WHITEPAPER

SWISSLEDGER:
An Institutional Blockchain For Governments, Banks, And Enterprises

Ledger

1. Executive Summary

The concept of cryptographically secured chains of blocks was described as early as 1991 [1], but blockchain technology gained mainstream awareness 17 years ago, mostly through cryptocurrency. Since then, the space has expanded into thousands of networks aggregated mostly in either of two directions.

On one end, we have public blockchains, which are open, global systems designed to let anyone participate [2]. They have proven that programmable value can exist without a central operator, but they also force institutions to accept trade-offs that are hard to justify for critical infrastructure, such as uncertain governance, complex compliance boundaries, and operational risk that can be outside any single jurisdiction [3].

On the other end, we have private or organisational blockchains: systems deployed inside a company or a closed group [4]. They can be efficient, but they often reproduce the same problems that modern digital infrastructure already has—fragmentation, siloed data, duplicated compliance, and over-reliance on a small set of operators. In the long run, fully private infrastructure also tends to concentrate power and underinvest in shared robustness.

SwissLedger sits at the frontier of a third model: government-promoted, consortium-operated blockchain infrastructure designed to bridge public legitimacy and private utility. SwissLedger is a public-permissioned blockchain network, promoted by the City of Lugano, where participation is open in purpose, but validation is carried out by authorised institutions under a predictable governance framework [5].

At its core, SwissLedger is built to function as a shared digital infrastructure, a common ledger that institutions can rely on in the same way modern economies rely on shared rails of payments, identity, registries, and standards. By treating core banking services as common infrastructure, many institutions can “ride” on its “railroad”, rather than each entity building a closed system [5].

1.1. What is SwissLedger?

SwissLedger is a public permissioned, institutional-grade blockchain network designed to operate as a shared digital infrastructure for public administration, regulated industries, banking, and finance.

Unlike fully open networks where validation is anonymous, or fully private systems where control is centralized, SwissLedger adopts a consortium-based governance structure in which public authorities, banks, technology providers, and academic institutions collectively oversee the network.

By distributing control among reputable and legally accountable participants, the network seeks to achieve ***decentralization without sacrificing trust*** [5].

At the consensus level, SwissLedger uses a Proof-of-Authority (PoA) mechanism, where authorized validator nodes confirm transactions and maintain the ledger. This design was chosen to ensure scalability, energy efficiency, and to offer faster validation and clearer oversight compared to Proof-of-Work or Proof-of-Stake systems [6].

SwissLedger incorporates an execution environment based on the Ethereum Virtual Machine (EVM), the most widely adopted smart-contract execution environment globally [7], and anchored to Bitcoin and Ethereum, periodically writing Merkle roots of its state to these public blockchains to reinforce long-term integrity and public verifiability.

Architecturally, SwissLedger is structured in multiple functional layers. Its core ledger layer ensures immutability, transparency, and a shared source of truth across participants, while the smart contract layer enables programmable logic that automates conditional payments, escrow arrangements, compliance workflows, and other financial processes directly on the ledger. This is complemented by the API and integration layers, as well as compliance and security layers. In addition, the platform natively supports asset tokenization, enabling the issuance and management of stablecoins and other regulated digital assets in a compliant environment.

Taken together, these components position SwissLedger as a modular, evolvable, and institutionally accountable infrastructure designed to replace fragmented proprietary systems with shared governance and open access.

1.2. Who is SwissLedger for?

SwissLedger is designed around the idea that certain forms of digital infrastructure behave less like proprietary products and more like a digital commons. “Digital commons” [8] refers to infrastructure that serves multiple participants at once and is more effective when governed collaboratively rather than duplicated across isolated proprietary systems.

Transactions, asset registrations, and compliance events are recorded on a network operated collectively by public authorities, financial institutions, technology providers, and academic partners.

For **policymakers and regulators**, SwissLedger offers a model of digital infrastructure that preserves institutional accountability while enabling innovation through shared standards. **For municipal and cantonal authorities**, it delivers verifiable, tamper-evident registries that strengthen document certification, identity workflows, and public administration processes. **For enterprises and solution providers**, it offers a trusted foundation on which to build compliance platforms, asset registries, and sector-specific applications. **For banks and financial institutions**, it provides a common rail for open finance, tokenization, and interoperable settlement—an alternative to isolated proprietary systems. And for developers, it provides a familiar smart-contract environment, a sandbox for experimentation, and an API-based integration model that connects directly to real institutional systems.

Ultimately, SwissLedger exists to solve a coordination problem. It recognizes that the future of digital finance and public infrastructure cannot rely solely on private silos or purely open networks. Instead, it advances a third path: shared, institutionally anchored infrastructure that combines interoperability, compliance, and resilience. SwissLedger aims to strengthen digital sovereignty while unlocking collaborative innovation across the Swiss financial and public ecosystem—and, potentially, beyond.

1.3. Current Status

SwissLedger is not merely conceptual. Rather, it is the product of a phased evolution already tested in real-world environments. Its origins trace back to **LVGA**, the City of Lugano’s municipal payment token launched in 2020. What began as a city-level initiative has grown into a functioning ecosystem with **47,547 users** and acceptance across **more than 500 merchants** [9].

Building on the foundation of LVGA, Lugano introduced **3Achain** in 2021 as a permissioned blockchain maintained by local institutions. This phase served as a live testing ground, enabling controlled experimentation with peer-to-peer payments, digital identity verification, and document certification while refining governance and technical architecture. In 2025, SwissLedger emerged as the next stage of this progression, transforming a municipal experiment into a broader institutional platform intended to operate as a Swiss-wide digital financial infrastructure [5].

Today, the network operates with **over 30 nodes** managed by a combination of public institutions, private enterprises, and academic partners, validating the consortium model in practice. Participation includes entities such as Swisscom, Acer, Avaloq, BancaStato, the Università della Svizzera italiana, the Canton of Ticino, BitcoinSuisse, and Tether [5].

Additionally, SwissLedger has processed millions of transactions since its inception and maintained consistent block production with low latency. The system has demonstrated stability in pilot deployments without reported security breaches or downtime, strengthening confidence in its suitability for institutional workflows.

Beyond payments, SwissLedger already supports live applications such as document authenticity solutions for public administration and compliance platforms like Wecan in the financial sector. Private-sector applications extend further into corporate document notarisation, digital asset management, and artwork certification through platforms such as ArtChain [9].

Taken together, these deployments demonstrate that SwissLedger functions as intended: a consortium-governed, operational blockchain infrastructure already embedded in municipal services, compliance systems, and sector-specific innovation.

2. Foundation and Motivation behind SwissLedger

Modern financial and public-sector systems depend on digital infrastructure that was not originally designed for interconnectivity at scale. Over decades, banks, regulators, municipalities, and enterprises have developed internal systems tailored to their own operational needs. While these systems often function efficiently in isolation, they rarely communicate seamlessly with one another. The result is fragmentation: duplicated records, manual reconciliation processes, siloed databases, and overlapping compliance procedures [10].

In finance, this fragmentation manifests as repeated Know-Your-Customer (KYC) checks across institutions, delayed settlement cycles between counterparties, and complex integration requirements for new entrants [11]. In public administration, it appears as disconnected registries, paper-based documentation, and limited interoperability between agencies. These structural inefficiencies are not necessarily the result of poor design, but of systems optimized locally rather than collectively.

It is within this context that Distributed Ledger Technology (DLT) emerged.

A **Distributed Ledger Technology (DLT)** is a database shared across multiple nodes in a network, where each participant maintains a synchronized copy of records. Instead of relying on a single central server, updates are validated collectively according to predefined rules. Once recorded, transactions become tamper-evident and auditable by design [12]. DLT systems vary in how they balance openness, control, and accountability. This distinction is often described through the lens of permissionless and permissioned networks.

A **permissionless network**, such as Bitcoin or Ethereum, allows anyone to participate in transaction validation. These systems rely on decentralized consensus mechanisms and economic incentives to maintain trust without centralized oversight [13]. They offer censorship resistance and global accessibility, but they also introduce trade-offs such as regulatory ambiguity, latency constraints, and exposure to adversarial environments.

By contrast, a **permissioned network** restricts validation rights to designated participants. These validators are known entities, often subject to legal and regulatory proof. Permissioned systems can offer higher throughput, stronger identity alignment, and clearer governance structures [14]. Yet they require trust in selected authorities and risk reintroducing centralization if governance is poorly designed.

Neither model is universally superior. Rather, the optimal design depends on the institutional environment and the nature of the application.

Another foundational concept worth referencing is **Open Banking** and, more broadly, **Open Finance**.

Open Banking refers to frameworks that allow financial data and payment initiation capabilities to be securely shared across institutions through standardized interfaces (APIs), typically with customer consent. It enables third-party providers to access banking infrastructure in a controlled manner, reducing barriers to innovation and allowing services to be built on top of existing financial systems without requiring direct ownership of underlying data or rails.

