ChainIT Transaction Truth

Stablecoins, Web3 Wallets, and Multi-Rail Commerce

A Zero-Trust Control Plane for Verified Identity, Organizational Authority, Runtime Compliance, Secure Wallet Execution, and Immutable Settlement Evidence

CHAINIT®

Executive White Paper

CIT-TT-EWP-2.1

Executive Core Edition

September 17, 2026

Companion documents: ChainIT Provable Authority (CIT-PA-WP-7.0); ChainIT Provable Compliance (CIT-PC-WP-4.0); and the ChainIT Transaction Truth Technical and Compliance Companion (CIT-TT-TCC-2.1).

Authors

Dr. Eric Tacl, Executive Vice President- Verified Payments and Commerce
Matthew Koepp, Chief Technology Officer
Tim Hines, Chief Product Officer
Russell Lessard, Chief Compliance Officer
Jason Patrick, Chief Commercial Officer
Jeremy Blackburn, Chief Executive Officer

This paper describes the ChainIT Transaction Truth Architecture at an executive and governance level. Detailed protocol, wallet, MPC, compliance, threat-model, and implementation-status material remains in the companion technical paper. This document does not constitute legal, regulatory, banking, custody, accounting, security-certification, or patentability advice.

© 2026, Scientia Potentia Est II, LLC. All rights reserved.

Publication Notice

This white paper and the information contained herein are the exclusive property of Scientia Potentia Est II, LLC and are protected by United States and international copyright laws.

Permission is granted to recipients to access, view, download, print, and retain copies of this white paper solely for personal, informational, or internal business purposes. Recipients may share an unmodified copy of this white paper in its entirety, provided all copyright and proprietary notices are retained and no fee is charged for distribution.

Except as expressly permitted, no part of this publication may be reproduced, distributed, transmitted, displayed, published, modified, translated, reverse engineered, incorporated into other works, or used for commercial purposes without the prior written consent of Scientia Potentia Est II, LLC.

No license, whether express, implied, by estoppel, or otherwise, is granted to patents, patent applications, copyrights, trademarks, trade secrets, or other proprietary rights except for the limited right to access and use this white paper as stated above.

> **Document precedence: CIT-PA-WP-7.0 controls shared Authority Protocol definitions and flows. CIT-PC-WP-4.0 controls shared Provable Compliance definitions and flows. The ChainIT Transaction Truth Technical and Compliance Companion, CIT-TT-TCC-2.1, controls the detailed wallet, MPC, execution, threat-model, schema, and architecture-status material. This executive paper does not modify those documents.**

Architecture status is stated by class: current platform foundation, published protocol architecture, development or MVP, proposed execution profile, and external dependency. This edition does not represent that every described component is generally available in every environment.

Contents

Document Precedence and Key Terms 5

Executive Summary 8

1. Market Transition: New Rails, Same Commercial Obligations 9

1.1 A multi-money operating environment 9

1.2 Stablecoin, blockchain, and wallet are distinct components 9

1.3 Stablecoins and tokenized deposits remain legally and economically distinct 9

2. The Control Gap: A Wallet Signature Is Not a Complete Authorization 10

2.1 Cryptographic validity answers a narrow question 10

2.2 Address identity is not legal identity 10

2.3 Authentication is not authority 10

2.4 Compliance is not a permanent badge 10

2.5 Network confirmation is not complete commercial settlement 11

3. ChainIT Strategic Position 11

3.1 Control the transaction, not the monetary instrument 11

3.2 Agnostic by architecture, selective by policy 11

3.3 The commercial value resides above and across the rail 11

4. How the Transaction Truth Architecture Operates 13

4.1 Four planes, one transaction 13

4.2 Execution is conjunctive 13

4.3 Executive transaction sequence 13

4.4 Non-negotiable zero-trust invariants 14

5. Individual and Organizational Wallet Transactions 14

5.1 The control model is subject-neutral, but the authority source differs 14

5.2 Organizational governance and cryptographic signing are orthogonal 15

5.3 Agent and scheduled-workflow initiation 15

6. Wallet and Custody Profiles 15

6.1 A wallet is a profile, not a single product category 15

6.2 MPC and Nitro Enclaves: custody security, not business authority 16

7. Runtime Compliance and Stablecoin Qualification 17

7.1 Compliance evidence remains attributable, current, and purpose-specific 17

7.2 Compliance does not confer authority 17

7.3 Stablecoin and Web3 transaction evidence domains 18
7.4 Regulatory perimeter remains activity-specific 18
7.5 Privacy and disclosure 18
8. Exact-Transaction Execution 19
8.1 Approval must follow the transaction, not merely the session 19
8.2 Canonicalization and digest 19
8.3 Decision, approval, reservation, and EAC 19
8.4 Asset, chain, destination, and contract qualification 19
9. Settlement, Reconciliation, and Immutable Evidence 20
9.1 Finality occurs in layers 20
9.2 Pactvera, lifecycle VDTs, and Valitorum 21
9.3 Dual-ledger privacy and selective disclosure 21
9.4 Refunds and later exceptions 21
10. Illustrative Commercial Use Cases 22
10.1 What changes for the customer 22
11. Business Value, Competitive Position, and IP Foundation 22
11.1 From wallet utility to enterprise control surface 22
11.2 Revenue across the transaction stack 23
11.3 Competitive differentiation 23
11.4 Intellectual-property foundation 23
12. Controlled Deployment and Governance 24
12.1 Architecture status 24
12.2 Phased deployment 24
12.3 Pilot success means invariants hold under attack and failure 25
13. Conclusion 25
References and Source Basis 27
Important Notices 29

Document Precedence and Key Terms

Authority definitions control. ChainIT Provable Authority, CIT-PA-WP-7.0, controls every shared authority term, subject classification, credential, decision artifact, and pre-execution process used in this paper. The Authority Protocol applies to individual, organizational, group, scheduled-workflow, and registered-agent activity across fiat, card, instant-payment, stablecoin, and on-chain transactions. [1]

Compliance definitions control. ChainIT Provable Compliance, CIT-PC-WP-4.0, controls every shared compliance artifact, evidence class, policy profile, disposition, freshness rule, and disclosure boundary used in this paper. A Compliance Decision Validated Data Tokens (VDT) supplies one signed, time-bounded predicate to the Authority Protocol. It does not create authority and does not independently authorize payment. [2]

Naming hierarchy and technical companion. ChainIT Transaction Truth is the umbrella name; the ChainIT Transaction Truth Architecture is the formal technical reference; and the Transaction Truth control plane is the functional pre-execution layer. CIT-TT-TCC-2.1 controls wallet profiles, MPC, exact-transaction mechanics, asset and chain controls, the threat model, pilot criteria, canonical object schemas, the ChainIT Wallet Execution Profile, and implementation status. [3][4]

Term	Executive meaning
Allow	The final compliance disposition assigned by the organization's Workflow Engine when every predicate required by the applicable Compliance Policy Profile has returned a current, reason-coded true result. Allow is one of the enumerated dispositions of the Compliance Protocol, alongside Allow with Controls, Step-Up, Review, Hold, Reject, Prohibit, and Stale/Unknown. Only a final Allow sets Compliance Decision Permits to true in the Authority Protocol. Allow permits compliance-side continuation for one reliance event only; it does not establish identity, confer authority, cure an altered digest or exceeded limit, or authorize execution. Any disposition other than Allow, including missing, stale, ambiguous, or contradictory evidence, is a controlled non-Allow state and stops the transaction from proceeding on the compliance side.
Authority Resolution Pactvera (ARP)	The canonical, versioned organizational authority record: who may act, in what role, for what purpose, within what limits, during what period, under what quorum or separation-of-duties requirements, and subject to what amendment or revocation?
Authority Policy Profile (APP)	The versioned authority-side rule set selected for a reliance event, varying by organization, role, subject, counterparty, transaction, value, rail, jurisdiction, risk tier, and purpose.
Authority Protocol	The complete pre-execution process by which a verified subject's present authority to perform one exact action is resolved from the Authority Resolution Pactvera under the applicable Authority Policy Profile, combined with the Compliance Decision, required approvals, and capacity reservation, and expressed as an Execution Authorization Credential. The Authority Protocol determines who may act; it is distinct from the Authority Policy Profile, which is the versioned rule set the Protocol applies at a given reliance event.
Compliance Policy Profile (CPP)	The versioned compliance-side rule set selecting required evidence, freshness bounds, predicates, review conditions, disclosure rules, and transaction-specific controls.

