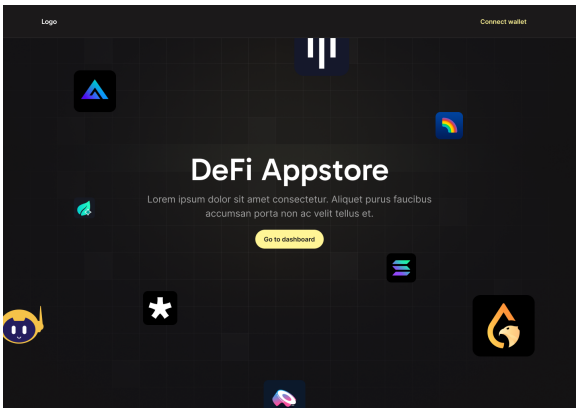
Lockton One: Between Freedom and Regulation

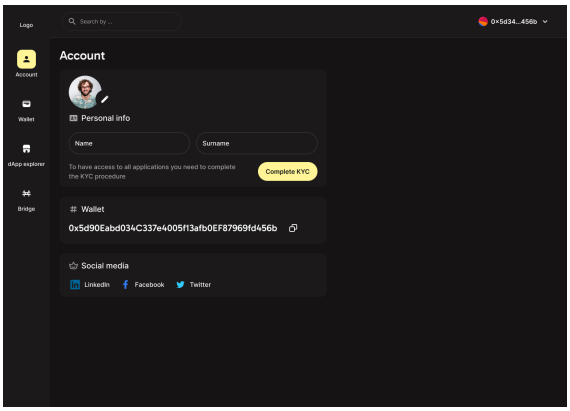
or

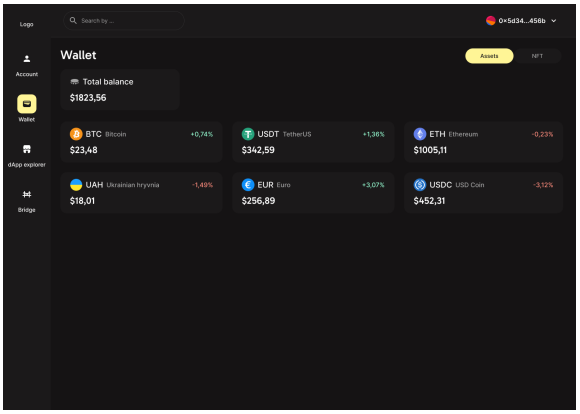
How to reach consensus in the blockchain industry?

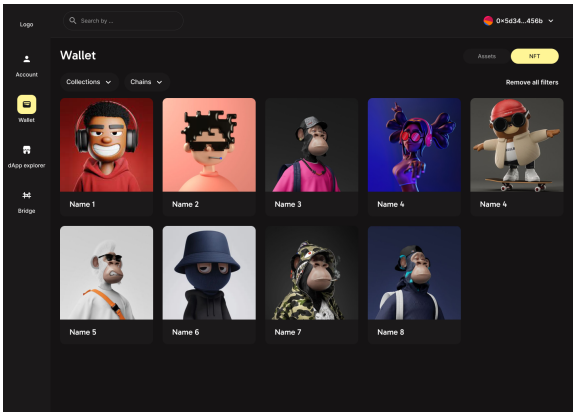
Table of contents

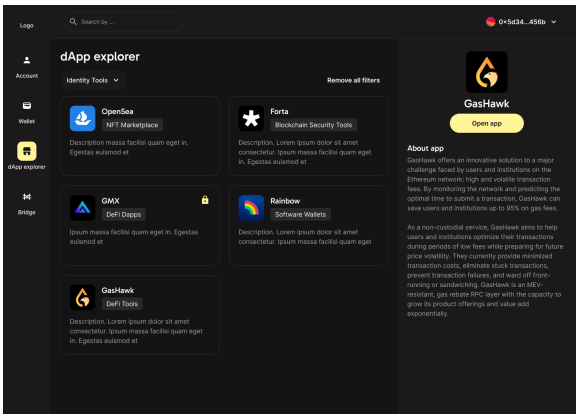
DAPPSTORE

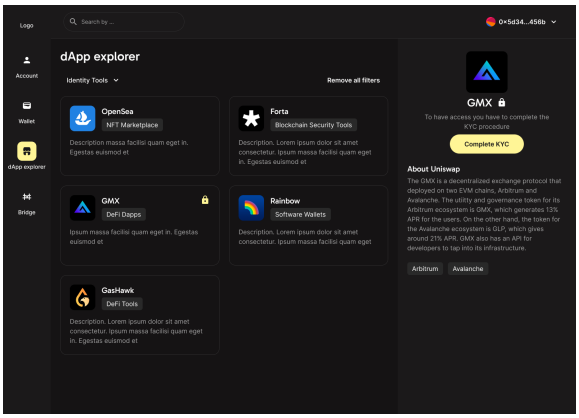

Logo
Connect wallet
DeFi Appstore
Lorem ipsum dolor sit amet consectetur. Aliquet purus faucibus accumsan porta non ac velit tellus et.
Go to dashboard

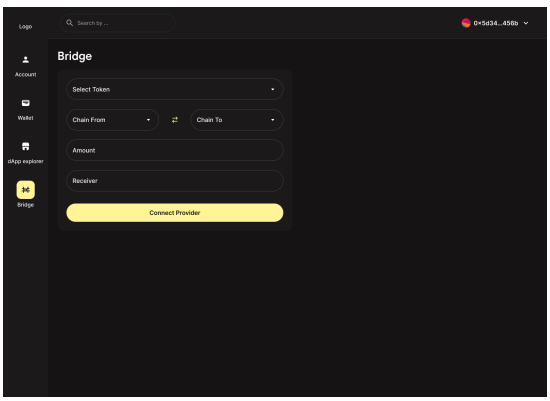

Account
Personal info
Name
Surname
Complete KYC
Wallet
0x5d90Eabd034C337e4005f13afb0EF87969fd456b
Social media
LinkedIn
Facebook
Twitter


Wallet
Assets
NFT
Total balance
$1823,56
BTC Bitcoin +0,74% $23,48
USDT TetherUS +1,36% $342,59
ETH Ethereum -0,23% $1005,11
UAH Ukrainian hryvnia -1,49% $18,01
EUR Euro +3,07% $256,89
USDC USD Coin -3,12% $452,31


Wallet
Assets
NFT
Collections
Chains
Remove all filters
Name 1
Name 2
Name 3
Name 4
Name 4
Name 5
Name 6
Name 7
Name 8


dApp explorer
Identity Tools
Remove all filters
OpenSea
NFT Marketplace
Forta
Blockchain Security Tools
GMX
DeFi Dapps
Rainbow
Software Wallets
GasHawk
DeFi Tools
GasHawk
Open app
About app

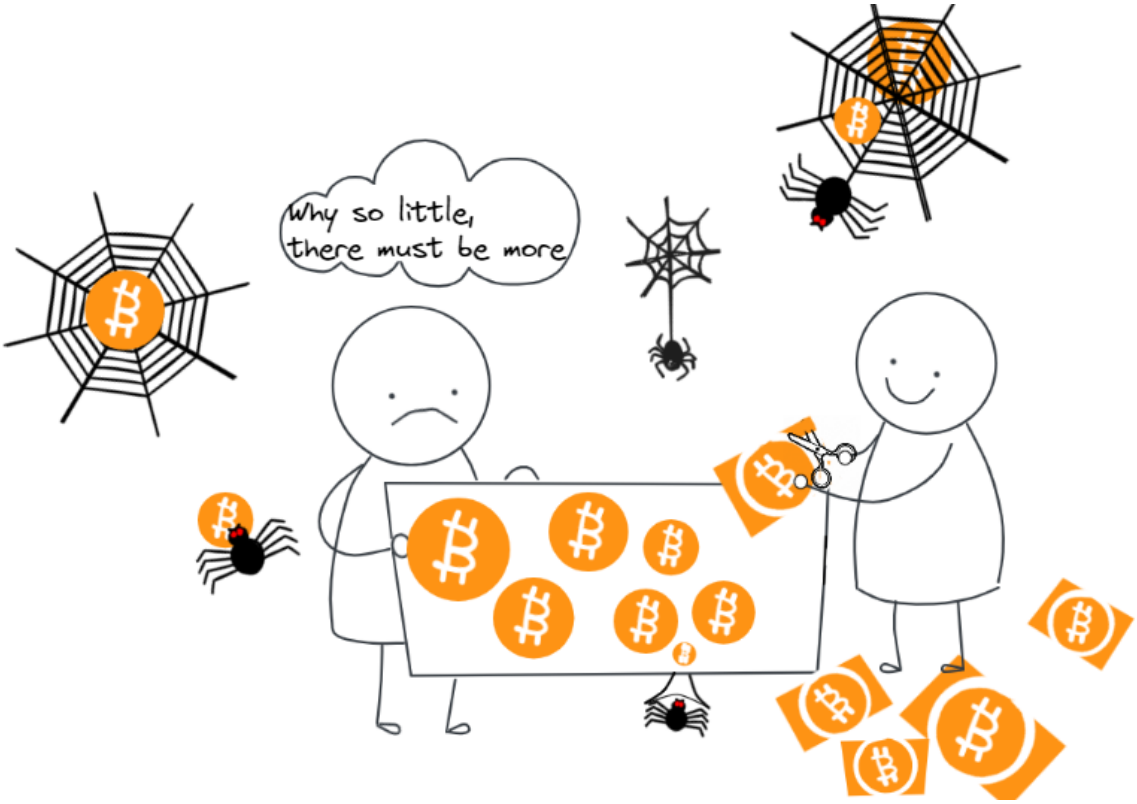

dApp explorer
Identity Tools
Remove all filters
OpenSea
NFT Marketplace
Forta
Blockchain Security Tools
GMX
DeFi Dapps
Rainbow
Software Wallets
GasHawk
DeFi Tools
GMX
Complete KYC
About Uniswap
Arbitrum
Avalanche


Bridge
Select Token
Chain From
Chain To
Amount
Receiver
Connect Provider

Introduction

The amount of funds stolen from blockchain platforms in 2022 is approximately $2.5 billion

In the modern world, blockchain technology emerges as an exciting and rapidly evolving field, transforming into a distinct era in the history of digital solutions. We believe that sooner or later, all accounting systems will leverage the properties of this technology. The unique ability to provide decentralized and transparent systems has become an integral part of this evolution, opening new horizons for various industries. However, against this innovative progress, new challenges and issues arise, demanding solutions.



Fraud schemes exploiting the complexities of blockchain regulation are becoming more sophisticated and challenging to overcome. As a result, regular users find themselves grappling with security threats and the complexity of engaging with innovative technologies.

Today, the average user must consider a myriad of factors when managing digital assets:

- Security: Striking a balance between easy access to funds and avoiding the risk of losing money due to an irresponsible service provider.
- Provable Non-Involvement: Monitoring incoming and outgoing transactions for the involvement of transferred funds in various fraudulent schemes or theft.

- Recoverability: Choosing between backing up keys (and how to do so) or opting for asset insurance (and trusting the digital asset insurer).
- Manageability: Building a sensible budget management structure, both for personal use and for a managed company budget.
- Audibility: Verifying that the logic of decentralized applications truly aligns with the declared goals. Checking for intentional or accidental vulnerabilities in smart contract code.

This is not an exhaustive list, but it suffices to understand that effective and secure management of digital assets is a labor-intensive process and a comprehensive solution that an ordinary user may not always afford.

The contrast between the potential of blockchain and the real issues faced by users underscores the need for efficient regulatory mechanisms and the protection of the interests of ordinary participants. This is crucial to ensure the sustainable development and safe integration of blockchain into everyday life, collectively reducing entry barriers and costs for end-users.

