WECAN 3.0

The Global Compliance-as-a-Service Backbone

White Paper

wecan®

Version 3.0 - 18.12.2025

Executive Summary

Something fundamental is changing. The world is becoming real-time.

Money moves instantly. Assets transfer globally. Contracts execute automatically. Businesses onboard customers at a distance. Governments digitize services. AI agents begin to act on our behalf. Robots and autonomous systems increasingly buy, sell, negotiate, and pay.

And yet, one invisible layer still holds everything back: trust.

Not trust as a feeling, but trust as a system. Trust that someone is who they claim to be. Trust that a transaction is allowed. Trust that a party is compliant with rules designed to protect society. Trust that actions can be audited later without exposing private data.

Today, that trust layer is still built the old way. We send documents. We wait. We repeat. We store sensitive data everywhere. We re-check the same people and companies again and again. Compliance becomes a cost center and a bottleneck. Meanwhile, the world accelerates.

Wecan 3.0 proposes a simple shift with enormous consequences: compliance should not be paperwork. It should be infrastructure.

Not an administrative process. A verifiable property of digital interactions.

Wecan introduces a new paradigm: Compliance as a Service.

Built on Hedera Hashgraph, secured by post-quantum, hardware-rooted institutional trust through SealSQ, governed by WiseID, orchestrated at industrial scale by Digital KYC, augmented by AI-driven automation, and supported by encrypted storage through Wecan Vault, Wecan 3.0 turns compliance into something radically different: always available, instantly verifiable, privacy-preserving, and enforceable by design.

Wecan is designed for the scale of the future. A world where compliance is not checked occasionally, but continuously. A world where transactions are not merely signed, but also verified against rules. A world where billions of transactions per day can be assessed for compliance as smoothly as the internet routes packets.

In the long run, Wecan aims to become the missing layer that enables safe, ethical, regulated interaction between humans, institutions, AI agents, administrations, and robots—without forcing society to trade privacy for security, or speed for control.

The Compliance Problem at Global Scale

Compliance is expanding. AML, CTF, sanctions, PEP monitoring, beneficial ownership, data protection, ESG obligations, cross-border reporting, and digital asset regulation are now part of the baseline. But the way we operate compliance is still stuck in a slow, fragmented world.

Every regulated institution builds its own “compliance perimeter.” The same individual and the same company are asked for the same documents in slightly different formats. The same beneficial owner identifies themselves repeatedly. Employees are verified again and again across entities. Meanwhile, changes that matter—new sanctions, a new director, an updated ownership structure, a new adverse media signal—propagate slowly and inconsistently.

This creates a structural mismatch. Transactions settle in seconds; compliance updates can take days, sometimes weeks. The faster the world becomes, the more compliance becomes the limiting factor.

Audits reveal the same problem. Too often, “proof” is assembled after the fact from documents, emails, screenshots, and internal logs. That is not verification. That is reconstruction. It is expensive, error-prone, and fragile—especially when the stakes are global.

Traditional compliance models were not designed for the speed of modern finance, the scale of machine interactions, or the coming wave of AI-driven automation. The world needs a compliance system that matches the pace of the systems it regulates.

From Compliance Processes to Compliance Infrastructure

The core problem is not that compliance is “hard.” The core problem is that compliance is treated like an activity, not like a layer.

In the same way that we do not “do the internet” manually—routing every packet by hand—we should not “do compliance” by manually exchanging the same files and repeating the same checks across institutions.

Wecan is founded on a fundamental shift in perspective. Compliance should not be treated as a process to be executed. It should be treated as infrastructure to be verified.

For compliance to operate as infrastructure, it must be cryptographic rather than documental. It must be reusable rather than duplicated. It must preserve privacy rather than spreading sensitive data. It must be machine-readable rather than interpretative. It must be enforceable at the moment it matters—when the transaction happens.

Wecan 3.0 embodies this transformation by turning compliance into a system of verifiable states embedded into identities, credentials, and transaction logic. Instead of exchanging raw data, participants verify cryptographic facts: whether a credential exists, whether it is valid, whether it has been updated, whether it is revoked, whether the policy allows the transaction.

This is the leap from “compliance work” to “compliance verification.”

The Wecan Premise: Compliance as a Native Network Function

Wecan begins with a simple idea that becomes obvious once stated:

Compliance should not be a process. It should be a property of the transaction itself.