Term	Executive meaning
Compliance Protocol	The runtime evaluation of current evidence against the applicable Compliance Policy Profile described as “Provable Compliance,” produces a transaction-specific, time-bounded decision from current evidence and policy.
Business Rules Engine (BRE)	The deterministic predicate-evaluation engine. It returns explicit, reason-coded true or false results; it does not assign the organization's final disposition.
Compliance Decision VDT	A signed, time-bounded, purpose-specific record of the organization-controlled compliance disposition for one reliance event.
Canonical Transaction Digest	A deterministic hash of the exact transaction object under a fixed encoding rule so any material change produces a different digest.
Evidence Assertion VDT	A signed, time-stamped record of a single compliance fact, such as "this person passed identity verification on this date" or "this entity was screened against the sanctions list with no match." Each one records where the fact came from, when it was observed, how long it stays valid, what it was gathered for, and how confident the source was. These records are the evidence the compliance process weighs; the decision itself is recorded separately as a Compliance Decision VDT.
Execution Authorization Credential (EAC)	A short-lived, audience-restricted, single-use credential authorizing one exact transaction, bound to the digest, reservation, subject or session, status, and expiration.
GENIUS Act	Guiding and Establishing National Innovation for U.S. Stablecoins Act.
Multi-Party Computation (MPC)	A cryptographic custody technique in which a private key is never assembled in one place; instead, the key is split into shares held by separate parties or systems, and a defined threshold of those shares must cooperate to produce a valid signature. MPC reduces single-key compromise risk and allows signer distribution across infrastructure, custodians, or devices. In the Transaction Truth Architecture, MPC operates only within the wallet and custody plane: satisfying the cryptographic signing threshold is independent of, and never substitutes for, verified identity, organizational authority under the ARP, a current compliance decision, or an exact-digest match.
Wallet Execution Profile (WEP)	The versioned wallet-specific control profile governing custody model, signer requirements, asset and chain scope, recovery, limits, destination policy, and evidence.
Pactvera / VDT / Valitorum	Pactvera governs transaction logic; VDTs record validated data, decisions, and lifecycle events; Valitorum seals the completed or otherwise terminal evidence chain without rewriting prior records.
Reliance Event	The moment a party relies on identity, authority, evidence, policy, or transaction state. Freshness and present eligibility are evaluated at that moment, not inherited indefinitely from onboarding.

Term	Executive meaning
Session Credential	The token or cookie a system issues after a user logs in so that it can recognize the user across subsequent requests without re-authentication. It proves only that an earlier login succeeded. In the Transaction Truth Architecture, a session credential never authorizes a payment; authorization requires a separate Execution Authorization Credential bound to the exact transaction.
Transaction Truth Architecture	The zero-trust control, execution, and evidence architecture that binds verified identity, current authority, transaction-specific compliance, the exact transaction digest, qualified wallet execution, settlement, reconciliation, and sealed evidence across four independently evaluated planes, so that value moves only on a commercially authorized transaction and the result is provable.

Five boundaries remain separate: 1) control of a key is not identity; 2) identity is not organizational authority; 3) authority is not compliance; 4) compliance is not execution authority; and 5) network confirmation is not complete commercial settlement.

Executive Summary

Stablecoins can transfer value continuously across programmable networks. Web3 wallets can authorize those transfers through cryptographic signatures. Neither capability, standing alone, establishes a complete commercial transaction.

A blockchain may prove that a transaction satisfied certain rules. A wallet may prove that sufficient cryptographic authority existed to sign it. Those facts do not independently prove who initiated the transaction, for which legal entity, under what current authority, against which compliance evidence, subject to what business terms, or whether the merchant ultimately received and reconciled the intended economic value.

> **Stablecoins and tokenized deposits are settlement instruments. Web3 wallets are cryptographic execution endpoints. ChainIT supplies the verified identity, organizational authority, runtime compliance, exact-transaction control, secure execution, multi-rail orchestration, reconciliation, and immutable evidence required to make them commercially usable.**

ChainIT addresses the gap through the ChainIT Transaction Truth Architecture: a zero-trust control, execution, and evidence architecture connecting ChainIT ID, ChainIT Org ID, the Authority Resolution Pactvera, Provable Compliance, exact-transaction decisioning, secure wallet execution, ChainIT Pay, Pactvera, lifecycle VDTs, ERP integration, and Valitorum.

Three controlling propositions

First, the wallet is downstream of authority and compliance. ChainIT ID and ChainIT Org ID validate the relevant person and entity. The ARP and APP resolve whether the individual, group, scheduled workflow, or registered agent may perform the proposed action. The Compliance Protocol produces a transaction-specific, time-bounded decision from current evidence and policy. Only the complete Authority Protocol can authorize execution. [1][2]

Second, approval is bound to the exact instruction eventually signed. The payer, source, payee, destination, amount, asset, chain, token contract, fees, validity window, nonce, and other material parameters are canonicalized and hashed. Human or quorum approval applies to that digest. Capacity is reserved. A one-time EAC is issued. The wallet boundary reconstructs the digest and rejects any mismatch, replay, wrong audience, stale decision, or expired authorization.

Third, custody security and governance security are independent controls. MPC and threshold cryptography can reduce single-key compromise risk. Confidential-computing environments can isolate sensitive signing operations and attest approved code. Neither establishes legal or organizational authority. Conversely, a valid corporate approval does not create a blockchain signature. A controlled transaction requires both governance approval and qualified cryptographic execution.

> **Commercially Authorized Transaction = Verified Subject AND Current Authority AND Compliance Decision Permits AND Exact Digest Match AND Required Approvals AND Capacity Reserved AND Qualified Wallet Execution**

The resulting model is issuer-agnostic, chain-agnostic, wallet-agnostic, bank-compatible, tokenized-deposit compatible, and multi-rail. It is not indiscriminate. Each asset, issuer, token contract, chain, bridge, wallet profile, custodian, bank, liquidity provider, and settlement path remains subject to qualification and current policy.

ChainIT therefore does not need to predict which stablecoin, blockchain, bank token, custodian, wallet, or instant-payment system will dominate. ChainIT can monetize the verified control, execution, and evidence layer across every qualified rail.

1. Market Transition: New Rails, Same Commercial Obligations

1.1 A multi-money operating environment

Enterprise payments are moving toward a hybrid environment in which cards, Automated Clearing House (ACH), wires, instant bank payments, stablecoins, tokenized deposits, internal ledgers, and future tokenized-money instruments coexist. Different instruments will remain useful for different purposes. Consumer credit, rewards, dispute rights, bank settlement, cross-border availability, programmability, operating hours, and cost do not collapse into one universal rail.

Stablecoins can improve speed, programmability, cross-border reach, and continuous availability. Tokenized deposits can provide bank-native digital settlement. Neither eliminates the commercial duties attached to identity, authorization, sanctions, contractual performance, custody, accounting, tax, audit, or dispute handling.

1.2 Stablecoin, blockchain, and wallet are distinct components

Market shorthand often calls stablecoin a payment rail. It is more precise to separate three components. The stablecoin is the settlement asset: a liability of its issuer that represents the value being transferred. The blockchain is the rail: the shared ledger that records and moves that value from one holder to another. The wallet is the control point: the software or service that holds the keys and signs the instruction to move it. These three layers may be supplied by different organizations, and each carries different legal, operational, and risk characteristics.

Component	Primary function	Unresolved without Transaction Truth controls
Stablecoin issuer	Issues and redeems the asset; administers reserves, token contracts, and issuer controls.	Does not inherently prove the payer's legal identity, corporate authority, commercial purpose, performance, or ERP result.
Blockchain or network	Orders transactions and updates ledger state according to protocol rules.	Does not inherently know the legal parties, governing contract, organizational approvals, or off-chain outcome.
Wallet or custodian	Controls credentials, keys, accounts, or signing policy.	Does not by itself establish current authority, transaction-specific compliance, or commercial settlement.
Bank or payment rail	Moves fiat or maintains a deposit relationship under its own rules.	Does not necessarily preserve portable, cross-rail evidence of the complete transaction.
ChainIT Transaction Truth Architecture	Binds verified parties, authority, current evidence, exact transaction, wallet execution, settlement, reconciliation, and evidence.	Does not replace the issuer, network, bank, custodian, or regulated institution; it controls and connects qualified participants.

1.3 Stablecoins and tokenized deposits remain legally and economically distinct

A payment stablecoin and a tokenized bank deposit may support similar user experiences, but they are not the same instrument. A stablecoin is generally an issuer obligation represented by a token and supported by eligible reserve assets. A tokenized deposit represents a deposit relationship with a regulated depository institution. ChainIT preserves that distinction in product disclosures, asset registries, custody treatment, accounting records, settlement instructions, risk controls, and customer interfaces. [11]

The ChainIT opportunity is therefore not to replace every payment instrument. It is to maintain one verified transaction-control model while selecting the qualified settlement instrument best suited to the customer, merchant, jurisdiction, value, risk, and operating condition.