From the Past to the Future - Regulatory Challenges

The OneCoin project gathered over 4 billion dollars and turned into fraud... The North Korean hacking group Lazarus Group used cryptocurrency to launder money by hacking an exchange... In 2022, hackers stole over 1 billion dollars from the Wormhole exchange.

All these situations are united by the nature of digital assets issued on decentralized systems and the lack of regulation.

Blockchain technology is rapidly penetrating various sectors, providing unique opportunities. However, on its path to integration into the world, there are already significant problems that require serious attention and effective regulation.

ICO Problem: Litmus Test for Fraud

The approach to Initial Coin Offering (ICO), despite its popularity, is becoming a platform for fraud. Many projects, using promises of high returns, attract investors but turn out to be nothing more than a deception. Ponzi schemes and pump-and-dump manipulations become commonplace, harming the interests of trusting investors. In turn, this also affects good projects - users fail to use clear criteria in their selection, and, having learned from bitter experience, lump everything related to "crypto" under one brush.

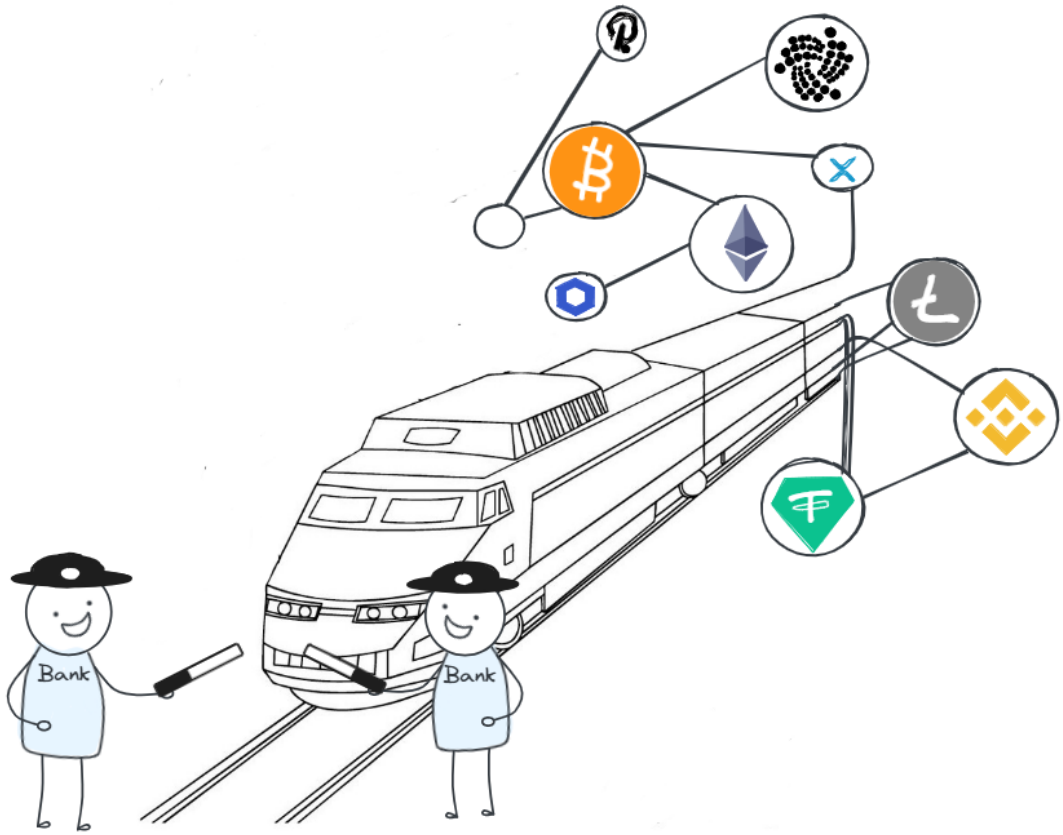
Lack of Consumer Protection and Taxation Threats

Blockchain technology provides anonymity (more precisely - pseudonymity) when managing digital assets, hiding the real user behind an anonymized address. This can lead (and naturally leads) to tax evasion and money laundering. Moreover, due to the decentralized nature, the lines of taxation are significantly blurred - P2P payments are truly P2P; they do not require intermediaries or connections between financial institutions for processing. The transaction can be initiated directly by the user, and its confirmation can be done by an unknown validator. Thanks to the mathematical transparency of events in the blockchain, regulators can happily observe what is happening, but in reality, there is little they can do to protect consumers.

Between Dreams and Limitations

The global cryptocurrency market, promising potentially high returns, faces a range of issues undermining its stability and reliability. One of the main problems is the lack of clear and enforceable rules. In such a semi-regulated environment, investors often fall victim to fraud, and the absence of legal protection only exacerbates the situation.

Regulators, seeking to gain control over the crypto industry, often employ outdated approaches that could be more effective and more counterproductive. For instance, the SEC directly combats services and projects, while regional regulators tighten regulatory screws, increasing the cost of entry for new solutions to enter the market.



However, the cryptocurrency market can become an excellent tool for expanding the possibilities of the traditional financial market. It helps balance the growing volume of assets not backed by a solid component.

Current regulatory requirements prove cumbersome and convoluted, increasing legal risks for market participants or pushing them into the "gray" area. For a market based on high technologies, an appropriate **high-tech regulatory** approach is necessary.

In the crypto enthusiasts' environment, the distorted perception of freedoms leads to the idealization of the industry as a utopian ecosystem. Absolute freedom is more likely to lead to chaos than harmony, as the absence of any rules and regulations creates a fertile ground for fraud, crime, and other negative phenomena. In the financial sector, anarchy has little in common with freedom.

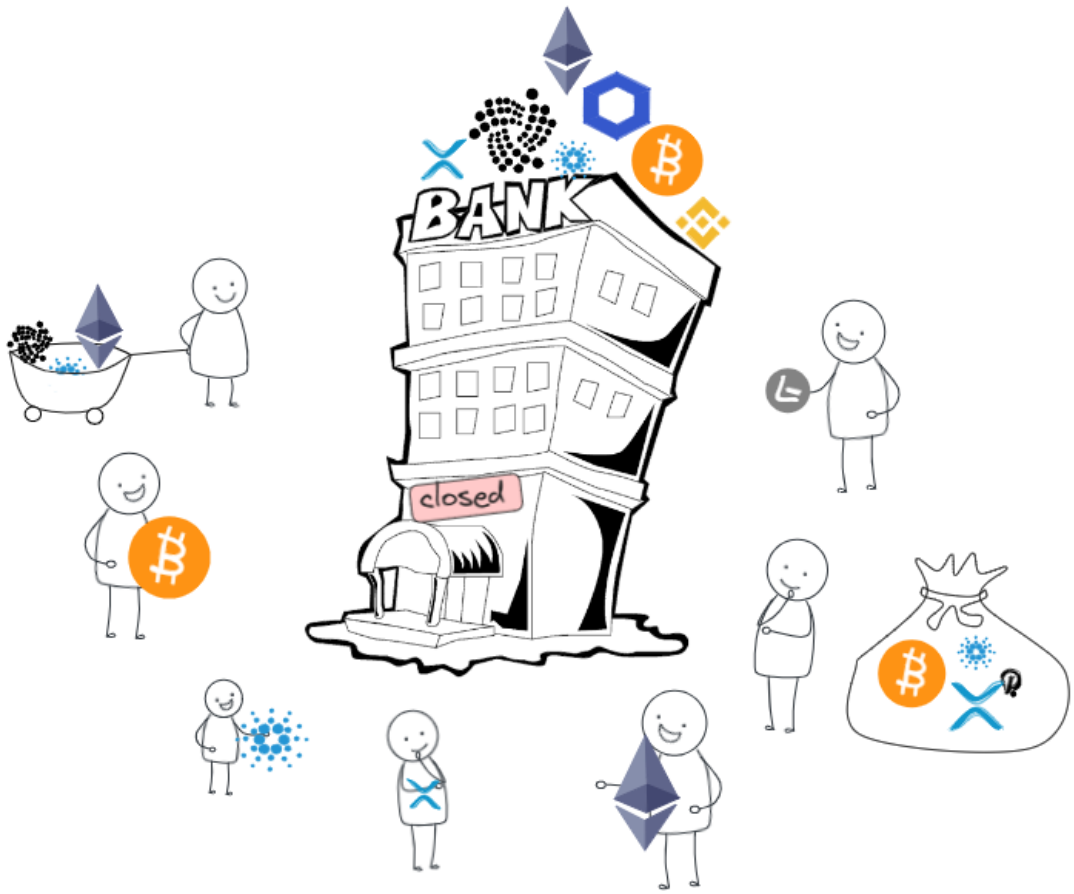
For participants who want to operate in accordance with the legal framework and have maximum compatibility with the traditional financial sector, the implementation of clear criteria and rules by regulators is the only possible scenario. Users who do not want to engage with the regulated segment can continue to leverage the properties of decentralized systems, as before.

The ideal market for an entrepreneur is not a realm of anything but rather a consolidating platform where decentralization and government regulation work in synergy, ensuring stability, clear rules, security, and accessibility for all participants.

Mint

On January 1, 2023, there were 22,157 digital assets on the cryptocurrency market, and its global market capitalization amounted to just $795.56 billion.

The issuance of assets is not only a technical process but also a highly complex regulatory task involving a series of mandatory procedures, audits, and checks. This is particularly relevant in the context of increasing interest in digital assets from the general public and businesses.



Many individuals entrust their digital assets to a bank, and the bank is responsible for ensuring the security of these assets.

For regulatory authorities, the process of regulating cryptocurrency issuance is a complex and resource-intensive undertaking that involves:

- **Project analysis** (business model, technological solutions, and security measures).
- **Audit of the solution's code** (requiring specialists capable of analyzing complex algorithms and data structures).
- **Interaction with developers and entrepreneurs** (balancing innovation support, technical solution security, and compliance with the legislative framework).

- **Coordination with other regulators and international organizations** (global-level coordination requires regulators to exhibit a high degree of diplomacy and a commitment to ensuring harmony in the global financial system).

In a scenario where traditional financial institutions are integrating crypto assets into their operations, there is an urgent need for reliable regulatory mechanisms.

The state, as the primary arbiter in financial matters, is responsible for the stability of the economy and the protection of its citizens' interests. Therefore, any attempts to create and issue digital assets without proper control will be considered a threat to economic stability and possibly as unlawful activity.

Quality is more important than quantity

In some blockchain networks, such as Ethereum 2.0, validators must stake cryptocurrency. This incentivizes validators to act honestly and in the network's best interests. It's evident that in regulated systems, any party contributing collateral cannot become a validator. Therefore, a separate reputation-based mechanism is required.

Validators in a blockchain network play a crucial role by confirming the mathematical correctness of transactions and ensuring the system's security and maintenance. The presence of high-quality validators (government entities, major companies) reduces the need for a large number of them. In cryptocurrencies, the fate of the system is determined by the majority of unknown participants; in a regulated environment, it could be a few reputable and trusted organizations (playing by common and pre-established rules). Reducing the number of validators enhances system throughput and reduces redundancy (costs + computational power).

Public transparency of validators strengthens the trust of users and regulators. The quality and responsibility of validators are essential for creating a reliable and resilient blockchain system.

At the same time, a separate role in such infrastructures belongs to auditors - participants who do not participate in achieving consensus but store and synchronize the current state of the accounting system to monitor and control all actions performed.

Thus, any accredited organization can enhance the transparency of processes in the accounting system without impacting its throughput.

Rollups as a way to scale

As of December 27, 2023, over 30 second-layer solutions are utilizing Rollup technologies.

