Whitepaper

SwissLedger: An Institutional Decentralized Ledger

Abstract

SwissLedger is a blockchain-based distributed ledger system designed for various applications and promoted by the City of Lugano. It is compatible with the Ethereum Virtual Machine (EVM) and uses Proof of Authority (PoA) consensus. SwissLedger combines efficiency, security, and regulatory compliance. This document describes the technical features of SwissLedger, its consensus model, and potential use cases.

Introduction

Blockchain technologies have revolutionised the way digital data and transactions are managed. However, institutional adoption of these technologies requires platforms that strike a balance between security, scalability, and regulatory compliance. SwissLedger addresses these challenges by providing a DLT solution designed to meet the needs of government and corporate entities.

Recognized for its excellence in technology and finance, Lugano has embarked on an ambitious project to promote digitalization and the adoption of blockchain technologies through the SwissLedger platform. Formerly known as 3Achain, this platform represents the evolution of a permissioned blockchain ecosystem designed to provide security, scalability, and regulatory compliance. With SwissLedger, Lugano aims to solidify its position as a global leader in technological and financial innovation.

SwissLedger is a versatile and innovative platform supporting a wide range of public and private applications. In the following sections, a description of the initiative, some use cases, and its technical foundations are provided.

SwissLedger and Swiss Digital Key: A Manifesto for Technological Innovation

SwissLedger: Evolution of the Initiative

The City of Lugano in Switzerland has emerged as a pioneering fintech and blockchain experimentation community. In 2020, the Municipality issued the first city-level payment token (LVGA) in Europe, a stable digital currency used as a cashback policy to promote local commerce. This initiative currently has 47’547 users and is accepted by 500 local retailers, demonstrating the city’s commitment to leveraging digital currencies for economic incentives.

In 2021, Lugano launched 3Achain, a permissioned blockchain network maintained by local institutions, as a public infrastructure project on which the LVGA is tokenized. The goal was to provide a Swiss institutional blockchain that businesses, universities, and governments could use as a shared ledger. Over 30 corporate and public partners joined the network, which processed thousands of transactions. Building on that foundation, in 2025, SwissLedger was conceived as the next evolution of Lugano's blockchain initiative. SwissLedger aims to scale the 3Achain concept into a national infrastructure for digital finance, transforming a city experiment into a Swiss-wide platform for banking and industry. In essence, SwissLedger proposes to treat core banking services as common infrastructure, analogous to making banking IT a shared "railroad" on which many can ride, rather than each institution building its closed system.

Swiss Digital Key, a Laboratory for Financial Evolution

One of SwissLedger's main goals is to create an infrastructure that facilitates innovation and collaboration among various actors in the financial and technological sectors. Within this framework, the Swiss Digital Key laboratory will be developed to test and create advanced solutions tailored specifically to the banking sector. This project aims to modernize financial services by leveraging blockchain technology to enhance security, transparency, and regulatory compliance. The Swiss Digital Key offers an opportunity for the Swiss banking system to adopt regulated technologies and innovate its operating models.

Swiss Digital Key is a collaborative network between the City of Lugano, Avaloq, HCLTech, Noku AG, UBQ SA, Università della Svizzera Itaaliana, and Scuola Universitaria Professionale della Svizzera Italiana. This initiative aims to promote open innovation in digital banking, blockchain-based payments, identity and authority verification, ledger certification, open banking, and other future-focused financial technologies. This groundbreaking initiative provides access to best-in-class solutions, incorporating key insights and technologies from systems already tested with innovative digital products developed by the City of Lugano and several project partners. These solutions have already been validated through thousands of transactions and the operation of a multi-node network involving over 30 corporate partners.

The project addresses structural and regulatory challenges in the Swiss financial sector, including:

- International Competitiveness: Enhancing Switzerland's attractiveness as a financial hub through cutting-edge technologies.
- Open Banking: Providing a technological framework to facilitate the transition to open and interoperable banking systems.
- Innovation and Sustainability: Creating an ecosystem that supports process automation and regulatory compliance.
- Accessibility: Ensuring fast, secure, and user-friendly services for consumers and businesses.