2. The Control Gap: A Wallet Signature Is Not a Complete Authorization

2.1 Cryptographic validity answers a narrow question

A blockchain checks that a transaction is technically correct: the signature is valid, the sender has the funds, the fees are paid, and any smart-contract rules are met. A multi-party wallet can produce that signature by having several key holders approve together. A smart account can approve it through rules written into the account itself. All of these answer the same narrow question: should the network accept this instruction? None of them answers the question a business actually cares about: should this instruction have been created in the first place, by this person, for this company, under this authority, and on today's compliance evidence?

Private-key or account control can be exercised by the legitimate owner, an authorized employee, an employee acting outside authority, a former employee, a compromised device, an infrastructure operator, a malicious insider, a scheduled workflow, or an AI agent acting outside delegated purpose. The chain usually cannot distinguish among these cases.

2.2 Address identity is not legal identity

A blockchain address is a protocol identifier. It may be pseudonymous, rotated, shared, derived, administered by a custodian, or controlled by smart-contract logic. It is not inherently a legal name, verified individual, registered organization, beneficial owner, officer, fiduciary, licensee, or authorized representative.

ChainIT ID supplies the verified individual anchor. ChainIT Org ID supplies the legal-entity anchor. Wallet-binding evidence links a wallet or account to the relevant subject under a defined assurance method. The evidence must also state what was not proven: a successful wallet challenge can demonstrate present control of a credential without proving source of funds, beneficial ownership of every asset, or authority to use organizational property.

2.3 Authentication is not authority

A person can authenticate correctly and still lack authority for the proposed action. A treasury analyst may prepare but not release a payment. A controller may approve ACH but not an irreversible stablecoin transfer. An employee may use an existing vendor but not change the destination address. An officer may be over an amount limit. A delegate may remain technically enrolled after the principal's authority changes.

At the moment of the transaction, the ARP and APP are checked together: the ARP confirms that this person or agent currently holds the role and authority in question, and the APP confirms that the rules applicable to this transaction permit them to use it. Authority exists only where both agree. It is not inferred from the fact that someone was onboarded in the past or holds a wallet credential. [1]

2.4 Compliance is not a permanent badge

A person, organization, wallet, issuer, asset, chain, jurisdiction, or counterparty is not universally and permanently "compliant." Evidence changes and is purpose-specific. A sanctions result, entity status, customer classification, wallet-risk observation, license, issuer status, or jurisdictional permission may be sufficient for one transaction and insufficient for another.

Provable Compliance therefore evaluates current Evidence Assertion VDTs against the applicable CPP at the reliance event. The organization's Workflow Engine composes BRE predicate results into a controlled disposition. A final Allow permits compliance-side continuation only; it does not cure absent authority, an altered digest, an exceeded limit, or an invalid wallet instruction. [2]

2.5 Network confirmation is not complete commercial settlement

An on-chain transfer may be confirmed while the commercial transaction remains incomplete. The merchant may have requested fiat settlement, conversion may fail, a payout may not post, a contractual condition may remain open, or the ERP record may not reconcile. The ChainIT Transaction Truth Architecture separates network acceptance from economic, commercial, accounting, and evidentiary completion.

> **Zero trust in this context means no person, device, wallet, address, custodian, asset, chain, policy result, or prior approval receives implicit authority. Each consequential transaction is re-evaluated against current identity, authority, evidence, policy, exact instruction, capacity, wallet profile, and outcome.**

3. ChainIT Strategic Position

3.1 Control the transaction, not the monetary instrument

Stablecoin issuance is regulated, reserve-intensive, distribution-driven, and dependent on redemption confidence, liquidity, banking access, and balance-sheet economics. Wallet infrastructure is increasingly competitive. Blockchain transaction fees tend toward commodity pricing. ChainIT's durable position is the layer that binds the chosen monetary instrument to verified commercial context.

The highest-value system determines who may transact, for whom, under what authority, subject to which current evidence and policy, on what exact instruction, through which qualified wallet and rail, after satisfaction of which conditions, with what finality, and with what resulting evidence.

3.2 Agnostic by architecture, selective by policy

ChainIT is designed to remain issuer, chain, wallet, custody, and rail-agnostic. Agnostic does not mean every provider is acceptable. It means the commercial transaction is not structurally dependent on one provider and can move among qualified alternatives without losing identity, authority, compliance, evidence, or reconciliation.

- **Settlement-asset independence.** The obligation remains denominated and governed independently from the selected stablecoin, tokenized deposit, or fiat rail.
- **Network independence.** Chain-specific fields and finality rules are isolated in controlled profiles rather than embedded throughout the commercial logic.
- **Custody independence.** The same authority and compliance decision may govern self-custody, ChainIT MPC, a qualified custodian, smart account, or bank wallet when the execution boundary enforces the required controls.
- **Provider portability.** Issuers, custodians, analytics providers, liquidity providers, node providers, banks, and rails may change without rewriting the transaction's identity, legal, or evidentiary layer.

3.3 The commercial value resides above and across the rail

ChainIT Pay can monetize the services that make digital value commercially operable: individual and organizational verification; authority creation and query; runtime compliance evidence; wallet policy; secure custody integration; route and quote management; conversion and payout coordination through authorized partners; conditional settlement; Pactvera execution; Valitorum evidence; ERP integration; exception handling; and merchant or marketplace operations.

The same architecture can support a stablecoin today, a tokenized deposit tomorrow, and a conventional bank rail whenever cost, risk, regulation, availability, or customer preference requires it.

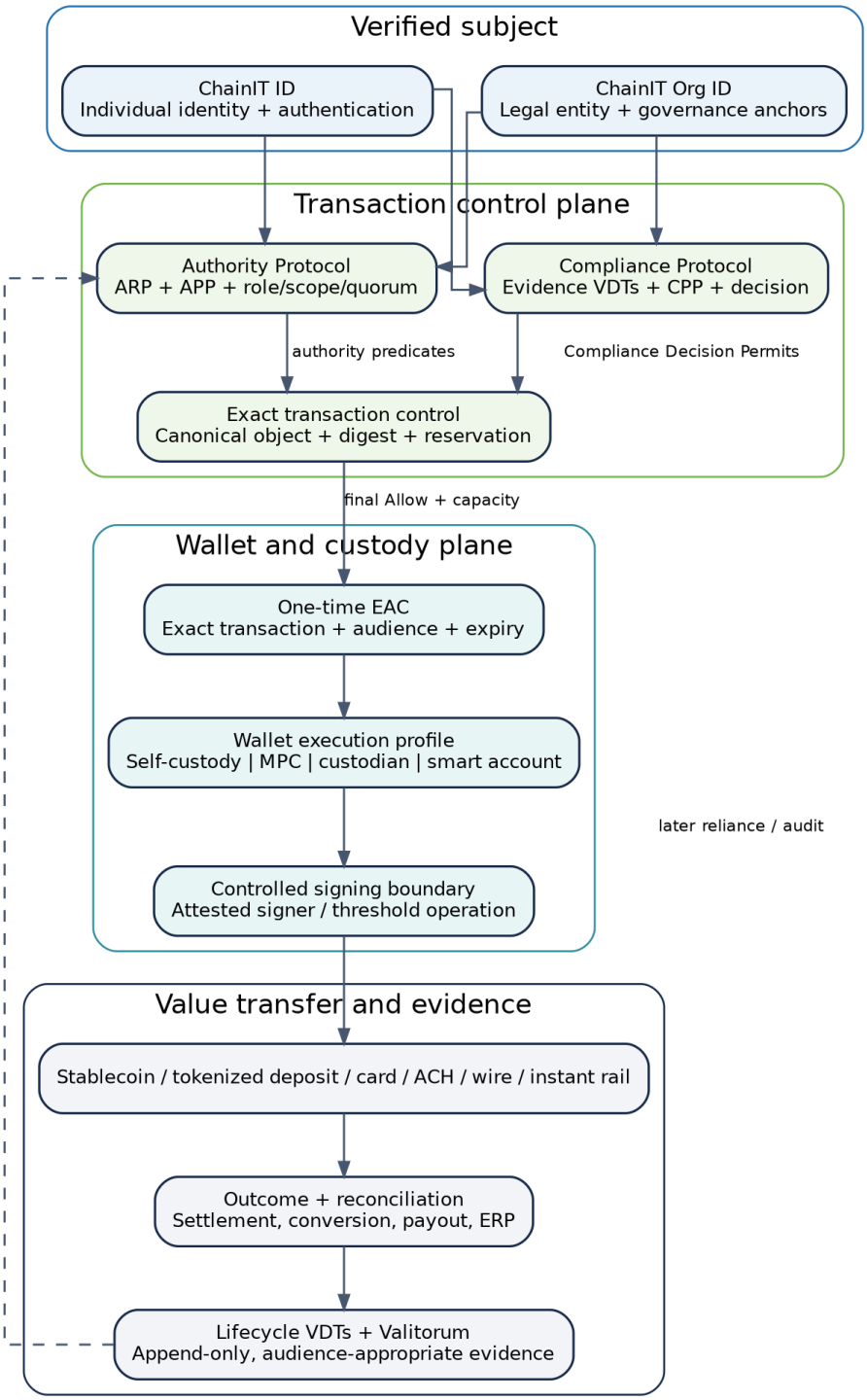


Figure 1. The ChainIT Transaction Truth Architecture separates verified subjects, transaction control, wallet execution, value transfer, and lifecycle evidence.

