Technical Whitepaper

The SoluTech Team

Scroll
Technical Whitepaper v1.0.1
March 14,2018

SoluTech

Scroll

The SoluTech Team
Technical Whitepaper v1.0.1
February 19,2018

Abstract

Behind every initiative is a mission built from the passion and innovation of problem solvers. It is the innovator's role as a power house of potential influence to automate and secure data management today. A Scroll Token proposes the adoption of the Hypernode Protocol to overcome Blockchain's modern day limitations. It would allow for mass adoption of Blockchain technology through the implementation of a cost-effective enterprise model.

Scroll Token: Introduction

SoluTech's mission is to facilitate the inexorable, yet currently unmanageable growth in industry. We provide the tools to streamline business processes and workflows by optimizing Blockchain technology to transform the Ethereum network into a non-compromising enterprise compatible model. Technology is limited by unborn innovation and technical short-cuts to a necessary design. Not only must we think ahead, but at minimum, we need to provide current solutions cohesive to the current tech available. Scroll Token represents a centralized distributed ledger that is responsive to the biggest prohibitor of the mass integration of Blockchain technology in industry today. The Scroll Network allows for scalable cost-effective transactions at a record Transaction Per Second (TPS) to gas commission ratio without compromising the block size. This will allow businesses to utilize Blockchain technologies with competitive transaction costs and velocities compared to the data management systems today.

Blockchain: The non-compromising Data management solution

All businesses that experience more than a few thousand transactions a minute are unable to scale efficiently to support their growing consumer and user base. As a business scales, the risk management engine needs to work harder and in response, constraints are inserted into the system to sustain the overall system. Today, businesses are utilizing relational, non-relational, and hybrid database architectures to manage client, in-house, and transaction data. Big enterprises are continuously scaling to support an increased userbase in their network in response to the adoption of new and growing markets. Current data management solutions involve functional compromises in latency, indexing capabilities, and analytics.[6] When a business scales the data management architecture becomes more expensive in response to the need for more processing power, memory, and storage.

Much of data management in business falls under the umbrella of Manage Transaction-Oriented Applications (OLTP), a relational database. OLTP databases can be thought of as "operational" databases, characterized by frequent, short transactions that include updated queries to provide concurrency to thousands of transactions. OLTP performs efficiently, but is limited to transactions only in the thousands. In the user case where a company needs to support a higher magnitude of transactions they are limited to non-relational data bases that are unstructured with poor consistency and unavailability of nodes within the network. Currently, the popular data management response to scaling businesses is to implement a hybrid data base architecture which leads to functional compromises that involve extensive training of the end user. [1]

[5] Salehnia, Ali. Comparisons of Relational Databases with Big Data: a Teaching Approach.Comparisons of Relational Databases with Big Data: a Teaching Approach.

[1] Foote , Keith D. "A Review of Different Database Types: Relational versus Non-Relational."DATAVERSITY, 6 June 2017, www.dataversity.net/review-pros-cons-different-databases-relational-versus-non-relational/.

Enterprise Data Integrity

Through the dependency of relational databases, under the central authority of third parties, businesses are now expected to have a data breach risk management plan because without a secure data management solution, a data breach is considered inevitable.[3] Cloud computing can increase these security risks because the data is stored with third-party data centers rather than an internal server. All businesses store sensitive information and risk employee and client information to data leaks. However, some sensitive proprietary data is kept in slightly less volatile private servers because proprietary and client information cannot legally be backed up in a third-party cloud server.

Scroll Network: Enterprise's key to Blockchain compatibility

An energy efficient relational data base Blockchain integration is the innovation businesses need to secure all data managed, as well as cost effectively scale a pre-existing and modular database Blockchain architecture. Blockchain technology currently has been ruled out as a sensible relational database upgrade due to Blockchain incompatibilities with an enterprise model.[6] The Blockchain technology is out of reach for many businesses as the multitude of drawbacks outweighs the advantages. These drawbacks include high latencies, low transaction rates, and significant energy consumption. Blockchain projects such as Ripple, HyperLedger, and the COCO (or Confidential Consortium) Framework have advanced the potential for mass Blockchain adoption in businesses by innovating the consensus model. The hypernode protocol is the first successful innovation to significantly minimize gas consumption rates needed in a Blockchain governed transaction.

