ZITCOIN

Project White Paper

Look back at the Layer 2 standard   Defining a new era of blockchain

ZTC optimizes the consensus algorithm to ensure the efficient and stable operation of the Bitcoin network

Table of Contents

Zitcoin

01/Introduction

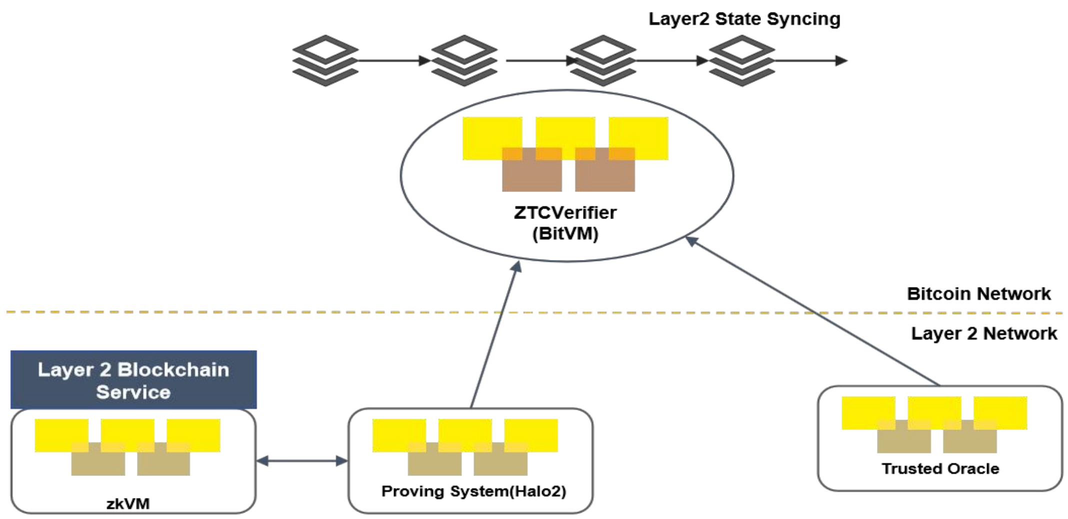
In the wave of digital transformation, blockchain technology, with its decentralized， transparent, and immutable characteristics, has become a significant driver of global technological innovation. As mainstream cryptocurrencies like Bitcoin become more widespread and their application scenarios continue to expand, the performance bottlenecks faced by blockchain networks have become increasingly prominent, posing a critical challenge to their further development. To address these challenges, the ZTC project has emerged, dedicated to revitalizing Bitcoin and other blockchain networks through cutting-edge Layer 2 solutions, and leading the innovation and development of blockchain technology.

Overview of ZTC

ZTC (Zitcoin) is a blockchain innovation project based on a Layer 2 architecture, aiming to optimize and expand existing blockchain networks through technological advancements. It provides high-performance, low-cost Layer 2 scaling solutions for mainstream blockchains like Bitcoin. By integrating cutting-edge technologies such as Zero-Knowledge Proofs (ZKPs) and quantum cryptography, ZTC significantly enhances the transaction speed and throughput of blockchains without compromising system security and decentralization.

In ZTC's Layer 2 architecture, an account model is used to manage the blockchain's state. To verify the entire blockchain's state, ZTC employs a zkVM (Zero-Knowledge Virtual Machine) based on the Halo2 proof system. This verification method ensures the synchronization of Layer 2 states with the Bitcoin main network, and all Layer 2 state updates are validated through Zero-Knowledge Proof (ZKP) verifiers implemented by BitVM.

For tracking and managing all Layer 2 states, ZTC uses a unified UTXO (Unspent Transaction Output) model. Additionally, ZTC introduces a trusted oracle mechanism, ensuring that only inputs and outputs complying with Layer 2 protocol specifications are allowed, thereby maintaining the system's security and stability.



ZTC Public Chain Plan:

- **ZTCV1 (Sidechain Version):** During the launch of the V1 version, the ZTC public chain will focus on the performance, security, and usability of the sidechain. Through continuous testing and optimization, ZTC aims to ensure that the sidechain meets user needs and provides developers with a rich set of development tools and API support.

- **ZTCV2 (UTXO Client Verification Version):** The launch of the V2 version will further enhance the performance and user experience of the ZTC public chain. With UTXO client verification, users can conduct transactions more quickly and securely, enjoying a smoother blockchain experience. At the same time, ZTC will continue to optimize and improve the UTXO client verification mechanism to ensure its stability and reliability in various scenarios.

The phased launch plan of the ZTC public chain aims to gradually validate and refine its blockchain technology, providing a more mature and stable blockchain platform for users and developers. Through the iterations and optimizations of V1 and V2 versions, ZTC will continuously drive the development and application of blockchain technology, contributing to the prosperity of the entire blockchain ecosystem.

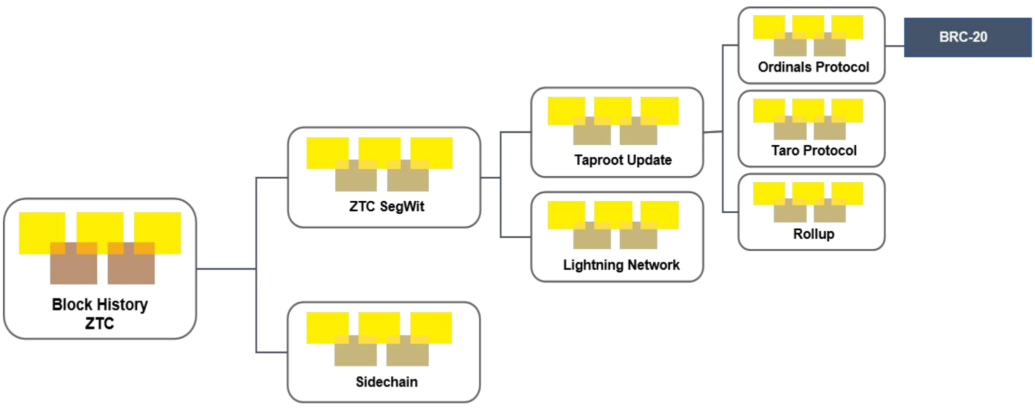
02/Driving Background

2.1 Challenges of the Bitcoin Network

As the Bitcoin network evolves, its performance issues have become increasingly severe. Slow transaction speeds, limited throughput, long block confirmation times, and network congestion not only affect the user experience but also limit Bitcoin's applications in broader fields. These issues urgently need to be addressed to drive the continued development of Bitcoin and the entire blockchain industry.

2.2 Rise of Layer 2 Solutions

Layer 2, as a significant innovation in blockchain technology, improves transaction speed and throughput by building an expansion layer on top of the main chain (Layer 1) while maintaining the security and decentralization of the main chain. This approach effectively addresses the performance issues faced by Bitcoin without requiring extensive modifications to the main chain. The rise of Layer 2 solutions has brought new development opportunities and possibilities to the blockchain industry.



2.3 Innovations of ZTC

Building on Layer 2 solutions, ZTC introduces innovative technologies to achieve higher performance and a better user experience.

- **High-Performance Consensus Algorithm：** ZTC introduces and optimizes the latest consensus algorithms, such as STARKs from StarkNet, to ensure high-speed transaction processing and low latency. These algorithms significantly improve transaction confirmation speed, providing users with a smoother blockchain experience.

- **Privacy Protection Technology：** ZTC fully leverages advanced privacy protection technologies such as Zero-Knowledge Proofs (ZKPs) to safeguard users' transaction privacy and anonymity. These technologies ensure that users' transaction information is not disclosed to third parties, meeting the high demands for privacy protection.

- **Decentralized Oracle：** ZTC's decentralized oracle system ensures seamless integration of on-chain data with real-time off-chain information. By utilizing real-time data provided by multiple independent oracle nodes, ZTC enhances the reliability and flexibility of smart contracts, offering developers a richer array of application scenarios.

- **SWAP（Swap Protocol）：** ZTC supports the SWAP protocol, which allows users to seamlessly exchange assets on-chain without the need for third-party intermediaries. This not only enhances the efficiency and security of asset circulation but also provides users with a more convenient way to conduct transactions.

- **UTXO Client-Side Validation：** In subsequent versions of ZTC, a UTXO client verification mechanism will be introduced. This mechanism allows users to locally verify the validity of transactions, reducing reliance on centralized verification services and further enhancing the system's security and privacy.

- **Proof of Stake ＋ Proof of Work Consensus Nodes：** ZTC adopts a hybrid consensus mechanism combining POS (Proof of Stake) and POW (Proof of Work). POW ensures the network's security and decentralization, while POS enhances transaction speed and energy efficiency. This hybrid mechanism achieves a good balance between performance and security.

The ZTC public chain employs a dual GAS model.In version 2, it uses a BTC and ZTC dual GAS consumption model, allowing users to choose freely. This model effectively supports both the BTC ecosystem and ZTC's deflationary model.

✓ **Dual GAS Model:** The ZTC public chain employs a dual GAS model. In version 2, users can choose between BTC and ZTC for GAS consumption. This flexibility supports the deflationary models of both the BTC ecosystem and ZTC, providing users with greater choice and helping to maintain a balanced and efficient ecosystem.

The successful implementation of the ZTC project will bring revolutionary changes to Bitcoin and other blockchain networks, driving the continuous development of the entire blockchain industry. ZTC looks forward to collaborating with various stakeholders to jointly create a new chapter in blockchain technology.