4. How the Transaction Truth Architecture Operates

4.1 Four planes, one transaction

Plane	Executive function
Subject and transaction-control plane	ChainIT ID, ChainIT Org ID, ARP, APP, CPP, Evidence Assertion VDTs, BRE predicates, Workflow Engine dispositions, approvals, and capacity reservation determine whether the exact action is eligible.
Wallet and custody plane	The WEP, EAC validation, signer attestation, MPC threshold, smart-account policy, external custodian Application Programming Interface (API), or self-custodial signer determine whether a qualified wallet may produce the required authorization.
Value-transfer plane	The blockchain, stablecoin issuer, tokenized-deposit platform, bank, card network, ACH operator, wire system, instant-payment rail, or smart contract moves or records value.
Evidence and integration plane	Pactvera, lifecycle VDTs, Valitorum, ChainIT Pay, ERP connectors, treasury systems, and reporting preserve the decision and outcome in commercially meaningful form.

4.2 Execution is conjunctive

A favorable result in one domain never substitutes for another. Strong MPC custody does not cure absent authority. A valid ARP does not cure a sanctions prohibition. A final compliance Allow does not cure a modified destination. A valid EAC does not cure an unapproved signer environment. A network confirmation does not cure failed merchant payout.

> **Commit Eligible = Effective Authority AND Compliance Decision Permits AND Exact Digest Match AND Required Approvals AND Capacity Reserved AND Qualified Execution Boundary**

4.3 Executive transaction sequence

Control outcome
Establish the verified individual, organization, group, workflow, or registered agent.
Bind the relevant wallet, custody account, or payment source under a defined assurance method.
Create the payment intent or Pactvera transaction and identify the commercial obligation.
Select current APP, CPP, and WEP versions and refresh required evidence.
Resolve authority and compliance for this reliance event.
Canonicalize the exact instruction and produce its digest.
Complete required human, quorum, or delegated-agent approvals against the same digest.
Reserve balance, budget, or aggregate capacity atomically.
Issue one short-lived, audience-restricted, single-use EAC.

Control outcome
Have the wallet boundary independently validate the EAC, digest, WEP, and signer state.
Sign or authorize, broadcast through the selected rail, and monitor the outcome.
Confirm conversion, payout, commercial completion, ERP reconciliation, and Valitorum.

4.4 Non-negotiable zero-trust invariants

- No Session Credential is payment authority.
- Every material transaction field is included in the canonical digest.
- Capacity is reserved before execution authority is issued.
- EACs are audience-restricted, short-lived, and single-use.
- The signing boundary independently reconstructs and verifies the digest (recomputes the fingerprint from the transaction it is about to sign and confirms it matches the one that was approved).
- Organizational approval quorum and cryptographic threshold are satisfied independently.
- Missing, stale, ambiguous, or contradictory evidence produces a controlled non-Allow state.
- Prior immutable records are never rewritten; later events are linked and appended.
- Sensitive evidence is disclosed only to the authorized audience and purpose.
- Automated systems may propose and coordinate but cannot bypass deterministic commit controls.

5. Individual and Organizational Wallet Transactions

5.1 The control model is subject-neutral, but the authority source differs

An individual may act for the individual's own account or under a valid delegation. An organization can act only through persons, groups, scheduled workflows, or registered agents whose authority is derived from organizational governance. The transaction sequence is shared; the identity, authority, approval, and capacity evidence differs.

Control	Individual transaction	Organizational transaction
Principal	The verified individual, unless acting for another principal.	The legal entity identified through ChainIT Org ID.
Identity anchor	ChainIT ID and wallet-control evidence.	ChainIT Org ID plus ChainIT IDs for authorized representatives.
Authority source	Personal control, legal capacity, or a valid delegation.	ARP, role, purpose, limits, quorum, separation of duties, and revocation.
Compliance context	Individual, counterparty, wallet, asset, chain, jurisdiction, and transaction.	Organization, beneficial ownership, authorized persons, supplier or merchant, wallet, asset, chain, jurisdiction, and transaction.
Approval	The individual approves the exact digest, with step-up when policy requires.	One or more authorized persons approve the same digest under the ARP quorum.
Capacity	Available assets, personal limits, risk buffer, and active reservations.	Treasury balance, budget, entity and department limits, counterparty limits, aggregate exposure, and active reservations.

Control	Individual transaction	Organizational transaction
Execution	Qualified self-custodial, MPC, custodial, smart-account, or bank wallet.	Qualified institutional, MPC, custodial, smart-account, bank, or embedded wallet under the WEP.
Evidence	Identity, authority or delegation, decision, approval, execution, outcome, and Valitorum.	Org ID, ARP, approvals, decision, reservation, signing, settlement, reconciliation, and Valitorum.

5.2 Organizational governance and cryptographic signing are orthogonal

An organization may require two officers to approve a transfer while an MPC wallet uses a different threshold among infrastructure signers. The officers may not hold key shares. The cryptographic signers may not possess legal authority to approve the payment. The two layers answer different questions and must not be conflated.

> **Authorized Organizational Transaction = Governance Quorum Satisfied AND Cryptographic Signing Threshold Satisfied**

5.3 Agent and scheduled-workflow initiation

A scheduled workflow or AI agent may create a proposal, retrieve evidence, calculate a route, or coordinate a transaction within a defined scope. It does not acquire authority merely because it can call a wallet API. A registered agent acts only under authority delegated by a verified principal, bounded by purpose, payee, transaction class, rail, amount, aggregate limit, time, step-up rules, and revocation. The exact transaction still passes through the same compliance, digest, reservation, EAC, wallet, and evidence controls. [1]

Crossing the delegated boundary, (such as a new beneficiary, changed destination, increased value, irreversible rail, or contract interaction outside scope) requires a new decision and any prescribed human or quorum approval.

6. Wallet and Custody Profiles

6.1 A wallet is a profile, not a single product category

The term wallet describes materially different control systems. Some place a private key entirely under user control. Some delegate signing to a custodian. Some use multiple on-chain signatures. Some perform off-chain threshold cryptography and produce one conventional signature. Some are smart accounts whose policies execute in contract code. Others are interfaces to an exchange, bank, or internal ledger. ChainIT governs these systems through a WEP rather than assuming one wallet label implies one security model.

Wallet profile	Primary control model	ChainIT control emphasis
Individual self-custody	User-controlled key or hardware signer.	Wallet binding, exact-digest presentation, beneficiary and contract controls, step-up approval, monitoring, and evidence of whether the transaction stayed inside the governed path.
ChainIT MPC profile	Threshold signing using protected shares and approved signer domains.	EAC-validating coordinator and attested signer components; threshold, signer set, recovery, and evidence governed by the WEP.

Wallet profile	Primary control model	ChainIT control emphasis
External custodian	Regulated or institutional provider controls keys and account policy.	Preflight authorization, signed sidecar or approval reference, account mapping, outcome reconciliation, and contractual responsibility allocation.
Smart account	On-chain program evaluates execution conditions.	Approved policy module, contract and calldata controls, upgrade-key governance, EAC or equivalent preflight, and chain-specific evidence.
Embedded merchant or marketplace wallet	Wallet provisioned within an application or commerce workflow.	ChainIT X or ChainIT Pay onboarding, transaction, custody boundary, merchant payout, recovery, and disclosure controls.
Bank or tokenized-deposit wallet	Bank controls the account or tokenized deposit.	Bank-native authorization integration, entity eligibility, settlement terms, and reconciliation without misclassifying the instrument as a generic stablecoin.