Scroll Token consistently performs to provide static low gas commission at extremely high transaction rates with zero involvement or need for miners. The Hypernode Protocol sustains enterprise quality Blockchain conditions through consistent low latencies, immediate transaction finality, high performance, and extensive scalability.

[3] " ITRC Sponsors and Supporters ." Identity Theft Resource Center, www.idtheftcenter.org/2017-data-breaches

[6] Croman, Kyle, et al. "On Scaling Decentralized Blockchains." SpringerLink, Springer, Berlin, Heidelberg, 26 Feb. 2016, link.springer.com/chapter/10.1007/978-3-662-53357-4_8.

[20] 'Mahoney , Paul, and Fenglian Xu. "Create Powerful Blockchain Queries with Hyperledger Composer." Https://Www.ibm.com/Developerworks/Cloud/Library/Cl-Create-Powerful-Blockchain-Queries-with-Hyperledger-Composer/Index.html, 26 Sept. 2016, www.ibm.com/developerworks/cloud/library/cl-create-powerful-blockchain-queries-with-hyperledger-composer/index.html.

The Scroll Network:

The Scroll Network is an upgrade to the Ethereum chain which provides record transaction speed that self-corrects coincident with an increasing user base. For a decade, businesses have prioritized developing a Blockchain ecosystem that provides competitive costs in comparison to the current big data management architecture schemas. The Scroll Network bridges this gap and differs from other centralized Blockchain enterprise targeted models by achieving an ever-scaling verified consensus network of data transactions while only incurring extremely low gas costs. The Scroll Network is a centralized enterprise focused model that sustains improved transaction rates at scaling block sizes. Other Blockchain technologies targeting businesses maximize the transaction speed by setting constraints on network capacities and block sizes and depending on the decentralized nature for security and load balancing. The Scroll Network surpasses the current Blockchain models ensuring mass adoption of Blockchain technology improving the functionally ductile data management tools today. A business always needs to be prepared to scale to support high volumes of data traffic. To achieve record Transaction Per Second (TPS): gas commission ratio, a Verified Peer agent communicates instantaneous algorithmic modifications to promote efficiency in an ever-scaling network.

The centralized Scroll Network achieves groundbreaking, high-capacity, fluid transactions with sub-second latency matching that of enterprise level databases. The desired performance is achieved through the utilization of both a permissioned and prioritized consensus model as well as the Hypernode Protocol.

Peer to Verified Peer [P2VP]: A Behavioral Permissioned Consensus

A P2VP Scroll Network consensus model is comprised of different node types. A node type represents an account type within a < business entity's Scroll Network > that has assigned privileges. Privileges are assigned based on the identified node type base privileges and node ID for privilege modification or revocation of any one account assigned to a base node type. All node types that are not classified as Peer node types are under the umbrella of Verified Peer node types. To sustain secure distributed governance with supported multi-layered access control, the peer node in an individual's Scroll Network will always be the majority node type at any given time. When a Peer node type is registered to a <business entity's Scroll Network>, a person's node ID is tethered to the base node type and enrolls in Verified Peer-determined certificates representing privileges. Each Peer node digital signature is linked to the previous and the next Peer node's digital signature. All decisions confirmed from a registered Verified Peer node is linked to the system's designated Peer node system at that time. If one node type takes a representative majority in the ecosystem that node type becomes the new Peer-node. In comparison, a Verified Peer node type can be representative of many different Base node types. Registration of node IDs and modification and design of base node type certificate assignment is confirmed by all Verified Peer nodes that are registered with the privilege to accept the new protocol to query, add or update blocks to the Blockchain. The active peer nodes in the Scroll Network are designed to automatically accept the Verified Peer's proposed addition to the Blockchain. Much of the peer node represents an ecosystem that prevents any malicious middle man's attempts to access or modify data.