03/Mission of ZTC

3.1 Significantly Improve Bitcoin Network Performance

In the realm of digital currency and blockchain, performance has always been a key factor in determining the success of a network.ZTC's primary mission is to significantly improve the performance of the Bitcoin network to meet the growing demands of users and application scenarios.

3.1.1 Enhance Transaction Speed and Throughput

Currently, the Bitcoin network faces limitations in transaction speed and throughput, causing users to pay high transaction fees and endure long confirmation times during peak periods. ZTC addresses these issues by introducing advanced Layer 2 technologies, such as State Channels and Sidechains, to offload most transactions to off-chain processing. This approach significantly reduces the burden on the main chain, thereby greatly enhancing transaction speed and lowering transaction costs. ZTC will continuously optimize its consensus algorithm to ensure the network remains efficient and stable even during surges in transaction volume.

3.1.2 Off-Chain Processing Scalability

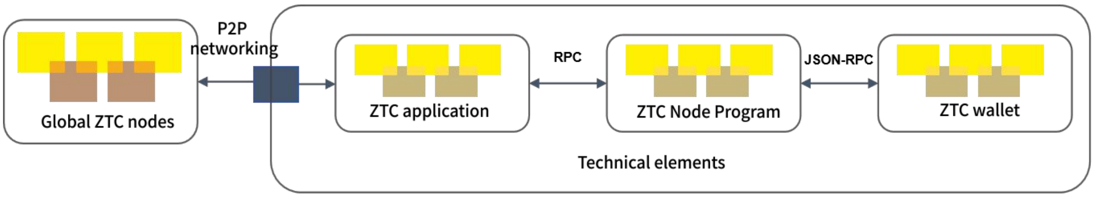
By leveraging off-chain processing, ZTC moves complex transaction logic and data handling off the main chain, thereby increasing transaction speed and reducing the risk of network congestion. Off-chain processing also provides developers with greater flexibility and room for innovation, enabling the realization of more complex application scenarios. Additionally, ZTC will actively explore other scalability solutions, such as sharding, to further enhance network performance.

3.2 Decentralized Security

In blockchain technology, decentralization and security are two crucial principles. In its design and implementation, ZTC will always adhere to these principles, ensuring the stable operation of the network and the safety of users' assets.

3.2.1 Decentralization Principle

Decentralization is one of the core advantages of blockchain technology and the foundation for the sustained development of the Bitcoin network. In its design and implementation, ZTC consistently adheres to the principle of decentralization, ensuring that the stable operation of the network does not rely on any centralized institutions or individuals. By employing technologies such as distributed ledgers and consensus algorithms, ZTC ensures the decentralized nature of the network, preventing issues like single points of failure and concentration of power.



3.2.2 Security Assurance

In terms of security, ZTC employs the latest cryptographic technologies and security mechanisms to ensure the safety of transactions and the integrity of data. By incorporating advanced encryption algorithms, digital signature technologies, and privacy protection methods, ZTC ensures that users' transaction information is not exposed to third parties and prevents any form of attack and tampering.ZTC has established stringent security audits and a bug bounty program to encourage users and security experts to actively participate in the maintenance and improvement of the network's security.

3.3 Introducing innovative applications of Layer 2 technology

ZTC actively explores the introduction of innovative applications of Layer 2 technology to enrich the Bitcoin network ecosystem and provide more value and convenience to users.

3.3.1 Cross-Chain Transactions and Interoperability

Through Layer 2 technology, ZTC enables cross-chain transactions and interoperability between different blockchain networks. By breaking down barriers between blockchains, it promotes resource sharing and collaboration among various networks, providing users with more flexible and convenient cross-chain services. For instance, users can seamlessly transfer assets, conduct transactions, and access smart contracts across different blockchain networks.

3.3.2 Decentralized Finance (DeFi)

DeFi, as an important branch of the blockchain field, is gradually transforming the financial industry. ZTC actively introduces Layer 2 technology to promote the development and innovation of DeFi. By building decentralized platforms for lending, trading, insurance, and asset management, ZTC provides users with a more secure, transparent, and efficient financial service experience. Additionally, ZTC collaborates with outstanding projects in the DeFi space to jointly drive the prosperity and development of the entire ecosystem.

3.3.3 Asset Tokenization

Asset tokenization is another important application direction of blockchain technology, which can convert various physical assets into tradable digital assets. ZTC explores application scenarios and solutions for asset tokenization to provide users with more convenient and efficient asset management and trading methods. Reduce the cost and threshold of asset tokenization and attract more users and institutions to participate. Cooperate with relevant industries to jointly promote the standardization and standardization development of asset tokenization.

04/ZTC Technical solutions

4.1 Technical overview

4.1.1 Layer 2 Trusted Oracle

ZTC’s Layer 2 architecture relies on a node composed of selected users responsible for overseeing the operation of the entire network. When the agreement encounters problems, it has the right to intervene and suspend the agreement to protect the assets of all users. In addition, a trusted oracle is introduced to verify the correctness of input/output UTXO and scripts to ensure the validity of Layer 2 transactions.

4.1.2 First level to second level interaction

In ZTC, Layer 2 protocols are represented by creating a single Taproot address. When UTXO is transferred to this Taproot address, the "recharge" process from the Bitcoin main network to Layer 2 is actually completed. Only protocols, trusted oracles, or committee accounts have “transfer” permissions for deposited UTXOs. Trusted oracles ensure that UTXO scripts in ownership transfer transactions are accurate.

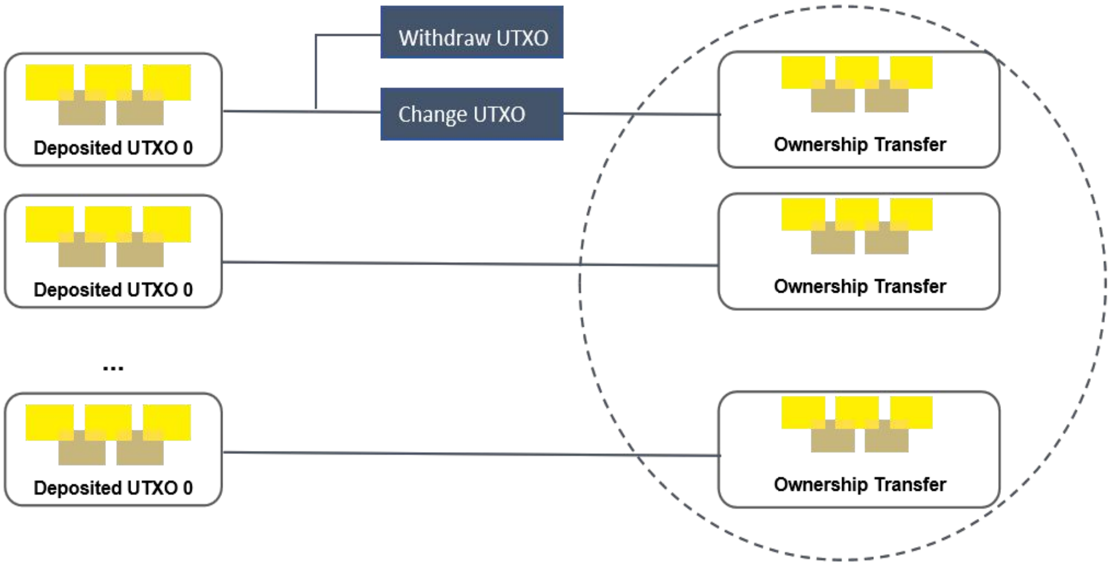
4.1.3 Sync to Bitcoin mainnet block

State updates from the Layer 2 network will be synchronized to the Bitcoin mainnet in the form of blocks. Each block contains transaction records, new account status, new UTXO, Bitcoin network block information and zero-knowledge proof (ZKP), which is used to verify the correctness of state transitions. These status updates are recorded in UTXO transaction history, ensuring Layer 2 transparency and traceability.

ZKP is used to verify the correctness of Layer 2, including transaction signature verification, account status correctness, recharge transaction processing, and UTXO distribution accuracy. To ensure the accuracy of block information, ZTC adopts a challenge and response scheme, combined with ZKP circuits and BitVM for verification. Each Layer 2 block has a unique binary circuit commitment, with public inputs checked for correctness by trusted oracles.

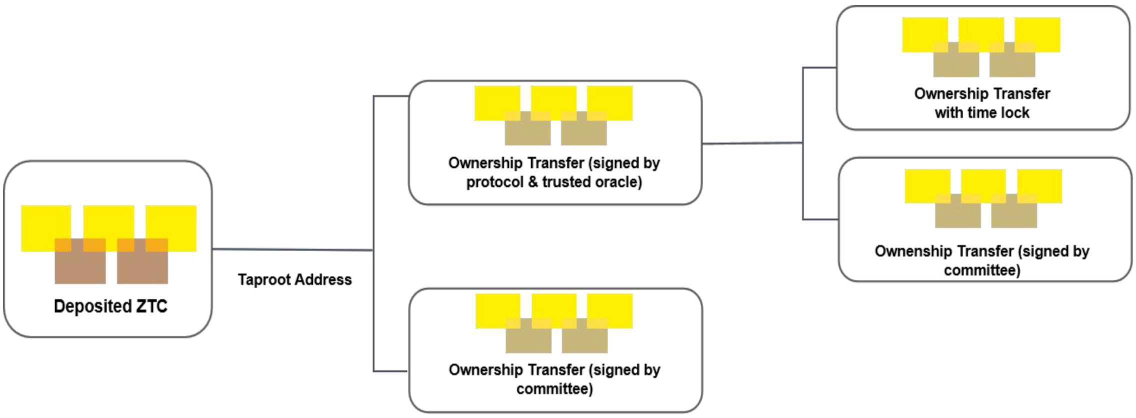
4.1.4 Exit mechanism

Assets can be transferred from Layer 2 to the Bitcoin main network, mainly through two methods: withdrawal (withdrawal) and force-withdrawal (force-withdrawal). Withdrawal transactions are triggered by Layer 2 and verified using ZKP circuits to ensure safe transfer of funds. The forced withdrawal transaction is initiated by the Bitcoin network and reflected in the next block status update.