In the same way a transaction must be signed to be valid, a regulated transaction must be compliant to be allowed. That compliance should be deterministically verifiable, without requiring the sharing of private data.

To make this possible, identity must be cryptographically verifiable. Credentials must be reusable. Institutions must be authenticated through hardware-rooted trust. Verification must not require disclosure. Rules must be embedded in transaction logic.

These are not optional features. They are the prerequisites for compliance to scale safely.

Wecan as a Compliance-as-a-Service Platform

Wecan 3.0 is not only a protocol. It is a platform layer designed for adoption.

In the traditional model, compliance requires long implementation projects, complex vendor setups, and heavy operational maintenance. In the Wecan model, compliance can be activated as a service. Institutions can self-onboard, configure what they need, and start verifying compliance without rebuilding the world.

The result is a new operating model: compliance becomes something you plug into your systems, not something you reinvent inside every institution.

It also changes incentives. If compliance is reusable and verifiable, then collaboration becomes possible without data sharing. Institutions gain efficiency without violating privacy. Regulators gain auditability without demanding more data exposure. Individuals gain simpler onboarding without losing control.

Compliance as a Service is not a slogan. It is a new architecture for the regulated world.

The Architecture of Wecan 3.0

Wecan 3.0 is structured as four layers that work together to make compliance verifiable, scalable, and privacy-preserving.

The Identity Layer is built on decentralized identifiers anchored on Hedera, providing a global identity framework for individuals, corporations, employees, and objects. These identities are resolvable at high throughput and interoperable by design.

The Credential Layer represents compliance results as verifiable credentials. KYC, KYB, KYE, KYO, AML checks, sanctions screening, ESG attestations, and risk states are stored encrypted off-chain. Only cryptographic commitments are anchored on Hedera, ensuring immutability and timestamping without exposing sensitive data.

The Compliance Logic Layer evaluates whether a transaction is allowed. It uses policy engines and, where relevant, smart contracts to determine whether credentials satisfy requirements. If a credential is missing, expired, invalid, or revoked, the transaction does not pass. This applies to both on-chain and off-chain transactions, making compliance consistent across systems.

The Verification Layer turns compliance into a scalable network function. Verifications consume Wecan tokens, and a fraction is burned. This connects the economics of the network to real compliance activity and supports planetary-scale verification demand.

Together, these layers create a compliance backbone that can grow from institutional onboarding to global transaction verification.

Post-Quantum, Hardware-Rooted Trust

Trust cannot be built on fragile foundations. Institutions operate on decades-long horizons. Regulators require long-term integrity. The future will include cryptographic disruption, including the potential impact of quantum computing.

Wecan integrates SealSQ secure elements to provide hardware-rooted institutional identity and post-quantum or hybrid signatures. Keys remain non-exportable. Institutions cannot be impersonated. Credential issuance and revocation become tamper-evident and provable. This is the kind of trust boundary regulated environments require, not as an upgrade, but as a baseline.

Post-quantum readiness is not a speculative feature. It is the responsible design choice for a compliance system meant to remain trustworthy for decades.

Digital Onboarding at Industrial Scale

Wecan is designed to work at real operational scale, not only in theory.

Digital KYC provides an industrial orchestration backbone, already capable of handling high volumes of onboarding. It coordinates remote identification, biometric and liveness checks, document verification, registry checks, organ and signatory verification, UBO resolution, sanctions and PEP screening, adverse media checks, and risk workflows with human oversight.

The key evolution introduced by Wecan is that the result of these regulated processes becomes a reusable verifiable credential, rather than a siloed file. Institutions can validate compliance without repeating the entire onboarding effort, and without copying sensitive documents across the ecosystem.

AI-Driven Automation and Rule Enforcement

The future of compliance will be shaped by AI—not because AI replaces regulation, but because AI will be required to operationalize regulation at scale.

Wecan integrates AI automation for document ingestion, structured extraction, normalization, confidence scoring, and provenance tracking. It reduces cost and increases consistency while strengthening auditability, because the system can explain where values came from and how they were derived.

More importantly, Wecan anticipates a world where rules are executed at transaction speed. Policy intelligence becomes critical. AI agents can assist in analyzing rule sets, detecting contradictions, simulating outcomes, and ensuring enforceability. Humans define the rules and the ethics. AI helps ensure those rules are respected continuously, consistently, and at scale.

In a world of billions of daily transactions, rule enforcement must become automatic. Wecan is designed for that world.