Open Finance extends this model beyond traditional banking to include investments, insurance, digital assets, and a broader range of financial services. Its objective is not just access, but interoperability across the financial system as a whole. By expanding the scope of shared data and services, Open Finance moves toward a more integrated financial environment where users can interact across institutions and asset classes without being constrained by fragmented infrastructure. [15]

Yet open banking initiatives often remain constrained by bilateral integrations and proprietary platforms. While APIs enable communication, they do not automatically create shared infrastructure. Institutions may still duplicate back-end processes, and integration complexity can persist beneath the surface.

This leads to a broader economic framing: the concept of a **digital commons**.

A digital commons refers to infrastructure that functions as a shared resource, essential to many participants simultaneously and difficult to replicate efficiently in parallel [8]. Historically, certain physical infrastructures—railroads, highways, telecommunications networks—have exhibited these characteristics. In digital finance, core ledger systems may share similar properties. When such infrastructure is privately owned, there is a risk of underinvestment in interoperability or inclusivity if those investments do not directly increase short-term profits. Conversely, when entirely state-controlled, innovation may stagnate without market participation [16].

The challenge, therefore, is both technological and structural. Modern economies must decide how foundational digital systems should be governed, funded, and evolved.

3. Evolution and Roadmap of SwissLedger

SwissLedger is best understood as the latest stage in a deliberate progression: starting with a civic payment instrument that could be tested in the real world, moving into a permissioned network operated by institutions, and then scaling that foundation into an infrastructural vision for Swiss finance and public services. Each phase clarified a different requirement: usability, governance, institutional trust, and ultimately, national-scale interoperability.

3.1. From LVGA to 3Achain

SwissLedger's origin traces back to a very practical question: how do you make digital innovation show up in everyday life?

In 2020, the City of Lugano introduced LVGA, a municipal payment token designed to encourage local spending and to help citizens gain hands-on familiarity with digital payments. The programme created a real feedback loop where merchants gained visibility and demand through app-driven discovery and campaigns, while citizens and tourists experienced a digital wallet as part of everyday city life [17].

It was distributed and used through the MyLugano app, where users could earn a 10% cashback in LVGA at participating merchants and then spend those tokens across the same local network. The token maintains a fixed value relative to the Swiss franc (100 LVGA = 1 CHF) [18].

Just as importantly, LVGA was not designed as a stablecoin since users could only purchase it with CHF but not vice versa. Moreover, it can only be used in the closed market of Lugano. It was positioned as a payment token, an incentive instrument to reward local commerce, support civic engagement campaigns, and even cover selected municipal fees [19].

LVGA was later tokenised on 3Achain when it launched in 2021. That marked a transition from an application-managed municipal payment system to a ledger-based infrastructure. LVGA was migrated from a centralized maintenance system onto a common infrastructure where transactions could be recorded, validated, and audited across multiple nodes [9].

3.2. 3Achain (2021–2024)

In 2021, Lugano launched 3Achain, a permissioned blockchain network maintained by local institutions, and the public infrastructure project on which LVGA was tokenised. The underlying intention was to provide a Swiss institutional blockchain that businesses, universities, and governments could use as a shared ledger [20].

3Achain attracted over 30 public, academic, and private partners and processed thousands of transactions. It served as evidence that multiple institutions can coordinate around a common ledger, proving the public-private consortium rather than keeping the blockchain inside a single organisation [21].

During this period, LVGA's growth provided a measurable adoption signal. By 2024, LVGA had 47,547 users and roughly 490 merchants in the network [9]. In addition, private use cases from local small-medium enterprises (SMEs) emerged in the fields of notarization and NFT creation [21].

3.3. SwissLedger (2025–)

SwissLedger was the next evolution of Lugano's blockchain initiative, an attempt to scale what worked in a city setting into a potential shared national infrastructure for digital finance. 3AChain scaled into a platform that offered core financial services as a common infrastructure [22].

At this stage, SwissLedger's live network includes public, academic, and private nodes, alongside tens of thousands of users and 500+ merchants through the LVGA token [9]. Moreover, the consortium is expanding, with ~36 nodes currently and an explicit target of 50 nodes.

Nodes undergo legal and contractual checks, and many are well-recognized organizations such as Canton Ticino, VAR Group, Signum Bank, Bitcoin Suisse, HCLTech Confinale, as well as Avaloq, Acer, UBQ, and many others.

It is also in this phase that the platform's use case is expanding beyond local payments into a broader set of institutional and enterprise applications. For instance, Verify Lugano is a working public-sector service for document authenticity, already piloted by the City's Statistical Office to certify publications and open government data, with verification producing a time mark and provenance information tied back to the ledger [24].

Beyond public administration, SwissLedger is increasingly being applied across private-sector and cross-industry contexts where verifiability and auditability are critical. These include the certification of physical artworks through digital proofs of authenticity, registration of sports performance data to ensure integrity and traceability, tokenisation of real estate assets, and the use of blockchain-backed analytics for energy systems and infrastructure monitoring. Additional applications extend into fraud detection in online and crypto-related environments, as well as the certification of KYC and KYB procedures, enabling institutions to verify compliance processes without duplicating them across systems.

This expansion is further supported by initiatives such as the Swiss Digital Key cooperative network, which brings together institutions to coordinate the development of digital identity and credential solutions, as well as applications in the banking and finance sector that can be implemented on SwissLedger [25].

3.4. Swiss-Wide Adoption And Global Standard-Setting

Looking ahead, Swisslegder aspires to gain Swiss-wide adoption. In this stage, it will move from a successfully operating, multi-institution network to an infrastructure that can serve as a broader standard for interoperable finance and regulated digital services across Switzerland. The horizon extends even further toward international connectivity, particularly in the context of open finance and shared digital infrastructure models that transcend national boundaries [26].

At its current stage, SwissLedger already operates as a consortium-based network supporting live public and private sector applications. The next evolution will involve deeper integration into the Swiss financial ecosystem, expanded institutional participation, and a governance model capable of enlarged scale

4. Design Principles & Governance Model

4.1. Design Principles

SwissLedger is built around a simple but demanding premise: if digital infrastructure is going to support finance and public services, it cannot be treated like a product owned by one entity, nor like a fully open network where accountability is loose. It has to behave more like shared civic infrastructure, that is, reliable, auditable, and durable, while still being programmable enough to support innovation.

That framing leads naturally to a **public–private consortium** model. In conventional government systems, the state often carries the burden of building and maintaining digital rails, which can create slow upgrade cycles and limited experimentation. In purely private systems, infrastructure can move faster, but it tends to optimise for proprietary advantage and can harden into gatekeeping over time. A consortium design tries to keep the best of both worlds: public legitimacy and continuity on one side, private execution capacity and product velocity on the other. In practice, this means the network is operated by a mix of public institutions, private enterprises, and academic partners, rather than being controlled by a single operator [27].

The second principle is **no single point of control**. In many "enterprise blockchain" deployments, the technology is distributed, but the power to change rules, admit participants, or influence outcomes sits with one company or a small internal committee. Rather than this farce of decentralization, SwissLedger distributes operational authority across multiple independent institutions so that no single party can unilaterally rewrite governance or block participation for competitive reasons. For government and private stakeholders, this reduces dependency and platform risk, respectively [5].

A third principle is **predictable governance**. Regulated industries do not need only security but also stability and clarity around decision-making. Predictability here means that the rules for how changes happen, how participants join, and how disputes are handled are legible to institutions. This is vital since these institutions must, in turn, justify operational choices to regulators, boards, and risk committees. Therefore, consortium governance creates a decision structure that is neither "whoever has the most tokens decides" nor "a single entity decides," but an institutional process with explicit approvals [3].

Closely linked is **auditability**, which is foundational in both public administration and finance. Government workflows require traceability for accountability. Financial systems require audit trails for compliance, risk management, and

dispute resolution. SwissLedger's design leans into this requirement by ensuring that records are tamper-evident and verifiable across a network of independent operators. The result is not simply "more transparency," but more reliable provenance [28]: who did what, when, and under which authorised process.

Then there is **regulatory compatibility**, which means building infrastructure that can support identity, compliance controls, and institutional accountability as foundational requirements. Public blockchains often place these concerns at the application layer, which can work for consumer use cases but become fragile when the base layer must support regulated assets, municipal services, or compliance workflows. SwissLedger's approach is to keep the network programmable and modern, while ensuring that participation and critical flows can align with legal responsibilities.

Finally, SwissLedger is designed for **long-term neutrality**. Neutrality is what allows shared infrastructure to become trusted infrastructure, a system users can build upon for decades. Neutrality ensures that governance can outlive any single administration or participant. It also refers to the cost and access structures that do not punish adoption or force participants through expensive processes. The network is structured so that the main costs are infrastructural (running nodes and integrations), rather than levies imposed by the city as an operator.

4.2. Governance Model

SwissLedger's governance is designed to mirror its principles.

At the operational level, the network is maintained by **validator nodes** run by participating institutions. These validators are not anonymous actors. Rather, they are known entities that can be held accountable in the way regulated systems require. This choice is tightly connected to the network's Proof-of-Authority consensus mechanism, where performance and finality can be achieved without relying on economic incentives like in Proof-of-Stake or Proof-of-Work. While the full technical mechanics of consensus will be explored in the next section, the governance point is straightforward: validation is a responsibility assigned to institutions that have reputational and legal incentives to operate correctly [6].

