filter. This is Hazel's programmability layer: the network's rules encoded as smart contract functions that execute as part of settlement.

9. Legal Structure

Hazel Network has a simple philosophy: tear down walls. Users should not be trapped inside walled gardens; instead, the network should be designed to maximize utility in lawful commerce. In the legal context, this means breaking through a legal wall inherent to incumbent stablecoins that poses a problem for their integration into traditional finance.

Before describing the inherent problem, here is a reminder: when Hazel Network users hold tokens within the consortium boundary, legally the tokens are bank deposits – with all of the rights and benefits that come with being a deposit holder (including take-free rules and FDIC insurance). Outside the consortium boundary, legally the tokens are stablecoins designed to comply with the GENIUS Act, subject to comprehensive regulation and providing holders with rights to the stablecoin reserves.

The inherent problem with the incumbent stablecoins to which we refer pertains to their treatment under commercial law.

The Problem:

Stablecoins today suffer from a legal barrier that prevents their true integration with the traditional banking system: no one can be certain that the stablecoin they own is free and clear of someone else's valid legal claim to that same stablecoin. In the crypto parlance, that's known as a "double-spend problem." Incumbent stablecoins have generally not solved the legal problem of ensuring that their users can buy their stablecoin free and clear of competing claims to it, such as a pre-existing lien.

Thankfully, the beginnings of a TradFi solution to this well-known legal problem with stablecoins was formally proposed in 2022 when the Uniform Law Commission proposed UCC Article 12 for "Controllable Electronic Records."[10] Commercial law in the US is defined by the States, not by Congress; a majority of US States[11] have enacted UCC Article 12 since 2022 – but many important States, such as Texas, have not. Moreover, some of the key States that have adopted UCC Article 12 chose to enact a non-uniform version of it, expressing concerns about misinterpreting it as tacit approval of a central bank digital currency ("CBDC").

So, while UCC Article 12 would solve the problem if it were already uniformly enacted by all US States, that isn't the case today, and may not ever be.

To solve this problem, stablecoin issuers have two basic choices:

1. Hope for the Best: Issue the token as a traditional stablecoin and hope that any adverse claims are brought in States that have adopted UCC Article 12; or
2. Maximize Utility: Adopt the hybrid solution chosen by Hazel Network, described below, which applies take-free protections to deposit accounts inside the consortium boundary and which we believe maximizes the utility of Avits under the greatest number of States' commercial laws outside the consortium boundary by maximizing the ***negotiability*** of Avit – in other words, by maximizing its transferability from one owner to another with minimal legal friction.

[10] Uniform Law Commission, UCC. https://www.uniformlaws.org/acts/ucc.

[11] Uniform Law Commission, enactment tracker for UCC Article 12. https://www.uniformlaws.org/committees/community-home?CommunityKey=1457c422-ddb7-40b0-8c76-39a1991651ac.

The Solution:

Hazel Network chose to use a legal structure for Avits that traditional banks will readily recognize: ***Avit is a negotiable instrument***, akin to a digital cashier's check and designed to confer the same rights and obligations as negotiable instruments that banks handle every day.

Here are the building blocks Hazel Network uses to achieve this result. Lawyers will spot key elements sourced from UCC Article 3 (Negotiable Instruments) and the Uniform Electronic Transactions Act.

Custodia agrees that Avit is a "Transferable Record" pursuant to Section 16 of the Uniform Electronic Transactions Act. As a Transferable Record, Avit is designed to provide rights and defenses for the purchaser of a negotiable instrument as set forth in the Uniform Commercial Code, which are commonly referred to as holder-in-due-course protections and which protect such purchaser from certain defenses and claims related to a prior purchaser of the negotiable instrument.

The terms of each Avit (the "Avit Terms"), as a Transferable Record, can be found in the source code of the implementation contract (via the proxy contract), located here: `https://eth.blockscout.com/address/0xCcdc193AcF86160dDC79E20F7e471e53f2AF8Ecb`.