4.2 Layer 2 Layer 2 expansion

Layer 2 technology is also widely recognized by the industry as layer 2 expansion technology. Its core concept is to enhance the performance of the existing blockchain main chain (Layer 1). By building additional layers under the chain, Layer 2 technology can significantly improve the transaction speed and throughput of the blockchain network and effectively reduce transaction costs while ensuring the security and decentralization of the main chain.



Principle exploration:

Layer 2 technology processes a large number of transactions off-chain and submits transaction results or status updates to the main chain for verification and confirmation. This method effectively avoids the congestion and delays caused by processing a large number of transactions on the main chain, thus achieving a significant increase in transaction speed. At the same time, since the transaction data processed off-chain is not directly written to the main chain, transaction fees are also significantly reduced.

Cutting edge advantages:

- Scalability: Layer 2 technology effectively expands the performance of the blockchain network by processing a large number of transactions off-chain, enabling it to support more application scenarios and user needs.

- Guarantee of decentralization and security: Layer 2 technology improves performance without sacrificing the decentralization and security of the main chain. All transaction results or status updates processed off-chain still need to be verified and confirmed by the main chain, ensuring the security and credibility of the entire system.

- Optimization of transaction speed:By processing transactions in parallel off-chain, Layer 2 technology significantly improves transaction speed.By processing transactions in parallel off-chain, Layer 2 technology significantly improves transaction speed.

4.3 Parallel processing and transaction speed optimization

ZTC makes full use of Layer 2 technology processing capabilities to achieve parallel execution of transactions. Build multiple off-chain channels and side chains, and distribute transaction processing to these channels or side chains. Through parallel processing, ZTC can process more transactions at the same time, thereby significantly improving transaction speed and throughput. Transaction sorting and batching mechanisms. By prioritizing and batching transactions, ZTC can further optimize transaction speed and reduce transaction delays. This ensures that high-priority transactions can be processed in a timely manner and improves the processing efficiency of the entire system.

4.4 ZTC focuses on state channel sidechain

After in-depth research and evaluation, ZTC focuses on State Channels and Sidechains, two mature and widely used Layer 2 technologies.

For State Channels, ZTC optimizes its shutdown mechanism. Traditional state channels need to submit a large amount of data to the main chain for verification and confirmation when closing, which may result in higher closing costs and longer closing time. In order to solve this problem, ZTC introduces advanced compression technology and verification mechanism to reduce closing costs and improve user experience.

For Sidechains, ZTC explores new construction methods. Traditional side chains usually have a weak coupling relationship with the main chain, which may lead to cross-chain transaction security and stability issues. In order to solve this problem, ZTC studies closer cross-chain protocols and mechanisms to ensure the stability and security of the side chain. Explore the interoperability of cross-chain assets and provide users with more flexible and convenient cross-chain services.

4.5 High-Performance Consensus Algorithm

4.2.1 STARKs technology applications

ZTC uses STARKs (Scalable Transparent ARgument of Knowledge) technology as the core technology of Layer 2 solutions. STARKs allow the correctness of transactions on Bitcoin and other blockchain networks to be verified without revealing specific inputs or calculation processes, thus providing an efficient verification mechanism for the ZTC network.

Brief description of principle:

In the ZTC project, STARKs technology is used to move transactions off-chain for execution, and the validity of the transactions is verified through mathematical proofs. The execution result of a transaction or status update is encoded as a mathematical proof that can be verified by any node with the appropriate verification key. Due to the transparency and verifiability of STARKs, as well as efficient verification speed, the ZTC project can support large-scale transaction processing and verification.

Characteristic analysis:

- **Efficiency:** The ZTC project uses STARKs technology to achieve rapid verification of off-chain transactions, which greatly

  Reduces the computational burden and transaction delays on the main chain.
- **privacy protection:** Using zero-knowledge proof technology, the ZTC project can protect users while verifying transactions.User privacy and data security.
- **Scalability:** Due to the architectural advantages of STARKs, the ZTC project has strong expansion capabilities and can enough to support growing transaction needs.

4.2.2 Algorithm optimization

In order to further improve the performance and stability of the ZTC project, the following optimizations and improvements will be made to STARKs technology:

- **Parallel processing:**By optimizing the algorithm architecture, parallel processing of transactions is achieved and the efficiency and speed of transaction verification are improved.
- **Improved verification efficiency:**Introduce advanced verification technology and algorithms to reduce the complexity and calculation of the verification process quantity to further improve verification efficiency.
- **Security enhancements:**Pay close attention to the latest security vulnerabilities and attack methods, and take corresponding security and protective measures in a timely manner to ensure the security of the ZTC project.

4.2.3 Performance and security analysis

Performance analysis:

- **Transaction verification speed:** By simulating transaction scenarios of different sizes and complexities, the average time required to verify a single transaction in the ZTC project is measured.
- **Throughput:** Test the number of transactions that the ZTC project can handle to evaluate the scalability of the system.
- **Delay:**Measure the time interval from when a transaction is initiated until it is verified and confirmed on the blockchain to evaluate ZTC Latency performance of the project.
- **System resource consumption:** Monitor the consumption of computing resources, storage resources, and network bandwidth by the ZTC project while it is running.

Security analysis:

- **STARKs technical security:** Evaluate whether there are known security vulnerabilities or attack methods in the application of STARKs technology in the ZTC project.

- **privacy protection:** Analyze whether the ZTC project can effectively protect user privacy during the transaction verification process and data security.
- **Resistance to attack:** Simulate various possible attack scenarios to test the anti-attack capabilities of the ZTC project. Code audit and vulnerability scanning: Entrust a professional security team to audit and vulnerability scan the code of the ZTC project to ensure its security and stability.

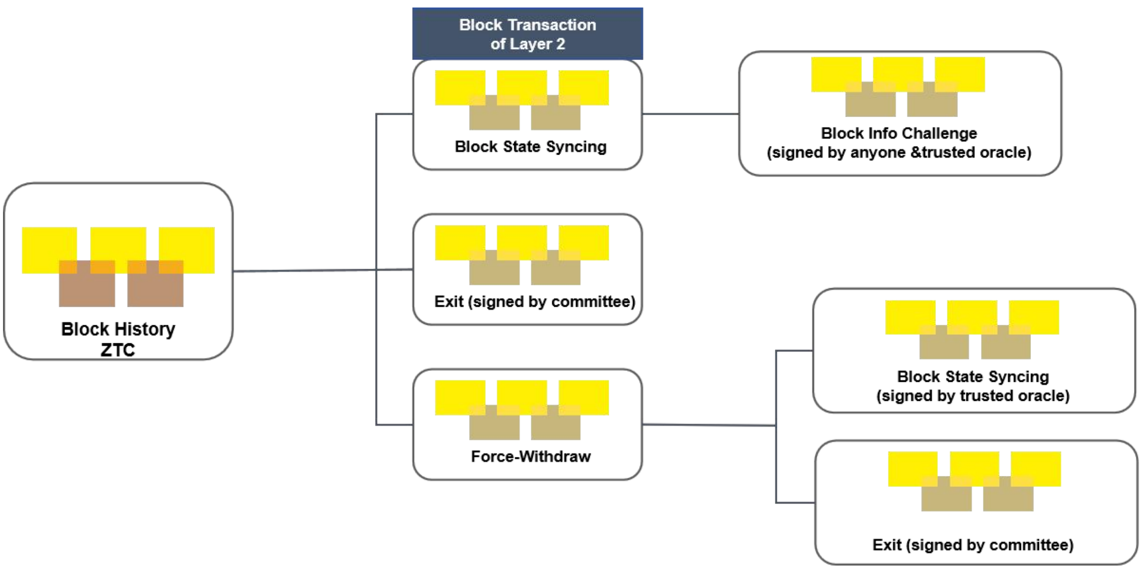
4.6 Data privacy protection

4.3.1、Deep integration of privacy protection technology

In the construction of ZTC, data privacy and protection are regarded as crucial core elements. In-depth research and integration of multiple cutting-edge privacy protection technologies to build a safe and reliable blockchain network.

1. Zero-knowledge proofs (ZKPs) technology

ZKPs are one of ZTC's core technologies for privacy protection. Through ZKPs, transaction information is converted into mathematical proof problems without disclosing the specific content of the transaction. Using STARK (Scalable Transparent ARguments of Knowledge) as the implementation method of zero-knowledge proof is highly efficient and can protect the privacy of transactions while ensuring the transparency of the verification process.



2. **Homomorphic Encryption**

Homomorphic encryption technology allows calculations to be performed on encrypted data without decrypting the data itself. In ZTC, homomorphic encryption technology is used to encrypt user transaction data to ensure the privacy and security of data during the transaction process. Homomorphic encryption also provides the ability to verify and calculate on encrypted data, further enhancing ZTC's privacy protection capabilities.