Institutions join through a defined onboarding process, which includes checks that the organisation is legitimate and suitable to participate. Once an institution is approved to join the consortium, governance mechanisms determine whether it can operate a node and in what role. The intent is not to create exclusivity, but to prevent the network from being undermined by illegitimate actors, and to preserve the credibility required for banking and public-sector use cases.

Validator admission follows an approval logic that is intentionally conservative. Rather than relying on a simple majority vote that can be gamed by shifting coalitions, the model is closer to "high-consensus governance": if there is a meaningful objection from within the validator set, that objection carries weight. The practical advantage is that it discourages rushed expansions that could compromise trust, while also making it difficult for any single player to "buy influence" or force entry through financial leverage.

SwissLedger's governance also extends beyond validators into account and participation controls at the edge of the network. Because the network is designed for low-fee or near-zero-fee operation, it requires protections against abuse that would otherwise be deterred by transaction costs. This is why identity-linked onboarding and administrative controls exist around wallet creation and usage patterns. In practice, it prevents the network from being overwhelmed by spam activity while keeping legitimate usage at near-zero costs for institutions and citizens.

The broader governance trajectory is also designed to evolve with scale. In earlier phases, city-level stewardship can accelerate coordination and keep execution focused. As the network expands—more institutions, more sectors, and more national relevance—the governance model is expected to mature into a structure that better reflects a wider constituency. That evolution is a nod to the neutrality principle. If the network is to become shared infrastructure, its governance must also be shared, not city-bound [22].

This combination—known institutional validators, structured onboarding, conservative admission thresholds, and an explicit path toward more inclusive governance as participation widens—is precisely how SwissLedger aims to prevent monopolisation and gatekeeping. A single private operator cannot capture it because authority is distributed across independent institutions. A single public entity cannot dominate it indefinitely because the model is designed to broaden as adoption grows.

Summarily, SwissLedger's governance is not a layer added on top of technology but a core aspect that ensures it is decentralised enough to avoid malicious attacks, accountable enough to support regulated use, and structured enough to remain stable as it scales.

5. System Architecture

SwissLedger is structured as a blockchain architecture designed to support regulated financial and public-sector applications without sacrificing programmability or interoperability. At its core, it maintains a shared ledger in which transactions are recorded and state is updated through the execution of smart contracts. This execution environment is based on the Ethereum Virtual Machine protocol, but implemented within the network and adapted through modifications to meet SwissLedger's specific operational requirements.

Around this core, the architecture incorporates permissioning and identity controls, compliance and security mechanisms, and anchoring processes that periodically extend the integrity of the ledger to public blockchains. Together, these components allow transaction recording, contract execution, access control, and external verification to function coherently within a single institutional infrastructure. The result is a system that is modular, auditable, and adaptable to a wide range of use cases.

5.1. Ledger & Execution Layer

EVM Compatibility

SwissLedger is fully compatible with the Ethereum Virtual Machine (EVM), meaning that it supports the same smart contract execution environment used by Ethereum [29]. This compatibility allows developers to deploy Solidity-based contracts without modification, reuse established tooling, and integrate with existing libraries and standards.

By adopting EVM compatibility, SwissLedger avoids creating a proprietary execution framework that would isolate it from the broader blockchain ecosystem. Instead, it leverages the maturity of Ethereum's execution model while operating within a permissioned and governance-controlled environment. Developers familiar with Ethereum can deploy, test, and interact with SwissLedger using standard RPC endpoints and development frameworks.

This ensures portability of smart contracts and lowers the barrier to institutional adoption.

Smart Contract Execution Environment

At the execution layer, SwissLedger processes transactions that trigger state transitions through smart contracts. Each transaction is validated, included in a block by an authorised validator, and executed deterministically across all nodes in the network. The resulting state changes are replicated across the validator set.

Because SwissLedger operates under a Proof-of-Authority consensus model, contract execution occurs in a predictable block production cycle. There is no probabilistic mining competition or gas-price auction. Instead, validators sequentially sign and produce blocks, which reduces latency and increases transaction finality predictability [6].

Role-based permissions interact directly with smart contract execution. Accounts assigned specific roles may deploy contracts, submit transactions, or maintain full administrative privileges. These permissions are enforced at the protocol level through smart contract logic.

Token Standards

SwissLedger supports the primary Ethereum token standards, enabling diverse asset representations:

· **ERC-20 for** fungible tokens, including payment instruments and utility tokens.

· **ERC-721** for non-fungible tokens (NFTs), applicable to digital certificates, collectibles, and identity-linked assets.

· **ERC-2980,** specifically designed to represent financial instruments compliant with Swiss regulatory requirements.

These standards [30] ensure interoperability and predictable contract behaviour. Moreover, SwissLedger maintains compatibility with wallets, analytics tools, and contract libraries already in widespread use.

Representation of Financial Assets

Financial assets on SwissLedger are represented as tokenised instruments implemented through smart contracts that encode ownership, transfer logic, and applicable restrictions [31]. Because the execution environment is programmable, asset contracts can embed specific rules governing issuance, transfer conditions, and lifecycle management.

This is particularly relevant for regulated financial instruments, where transfer restrictions, ownership eligibility, or compliance checks may need to be enforced at the contract level. Through EVM compatibility and custom contract logic, SwissLedger allows financial assets to be represented digitally while aligning with jurisdictional regulatory requirements.

Financial Mechanics

At a mechanical level, SwissLedger processes transactions through state transitions recorded on-chain. When a transaction is submitted, it enters the mempool (subject to rate limiting), is selected by the next validator in the round-robin sequence, executed against the current state, and committed to a new block.

Because transaction fees are minimal or near-zero, the network does not rely on gas auctions for inclusion priority. Instead, predictability is achieved through validator sequencing and controlled participation.

Role-based controls interact with transaction processing by restricting which accounts may deploy contracts or perform specific operations. This ensures that system-level actions, such as validator changes or permission updates, remain restricted to authorised entities.

Integration Layer

SwissLedger exposes standard, Ethereum-compatible interfaces that allow developers, institutions, and application providers to connect to the network, submit transactions, query state, and deploy smart contracts using familiar tooling. This integration surface is central to SwissLedger's "plug-in" design: banks can connect core systems to shared ledger rails, fintechs can build products without negotiating integrations with other institutions, and public-sector applications can rely on a jointly maintained, consensus-driven ledger of record.

SwissLedger also enables a sandbox model for experimentation. In this sandbox

approach, new services can be piloted in a controlled setting—potentially using dummy assets, limited real funds, and/or a constrained environment—so that performance and compliance behaviour can be tested under realistic infrastructure conditions without exposing the broader network to unnecessary risk.

Regulators and public actors can observe system behaviour early, monitor emerging patterns, and evolve safeguards in step with innovation rather than after the fact.

5.2. Consensus Mechanism

SwissLedger operates under a Proof-of-Authority (PoA) consensus model using the Clique protocol [32]. Unlike proof-of-work or proof-of-stake systems, block production is not determined by computational competition or token-weighted voting. Instead, a predefined set of authorised validator nodes is responsible for producing and signing blocks.

In this model, validators are known institutions rather than anonymous participants. Each validator possesses a cryptographic signing key and participates in block production according to a structured rotation schedule. Because validators are permissioned and identifiable, the network does not rely on economic mining incentives to maintain integrity. Instead, trust derives from institutional accountability and collective governance.

Round-Robin Block Production

Clique consensus operates through a round-robin mechanism. Validators take turns proposing blocks in a predictable sequence. When it is a validator's turn, it assembles pending transactions into a block, signs it, and broadcasts it to the network. The next validator in the sequence then assumes responsibility for the subsequent block.

This rotation eliminates the unpredictability associated with mining-based systems. There is no race to solve cryptographic puzzles, no probabilistic leader election, and no gas-price auction to determine inclusion priority. Block production follows a known schedule, which significantly improves timing consistency [32].

Because validators are pre-authorised and network latency between them is relatively stable, block propagation times remain low, block variance is reduced and there are predictable block intervals. These features are particularly important for financial and public-sector applications where timing assumptions affect settlement logic and system integration.

Epoch-Based Validator Updates

Validator membership is not static. The Clique protocol supports structured updates to the validator set through epoch-based transitions [32]. At defined intervals (known as epochs), the network can incorporate changes to the validator list that have been approved through on-chain voting.

When a new institution seeks to join the validator set, an on-chain proposal is submitted. Existing validators cast approval or rejection votes using their signing keys. If the proposal receives the required majority, the new validator is incorporated into the active set at the next epoch boundary. Similarly, validators can be removed through the same structured voting process. All membership changes are recorded on-chain, ensuring transparency and auditability.

Majority Voting and Distributed Authority

The inclusion or removal of validators requires majority agreement among the existing validator set. No single institution can unilaterally alter network composition. This distributed approval model prevents concentration of control while preserving operational efficiency.

Because validators are identifiable institutions, voting decisions carry institutional accountability. Governance changes are therefore not only technically recorded but also reputationally anchored.

Resilience and Fault Tolerance

SwissLedger's PoA configuration is designed to tolerate partial validator failure. The network remains operational as long as a majority of validators are online and able to sign blocks. If fewer than half of the validators are offline, the remaining active majority can continue producing and propagating blocks without interruption [33].