6.2 MPC and Nitro Enclaves: custody security, not business authority

MPC distributes signing capability so no single conventional private key or participant must act alone. The security benefit depends on the protocol, threshold, participant independence, distributed key generation, share protection, recovery, software integrity, and operating procedures. MPC reduces a class of single-key failures; it does not establish who is legally authorized to cause the signature.

The ChainIT MPC Wallet MVP profile uses Amazon Web Services (AWS) Nitro Enclaves as a confidential-computing boundary for approved signing logic and protected share operations. Enclaves can isolate memory from the parent instance, produce attestation documents identifying the measured software, and support policy-bound access to protected material through AWS Key Management Service (KMS). The wallet profile must still validate the EAC, exact digest, WEP, nonce, status, and attestation before any threshold participant signs. [4][20]-[22]

The detailed share count, threshold, cloud-account topology, region, key ceremony, recovery method, supported chains, and service levels remain controlled by the current internal engineering architecture and deployment configuration. The executive conclusion is simpler: protected signing components may execute only a transaction already approved by the independent authority and compliance control planes.

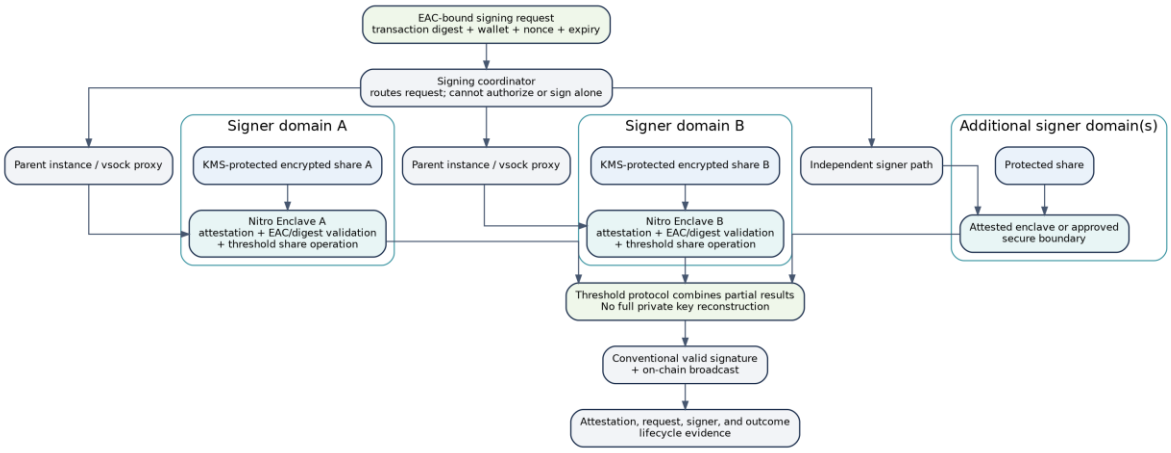


Figure 2. Abstract MPC profile: independent signer domains validate one approved transaction and contribute partial results without acquiring organizational authority.

7. Runtime Compliance and Stablecoin Qualification

7.1 Compliance evidence remains attributable, current, and purpose-specific

Provable Compliance does not reduce a person or organization to a universal compliant or noncompliant label. Each sourced fact is represented as an Evidence Assertion VDT with source class, provenance, observed time, effective time, freshness or expiration, jurisdiction, purpose, confidence or match state, and privacy classification. Evidence may come from an authoritative source, a qualified third party, or the institution itself. [2]

The CPP selects the evidence and controls applicable to the institution, product, subject, counterparty, transaction type, value, rail, payer and payee jurisdiction, customer category, risk tier, and intended purpose. The BRE returns deterministic, reason-coded predicate results. The organization's Workflow Engine composes those results into an explicit disposition such as Allow, Allow with Controls, Step-Up, Review, Hold, Reject, Prohibit, or Stale/Unknown. The wallet independently checks that the transaction in front of it is identical, detail for detail, to the one that was approved, and refuses to sign if anything has changed.

7.2 Compliance does not confer authority

Compliance Decision VDT does	Compliance Decision VDT does not
Records the issuing organization or authorized decision service, audience, CPP version, evidence references, freshness, reason codes, and disposition.	Create an ARP grant, change an officer's role, expand a transaction limit, or establish governance authority.
Determines whether current compliance-side evidence and policy permit continuation for one reliance event.	Authorize a wallet signature, consume capacity, select a final payment instruction, or bypass the Authority Protocol.
Supports controlled disclosure to the subject, institution, partner, auditor, regulator, or other authorized audience.	Turn restricted evidence into public blockchain data or disclose Suspicious Activity Related (SAR)-related information to an unauthorized party.
Produces append-only review, override, and supersession evidence.	Rewrite an earlier evidence or decision record.

7.3 Stablecoin and Web3 transaction evidence domains

- Individual and organizational identity, beneficial ownership, entity status, and representative relationship;
- Authority, role, delegation, quorum, limits, and revocation;
- Customer and counterparty risk, sanctions, Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT), transaction monitoring, and source-specific reviews;
- Wallet ownership or control, address and transaction risk, beneficiary history, and destination changes;
- Issuer authorization, reserve and redemption structure, token contract, freeze capability, and geographic eligibility;
- Backing-mechanism classification (off-chain collateralized, on-chain collateralized, uncollateralized/algorithmic, or hybrid/synthetic), reflecting materially different failure modes and control focus;
- Native, bridged, or wrapped asset status; chain security, finality, outages, and concentration;
- Custodian, bank, liquidity provider, conversion provider, and settlement pathway; and
- Transaction purpose, value, velocity, jurisdiction, product, rail, and policy-specific evidence.

A shared peg does not imply a shared risk profile. Collateralized and uncollateralized (algorithmic) stablecoins fail in different ways: an off-chain, fiat-collateralized instrument depends on issuer solvency and reserve attestation, an on-chain collateralized instrument depends on collateralization ratio and liquidation mechanics, and an algorithmic instrument depends on protocol incentives with no independent redeemable reserve. ChainIT records backing-mechanism classification as a first-class registry attribute, versioned like any other field, rather than inferring it from a stablecoin's name or marketing description. Recent research reaches a consistent conclusion on why this matters: reserve quality and transparency, not the collateralization label alone, drive run risk, and overcollateralization plus disclosure requirements measurably reduce run and insolvency risk. [24][25]

7.4 Regulatory perimeter remains activity-specific

The U.S. stablecoin framework reinforces the need to separate issuer obligations from transaction controls. The GENIUS Act establishes a federal framework for permitted payment stablecoin issuers, reserves, redemption, disclosure, supervision, AML/CFT, sanctions, and related requirements. Current rulemakings address issuer and customer-identification obligations, while Financial Crimes Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC), banking, custody, money-transmission, and institutional requirements continue to depend on the actual activity and flow of funds. [11]-[18]

ChainIT should maintain an explicit responsibility matrix identifying who receives funds, controls private keys, performs conversion, selects counterparties, holds merchant funds, executes sanctions and transaction monitoring, files reports, handles blocked property, manages refunds, bears settlement risk, and retains evidence. Regulated functions should be performed by the appropriately authorized ChainIT entity or qualified partner.

7.5 Privacy and disclosure

Compliance does not always require every merchant or counterparty to receive the underlying identity record. ChainIT may provide purpose-limited assertions such as identity verified, organization verified, authority current, sanctions screening completed, jurisdiction permitted, or transaction limit not exceeded, while preserving restricted evidence in the proper environment. The disclosure result must identify its audience, purpose, source, time, and limitations.

8. Exact-Transaction Execution

8.1 Approval must follow the transaction, not merely the session

A user may be correctly authenticated while a transaction changes between presentation and signing. Destination substitution, fee modification, token-contract changes, altered calldata, changed chain, route fallback, quote expiration, or compromised middleware can cause the instruction executed by the wallet to differ from the instruction approved by the person or organization.

ChainIT addresses this through an exact-transaction control sequence rather than a general logged-in state.

8.2 Canonicalization and digest

The transaction object includes the payer, source wallet or account, payee, destination, amount, currency or asset, issuer, token contract, chain, method or calldata hash, nonce, fees, quote, validity window, commercial reference, and other material rail-specific fields. A fixed canonicalization method produces one digest. Any material change produces a different digest. [23]

8.3 Decision, approval, reservation, and EAC

Control	Purpose
Transaction Policy Decision VDT	Binds the current authority and compliance result, risk tier, policy versions, evidence, conditions, and disposition to one exact digest.
Exact-digest approval	The individual or every required organizational approver authorizes the same digest and material fields.
Atomic reservation	Balance, budget, counterparty limit, aggregate exposure, or other capacity is reserved before execution authority is issued.
One-time EAC	A short-lived credential authorizes one digest for one wallet or rail audience and cannot serve as a standing payment entitlement.
Wallet-bound verification	The wallet or custodian independently reconstructs the transaction, validates the digest and EAC, and rejects mismatch, replay, wrong audience, stale status, or expiration.
Idempotent submission	Retries do not create duplicate economic transfers, and an unknown result remains controlled until resolved.