3. **Secure Multi-Party Computation (MPC)**

Secure multi-party computing technology allows multiple participants to jointly calculate a function without revealing their secret inputs. In ZTC, MPC technology is used to realize collaborative verification and calculation between nodes. Through MPC technology, transaction information can be securely shared and verified among multiple nodes, while protecting user privacy and data security.

4.3.2、ZKPs used in privacy protection

ZTC applies ZKPs technology to ensure the privacy of transactions. It is based on the ZKPs privacy protection transaction protocol, which converts transaction information into mathematical proof problems. The correctness of these proofs is verified through ZKPs technology, without revealing the specific content of the transaction. , to achieve transaction verification and confirmation.

The scalability and flexibility of ZKPs technology are also used to optimize algorithm parameters and improve data structures to further improve the performance and efficiency of ZKPs technology in ZTC.

4.3.3、Encryption and anonymity

Encryption technology is applied to protect users ' transaction data, and anonymity technology is combined to further enhance users' privacy protection capabilities. Advanced encryption algorithms encrypt user transaction data to ensure the security of data during transmission and storage. At the same time, anonymity technologies such as ring signatures and confusion networks hide users ' true identities and transaction paths to prevent users' privacy from being leaked or tracked.

The perfect combination of encryption technology and anonymity brings ZTC to a new level in protecting user privacy and data security.

4.3.4、Privacy protection mechanism

1. Privacy protection smart contract

With the widespread application of smart contracts on the blockchain, ZTC has designed and implemented privacy-protecting smart contracts, so that the execution process and results of smart contracts can be verified and recorded without leaking user privacy. By combining privacy protection technologies such as zero-knowledge proof and homomorphic encryption, the privacy and security of smart contracts are ensured.

2. Privacy protection cross-chain transactions

With the continuous development of blockchain technology, cross-chain transactions have become a key technology to realize value circulation between different blockchains. However, privacy protection issues in cross-chain transactions have become increasingly prominent. ZTC proposes a privacy-protecting cross-chain transaction mechanism. By utilizing zero-knowledge proof technology, privacy-protected cross-chain transactions between different blockchains are realized to ensure user privacy and data security during the transaction process.

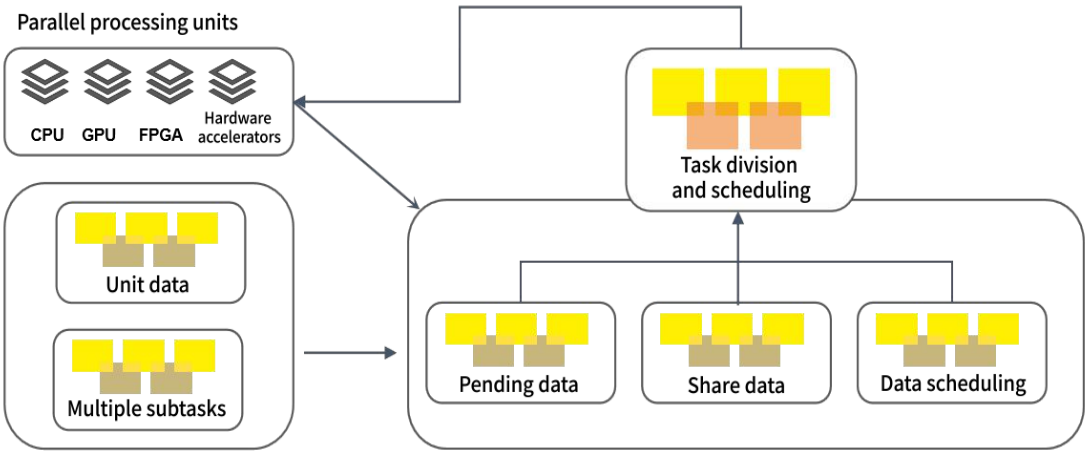
3. Privacy protection node collaboration

In the ZTC network, cooperation between nodes is the key to ensuring the normal operation of the network. However, collaboration between nodes may also bring the risk of privacy leakage. In order to solve this problem, by utilizing secure multi-party computing technology, we ensure that transaction information is safely shared and verified among multiple nodes, protecting user privacy and data security. This mechanism not only improves the efficiency and security of node collaboration, but also further enhances ZTC's privacy protection capabilities.

4.7 Smart contract support

4.4.1、Layer 2 implementation

Recognizing the performance limitations of the Layer 1 main chain, ZTC chose to implement smart contracts at Layer 2. Layer 2 solutions, such as State Channels, Sidechains, Sharding, and Rollups, allow most calculations and data processing to be performed off-chain, with only critical data or status updates submitted to Layer 1 for verification and documentation.



The main advantages of this architecture are:

1.Performance improvements: Since most calculations and data processing are performed off-chain, Layer 2 can support higher transaction throughput and faster contract execution speed.

2.Reduce costs: Since Layer 2 off-chain transactions do not require high miner fees, the execution cost of smart contracts can be significantly reduced.

3.User experience optimization: Faster transaction speeds and lower costs will lead to better user experience, especially in smart contract applications that require frequent interactions.

4.4.2、Application of parallel execution environment in smart contract execution

ZTC uses Parallel Execution Environment (PEE) technology. Allows multiple smart contract calls and status updates to be processed simultaneously, thereby achieving efficient contract execution. Specific implementation methods include：

- **State sharding：** The blockchain's state data is divided into multiple shards, and each shard is processed in parallel by one or more nodes. The execution of smart contracts can be carried out in parallel on different state shards, thereby significantly improving throughput.

- **Intelligent scheduling:** The system intelligently schedules the execution sequence of contracts based on the priority of the contract, resource requirements and other factors to ensure effective utilization of resources and rapid response of the contract.

- **Lightweight virtual machine:** Adopt optimized lightweight virtual machine technology to reduce the calculation required to execute smart contracts

Computing and storage resources to improve execution efficiency.

- **Transaction pipeline:**： Decompose the transaction processing process of smart contracts into multiple stages, and process them in different Parallel execution in the unit forms a transaction pipeline to maximize resource utilization.

4.4.3、Cross-chain smart contracts

As the demand for blockchain interoperability increases, ZTC will support the deployment and testing of cross-chain smart contracts. Cross-chain technology allows smart contracts to seamlessly interoperate between different blockchain networks, expanding the application scope and flexibility of smart contracts.

- **Cross-chain bridging:** Build a bridge protocol to connect different blockchain networks to achieve cross-chain communication and data transmission. This can be based on existing Relay Chain or Sidechain technology.

- **Cross-chain consensus:** Design a cross-chain consensus mechanism to ensure the

consistency and security of cross-chain transactions. This may involve

and the consensus algorithm coordination and verification process between multiple blockchain networks.

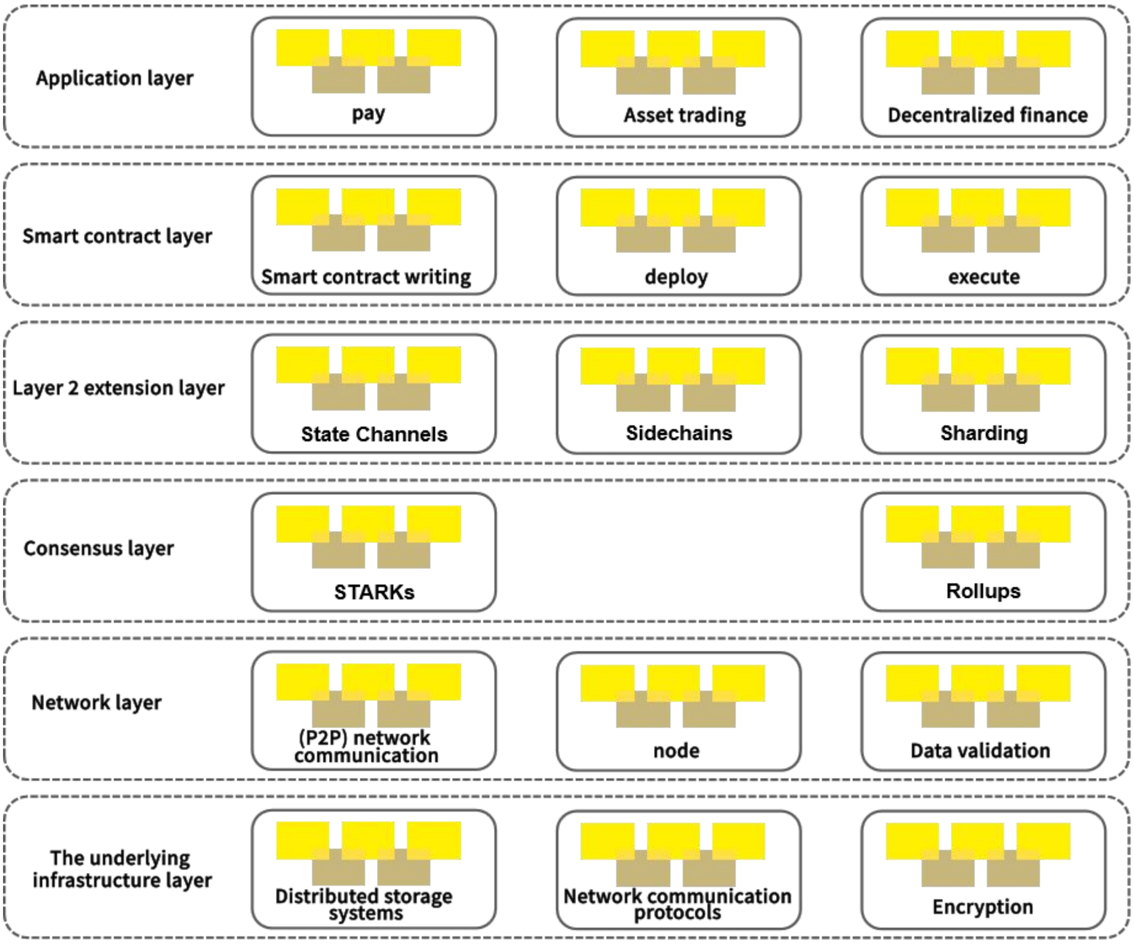
- **Cross-chain verification:**Provides a cross-chain verification mechanism to ensure the correctness and security of cross-chain smart contracts. This can
It can include verification of cross-chain transactions, synchronization and verification of status data, etc.