As described in the Avit Terms, Custodia unconditionally promises to pay Holder one (1) U.S. dollar to redeem one (1) Avit on demand upon an Instruction from Holder and Delivery of one (1) Avit to Custodia. An Avit "Holder" controls the private key for the particular Blockchain Address at which an Avit is located. Custodia's obligation to redeem this Avit for one (1) U.S. dollar applies only to Holder. For definitions of capitalized terms, please refer to the Avit Terms.

Custodia is at all times subject to applicable Law, including, without limitation, that any Avit may be forfeited or subject to forfeiture to, or seizure by, a law enforcement agency, if the Avit has been or is being used for illegal activity or is subject to a legal order or other process, and that any Avit subject to such forfeiture or seizure, or that is otherwise subject to freezing or any similar limitation or use, may be wholly and permanently unrecoverable and unusable and may, in appropriate circumstances, be destroyed.

For more information, please refer to the terms of each Avit located in its source code.

10. Economic Model

The economic case for joining the Hazel Network is straightforward. Hazel Network is faster and cheaper than standard payment rails banks use today, and the savings accrue to both the bank and its customers. Tokenized deposit transfers between member banks do not incur a stablecoin issuer's spread, and do not require intermediary payment along the way. The dollar moves at par.

The serviceable addressable market for Hazel is approximately $6.8 trillion in US demand deposits, and the total addressable market extends to roughly $19 trillion across total US commercial deposits over the longer horizon.

Table 7: *Market context: scale of the US deposit base, payment-cost landscape, and stablecoin activity.*

Metric	Value	Source
US demand deposits	∼$6.8 trillion	FRED, Federal Reserve Bank of St. Louis[12]
US commercial deposits	∼$19 trillion	FRED, Deposits, All Commercial Banks[13]
Annual ACH volume (2025)	∼$93 trillion	Nacha ACH Network Statistics[14]
Wire transfer fee	$25–30 domestic; ∼$50 international	Bankrate, 2025[15]
Cross-border payment cost	1.6–6.4% per transfer	McKinsey Global Payments Report[16]
Stablecoin market cap (May 2026)	∼$322 billion	CoinMarketCap stablecoin index[17]

Against such scale and legacy costs, conventional payment infrastructure imposes a meaningful drag. Wire transfers carry per-transaction fees of $25–30 domestically and around $50 for international transfers, while cross-border payments cost 1.6–6.4 percent per transfer on average. Even bank-to-bank transfers are expensive compared to Hazel Network – and the automation offered by Hazel Network also enables banks to cut back-office costs. Cross-border transfers add foreign exchange costs on top. These costs compound at every step, and Hazel Network removes most of them since the dollar does not require conversion or intermediation to move between member banks.

The design of the Hazel Network passes savings to both sides of the bank-customer relationship.

Hazel's economics improve member banks' margins per transaction. A member bank routing payments through Hazel pays less than it currently pays for the same payment movement through conventional infrastructure, so unit economics are designed to improve from the first transaction. Hazel's revenue-sharing model returns network fees to participating banks in proportion to their activity. As volume grows, each bank's net cost of using the network falls toward zero. At sufficient scale, the revenue share is designed to flip to accretive.

Vantage handles network membership and onboarding. Custodia operates all on-chain infrastructure, relieving member banks of on-chain fees ("gas"), key management, and blockchain operations. The infrastructure providers earn at scale; member banks earn improved unit economics from day one and accretion as the network grows.

[12]Federal Reserve Bank of St. Louis, FRED, Demand Deposits. https://fred.stlouisfed.org/series/DEMDEPSL.

[13]Federal Reserve Bank of St. Louis, FRED, Deposits, All Commercial Banks. https://fred.stlouisfed.org/series/DPSACBW027SBOG.