8.4 Asset, chain, destination, and contract qualification

The same exact-transaction decision must reference a qualified issuer, token contract, blockchain, custody profile, and destination. ChainIT should maintain versioned registries covering legal and operational status, native versus bridged or wrapped form, redemption path, freeze or blacklist capability, chain finality, bridge dependencies, supported custodians, conversion routes, liquidity, geographic restrictions, concentration limits, and emergency status.

Destination and smart-contract controls should distinguish an established verified beneficiary from a first-use address, a verified contract from an arbitrary call target, and a limited method from an unrestricted approval. A material change after approval invalidates the prior digest and requires a new decision. Fallback routing may change the rail only when the commercial terms and authorization permit that change; otherwise renewed authorization is required.

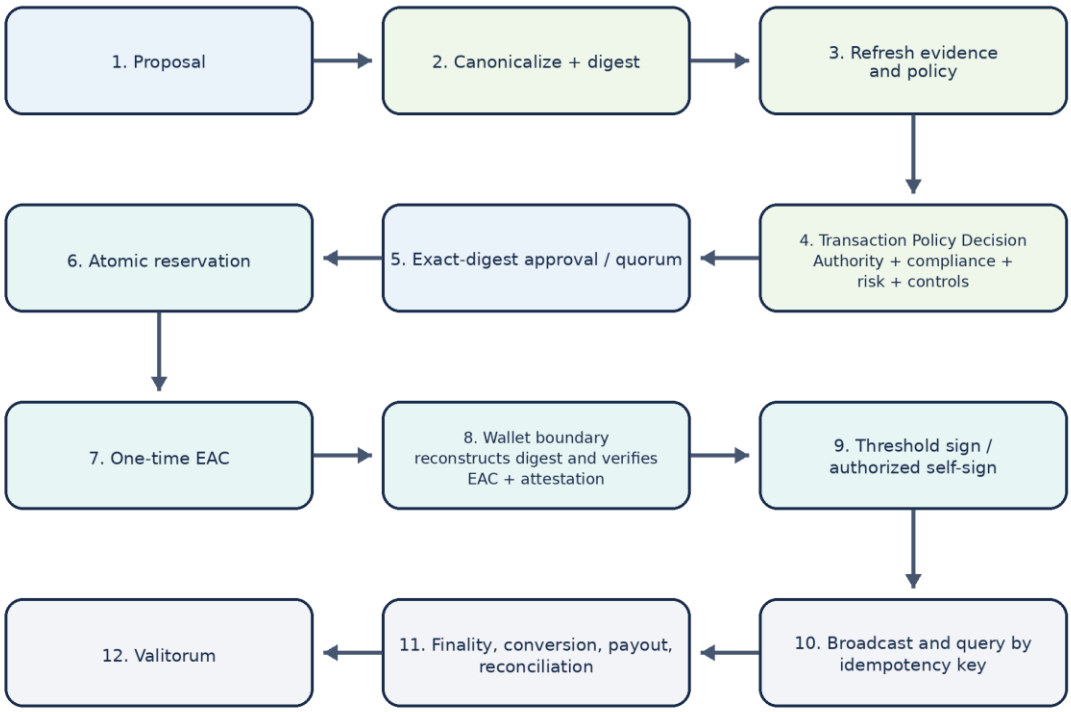


Figure 3. Exact-transaction commit sequence: proposal, current evidence and policy, decision, approval, reservation, one-time EAC, wallet validation, signing, settlement, reconciliation, and Valitorum.

9. Settlement, Reconciliation, and Immutable Evidence

9.1 Finality occurs in layers

Finality layer	Meaning
Signature finality	The required key or threshold operation completed.
Network finality	The transaction was accepted and reached the required consensus confidence.
Issuer finality	The token remains recognized and transferable under issuer controls.
Conversion finality	The digital asset was exchanged at the recorded rate and fees.
Bank or merchant payout	The requested fiat or deposit proceeds were credited.
Commercial finality	The underlying Pactvera conditions, delivery, milestone, or other obligation were satisfied.
Accounting finality	The transaction, fees, conversion, and payout were reconciled to the ERP and general ledger.
Evidentiary finality	The required lifecycle evidence was sealed in Valitorum.

A blockchain confirmation should not be presented as completed merchant settlement when conversion, payout, contractual performance, or reconciliation remains open.

9.2 Pactvera, lifecycle VDTs, and Valitorum

Pactvera binds the transaction's parties, authority, terms, consideration, conditions, payment intent, approvals, execution, and outcome. Lifecycle VDTs record discrete sourced facts and state changes without rewriting prior entries. Valitorum seals the completed or otherwise terminal evidence chain under a defined completeness rule.

The evidence graph should answer who acted, for whom, under what authority, against which current evidence and policy, on what exact instruction, through which wallet and rail, what value moved, whether conversion and payout occurred, how the transaction was booked, and what later exception followed.

9.3 Dual-ledger privacy and selective disclosure

Sensitive commercial, identity, bank, tax, and compliance data may remain in protected storage while hashes, signatures, timestamps, state transitions, and integrity references are recorded in immutable or tamper-evident form. Authorized reviewers can verify the protected record without publishing restricted evidence to a public chain.

9.4 Refunds and later exceptions

An irreversible on-chain transfer is not erased by describing a later event as a reversal. A refund is modeled as a new compensating transaction linked to the original. The original Valitorum remains unchanged. A Supplemental Valitorum records the return, dispute, recall, recovery, chargeback, or other later exception and preserves the relationship between both economic events.

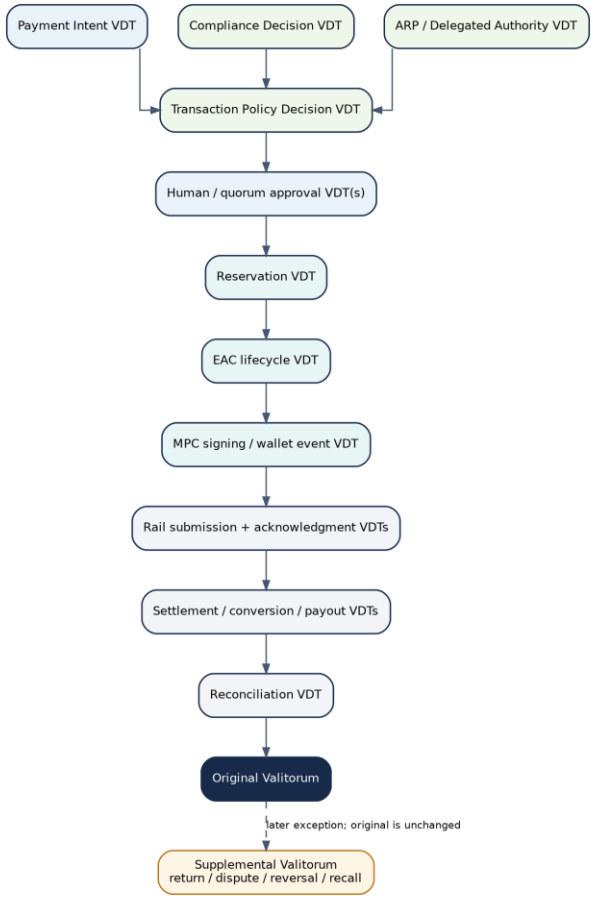


Figure 4. Append-only evidence graph: transaction intent, authority, compliance, approval, reservation, wallet execution, settlement, reconciliation, original Valitorum, and linked later exceptions.