05/Technical architecture and implementation

5.1 Detailed explanation of ZTC system architecture

Overview of the overall system architecture

The overall system architecture of ZTC is built based on the layered design concept to achieve high-performance, high-security, high-scalability and high-interoperability blockchain services. The architecture includes from bottom to top: underlying infrastructure layer, network layer, consensus layer, Layer 2 extension layer, smart contract layer and application layer.



Functions and interactions of components at each level

- **Underlying infrastructure layer:** Provide hardware and software infrastructure support, including distributed storage systems (such as IPFS, Swarm, etc.), network communication protocols (such as Libp2p, gRPC, etc.) and encryption technologies (such as elliptic curve encryption algorithms, hash functions, etc.). The redundancy and persistence of data are ensured through distributed storage, the network communication protocol ensures the efficiency and security of communication between nodes, and the encryption technology protects the confidentiality and integrity of the data.

- **Network layer:** Responsible for communication and data transmission between nodes to achieve real-time, efficient and reliable dissemination of information. Ensure the stability and security of the network through mechanisms such as point-to-point (P2P) network communication, node discovery, data verification and synchronization.
- **Consensus layer:** Use high-performance consensus algorithms (such as STARKs, Rollups, etc.) to ensure that transaction data in the network are verified and confirmed fairly, reliably and consistently. Through collaboration and competition among validator nodes, rapid confirmation of transaction data and synchronization of the entire network are achieved.
- **Layer 2 extension layer:** Through technologies such as State Channels, Sidechains, and Sharding, off-chain transaction processing is implemented to increase transaction speed and throughput, and reduce transaction fees. The status channel allows both parties to establish a private communication channel to conduct high-frequency, small-amount transactions without writing to the main chain every time; the side chain serves as a blockchain separated from the main chain and is connected to the main chain through cross-chain bridging. Chain interoperability; sharding splits the main chain into multiple sub-chains to process transaction data in parallel.
- **Smart contract layer:** Support the writing, deployment and execution of smart contracts to realize the development and operation of decentralized applications. Smart contracts are automatic execution programs based on blockchain technology and contain a set of conditions and operation rules. Developers can use programming languages such as Solidity and Vyper to write smart contracts, and convert them into bytecode through a compiler to deploy on the blockchain.
- **Application layer:** Provide users with a wealth of blockchain application scenarios and services, such as payment, asset trading, decentralized finance (DeFi), etc. Call the smart contract interface to implement business logic and data processing of various blockchain applications.

Selection and configuration of underlying technology stack

ZZTC's underlying technology stack is mainly based on the widely used blockchain technology stack, including:

- **Crypto library:** Such as OpenSSL, libsodium, etc., used to provide security functions such as encryption algorithms and hash functions.
- **Consensus algorithm library:**For example, Stark Net's STARKs algorithm, Optimistic Rollups algorithm, etc. are used to achieve an efficient and secure consensus mechanism.
- **Network communication library:** Such as Libp2p, gRPC, etc., used to realize communication and data transmission between nodes. Choose an appropriate technology stack based on actual needs, and configure and optimize it accordingly to ensure system stability and performance.

Implementation of Layer 2 extension technology

Implement Layer 2 scaling technologies to increase transaction speed and throughput:

- **State Channels：**

The state channel allows both parties to establish a private communication channel and conduct high-frequency, small-amount transactions within the channel. Only the final settlement results will be submitted to the main chain for verification and recording.

Achieve efficient transaction processing while reducing transaction fees. However, users need to ensure the security of the channel and manage the life cycle and status of the channel.

- **Sidechains**

Sidechains are blockchains that are separate from the main chain and have their own block parameters and consensus model. Side chains can run independently and support more complex application scenarios. Through cross-chain bridging technology, interoperability between the main chain and side chains is achieved. Smart contracts deployed to the main chain can also be deployed to the side chain and executed on the side chain. The introduction of side chains can expand the application scope of ZTC and improve the throughput and performance of the entire system.

5.2 Consensus Algorithm

STARKs algorithm implementation

In order to pursue the ultimate transaction performance and security, ZTC chose the consensus algorithm of STARKs (ZK-SNARKs/ZK-STARKs). The core idea of this type of algorithm is to verify the correctness of transactions through mathematical proofs without disclosing specific transaction content, thereby achieving efficient and trustless transaction verification and confirmation.

Algorithm principle

STARKs allows transactions to be conducted off-chain and the compressed transaction proof (i.e., zero-knowledge proof) is submitted to the chain for verification. This design allows a large number of transactions to be processed in parallel off-chain, thus greatly improving transaction speed and throughput.

Both parties to the transaction first execute the transaction in an offline, trusted environment (called a "validator") and generate corresponding transaction proofs. This proof is then sent to the chain to be verified by other nodes. Due to the characteristics of zero-knowledge proof, the verification node does not need to know the specific transaction content and only needs to verify the correctness of the proof.

Implementation

- **Validator deployment:** Deploy a certain number of validator nodes in the network. These nodes are responsible for executing transactions off-chain and generating corresponding transaction proofs.
- **Transaction execution and proof generation:** When a user initiates a transaction, the validator node executes the transaction and generates a zero-knowledge proof containing the transaction execution result. This proof will be sent to the chain.
- **On-chain verification:** After receiving the proof, the nodes on the chain will use the STARKs verification algorithm to verify the correctness of the proof. If the verification passes, the transaction is considered valid and added to the blockchain.

- **Fraud detection and punishment:** If a validator node is found to have generated a wrong proof, the system will punish it to ensure the security and credibility of the system.

Performance testing and security verification

In order to ensure the effectiveness and security of STARKs in ZTC.

Performance testing will focus on the following key metrics:

- ✓ **Execution speed:** How quickly a validator node executes transactions and generates proofs.
- ✓ **Throughput:** The number of transactions that the system can process per unit time.
- ✓ **Delay:** The time interval from when a transaction is initiated until it is confirmed and added to the blockchain. Use professional performance testing tools and methods to conduct detailed performance testing on ZTC, and make corresponding optimizations and improvements based on the test results.

Security verification

Security verification will focus on the following aspects:

- ✓ **Resistance to attack:** Whether the system can resist various network attacks, such as double payment attacks, 51% attacks, etc.
- ✓ **Proof of correctness:** Whether the proof generated by the validator node can be correctly verified and there is no risk of tampering.
- ✓ **Fraud detection and punishment mechanism:** Whether the system can detect and punish fraud in a timely manner to ensure the security and credibility of the entire system.

5.3 Data privacy and security

5.3.1 Specific applications of privacy protection technology

ZKPs are a technology that allows one party (the prover) to prove to another party (the verifier) that a certain statement is true without revealing any additional information. This technology is particularly suitable for blockchain scenarios because it can verify the validity of transactions without leaking specific transaction data.

- **Application in ZTC:** We will use ZKPs technology to implement private transactions. Specifically, both parties to the transaction can generate a ZKPs certificate to prove that the transaction is valid, and then submit this certificate to the blockchain for verification without disclosing the specific transaction content.
- **Deployment and testing:** In the deployment phase, we will select the appropriate ZKPs algorithm, such as zk-SNARKs or zk-STARKs, and perform parameter configuration and environment settings according to the specific needs of ZTC. During the testing phase, we will focus on the execution efficiency, correctness and security of the algorithm to ensure its effective application in ZTC.

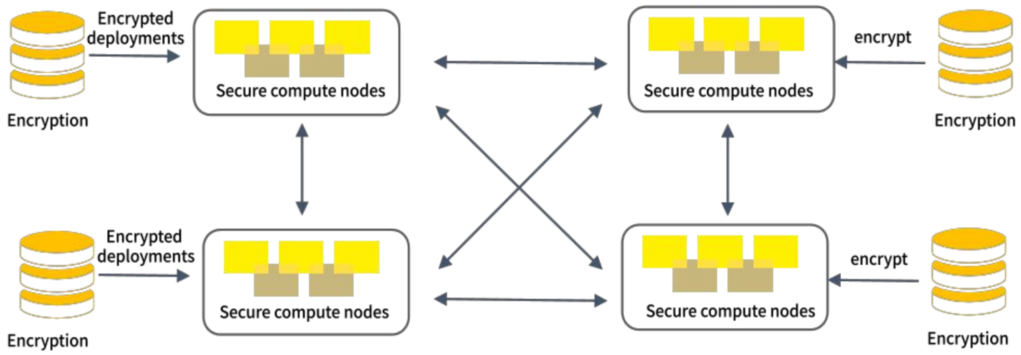
5.3.2 Homomorphic encryption technology

Homomorphic encryption is an encryption technology that allows calculations to be performed on encrypted data and the encrypted result obtained. This technology can process and analyze data without decrypting it, thus protecting the privacy of the data. Utilize homomorphic encryption technology to achieve privacy processing of sensitive data. For example, in smart contracts, homomorphic encryption technology can be used to encrypt user assets, and then transfer and calculate assets in an encrypted state, thereby protecting the user's asset privacy.