The Hypernode Protocol

The Scroll Network minimizes transaction rates in high traffic network conditions by communicating transactions through a system of Verified Peer nodes through utilization of the Hypernode Protocol. Standard Blockchain platforms automates peer to peer consensus in the network. Meaning, the transactions processed and annexed to the ledger cannot be controlled or prioritized. As a result, all nodes download the entire ledger history and exhaust incredible computational power to add blocks of data to the ledger. Traditionally, the order in which the blocks are added is dependent on which user's computer exhausts a given gas rate needed for the Ethereum smart contract to execute first. The Hypernode Protocol removes the uncontrolled automated nature of the standard Blockchain transaction processing methods. Instead, algorithmic modifications governed by the user's base recorded transactional data and a Verified Peer customized priority engine allows for an optimized transaction process. To sustain and achieve the optimizing behavior of the Scroll Network, the nature in which data is moved is fed to the self-correcting algorithm. This ensures the hypernode transit protocol is updated resulting in minimized transaction costs and maximized transaction processing rate in response to the new inputs in the system.

The Hypernode Protocol has already been tested and due to its operational resilience, the following enterprise use cases defined below are manageable with the insertion of a Hypernode Protocol in the Ethereum chain:

1. Transactions involving confidential or sensitive information:

For a business to acquire a secure Blockchain infrastructure as a data management system, supporting transactions involving role-based privileges is necessary. For example, a real estate company adopts the Scroll Network and has base node types for an agent and a buyer. There will be more buyer base node types than agent base node types and therefore, all buyer node types act as a cluster of Peer nodes and the agent's base node types act as the Verified Peer node. The agent node would have base privileges initially defined during the onboarding enrollment process in the Scroll Network to assign the privileges of the default agent base type node. However, Agent A and Agent B have different node IDs so that a Verified Peer and all peer nodes can allow an addition or removal of privileges for that specific node ID. The buyer type nodes, which acts as the peer-node type at a given time due to the majority representation in the ecosystem, will all have the same privileges regardless of node ID. Agent A has information on Client C and Agent B should not have access to the Client C information data sets. In this case, Agent A is equipped with a unique node ID, granted access to a private ledger of their client's information by a Verified Peer supported consensus. The buyer node type (in this case the Peer node) privileges are replicated and stagnant for all peer nodes. In this case, all buyer nodes would have zero access to all client information, but would have access to their own profile. The modular and secure registration of privilege assignments exemplify the capability for the Scroll Network to support role-based access and transfer of data to ensure the integrity of proprietary and confidential information.

2. Transactions with multiple entities:

Unlike your standard Blockchain model with two participants per transaction, an enterprise model supporting transactions with multiple entities involved are required. Although certain node ID's have varying privileges, they should still be able to make transactions with a higher or lower privileged level node. To achieve a transaction with a block data that has role based sensitive data, a multi-layered selective encryption must be utilized. This means based on the node ID's privileges, they will only be able to decrypt data their associated privilege has deemed available. This model allows smart storage of data in blocks to minimize the network's work intensity, as data is strategically stored in transaction node.

A Secure Way to Scale

A business scales in tandem with advancing technologies to preserve their value proposition and, therefore, place in the market . Unfortunately, with the insertion of these new technologies into the workflow, there is a growth in the potential cybersecurity risks. Cloud computing platforms are currently the most cost-effective utility for a scaling business to store and access data. As a result, online data storage has also led to a multitude of sensitive data breaches. However, the business practice of entrusting 3rd party servers to hold confidential information is still commonplace due to the need for a cost-effective method to scale big data, which some believe outweighs the risks involved.