[14]Nacha, ACH Network Volume and Value Statistics. https://www.nacha.org/content/ach-network-volume-and-value-statistics.

[15]Bankrate, Wire Transfer Fees, 2025. https://www.bankrate.com/banking/wire-transfer-fees/.

[16]McKinsey & Company, Global Payments Report. https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-report.

[17]CoinMarketCap, Stablecoin Market Cap. https://coinmarketcap.com/view/stablecoin/.

In sum, Hazel Network is designed for scale rather than collecting rents on each transaction. A bank participating in Hazel captures more of the primary banking relationship, more of the on-ramp economics, and more of its customer's payment activity than non-participant banks.

11. The Sidecore Thesis

The architecture of US payment systems reflects a 1970s decision to manage scale through middleware. Faced with roughly 10,000 master-account holding financial institutions[18], the Federal Reserve chose to require them to connect through a small number of Fed-preferred technology providers rather than offering direct connectivity for every institution. Today, three companies (FIS, Fiserv, and Jack Henry)[19] intermediate payments for the vast majority of those banks, and they do so using proprietary integrations. Banking therefore stands in stark contrast to securities markets, where broker/dealers integrate with their clearinghouse, the Depository Trust & Clearing Corporation ("DTCC"), using the open Financial Information eXchange ("FIX") standard for trade matching. Banks, in stark contrast, integrate with their clearinghouse, the Fed, through closed-source and proprietary middleware providers (with the exception of the largest institutions, which the Fed allows to connect directly[20]). Community banks, regional banks, and credit unions must pay for a proprietary ledger with substantial switching costs and an innovation cadence they do not set themselves.

The results speak volumes: compare the technology capabilities of the securities versus payments industries since FIX was introduced in 1995; it's clear which of the two industries won the technology race.

While the Fed's decision to limit the number of approved integrators was considered a reasonable engineering choice in its era, it now serves as a punitive constraint. Over time, the three banking core providers grew in scale and pricing power, alongside the Fed's dependence on the three-provider model. Small institutions pay licensing and integration fees for systems whose roadmaps reflect the collective installed base rather than the priorities of any single customer. Innovation moves at the pace of the middleware roadmap. A community bank that wants to offer a new product must wait for its core to support it.

Hazel Network is a sidecore. This means it runs alongside banks' existing cores, rather than in lieu of them. A Hazel Network member bank can leave its existing core in place; its general ledger also does not need to change. What does change is the bank's payment path to settlement infrastructure: rather than routing all payments through the existing three-provider concentration, the bank can now move some of its activity through Hazel and onto programmable on-chain rails.

[18] Federal Reserve, Master Account and Services Database. `https://www.federalreserve.gov/paymentsystems/master-account-and-services-database-about.htm`.

[19] FIS, `https://www.fisglobal.com/`. Fiserv, `https://www.fiserv.com/`. Jack Henry, `https://www.jackhenry.com/`.

[20] Federal Reserve Financial Services, FedLine Solutions. `https://www.frbservices.org/fedline-solutions`.

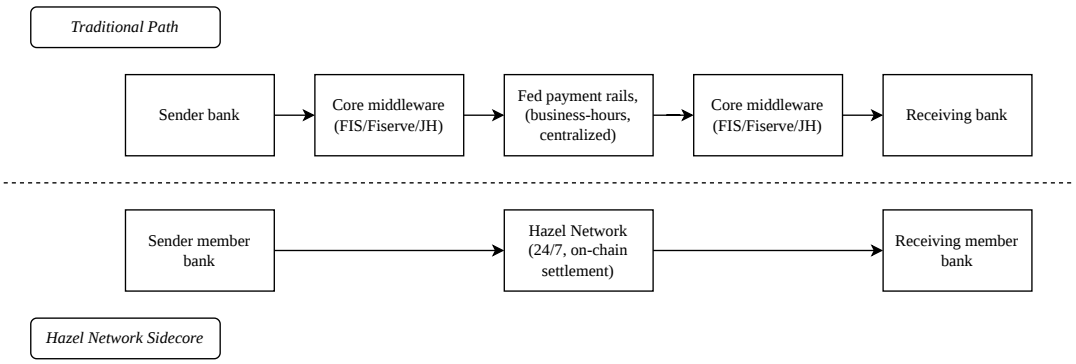

Figure 7: *A payment from one bank to another under the traditional path routes through two core middleware vendors and the Federal Reserve before reaching the recipient bank. Under the sidecore path, the same payment moves between member banks through the Hazel Network.*