Now, let's touch upon the issue of network scalability. The throughput of any system, whether centralized or not, is limited. For some systems, this limitation is within the range of 3-5 transactions per second (tps), while for others, it can be tens of thousands of tps. As the level of decentralization increases, the reverse effect becomes a decrease in its throughput (influencing the consensus process among validators).

Another crucial aspect is unpredictability. When designing an accounting system, developers must consider the potential load on it. Depending on these requirements, specific technologies may be chosen for implementation (consensus mechanism, accounting model, etc.). However, if situations of overestimated load don't critically impact the system, underestimating it leads to:

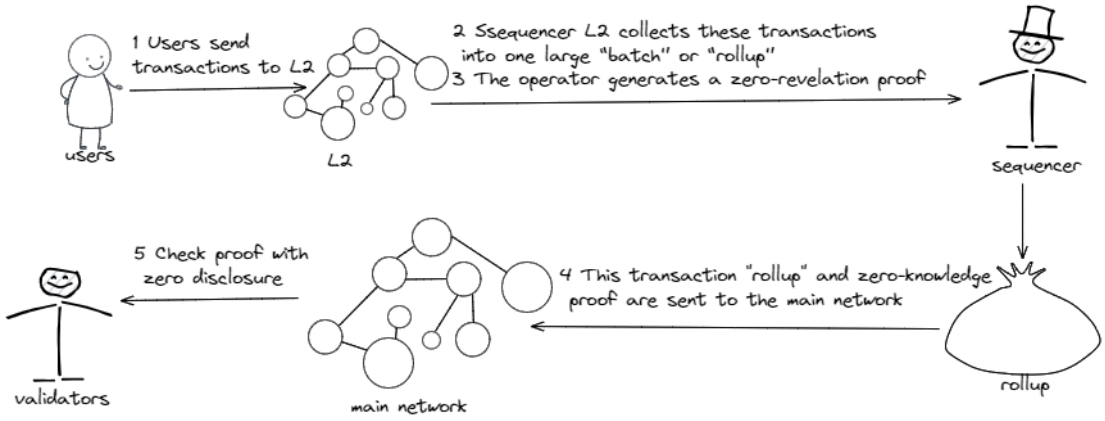
- competition within block limits and consequently, an increase in transaction fees;
- service denial to users who cannot compete.

One method of scaling an accounting system is through rollups. A key distinction is their ability to launch parallel subsystems without altering the basic architecture of the accounting system (unlike sharding). At the L1 level, each such subsystem is represented by a verification smart contract, periodically updating the state.

Briefly, the functioning of zkRollups can be described as follows:

1. Users submit transactions to L2 (second-level subsystems) that operate concurrently with the main network. Transactions stand out for their speed and cost-effectiveness.
2. The L2 operator (sequencer) aggregates these transactions into a single "rollup" or "batch." The operator generates a zero-knowledge proof (zk-SNARK) confirming the validity of all transactions in the rollup, adhering to the network rules.
3. This "batch" of transactions and the zero-knowledge proof are sent to the main network. Validators on the main network verify the proof (regarding state transition). After successful proof verification, all transactions in the rollup are considered confirmed on the main network (considering assumptions about the finality of the main network).
4. The state of accounts or smart contracts involved in these transactions is updated on the main network, taking into account all transactions conducted on L2.

It's also important to note that the proof of the validity of the final state of the rollup can be verified by any participant in the network.

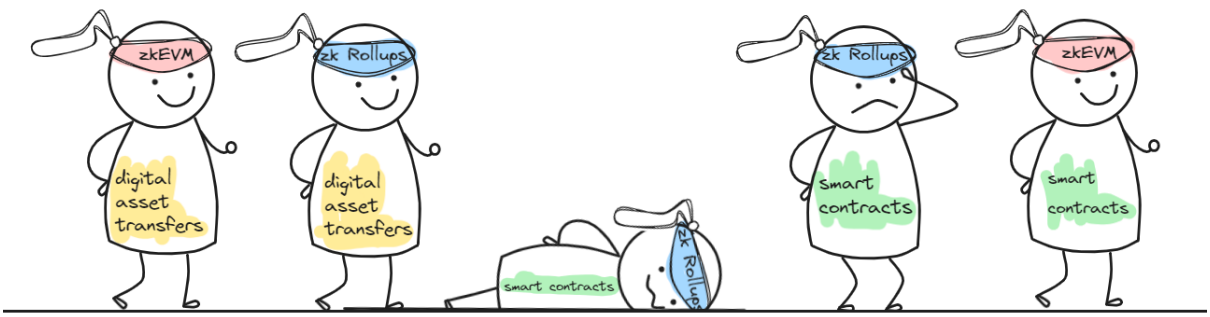


The key advantage of zk-rollups is their ability to process a large number of transactions off the main chain, followed by the submission of only the final state hash and proof to the main blockchain.

This increases significantly the network throughput and reduces transaction costs, making the technology highly appealing for a wide range of solutions, from financial operations to decentralized applications.

Now, a bit about zkEVM. Zero-Knowledge Ethereum Virtual Machine is a technology that aims to combine zero-knowledge proof technology with the Ethereum Virtual Machine.

While some zk rollups can efficiently aggregate simple transactions like digital asset transfers, implementing them for smart contracts is challenging. zkEVM represents an attempt to make zero-knowledge proofs compatible with the full functionality of the EVM, including all OP codes.



Why it matters:

1. Efficiency (the main network is not overloaded with additional logic)
2. Confidentiality (everything that happens in L2 stays in L2)
3. Compatibility (developers can use existing tools and programming languages to create smart contracts on L2)

How it works:

1. A developer creates a smart contract and deploys it on L2 (zkEVM-compatible).
2. Transactions are initially processed on L2.
3. After several transactions are bundled in a rollup, a zero-knowledge proof (zkp) is generated for the entire package.
4. Then, this proof is verified and recorded on the main network.
5. After successful verification, the state of all involved smart contracts is updated on the main network.

In an era where blockchain technologies become an integral part of the financial and corporate world, zero-knowledge rollups stand out as one of the most promising solutions for optimizing throughput and enhancing confidentiality.

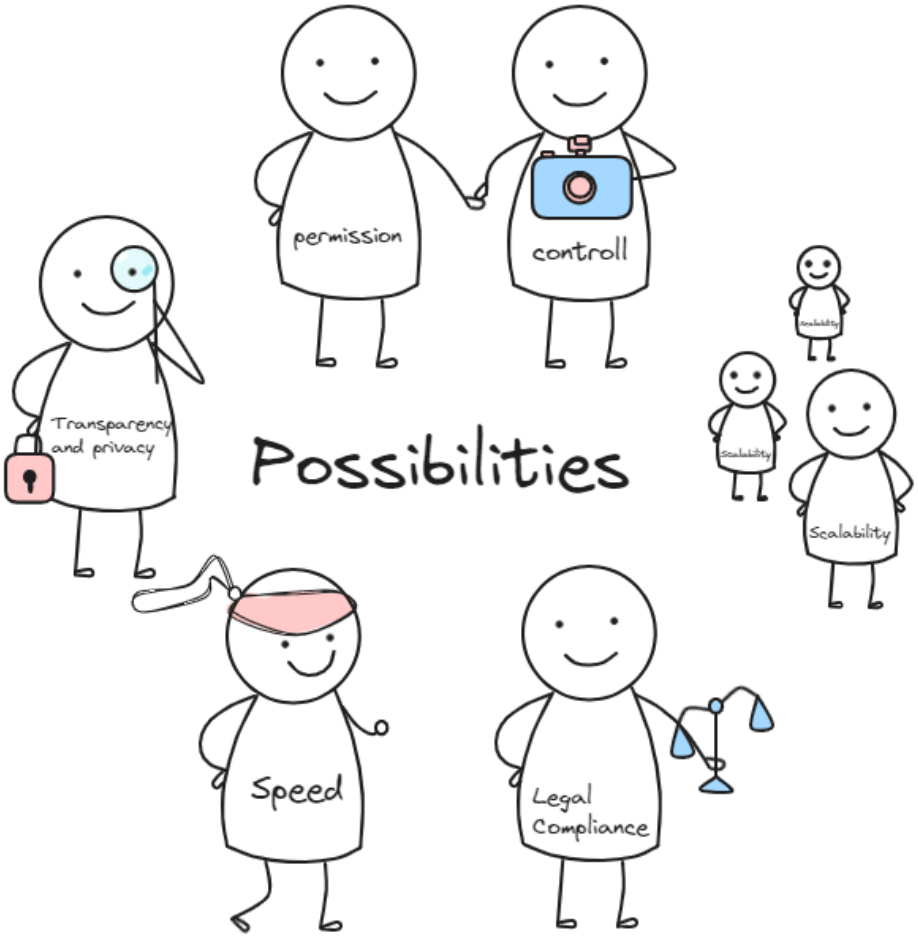
These algorithmic constructs not only simplify the transactional load on the main network but also provide cryptographic anonymity, allowing validation of transactions without revealing their content. In this combination, we achieve mathematically substantiated anonymity that satisfies regulators.

The integration of this technology represents a step forward in creating more efficient, secure, and scalable blockchain ecosystems.

Possibilities

According to a study conducted by McKinsey, improperly formulated system requirements are the cause of failure in 25-50% of projects.

If, in addition to understanding the accumulated problems, we can formulate system requirements that contribute to their resolution, then we will have a clearly outlined list of criteria.



- **Transparency and Privacy**: the system should ensure complete transaction transparency for specific participants while maintaining the confidentiality of data for other participants.
- **Permissions and Access Control**: the ability to establish restricted access to specific parts of the accounting system's functionality.
- **Cryptographic Protection** (Security): the use of robust cryptographic algorithms to safeguard data.

- **Speed**: high throughput - the system should be capable of processing a large volume of transactions per second.
- **Scalability**: the system's ability to adapt to high loads (an increase in the number of transactions that need to be processed in a unit of time).
- **Legislative Compliance**: the ability to easily adapt the system to regional or international legal requirements.
- **Control and Reporting**: built-in tools for monitoring, conducting audits, and generating reports, accessible only to authorized parties.
- **Compatibility**: the ability to operate with a wide range of third-party assets.
- **Compatibility at Various Levels**: API and SDK - the presence of a comprehensive set of APIs and SDKs to facilitate integration with other systems and applications.

Now, in accordance with the criteria outlined above, let's describe the capabilities of the "ideal" platform.

Such a platform provides an environment where each user has a significant number of rights and freedoms. These freedoms are based on the platform's ability to control user actions to comply with established policies. The ability to generate real-time reports is ensured without revealing private information. In the context of the modern financial world, where the presumption of guilt prevails over objectivity, this platform creates a fairer and more transparent environment, addressing issues of bias and lack of transparency in financial matters.

This system ensures privacy until a breach of the law (certain system rules) occurs.

It's an honest and fair agreement that eliminates the need to exaggerate requirements or prohibit certain operations that the regulator could not track before.

In such a system, it's sufficient to undergo the identification process once, after which compliance checks can be conducted in various services without disclosing personal data. These features apply not only to applications deployed on the main platform but also to all connected rollups.

Additionally, let's add the ability to work with hundreds of crypto assets in various network services, including the ability to create your own smart contracts, launch L2 projects, integrate with the network via APIs, and provide network services to your users, even if you have a small project!

A platform built on these principles will be distributed among institutional validators, and fishers, owners of full nodes (auditor nodes), representing the community, will be responsible for public control.

For a regulator owning such a system, there is no need to set procedural barriers, restrict the banking sector from the crypto segment, or prohibit any activity due to the inability to control it.