This resilience is critical for infrastructure serving public institutions and financial actors. Temporary outages at individual nodes do not halt the system. Block production continues under the round-robin sequence among active validators. The absence of mining competition also eliminates certain instability risks common in public proof-of-work networks, such as chain reorganisations driven by hash-rate fluctuations.

Latency and Predictability Advantages

Because validators are known entities operating under coordinated infrastructure standards, network latency between nodes can be optimised [34]. Communication paths are more stable than in globally distributed anonymous mining networks. This produces lower propagation delay and more consistent block finality times.

Predictable block intervals improve integration reliability for institutions connecting core banking systems or municipal platforms to the ledger. Transaction settlement assumptions can be engineered with tighter tolerances because block production variance is reduced.

In effect, the consensus model trades anonymous decentralisation for operational predictability and institutional accountability.

DDoS Resistance in Context

SwissLedger's consensus mechanism interacts with its permissioned access model to reduce exposure to denial-of-service risks. Because wallet creation and transaction submission are controlled through authorised onboarding processes and rate-limiting mechanisms, the network is not open to unrestricted transaction flooding by anonymous actors.

Validators process transactions from known or provisioned accounts, and mempool behaviour is managed accordingly. While no network is immune to infrastructure-level attacks, the permissioned architecture reduces the surface area for large-scale spam attacks that commonly affect public blockchains.

By combining round-robin PoA consensus, majority-governed validator updates, and controlled transaction entries, SwissLedger achieves a balance between distributed authority and operational stability.

5.3. Node Roles

SwissLedger operates through a distributed network of nodes that perform distinct but complementary functions. While all nodes maintain visibility into the ledger state, not all nodes participate equally in consensus. The architecture distinguishes between validators, relayers, and simple nodes, each serving a specific operational purpose .

Validators

Validators are the core consensus participants within SwissLedger. These nodes are authorised to produce and sign blocks under the Proof-of-Authority model. Each validator holds a cryptographic signing key and participates in the round-robin block production schedule defined by the Clique protocol.

Validators are operated by recognised institutions, both public and private. Their responsibility is to:

- Propose and sign blocks when it is their turn.
- Verify blocks proposed by other validators.
- Participate in validator set updates through on-chain voting.
- Maintain full copies of the ledger state.

Because validators form the consensus backbone of the network, their infrastructure must meet reliability and availability standards. However, participation does not involve mining rewards or staking economics. Instead, it is motivated by institutional utility, governance participation, and strategic alignment with shared digital infrastructure. The only operational costs borne by validators are infrastructural: server hosting, network connectivity, and maintenance. SwissLedger itself does not levy transaction or participation fees from validator institutions.

At present, the network includes more than thirty nodes distributed across both public-sector entities and private organisations. This diversity contributes to operational resilience and reduces reliance on any single institutional actor.

Relayers

Relayers function as intermediary nodes that facilitate transaction propagation and integration with external systems. While they do not participate directly in block production, relayers help route transactions to validators and may provide RPC endpoints for application developers and institutional users.

Essentially, relayers serve as connectivity bridges. They allow applications, fintech platforms, and institutional systems to interact with the network without necessarily operating a full validator node. This reduces the barrier to entry for participation while contributing to network robustness by distributing transaction ingress points. Instead of routing all activity through a single gateway, multiple relayers can operate in parallel, reducing congestion risk and improving availability.

Simple Nodes

Simple nodes maintain a copy of the blockchain state but do not produce blocks or participate in validator voting. Their primary purpose is observation, auditing, analytics, or application-level interaction.

Because SwissLedger is designed for transparency and auditability, simple nodes allow institutions, regulators, and ecosystem participants to independently verify ledger state without assuming consensus responsibility. Simple nodes may also be deployed in sandbox or testing environments, enabling experimentation without affecting the validator set.

Institutional Onboarding and Participation

Institutions seeking to operate validator nodes undergo a structured onboarding process. Participation requires technical configuration, key provisioning, and formal inclusion into the validator set through on-chain voting by existing validators. This ensures that new nodes are technically prepared and collectively approved before assuming consensus responsibilities.

The network's growth model is therefore permissioned but not centrally controlled.

5.4. Anchoring to Public Blockchains

SwissLedger strengthens the integrity of its permissioned ledger by periodically anchoring selected portions of its blockchain state to public blockchains. This

anchoring mechanism creates externally verifiable proof that specific data existed at a given time, without exposing the underlying transactional content.

Block Span Hashing and Merkle Root Aggregation

Anchoring begins by selecting a defined span of SwissLedger blocks. Rather than publishing all block data externally, the system aggregates the selected block range into a cryptographic summary. This is typically done by computing a Merkle root [35] over the relevant block headers or state representations.

A Merkle tree allows multiple data elements to be compressed into a single hash value while preserving verifiability. Each block contributes to the tree, and the resulting Merkle root acts as a compact representation of the entire block span. Any alteration to any block within that span would produce a different Merkle root.

This root is then processed through a SHA-256 [36] hashing function to generate a fixed-length digest suitable for anchoring on external networks.

SHA-256 Digest Generation

The SHA-256 digest serves as the cryptographic fingerprint of the selected block range. Because SHA-256 is collision-resistant, it is computationally infeasible to generate a different data set that produces the same digest. This ensures that the anchored value uniquely corresponds to the original SwissLedger state.

Importantly, the digest contains no transactional details. It is a one-way cryptographic representation. External observers can verify the existence and timestamp of the digest without accessing sensitive underlying data.

Multi-Signature Approval Workflow

Before anchoring occurs, the process follows a structured on-chain approval mechanism. An authorised administrator proposes the anchoring of a specific block range by submitting the computed digest to a designated anchoring smart contract. Additional authorised administrators review and sign the proposal.

Once the required number of signatures is reached, the anchoring operation is finalised. This multi-signature requirement ensures that no single party can unilaterally anchor data or misrepresent the ledger state. The proposal, approvals, and finalisation are themselves recorded on SwissLedger, creating a transparent audit trail of anchoring activity.

If the administrator assigned to complete the anchoring does not perform the external submission within the defined timeframe, responsibility can be reassigned. This prevents operational delays and ensures continuity of the anchoring process.

OpenTimestamps and Bitcoin Anchoring

After internal approval, the SHA-256 digest is submitted to the Bitcoin blockchain using the OpenTimestamps protocol [37]. OpenTimestamps allows data hashes to be embedded into Bitcoin transactions in a scalable and cost-efficient manner.

Once confirmed on Bitcoin, the anchored digest benefits from Bitcoin's proof-of-work security and immutability. Because Bitcoin is widely regarded as one of the most secure public blockchains, anchoring to it provides strong external timestamping guarantees.

An OpenTimestamps proof file is generated, allowing any party to independently verify that the SwissLedger digest was committed to Bitcoin at a specific time. This verification can be performed without trusting SwissLedger operators. Anchoring mechanisms may also support interaction with Ethereum where appropriate, though Bitcoin anchoring remains the primary integrity reference due to its security characteristics.

Strengthening Auditability Beyond Permissioned Trust

Anchoring extends SwissLedger's trust model beyond its validator set. While consensus within SwissLedger is maintained by authorised institutions, anchoring ensures that historical ledger states can be independently validated against an external, globally distributed blockchain.

If an attempt were made to rewrite historical data within SwissLedger, the Merkle root corresponding to the altered blocks would no longer match the digest anchored on Bitcoin. This mismatch would be detectable by any auditor.

By combining permissioned consensus with public-chain anchoring, SwissLedger achieves auditability that does not depend solely on institutional coordination. Instead, it leverages public blockchain immutability to reinforce its own ledger guarantees.

6. Security, Compliance & Identity

SwissLedger's security framework addresses cryptographic integrity, operational abuse, regulatory expectations, and governance accountability. This section explores how SwissLedger enacts those safeguards in practice.

6.1. Low-to-Zero Fee Transaction Design

SwissLedger's economic model does not rely on high transaction fees to incentivise validators. Instead, validators are known institutions operating under reputational and governance incentives.

The absence of significant gas costs serves three main practical purposes. The first is that it ensures that public-sector workflows, such as document certification and registry updates, remain inexpensive. In addition, financial institutions can automate compliance-heavy processes without charges, and lastly, end-users interacting through approved applications are shielded from unpredictable cost spikes during congestion.

6.2. Anti-Flooding and Transaction Control

As established, SwissLedger is designed to support low- or zero-fee transactions, to improve usability for public services and institutional integrations. However, removing financial friction introduces a classic blockchain risk: spam and denial-of-service attacks [39].

To mitigate this, SwissLedger implements rate limiting at the mempool level. By default, a single address may have a maximum of eight pending transactions at any given time. If a ninth transaction is submitted before earlier ones are confirmed, it is rejected. This limit can be adjusted by individual nodes, but network consistency is maintained through majority alignment.

This mechanism performs two important functions. Firstly, it prevents automated flooding of the network from a single wallet, and secondly, it ensures that the zero-fee design does not compromise network stability.

Unlike public networks, where transaction fees act as the primary spam deterrent, SwissLedger provides controlled throughput and identity-linked participation as a substitute.