Hazel Network adds a path rather than replacing the core. A bank can offer Hazel for payments demanding programmable settlement, and continue to use its core for everything else. Over time, the proportion of the bank's activity that benefits from sidecore routing rather than core routing is likely to grow. The middleware layer will thin over time as that proportion increases. Banks gain a choice they did not have before; customers can vote with their feet.

In a five-year horizon, *we believe banks will rely far less on their cores than they do today.* Settlement activity will migrate increasingly to on-chain rails. The cores will remain useful for general-ledger and customer-facing systems where they have advantages, but lose ground to programmable payments. The middleware concentration that has defined US banking for fifty years becomes one architecture among several, rather than the only one.

Hazel Network offers banks a path to programmable settlement that does not require banks to leave their existing systems behind.

Further, we anticipate whole new markets, such as payment routing optimization businesses, will be created in the coming five years. That is exactly what happened in the securities industry once FIX was introduced. A whole new class of fintechs cropped up to allow asset managers to optimize for their particular needs for each individual trade (i.e., fast execution, low bid-offer spreads, privacy). This is coming to payments next. Soon.

We welcome technology-forward members of Hazel Network to build such new applications on top of our open protocol, as well as to monetize your software by selling it to the Network. Such flexibility is a key reason why we architected Hazel Network as a sidecore, with our initial implementation on Ethereum and with bank-level operational and compliance controls embedded at the protocol layer of our system. Let's tear down walls together!

12. Hazel Network Enables Banks to Engage in Agentic Payments

Agentic commerce is the use of autonomous AI agents to act on a person's or organization's behalf: anticipating needs, comparing options, negotiating terms, and completing payments. It represents a structural shift in how value moves between consumers and merchants, and the projected scale of agentic commerce is substantial.

Table 8: *Agentic commerce market projections.*

Source	Projection by 2030
McKinsey (2025)[21]	US B2C agentic commerce: ∼$1 trillion; global: $3–5 trillion
Bain (2025)[22]	US agentic commerce: $300–500 billion (15–25% of US e-commerce)

Conventional banking payment rails were not designed for agent-initiated activity. Per-transaction fees, batch cycles, and the constraint of regular business hours prevent legacy payment rails from meeting the demand. An autonomous agent transacting on a customer's behalf needs settlement that is near real-time, programmable, and continuously available. The infrastructure that supports today's payments was built for a different kind of customer.

Stablecoins and tokenized deposits both enable programmatic settlement, support per-transaction granularity at scale, and integrate natively with the emerging agent-payment protocols such as Google's Agent Payments Protocol, Coinbase's x402, and Stripe's Agentic Commerce Protocol. Different use cases call for different forms. A tokenized deposit fits when the customer wants funds to remain on the originating bank's balance sheet during the agent's activity, and a stablecoin fits when the agent transacts with parties outside the consortium.

Hazel Network is built for compatibility with ISO 20022[23], the structured-data standard underpinning both modern bank messaging and agentic payment systems.

Agentic commerce raises a governance question that has not existed at scale before. How does a customer authorize an agent to transact on their behalf while preventing the agent from spending too much, interacting with the wrong counterparties, or executing transactions the customer never approved? Guardrails of this kind are difficult to enforce inside the agent itself but are straightforward to enforce at the money layer, and Hazel has already automated such functions into the smart contracts. Hazel supports smart treasury (smart contracts that execute logic based on conditionals). A transaction can be required to meet predefined limits, counterparty whitelists, or time-of-day constraints before it settles. Governance is baked into the rails rather than bolted on after the fact.