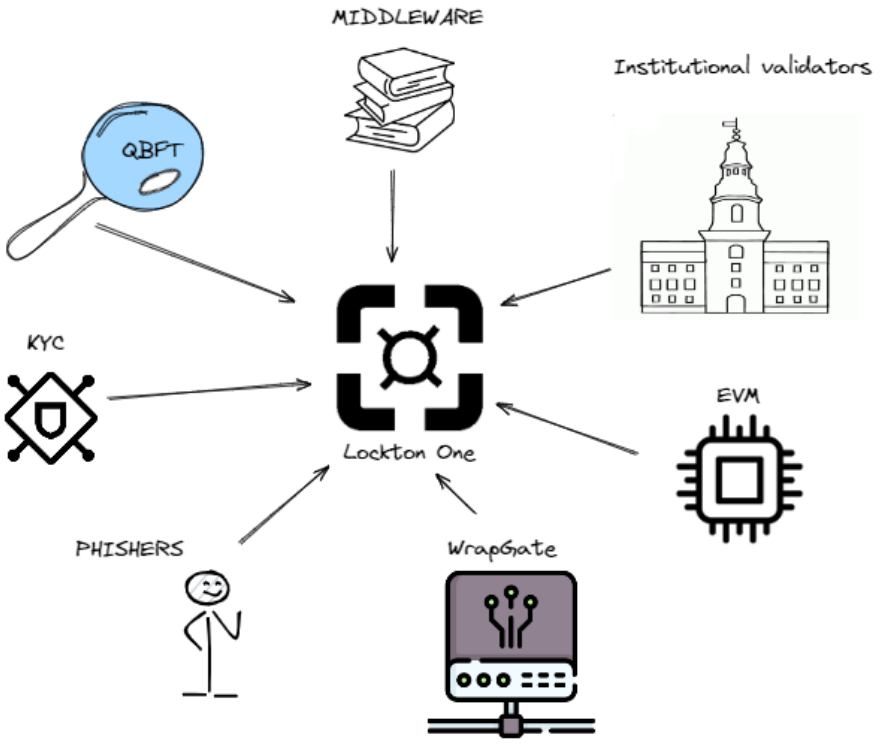
The legal framework, designed with technological regulation in mind, will be concise and enforceable, and the deployment of a platform capable of attracting a wave of investments to the region is possible in a short period.

Society is quite accepting of existing state telecommunications networks, unitary railway and aviation enterprises. Why can't state blockchain platforms emerge? It's an excellent consolidating solution for the circulation of crypto assets, launching projects, and operating existing services willing to work within the legal framework of specific jurisdictions!

What is Lockton One?

Based on these criteria, we can envision what the formula of the technical architecture of the platform will look like:

QBFT+MIDDLEWARE+Institutional_validators+EVM+ZkEvm+WrapGate+
PHISHERS+ONCHAIN_KYC +OPEN_SOURCE=Lockton one



where:

- **QBFT** - a consensus mechanism with high throughput;
- **MIDDLEWARE** - The business logic layer that deploys on top of the system core and provides the ability to connect third-party applications to the system. This layer also allows building diverse policies, facilitating advanced management of user data, delegating control and regulation to an authorized organization, thereby simplifying the prerequisites for launching projects in the legal field;
- **Institutional validators** - specialized government agencies and institutional participants as validators;
- **EVM** (Ethereum Virtual Machine) — a virtual machine designed for executing smart contracts. Thus, the Ethereum Virtual Machine enables participants to create their

projects and applications on an EVM-compatible platform and use the existing range of libraries and applications to run them in more regulated conditions;

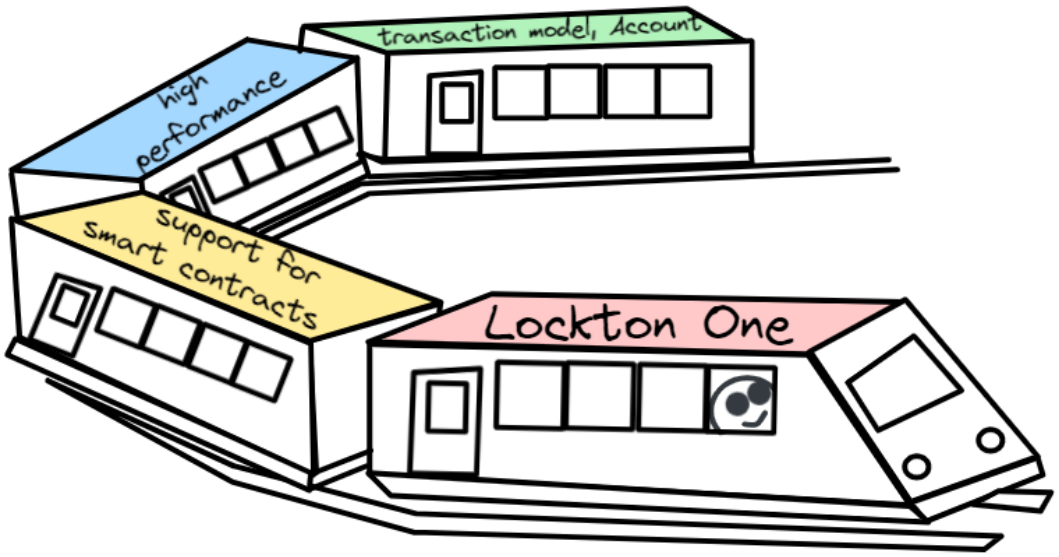
- **ZkEvm** - a technology that allows building second-layer compatible applications with verifiability of executed transactions in the main network. Solves scalability and confidentiality issues;
- **WrapGate** – A gateway capable of wrapping assets (physical and digital) to operate them within the system;
- **PHISHERS** - auditors: owners of full nodes who can monitor the validity of the blockchain;
- **ONCHAIN_KYC** - built-in KYC service allowing storing the state of account data in the blockchain.
- **OPEN_SOURCE** - open-source code ensures that the declared logic at the protocol level aligns with the actual, providing additional community oversight.
- **Lockton One** – a platform developed by the Lockton Solutions group of companies.

Under the hood

Lockton One is an innovative platform currently in development, offering the opportunity to efficiently implement and deploy financial organizations in a regulated environment.

The project is based on the use of the Ethereum virtual machine, a permissioned approach to consensus, and an operating system that allows the deployment of decentralized applications on top of the administration layer, including embedded smart contracts.

Lockton One aims to create an exceptional solution by combining high performance, smart contract support, account management, and transaction modeling. The project's protocol is designed to build a reliable and modular system supported by trusted institutional participants (authorities). It is important to note that Lockton One is actively in development, striving to create an advanced solution for the financial environment.



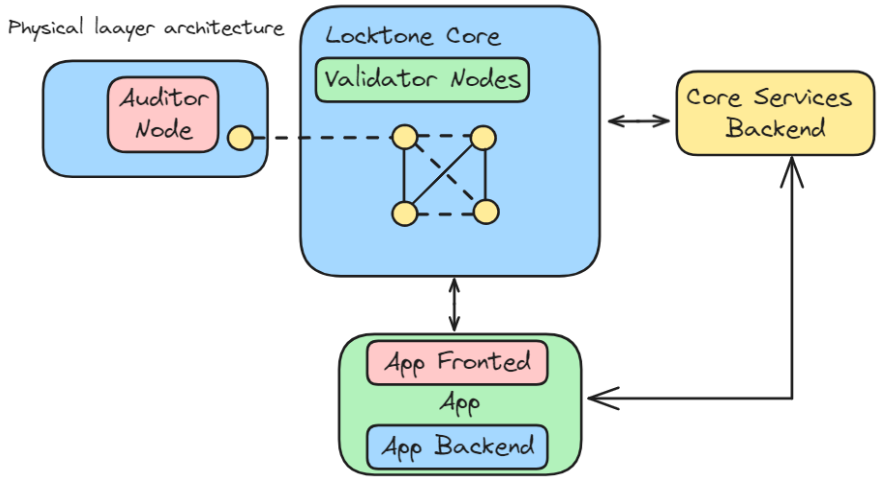
Lockton One facilitates the interaction of financial institutions in the digital asset space without intermediaries. The platform provides clients with services featuring transparent accounting and real irreversibility. It streamlines access to reporting, reduces costs for secure infrastructure (eliminating the need for a proprietary immutable layer), and supports institutional accounts. Lockton One provides an API for auditing and integration with third-party systems, as well as offering account opening, maintenance, and administration with full customization.

The primary target audience for Lockton One includes the following users and organizations:

- **Entrepreneurs** wanting to work with digital and cryptocurrencies while ensuring compliance with specific regulatory norms of a particular region.
- **Traditional financial institutions** requiring advanced and more transparent monitoring functions with the ability to provide "customer-centric" security to their users.
- **Exchanges** operating with digital and cryptocurrencies.
- **Decentralized projects** requiring user identification and the regulatory control of their actions based on assigned roles.
- **Banks** providing a new type of financial services on algorithmic protocols.

Lockton One Architecture

According to a study conducted by McKinsey, investments in system architecture can lead to a 10-20% increase in efficiency.



At the physical level, Lockton One consists of a group of specialized computers called validator nodes that interact with each other to coordinate the current state of the system. There are also auditor nodes that maintain a copy of the current state of the system.

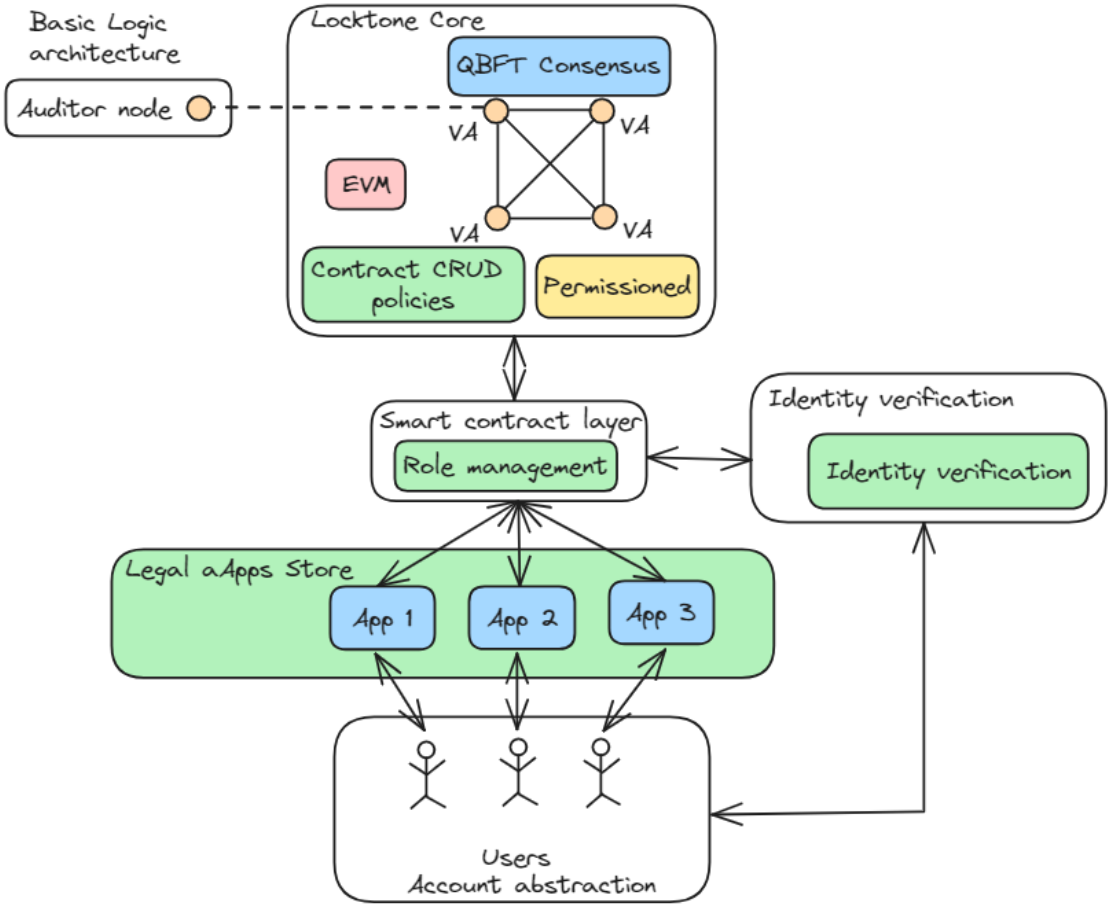
The core of the system, called Core Services Backend, processes various services such as identity verification, creating platforms for decentralized autonomous organizations (DAOs), building systems for anonymous transactions, and other tasks that require the use of servers. The Core Services Backend is like a framework that connects a set of individual servers, not a single server that performs all functions simultaneously.

