AUTHERIUM

Standard Cross Finance Chain

High-Performance Public Chain for Next- Generation

Cross-Chain Financial Interactions Standard

V2.1.5

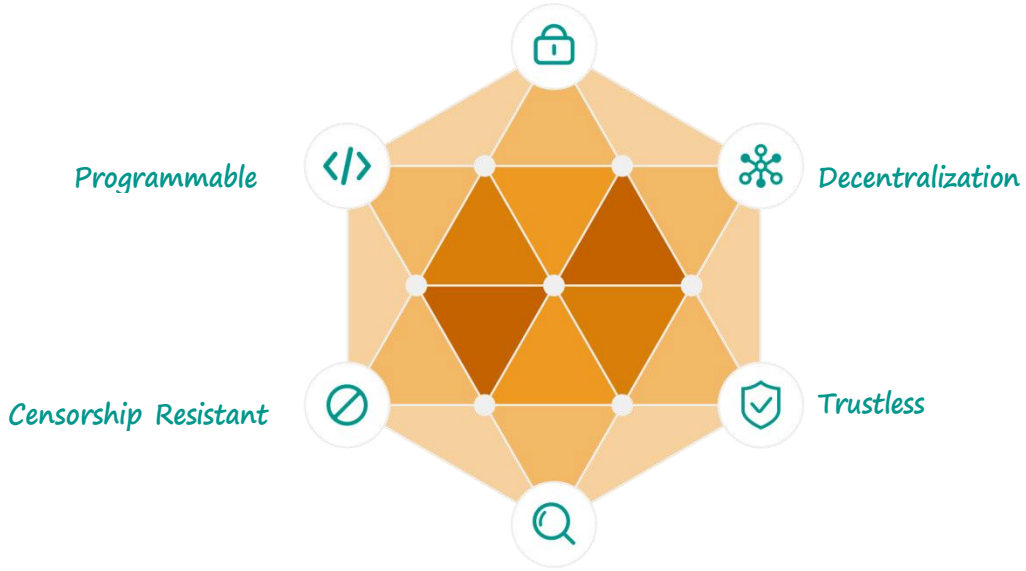
Table of Contents

Background

Over the past century, the financial sector has provided society with rapid access to original capital, significantly advancing the development and progress of human culture. Yet, as capital expanded, mainstream financial institutions and regulators prevailed and began to dominate the financial system with an unshakable standing progressively. However, they were criticized for their over-centralized power and operational loopholes. These financial institutions and so-called regulators have been repeatedly questioned for manipulating the market in their own interest, resulting in greater risk to investors' assets. Traditional financial models and regulatory approaches failed to address the root causes of investors' concerns about the safety of their money, rendering the investment environment deteriorating. For this reason, the financial market is in dire need of a change to transform this situation.

DeFi

At length, beginning in 2019, decentralized finance (DeFi), underpinned by blockchain technology, has enabled people to explore a whole new market paradigm, where code is the law and investors can operate financial activities entirely on a blockchain that requires no trust.



The distributed ledger technology (DLT) enables more transparent and secured financial transactions and asset depository.

Smart contracts and immutability eliminate the risky manual operation process and the potential hazard of intermediary doing evil, further enhancing the security of financial data and matchmaking efficiency.

A batch of innovative models such as flash loans and algorithmic stablecoins, which are inconceivable in traditional finance, have sprung up, leveraging the underlying characteristics of consensus. Undoubtedly, blockchain finance is making the world even more fascinating and beautiful. However, we are keenly aware that many urgent challenges are standing in the way of innovation.

The throughput of existing public chains can hardly meet the centralized and concurrent response of large-scale financial services, the data/information silos caused by multi-chain competition are aggravating, and cross-chain financial interactions are yet to be adequately addressed. Furthermore, the high development threshold in crypto has turned away many excellent teams and traditional institutions committed to DeFi. The Web 3.0 world calls for an ultra-high-performance public chain that can bridge the technical gap among traditional finance, crypto finance, and multi-chain interaction, serving as the cornerstone for DeFi's robust development and popularity.

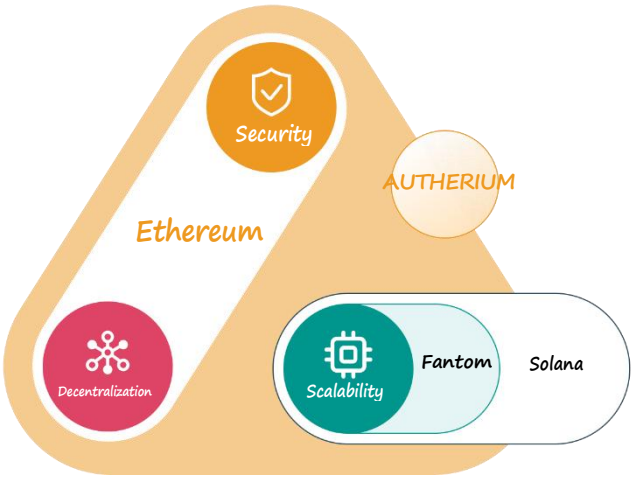
1. Introduction

In pursuit of a better DeFi infrastructure, Bob Lambert and William Thompson, both Stanford graduates, have formed a team of blockchain senior technologists and fintech academics to create AUT, a public financial chain with a dual-chain architecture. Ultimately, all public chains seek to optimize the impossible blockchain triangle, namely high performance (i.e., scalability), security, and decentralization based on their goals.

Decentralization is about leveraging a large number of network nodes to pack blocks for data validation. Typically, the more nodes there are and the more dispersed they are, the higher the decentralization (closer to the ideal blockchain concept). Security is the cost of gaining control of the network and is usually anchored to real-world assets during the design of consensus mechanisms. For example, the Proof-of-Work (PoW) mechanism is anchored to the hash rate. Performance can be briefly construed as the number of transactions processed per second. The primary cause of blockchain inefficiencies is the time required to agree on data across more nodes for each transaction.

The traditional single-chain structure cannot reconcile the balance of the three, which is determined by the law of logic.

AUT has a concurrent performance over Ethereum. Besides, it has a massive number of nodes for computation and verification that are hard to look away from for Solana and other insufficiently decentralized chains, which expands the performance and improves the ecology based on



We believe that financial innovation is an ultimate proposition that accompanies social development. In the future Web 3.0 network, innovations are bound to flourish, and only an all- around public chain with sufficient foresight and inclusiveness can become the infrastructure matrix of DeFi.

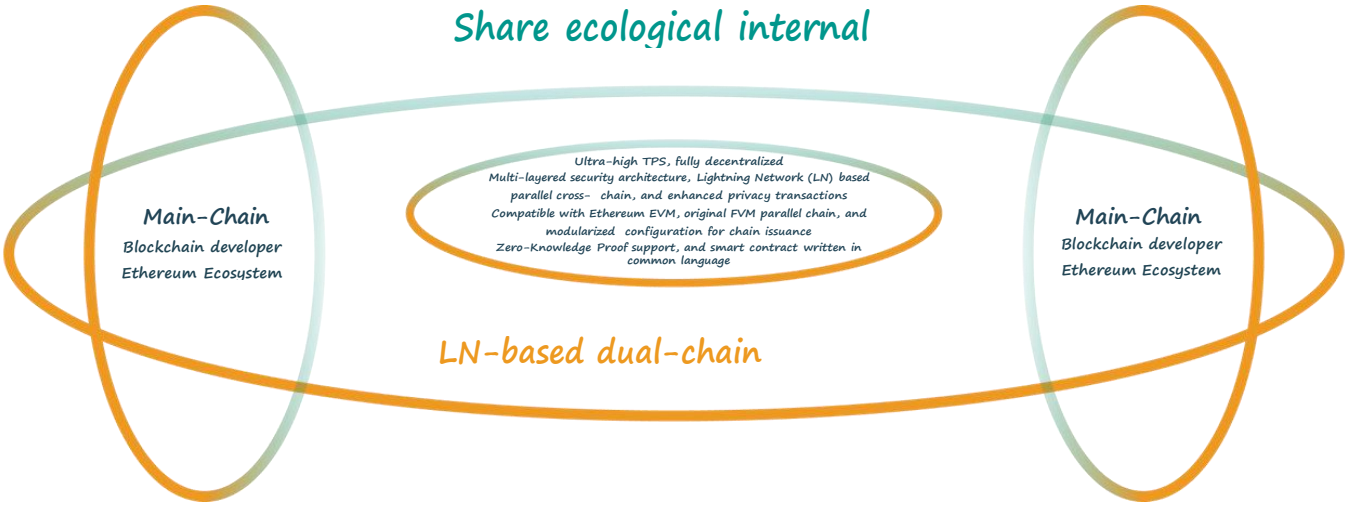
In designing AUT, we build the network layer through the dual-chain structure and the cross- chain ecology through atomic exchange and a standard programming interface. Combined with the next cross-chain DEX, we demonstrate the innovative practice of the application layer,

providing a systematic methodology for the industry. Finally, we establish the next-generation standard model for cross-chain financial interaction.

2. Dual-Chain Architecture

2.1 Structure

AUT which stands for Standard Cross Finance pioneers a dual-chain structure and serves the blockchain industry and traditional financial institutions, respectively. Each chain performs its own function and interacts with one another efficiently, solving the challenges of performance, security, decentralization, cross-chain transactions, and ecological scalability for the financial sector. The network layer of the AUTHERIUM comprises the Main-Chain and the Fin-Chain.



2.2 Main-Chain features

The Main-Chain is cornerstone of AUTHERIUM's existence, geared towards blockchain developers and users, handling contractual interactions between native governance tokens and the Ethereum EVM projects. The functions and features of Main-Chain are:

- Executing smart contracts

Executing smart contracts efficiently, performing token creation and native transactions, and supporting smart contract development in Solidity language.

- Compatible with Ethereum EVM

Helping developers quickly transplant Ethereum DApp to the AUT ecosystem.

- Generating APoS consensus for blocks

Processing APoS consensus of the main block of the public chain for transaction verification and validation.

- Assets cross-chain off atomic swap chains

Helping users quickly transfer assets from various chains to AUTHERIUM.

2.3 Fin-Chain features

Originated from and standing for finance, the Fin-Chain is designed for the massive traditional financial institutions to rapidly transplant their applications onto the chain. The functions and features of Fin-Chain are:

- LN-based parallel cross-chain

Unlike assets cross-chain off the atomic swap chain of the Main-Chain, the Fin-Chain enables efficient interaction of data and assets between dual chains and Fin-Chain's parallel chains with different consensus through the Lightning Dog underlying contract. While ensuring node stability, the Fin-Chain provides more inter-chain connections to form the Lightning Network, with a fantastic second-level cross-chain response efficiency. As a result, the projects among public chains will be connected to creat a more robust inner-loop symbiosis. (Privacy chain data can only be accessed by the nodes and approved addresses that constitute a privacy channel)

- Zero-Knowledge Proof based privacy transactions

- Both AUTHERIUMs support "Zero-Knowledge Proof" technology, which enables several cutting- edge and critical applications such as off-chain scaling, transaction privacy protection, anti- complicity, and on-chain compression. This technology will be discussed in later sections.

- Modularized deployment for one-click chain issuance

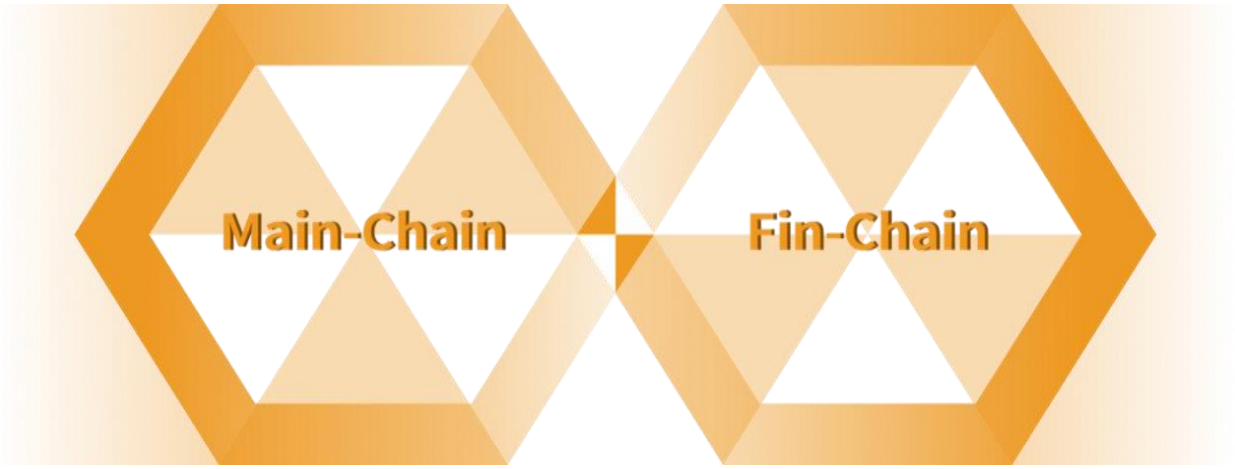
Third-party developers can build their own parallel chains (PBFT, PoW, PoS, APoS) and choose different consensus mechanisms with supporting facilities, including block browsers, wallets, etc. This modularized deployment technology significantly reduces the development costs for enterprises to build complex DApp services and their public chains.