Banks face a strategic choice. If they do not offer a stablecoin-based path for their customers' agentic activity, that volume will flow to non-bank stablecoin issuers – and core deposits with it. Banks that depend on customer deposits, transaction fees, or treasury services are exposed to the same disintermediation dynamic already present in the broader stablecoin space, but accelerated by the velocity and scale of agent-mediated commerce.

[21] McKinsey & Company, "The agentic commerce opportunity: How AI agents are ushering in a new era for consumers and merchants," October 2025. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-agentic-commerce-opportunity-how-ai-agents-are-ushering-in-a-new-era-for-consumers-and-merchants.

[22] Bain & Company, "2030 Forecast: How Agentic AI Will Reshape US Retail," December 2025. https://www.bain.com/insights/2030-forecast-how-agentic-ai-will-reshape-us-retail-snap-chart.

[23] ISO 20022. https://www.iso20022.org/.

Hazel Network gives banks a path that keeps agentic activity within the banking system. Any member bank's tokenized deposit account holder can receive Avit-denominated agentic payments without leaving the bank. The compliance pipeline that programmatically pre-screens every transfer on the network applies equally to agent-initiated transactions: sanctions checks, reserve enforcement, and the operational controls all execute at the smart contract level; wallet screening and, as applicable, transaction screening, are automated by the Hazel Network platform. Hazel Network allows agents to transact on bank-grade compliance rails.

The architecture extends beyond agent-initiated payments. Any application that transacts in Avit inherits the same on-chain compliance protections. The same on-chain checks that protect human-initiated transfers protect agent-initiated and application-initiated transfers as well. Hazel enables open-ended development of software applications that, by definition, run on bank-grade compliance rails. Agentic payments are the most immediate application of this property, though the architecture supports many others.

a16z co-founder Marc Andreessen recently tongue-in-cheek warned[24]: *"If you don't give [your AI agent] a bank account, it's just going to break into your bank account anyway. And take your money. So you might as well do it."*

He was only half-joking.

That's Hazel Network's message to banks too. Agentic payments are coming. So you might as well do it. Hazel Network has already built a system that enables banks to do it – to offer this service to customers – in a compliant way. Join us.

13. Conclusion

Hazel Network is a joint platform of member banks, a settlement bank, a blockchain infrastructure provider designed to be a GENIUS Act-compliant stablecoin issuer, and a platform provider. When the unified token is held inside the consortium, it is a tokenized deposit issued by a chartered US bank. When it is held outside the consortium, the same on-chain balance is a stablecoin issued by Custodia, designed to comply with the GENIUS Act.

One smart contract, one balance, two legal characters.

The design reflects a banking standard. Reserves are mapped one-to-one and enforced by the smart contract for every out-of-consortium transfer. Compliance runs automatically at the protocol level, with three independent screening layers executing before any transfer settles: fiat-side checks at initiation, blockchain compliance screens on every wallet, and an on-chain query to the sanctions oracle. Member banks retain the customer relationship and the obligor role for their deposits. Custodia is the obligor for the stablecoin form, backed one-to-one by segregated reserves.

Participation scales with operational appetite. A bank can participate through the Basic model with no integration on its side, through the Advanced model with scheduled file feeds into its core and compliance systems, or through the Enterprise model with real-time API integration and the ability to build programmable products on the settlement layer. The same smart contracts, compliance protections and network rules apply across all three.

[24] Latent Space: Marc Andreessen introspects on The Death of the Browser, Pi + OpenClaw, and Why "This Time Is Different." `https://www.latent.space/p/pmarca`.