Each application running on Lockton One can include external and internal modules that operate on different physical devices.

The basic logical architecture includes:

- The **Lockton core** includes **validator nodes** operating in accordance with QBFT consensus. The Ethereum virtual machine ensures the execution of operations to change the core's state. CRUD policies control the logic of deploying and managing smart contracts at the consensus level.
- The **smart contract** level is built on top of the **Lockton core** and is responsible for managing roles and permissions.
- The **Backend module** includes identity verification (KYC) services and integration with existing (web2) solutions.

- **Auditor nodes** have almost the same logic as **validator nodes**, but they cannot participate in achieving **consensus**. Their main goal is to locally preserve the system's state and verify that everything in it is functioning normally.
- **Authorized dApps store**: the user goes through the registration process and gains access to a list of applications that they have permission to interact with (based on their identity and permissions).
- **Account abstraction**: allows the implementation of arbitrary complex account management logic.



Account abstraction

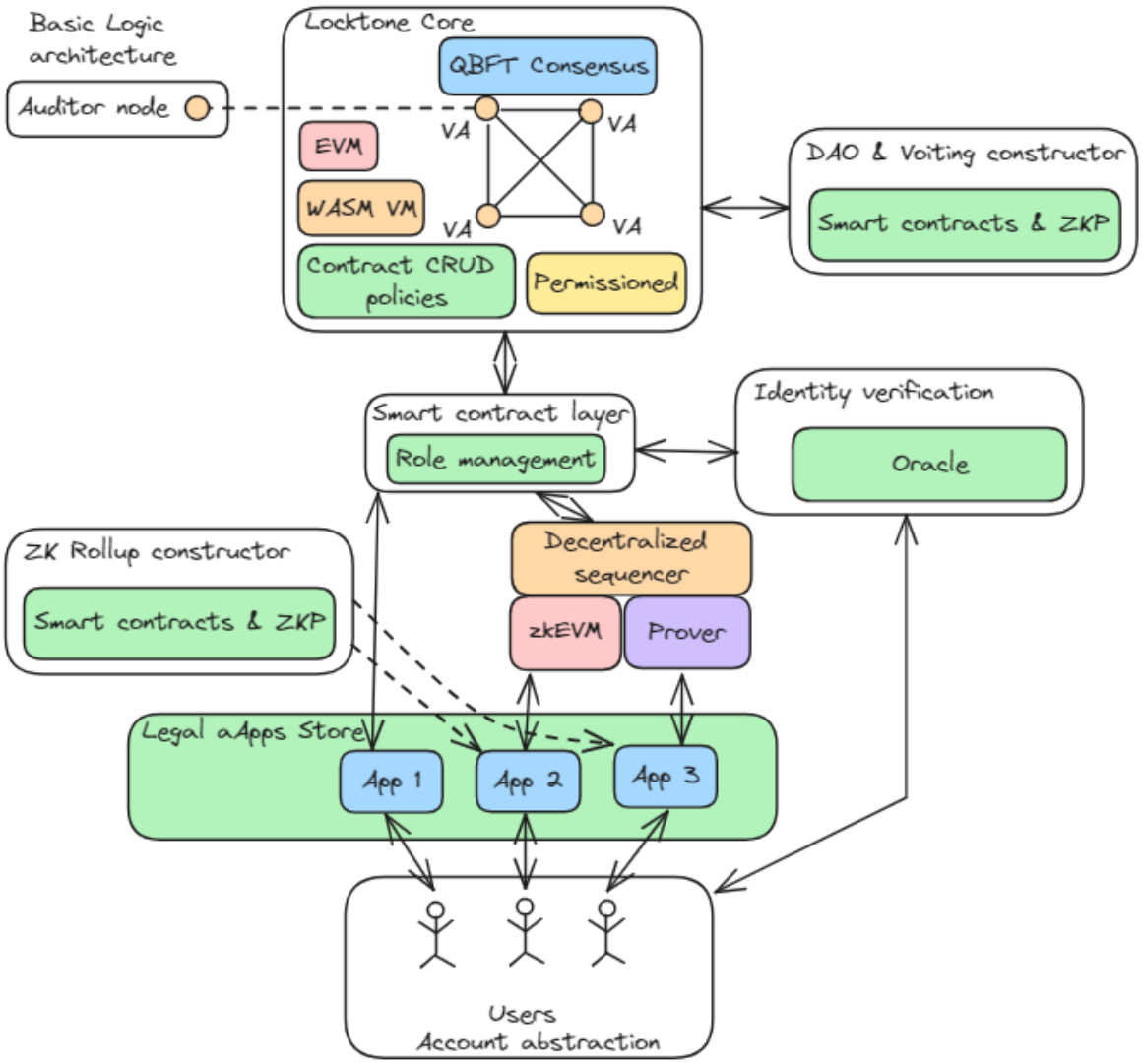
Use Cases (why it's needed):

- **Assets** can be **frozen** on the account if the user is suspected of some illegal activity;
- **Assets** can be **transferred** from the account to a new one in case some number of trusted authorities agree on that (for example, in case of losing access to the account, the user can restore access if his family members and close friends confirm that);
- **KYC** provider **services** will have the ability to **restore access** to the account in case users lose their keys after they prove their identity;
- **Applications** can get some kind of **limited access** to users` accounts. For example, a game will receive a limited access key to interact only with game smart contracts. This will

eliminate the need for users to sign transactions for each interaction, thus improving user experience without compromising security.

Applications will need to pass the verification process and get corresponding roles. Then they can interact with the Lockton Core through RBAC (role-based access control) defined on the smart contract layer of the protocol. The corresponding backend module is responsible for the verification process. This centralized service will check users/application documentation and emit corresponding roles that will grant access to the Lockton One protocol.

Future improvements version:



Advanced architecture is designed to show the goal of future development and subsequent releases:

- **DAO & Voting constructor**: this module will allow the form of local communities with their own governance rules with custom rules (including anonymous voting).
- **ZK rollup constructor**: this module will allow you to construct verifiable rollup-based applications by setting up the rules of the application.
- **Decentralized shared sequencer**: A shared sequencer can handle atomic cross-rollup operations (when transactions are executed either on both rollups or are not executed at all). It also eliminates a single point of failure of centralized sequencer architecture and allows fast transaction finality on rollups.

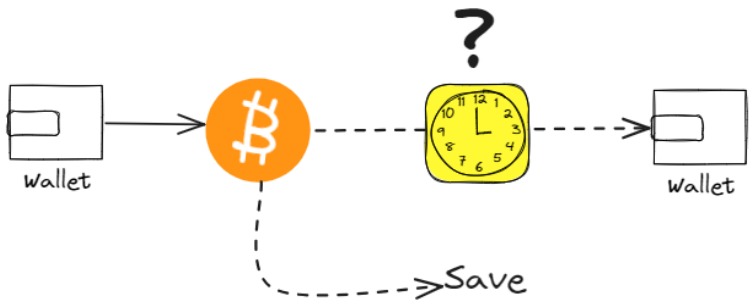
The number of accounts

The Lockton protocol network will operate at the national level, capable of handling millions of accounts with scalability. Technical constraints are related to the number of requests, and the system plans to process up to ~1000 requests per second, with the potential for further scalability. It is important to note that EVM operates with 160-bit addresses, allowing storage of up to ~2^160 ≈ 10^47 accounts, which is a crucial aspect of the system. By using accumulator batches, the system can achieve performance of tens of thousands of transactions per second and support millions of users.

Early stages: ~1`000 - 3`000 active users, ~100'000 in total.
The aim of future improvements: ~100'000-200'000 active users, 10'000'000-50'000'000 in total.

Performance requirements

The basic version of the Lockton One protocol processes about 100 transactions per second. For node validators, servers of average power are sufficient. Performance is enhanced by applications based on accumulation packets, storing transactions on their equipment and periodically sending proofs to the system. This allows Lockton Core to guarantee compliance with protocol rules. Storing unprocessed transactions by applications enhances performance but also carries risks (potential loss of access). A decentralized shared sequencer can address this issue, ensuring data availability. Several independent sequencers will solve bottleneck issues, improving scalability to tens of thousands of transactions per second. Validator nodes will not directly process view requests to prevent DOS attacks, while auditor nodes will keep a copy of the system state, executing complex view queries.

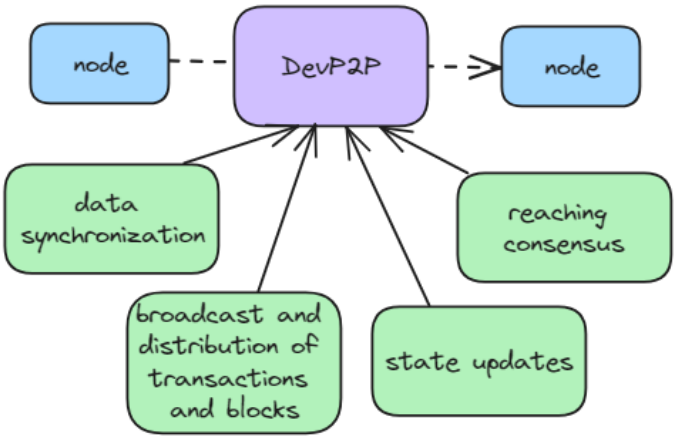


Early stages: 100-500 TPS
The aim of future improvements: 50 000-200 000 TPS.

API and the model of API reaching

The Lockton One protocol will use JSON-RPC API (remote procedure call) to receive application requests. This API can be used for managing an account (check balances, send transactions), deployment, management, and interaction with smart contracts, blockchain data retrieval, event handling, etc. The main difference with the Ethereum API is that all requests (even "GET" that does not change the system state) should be signed because of the permissioned design of the system. Only authorized parties can review the system state.

To communicate between nodes, a peer-to-peer protocol will be used (specifically DevP2P, which is commonly used in Ethereum-like networks). Those communications will include data synchronization, transactions and blocks broadcasting and propagation, consensus reaching, state updates, etc. Auditor nodes will synchronize with the network state using the same peer-to-peer protocol.



Smart contract supporting

The Lockton One protocol is based on a modified version of Geth (Ethereum node written in Go). It executes EVM-smart contracts, meaning that most existing dApps can migrate to the protocol with few changes in the base code. Still, the Lockton protocol has several peculiarities, as its aim is the creation of a regulated environment supported by authorities, which means that applications will need to implement protection against interaction with unauthorized users. The protocol provides built-in tools that make it much easier to integrate existing solutions.

Furthermore, Ethereum Virtual Machine has several significant drawbacks (mainly in the performance parameters), so in future releases, a parallel VM that will execute WebAssembly (WASM) can be built in. This will allow the protocol to execute complex operations more efficiently. For more information about the WASM VM module function, see the Additional Protocol Enhancements section.