- Complex smart contract development in common languages

It supports smart contract development in Java, GO, and other mainstream languages, which is the

friendliest access to non-blockchain developers in the finance and Internet sectors.

The APoS of AUTHERIUM refers to Asset Proof of Stake. The APoS consensus mechanism inherits and develops the existing PoS, which follows the decentralized path of PoW consensus and is more eco-friendly and energy efficient. Meanwhile, its economic model that integrates PoS and DPoS also avoids the drawbacks of its over-centralization.



AUT's dual-chain architecture provides the optimal solution for the impossible triangle in finance. Processing of simple and complex contracts with different chains reduces the computational load of the whole chain and facilitates resource isolation. The eco-projects on the Fin-Chain can increase their TPS based on their own hardware clusters without any limit, thus enabling the performance to skyrocket.

3. Performance and Demand Assessment

The performance of public chains is usually measured based on TPS (Transactions Per Second). The Main-Chain has an average TPS of over 7500+ and the Fin-Chain over 80000+ based on hardware performance, which can better meet the extreme concurrent demand of super large- scale financial applications than other public chains.

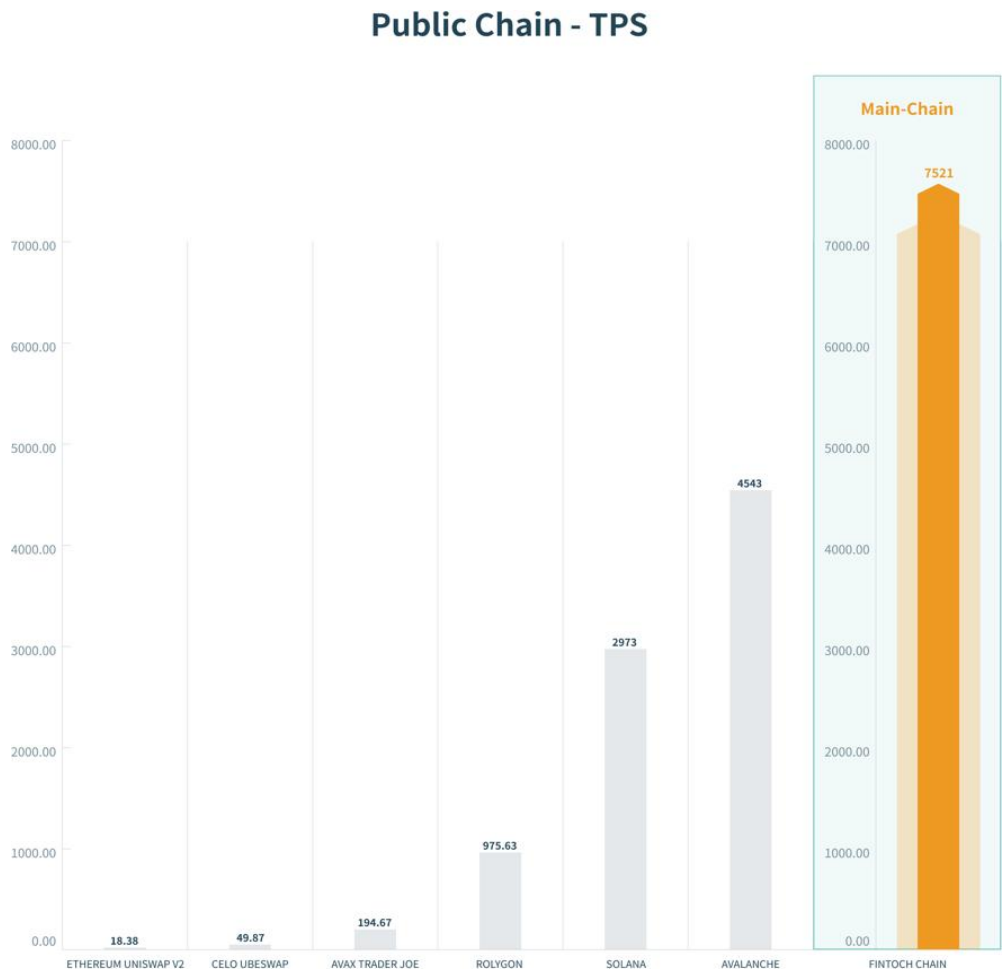
Currently, the TPS values (in thousands) provided by various public chains in the market are theoretical peaks under ideal conditions for the sake of differentiated competition with ETH. Once the nodes are deployed on a large scale, the real average TPS will decay tens or hundreds of times due to multi-node network differences, code optimization, cross-border firewalls, and complex applications.

The most scientific approach for public chain performance assessment is to calculate the Swap contract interaction consumption of Gas with the formula:

$$TPS = \frac{\mathrm{GasLimit}}{\mathrm{GasUsedPerTx}} \div AverageBlockTime$$

Solana is rather unique in that there is no Gas Limit and exceeding the TPS limit brings problems such as block blocking, synchronization delays, and transaction failures. However, we can observe the upper limit it may reach by looking at historical data on the browser.

This formula is a relatively fair calculation recognized by the public, as each chain has different transaction components, and the differences would be enormous by just calculating common transactions.



From the above chart, we can see that among the main chain of each public chain, AUT has the highest TPS limit of 7521, followed by Avalanche at 4543 and SOL at 2973. Among the EVM- compatible chains, the highest is Coin BSC at 194 and ETH at 18. The main chain TPS of AUT is 417 times that of Ethereum.

Each chain has suffered performance problems, and the AUT dual chain addresses the following issues fundamentally:

Ethereum: Since its inception, Ethereum has experienced several rounds of sustained massive block congestion events every year. In April 2021, Ethereum's single transaction fee at Uniswap was up to $100, and its synchronous latency grew tens of times, failing to carry demanding financial services.

Solana: It has limited the flow of requests during peak periods and experienced several downtime disasters that brought down the entire Sol blockchain. Though data flow control technology was introduced, and the Gas model improved later, the effect was evaluated by experts to be limited.

Avalanche: A cross-chain function error was triggered by a high DEX Pangolin load, which caused some short-term panic in the community.

BSC/Polygon: There was congestion in Q2 2021 due to a burst of on-chain activity, which was followed by a spike in Gas fees.

Measured in terms of usage: Assume X is the number of transactions per day and the required TPS is T.

According to the Pareto Principle (80/20 Rule): 80% of X transactions need to be completed in 20% of the time, and T1 needs to meet the peak requirement. These yields:

T1 ≈ X * 80%/（24h * 20%）* 3600）≈ X / 21600

Given a stable network and user demand growth, we can further consider an average user distribution to derive an average TPS demand.

T2 ≈ X /（24h * 3600）≈ X / 86400

Actual TPS required for the average daily transaction of a public chain: See the following table

Development	Total average daily transaction	T1 demand (TPS)	T2 demand
Startin	10,000	0.46	0.12
Developmen	1,000,000	46.3	11.6
Surging	10,000,000	463.0	115.7
Maturit	30,000,000	1388.9	347.2
y	150,000,000	6944.4	1736.1

The above table shows that a TPS of about 7000 enables the processing of 150 million transactions per day.

The Main-Chain can process an average of 150 million transactions per day for applications of native governance tokens and their contractual interactions.

Depending on its hardware deployment, a Fin-Chain eco-project can handle a data volume exceeding that of a VISA credit card, with an average of 1.5-2 billion transactions per day.

AUT will become the only super financial public chain on the market that can meet the needs of traditional financial giants to integrate into the ecosystem.

4. Consensus Mechanism

4.1 Main-Chain consensus

The high energy consumption of PoW is gaining prominence in the context of global carbon neutrality, constraining to a certain extent the widespread adoption of blockchain networks worldwide. After evaluating various aspects such as security, performance, energy efficiency, and user-friendliness, the Main-Chain decided to adopt APoS consensus.

Let's take a quick look at the PoS consensus. Unlike PoW, which requires tremendous power consumption to solve a mathematical puzzle, PoS is a pledge-based algorithm where the pledge is the keyword. To simulate the process of the equity-based validator (in PoS, we prefer the term validator rather than miner) selection, we adopted the algorithm which follows Satoshi Nakamoto (FTS) in many PoS-based blockchain networks (e.g., Cardano, Dash, etc.).

The probability Pi of selecting node i as a validator in a network with N participants is:

$$P_i = \frac{S_i}{\sum_{j=1}^{N} S_j}$$

Si represents the share (Token holding share) of participant i. This means that the more shares a node holds, the higher the chance for it to be selected as a validator, The verifier receives tokens as a reward.

Now let's move on to the improved APoS, Asset Proof of Stake. The APoS consensus mechanism inherits and develops the existing PoS, which follows the decentralized path of PoW consensus,but is more eco-friendly and energy efficient. Meanwhile, its economic model that integrates PoS and DPoS also avoids the drawbacks of its over-centralization.

APoS can better optimize and present a peer-to-peer electronic cash system based on the cross- chain gateway, outperforming all other public chains in terms of payments. You can settle your transactions in the Main-Chain with multiple cryptocurrencies,as the Main-Chain introduces a cross-chain relay to the consensus layer.Communication and consensus are performed through the Hot Stuff protocol, which dramatically speeds up communication and consensus on a secured basis.

In theory, the Main-Chain enables nodes with any digital assets to participate in the main chain consensus and any public chain Token to participate in the stake pledge to get the AUT incentive of blocks generated by the main network, including AUT's governance token AUT, making it the most user-friendly consensus participation mechanism.

4.2 APoS consensus operation mechanism

In the below diagram, each actor can subscribe to support their preferred super node candidate, who is

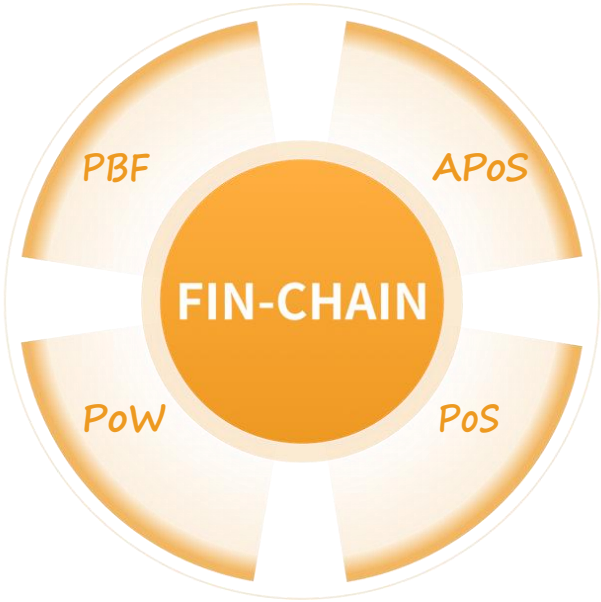
then elected as a validator, and Validator 100 will be selected in a network-wide election.

Anyone with suitable blockchain resources (hardware, servers, bandwidth) and sufficient crypto assets can apply to be a super node candidate by running for election. A total of 100 super nodes are set across the network. The APoS consensus mechanism selects the 100 super nodes as Block Validators and then elects a super node as a validator by a Zero-Knowledge Proof random algorithm. Afterward, if the chosen validator does evil or the hardware goes offline, a corresponding slashing (penalty) will be triggered. A new super node will be elected as a renewed validator when the penalty reaches a threshold. A super node that does grave evil will be disqualified as a node. The verifier employs an algorithm of discrete loop mechanism to sequentially generate blocks and obtain AUT rewards, which are then distributed to each super node by a built-in smart contract.

4.3 Fin-Chain consensus

Designed for scalability and compatibility, Fin-Chain revolutionarily allows project owners to freely choose different consensus mechanisms by customizing their public chains to match their business needs.

The first four types of consensus mechanisms supported and under development are PBFT, APoS, PoS,and PoW.