6.3. Account Management and Role-Based Controls

SwissLedger does not operate as an open-permission wallet system in the style of public blockchains. Instead, it implements a role-based permission framework managed through the WhitelisterAdmin smart contract.

This contract defines structured roles to be :

1. READONLY
2. TRANSACT
3. CONTRACTDEPLOY
4. FULL

Administrators are granted authority through explicit smart contract functions. Each administrator can assign roles to user accounts, and once assigned, that administrator becomes the **permissionsHolder** for that account. Other administrators cannot modify that account's permissions unless specific conditions are met.

Additional safeguards are built directly into the permission system to prevent conflicts and concentration of authority. For instance, an account that is already designated as an administrator cannot be reassigned casually, and certain protected roles—such as the Guardian—are insulated from modification by standard administrators. Only the contract owner retains the authority to remove administrators or modify core contract-level configurations.

Furthermore, if an administrator attempts to modify an account already managed by another permissions holder, the transaction automatically fails. These constraints are enforced at the smart contract level, not through informal governance, ensuring that access control cannot be overridden by discretion or convenience.

This structure achieves several outcomes. Multiple authorised administrators can manage different segments of the network, yet each remains accountable for the accounts under their control. Moreover, permission changes are executed and recorded on-chain, so they are transparent, traceable, and auditable.

This system mirrors the internal access control frameworks used by regulated institutions, but with the added advantage of programmed enforcement logic and accountability.

6.4. Identity-Linked Participation

SwissLedger is not designed as an anonymous, open-access network. Wallet creation and participation occur through approved administrative processes, typically embedded within application layers such as MyLugano [9] or institutional platforms. This means that wallets are not generated freely at the protocol level by unknown actors. Instead, onboarding follows defined pathways managed by authorised administrators and, where applicable, sub-administrators operating within approved jurisdictions.

Because wallet issuance is controlled, accounts can be linked to identity or compliance status when required by the use case. This structure enables identity-aware workflows without forcing a universal identity model onto all participants. While the protocol does not cryptographically enforce a strict “one person, one wallet” rule, it does prevent unrestricted anonymous wallet proliferation by limiting how accounts are created and authorised.

When combined with mempool rate limiting, this approach significantly reduces the attack surface that typically exists in permissionless environments, where actors can generate unlimited wallets and attempt to overwhelm the network.

6.5. Optional KYC, KYB, and AML Modules

SwissLedger is designed to support regulated environments without imposing a single compliance model on all participants. The base protocol does not mandate universal identity verification for every transaction. Instead, it provides flexibility for regulated actors to integrate compliance frameworks at the application or workflow level to meet their operational requirements.

This means that financial institutions using SwissLedger can implement KYC (Know Your Customer), KYB (Know Your Business), and AML (Anti-Money Laundering) procedures within their own systems before interacting with the ledger. In this model, compliance is enforced at the institutional layer, and transactions submitted to the network reflect decisions that have already passed regulatory checks. This preserves flexibility while ensuring that regulated participants can operate in alignment with existing legal obligations.

Beyond this flexible model, SwissLedger is exploring deeper integration of compliance logic directly into the execution layer of the network. The objective is to make certain regulatory conditions programmable within smart contracts themselves. Rather than relying solely on off-chain verification processes, compliance requirements could be embedded into the logic governing asset transfers or contract execution.

In such a design, a tokenised financial asset could enforce transfer restrictions automatically, allowing movement only between wallets that satisfy predefined regulatory criteria. Digital identity credentials could be verified on-chain across institutions, and access to financial services could be conditioned on programmable compliance checks that execute at the moment of transaction.

6.6. Validator Security and Resilience

SwissLedger operates using a Proof-of-Authority (PoA) consensus mechanism based on Clique [32], where a predefined group of authorised validators produces blocks in a round-robin sequence. In this model, validators are known institutions rather than anonymous participants, and each validator signs blocks in turn, ensuring predictable block production and consistent network performance.

The resilience of this approach lies in its tolerance for partial validator failure. The network is designed to remain operational even if up to half of the validators are offline. Because block production rotates among the validator set, temporary outages do not halt the system. This is particularly important for financial and public-sector infrastructure, where uptime and reliability are non-negotiable requirements.

In addition, validator membership is not static. The validator list can be updated through a transparent on-chain voting process. When a new validator seeks inclusion, an on-chain voting transaction is submitted, and existing validators review the proposal and cast approval or disapproval votes. At the conclusion of the defined voting period, the candidate is added to the validator set if the required majority is achieved.

All validator inclusion and removal decisions are recorded on-chain, creating a permanent and auditable trail of governance actions. No single validator can unilaterally alter the composition of the network, and the decision-making process remains transparent to participants and observers.

While PoA consensus does not provide immediate absolute finality in the strictest theoretical sense, its round-robin structure significantly reduces the likelihood of forks or reorganisations. The result is practical finality that is stable and predictable, which aligns with the operational expectations.

Taken together, this validator framework prevents unilateral control, distributes operational authority across independent institutions, and preserves high performance. It achieves the reliability expected of financial-grade infrastructure without relying on energy-intensive mining or purely economic incentive models.

7. Use Cases & Adoption

The preceding sections described SwissLedger as infrastructure: its governance, consensus model, layered architecture, and security design. This section moves from structure to application. It examines how the network is being used in practice, who is using it, and what forms of adoption have already materialised.

Table 1. *Main indicators of the SwissLedger blockchain.*

Indicator	Value
Total Blocks	25,544,087
Average Block Time	5 s
Number of Wallet Addresses	56,310
Total Transactions	1,130,790
Number of Nodes	33
Number of Public Entity Nodes	8
Number of Private Entity Nodes	23
Number of Academic Institutions' Nodes	2

Source: [48]

SwissLedger's use cases span municipal infrastructure, regulated finance, and private-sector certification. Each category reflects a distinct domain of application, yet all rely on the same underlying ledger, execution environment, and anchoring mechanisms described earlier.

7.1. Public, Municipal & Civic

SwissLedger's earliest and most visible deployments are rooted in municipal infrastructure. Lugano serves as the primary proving ground [9], but the architecture is not city-specific. The model is designed to be replicable across public administrations, enabling municipalities, regional authorities, and national institutions to adopt shared ledger infrastructure for certification, payments, and digital coordination without redesigning the core protocol.

Municipal Payment Token LVGA

At the centre of SwissLedger's municipal adoption is the LVGA payment token [9], which fosters digital participation in the MyLugano ecosystem. LVGA is issued by the city and operates as a municipal payment and incentive instrument [17].

LVGA is actively used by a broad population within Lugano's community.

Table 2. *Main Indicators of the LVGA Payment Token.*

Indicator	Value
Users	47,547
New Users (2024)	+43%
Youngest User's Age (Years)	14
Oldest User's Age (Years)	96
Average Age	25
LVGA in Circulation (CHF)	580,000
Merchants	490
New Merchants (2024)	110
Increase in LVGA Merchants' transaction volume (2024)	+97%

It has been activated by 47,547 distinct users, with diverse demographic participation—from as young as 14 to as old as 96—and an average user age of 25.

LVGA's circulation within the local economy is also substantial, with approximately 580,000 CHF worth of tokens active in the ecosystem, and nearly 490 merchants participating in the MyLugano network. In 2024 alone, 110 new merchants joined the LVGA programme, demonstrating accelerating interest from local businesses in integrating blockchain-enabled payments into their customer experience. Notably, the token's integration correlated to measurable economic value for participating merchants who reported a 97 % increase in revenue [9].

Statistical Reporting and Open Government Data Certification

SwissLedger addresses a core challenge in modern public administration: ensuring that published data remains trustworthy, verifiable, and resistant to manipulation over time. Traditional systems for managing and disseminating official statistics are often fragmented and centrally controlled, creating vulnerabilities around data integrity, version control, and auditability.

Through services such as Verify Lugano, the City of Lugano has implemented a system where statistical reports and open datasets are anchored to the ledger using cryptographic timestamping. Each publication is registered with a verifiable proof of authenticity, allowing users to independently confirm that the data they are accessing corresponds exactly to the version issued by the statistical authority [24]. Any alteration, whether accidental or malicious, becomes immediately detectable.

This shifts public data systems from a model of declared transparency to one of verifiable transparency. Researchers, policymakers, and citizens no longer rely solely on institutional assurances of correctness. Instead, they can validate data integrity directly. In doing so, SwissLedger enables public statistical offices to strengthen credibility, reduce reliance on centralised trust assumptions, and establish a reproducible and auditable foundation for data-driven decision-making.

7.2 Private Sector Applications

Beyond municipal and financial-sector deployment, SwissLedger is actively used by private enterprises that require verifiable records, programmable logic, and tamper-resistant audit trails. These integrations span multiple industries, each addressing a specific trust or coordination problem through shared ledger infrastructure.

NFT Creation

Within the SwissLedger ecosystem, NFT [40] creation is supported through infrastructure providers such as Noku [41], which enable the issuance and management of tokenised digital assets using standard EVM-compatible frameworks. This allows organisations to create verifiable digital representations of assets such as certificates and creative works, while anchoring their authenticity and ownership history on a shared ledger.