Early stages: only Ethereum Virtual Machine smart contracts.
The aim of future improvements: both Ethereum Virtual Machine and Webassembly Virtual Machine smart contracts

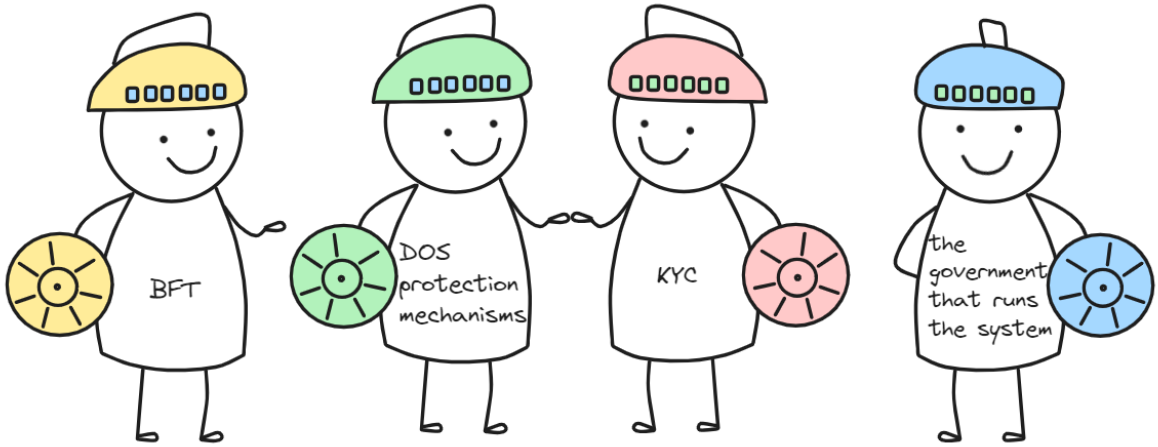
System fee requirements in the Lockton One Protocol

The protocol uses computation credits (CC) to incentivize and protect its work from spam. With account abstraction, it's possible to create a model where the application will pay for the user (and receive the revenue based on its business model). When the user forms the transaction, it will be sent to the application aggregator, the final publisher of transactions, and a transaction fee will be paid. Those credits will be provided (sold) by the protocol owners (like the government).

Applications develop their business model to get resources for operating on the Lockton One protocol. In that case, the end users would not directly pay fees to the Lockton One protocol.

System protection methods

The Lockton One protocol is a permissioned network. Permissioned blockchain platforms require all participants to be identified and authorized, making it more difficult for attackers to access the network. All users and nodes should be required to authenticate with strong credentials, and access to sensitive data and functions should be restricted to authorized users and nodes.



DOS-protection mechanisms (IP blacklisting/whitelisting, request rate limitation, backup nodes usage) should be implemented to protect validation nodes from failure by executing denial-of-service attacks, as well as spam and flood attacks.

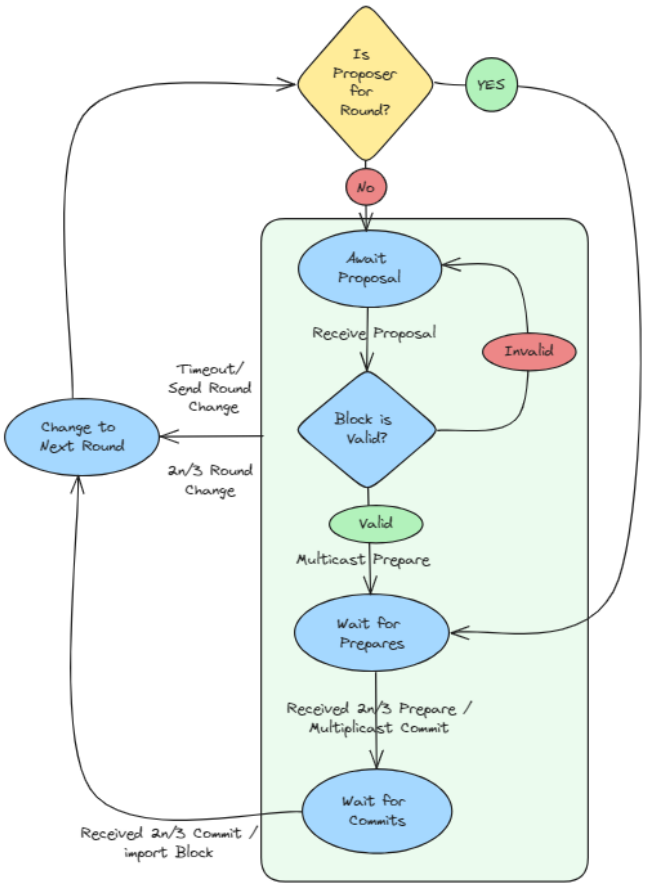
Protection from a Sybil attack is done by the fact that the network is permissioned, and to access it, users should pass the know-your-customer (KYC) verification process, which makes the execution of such an attack extremely hard.

An attack with history reorganizing does not make much sense, as it can be executed only if an attacker controls the government that runs the system. In that case, there is not much the system can do. Otherwise, if an attacker does not control the government, the system will fail if an attacker can make more than 33% of nodes act maliciously, which is practically impossible because those nodes are controlled by the government, which an attacker does not have control over. BFT-based consensus mechanisms allow instant transaction finality; if validators have agreed on the state change, they cannot revert it.

Consensus reaching mechanism

In blockchain networks with a limited number of participants, it does not make sense to use unproductive and fully distributed consensus types like Proof of Work and Proof of Stake. The BFT-based consensus-reaching mechanism will be used to get high transaction throughput and finality in a permissioned system. Specifically - QBFT (Quorum Byzantine Fault Tolerance) is a modification of Istanbul BFT. QBFT works in permissioned protocols, meaning only pre-approved nodes can participate in the consensus process.

The main objective of these mechanisms is the increased simplicity, reliability, and performance in closed networks, which simultaneously fully preserve the main properties of private blockchains - immutability, verifiability, and traceability of data.



Consensus algorithms based on BFT can scale to a significant number of nodes without compromising performance and security.

Early stages: QBFT for devnet and testnet and production use.

Number of validators should support the system

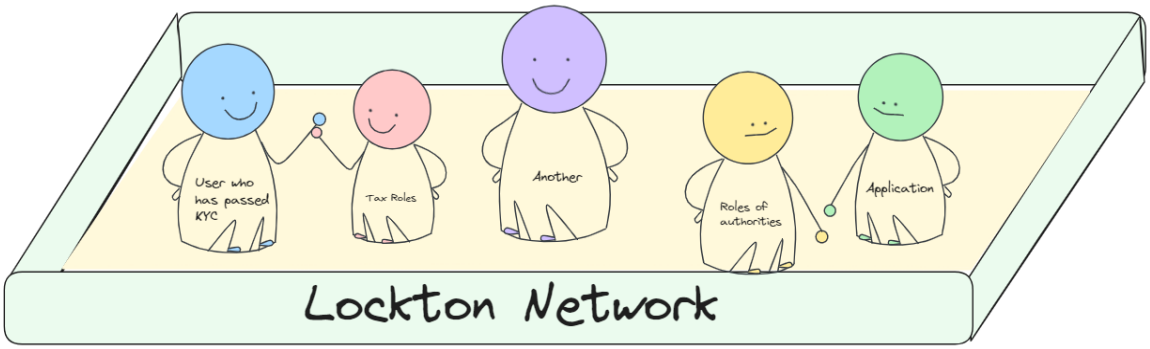
Number of validators that should support the system depends on security and performance requirements, as well as protocol consensus limitation. The minimum number of validator nodes that can reach consensus under QBFT consensus is 4, and the recommended number depends on the expected fault tolerance (the system's operational resilience in the presence of potentially malicious nodes). Because the protocol is permissioned and validators are selected or operated by the "government" entity, the system can stay relatively secure even with a few validator nodes.

Early stages: 4 - 7 validator nodes;
The aim of future improvements: 11 - 25 validator nodes.

Users roles and their permissions

Lockton network is a permissioned network, meaning users should receive permission to interact with it. Specifically, we expect Lockton One to have role-based access control, which means that each user will have roles that will allow them to perform some specific set of operations on the network. For example:

- KYC-passed user
- Application
- Job-specific roles (police, medical staff, certified trader)
- Authorities roles
- Regional roles (citizens of city X)
- Taxes roles (legal entity, individual)
- Other.



Supported Asset Types in the System

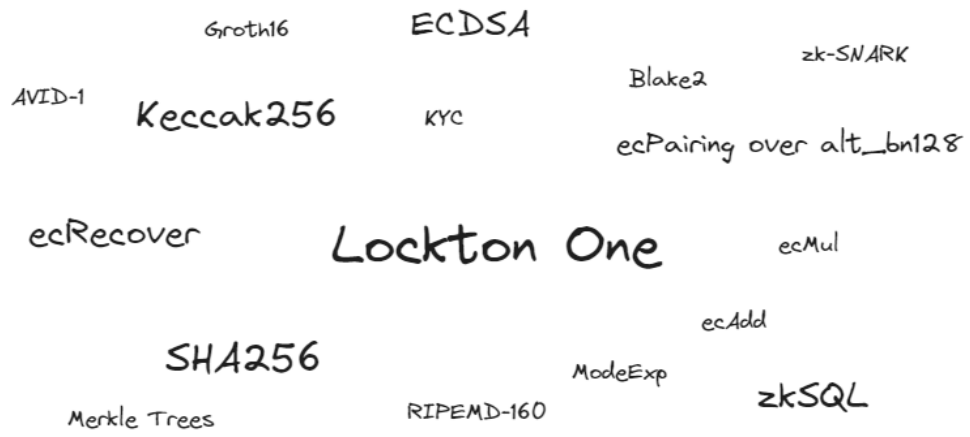
The default system asset is Computation Credits, primarily utilized for network operation payments. In addition to Computation Credits, applications have the flexibility to introduce their own asset types. These assets can conform to industry-standard token standards like **ERC20, ERC721, ERC1155,** or may employ custom application-specific logic. Contracts with custom logic should be verified by authorities and whitelisted.

Should the privacy of transactions be achieved?

Network data will be open to permitted applications. The current protocol design allows applications deployed on top of the Lockton One protocol to operate in two formats: directly perform transactions and use rollup-based operation models. The first one is pretty straightforward: applications with permission and computational credits can execute transactions.

The second one has some challenges: for applications to run their rollup systems, some zk-circuits should be implemented. However, applications may have different logic and cannot all be verified by the same circuit. At the same time, the Lockton protocol is controlled by the government, and the government should decide what schemes are allowed and which are not. To address this issue, some constructor-like systems that will consist of government-approved functionality should be built. In that case, applications would just construct their business logic out of approved components. This will allow the protocol to have application-specific rollups without losing security.

Used cryptographic mechanisms



Base cryptographic mechanisms are the same as in the Ethereum:

- **ECDSA key pair** (specifically secp256k1). ECDSA is a cryptographic method used for creating digital signatures, and secp256k1 is a specific set of elliptic curve parameters used in this context for key pair generation. This parameter set ensures security and efficiency within the ECDSA algorithm.
- **Keccak256 hash function**. A cryptographic function used to transform input data of arbitrary length into a unique string of fixed length, known as the hash value. It is part of the Keccak family of hash functions designed to provide security in various cryptographic protocols.
- Built-in **precompiled contracts** (ecRecover, SHA256, RIPEMD-160, ModeExp, ecAdd, ecMul, ecPairing over alt_bn128, Blake2).
- The **identity verification module** will use EdDSA to sign statements that users undergo the KYC process.
- The **Rollup module** will use zk-SNARK (zero-knowledge succinct non-interactive arguments of knowledge, specifically the Groth16 scheme) to efficiently verify the authenticity of Rollup transactions without compromising the system's privacy.
- Decentralized sequencers will use the **Verified Information Distribution** (VID) scheme, specifically AVID-1 (Asynchronous Verified Information Distribution 1). Other storage implementations within the protocol may also use this data storage scheme.
- The module for **organizing anonymous voting** will use Merkle Trees, as well as zk-SNARK.
- zk-schemes are required for **proving confidential data**. The use of zkSQL (additional research required) is also possible.