10. Illustrative Commercial Use Cases

Use case	Business objective	ChainIT control and evidence
Merchant stablecoin acceptance with fiat settlement	A customer pays an approved stablecoin; the merchant receives fiat.	Customer and merchant identity, asset and chain qualification, wallet screening, exact payment intent, conversion, merchant payout, ERP reconciliation, and Valitorum.
Organizational supplier payment through MPC	A corporation pays an approved supplier under a two-approver treasury policy.	ChainIT Org IDs, ARP roles, supplier evidence, same-digest quorum, atomic capacity, EAC, attested threshold signing, finality, invoice reconciliation, and evidence.
Conditional marketplace settlement	Funds are held or reserved until asset, delivery, inspection, or acceptance conditions are satisfied.	Verified buyer and seller, VDT-linked asset, Pactvera conditions, compliance, escrow or conditional release, multi-party allocation, and Supplemental Valitorum for later disputes.
Tokenized-deposit treasury transfer	Institutions move value through a bank-issued digital deposit instrument.	Instrument classification, bank eligibility, Org ID, authority, transaction policy, bank-native execution, treasury reconciliation, and evidence without treating the deposit as a generic stablecoin.
Agent-initiated commerce	A registered agent proposes a purchase or payment within delegated bounds.	Agent Registration VDT, Agent Authority VDT, sponsoring organization, purpose and budget limits, current compliance, exact digest, step-up outside scope, EAC, and sovereign wallet boundary.
Cross-border B2B settlement	A buyer settles an invoice through a qualified digital or bank rail selected for cost, time, jurisdiction, and risk.	Counterparty and beneficial-owner evidence, route and quote, sanctions and payment transparency, exact instruction, conversion or local payout, ERP posting, and evidence.

10.1 What changes for the customer

The merchant or enterprise does not have to treat every wallet, stablecoin, chain, or provider as a separate operating model. ChainIT presents one controlled transaction lifecycle: verified parties, current authority, transaction-specific compliance, qualified settlement options, exact approval, secure signing, normalized status, reconciliation, and auditable evidence.

The customer may select a preferred custody model or settlement asset, while the Transaction Truth Architecture preserves the same governance and evidentiary requirements across qualified alternatives.

11. Business Value, Competitive Position, and IP Foundation

11.1 From wallet utility to enterprise control surface

Conventional wallet products compete on custody, asset support, user experience, and transaction fees. ChainIT adds the enterprise control surface: verified individual and organizational identity; portable authority; runtime compliance; exact transaction approval; secure wallet execution; multi-rail orchestration; conditional commercial logic; ERP reconciliation; and immutable evidence.

The value proposition changes from "store and send tokens" to "execute a verified commercial transaction under provable authority and compliance."

11.2 Revenue across the transaction stack

Revenue layer	Representative services
Identity and organization	ChainIT ID, ChainIT Org ID, authentication, Know Your Business (KYB), beneficial-owner, and attribute-verification services.
Authority and compliance	ARP creation and query, delegation, revocation, evidence ingestion, policy execution, decisioning, and controlled disclosure.
Wallet and custody	Wallet provisioning, MPC profile, custody integration, policy administration, recovery, and transaction control.
Payment and settlement	Multi-rail orchestration, stablecoin acceptance, route and quote services, conversion and payout coordination, and treasury operations through authorized providers.
Transaction logic and evidence	Pactvera, conditional settlement, VDT lifecycle records, Valitorum generation and verification, disputes, and Supplemental Valitorum.
Enterprise integration	ERP, treasury, marketplace, reporting, monitoring, analytics, and exception management.

11.3 Competitive differentiation

Provider category	Commonly controls	ChainIT adds
Stablecoin issuer	Issuance, reserves, redemption, and token controls.	Verified parties, authority, policy, wallet governance, multi-rail choice, reconciliation, and evidence.
Wallet or custodian	Keys, signing, accounts, and asset storage.	Legal and organizational context, current compliance, exact-digest authority, Pactvera, and Valitorum.
Blockchain	Consensus and state transition.	Commercial meaning, off-chain evidence, authority, policy, payout, and ERP outcome.
Identity or compliance provider	Identity proofing, screening, or monitoring result.	Portable organizational authority, transaction-specific composition, commit-time enforcement, settlement, and evidence.
Payment processor	Authorization and settlement on supported rails.	Web3 wallet control, stablecoin and tokenized-value support, programmable conditions, and immutable lifecycle evidence.
ERP or treasury system	Accounting, approval, cash management, and reporting.	Verified subject, portable authority, wallet and chain execution, and cryptographic outcome evidence.

11.4 Intellectual-property foundation

The ChainIT Transaction Truth Architecture builds on the documented ChainIT portfolio and applications addressing verified individuals and events; portable privacy-preserving identity; immutable representations and VDTs; paired physical and digital assets; digital financial events and multiple payment mechanisms; smart-contract conditions and payment release; Pactvera transaction formation and conditional compensation; marketplace and wallet integration; authority, revocation, and compliance; and Valitorum evidence. [5]-[10]

U.S. Patent No. 12,321,940 describes verification and immutable association of financial events and payment records, with specifications encompassing stablecoin, cryptocurrency, ACH, Electronic Funds Transfer (EFT), card, bank-transfer, and wallet-transfer mechanisms. The Marketplace and Pactvera materials provide additional foundations for verified identity, token and value transfer, conditional logic, payment routing, authority, compliance, and immutable transaction evidence. [6]-[9]

References to patents and applications identify technical source foundations. They do not represent that every implementation described here is covered by an issued claim or currently deployed. Wallet-specific and integrated protocol mechanisms remain subject to patent-counsel review for written description, enablement, continuity, priority, inventorship, and filing route.

12. Controlled Deployment and Governance

12.1 Architecture status

Status class	Public meaning
Current platform foundation	ChainIT ID, ChainIT Org ID, ChainIT Pay, Pactvera, VDTs, Valitorum, and related documented platform capabilities used as the foundation.
Published protocol architecture	Provable Authority and Provable Compliance definitions, evidence, policy, decision, reservation, EAC, and lifecycle controls incorporated by reference.
Development / MVP	MPC wallet components, integrations, and controlled validation work not represented as generally available in every environment.
Proposed execution profile	WEP, signer-domain EAC enforcement, attestation-bound share access, asset and chain registries, and other wallet-specific controls defined for implementation and testing.
External dependency	Stablecoin issuers, blockchains, banks, custodians, cloud providers, analytics providers, liquidity providers, and other regulated or technical partners.

12.2 Phased deployment

Phase	Required outcome
0 - Responsibility and architecture clearance	Finalize entity scope, flow of funds, control of keys, regulatory responsibility, Authority-Compliance interface, canonical transaction schema, WEP, registries, evidence model, incident controls, and patent/public-disclosure clearance.
1 - MPC component validation	Prove attestation, KMS conditions, share protection, threshold signing, coordinator non-sovereignty, digest and EAC validation, replay rejection, outage behavior, rotation, recovery, and emergency suspension without live customer funds.
2 - Individual wallet pilot	Deploy a bounded individual profile with approved assets and chains, identity and wallet binding, current compliance, exact-digest approval, controlled signing, monitoring, reconciliation, and Valitorum.

Phase	Required outcome
3 - Organizational wallet pilot	Add ChainIT Org ID, ARP roles, maker-checker or quorum approval, aggregate capacity, MPC or custodian execution, supplier controls, ERP integration, revocation, and recovery.
4 - Stablecoin acceptance and conversion	Add merchant acceptance, route and quote, stablecoin receipt, authorized conversion, fiat payout, refunds, exception handling, and settlement evidence.
5 - Multi-rail and institutional interoperability	Expand to cards, ACH, wires, instant payments, tokenized deposits, additional qualified wallets, banks, custodians, and treasury systems.
6 - Controlled agentic execution	Permit registered agents to propose and coordinate within delegated scope while retaining deterministic authority, compliance, capacity, exact-transaction, wallet, and evidence controls.

12.3 Pilot success means invariants hold under attack and failure

A successful pilot is not a favorable demonstration. It proves that required invariants remain true under transaction mutation, replay, stale evidence, revoked authority, concurrent requests, wrong audience, signer outage, unapproved enclave measurement, destination substitution, provider failure, policy change, and disclosure-boundary probing.

- Every governed material-field mutation changes the digest and is rejected by the execution boundary.
- A consumed, expired, canceled, wrong-audience, wrong-wallet, or replayed EAC cannot authorize signing.
- A session or ordinary authenticated state cannot trigger payment.
- Revoked, expired, out-of-scope, over-limit, wrong-payee, wrong-rail, or insufficient-quorum transactions remain non-executable.
- Parallel requests cannot consume the same capacity or exceed aggregate limits.
- Unapproved signer software or stale attestation cannot access protected signing material.
- Settlement, conversion, merchant payout, ERP reconciliation, and Valitorum can be traced to the same transaction.
- Restricted evidence remains within its authorized audience and purpose.

Executive governance should include Product, Engineering, Payments, Information Security, Compliance, Legal, Finance, Treasury, Risk, Operations, and senior management. New assets, issuers, chains, custodians, liquidity providers, risk limits, finality policies, emergency actions, material BRE or Workflow changes, and production deployment claims should require explicit approval and recorded ownership.

13. Conclusion

Stablecoins and Web3 wallets improve the mechanics of moving value. They do not eliminate the need to establish who is acting, for whom, under what authority, against which current evidence, subject to what policy, on what exact transaction, through what custody system, with what commercial outcome, and with what proof.