In this section, we will focus on the Practical Byzantine fault tolerance (PBFT) consensus. The Fin-Chain's PBFT takes IBM's Hyperledger Fabric as the blueprint for development and employs the "endorsement –> ordering –> verification" approach for consensus.

Traditional distributed consistency algorithms generally address consensus issues by negotiation, which provides (n-1)/3 fault tolerance for a network with n nodes while ensuring liveness and safety. Byzantine nodes can be considered as nodes that adversaries attack and reducing the creation of Byzantine nodes entails making it more difficult for adversaries to attack. For this reason, we can either increase the number of nodes or randomize the nodes that generate blocks.

The Fin-Chain is a parallel chain platform that allows multiple parties to participate, develop, deploy,

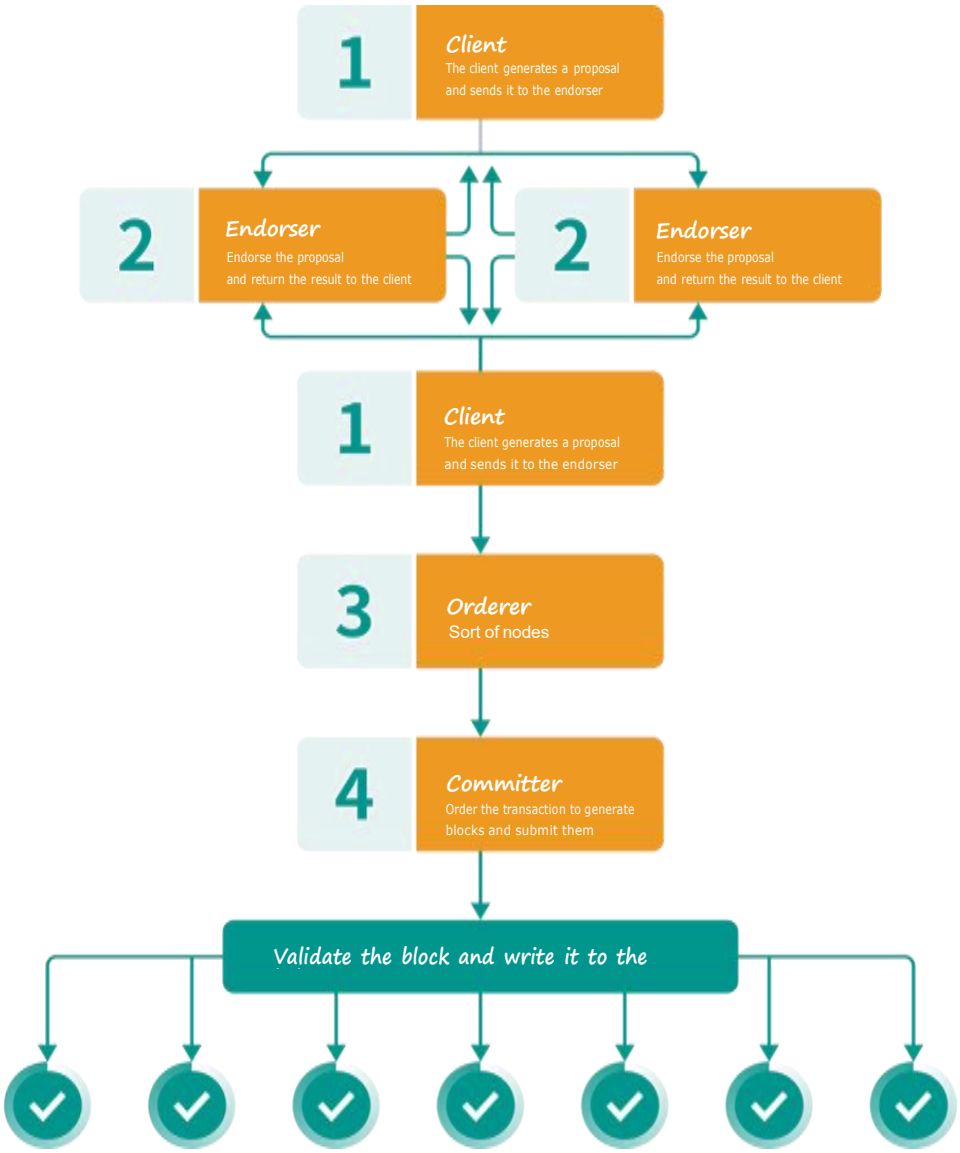
and operate blockchain applications. The Fin-Chain adopts Hyperledger Fabric to create a modularized and scalable blockchain development framework, providing solutions for developing enterprise-level blockchain applications. The Hyperledger Fabric blockchain system comprises the following main components:

Chaincode: A smart contract in Hyperledger Fabric that anchors complex business logic in the Fabric system in the form of code. A chain code is executed when certain conditions are met.

Client: An access point between users and the Hyperledger Fabric network, on which a proprietary SDK is deployed. Users can initiate a transaction request, i.e., ProPoSal, using the client.

Endorser: In Hyperledger Fabric, when a client wants to initiate a transaction, it first needs to get a certain number of endorsements for the transaction. These endorsements come from the endorser. The endorser executes a simulated transaction by running the chain code, generates a read-write set, and then endorses the transaction (signing the read-write set and attaching its identity) to prove that the endorser has processed the transaction.

Orderer: Hyperledger Fabric provides ordering services through multiple orderers. The ordering service receives all transactions from across the network and packages them into blocks in chronological order. The ordering service does not involve in the execution and validation of transactions and therefore pays no attention to the specifics of the transactions. The goal of the ordering service is to agree on the order in which the transactions are generated and to broadcast the result.
Committer: A main body that maintains the ledger in the Hyperledger Fabric network. The committer receives the blocks packed by the ordering service, verifies the validity of the transactions in the blocks, and commits the valid transactions to the ledger accordingly. In addition, the endorser also belongs to the submitter, and endorsement is an additional function of the endorser on top of ledger maintenance.



The Fin-Chain also supports the classical Proof of Work (PoW) method of randomly selecting block generators. "Mining" involves each node constantly trying to solve a mathematical puzzle that is difficult to solve but easy to verify. The node that solves the puzzle fastest gets the right to publish the following block (bookkeeping right) and a reward from the system. The randomness of PoW relies on the even distribution of hash function values. Yet a large amount of hash computation is accompanied by massive energy consumption, and the problem to be solved by such consumption is meaningless. Meanwhile, with the emergence and development of "mining machines," the computation is gradually monopolized by some large mining pools, posing a threat to system security. In addition, PoW consensus is less efficient, and its long block generation and transaction confirmation times make it challenging to meet realistic demands.

Although Proof of Stake (PoS) also selects block generators via "mining," the probability of successful "mining" relates to the node's equity. The greater the equity held by a node, the higher the probability of successful "mining." These speeds up the block generation rate and improves consensus efficiency. At the same time, as the amount of computation is no longer a major factor influencing "mining" in PoS resource wastage due to the reduction of heavy computation.

Notably, based on PoS, the Delegated Proof of Stake (DPoS) achieves higher consensus efficiency by sacrificing certain "decentralization" features. Each node can vote for a representative with its equity. The top N users with the most votes will constitute the consensus participation "committee" where each member takes turns to package transactions and generate blocks. Thanks to the reduced number of participating consensus nodes, DPoS offers high transaction speed. However, the proxy nodes created by DPoS in the decentralization process make the adversary's attack target more specific-clearer and reduce the cost of the adversary's attack; therefore Fin-Chain has no plans to support it for the time being.

5. Zero-Knowledge Proof

Zero-Knowledge Proof is one of the Layer2 scaling schemes supported by both AUTHERIUMs and is an optional module when building parallel chains through the Fin-Chain.

A Zero-Knowledge Proof is defined as the ability of a prover to convince a verifier that an assertion is correct without providing any helpful information to the verifier. As an iterative fruit of cryptography, the application scenarios of Zero-Knowledge Proofs include but are not limited to:

- Collusion and evil resistance
- Decentralized storage
- Off-chain scaling - improving transaction throughput
- On-chain compression - dramatically reducing on-chain data and block size to improve verification efficiency
- Full protection of user data privacy (e.g., mixed-currency applications, where the actual transaction address is unknowable)

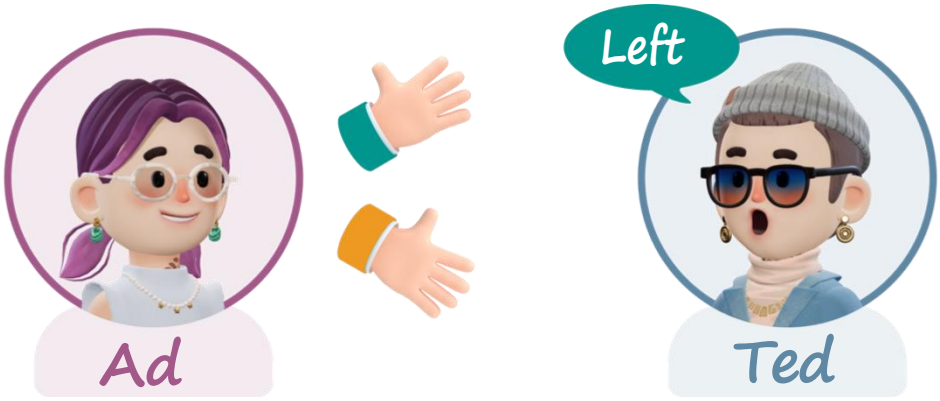
By deepening the applications above, AUT's system will be more secure and robust, with proper isolation of user privacy. Sustained development can even revolutionize how data is shared and blockchain works. The modern Zero-Knowledge Proof system originated from the paper "The Knowledge Complexity of Interactive Proof Systems," co-authored by Goldwasser, Micali and Rackoff, which was modified by crypto pioneers and AUT. The non-interactive system born on this basis features completeness, making it the perfect option for the Zero-Knowledge Proof system.

To facilitate understanding of this important technique, let's take a classic example of Zero- Knowledge Proofs:

5.1 Interactive Zero-Knowledge Proof (A game for color-blind people)

Suppose Ada is color blind and Ted is not. Ted has two balls of absolutely the same size and shape in his hands, but one is green and the other is yellow. He is required to prove to Ada that the two balls are of different colors. In this classic case, Ada is the verifier, who needs to verify whether Ted's statement is correct or not, and Ted is the prover, who needs to prove to Ada the fact that the two balls are not of the same color if Ada cannot identify the color. This is a common explanation of the Zero-Knowledge Proof.

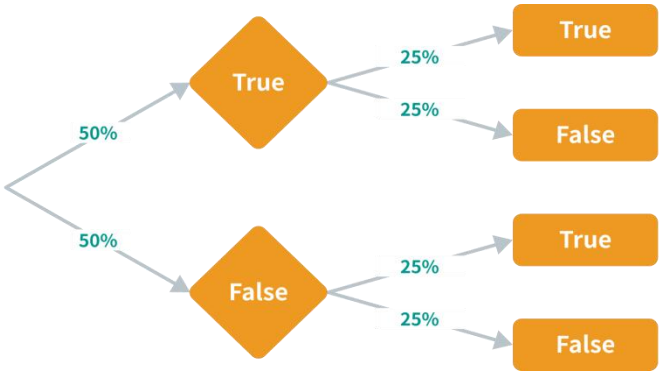
The process is as follows:
Ada picks up the two balls in front of Ted, with the green one in her left hand and the yellow one in her right hand, and then puts her hands behind her back so that Ted cannot see the balls. Ada randomly exchanges the balls in her left and right hands behind her back. After the exchange, Ada extends her hand and asks Ted if the two balls have exchanged positions. If Ted is able to identify the color of the balls, then he will be able to answer Ada's question correctly each time she changes the position of the balls.



For the first time, Ada secretly exchanges the position of the balls in her hands, then asks Ted if she has exchanged the position of the balls. If Ted's answer is Yes, then Ada has a 50% probability of believing that Ted can distinguish the colors of the two balls, because Ted has a 1/2 probability of making a correct guess. Ada can therefore test Ted a second time. If Ted's answer is No, then Ada is sure that Ted cannot distinguish the colors of the two balls.

For the second time, Ada does not exchange the position of the balls in her hand, and then asks Ted if she has exchanged the position of the balls. If Ted's answer is No, then Ada has a 75% probability of believing that Ted can distinguish between the colors of the two balls.

The following is the probability tree for the above case:



After the first iteration, the probability that Ada can assert that Ted's statement is true is 50%. If Ted gives the correct answer the second time, then the probability goes to 75%, and after the third iteration, it will be 87.5%. If Ted passes the tests n times in a row, then Ada has a probability of 1 – (1/2) ^n to believe that Ted's statement is true.