The Scroll Network provides a secure data management solution, while matching all the benefits of a traditional cloud-based data management infrastructure, including a cost-effective method to manage transactional data with high availability. With the integration of Blockchain technology as a data management utility in enterprise, many of the security risks are removed. Data in the Scroll Network is protected through cryptography, P2VP consensus protocol, mononitration, and back up storage capabilities to mitigate the current security risks embedded in the cloud server solution outlined below:

Data Breaches

A Cloud's weakness:

Most of the data breaches experienced in 2017 were attributed to a configuration error which left confidential data, decryption keys, plaintext passwords, authentication credentials, and cloud data mapping classified material publicly exposed. A file repository misconfigured grants public access to download closed sourced material, proprietary information, as well as health, financial, and identity sensitive information. With authentication credentials and cloud data mapping specification left exposed, the ease of infiltrating more sensitive information is inevitable. Most of the configuration security failures are not discovered for months, allowing for malicious entities to store and utilize data from public containers to acquire more sensitive information within a database.

The Scroll Network Response: A Centralized Use Private Network

The centralized use design allows for a business to store, access, and analyze structured data sets in a private secure Blockchain, removing all vulnerabilities of publicly exposing data to third-party servers. For any users to access the Blockchain they need to be registered with a node ID to interact with the data in the Blockchain. Each node ID will be able to access Verified Peer determined data substantiated by P2VP confirmations based on a node ID's certificates. If a node ID does not have the privilege to access a data set, the transaction to observe the data will be unconfirmed by the P2VP trust network.

Inadequate Credential Management and Insider Vulnerabilities

A Cloud's weakness:

The adoption of cloud computing has fast-tracked the accessibility to data stored while minimizing data management scaling expenses. However, this accessibility allows for illegitimate users to masquerade as users to read, write, and remove data. This vulnerability, due to the lack of a robust identity management engine allows for the malicious middle man to read or switch data being stored in transit and can potentially be utilized as a "back door" to embed malware that unknowingly is a credible source from all users leading to severe cybersecurity attacks potentially impacting all end users.

The Scroll Network Response:

The Scroll Network is constantly recording the data transit route clusters of similar transactions to optimize the method in which data is transacted and, therefore, maximizes transaction speed. In addition to recording transit data, the Scroll Network also monitors the proposed transactions of all given node ID's. If any bizarre behavior were to occur the node is transformed into a ghost node, freezing all access until a system administrator updates the node's certificates to allow for the tracked uncharacteristic behavior. Until then, a ghost node's previously acquired certificates are revoked to preserve the integrity of data accessed and modified.

The Scroll Network also protects any registered nodes from accessing confidential data within the network through selective cryptography to support multi-layered access control. This means depending on the node ID, one user can access a transaction with multiple documents involved and only the documents cleared by the node's ID will be decrypted when the file is unzipped.

[3] CLOUD SECURITY ALLIANCE The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights. Cloud Security Alliance , 2017, CLOUD SECURITY ALLIANCE The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights, downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf.

[4] Abadi, Daniel J. Data Management in the Cloud: Limitations and Opportunities. Data Management in the Cloud: Limitations and Opportunities, www.cs.yale.edu/homes/dna/papers/abadi-cloud-ieee09.pdf.

Conclusion

The Scroll Networks utilizes the Hypernode Protocol to provide a non-compromising cost effective data management solution. Modernization of the implementation of Blockchain technology as a database in business provides optimal security, performance, scalability, and supportability for elastic and flexible design implementations. The Scroll Network allows for a cost effective Blockchain upgrade in a company's data infrastructure through an innovative design proved to minimize gas consumption while maximizing transaction rates. Unlike traditional server farms and cloud-based data management systems the advent of Blockchain technology in enterprise removes today's inefficiencies including data redundancy, data losses, and data syncing compatibilities. All facets of a business are information driven today and in response, big data has revitalized data storage, transfer, and usage, reinforcing a market need for secure data management at high performance rates.