Technical Characteristics of SwissLedger

SwissLedger is a permissioned blockchain based on the Ethereum Virtual Machine (EVM) and employs a Proof-of-Authority (PoA) consensus protocol using Clique. The network utilizes a predefined group of validators, including prominent institutions such as Bitcoin Suisse AG, Avaloq, and NOKU AG, which coordinate in a round-robin mechanism to efficiently and reliably add new blocks.

PoA Clique Consensus

- Round-robin Validators: Validators sequentially sign blocks, ensuring rapid and consistent block production.
- Flexible Validator List: Validators can be added or removed through on-chain voting procedures, with changes taking effect after defined epochs.
- Resilience: The Clique consensus maintains network functionality even if up to 50% of validators are offline.
- Eventual Finality: While forks or reorganizations may occur due to competing blocks, the round-robin management greatly minimizes these events.

Validator Voting Process

- A prospective validator node requests inclusion by submitting an on-chain voting transaction.
- Existing validators cast their votes by approving or disapproving the inclusion.
- At the end of the voting epoch, the candidate validator is added if the majority of votes support inclusion, updating the validator list within the smart contract.
- The entire voting process is transparent, traceable, and auditable via blockchain records.

Token Standards

SwissLedger supports the main Ethereum token standards:

- ERC-20: For fungible tokens such as cryptocurrencies and utility tokens.
- ERC-721: For non-fungible tokens (NFT), applicable in artistic and digital applications.
- ERC-2980: Specifically designed to represent financial assets compliant with Swiss regulations.

Security Mechanisms

Transaction Limiting

Rate limiting in the mempool ensures blockchain security and efficiency, particularly for fee-less transactions. The limit for pending transactions per single address is initially set at 8, based on SwissLedger's default configuration. Given the fully decentralised system, nodes can independently adjust this limit. Network consistency is maintained through majority consensus, allowing dynamic adaptation to user needs, balancing security and performance.

Node Management

Network access is restricted exclusively to approved nodes meeting rigorous security standards. Nodes must provide verified credentials, complying with smart contract-defined security criteria.

Account Management

SwissLedger uses a role-based permission system managed through the WhitelisterAdmin smart contract. This system allows approved sub-administrators to assign roles to user accounts securely and traceably. These sub-administrators are granted full administrative permissions by the contract owner through the addAdmin(address) function. Once authorized, an administrator can manage the roles of other users using the assignAccountRole function.

Available Roles

Roles are assigned as strings and correspond to the following permission levels:

- "READONLY" (0): View-only access.
- "TRANSACT" (1): Ability to perform transactions.
- "CONTRACTDEPLOY" (2): Ability to deploy smart contracts.
- "FULL" (3): Complete access, including network configuration, node approval, and permission management.

Role Assignment Process

To assign a role, an administrator calls the assignAccountRole(address account, string memory roleId) function with:

- account: the address to authorize
- roleId: one of the predefined role strings

This operation grants the user view-only access and assigns the calling admin as the permissionsHolder for that user, preventing other admins from modifying the account's permissions.

Required Conditions

- The target account must not already be an admin.

- The target account must not be the Guardian.
- The calling administrator must be recognized as an admin and must either already be the permissionsHolder or no permissionsHolder must be set for the account.

Protections and Restrictions

- If another admin tries to modify an account managed by someone else, the transaction will fail.
- Only the contract owner can remove admins or change contract-level settings.
- Guardian and external super-admin accounts are not modifiable by regular admins.

Additional Functions

- isAdmin(address account): Returns true if the address has admin rights.
- modifyPermissionsHolder(address account, address newHolder): Manually reassigns the permissionsHolder of a user.

This system ensures decentralized control over account permissions while maintaining strict access control, auditability, and conflict prevention. Each admin is fully accountable for the accounts they manage, promoting secure and transparent administration across the SwissLedger network.

Anchoring System to Bitcoin

The SwissLedger Anchoring system ensures data immutability and temporal verifiability within a permissioned blockchain by leveraging the OpenTimestamps protocol to generate reliable cryptographic proofs. The core of this process is managed by the "BlockchainAnchor" smart contract, which utilizes a multi-signature mechanism to ensure that each anchoring event receives approval from multiple administrators.