As a sidecore, Hazel runs alongside a bank's existing infrastructure. It adds a path to programmable settlement that does not require the bank to leave its core, its general ledger or its existing payment rails. Banks join on terms that fit their operations today and gain a route to settlement properties that legacy rails were not built to provide: round-the-clock availability, atomic execution, real-time auditability, and a customer relationship that survives the on-chain boundary.

Hazel Network is live on Ethereum mainnet. Programmatic and agentic payments inherit the same automated compliance protections as any other transfer through the network. The architecture is open to new member banks, new implementations, and new applications that meet the network's standards. Banks that join early shape the standards by which the consortium expands.

Disclaimer

This white paper is provided solely for informational purposes to describe the design and operation of the Hazel Network and the unified token. The information contained herein reflects current views as of the date of publication and is subject to change without notice. No representation or warranty, express or implied, is made as to the accuracy, completeness, or reliability of the information contained in this white paper.

This white paper does not constitute an offer to sell, or the solicitation of an offer to buy, any token, security, deposit, or other instrument, and does not constitute investment, legal, tax, accounting, or other advice. It should not be relied upon as the basis for any investment, commercial, or other decision. The regulatory environment surrounding digital assets and blockchain technology continues to evolve. Readers are encouraged to independently review the applicable laws and regulations and to consult their own legal, financial, tax, and regulatory advisers before taking any action related to the concepts described herein. This white paper is intended for institutional audiences and is not an offer of any retail product or service.

When held inside the consortium by an onboarded member bank, the unified token is a bank deposit at the member bank, subject to FDIC insurance limits and aggregation rules applicable to deposits at that institution. When held outside the consortium, the unified token operates as a stablecoin issued by Custodia Bank, Inc. and designed to comply with the GENIUS Act; the stablecoin form is not FDIC-insured. No statement in this white paper should be treated as a promise or representation regarding the future availability, functionality, transferability, liquidity, value, legal treatment, regulatory classification, or market for the unified token or the Hazel Network.

This white paper contains forward-looking statements, including statements regarding the design, development, expected functionality, market opportunity, anticipated participation, and potential utility of the Hazel Network and the unified token. Any forward-looking statements are based solely on current expectations and assumptions and should not be relied upon as predictions of future events or outcomes. Custodia and Vantage Bank undertake no obligation to update or revise any forward-looking statement to reflect subsequent events, developments, or changes in circumstances, except as required by applicable law.

Custodia Bank, Inc. is a Wyoming-chartered Special Purpose Depository Institution supervised by the Wyoming Division of Banking. Deposits held at Custodia Bank are not insured by the Federal Deposit Insurance Corporation (FDIC). Vantage Bank is a Texas-chartered, FDIC-insured commercial bank supervised by its primary federal and state regulators. Each entity acts within its respective charter and supervisory framework. References to third-party platforms, vendors, and service providers (including Ethereum, Chainalysis, OpenZeppelin, and Infinant) are descriptive and do not constitute endorsement; these relationships are subject to change. Features, parameters, and operational specifications described herein may be modified, subject to applicable regulatory requirements and contractual obligations.

The Hazel Network and the unified token are designed for use within the United States by institutional participants. References herein to regulatory frameworks (including the GENIUS Act, FDIC insurance, and Wyoming SPDI supervision) apply solely to United States law. The distribution of this white paper may be restricted by law in certain jurisdictions. The Hazel Network may not be available in jurisdictions where its offering is restricted or prohibited. It is the responsibility of the reader to ensure compliance with the laws and regulations applicable to its jurisdiction.

Custodia, Vantage Bank, and each of their respective affiliates, subsidiaries, parent entities, directors, officers, employees, partners, representatives, advisers, contractors, and agents expressly disclaim any and all liability for losses or damages arising from the use of or reliance on this white paper or its contents, including any consequential, special, or similar damages, even if advised of the possibility of such damages. Users, counterparties, and prospective member institutions are responsible for their own regulatory compliance.