A Zero-Knowledge Proof is a probability-based verification method in which the verifier asks the prover questions with some randomness. The prover has a high probability of possessing the "knowledge" he claims if he can provide correct answers. A Zero-Knowledge Proof is not a proof in the mathematical sense, because it involves a small probability of error, that is, an evil-doing prover may deceive the verifier by making a false claim. In other words, a Zero-Knowledge Proof is a probabilistic proof rather than a deterministic one. However, technology can reduce the error to a negligible value.

According to the definition of Zero-Knowledge Proof, we can learn that it has the following three important properties:

1） Completeness: If the prover possesses the relevant knowledge, then he can pass the verifier's verification, that is, the prover has a large enough probability to convince the verifier.

2） Soundness: If the prover does not possess the relevant knowledge, then he cannot pass the verifier's verification, that is, the probability that the prover deceives the verifier is negligible.

3） Zero-Knowledge: The prover reveals only to the verifier whether or not he possesses the relevant knowledge during the interaction, without revealing any additional information about the knowledge.

In this example, if Ted does possess the knowledge to distinguish the color of the balls, then he will answer correctly every time, which is considered as completeness. If Ted does not possess the relevant knowledge to distinguish the colors of the balls, then he cannot tell whether Ada has exchanged the balls or not. This is referred to as soundness. In this protocol, Ada cannot see the color of the balls, which is Zero-Knowledge.

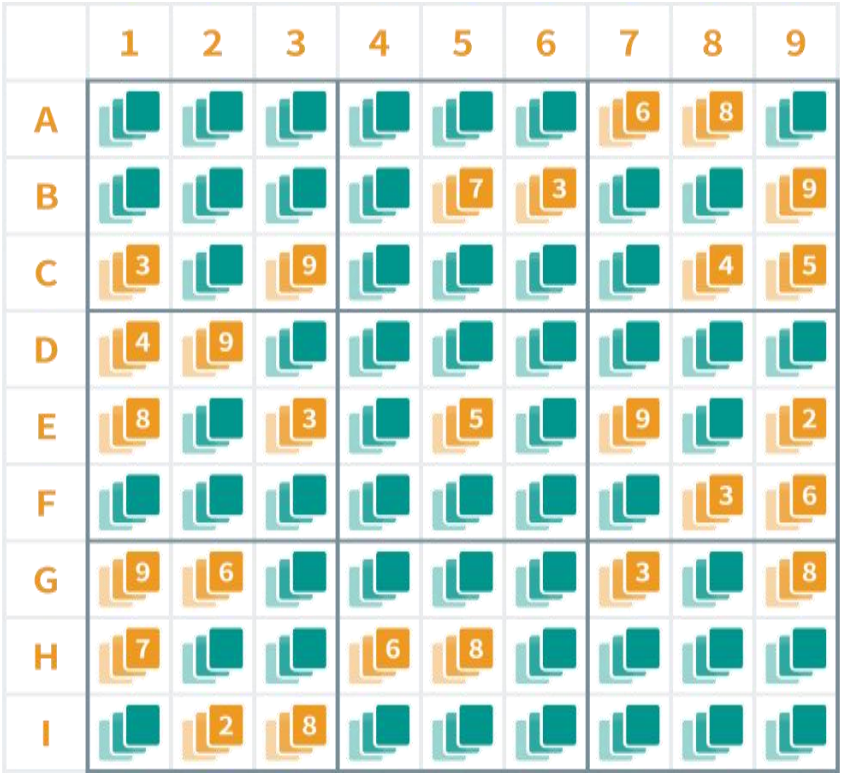
Non-Interactive Zero-Knowledge Proof — Sudoku

Interactive Zero-Knowledge Proof protocols rely on random attempts by the verifier and require multiple interactions between the prover and verifier to complete. Non-Interactive Zero-Knowledge (NIZK) Proof reduces the number of interactions to one, enabling offline proofs and public verifications. In AUT's Zero-Knowledge Proof application scenarios, the non-interactive nature is necessary because in a blockchain system, it cannot be assumed that both parties are always online and interacting. On a AUTHERIUM, the prover simply broadcasts a proof transaction to the entire network, and miners on the network help the prover verify the Zero-Knowledge Proof when they pack this transaction into the block.

We can understand the super-efficient non-interactive proof of AUT by a Sudoku case: Sudoku is a numerical logic reasoning game that originated in Switzerland in the 18th century, in which calculations are performed using both pencil and paper. Players need to deduce the numbers of all remaining spaces according to the known numbers on the 9×9 disk and satisfy the requirements that the numbers in each row, each column, and each thick-line palace (3*3) contain 1—9 without repetition.

To prove to Ada that he has solved a Sudoku puzzle, Ted creates a tamper-proof machine into which he puts the generated Sudoku answers, and the machine can send the proof to Ada.

The machine follows the following publicly verifiable protocol:
Firstly, the original Sudoku puzzle that has not yet been solved is entered into the machine with three puzzle cards facing up. For example, cell C3 has three face-up cards of number 9.
Next, Ted places his answers face down on the corresponding cell, again with three cards per cell.



Finally, Ada obtains a proof from the machine, which returns three categories of 27 bags to Ada:

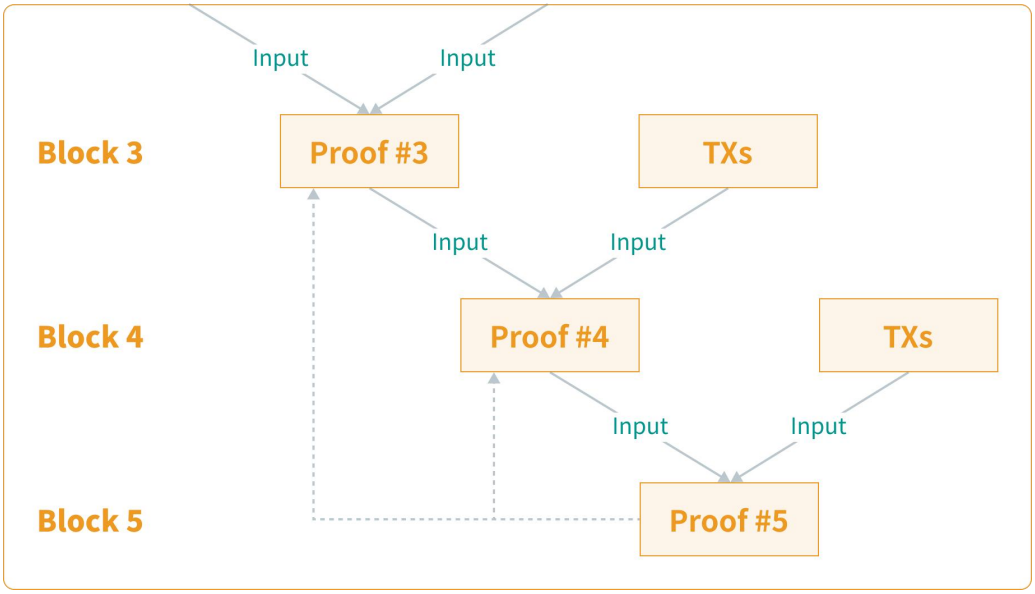
- Category I The machine takes out 9 cards from each row of the Sudoku, mixes them up separately and puts them into one bag, making a total of 9 rows and 9 bags.
- Category II The machine takes out 9 cards from each column of the Sudoku, mixes them up separately and puts them into one bag, making a total of 9 columns and 9 bags.
- Category III The machine takes out 9 cards from each thick-line palace (3*3) of the Sudoku, mixes them up separately and puts them into one bag, making a total of 9 thick-line palaces and 9 bags.

Ada then checks each of these 27 bags. If the cards in each bag contain the numbers 1 through 9 without missing or repeated numbers, then Ada can confirm that Ted has indeed solved the Sudoku. Besides, Ada does not gain any knowledge of the Sudoku solution from the proof returned by the machine, because the numbers in the bags returned by the machine were randomly scrambled.

5.2 Recursive Zero-Knowledge Proof

AUT supports a more efficient recursive Zero-Knowledge Proof generation: It takes the proof of the previous state and the current transaction as input, and then verifies whether the proof of the previous state and the current transaction are valid. If all the proofs are verified, the program outputs a new

state and a proof, as shown in the following diagram:

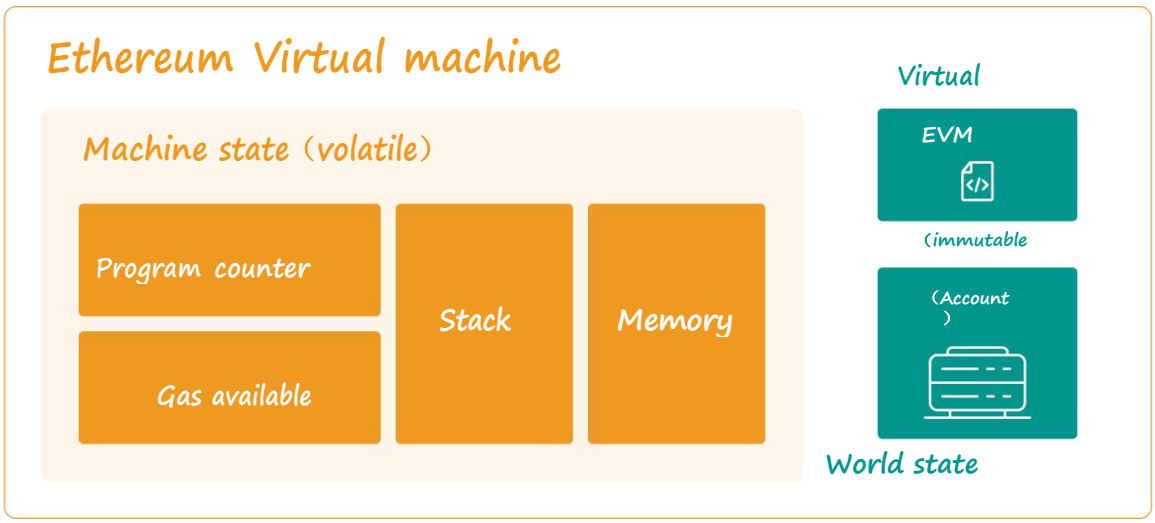


The state of the entire chain can be verified by simply verifying the proof of the previous state, i.e., recursive Zero-Knowledge Proof verification. For example, when Proof #5 is verified to be correct, it is equivalent to recursively verifying Proof #4 and Proof #3.

6. Compatibility with Ethereum's EVM

(Additional Features of the Main-Chain)

AUT is compatible with the Ethereum Virtual Machine (EVM) through eBridge, which enables more than 4,000 active Ethereum developers to quickly transplant DApps to the AUT public chain every month. EVM is a dominant standard for smart contract execution. EVM compatibility will significantly facilitate cross-chain liquidity and optimized migration of financial projects.



EVM operates like a stack machine that pushes a transient to and from the push-down stack, with a depth of 1024 items, each of which is a 256-bit word. It also maintains a temporary memory in the form of an array of bytes that changes between two transactions on the Ethereum blockchain. Compiled smart contract code is executed by the EVM as a collection of 140 standard opcodes, and other blockchain-specific stack operations are also implemented by EVM.

7. Atomic Swap Asset Cross-Chain

(Additional Features of the Main-Chain)

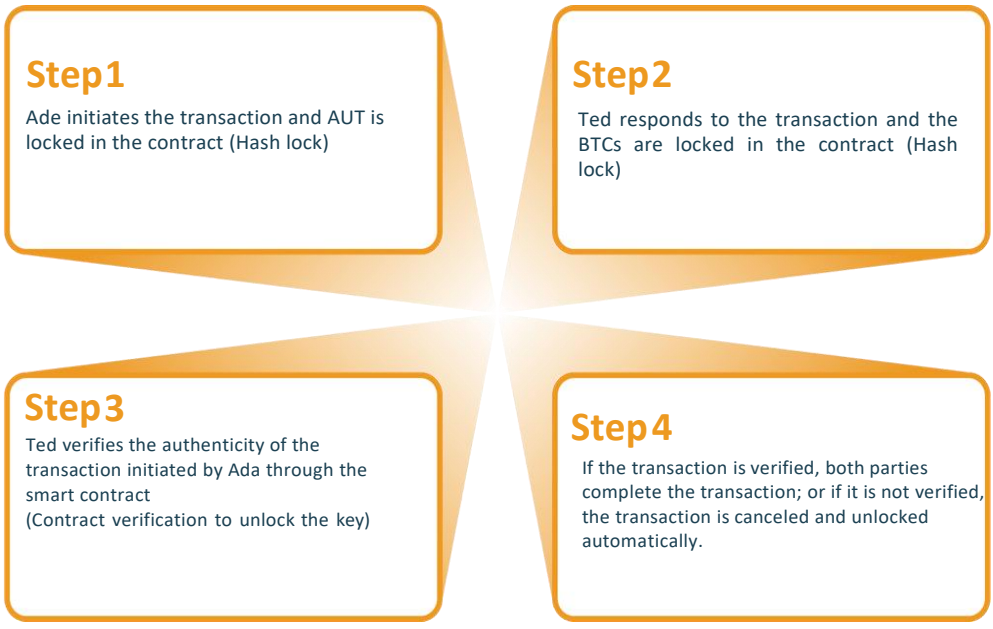
AUT supports digital asset interaction with other public chains through "atomic swaps", which is a peer-to-peer (P2P) transaction system using different blockchains to allow full release of asset liquidity and further enhance user experience.