Approaches to the key management

Due to the permissioned design of the system, users will not be able to use popular digital wallets (like MetaMask or TrustWallet), as it involves additional cryptographic mechanisms being implemented to protect the system from unauthorized requests.

The Lockton One protocol has many differences from the existing systems, so a solution should be engineered to create a protocol-compatible wallet. One of the solutions is to use MetaMask Snaps, which will allow adding custom logic to the MetaMask to be compatible with the Lockton One protocol.

Each solution has its benefits and disadvantages. Modifying the framework basic wallet will allow the implementation of any custom logic, but users need to install another extension, while MetaMask is the most commonly used digital wallet. It is worth noting that both solutions may be implemented, which will allow a user to select the preferred one.

The account-based system will allow users to implement the logic for restoring access to the account in case of losing access to the keys (see part 21 for more details).

Early stages: one protocol-compatible wallet solution implemented;
The aim of future improvements: both solutions are implemented, and R&D of other solutions.

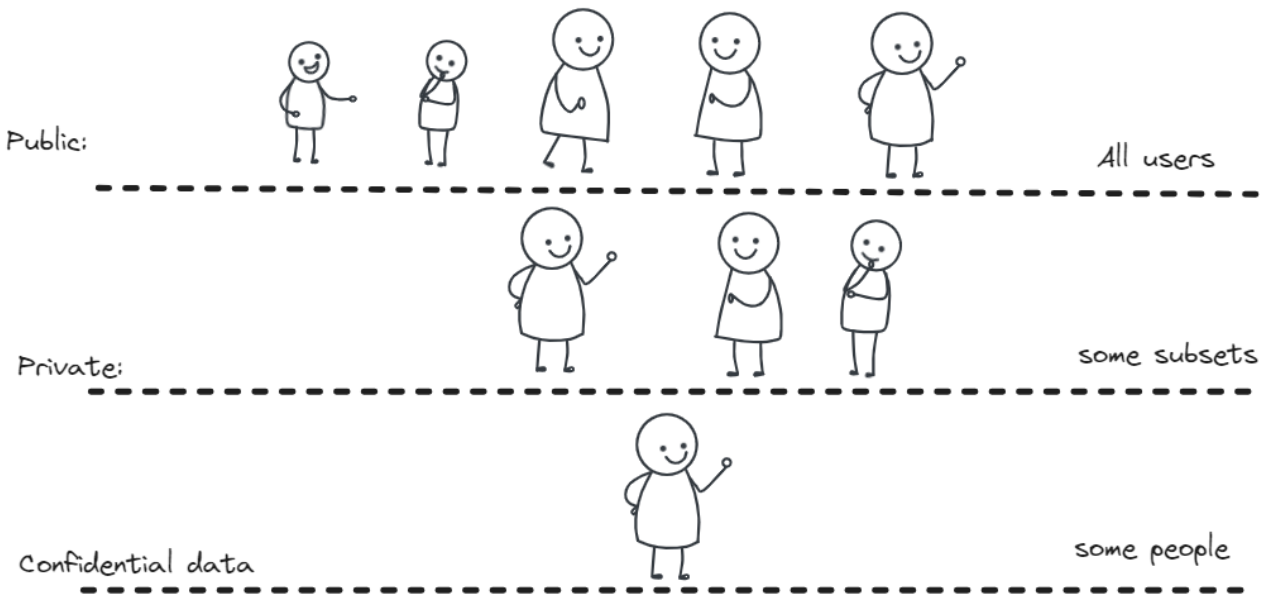
Requirements for the data storage

Based on the system's purpose, we split stored data into three main groups:

Public:
Every user with access to the Lockton One protocol can access this data. Examples of public data can include weather forecasts, research papers, public registers, etc. Information dispersal schemes (like AVID-1) might be used to store such data persistently.

Private:
This includes the data open only to some subset of parties in the Lockton One protocol. An example of private data is the Lockton Core blockchain history (available only for authorities and authorized applications deployed on the network). This may also include private registers (like criminal records only accessible to the police department, educational test scores for teachers, etc).

Sensitive data (additional research required):
Sensitive data is private by default. The difference with private data, is that the user should have instruments to make claims about that data without disclosing it.



This also includes use cases with privacy-oriented applications (like banks) that will process data in a roll-up mode and only make claims that it was processed correctly according to predefined rules. Shared sequencer usage aggregates sensitive transaction data from different rollup-based applications (like banks) and stores it in raw format to be accessed later in case of issues. Given the potential presence of significant volumes of sensitive data, it is imperative to establish robust access policies and security protocols.

Early stages: data storage infrastructure and privacy policies protection techniques.
The aim of future improvements: information dispersal schemes for distributed data storage and methods for zero-knowledge claims about sensitive data.

Environment where the system will be deployed

Nodes can be deployed on any server with sufficient computational power. As validator nodes are key components of the system, they should be online as much as possible, which is why deploying them on cloud services with high uptime (99.9%+) is recommended. Validator nodes can also be deployed manually on dedicated servers, but additional actions should be taken (like backup power supply, reserve data link sources, and geographical disperse). Core Backend Services are also important for the system, so the same measures may be applied to them. Still, their downtime will not corrupt the system security, but rather make some functionality unavailable.

Applications may decide where to host their components (like frontend and backend) on their own, as their downtime will not corrupt the Lockton One protocol security. The same logic applies to the auditor nodes.

Open source

Recognizing the potential benefits of open-source code in specific segments of the Lockton One project's codebase, it is noted that the entire system remains permissioned and under the control of authorized authorities, and the opening of the code is neither mandatory nor does it alter the fundamental characteristics of the Lockton One project.

Analytics

Platform	R3 Corda	we.trade	XRP	Stellar	Lockton One
Description	An open-source blockchain platform designed for financial services companies.	A blockchain-based platform for trade finance developed by a consortium of European banks.	A digital currency developed by Ripple.	An open-source blockchain platform that aims to make financial services accessible to everyone.	Processing blockchain center, for financial institutions in a network, distributed among institutional participants.
Key feautures	Uses a unique consensus mechanism called "Notary Cluster" to validate transactions. Offers a high degree of privacy and security for transactions. Designed to be highly modular, allowing for easy integration with existing systems.	Facilitates secure and efficient trade transactions between participating banks. Built on IBM's Hyperledger Fabric platform. Offers a range of trade finance services, including letter of credit, invoice financing, and trade payments.	Designed for use in international money transfers. Can be used to facilitate real-time cross-border payments. Has a high transaction processing capacity, allowing for high volumes of transactions to be processed quickly.	Offers fast, low-cost, and secure transactions. Has a built-in decentralized exchange (DEX) for trading assets.	The platform provide the technological basis for the introduction of digital asset services into the existing financial ecosystem, both in certain jurisdictions as well as worldwide. Offers a range of trade finance services. Designed to be highly modular, allowing for easy integration with existing systems.
Consensus mechanism	Single notary, Raft, BFT-SMaRt	Hyperledger Fabric consensus	Ripple Protocol Consensus Algorithm	Stellar Consensus Protocol	QBFT
Privacy/Security	**High**	**High**	Average	Average	**High**
Modularity	**High**	N/A	N/A	N/A	**High**
Trade finance capabilities	N/A	**Yes**	N/A	N/A	**Yes**
Cross border payments capabilities	N/A	N/A	Average	Average	**High**
Smart contracts	N/A	N/A	N/A	N/A	**Yes**
Decentralized exchange	N/A	N/A	N/A	**Yes**	**Yes**

R3 Corda: The platform supports multiple consensus algorithms: Single Notary, CFT, and BFT-based. It ensures a high level of confidentiality through various approaches, including Selective Disclosure, Transaction Tear-offs, and transaction encryption. The platform is relatively modular but may be challenging to adapt to specific user needs requiring certain custom logics. It offers features to support trade, financing, and cross-border payments. While it supports smart contracts, their usability is limited.

we.trade: The platform utilizes Hyperledger Fabric as the core accounting system, ensuring high security and efficiency. It doesn't provide privacy by default but offers transaction anonymization features. The platform is relatively modular but may be challenging to customize for specific user needs. Its primary focus is on international trade, with integrations with banks being a top priority, making it less accommodating for individual projects, especially in DeFi.

Ripple: Ripple also focuses on cross-border payments, offering its digital currency as an intermediate asset. It stands out for its system throughput and low transaction costs, making it more efficient than traditional banking transfers in some cases. However, it has limitations, such as a significant level of centralization (most validator nodes are supported by one company) and constraints on creating arbitrary application logic (lack of support for Turing-complete contracts).

Stellar: The platform uses the Stellar Consensus Protocol, which is highly scalable and resembles a "social consensus" model. It is relatively modular but may be challenging to adapt to specific user needs, lacking the ability to write arbitrary logic. Stellar's key aspects include asset tokenization and decentralized exchange, allowing asset exchange without a direct pair of orders through intermediate currencies.

Lockton One: The platform employs the QBFT consensus mechanism, ensuring high throughput and "instant" finality. It is fully modular, allowing the implementation of any required user interaction model with the platform and deployed applications (applications can have arbitrary logic in their contracts). The platform lacks an internal currency for user fee payment; instead, computational credits are paid for by application owners, confirming their clients' transactions (ensuring the necessary throughput within their own application). Additionally, the platform combines identity management with privacy, allowing only authenticated users to perform required actions without disclosing sensitive data, only verifying that the logic is executed correctly.

Summary

This document presents the worldview and value system that can serve as the foundation for creating a global WEB3 platform.

This platform can contribute to the development of an infrastructure where nations, emirates, specialized economic zones, or major corporations can provide users and businesses with specific mechanisms to conduct their activities in accordance with established regulatory norms. Monitoring, reporting, and compliance procedures are integrated into the architectural design of the system, leading to a reduction in operational costs and making the industry more accessible to projects of various scales, including startups and small enterprises.

Moreover, this concept will facilitate the interaction between the traditional financial sector and the crypto sector. Additionally, banking institutions can use such a platform as a cost-effective transport system for any traditional assets.

Many control procedures can be confirmed without disclosing personal or sensitive data, which is challenging or even impossible in traditional accounting systems. However, the choice, as always, remains with the market and is determined by its needs.

Additional protocol improvements

Some system components are essential and/or required for the system to be operational. They must be implemented in the first version of the protocol. This includes:

- Validator node;
- Auditor node
- EVM execution;
- Role management module with role-based access control;
- Identity verification module;
- Legal dApp store
- Account abstraction

Other components can be added to the system later in subsequent releases.

Iden3 as identity infrastructure core

Iden3 is the protocol that allows the implementation of self-sovereign identity (it means that identity can issue claims on another identity, which can be for an individual, an organization, or a system/machine). This module will allow us to organize user`s identities, manage access policies, and make verifiable statements by different organizations and applications.

Use cases:

- A university issues a certificate that their student has a degree. The university itself also has a certificate from the ministry of education. Employers can verify the certificate of the student.
- Brand issues a new collection and wants all its items to be verifiable. For each purchase, they create a verifiable claim that will allow anyone to verify item authenticity. At the same time, item owners can leave some feedback and claim that this feedback is indeed from the user that has purchased this item.