5.3.3 Secure multi-party computation (MPC)

MPC is a technology that allows multiple parties to jointly compute a function without trusting each other. Each participant can only see its own input and output, and cannot obtain the input information of other participants. This technology is particularly suitable for scenarios that require multiple parties to jointly process sensitive data.

Utilize MPC technology to achieve cross-chain interaction and multi-party collaboration. For example, in cross-chain transactions, MPC technology is used to ensure that both parties complete the transaction without revealing their respective asset information. In multi-party collaboration, ensure that all parties can complete a certain task together without revealing their respective sensitive information.



Deployment and testing of MPC technology will focus on its practical application in ZTC. Select the appropriate MPC protocol and algorithm, and perform parameter configuration and environment settings. During the testing phase, the performance, security, and ease of use of the MPC protocol are comprehensively evaluated, and corresponding optimization and improvements are made based on the test results.

5.5.4 ZKPs algorithm

- **Choosing the right ZKPs algorithm:** Choose the appropriate ZKPs algorithm, such as zk-SNARKs or zk-STARKs, according to the specific needs of ZTC.
- **Configuration parameters and environment:** Configure the appropriate parameters and environment settings according to the requirements of the selected algorithm.
- Write test cases: Write test cases covering various scenarios and boundary conditions to fully evaluate the performance, correctness, and safety of your algorithms.
- Execute the test: Use automated testing tools or manually execute test cases to get test results.
- Analyze test results: Conduct detailed analysis of test results to identify potential issues and areas for improvement.
- Optimizations and improvements: Carry out corresponding optimization and improvement based on the test results to improve the performance and security of the algorithm.

5.5.5 Anonymity implementation details

We will take the following measures to achieve private transactions and anonymity:

- **Encrypt user identity and transaction information:**Use advanced encryption algorithms to encrypt and protect user identity and transaction information to prevent unauthorized access and leakage.
- **Using anonymous transaction protocol:**Design and implement an anonymous transaction protocol to hide sensitive information such as the identities of both parties to the transaction and the transaction amount. This may involve the use of coin mixing, ring signatures or other anonymization techniques
- **Verification and auditing mechanisms:** Establish strict verification and audit mechanisms to ensure the authenticity and legality of transactions while preventing fraud.

5.5.5 Security audit

To ensure the security of ZTC we will conduct regular security audits and vulnerability management:

- **Security audit:** Conduct comprehensive security audits of the system regularly to identify potential security vulnerabilities and risk points. This can be done through an internal security team, external security consultants, or automated security scanning tools.

- **Vulnerability management:** Establish an effective vulnerability management mechanism to ensure timely discovery, reporting, repair and verification of vulnerabilities. This may involve measures such as setting up a bug bounty program, establishing a vulnerability response team, and developing a vulnerability remediation process.

5.5.7 Monitoring and logging

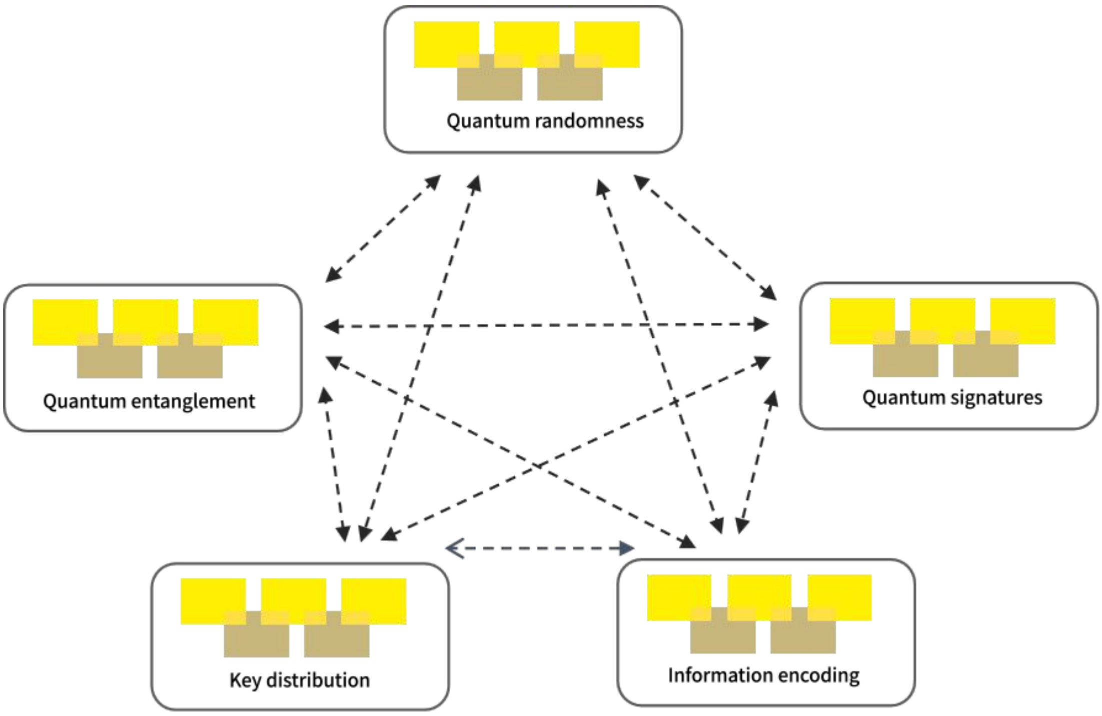
Monitoring and logging are critical components in ensuring system security and stability. By monitoring the running status of the system in real time and recording key events, potential security issues, performance bottlenecks or errors can be discovered in time, and corresponding measures can be taken to repair and optimize.

System status monitoring: Monitor node status, network connectivity, system resource utilization and other key indicators to ensure stable operation of the system.

- **Transaction monitoring:** Monitor the creation, verification, execution and confirmation process of transactions to ensure the correctness and timeliness of transactions.
- **Security event monitoring:** Monitor abnormal behaviors, potential attacks and other security events, promptly report to the police and take countermeasures.
- **Detailed log:** Record detailed logs of system operation, including transaction logs, node logs, security logs, etc., for subsequent auditing and troubleshooting.
- **Encrypted storage:** Encrypt and store sensitive logs to ensure data security and privacy.
- **Log analysis:** Use log analysis tools to mine and analyze log data to discover potential security risks or performance bottlenecks.

5.5.8 Quantum cryptography applications

Algorithm selection: Choose post-quantum cryptography algorithms that have been extensively researched and verified, such as lattice-based cryptography algorithms, hash-based cryptography algorithms, etc.

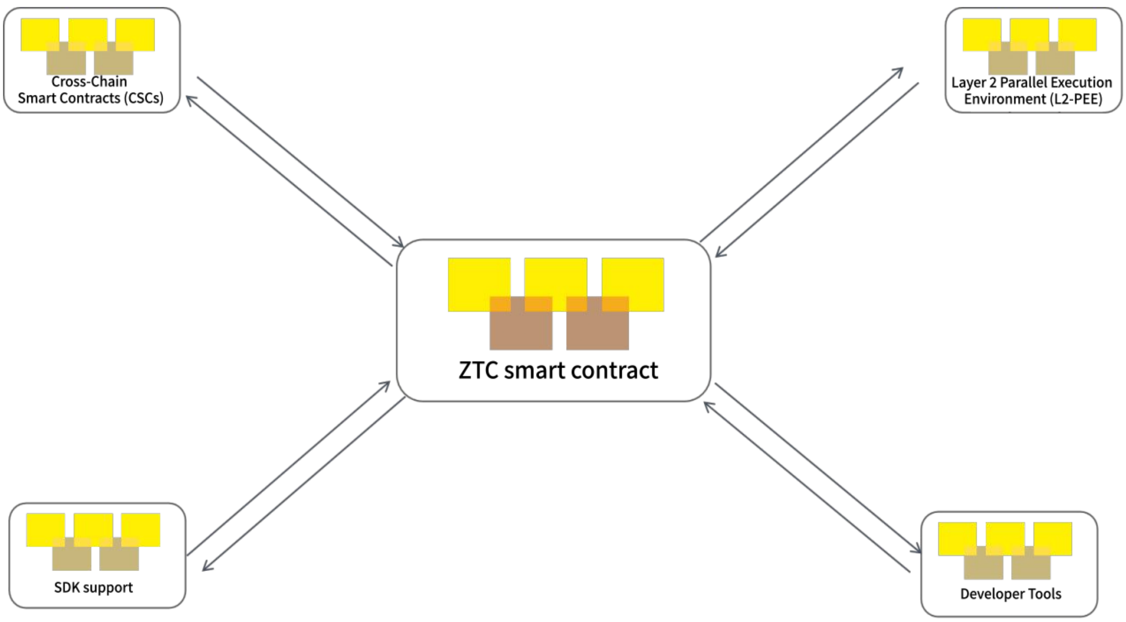


Key management: Design and implement a secure key management scheme to ensure the security and availability of keys in post-quantum cryptography algorithms.
Step by step migration: Gradually replace traditional cryptography algorithms with post-quantum cryptography algorithms to ensure a smooth transition and security of the system.
Regular assessment: Regularly evaluate and test the security of the system to ensure the effectiveness and security of post-quantum cryptography algorithms in the system.
keep improve: Based on the evaluation results and the latest research progress, post-quantum cryptography algorithms are continuously improved and optimized.