7.1 How atomic swaps work

Atomic swap protocols are designed to prevent fraud between counterparties. To better understand how they work, let's assume that Ada wants to exchange her AUTs with Ted's Bitcoins (BTCs).

At first, Ada deposits her AUTs into a contract address, which is similar to a safe deposit box. With the security created in this way, Ada generates a key to access it. She then shares the encrypted hash of this key with Ted. Note that Ted does not have access to Ada's AUTs at this point, because he only has the hash of the key, not the key itself.

Next, Ted uses the hash provided by Ada to create another secure contract address to deposit his BTCs. If Ada wants to swap for BTCs, she needs to use the same key as that address, and at the same time, she needs to present the AUT key to Ted (with the help of a special feature of hashlock). This means that once Ada makes a request to swap for BTCs, Ted gets access to the AUTs of Ada at the same time, and the transaction process of that atomic swap is completed.



The term "atomic" represents the consistency of a transaction, i.e., it is either completely successful or completely unsuccessful. If either party abandons or fails to perform as expected a transaction, the contract is canceled, and the funds are automatically returned to their original owner.

Atomic swaps can be performed either on-chain or off-chain. On-chain atomic swaps take place in the online network of the blockchain for any cryptocurrency.

Off-chain atomic swaps, on the other hand, take place off-chain. This type of atomic swap is usually based on a two-way payment channel, similar to the channel payments used in Lightning Networks.

Technically, most decentralized transaction systems are done based on multiple signatures and Hash TimeLock Contract (HTLC).

7.2 Hash TimeLock Contract (HTLC)

Hash TimeLock Contract (HTLC) is one of the key components of atomic swaps. As the name implies, it is based on the two key functions of hashlock and timelock.

Hashlock freezes the funds if the associated key data (Ada's key in the above case) is not presented, and timelock ensures that smart contracts are executed only within a predefined time frame. Consequently, the use of an HTLC eliminates the need for centralization by creating specific rules, which prevent atomic swaps from being partially executed.

The biggest advantage of atomic swaps comes with decentralization. Atomic swaps eliminate the need for centralized swaps and any other type of intermediaries, as cross-chain swaps can be executed between two or more parties without them trusting each other. The level of security is also substantially improved as users are not required to make funds available to centralized exchanges or third parties. Transactions can be initiated directly through the user's personal wallets.

In addition, peer-to-peer transactions allow very low transaction fees and faster transactions. As a result, a higher level of interoperability is achieved.

8. Modularized Parallel Chain

(Additional Features of the Fin-Chain)

Fin-Chain will be the first in the industry to realize the function of modularized configuration for one-click chain issuance. A vast number of traditional financial enterprises can easily configure parallel chains that match the features of their own business clusters for more complex and large- scale financial services than conventional DApps. Meanwhile, they can develop their own parallel chain ecosystem, and reduce the development cost by tens or even hundreds of times.

<table>
<tr><th>Comparison items</th><th>Targeted developers</th><th>Rapid application development</th><th>L2 sub-chain development</th><th>New public chain development</th></tr>
<tr><td>Other public chain eco-developers</td><td>Coin circle</td><td>DApp</td><td rowspan="2">Higher technical and time costs required
On a 1-3-year basis</td><td rowspan="2">Massive technical and time costs required
On a 3-6-year basis</td></tr>
<tr><td>Main-Chain Eco-developers</td><td>Coin circle</td><td>DApp</td></tr>
<tr><td>Fin-Chain Eco-developers</td><td>Finance circle
Internet circle
Coin circle</td><td>Parallel chains
DApp</td><td colspan="2">Modularized configuration of parallel chains
Hundred times lower technical and time costs On a weekly or even daily basis</td></tr>
</table>

Fin-Chain has a highly modularized and configurable architecture (infinitely scalable parallel channels) and offers versatile innovation and optimization for industry cases such as banking, finance, insurance, healthcare, metaverse, HR, supply chain, and even digital music delivery. The CAs, databases, and consensus algorithms in the Fin-Chain are pluggable, and the chain code is implemented via Docker.

Through the unique parallel chain architecture, it solves the problem that blockchain cannot meet scalability, security and decentralization requirements at the same time. The system provides a complete set of solutions to help business users who want a public chain of their own to build an exclusive application chain.

In the future, developers can deploy an application chain in a few minutes by simply entering such parameters as the number of application chain nodes, margin, and consensus mechanism required for an application chain from their cell phones. Afterwards, they can monitor the blocks generated and the operation status of the new chain by registering the contract address, port and other information of the application chain on the block browser.

Optional consensus modules supported by parallel chains are PBFT, APoS, PoS, and PoW.

Typical configurations of parallel chains:

Created with configin.yaml file and configingentool. Usage of
configingen: -chainCreateTxBaseProfile string
Config file specifying the underlying transaction, needs to be used along with 'outputCreateChainTx' -chainID string
Chain name (cannot be repeated) -configPath string Config
file path –inspectBlock string

Block storage path -inspectChainCreateTx string

Blockchain transaction storage path -outputCreateChainTx string -outputCreateChainTx string Path written when the blockchain creates configin -version

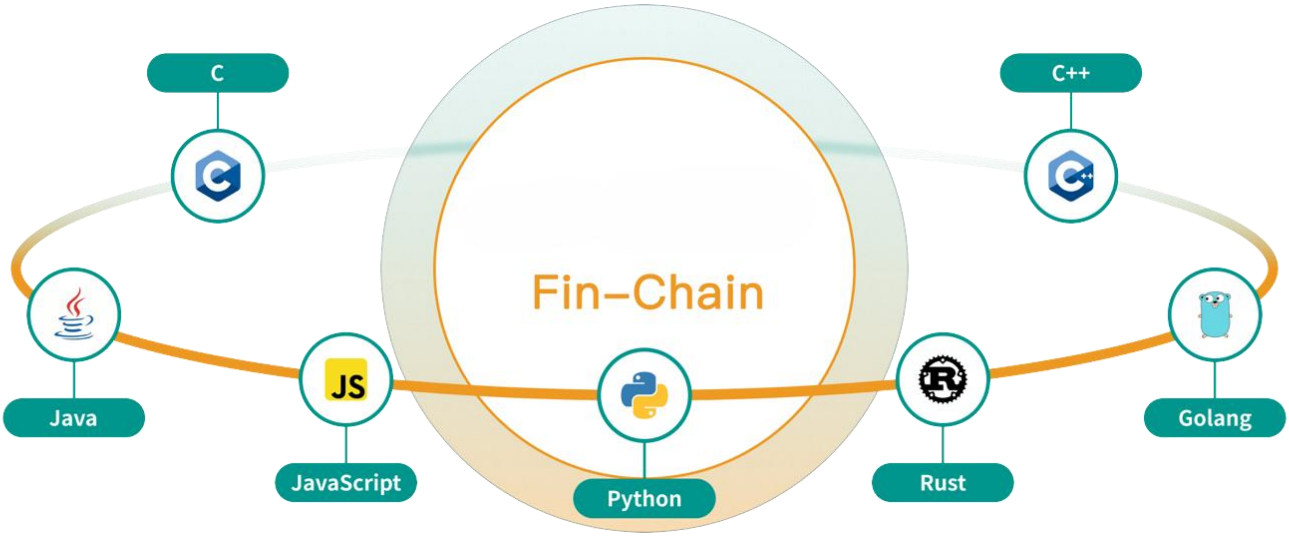
Version information

9. Common Programming Contract Development

(Additional Features of the Fin-Chain)

Fin-Chain's parallel-chain virtual machine (FVM) is Turing-complete, so it can run any program written in any programming language. This allows non-blockchain developers to easily create custom smart contracts and DApp for the emerging Web 3.0 industry. FVM supports smart contracts created in major programming languages such as Java/Go/C++/JS.

Thanks to that, enterprises can cut down the costs of technical personnel such as Soldity/Rust, and non-blockchain enterprises can also develop decentralized applications at low cost. Together with the modularized parallel chain service, traditional enterprises can lower the cost of getting on the chain to the lowest threshold.



10. AUT Governance and Incentives

AUT is the native token of AUTHERIUM, which is governed and incentivized based on AUT tokens.

10.1 AUT Insurance and Establishment

AUTHERIUM (AUT) has a total issue volume of 1 Billion.

10.2 AUT Token Allocation Strategy

IDO: 25%, all produced by market IDO, not locked, and all released before going online.

Technology: 15%, locked for 5 years, and then released 1% each year until all released.

Operation: 15%, reviewed by the foundation, issued irregularly, and the specific release ratio will be announced in the community.

Foundation: 19%, locked for 2 years, and then released 1% every quarter. This part of the tokens is mainly used for public relations, community building, marketing promotion, and rewards for users and institutions who have made outstanding contributions to the platform.

Airdrop: 10%, conditional airdrops for active users or users who meet specific conditions to encourage community participation and ecological construction.

Mining: 16%, produced through user data mining, encourage users to actively participate in ecological activities and contribute value.

11. AUT Financial Infrastructure

AUT is a financial public chain which comes with basic services and infrastructure supporting the modern financial system and future-oriented finance. These infrastructures are built on top of AUT's core technology and are offered as protocol and service layers for use by the AUT ecosystem.

11.1 FinSwap Cross-chain asset trading

The crypto industry has entered the cross-chain era. With the proliferation of public chains and aggregation layers in the Web 3.0 world, many applications are built on different isolated ecosystems. While some of these applications are deployed on multiple blockchains on trial, their liquidity is inevitably fragmented. Once cross-chain transactions are involved, users will have to transfer their assets via CEX or clumsy cross-chain bridges, with complicated operations, high Gas fees, low privacy, and even more opportunities for hackers due to overly lengthy processes.

As a public chain specializing in crypto financial services, AUT, based on its own dual-chain lightning interaction architecture and atomic swap service, will launch a demonstration-level innovative application – FinSwap, a cross-chain swap, to address the industry challenge of decentralized cross-chain liquidity.

FinSwap is a combinable all-chain liquidity aggregation protocol where asset cross-chain and swap processes are fast and split-second to users. Moreover, the contracts for processing transactions are executed on Fin-Chain with TPS up to 80,000+, enabling users to enjoy a transaction experience close to CEX, which is unimaginable in traditional swaps.
Notably, FinSwap aggregates liquidity from all blockchains using the ALLIM messaging cross- chain framework while allowing other DApps to access the depth to help them capture liquidity from different blockchains. As a result, users can benefit from the deepest liquidity, achieving optimal exchange rates and minimal slippage swaps with the least cost.

On a market-making algorithm basis, FinSwap will be the only cross-chain swap where LPs can finely control the price range of their capital allocation using the third-generation AMM automatic market maker mechanism, thereby further improving capital efficiency and reducing slippage while preventing any asset flash drops.

Economist Robin Hanson first referred to the AMM algorithm in 2002 in his research on digital market scoring rules. In 2016, Uniswap introduced automatic market makers to the crypto space in an efficient way when they proposed the Constant Product Market Maker (CPMM) model to ensure constant token trading in Ethereum with liquidity, with the following formula:

$$(Rx - \Delta x)(Ry + (1 - f)\Delta y) = k$$

where Rx and Ry are the reserves of each type of token, f is the transaction fee, and k is a constant. The simplified formula is as follows:

$$x * y = k$$

where x is Token1, y is Token 2, and k is a constant.
In essence, AMM combines two assets that are being traded into a liquidity pool, aiming to ensure that the asset size of the liquidity pool remains constant regardless of the size of the transaction.