Wecan Vault and the Rise of Individual Sovereignty

Privacy is not negotiable. The future cannot require everyone to upload their most sensitive information to countless institutions and platforms.

Wecan Vault provides encrypted storage, access controls, and auditable sharing for sensitive documents and data. It enables compliance verification without forcing raw data disclosure. It also unlocks a deeper long-term shift: individual sovereignty.

One day, every person may choose to secure their personal information through Wecan-enabled wallets, not as a speculative concept, but as a practical necessity. People will interact with institutions, administrations, and service providers through digital channels, and AI agents will increasingly mediate those interactions. Individuals will need a way to prove compliance facts without spreading their private data everywhere.

Wecan provides a trust framework where individuals can authorize disclosure selectively, allow trusted agents to act on their behalf, and still keep control. This is how compliance becomes simpler for people, safer for society, and more efficient for institutions.

Beyond Humans and Companies: Compliance for Robots

The next economy will not be populated only by humans.

Robots, autonomous systems, and machine agents will become ubiquitous. They will buy and sell services, pay for energy, negotiate contracts, and move assets. In many contexts, robots may become far more numerous than humans. Their transaction volume could dwarf human transaction volume.

This raises a new question: how do we ensure that machines respect human rules?

Wecan extends compliance to objects and machines through KYO identities and credentials. It enables transaction rules to apply to robots in the same way they apply to humans and companies. It allows policy constraints—defined by humans and aligned with ethical principles—to be enforced at transaction time, not after damage is done.

This is not simply compliance. It is governance for autonomy.

When robots transact, society must be able to enforce constraints that protect safety, fairness, and legality. Wecan is designed to provide the compliance layer for that future.

Token Economics: Verification at Planetary Scale

Wecan tokens power the verification layer. When compliance is verified, tokens are consumed, and a fraction is burned. This ties the economics of the system to real usage, not to speculation.

Wecan's dual-chain architecture across Ethereum and Hedera enables both liquidity and high-performance verification. Supply conservation is maintained through a burn-and-mint mechanism across chains. Tokens minted on Hedera are infrastructural, enabling high-throughput verification and operational liquidity required for global adoption, while preserving total supply constraints across ecosystems.

The key point is simple. If the world moves toward billions of compliance verifications per day—across payments, asset transfers, and machine transactions—then verification capacity becomes a fundamental utility. Wecan tokens represent access to that utility.

The more compliance becomes transaction-native, the more verification becomes continuous. The more verification becomes continuous, the more a dedicated verification economy becomes necessary.

Business Cases

In private banking, onboarding can take weeks because trust is assembled manually. With Wecan, compliance becomes verifiable. A client's KYC state can be validated without repeating the entire document exchange. AML status can be checked continuously. Auditability becomes native. Onboarding collapses from weeks to minutes, not by lowering standards, but by upgrading the architecture.

In telco onboarding, duplication is structural. The same person proves the same facts repeatedly. With Wecan, those facts become reusable credentials. Updates propagate through credential lifecycle events. Verification becomes instant, privacy-preserving, and scalable.

In machine-to-machine payments, compliance becomes essential. An electric vehicle paying a charging station, a robot purchasing spare parts, a smart building paying for energy—these interactions require identity, authorization, and policy enforcement. Wecan enables them with deterministic compliance checks.

In ESG verification and tokenization, trust must be provable without forcing disclosure of sensitive data. Wecan enables ESG attestations to be verified as cryptographic states, auditable by regulators without becoming a data leakage vector.

These business cases are not separate markets. They are early expressions of the same future:

a world where compliance becomes a programmable layer of digital society.

Vision: The Global Compliance Operating System

Wecan 3.0 is not a compliance application.

It is a global compliance operating system for regulated institutions—and ultimately for a world where humans, AI agents, administrations, and robots interact through digital wallets and programmable transactions.

In that world, everyone carries a wallet. Not only for money, but for identity and permissions. Every payment, every asset transfer, every contract execution, every automated exchange can be validated against rules designed by humans and enforced by systems.

Wecan ensures that compliance becomes as natural as cryptographic signatures: always present, always verifiable, privacy-preserving, and auditable. It protects individuals by reducing unnecessary data exposure. It helps institutions by removing duplication and enabling continuous monitoring. It helps societies by enabling rules to be enforced at the speed of digital systems.

Compliance is no longer paperwork. It is protocol—secured for the post-quantum era, enforced at transaction time, and scalable to planetary adoption.

Note: Please find the link to the previous version of the white paper.