5.4 Smart contract platform

5.4.1 Construction of smart contract platform

ZTC's smart contract platform is based on Layer 2 solutions, supports multiple smart contract programming languages Solidity, and provides rich tool chain support, such as Truffle, which provides developers with great convenience. The platform's modular design allows for easy expansion and integration of new features and components to meet growing business needs.



5.4.2 Layer 2 parallel execution environment configuration

To improve the execution efficiency of smart contracts, the ZTC project introduces the concept of Layer 2 Parallel Execution Environment (L2-PEE). L2-PEE enables multiple smart contracts to be executed in parallel through optimization algorithms and distributed computing technology, thereby significantly improving transaction speed and throughput. The ZTC project will select the L2-PEE implementation that has been rigorously tested and optimized, and conduct fine configuration and adjustment to ensure its stable and efficient operation in ZTC.

5.4.3 Development and testing of cross-chain smart contracts

Regarding interoperability between different blockchain networks, the ZTC project will conduct in-depth research and develop cross-chain smart contracts (CSCs). This includes developing a complete cross-chain smart contract development framework and tool chain, as well as designing the Cross-chain Communication Protocol (CCP) and Cross-chain Adapter (CA) to provide developers with a A one-stop solution. The ZTC project will establish a testing environment for cross-chain smart contracts to conduct comprehensive tests on the correctness, security and performance of CSCs to ensure their stability and reliability in practical applications.

5.4.4 Developer tools and SDK support

To lower the threshold for developers to develop smart contracts on ZTC, the ZTC project will provide a set of powerful and easy-to-use developer tools and SDK support. These tools include smart contract integrated development environment (IDE), debugging tools (Debugging Tools), testing framework (Testing Framework), as well as detailed documentation and sample code. The ZTC project team will regularly update and maintain these tools to ensure that they are compatible with the latest version of ZTC and provide developers with continuous and stable technical support.

06/Application ecology

6.1 Application scenario analysis

❖ High performance transactions and payments

Based on its high-performance architecture, ZTC has brought revolutionary changes to the fields of transactions and payments. Through its optimized consensus algorithm and distributed ledger technology, ZTC can achieve low-latency, high-throughput transaction processing, providing an ideal solution for high-frequency trading scenarios such as retail payments, cross-border payments, and securities transactions. In the field of retail payments, ZTC's instant confirmation and low-cost features enable consumers and merchants to enjoy a smoother and more efficient payment experience. In the field of cross-border payments, the decentralized nature of ZTC eliminates the intermediary links in traditional cross-border payments, reduces transaction costs and risks, and increases transaction speed. In the field of securities trading, ZTC's high performance and scalability can meet the needs of large-scale transactions and provide investors with a more convenient and secure trading environment.

❖ Decentralized Finance (DeFi) Applications

ZTC’s smart contract platform provides a solid foundation for DeFi applications. Through its efficient and scalable smart contract execution environment, ZTC is able to support various DeFi applications, including lending, asset exchange, derivatives trading, etc. In the field of lending, ZTC's smart contracts can ensure the transparency and fairness of the lending process, while providing low interest rates and flexible repayment methods. In the field of asset exchange, ZTC's smart contract can realize decentralized asset exchange and provide users with a more convenient and secure transaction method. In the field of derivatives trading, ZTC's high performance and scalability can meet the needs of complex derivatives trading and provide investors with richer trading strategies.

❖ Privacy protection and asset security

In the field of blockchain, privacy protection and asset security have always been the issues that users are most concerned about. ZTC provides users with powerful privacy protection capabilities by adopting advanced privacy protection technologies, such as zero-knowledge proofs (ZKPs) and coin mixers. These technologies can ensure the transparency and fairness of transactions while protecting user privacy. In addition, ZTC also adopts highly secure consensus algorithms and encryption technologies, such as consensus algorithms based on sharding technology and advanced encryption algorithms, to ensure the security and stability of the blockchain network. These security measures allow users to conduct transactions and asset management on ZTC with confidence without worrying about privacy leaks and asset security issues.

6.2 Commercial application examples

Specific business use case analysis

- **Retail payments:** As a new digital currency payment method, ZTC can be seamlessly integrated with existing retail payment systems. By integrating ZTC payment functions, retailers can provide users with more flexible and convenient payment methods, while reducing transaction costs and improving payment efficiency. For example, online stores can accept ZTC as a payment method to attract more digital currency users; physical stores can also install payment terminals that support ZTC to facilitate consumers to make digital currency payments.
- **Cross-border payment:** Traditional cross-border payments have many pain points, such as high cost, slow speed, and high risks. ZTC provides a new solution for cross-border payments through its decentralized features and smart contract technology. Through smart contracts and decentralized networks, ZTC can achieve fast, low-cost, and secure cross-border payments. For example, merchants in two different countries can conduct cross-border transactions through ZTC without going through the cumbersome bank transfer and currency exchange process, which greatly improves transaction efficiency and reduces costs.
- **DeFi Lending:**ZTC's smart contract platform can support decentralized lending applications. Users can use their assets as collateral to post borrowing requirements on the platform, and realize automated approval and lending through smart contracts. This lending method has the advantages of low interest rates, high transparency and flexibility, providing users with more convenient and safer lending services. At the same time, smart contracts can also ensure the fairness and transparency of the lending process and avoid the risks of fraud and default in traditional lending.

Partners and integration cases:

ZTC will establish close cooperative relationships with multiple partners to jointly promote the application and development of blockchain technology. Establish cooperative relationships with financial institutions, payment platforms, DeFi projects, etc., and provide users with more comprehensive and high-quality blockchain services by integrating ZTC's technology and services.

6.3 Ecosystem construction

ZTC will establish an active developer community and provide developers with rich resources and support. Provides detailed developer documentation, powerful SDK, sample code, tutorials and online support to help developers quickly get started and efficiently develop ZTC-based applications.

07/Economic ecology

7.1 Issuance plan

ZTC issuance

Token name:ZTC

Total amount:23.3 billion ZTC

Allocation plan:

- **ZTCY inscription exchange (10%):** The initial 10% ZTC will be redeemed through ZTCY inscriptions.
- **Investors generate (20%):** 20% of ZTC will be generated through investment, including from venture capital (VC) and direct user investment.

Team Reserve (10%): The team will reserve 10% of ZTC for project operations and team compensation. This part of the tokens will be gradually unlocked within 5 years, with 2% unlocked every year to ensure the long-term participation and stability of the team.

Liquidity (5%): In order to ensure the liquidity of tokens in the market, 5% of ZTC will be reserved for market circulation and transactions.

Interactive airdrop (5%): Through interactive airdrop activities, users receive additional ZTC rewards.

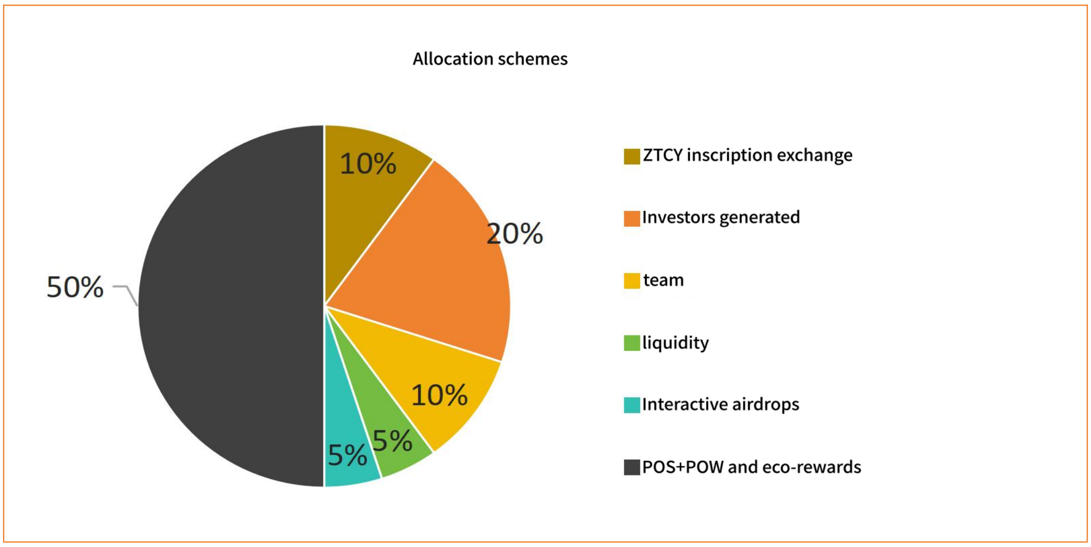
POS+POW and ecological reward output (50%): The remaining 50% ZTC will be rewarded through the Proof of Stake (POS) and Proof of Work (POW) mechanisms.

Team Reserve (10%): The team will reserve 10% of ZTC for project operations and team compensation. This part of the tokens will be gradually unlocked within 5 years, with 2% unlocked every year to ensure the long-term participation and stability of the team.

Liquidity (5%): In order to ensure the liquidity of tokens in the market, 5% of ZTC will be reserved for market circulation and transactions.

Interactive airdrop (5%): Through interactive airdrop activities, users receive additional ZTC rewards.