A paradigm shifts of AMM, the CPMM model is a decentralized mechanism that removes the middleman completely while enabling a combination of liquidity, fast trading, and on-chain mechanisms to quote at the right price. However, it also suffers from obvious flaws such as slippage, impermanent losses, and security risks.

Around 2020, a new generation of AMMs began to grow rapidly, and the CPMM model gradually merged with the CSMM model to create the hybrid CPMM. This formula makes exponentially dense liquidity. Most of this curve belongs to the linear exchange rate:

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

where x is the reserve of each asset, n is the quantity of the asset, D is the invariant (the total value in reserve), and A is the amplification factor (similar to "leverage",” which represents the degree of curve curvature).

Next, FinSwap will bring the swap algorithm to a higher level with more sophisticated solutions. We will introduce centralized liquidity, multiple fee tiers based on the second-generation AMM, and access to an active market-making mechanism and a Pyth prediction machine. The second- generation AMM will eliminate the dependence of the liquidity pool on arbitrageurs to keep prices accurate and significantly reduce the risk of unpredictable losses.

In the future, FinSwap will allow liquidity to be priced into fixed positions, taking centralized liquidity a step further and allowing DEX to operate close to the smooth experience of CEX.

11.2 Decentralized proof of credit

Credit lies at the core of the financial industry, and the establishment and expansion of credit require a reliable mechanism to ensure its authenticity and credibility. As a financial public chain, AUT public chain provides a basic design for decentralized credit expansion in the financial industry through blockchain technology, smart contracts and other technical means, realizing highly secured and credible sharing management of credit information, thus providing customers with more high-quality, efficient and convenient financial services.

The credit information of off-chain customers can be put on the AUTHERIUM through Zero-Knowledge Proof in the following steps:

1) An off-chain customer requests the credit institution to generate the proof of credit: The customer provides the credit institution with data such as his personal information and credit history and requests the credit institution to generate the corresponding proof of credit.

2) The credit institution generates the proof of credit: The credit institution signs the data provided by the customer with its own private key and generates a digital certificate as an identification of the customer's proof of credit. Meanwhile, the credit institution uploads the digital certificate to the chain and stores it in the specified smart contract.

3) The customer generates a Zero-Knowledge Proof: The customer uses the Zero-Knowledge Proof technology to generate a Zero-Knowledge Proof based on his personal information and credit history. The proof does not contain any specific personal information, but only the proof of a corresponding digital certificate owned by the customer.

4) The customer uploads the Zero-Knowledge Proof: The customer uploads the Zero-Knowledge Proof generated by himself to the chain with his own digital certificate identification.

5) The on-chain smart contract verifies the proof: Upon receiving the digital certificate and Zero-Knowledge Proof from customers, the on-chain smart contract first verifies the validity of the digital certificate then checks the customer's credit information through the Zero- Knowledge Proof, and finally confirms whether the customer's proof of credit is valid.

AUT decentralized proof of credit verifies a customer's credit using the interactive Zero- Knowledge Proof method in AUTHERIUM, which is accomplished by the following process:

- The customer stores his credit information in a local device and encrypts the information to generate an encrypted hash.
- The customer generates a set of random numbers and encrypts them with an encryption algorithm to generate an encrypted random number.
- The customer generates a non-interactive Zero-Knowledge Proof using the encrypted random number and the encrypted hash of the credit information.
- The customer sends the Zero-Knowledge Proof to AUTHERIUM's smart contract, which verifies the correctness of the proof and stores the encrypted hash on the chain if the verification is successful.

In the above scheme, the non-interactive Zero-Knowledge process:
Assuming that the customer wants to prove that he knows the hash H of his credit information without revealing the information itself, the proof process is as follows:

- The customer generates a set of random numbers r and encrypts it with an encryption algorithm to generate an encrypted random number R.
- The customer generates two values: s1 = H ^ r and s2 = r, where ^ denotes the XOR operation.
- The customer proves s1 and s2 using a Zero-Knowledge Proof system, without revealing the values of H and r in the proof process.
- The customer sends the proof result to the chain and the contract verifies the correctness of the proof and stores H on the chain if the verification is successful.

In the above scheme, the customer uses the Zero-Knowledge Proof system to prove that he knows the values of H and r, while not revealing the specific values of H and r. This ensures that the customer's privacy is not compromised and proves that the customer does know the hash of the credit information.

All the above credit institutions must be nodes of AUTHERIUM and satisfy the following conditions:

1) Node reward mechanism: Each time a node successfully generates a proof of credit and uploads it to the chain, the node can receive a certain amount of AUTs as a reward. The number of rewards can be dynamically adjusted according to the credit rating of the node and the complexity of the proof of credit to secure a reasonable reward for the node's motivation and contribution.
2) Punishment mechanism: If the proof of credit generated by a node is found to be falsified, the node will be punished accordingly. Specifically, if a node is found to be falsified, it will lose all the rewards obtained previously, and a certain credit rating score will be deducted. At the same time, the node will also be removed from the node list and will no longer be allowed to generate proofs of credit.
3) Credit rating mechanism: The credit rating of a node can be calculated by various factors, including but not limited to the number of proofs of credit generated by the node, and its authenticity and complexity. The rating results serve as a reference for node reward and punishment mechanisms to better adjust the behavior of nodes.

The node reward and punishment mechanisms enable credit institutions, as nodes, to guarantee the authenticity and trustworthiness of proofs of credit and improve the trust and efficiency of the whole system by constantly optimizing and adjusting the behavior of nodes through the credit rating mechanism.

11.3 Financial soul-bound tokens (FinSBTs)

SBTs are non-transferable NFTs that describe a user's origin, education, salary, spending level, credit status, etc. in a decentralized network. In short, it is "proof of who you are, what you have done, what you have accomplished, your network of connections," and so on.

SBTs can be divided into many categories. One can have multiple SBTs in the blockchain world. One of the key functions of AUT is to build financial SBTs for each AUT account, i.e., FinSBTs. This function enables users to map their full financial identity in reality in the blockchain network and establish a financial identity system for the users.

That means FinSBTs are carried natively by AUT addresses and are the underlying infrastructure of the entire AUTHERIUM.

The detailed scheme of AUTHERIUM to build SBTs is as follows:

1) Defining the content of FinSBTs: FinSBTs contain users' basic personal information, education, occupation, income, financial status, credit rating, etc. All the information needs to be collected and verified through user authorization and institutional verification.
2) Determining the standards of SBTs: Based on the content of FinSBTs, we develop standards including data formats, storage methods, and encryption algorithms.

3) Developing smart contracts: According to the standards of SBTs, we develop smart contracts to enable FinSBTs information authorization by user's and verification by institutions, as well as the storage and update of FinSBTs information.
4) Collaborating with credit institutions and nodes: AUTHERIUM needs to collaborate with credit institutions to obtain their data on users' credit ratings and add them to FinSBTs.
5) Implementing privacy protection: Since FinSBTs contain sensitive information of users, privacy protection needs to be implemented. Technologies such as Zero-Knowledge Proof are used to prevent users' data from being leaked.
6) Issuing SBTs: According to the content of FinSBTs, corresponding SBTs are issued. Each user can have multiple SBTs, including financial identity, credit rating, etc.
7) Using SBTs: Users can use SBTs for financial activities such as trading, lending, and investment on AUTHERIUM. In these activities, the users' FinSBT information can be used as the basis for credit rating and identity verification to improve the security and efficiency of transactions.
8) Updating SBTs: Users can update their FinSBT information such as career change, income increase, etc. at any time. After the update, the corresponding SBTs will be updated accordingly.

With the above schemes, AUTHERIUM can build a complete financial identity system to improve the efficiency and security of financial activities. Meanwhile, SBTs can embody users' financial identity and help them obtain more financial services and opportunities.

11.4 Native stablecoins (FinUSDs)

AUT issues a type of native stablecoin, which we call FinUSD, or FUSD for short. AUT manages, issues, and destroys FUSDs and maintains the operation of FUSDs through a set of smart contracts.

The issuance of FUSDs must be backed by sufficient collateral, and its specific minting and issuance process is as follows:

1) Users obtain the corresponding FUSDs by pledging mainstream digital currencies such as AUTs and BTCs on AUTHERIUM.
2) For FUSDs to be earned, the collateral needs to reach a certain value. The percentage is controlled by AUTHERIUM's pledge rate combined with the credit rating of the user's SBTs.
3) When the users pay off their FUSD loan, they can get their collateral back.
4) The fluctuations in the price of the collateral may result in loan risks. If the value of the collateral drops to a certain level, the system will force the closing of the position and sell the collateral to cover the borrowing.
5) To ensure that the value of the collateral is sufficient to cover FUSD issuance, AUTHERIUM regularly audits the value of the collateral and makes necessary adjustments based on market fluctuations.

Users can get the following proceeds after pledging minted stablecoins:

1) Investment proceeds: The platform uses the collateral of stablecoins for investment, such as buying

bonds, stocks, digital assets, etc., and receives proceeds from the investment. Part of the proceeds can be distributed to the stablecoin holders.

2) Loan proceeds: The platform can issue loans with stablecoin collateral and collect interest from the borrower. Part of the interest can be used as proceeds for stablecoin holders.

3) Stablecoin transaction fee proceeds: The platform can charge a commission for stablecoin transactions and allocate a portion of the commission as proceeds for stablecoin holders.

4) FinPAY payment proceeds: FinPAY settles payment settlements between traditional banking systems and uses a portion of the fees as proceeds for stablecoin holders.

5) Collateral price fluctuation proceeds: Since the collateral of stablecoins contains a certain percentage of cryptocurrency, fluctuations in collateral prices may have an impact on the proceeds of stablecoins. If the collateral price rises, the platform may sell a portion of the collateral for proceeds and distribute a portion of the proceeds to stablecoin holders. On the contrary, if the collateral price falls, the platform may need to inject additional collateral to maintain the value of stablecoins. However, this may also result in additional collateral proceeds for stablecoin holders.

In a nutshell, the return of AUT FUSDs is expected to be between an annualized rate of 20% and 300%.

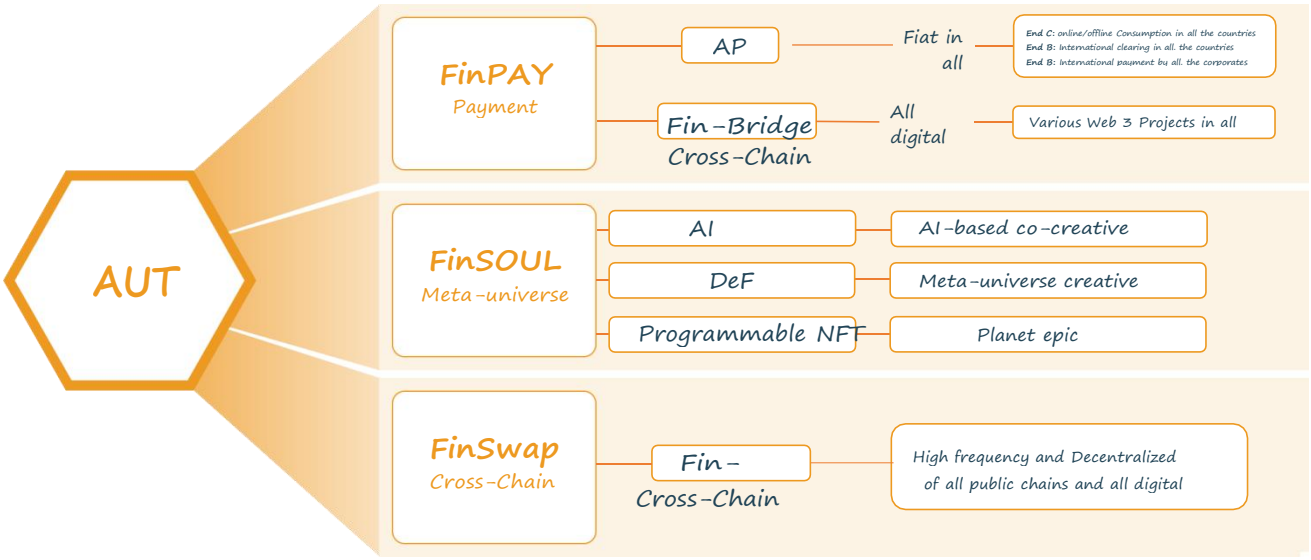
12. AUT Ecological Applications

As an epoch-making financial public chain, AUT not only builds a solid dual-chain underlying consensus but also develops an advanced demonstration platform at the application layer, including five modules: Super Payment Gateway, Cross-chain Swap, AIGameFi, Defi, and NFT, of which the latter three are integrated into In the FinSOUL platform.