For an individual, ChainIT binds verified identity, wallet control, personal or delegated authority, current compliance, exact-digest approval, qualified signing, settlement, and evidence.

For an organization, ChainIT binds ChainIT Org ID, the ARP, delegated roles, quorum, separation of duties, capacity, current compliance, the exact transaction, MPC or custodian policy, authenticated settlement, ERP reconciliation, and Valitorum.

MPC and confidential computing strengthen custody by distributing signing capability and isolating sensitive operations. They do not create authority. The Authority Protocol determines who may act. The Compliance

Protocol determines whether current evidence and policy permit continuation. Exact-transaction controls determine what instruction is approved. The WEP determines how a qualified wallet may sign. The rail moves value. Valitorum proves the resulting lifecycle.

> **ChainIT does not need to become the stablecoin, the blockchain, or the custodian. It must become the control and evidence infrastructure through which qualified money and wallets become commercially verifiable.**

That position allows ChainIT to remain issuer-agnostic, chain-agnostic, wallet-agnostic, bank-compatible, tokenized-deposit compatible, and multi-rail while preserving one consistent model for verified commerce.

Stablecoins move value. Wallets sign instructions. ChainIT establishes who may act, whether the action is permitted now, what exact transaction may be executed, how it settles, and what proves the result.

References and Source Basis

[1] ChainIT, Provable Authority: A Protocol for Verifiable Authority Resolution and Control Across Human, Organizational, and Agentic Transactions, ChainIT Authority Protocol, CIT-PA-WP-7.0, September 1, 2026.

[2] ChainIT, Provable Compliance: A Protocol for Runtime Compliance Evidence and Transaction-Specific Decisioning, ChainIT Compliance Protocol, CIT-PC-WP-4.0, September 2026.

[3] ChainIT, ChainIT Transaction Truth: Stablecoins, Web3 Wallets, and Multi-Rail Commerce, Technical and Compliance Companion, CIT-TT-TCC-2.1, September 2026.

[4] ChainIT, MPC Wallet MVP Architecture - Secure Multi-Party Custody Using Nitro Enclaves, internal Confluence architecture page.

[5] U.S. Patent Application Publication No. US 2025/0165575 A1, System for Creating, Storing, and Portably Utilizing Verified Digital Identities.

[6] U.S. Patent No. 12,321,940 B2, System for Verification and Management for Digitally Cash Transactions, June 3, 2025.

[7] ChainIT / Scientia Potentia Est II, LLC, System and Method for Managing Verified Digital Identities, Tokenized Assets, and Conditional Transactions in a Blockchain-Based Marketplace, filed application materials.

[8] ChainIT / Scientia Potentia Est II, LLC, System and Method for Verifiable Tokenized Transaction Execution and Conditional Compensation, Pactvera Application A.

[9] ChainIT / Scientia Potentia Est II, LLC, System and Method for Verifiable Tokenized Transaction Execution and Conditional Compensation, Pactvera Application B.

[10] U.S. Patent No. 11,288,761 B2, Decentralized System for Verifying Participants to an Activity, March 29, 2022; U.S. Patent Nos. 11,288,308 B2 and 11,521,157 B2 concerning verifiable physical and digital asset pairing.

[11] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, approved July 18, 2025. https://www.govinfo.gov/app/details/PLAW-119publ27

[12] U.S. Department of the Treasury, Notice of Proposed Rulemaking Regarding the Issuance, Offering, and Sale of Payment Stablecoins in the United States, August 17, 2026. https://home.treasury.gov/news/press-releases/sb0605

[13] FinCEN, OCC, Federal Reserve, FDIC, and NCUA, Proposed Rule to Implement GENIUS Act Customer Identification Program Requirement, June 18, 2026. https://www.fincen.gov/news/news-releases/fincen-agencies-propose-rule-implement-genius-act-customer-identification

[14] FinCEN and OFAC, Permitted Payment Stablecoin Issuer AML/CFT Program and Sanctions Compliance Program Requirements - Proposed Rule, April 8, 2026. https://www.fincen.gov/news/news-releases/treasury-proposes-rule-implement-genius-acts-requirements-counter-illicit

[15] Office of the Comptroller of the Currency, GENIUS Act Regulations: Notice of Proposed Rulemaking, OCC Bulletin 2026-3, February 25, 2026. https://occ.gov/news-issuances/bulletins/2026/bulletin-2026-3.html

[16] FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, May 9, 2019. https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models

[17] Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry, October 15, 2021. https://ofac.treasury.gov/recent-actions/20211015

[18] Financial Action Task Force, Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs, July 16, 2026. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

[19] National Institute of Standards and Technology, Zero Trust Architecture, NIST SP 800-207, August 2020. https://csrc.nist.gov/pubs/sp/800/207/final

[20] National Institute of Standards and Technology, Multi-Party Threshold Cryptography Project and NIST IR 8214C, NIST First Call for Multi-Party Threshold Schemes, January 2026. https://csrc.nist.gov/projects/threshold-cryptography

[21] Amazon Web Services, AWS Nitro Enclaves Concepts and Security. https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave-concepts.html

[22] Amazon Web Services, Connect an Enclave with AWS KMS for Cryptographic Attestation and Secrets Management. https://docs.aws.amazon.com/enclaves/latest/user/connect-enclave-kms.html

[23] Internet Engineering Task Force, JSON Canonicalization Scheme, RFC 8785, June 2020. https://www.rfc-editor.org/rfc/rfc8785.html

[24] Tacl, E. (2025). National Innovation Capability Enablers and Outcomes, Corruption, and Progression to Higher Stages of CBDC Adoption [Doctoral dissertation, Saint Mary's University of Minnesota]. https://www.researchgate.net/publication/397941663

[25] Castrén, O., & Russo, R. (2026). Runs, transparency and regulation: On the optimal design of stablecoin frameworks. Economics Letters, 258. https://doi.org/10.1016/j.econlet.2025.112720

[26] Eichengreen, B., Nguyen, M. T., & Viswanath-Natraj, G. (2025). Stablecoin devaluation risk. The European Journal of Finance, 31(11), 1469-1496. https://doi.org/10.1080/1351847X.2025.2505757

Important Notices

This document is an executive strategic and technical white paper. It is not legal, regulatory, banking, custody, accounting, tax, investment, security-certification, or patentability advice. It does not replace a regulated institution's AML/CFT, sanctions, customer-identification, custody, cybersecurity, or risk-management program.

The legal characterization of a stablecoin, tokenized deposit, wallet, custody arrangement, conversion service, smart account, payment activity, escrow structure, or transaction-orchestration service depends on applicable law and the specific facts, contracts, flow of funds, control of assets, control of private keys, and activities performed.

References to current or proposed U.S. stablecoin requirements reflect sources identified in this paper as of September 2026. Proposed rules may change before adoption. ChainIT, its customers, and its partners must evaluate final rules and jurisdiction-specific requirements before deployment.

References to ChainIT patents and patent applications describe issued claims, disclosed embodiments, pending claims, or technical source foundations. They do not represent that every described feature is currently deployed or that every commercial implementation falls within an issued claim.

References to immutable records mean records designed to be tamper-evident, chronologically verifiable, and resistant to unauthorized alteration. Immutability does not establish that original source data was accurate unless source, provenance, capture method, and verification were themselves validated.

References to MPC, threshold cryptography, or confidential computing do not imply that every implementation provides identical security. Security depends on the protocol, threshold, participant count, key-generation process, implementation, adversary model, signer independence, recovery process, attestation policy, and operational controls.

Pactvera, VDTs, and Valitorum are designed to capture and preserve evidence relevant to identity, authority, assent, consideration, conditions, execution, and outcome. Actual enforceability and admissibility remain subject to applicable law, jurisdiction, transaction structure, and judicial or administrative determination.

Stablecoins should not automatically be characterized as legal tender, insured deposits, cash, cash equivalents, risk-free assets, or obligations of the United States. Issuer, reserve, redemption, liquidity, depeg, freeze, custody, chain, bridge, smart-contract, sanctions, and operational risks must be evaluated separately. Depeg risk is not limited to algorithmic designs: market-based estimates for one major fiat-collateralized issuer put the average annual probability of a full depeg at roughly 60 basis points, rising above 200 basis points during the 2022 Terra-Luna stress episode, with market volatility and elevated interest rates as leading indicators. [26]

ChainIT should perform regulated financial functions directly only where appropriately authorized and should otherwise integrate properly licensed or regulated issuers, banks, custodians, acquirers, money transmitters, liquidity providers, and other partners.