Unlike public NFT platforms, where counterparties are often anonymous and governance is external, SwissLedger provides a controlled environment in which

validators are known institutions. This ensures accountability in the validation process and allows NFT-based systems to be integrated into enterprise or institutional workflows where trust, compliance, and service reliability are required.

Digitalisation of Corporate Documentation

SwissLedger is used by enterprise technology providers such as Palo Alto SA and Owl Solutions SA to support the digitalisation and certification of corporate documentation. In this context, the ledger functions as a verification layer for critical business records, including contracts, compliance documents, and operational reports.

By registering cryptographic proofs of documents on-chain, organisations can ensure that records remain tamper-evident and independently verifiable over time. This reduces reliance on internal database controls and enables secure document exchange across organisational boundaries without requiring direct system integration or bilateral reconciliation processes.

Certification of Physical Works of Art

In the art and collectibles market, SwissLedger is applied to the certification of physical artworks through integrations such as OfficineBit. The core challenge in this domain is establishing provenance and authenticity for physical pieces, which are often subject to forgery or incomplete documentation.

Using SwissLedger, digital certificates linked to physical artworks can be registered with cryptographic proofs, creating a permanent and verifiable record of authenticity. This allows collectors, galleries, and institutions to validate provenance independently, reducing fraud risk and strengthening trust in high-value asset transactions [42].

KYC/KYB Deployment

Compliance platforms such as Wecan Group leverage SwissLedger to support Know Your Customer (KYC) and Know Your Business (KYB) processes. These procedures are essential in regulated industries but are often duplicated across institutions, leading to inefficiencies and inconsistent verification standards.

By anchoring proofs of completed KYC/KYB processes on a shared ledger,

institutions can verify that compliance checks have been performed without needing to repeat them or access underlying sensitive data. This enables a model of reusable compliance, where verification is shared while confidentiality is preserved. It also simplifies multi-party onboarding processes and reduces operational friction across financial and enterprise networks [11].

Enterprise Infrastructure and Integration Layer

SwissLedger also functions as an integration layer for enterprise IT providers such as Var Group, which support organisations in incorporating blockchain-based verification into existing digital systems. In this role, SwissLedger does not replace core enterprise software but complements it by providing a shared coordination and verification infrastructure.

Through API-based integration and smart contract execution, organisations can embed auditability, traceability, and rule-based logic into their workflows without redesigning their entire technology stack. This enables cross-organisational coordination while preserving system independence, reducing duplication of trust mechanisms, and allowing multiple parties to operate against a common, verifiable source of truth.

7.3. Financial Sector

SwissLedger's financial-sector positioning is grounded in a structural problem: modern financial infrastructure is predominantly privately owned, fragmented, and siloed. Core banking systems rarely interoperate seamlessly. Data exchange lacks standardisation. Innovation often requires duplicative investment by individual institutions building parallel systems [43]. While digital finance has advanced rapidly, its foundational infrastructure remains institution-specific rather than shared.

SwissLedger addresses this structural inefficiency by proposing a consortium-governed ledger designed to function as a common financial infrastructure. Rather than replacing banks, it provides a shared execution layer on which banks, fintech firms, and regulated institutions can build interoperable services [44].

Open Banking Infrastructure

Switzerland's approach to open banking [45] has been market-led. Unlike the EU's PSD2 framework, Switzerland has not imposed compulsory API standardisation [46]. This has created both flexibility and fragmentation.

SwissLedger introduces a ready-to-use, API-driven ledger environment capable of supporting open banking services through standardised interfaces. By combining EVM compatibility with a consortium governance model, the network provides: shared transaction rails for financial messaging and settlement, smart contract automation for rule-based financial processes, and interoperable APIs enabling fintech participation without requiring each bank to deploy its own blockchain infrastructure.

The objective is not to impose uniformity but to reduce redundant infrastructure costs. In this model, financial institutions can share a core ledger while maintaining competitive product layers above it.

Tokenisation of Financial Assets

SwissLedger includes a dedicated asset tokenisation module that supports the digitisation of real-world financial instruments, including bonds, currencies, real estate, and structured financial products. These tokenised representations [31] can embed regulatory attributes directly into their on-chain structure through the ERC-2980 Advanced standard introduced within the ecosystem.

Unlike regular ERC-20 tokens, this extended format allows regulatory conditions and asset-specific parameters to be encoded directly within the asset model.

For financial institutions, tokenisation on SwissLedger can reduce settlement friction, simplify asset transfer processes, and create programmable financial instruments aligned with Switzerland's DLT legal framework enacted in 2021 [46].

Custodial and Institutional Services

SwissLedger's architecture also supports institutional custody and multi-signature configurations suitable for banks and asset managers. The permissioned validator model and role-based wallet controls enable structured custodial arrangements that align with regulatory expectations for asset protection and fraud prevention [47]. This is particularly relevant for institutions integrating crypto-assets alongside traditional financial products.

Summarily, Swissleger offers varying benefits across different stakeholder groups. Consumers may experience faster settlement, lower transaction friction, and more portable digital identity processes, while banks benefit from shared infrastructure, reducing the need for duplicative blockchain investment.

Fintech firms gain access to standardised APIs and smart contract environments without negotiating bilateral infrastructure access with each institution. Finally, regulators and public authorities secure an auditable infrastructure with embedded compliance capabilities.

Swiss Digital Key

Swiss Digital Key is a cooperative initiative designed to promote and coordinate the development of digital identity, certification, and interoperability solutions within the SwissLedger ecosystem. It functions as a forum in which public institutions, financial actors, and technology providers collaborate to explore and define future applications of shared infrastructure [25].

Rather than directly implementing identity systems or compliance mechanisms, Swiss Digital Key operates as a catalyst for innovation. It brings together stakeholders to align on standards, identify use cases, and support the development of solutions that can later be deployed on SwissLedger by participating organisations. In this sense, it acts as a bridge between conceptual development and real-world implementation.

Its role within the broader ecosystem is therefore not to deliver technology directly, but to enable it. The developments associated with Swiss Digital Key are realised through the institutions and partners that participate in the network, many of which go on to implement these ideas as concrete applications on SwissLedger. In this way, it supports the evolution of the ecosystem while remaining distinct from the infrastructure itself.

7.4. Use Cases in Development

SwissLedger has a number of use cases in development. However, the common thread is that these use cases are not new products layered on top of the network, but extensions of the execution environment itself. They include features designed to make the ledger more usable for institutions that must operate under strict compliance, identity, and audit constraints.

One of the most important items in this pipeline is an **EVM-compatible financial compliance layer**. The intent is to make compliance conditions enforceable inside transaction and smart-contract logic. In practical terms, this means that the ability to issue, hold, or transfer certain tokenised assets can be made conditional on meeting defined requirements—such as KYC/KYB status, AML rules, or other policy constraints—so that regulated behaviour is enforced at the moment of execution.

It is best understood as a programmable compliance toolkit: institutions can opt into it when their use case demands it, and it can be applied to workflows like token issuance, asset transfers, or contract-triggered settlement, without forcing a single compliance model on every application running on the network.

Closely linked to this is the development of **decentralised digital identity** [48] **and storage** capabilities. The direction here is not simply "identity on blockchain," but identity as a reusable institutional primitive: a person or organisation can establish a digital identity, store relevant documents securely, and selectively share verified information with banks or service providers when required. This shifts KYC from repeated, siloed onboarding processes toward a model based on verified credentials. Importantly, the emphasis is on privacy-preserving sharing and regulated usability: documents do not need to live openly on-chain for the network to support verification and portability.

In addition to the compliance and identity layers under development, the roadmap includes further refinement of tokenisation standards and programmable transfer controls for regulated financial instruments.

SwissLedger's ultimate objective is to reduce integration friction for institutions, shorten development cycles for new financial services, and ensure that regulatory alignment is engineered into the infrastructure rather than layered on afterward.

7.5. Ecosystem & Partners

SwissLedger is not an isolated municipal experiment. It is embedded within a broader strategic initiative and supported by a growing institutional ecosystem.

At the centre sits Lugano's **Plan ₿** [49] programme, one of Europe's most visible city-level blockchain initiatives. Plan ₿ is a structural commitment to digital finance, innovation, and infrastructure, and SwissLedger operates as the regulated ledger backbone within that vision, supporting municipal payments, certification services, and enterprise experimentation under a coordinated governance model.

The validator network reflects this seriousness. Today, more than thirty nodes operate across public institutions and private entities, and the network is expanding towards a target of fifty nodes to deepen institutional distribution, resilience, and shared stewardship across sectors.

The ecosystem spans multiple categories.

On the public side, the City of Lugano sits as the promoter of the initiative, with expansion that already includes Canton Ticino and other Swiss-facing stakeholders. On the private side, the network includes major banking and digital-asset players such as Sygnum Bank and Bitcoin Suisse, alongside the kinds of firms banks already rely on to run critical systems — Avaloq and HCLTech (Confinale Wealth Solutions).

On the enterprise and technology front exist partners like Acer, plus large-scale IT and cybersecurity groups like Var Group, and Web3-native builders such as UBQ. Then there are the specialist operators and integrators that make the network usable in practice, including Noku, which contributes to operational onboarding and node activation flow.