12.1 FinPAY payment app

FinPAY is a AUT-based decentralized cross-domain and cross-chain payment gateway. At this stage, it is mainly used for payment and settlement between the banking systems in collaboration with AUT.

It can be regarded as a super-integrated protocol of SWIFT+PALPAY+VISA. We have reached a preliminary cooperative partnership with Wall Street's Wells Fargo, HSBC, Citigroup, Goldman Sachs, and other multinational banks. FinPay can realize low-cost and efficient transfers between fiat currencies of various countries and public chain assets via a safe and anonymous process.



Its application scenarios are revolutionary, such as:

1) Euros can be quickly converted into Ax tokens on Project A of the POLYGON public chain in 3 seconds.
2) The Bx tokens on the Ethereum public chain B project can be quickly converted into Indian liras or Russian rubles.
3) A large sum of Japanese yen from a Japanese bank/enterprise can be quickly converted into equivalent U.S. dollars or fiat currencies of other countries.
4) The governance tokens of the X public chain Y project can be used to purchase goods and consumer services in stores, convenience stores, or online shopping malls in various countries.
5) All kinds of Defi projects on each public chain can receive any fiat currency and Token supported by FINPAY to conduct business.

Let's take SWIFT as a comparative analysis. SWIFT (Society for Worldwide Interbank Financial Telecommunications) was established in 1973 as a global interbank international partnership organization. It is a global interbank international cooperation organization whose function is to transmit financial information such as international clearing and payment among organization members.

Although SWIFT has made progress regarding fee standards and fund transfer speed, it is still non-free-of-charge, not real-time and digital currency non-transferable. These are precisely the problems that FinPAY solves:

1) Low Cost of Operation of the System

FinPAY is a decentralized architecture with the core concepts of "consensus," "sharing," "trustless," and "free." SWIFT is a centralized organization with extremely high maintenance costs. For example, salaries in the system, server clusters, and other equipment costs, trust communication costs, resulting in its cross-currency, cross-border, cross-regional operating expenses, and fee standards have always remained high. However, any currency in the FinPAY system can be freely converted at close to zero cost, and there is no difference between different places, cross-banks, and cross-border payments.

2) Lightening Transfer Speed

The transfer under the FinPAY system is as swift as sending an email in about 3 seconds, while the SWIFT international remittance takes one to two days, a difference of thousands of times. The FinPAY system is a phenomenal innovation for the financial industry where every second counts.

3) Any Currency Flow

FinPAY is a super gateway for any conversion between digital and fiat currencies, while SWIFT only applies to national fiat currencies of various countries. As long as an exchange rate is available, any currency can be freely exchanged in the FinPAY system.

4) Support Anonymous Transactions

FinPAY offers an option for anonymous transactions, while SWIFT transactions must reveal the identities of both parties. Optional anonymity is very important for WEB3.0 finance.

5) Free Access to API

The crypto industry projects, traditional banks, Internet companies or even an offline entity or individual organization can all freely access FinPAY's API in compliance with the system's rules to enable the all-inclusive gateway service without any strict entry thresholds and lengthy vetting processes. At the same time, the API will also implement security defense and appropriate punishment for any malicious behavior based on smart contracts. It can identify malicious merchants and isolate them accordingly to the black sandbox to ensure the integrative operation of the system.

In addition, FinPAY also has application advantages over Ripple, which is the aging open payment network, in several ways:

Items to compare	Ripple	FinPAY	Illustration of the Comparison
TPS	1500+	7500+（Main-Chain） 80000+（Fin-Chain）	The super scale of 5 to 53 times Concurrency performance gap
single simultaneous transaction	5s-10s	<3s	A block synchronization time of less than 1 second can be well applied to various payment scenarios and FinPAY have a more comprehensive range of business applications
business focus	International banks clearing	International banks clearing All international transaction Fiat payment in a small amount Digital currency in a small amount payment	
Cross-chain transactions	Interledger Protocol agreement, in general	Lightning Dog Chain Lightning Parallel Cross-chain Atomic swaps	FinPAY executes cross-chain transactions more effectively
Degree of decentralization and Branding credibility	The total issuance of XRP is 1 trillion pieces The founding team owns more than 200 million. Selling and cashing out are extremely serious	Open, fair, scientific consensus output mechanism	In Oct. 2020, SEC filed a lawsuit against Ripple till now

From the near collapse of the price of XRP on the Ripple network, we recognized that technology is the foundation of innovation. Still, a fair system and the heart of not doing evil are the pillars for the long-term development of the platform.

We can foresee that FinPAY will become the ultimate solution for cross-border and cross-chain payments and the necessary infrastructure for human beings to move toward future financial civilization.

12.2 Cross-chain financial bills trading marketplace (FinBills)

Bills are marketable securities used for payment purposes. The traditional bank bill business is at the heart of the modern financial system. In fact, in many countries, cash bills themselves can be regarded as promissory bills accepted across banks.

The traditional financial bill business is divided into the following categories:

Types	Description	Difference
Bill of exchange	An instrument issued by the drawer, who entrusts the payer to pay a definite amount to the payee or bearer unconditionally at sight or on a specified date.	**Different people who see the bills**
Promissory note	An instrument issued by the drawer who promises to unconditionally pay a definite amount to the payee or bearer at sight.	
Cheque	An instrument issued by the drawer, who entrusts the bank for check deposit to unconditionally pay a definite amount to the payee or bearer at sight.	

According to different issuing units, Bill of exchange can be divided into two categories: Bank draft and

commercial draft：

Types	Description	Difference
Bank draft	An instrument issued by the issuing bank, which is unconditionally paid to the payee or bearer at sight in accordance with the actual settlement amount.	Different issuers
Commercial draft	An instrument issued by the drawer, who entrusts the payer to unconditionally pay a definite amount to the payee or bearer on a specified date.	

FinBills, as the basic ecosystem of AUT public chain, will implement the above three financial bill businesses in a decentralized way with the concept of WEB3.0.

FinBills will provide customers with the following services:

1) Issuing financial instrument NFTs: Financial institutions can issue various types of financial instrument NFTs on AUT, such as commercial drafts, trade finance notes, etc. Each financial instrument NFT has a unique identifier to ensure that it cannot be copied or tampered with.
2) Trading financial instrument NFTs: Financial institutions can put the issued financial instrument NFTs into the market for trading. Users holding financial instrument NFTs can buy, sell and pledge them through the trading market for proceeds.
3) Providing liquidity support: AUT can support the trading of financial instrument NFTs by providing a liquidity pool. Users can pledge digital currencies such as AUTs, BTCs and ETHs into the liquidity pool in exchange for the corresponding liquidity tokens. These liquidity tokens can be used to trade financial instrument NFTs, while the corresponding digital currencies can be redeemed at any time.
4) Enabling decentralization: AUT's financial bills marketplace adopts a decentralized design, i.e., financial institutions transact directly with users without the involvement of intermediaries. This decentralized model can reduce transaction costs and increase the transparency and security of transactions simultaneously.
5) Providing credit assessment service: AUT can provide credit assessment service for users by using their data on the platform in combination with the FinSBTs infrastructure. It helps help financial institutions better understand the credit status of borrowers and reduce the risk of default.
6) Providing data query service: AUT can provide query service to help financial institutions query users' credit data, borrowing records and other information to aid decision-making. Meanwhile, users can also query their own data to protect their rights and interests.

12.3 Derivatives exchange (FinEX)

FinEX is the decentralized derivatives exchange of AUT. FinEX will provide a wide range of derivatives for trading, including futures, options, CFDs, etc. Users' digital assets will be stored in smart contracts to ensure security and transparency. Users can connect to FinEX through their wallets and trade with their digital assets.

FinEX has the following features:

1) Margin trading: Users are required to deposit margin prior to trading to ensure smooth transactions. The margin can be in digital currency or stablecoins, but the system recommends FUSDs. FinEX will offer a variety of margin ratios for users to choose from in order to meet different risk appetites.
2) Transaction match-making: FinEX will utilize a decentralized match-making mechanism to ensure fair, transparent and efficient transactions. Transaction data will be stored on the blockchain to ensure its tamper-evident nature.
3) Fee structure: The fee structure of FinEX will include transaction fees, platform usage fees， and withdrawal fees. The exact rates will be based on the type and volume of transactions and will be disclosed on the platform.
4) Risk management: FinEX will implement comprehensive risk management measures, including limiting the maximum transaction amount for users and monitoring transaction risks in real- time. At the same time, FinEX will provide risk insurance to ensure that users' digital assets are protected.
5) User support: FinEX will provide 24/7 user support services to help users solve any problems during trading. Meanwhile, FinEX will provide trading education and technical support to help users better understand and use the platform.

FinEX adopts a hybrid transaction match-making mechanism that ensures both decentralization and efficiency.

First of all, FinEX takes advantage of decentralized trading, where all transactions are executed on the chain and users' assets are controlled by themselves with no centralized institutions involved, thus ensuring security and trustworthiness.

At the same time, to improve transaction efficiency, FinEX also introduces a centralized liquidity and multi-fee level transaction match-making mechanism based on the hybrid CPMM, which can match counterparties faster and deliver high liquidity and low transaction fees. This hybrid mechanism ensures both decentralization and efficiency of trading.

In addition, FinEX employs a number of other technological means to further improve the efficiency and user experience of trading. For example, the Lightning Network is introduced for faster trade confirmation and lower transaction fees.

12.4 WEB3.0 social platform (FinBox)

FinBox is a decentralized instant messaging and content social platform. It is the first WEB3.0 social platform supported by AUT public chain. FinBox can connect wallets, import and create new wallet IDs and AUT SBTs in one click in the app, and join FinBox's social network.

Instant messaging: Users can log in with their wallet ID and chat with and send messages to other users.
Social function: Users can create profiles, post statuses and pictures, and follow other users.
Wallet connectivity: Users can connect their digital wallets in order to make transactions and transfers on the platform.
AUT NFTs support: FinBox will support NFTs on the AUT public chain and allow users to buy, trade and

display their NFTs.

FinBox enables WEB3.0 decentralized networking through the following technologies:

1) Blockchain technology: Uses the AUT public chain to support FinBox's cryptocurrency trading and NFT functionality.

2) IPFS: Uses IPFS as a protocol for file storage and transfer to ensure the security and reliability of data in a distributed network.

3) Encryption technology: Uses encryption technology to secure user chat, transactions and data storage.

12.5 FinSOUL Next Generation GameFi

FinSOUL is a titanic innovative masterpiece that combines co-creative AIGameFi, programmable NFT, and Metaverse DeFi. It currently has no direct benchmarking products and can be understood as a pioneer project of Metaverse 2.0.