POS+POW and ecological reward output (50%): The remaining 50% ZTC will be rewarded through the Proof of Stake (POS) and Proof of Work (POW) mechanisms.



7.2 ZTC value

The value of ZTC stems from its unique distribution scheme, extensive ecological strategy, and far-reaching influence. The total amount is set at 23.3 billion, which corresponds to 233 countries and regions around the world. This design not only reflects ZTC's global vision and inclusiveness, but also indicates its potential for widespread application on a global scale. Combining technological innovation, meeting growing ecological needs, and the consensus and support of community members, ZTC has demonstrated significant value growth potential. This global layout and positioning makes ZTC expected to become an important bridge connecting all parts of the world and promoting the popularization and application of blockchain technology.

7.3 ZTC incentives

ZTC will use a variety of incentive mechanisms, including node rewards, developer rewards and community contribution rewards, to attract and motivate more users, developers and partners to participate in the construction and development of the ZTC ecosystem. These incentives will promote ecological prosperity and diversity and bring long-term stable returns to investors and community members.

7.4 ZTC is a completely decentralized and fair launch pad

As a completely decentralized fair launch pad, ZTC aims to prevent LP (liquidity provider) runaway and rat warehouse risks through its unique design and mechanism. In the field of blockchain and digital currency, LP runaway and rat position risks have always been the focus of investors and community members. ZTC reduces these risks by providing investors with a safe and reliable platform through its decentralized nature and fair launch mechanism.

08/Development roadmap

June 2022

The ZTC concept was first proposed by the ZTC Innovation Laboratory as an innovative blockchain solution based on Bitcoin Layer 2;

December 2022

The ZTC project team was established and began detailed discussions and project establishment;

Start building a partnership network, covering Layer 2 technology providers, blockchain development institutions, etc.

May 2023

Conduct in-depth research on the market demand for Layer 2 and conduct technical feasibility analysis;

Continue to recruit professionals in blockchain technology, marketing and other fields to strengthen team building;

September 2023

Form a professional technical team, start to develop ZTC's core technology, establish a ZTC community, and establish connections with blockchain enthusiasts, developers, etc.Complete the first phase of investment in the ZTC project and provide financial support for project development;

December 2023 June 2024

Start building the ZTC service platform, including Layer 2 expansion solutions, smart contract support, etc.;

White paper release;

Release ZTC functional platform;

Launch a developer support plan to encourage developers to develop innovative applications based on the ZTC platform; Attract more users to use ZTC services and improve the ecosystem;

July 2024

Establish cooperative relationships with blockchain investment institutions;

Continue to invest in research and development, optimize the technical performance of ZTC, and improve user experience;

November 2024

Establish and improve ZTC's community governance system, conduct global roadshows, ensure the stable operation and continuous innovation of the project, and start the development of the ZTC public chain V2 version;

January 2025

List ZTC tokens (ZTC) on mainstream exchanges and launch a global operation strategy; expand the market, establish cooperative relationships with more brands and enterprises, and enhance the brand influence of ZTC;

June 2025

Establish cooperative relationships with more blockchain projects and technology suppliers to jointly promote the development of the blockchain industry;

Carry out user education activities to improve users' understanding and ability to use ZTC;

August 2025

Develop V2 ZTC Layer 2 technology to continuously optimize the performance and security of

ZTC;

Explore more ZTC application scenarios;

2026-

Develop a global expansion strategy, set up offices in more countries and regions, and expand market coverage;

Deepen cooperative relationships with existing partners to jointly promote the development of ZTC in the global market;

Participate in social welfare undertakings and enhance the social influence and brand image of ZTC projects;

Carry out cross-industry cooperation to explore the applications and possibilities of ZTC in more fields.

09/Project team

9.1 Foundation

The ZTC Foundation is a non-profit organization registered in Singapore that focuses on promoting the development and application of the Zitcoin (ZTC) blockchain project. As the core supporting organization of the ZTC project, the Foundation is committed to providing a solid guarantee for the long-term development of the ZTC project through various efforts including financial support, technology research and development, and community building. The members of the foundation are composed of experts in the field of blockchain, technology developers, financial practitioners and people from all walks of life who are enthusiastic about the development of blockchain technology. The team members are committed to creating a safe, efficient and scalable blockchain ecosystem. system, bringing a more convenient and secure financial service experience to global users.

9.2 Team member

The ZTC team has more than 20 members, the following are some of them

Y C - CEO

YC is currently the CEO of ZTC and is responsible for the company's overall product development and strategic planning. He has more than 10 years of team management experience and more than 12 years of entrepreneurial experience, and is proficient in emerging industries such as blockchain finance, financial technology and Internet finance. YC once served as an executive in a world-renowned company, entered the blockchain field in 2016, and successfully participated in the launch of multiple blockchain products.

Victor Ma - COO

Victor Ma is currently the chief operating officer of ZTC, responsible for global market operations and business development planning. Based on the company's overall strategic plan, he organizes the formulation of mid- to long-term development plans and promotes the implementation of global strategies and projects. Victor Ma has more than 5 years of operational management experience, focusing on the Internet and blockchain fields. He is good at handling complex operational issues and has established good cooperative relationships with various financial institutions. Victor Ma graduated from PBC College of Tsinghua University in China with a bachelor's degree and worked as a manager in the world's top securities firms.

Anthony - CTO

Anthony is currently the Chief Technology Officer of ZTC, responsible for the architecture design and development of blockchain technology. He is proficient in various mainstream consensus algorithms and proficient in blockchain system development language. Anthony has more than 10 years of experience in Internet game development and blockchain technology, and has successfully participated in the listing of multiple exchanges and digital wallet projects.

Richie -CFO

Richie is responsible for the financial work of ZTC. He has many years of financial management experience. He graduated from a world-renowned financial school. He is good at financial growth and has established good cooperative relationships with government agencies in various countries. He is currently focusing on exploring investment opportunities in the blockchain industry. Served in one of the world's top five accounting firms.

Rison- MM

Rison is responsible for ZTC's global marketing strategy. He has more than 3 years of experience in corporate marketing management and is good at discerning market opportunities and formulating marketing strategies to enhance brand influence and product promotion. Rison is proficient in brand management in the Internet, e-commerce and financial technology fields, and has helped many start-up companies successfully transform their brand images. Possess rich practical experience and the ability to successfully create brand influence.

Austin koch- LIA

Austin Koch is responsible for ZTC's venture capital and new business investments. Before joining ZTC, Austin Koch participated in the design of more than 10 digital currencies and discovered several security vulnerabilities. He was a trustworthy member of the digital currency community. In addition, he is involved in the development of multiple cryptocurrency projects.

Louis Hu- PM

Louis Hu is responsible for ZTC's partnership management, including cooperation with portfolio companies, subsidiaries, investors and extensive networks. Drawing on his extensive experience in venture capital and nonprofit technology advocacy, he brings valuable data, research, and community organizing support to the team to advance emerging technologies. Louis Hu has in-depth research and unique insights into business operation models, as well as professional financial knowledge and rich experience.

Alexander ingold- BD

Alexander ingold is an experienced blockchain developer and enthusiast. He graduated from the computer department of a global QS100 university. Alexander ingold’s expertise and experience provided valuable input into the design of the ZTC project.

Luca-SE

Luca is an experienced blockchain developer and enthusiast who once worked for a world-renowned game company. He has been involved in the blockchain industry since 2016 and has participated in the development of multiple cryptocurrency projects. Luca’s expertise and experience provide valuable technical support for the ZTC project.

Bella-CD

Bella is an experienced designer who has been in the design industry for several years, she has participated in the design of more than dozens of digital currencies, and is responsible for organizing ZTC to review the design plan, clarify the design points and market design needs, and coordinate

Other relevant departments to promote the realization of the goals of the ZTC project.

10/Disclaimer

This document is only used for information transmission, and its content is for reference only and does not constitute a recommendation, inducement or offer for the purchase or sale of stocks or securities of the ZTC platform and its related companies. This document does not constitute any form of transaction, contract or commitment.

In light of unforeseen circumstances, the objectives listed in this white paper are subject to change. Although our team will do its best to achieve all goals in the white paper, all individuals and groups purchasing ZTC should do so at their own risk. As the project progresses, the content of the document may be adjusted accordingly in the new version of the white paper, and the team will make the updated content public through website announcements or new versions of the white paper.

This document is only for use by specific persons who proactively seek project information. It does not constitute any investment advice, nor is it any form of contract or commitment.

ZTC explicitly states that it is not responsible for direct or indirect losses caused by participants, including but not limited to:

1.Once a participant participates in the ZTC token distribution plan, it means that they have fully understood and accepted the project risks and are willing to bear all the consequences themselves. The project team clearly states that it does not provide any promise of return, nor is it responsible for any losses caused directly or indirectly by the project.

2.The tokens involved in this project are only virtual digital codes in the transaction process and do not represent project equity, income rights or control rights.

3.In view of the many uncertainties in digital currency itself (including but not limited to the regulatory environment of digital currencies in various countries, fierce competition in the industry, digital currency technical loopholes, etc.), we cannot ensure the absolute success of the project, and there is a certain risk of failure in the project, and The value of the token may return to zero.

The team will make every effort to achieve the goals mentioned in the document, but due to the existence of force majeure, no complete guarantee can be made. To the maximum extent permitted by law, the team is not responsible for any damages and risks arising from participation in this project, including but not limited to direct or indirect personal damages, loss of business profits, loss of business information or any other economic losses. any liability.