This institutional depth has not gone unnoticed, and Lugano became the first municipality to join the Swiss Blockchain Federation. What began as a municipal innovation under Plan ₿ is evolving into infrastructure designed for Swiss-wide interoperability across banking, public administration, and enterprise systems. From there, the ambition is to offer a regulated, consortium-led blockchain architecture that other jurisdictions can replicate.

The goal is clear: build trusted digital infrastructure for Switzerland first, and in doing so, create a framework capable of extending globally.

8. Limitations & Future Work

8.1. Limitations and Proposed Solutions

Like any infrastructure designed for long-term institutional use, SwissLedger utilizes deliberate trade-offs. These choices enable reliability, auditability, and regulatory compatibility [50], but they also define the boundaries of its current capabilities and the areas where further evolution is both expected and actively underway.

One of the most visible limitations today is that SwissLedger operates primarily as institutional infrastructure rather than as a consumer-facing application platform. Most of its functionality is embedded within municipal services, financial integrations, and enterprise systems, meaning that end users often interact with SwissLedger indirectly through applications such as MyLugano or partner-operated platforms. This is not a technical constraint of the ledger itself, but a consequence of its positioning as a foundational layer rather than a retail application environment. The network addresses this by maintaining full smart contract programmability and EVM compatibility, allowing third parties to build user-facing applications without modifying the underlying protocol. As adoption expands beyond initial municipal deployments, the architecture already supports the development of richer applications that can expose SwissLedger's capabilities more directly to individuals and businesses.

Interoperability across heterogeneous blockchain environments [51] is another area where constraints naturally arise. SwissLedger strengthens its integrity by anchoring to public blockchains, but anchoring alone does not provide full bidirectional interoperability or native execution across external networks. This means that assets and workflows may require structured integration layers when interacting with other ecosystems. The architectural response to this limitation lies in its deliberate use of EVM compatibility, which aligns SwissLedger with the most widely adopted smart contract environment in the blockchain ecosystem. This design choice reduces integration friction and allows existing tools, contracts, and interoperability frameworks to be adapted for use on SwissLedger. As a result, while cross-chain execution is not the network's primary focus today, its technical foundation is aligned with widely supported standards that enable interoperability pathways to expand over time.

Another important limitation relates to extreme throughput conditions. SwissLedger's consensus model and validator topology are designed to deliver predictable performance under institutional workloads, and current deployments—municipal payments, certification services, and enterprise integrations—operate well within

these parameters. However, the network has not yet been subjected to sustained, large-scale transaction volumes so its behaviour under extreme load remains primarily a matter of engineering expectation rather than empirical observation. The protocol's design nonetheless provides a clear pathway for scaling. The modular structure of the system also allows application-level scaling strategies—such as batching, off-chain processing layers, or specialised execution environments—to be introduced where necessary. As adoption grows, real-world operational data will provide the basis for further optimisation.

8.2. Future Work

Beyond these present-day constraints, SwissLedger's development trajectory is focused on expanding its capabilities while preserving its core guarantees. One major direction is the continued development of programmable compliance infrastructure, enabling regulatory logic to be integrated directly into smart contract execution. This will allow tokenised assets, identity credentials, and financial workflows to enforce compliance conditions automatically at the protocol level rather than relying entirely on external verification systems.

Digital identity infrastructure [48] is another area of active development. The integration of verifiable identity layers would allow institutions and public-sector entities to issue and validate digital credentials directly on the ledger, enabling secure authentication, certification, and access control across organisational boundaries. This would extend SwissLedger's role into serving as a shared trust layer for identity and certification across institutional ecosystems .

Governance itself is also expected to evolve alongside adoption. As the validator network expands and participation broadens beyond its initial geographic and institutional base, governance structures may transition as well. This could include the establishment of a foundation designed to represent a wider set of stakeholders while preserving the neutrality and stability of the protocol [8]. Such evolution would reflect the network's transition from a municipally anchored deployment to infrastructure capable of serving national and potentially international ecosystems.

Taken together, these limitations and development directions reflect the realities of building regulated digital infrastructure. SwissLedger is not designed to maximise openness at the expense of trust. Its roadmap instead follows a different objective: to expand capability while maintaining the governance, security, and compliance properties required for real-world institutional adoption.

9. Funding, Backing & Sustainability

SwissLedger was initially developed within the context of Lugano's Plan ₿ initiative [49], which provided the public-sector backing necessary to design, deploy, and stabilise the core infrastructure. This early-stage support enabled the establishment of validator nodes, integration tooling, and operational governance without requiring a monetisation layer at the protocol level.

Today, the network operates through a distributed infrastructure model. Validator nodes are run by participating organisations across public institutions, financial entities, and enterprise technology partners. Each validator assumes responsibility for maintaining its own infrastructure, and this distributes the operational burden across the ecosystem rather than concentrating it in a single operator.

At present, SwissLedger does not impose mandatory transaction fees or validator rewards. However, sustainability planning anticipates the introduction of structured contribution mechanisms as network utilisation increases. Participating institutions may contribute through modest annual infrastructure fees in the range of 3,000 to 5,000 Swiss francs per validator node per year. These contributions are intended to fund core operational functions, including protocol maintenance, security monitoring, software upgrades, and continued engineering development.

As utilisation grows, Swissledger's structured contribution models and expanded validator participation, will ensure that the infrastructure continues to evolve, scale, and operate reliably over the long term.

10. Conclusion

Digital infrastructure underpins every modern financial system, public registry, and institutional workflow. Yet for decades, these systems have been built in isolation, with each institution maintaining its own databases, verification processes, and compliance controls. Public blockchains introduced a new paradigm with shared ledgers that anyone could verify. But their open, anonymous structure made them difficult to align with the accountability and governance requirements of regulated institutions. Private systems, by contrast, preserved control and compliance but perpetuated fragmentation and dependence on individual operators.

SwissLedger was designed to resolve this divide. It brings together the shared verification and cryptographic integrity of distributed ledgers with the governance, accountability, and operational predictability required by public institutions and regulated enterprises. Through its consortium validator model, programmable execution environment, and anchoring to public chains, SwissLedger creates a shared ledger that institutions can trust.

What began as a municipal digital payment initiative has matured into a multi-institutional ledger supporting certification services, programmable asset logic, and enterprise integrations. Public administrations use it to issue verifiable records and operate digital payment systems. Enterprises use it to anchor proofs, and manage digital assets. Financial institutions can integrate programmable compliance and tokenisation capabilities within an execution environment designed for regulated use. Validator nodes now operate across public and private entities, distributing responsibility for maintaining the ledger's integrity.

SwissLedger is not limited to a single use case, organisation, or sector. Instead, it provides a neutral execution layer upon which institutions can build interoperable systems while retaining independence. It ensures that digital coordination can occur without requiring blind trust in any single operator.

As adoption expands, the network is positioned to serve as foundational infrastructure across Switzerland, and then global financial and administrative systems. Its design allows new institutions to join without disrupting existing operations, and its governance model supports gradual, coordinated evolution. The same properties that enable municipal deployment today allow for global institutional adoption tomorrow.

SwissLedger ultimately represents a shift in how institutional infrastructure can be designed and governed. It demonstrates that shared digital systems can be both

verifiable and accountable, both programmable and regulated, both decentralised in operation and structured in governance. In doing so, it establishes a durable foundation for the next generation of public and financial infrastructure—one built not around isolated systems, but around shared, verifiable, and institutionally trusted digital commons.

11. For Further Reading

Learn more about Swissledger through these resources.

1. *Institutional Blockchains as Sustainable Commons: The Case of SwissLedger*.
L. Barisone and R. Bregy, "Institutional blockchains as sustainable commons: The case of SwissLedger," in *Proc. 2025 IEEE 45th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 493–499, Jul. 2025. [5]

2. *Blockchain Adoption in Local Government: The Case of Lugano.*
L. Barisone, E. Beretta, R. Bregy, V. Carbone, R. Gorini, and G. Zucco, "Blockchain adoption in local governments: The case of Lugano," FinTech, vol. 5, no. 1, p. 24, 2026. [9]

3. *SwissLedger and the Finternet Vision: The Path for a Unified Financial Ecosystem*.
L. Barisone, R. Bregy, and G. Perletti, "SwissLedger and the Finternet vision: The path for a unified financial ecosystem," in *DE CIFRIS KOINE Book Series, vol. VII, Preproceedings FCiR25 Acta Draft*, pp. 42–56, 2025. [22]

12. References

[1] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.

[2] A. A. Monrat, O. Schelén, and K. Andersson, "Performance evaluation of permissioned blockchain platforms," in *Proc. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 2020. [Online].
Available: *https://ieeexplore.ieee.org/document/9411380*

[3] M. Zachariadis, G. Hileman, and S. V. Scott, "Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services," *Information and Organization*, vol. 29, no. 2, pp. 105–117, 2019.

[4] B. C. Ghosh et al., "Leveraging public-private blockchain interoperability," in *Proc. IEEE INFOCOM Workshops, 2021*. [Online].
Available: *https://arxiv.org/pdf/2104.09801*

[5] L. Barisone and R. Bregy, "Institutional blockchains as sustainable commons: The case of SwissLedger," in *Proc. 2025 IEEE 45th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 493–499, Jul. 2025.