When proposing to anchor a specific range of blocks (defined by the blockSpan smart contract variable), an administrator calculates the SHA256 digest of the data. The proposal undergoes validation to confirm that the proposed interval starts immediately after the last anchored block and concludes accurately. Subsequently, additional authorized administrators add their signatures. Once the minimum required signatures are collected, the anchoring is finalized: the system updates the state of the last checked block and assigns the responsibility for uploading the OpenTimestamps (OTS) proof.

The assigned validator then creates and uploads the OTS proof, verifying that the digest matches the original anchor hash. If the designated administrator fails to upload the proof within the defined timeframe, the system allows another administrator to assume this responsibility through a first-come, first-served reassignment procedure. The entire process is supported by decentralized monitoring, automating proposal submissions and anchoring uploads, thus ensuring continuous operation and efficient management.

System Architecture and Key Components

1. BlockchainAnchor Contract
    - Central component managing all anchoring operations.
    - Utilizes multi-signature to secure consensus among administrators.
    - Stores anchoring data (hashes) and corresponding OTS proofs.
2. Permission System
    - Validator management through the OpenZeppelin AccessControl smart contract.
    - Critical operations limited to authorized administrators.
3. OpenTimestamps Verification Mechanism
    - Validates OTS files by deserializing byte arrays, verifying payload, OTS version, and hash types.
    - Retrieves and compares digest from OTS file to original anchor hash.

Detailed Operational Workflow

Initialization

- Deploy contract referencing permissions management contract.
- Define minimum required signatures (requiredSignatures).

Multi-signature Anchoring Process

- **Anchoring Proposal:**
    - Administrator proposes anchoring by computing SHA256 digest.
    - Proposal validated by verifying correct block intervals and administrator authorization.
    - Initial proposal registers automatically the proposing administrator's signature.
- **Signature Collection:**
    - Additional authorized administrators approve the anchoring by adding signatures.
    - Signatures counted; reaching minimum threshold finalizes anchoring.
- **Finalization:**
    - System updates the last checked block upon reaching minimum required signatures.
    - Assigns the administrator responsible for uploading the OTS proof.

OTS Proof Management

- **OTS Upload:**
    - Assigned administrator generates and uploads OTS proof, verifying digest consistency.
- **Reassignment Mechanism:**
    - If the assigned administrator fails to upload within the specified timeframe (currently 30 minutes), another administrator may claim responsibility via a first-come, first-served reassignment.

Off-chain Monitoring

- Nodes continuously propose anchoring via automated cron jobs.

- Actively manage and monitor OTS proof uploads, ensuring timely and verified operations.

Auditability and Security

- Each anchoring event records detailed logs of administrative actions, providing full transparency and auditability.
- Multi-signature consensus significantly enhances security, distributes validation responsibility, and maintains operational continuity and reliability.

Connecting to the Network

To interact with the SwissLedger blockchain, you can connect to either the Mainnet for production-level applications or the Testnet for development and testing purposes.

Mainnet

- Public RPC: https://swiss-ledger-rpc.noku.io
- Explorer: https://explorer.ledger.swiss
- ChainID: 110

Testnet

- Public RPC: https://testnet-swiss-ledger-rpc.noku.io
- Explorer: https://explorertest.ledger.swiss
- ChainID: 222

Use Cases *(non-exhaustive list)*

Digital Identity

SwissLedger enables the creation of secure, verifiable digital identities that comply with data protection regulations.

Supply Chain Traceability

The platform provides tools to track products along the entire supply chain, ensuring transparency and authentication of assets.

Tokenisation of Financial Assets

Thanks to Ethereum-compatible standards, SwissLedger facilitates the digital representation of stocks, bonds, and derivatives.

Gaming and Entertainment Applications

NFT support enables the creation of unique digital assets, ideal for gaming platforms and digital collectibles.

Piece of Art Certification

SwissLedger provides services to legally certify, thorough blockchain, a physical piece of art, ensuring traceability, trustworthiness, and high legal standards.

Conclusion

SwissLedger is an institutional blockchain platform designed to address security, efficiency, and regulatory compliance challenges. Its PoA system, combined with advanced functionality and a focus on innovation, is an ideal solution for government agencies and corporations wishing to adopt blockchain technology in a secure and scalable manner.