WebAssembly Virtual Machine

Use case:

- The Lockton Protocol is deployed in country X, with its specific set of cryptographic algorithm standards (hash function, digital signature, decryption, etc). Those algorithms can be implemented as smart contracts to ease integration. However, EVM is quite slow, so the parallel WASM virtual machine can significantly increase the efficiency of such algorithm execution.

WASM contracts can act like precompiled contracts in Ethereum, but they can be deployed on the network without forks and will be executed on a parallel VM. This allows smooth integration for computational-intensive business logic.

Privacy pools

As data on the Lockton One core can be accessed by many parties (like applications), this might impose privacy issues. Privacy pools protocol allows the hiding of transaction history by mixing assets, ensuring customer privacy.

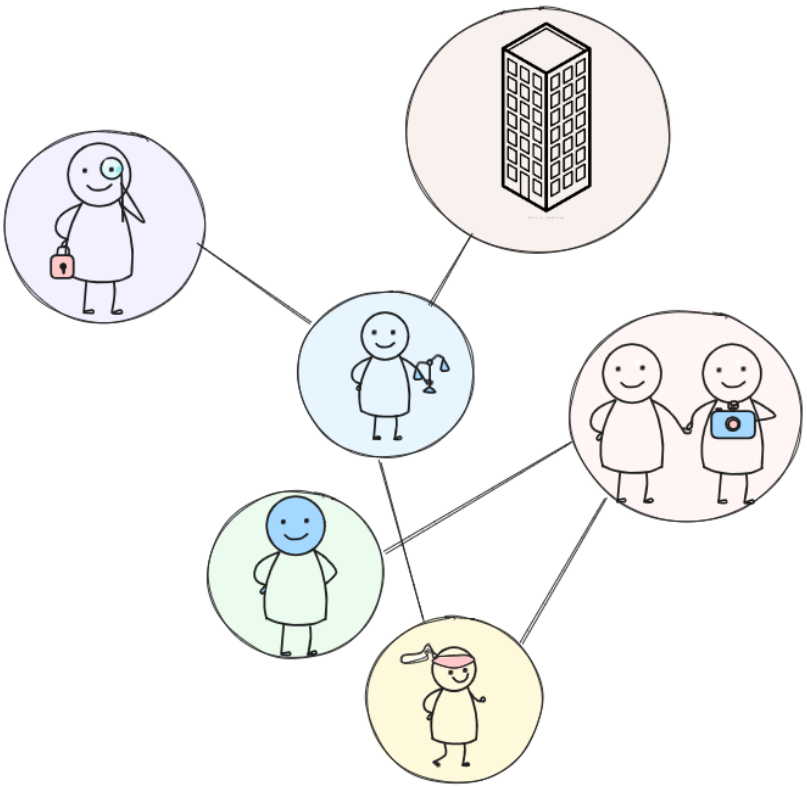
Basically, it works as follows: accounts send assets to the smart contract and then generate proof that they were in some subset of users who made deposits to withdraw.

As in the Lockton One protocol, all accounts must pass the verification procedure; this protocol will not allow the hiding of illegally obtained assets from authorities but can make it much more difficult to track down users' action history by other parties.

DAO & Voting construction framework

Use Cases:

- House residents want to cooperate to manage the house collectively. This framework allows them to easily create, set up, and manage their community as a decentralized autonomous organization. As in the Lockton protocol, all users' identities are known, and it is possible to allow only residents to participate in the decision-making.
- The Lockton protocol is deployed in some countries, and in city X of that country, city council elections should be made. Voting must be held anonymously, but only citizens of that specific city have the right to vote.



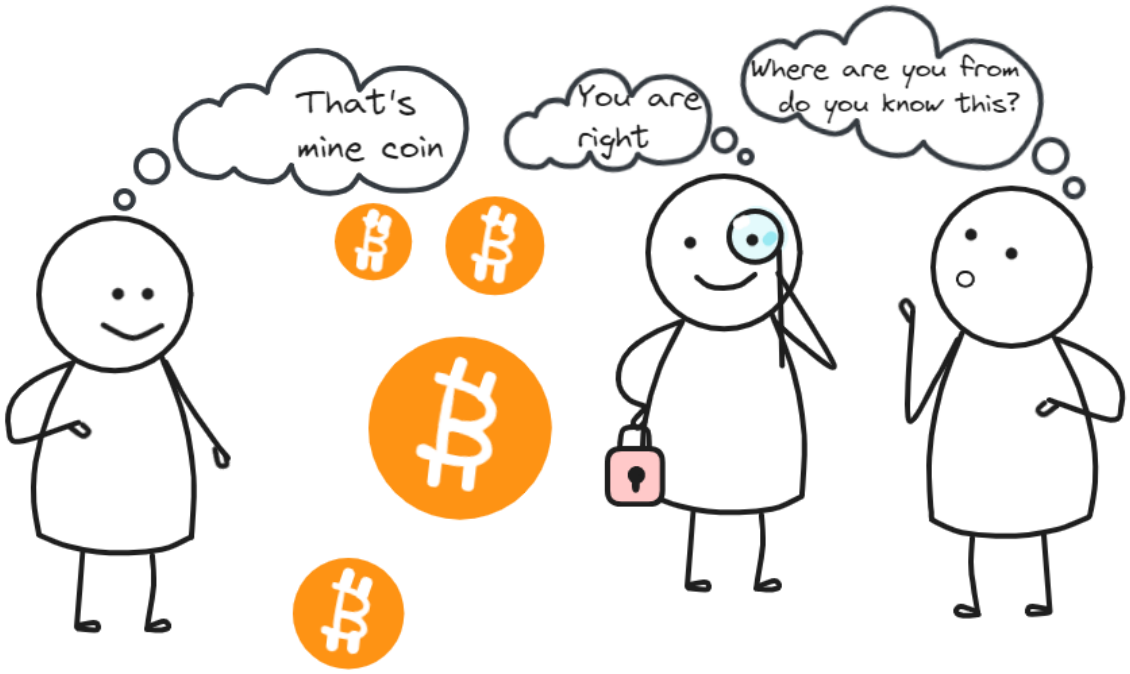
Such use cases can be solved with the DAO & Voting construction framework, which will act as a constructor when designing systems for collective decision-making. Technically, this will be a set of built-in smart contracts and zero-knowledge proof schemes that users can configure for their specific needs.

Retrieving sensitive data with zero knowledge

(additional research is required)

This module will allow making statements about sensitive data without its disclosure. It might use zk-SQL as well as other engineered circuits, but additional research is required.
Use case:

- The employer wants to prove that he has not less/more than X employees emigrants, but cannot disclose either their personal data or companies employees' records. Using ZK schemes, claims about sensitive data can be made without disclosing its exact value.



Shared sequencer

(additional research is required)

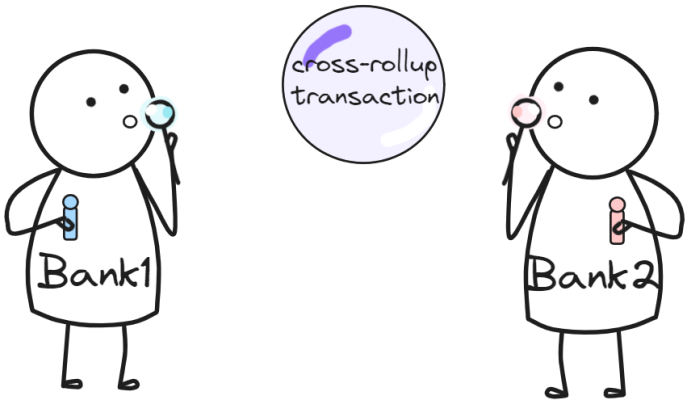
A shared sequencer can handle atomic cross-rollup operations (when transactions are executed on either rollup or are not executed at all). It also eliminates a single point of failure of centralized sequencer architecture and allows fast transaction finality on rollups.

As a basis for a decentralized shared sequencer for rollups, we suggest the Espresso Sequencer. It uses a very resilient multi-layer data availability module (the main goal of it is to store sequenced batched transactions so that they can be accessed later on). As the government controls the

Lockton network, there is not much need to use such secure and resource-intensive DA infrastructure as Espresso Sequencer is using. The second layer, which keeps full data chunk blocks on multiple DA nodes, should be enough as long as we trust the government to keep most of the DA nodes operational (malfunction in some will not cause the system to crash).

Use case:

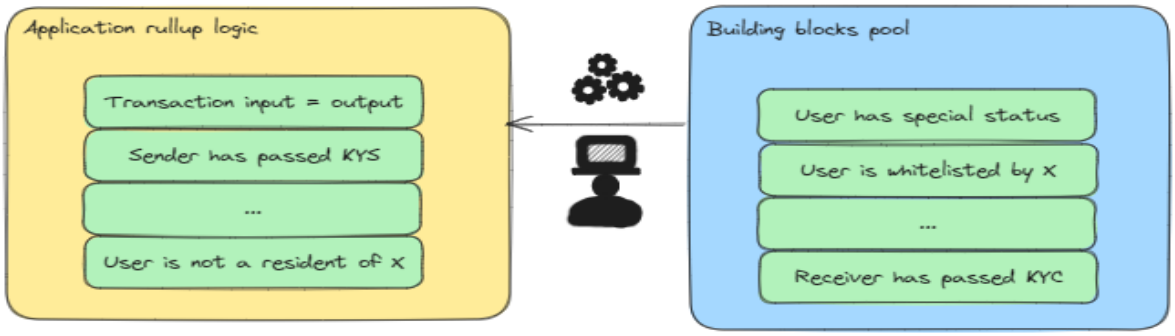
- Bank X and Y are deployed on the Lockton protocol as rollups. The client wants to transfer funds from bank X to bank Y, so the cross-rollup transaction is required. A shared sequencer is used to execute transactions on both rollups atomically.



Application-specific rollup constructor

(additional research is required)

Rollups based on zero-knowledge proofs are required to provide services that require privacy (like banks) and also to scale the network. On the other hand, the Lockton protocol is designed to be controlled by the authorities, which means applications cannot just create arbitrary validity verification on rollups. That is why those rollups must be constructed from predefined building blocks that are approved by the authorities.



Q1 2024 Iden3

Iden3 is a protocol that enables self-sovereign identification.

Features:

- User identification;
- Access policy management;
- Creation of verifiable statements from various organizations and applications.

WebAssembly

WebAssembly is a virtual machine designed to enhance the efficiency of algorithm execution.

Features:

- Improved algorithm execution efficiency;
- Seamless integration of business logic with intensive computations.

Q2 2024 Privacy Pools

Privacy Pools are a mechanism that ensures the confidentiality of data within the platform's core.

Features:

- Transaction history concealment;
- Asset blending.

Q3 2024 DAO and Voting Structure

DAO & Voting Framework is a constructor for designing systems of collective decision-making, comprising built-in smart contracts and zero-knowledge proof schemes.

Features:

- Anonymous voting;
- Community structure creation;
- Community management;

- Integration with smart contracts;
- User identification.

Q4 2024 zk-SQL и zk-ML

zk-SQL and zk-ML are technologies that use zero-knowledge proofs to ensure data confidentiality and security.

Features:

- Statement of confidential data without revealing their exact values.

Q1 2025 Common Sequencer

A Common Sequencer is a component of the system responsible for processing atomic cross-join operations.

Features:

- Atomic transaction execution;
- Cross-join management;
- Elimination of a single point of failure;
- Ensuring quick transaction completion.

Q2 2025 Fold Constructor for Specific Applications

Fold Constructor for Specific Applications is a tool or set of tools that applications can use to generate and verify summary data.

Features:

- Zero-knowledge proof-based unions;
- Definition of building blocks.

Thank you for your attention!
lockton.one