[6] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs. Proof-of-Authority: Applying the CAP theorem to permissioned blockchain," in *CEUR Workshop Proceedings*, pp. 1–11, 2018.

[7] Market.us, "Smart contracts market." [Online].
Available: *https://market.us/report/smart-contracts-market/*

[8] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge, U.K.: Cambridge Univ. Press, 1990.

[9] L. Barisone, E. Beretta, R. Bregy, V. Carbone, R. Gorini, and G. Zucco, "Blockchain adoption in local governments: The case of Lugano," *FinTech*, vol. 5, no. 1, p. 24, 2026.

[10] D. C. Mills, K. Wang, B. Malone, A. Ravi, J. Marquardt, et al., "Distributed ledger technology in payments, clearing, and settlement," Federal Reserve Board, 2016. [Online].
Available: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881204*

[11] M. M. Kowsar and A. A. Mintoo, "Blockchain in banking: A review of distributed ledger applications in loan processing, credit history, and compliance," *American Journal of Smart Research and Innovation*, 2025. [Online].
Available: *https://researchinnovationjournal.com/index.php/AJSRI/article/download/33/22*

[12] S. G. Savadatti, S. Krishnamoorthy, and R. Delhibabu, “Survey of distributed ledger technology (DLT) for secure and scalable computing,” *IEEE Access*, 2025. [Online].
Available: *https://ieeexplore.ieee.org/document/10836671*

[13] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online].
Available: *https://bitcoin.org/bitcoin.pdf*

[14] C. Cachin, “Architecture of the Hyperledger blockchain fabric,” IBM Research, 2016. [Online]. Available: *https://arxiv.org/abs/1606.02350*

[15] D. A. Zetzsche, R. P. Buckley, and D. W. Arner, “Open banking, data sharing, and the G20,” Univ. of Hong Kong Faculty of Law Research Paper, 2020. [Online].
Available: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3392214*

[16] F. Nagle, “Strengthening digital infrastructure: A policy agenda for free and open source software,” Brookings Institution, May 2022. [Online].
Available: *https://www.brookings.edu/articles/strengthening-digital-infrastructure-a-policy-agenda-for-free-and-open-source-software/*

[17] E. Marchiori, J. Trautmann, and R. Bregy, “The key role of a living lab in creating a blockchain-based digital ecosystem to support local businesses,” in *Digital Living Lab Days Conference Proceedings*, 2021. [Online].
Available: *https://surd.nl/wp-content/uploads/2023/06/DLLD_2021_-_Proceedings1.pdf*

[18] MyLugano, “LVGA / FAQ.” [Online]. Available: https://my.lugano.ch/faq/

[19] E. Beretta, R. Bregy, and G. Zucco, “From Bitcoin to stablecoins and their contribution to the monetary landscape: The case of Lugano’s Plan ₿,” *Vierteljahreshefte zur Arbeits- und Wirtschaftsforschung*, no. 2, pp. 249–260, 2025.

[20] 3Achain, *Accountable, Authoritative, Accessible: 3Achain White Paper*, 2021.

[21] Ticino Blockchain Technologies Association, *Swiss Digital Asset Market Report 2022 – Lugano’s 3Achain*, 2022.

[22] L. Barisone, R. Bregy, and G. Perletti, “SwissLedger and the Finternet vision: The path for a unified financial ecosystem,” in *DE CIFRIS KOINE Book Series, vol. VII, Preproceedings FCiR25 Acta Draft*, pp. 42–56, 2025.

[23] SwissLedger, “SwissLedger: An institutional decentralized ledger.” [Online].
Available: *https://ledger.swiss/en/#technology*

[24] Città di Lugano, “Blockchain notarization / Verify Lugano municipal communication,” 2023. [Online]. Available:
https://www.lugano.ch/dam/jcr:9e2d07b3-777b-4cb1-b45f-590cae90cc91/20230308-cs-notarizzazione-blockchain.pdf

[25] Città di Lugano, “SwissLedger – Swiss Digital Key announcement,” 2025. [Online].
Available: *https://www.lugano.ch/news/20250313-swissledger-swiss-digital-key.html*

[26] A. Carstens and N. Nilekani, “Finternet: The financial system for the future,” BIS Working Papers, no. 1178, 2024. [Online].
Available: *https://www.bis.org/publ/work1178.htm*

[27] E. Tan, S. Mahula, and J. Crompvoets, “Blockchain governance in the public sector: A conceptual framework for public management,” ***Government Information Quarterly***, vol. 39, no. 4, p. 101704, 2022. [Online].
Available: *https://www.sciencedirect.com/science/article/pii/S0740624X21000617*

[28] S. K. Radha, ***Formal and Decentralized Framework for Verifiable Trust: Self-Sovereign Identity, Blockchain Provenance, and Hardware-Rooted Assurance***. Notre Dame, IN, USA: Univ. of Notre Dame, 2026. [Online].
Available: *https://curate.nd.edu/articles/thesis/Formal_and_Decentralized_Framework_for_Verifiable_Trust_Self-Sovereign_Identity_Blockchain_Provenance_and_Hardware-Rooted_Assurance/31450135*

[29] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” 2016. [Online].
Available: *https://ethereum.github.io/yellowpaper/paper.pdf*

[30] Ethereum Foundation, “Ethereum improvement proposals (EIPs): Token standards (ERC-20, ERC-721, ERC-2980).” [Online].
Available: *https://eips.ethereum.org/EIPS/eip-20*;
https://eips.ethereum.org/EIPS/eip-721; https://eips.ethereum.org/EIPS/eip-2980

[31] OECD, “Tokenisation of assets and distributed ledger technology in financial markets,” 2025. [Online].
Available: *https://www.oecd.org/finance/tokenisation-of-assets.htm*

[32] Ethereum Foundation, “EIP-225: Clique Proof-of-Authority consensus protocol,” 2017. [Online].
Available: *https://eips.ethereum.org/EIPS/eip-225*

[33] M. M. Islam, M. M. Merlec, and H. P. In, “A comparative analysis of Proof-of-Authority consensus algorithms: Aura vs Clique,” in ***Proc. 2022 IEEE International Conference on Services Computing (SCC)***, 2022. [Online].
Available: *https://ieeexplore.ieee.org/document/9860157*

[34] X. Chen, K. Nguyen, and H. Sekiya, “On the latency performance in private blockchain networks,” ***IEEE Internet of Things Journal***, 2022.

[35] R. Merkle, “A digital signature based on a conventional encryption function,” 1987.

[36] National Institute of Standards and Technology, ***Secure Hash Standard (SHA-256), FIPS 180-4***, 2015. [Online].
Available: *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf*

[37] P. Todd, "OpenTimestamps: Scalable, trust-minimized timestamping with Bitcoin," 2016. [Online].
Available: *https://opentimestamps.org*

[38] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "On the security and performance of Proof of Work blockchains," in Proc. ACM CCS, 2016.

[39] X. Xu, I. Weber, and M. Staples, ***Architecture for Blockchain Applications***. Cham, Switzerland: Springer, 2019.

[40] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," 2021. [Online].
Available: *https://arxiv.org/abs/2105.07447*

[41] Noku, "Noku." [Online].
Available: *https://www.noku.io/*

[42] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," ***Applied Innovation Review***, vol. 2, pp. 6–19, 2016. [Online].
Available: *https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf*

[43] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the Fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services," ***Journal of Management Information Systems***, vol. 35, no. 1, pp. 220–265, 2018. [Online].
Available: *https://doi.org/10.1080/07421222.2018.1440766*

[44] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and J. N. Barberis, "Decentralized finance (DeFi)," ***Journal of Financial Regulation***, vol. 6, no. 2, pp. 172–203, 2020.

[45] G. Colangelo and P. Khandelwal, "The many shades of open banking: A comparative analysis of rationales and models," ***Internet Policy Review***, vol. 14, no. 1, 2025. [Online].
Available: *https://policyreview.info/articles/analysis/many-shades-open-banking*

[46] Federal Council of Switzerland, "Legal framework for distributed ledger technology and blockchain in Switzerland," 2018. [Online].
Available: *https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73535.html*

[47] D. Yermack, "Corporate governance and blockchains," ***Review of Finance***, vol. 21, no. 1, pp. 7–31, 2017. [Online].
Available: *https://doi.org/10.1093/rof/rfw074*

[48] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," Sovrin Foundation, 2016. [Online].
Available: *https://sovrin.org/library/the-inevitable-rise-of-self-sovereign-identity/*

[49] Città di Lugano, "Lugano Plan ₿ initiative," 2022. [Online].
Available: *https://planb.lugano.ch/*

[50] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," ***Communications of the ACM***, vol. 63, no. 7, pp. 80–90, 2020. [Online].
Available: https://doi.org/10.1145/3359552

[51] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," ACM Computing ***Surveys***, vol. 54, no. 8, pp. 1–41, 2021. [Online].
Available: *https://doi.org/10.1145/3471140*


Ledger
L V
G A
Città
di Lugano