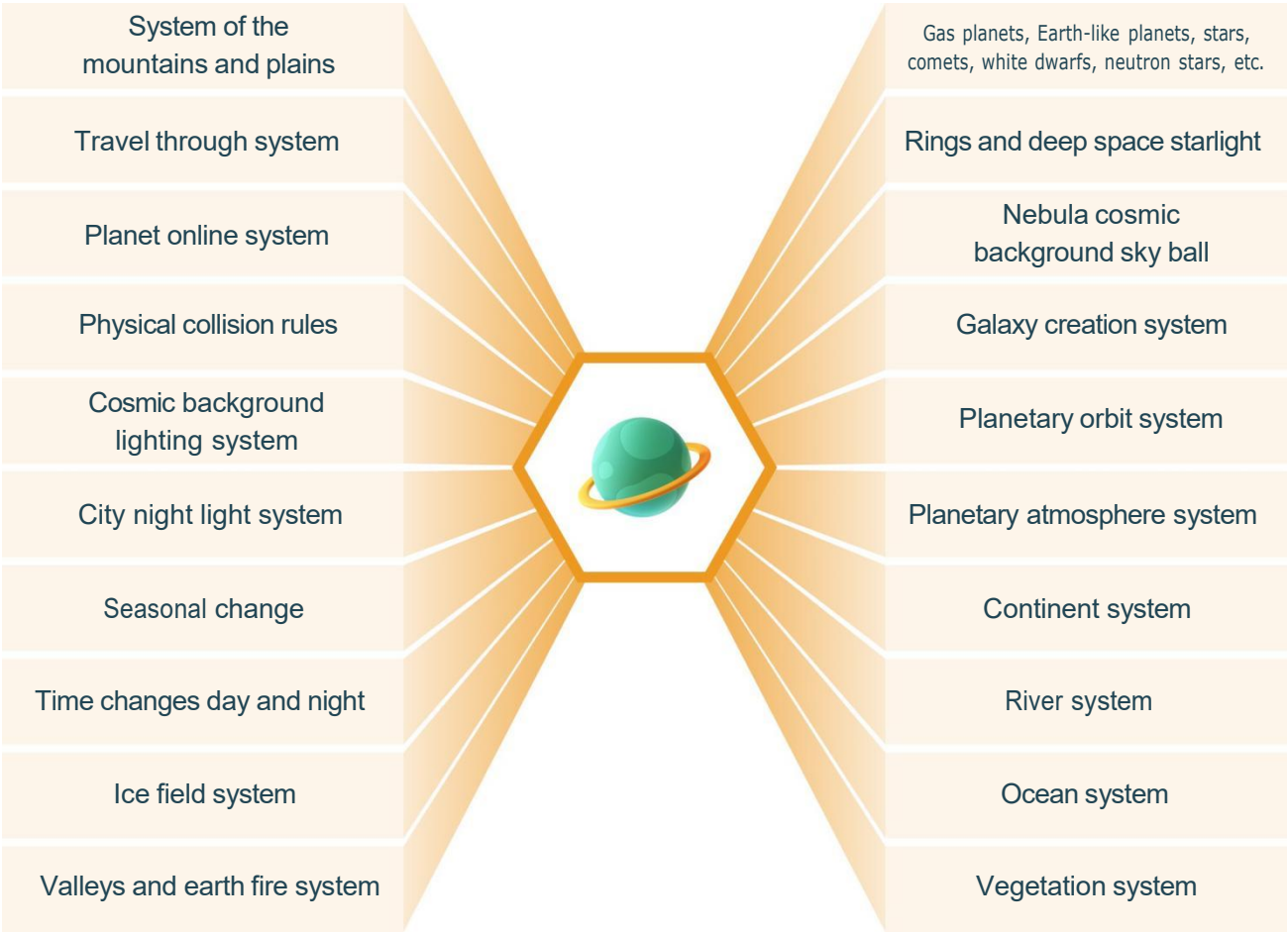
2021 is called the first year of the metaverse, but in the view of the AUT team, the previous projects were more hype and market value operations because the concept was ahead of the technology. The core of most projects is still only traditional games, and some chain reform projects are nothing more than a layer of WEB3.0 gimmicks, which are far from the ideal Metaverse.

The AUT team will develop the soulful, attractive, valuable Metaverse 2.0 world FinSOUL based on the double-chain gene.

FinSOUL is based on a programmable NFT planet with access to the ChatGPT core. Each player can create a unique AI partner in it, experience the magnificent interstellar adventure with more players, and harvest decadent SOUL tokens during the adventure.

FinSOUL is developed based on Unreal Engine5, where each player first mints his AI partner and NFT planet through governance tokens and then enters the metaverse market to play various free or paid game copies and purchase various game NFT assets.

Users can finely customize hundreds of parameters such as gender, appearance, makeup, body shape, attire, skills, etc., of partners according to their own preferences and match the personality and behavior of partners in the ChatGPT-NPC awareness library that has undergone targeted training, and then discuss with partners to create a player's NFT planet, the range that can be formulated includes but is not limited to:



FinSOUL will open up the gameplay editor and API to the industry, allowing creative teams worldwide to develop various sandbox world gameplay and replicas of the grand FinSOUL universe, competition not limited to multiplayer only, travel experience, socialization, MMORPG, gun battle, air combat, action-adventure, interstellar trade, interstellar colonization, city building, simulation management, quiz game...

This is a metaverse with actual lasting vitality. One day, FinSOUL may become our second life.

13. Summary of Differentiated Core Competencies

13.1 Analysis of Technical Competence

	Bitcoin	Ethereum	BSC	AUTHERIUM	AVAX	Solana	Polkadot
Two Chains Structure	No	No	No	Yes	No	No	No
Modular Parallel Chain	No	No	No	Yes	No	No	No
Flash Parallel Cross-Chain	No	No	No	Yes	No	No	No
Scalability	Low	Low	High	High	High	High	Medium
Decentralization	High	High	High	High	Medium	Medium	High
Security	High	High	Medium	High	Medium	Medium	High
Realistic TPS	7	18	100	Main-Chain 7500 Flexibility of Fin-Chain Without Limit	4500	2900	400
Transaction Confirmation Time	30-60min	5min	75sec	3sec	3sec	1sec	30sec
Average Gas Fee	$12	$3	$0.01	$0.0001	$0.001	$0.0001	$0.15
Contract Development Languages	/	Solidity	Truffle Solc	JAVA/GO/Solidity Etc	Solidity GO	Rust	Rust
Type	Layer1	Layer1	Layer1	Layer1	Layer1	Layer1	Sharding
Energy Efficiency	No	No	Yes	Yes	Yes	Yes	Yes

13.2 Financial forecasts

AUTHERIUM generates revenue from the following sources:

1） AUTs earned from super node mining

2） Profits from Gas fees consumed by on-chain transactions 3）

Interest from the collateralized issuance of FUSDs 4）

Commissions from FinEX transaction matchmaking 5）

Advertising revenue from FinBox social platform

Concurrently, the following costs and expenses are incurred:

1） Node operating cost 2）
Marketing and operational cost 3）
Risk reserve fund cost
4）Cost of developing and maintaining public chain technologies

The number of AUT public chain users is currently in the tens of millions and is expected to eventually hit the hundreds of millions.

AUT public chain's share of the cryptocurrency market will go from zero to billions of dollars, and is expected to eventually hit tens of billions of dollars.

Assuming a market volume of one-tenth of ETH, a profit margin of 30%, and a PE of 30x, the following financial forecast table is presented:

Year	Revenue (USD million)	Profit (USD million)	Growth rate	Total market capitalization (USD billion)
2024	300	90	300%	9
2025	900	270	300%	27
2026	2700	810	300%	81

We expect AUTHERIUM's total market capitalization to hit USD81 billion in 2026.

14. Development Roadmap

January 2020 Founding meeting of the core team.

February 2020 Co-founded in 2019 by Bob Lambert and William Thompson, both Stanford graduates, together with their close friends including Bruce.

January 2022 The brand new HyBriid security technology was developed.

December 2022 A breakthrough in HyBriid technology resulted in the AUT team winning the DeFi Technology Contribution of the Year award at the Pan American Blockchain Summit.

March 2023 Being match-made by Jorge, vice president of Morgan Stanley, the two companies completed the contracting process and were ready to form a new company. The AUT team made a name for itself and gained a lot of attention from the market.

April 2023 Funded by JPMorgan and with technology provided by DF, Morgan DF AUT was officially incorporated.

May-June 2023 AUT publicly solicited major financial companies and institutions worldwide to serve as regulatory nodes, including 100 platforms such as Washington's Coin Center, California's BitGive, Australia's Cryptos, and Singapore's LinkCove, to jointly safeguard user funds and bring the risk factor infinitely close to zero.

June-July 2023 AUT held a special subscription partner event, in which 100 partner subscribers were invited to witness AUT's prosperity.

July 2023 AUT was officially launched.

August 2023 Financial coupons worth USD1 million were distributed to AUT's global communities to benefit more users around the world.

September 2023 AUT gradually established a global community service center and held meetings and market launch conferences for communities in various countries.

October 2023 AUT set up a special foundation to cultivate technical talents in blockchain- related sectors and held a hackathon to reward teams that help optimize AUT's security and R&D innovation security technologies.

November 2023 AUT traveled around the world for roadshows and launch events, including Silicon Valley, London, Toronto, and key cities in Asia Pacific such as Singapore, Kuala Lumpur, Tokyo, Seoul, Hong Kong, and Macau.

December 2023 HyBriid 2.0 smart contract protocol was upgraded to support lending in most

mainstream coins and borrowing with up to 5x leverage to increase capital utilization.

January 2024 To gather a large amount of user data for ongoing improvement of the performance of the financial public chain and to give back to participants, AUT offered community users a chance to participate in a six-month internal test of the public chain. That allowed users not only to experience the features and convenience of the AUT financial public chain ahead of others, but also to gain a firm foothold in the future crypto world and maximize their asset returns.

January 2024 The Middle East royal family injected USD1 billion for an 18% stake, and the company began restructuring. The listing process was accelerated with the financial support of the royal family.

February 2024 Former Morgan DF AUT LLC completed restructuring into AUT LLC, with William Thompson as Chairman of the Board.

February-June 2024 In-depth negotiations are planned with multinational banks such as Wells Fargo, HSBC, Citi, Goldman Sachs, etc. to bridge critical capital on the Wall Street, seamlessly connect traditional centralized finance with decentralized finance, and make the blockchain financial market more mature.

June 2024 AUTHERIUM (AUT) is launched globally.

June-December 2024 AUT makes every effort to establish strategic partnerships with enterprises and businesses in third-world countries to assume its social responsibility, helping them catch up by leveraging blockchain.

End of 2024 Community users of Finton will reach the milestone of 100—million-scale, covering more than 100 countries and thousands of cities worldwide, fulfilling AUT's vision of win- win cooperation.

2025 – 2026 AUT will seek its global footing with the number of global users exceeding hundreds of millions, and to be listed on NASDAQ, becoming a unicorn blowing up blockchain finance worldwide.

15. Reference Appendix of the Technical Framework Inspirations Section

AUT is a super public chain that epitomizes the cutting-edge blockchain technologies and boasts irreplaceable advantages in core applications for the financial sector. We are deeply grateful to the industry pioneers and elites for their explorations with wisdom. This appendix is dedicated to the experts and scholars who have contributed a lot to the development of the industry and AUT's technical architecture:

A Proof-of-Work Parallel-Chain Architecture for Massive Throughput
https://neironix.io/documents/whitepaper/6793/chainweb-v15.pdf

Proceedings of the 2018 International Symposium on Communication Engineering & Computer Science
https://www.atlantis-press.com/proceedings/cecs-18/25902503

Practical Byzantine Fault Tolerance https://pmg.csail.mit.edu/papers/osdi99.pdf

Replication Theory and Practice
https://link.springer.com/book/10.1007/978-3-642-11294-2#toc

An Attack-Tolerant Agreement Algorithm for Block Chain
https://ieeexplore.ieee.org/abstract/document/8639577

The knowledge complexity of interactive proof-systems
https://dl.acm.org/doi/abs/10.1145/3335741.3335750

Pinocchio: nearly practical verifiable computation
https://dl.acm.org/doi/abs/10.1145/2856449

A No BS Look at L1 Performance
https://medium.com/dragonfly-research/the-amm-test-a-no-bs-look-at-l1-performance-4c8c2129d581

On the Size of Pairing-based Non-interactive Arguments
https://link.springer.com/chapter/10.1007/978-3-662-49896-5_11

Bulletproofs: Short Proofs for Confidential Transactions and More
https://eprint.iacr.org/2017/1066.pdf

Scalable, transparent, and post-quantum secure computational integrity
https://eprint.iacr.org/2018/046

P2PTradeX: P2P Trading between cryptocurrencies
Https://bitcointalk.org/index.php?topic=91843.0

Alt chains and atomic transfers
https://bitcointalk.org/index.php?topic=193281.msg2003765#msg2003765

Solidity 0.8.18 documentation https://docs.soliditylang.org/en/v0.8.18/

Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

Atomic Cross-Chain Swaps https://dl.acm.org/doi/abs/10.1145/3212734.3212736

A Review of the Current State of Decentralized Finance as a
Subsector of the Cryptocurrency Market

https://static1.squarespace.com/static/553d790de4b08ceb08ab88fd/t/5f5c2a4d381d4c58ce97cde2/1599875 662625/DeFi_P2_SciPaper_3.pdf

A Next-Generation Smart Contract and Decentralized Application Platform.
https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

A Survey of Blockchain From the Perspectives of Applications，Challenges，and Opportunities https://ieeexplore.ieee.org/abstract/document/8805074

Trusted and Secured E-Voting Election System Based on Block Chain Technology
https://link.springer.com/chapter/10.1007/978-3-030-43192-1_9

Finance and Economics Discussion Series
https://www.federalreserve.gov/econres/feds/decentralized-finance-defi-transformative-potential-and-associated-risks.htm

Bidl: A High-throughput, Low-latency Permissioned Blockchain Framework for Datacenter Networks https://dl.acm.org/doi/10.1145/3477132.3483574

PROOF-OF-STAKE (PoS)
https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Addressing Scalability and Storage issues in Block Chain using Sharding https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3446547

Securing Proof-of-Stake Blockchain Protocols
https://link.springer.com/chapter/10.1007/978-3-319-67816-0_17

Initial Evidence from the Ethereum Ecosystem https://www.nber.org/papers/w30949