

A Quantum blockChain

Quantum Chain

WHITE PAPER

This white paper explains the concept and technical structure of Quantum Chain, a blockchain mainet based on quantum computing.

BY — Quantum Chain Foundation

CONTACT — contact@quantumchain.it

Quantum Chain leverages the unique characteristics of quantum computing to overcome performance and security challenges that are difficult to address in traditional blockchain systems.

ver 1.00 (09.07.24)

01 Introduction

This document presents the technical design of QUANTUM CHAIN, a cryptocurrency that leverages the performance of quantum computers to perform high-performance computing operations within a mainnet and blockchain token ecosystem. This platform supports the exchange of data across various digital ecosystems on its proprietary blockchain infrastructure, thereby establishing a distributed computing environment where quantum computers act as validators. This setup provides a foundation for various applications within the network to interact with one another.

Quantum computers process information based on the principles of quantum mechanics, using qubits as their fundamental unit of operation. Qubits can exist in a superposition state, allowing them to represent both 0 and 1 simultaneously. This provides exponentially improved parallel processing capabilities compared to traditional binary-based computers. As a result, QUANTUM CHAIN can efficiently perform complex calculations that are challenging for existing computing environments, thereby presenting new possibilities for blockchain technology.

QUANTUM CHAIN is set to incorporate quantum-resistant algorithms to address potential security threats posed by quantum computers. These algorithms are designed to counter the ability of quantum computers to quickly decrypt existing encryption methods, ensuring the security of the network and resolving potential security issues that may arise as quantum computing technology advances. This approach will allow QUANTUM CHAIN to protect the integrity of the network and provide a secure and reliable blockchain environment even in the era of quantum computing.

This system aims to build a next-generation blockchain network by leveraging the exceptional performance of quantum computing. It seeks to address scalability issues within blockchain systems and overcome the limitations of future technologies based on enhanced computing capabilities.

02 Outline

Quantum computing is a new computing paradigm that utilizes the principles of quantum mechanics to process information with qubits, or quantum bits, rather than the traditional bits of 0s and 1s used by classical computers. Unlike classical computing technologies that represent information solely as 0s and 1s, qubits can exist in a superposition state, allowing them to represent both 0 and 1 simultaneously, as well as intermediate states. This superposition enables the storage of significantly larger amounts of information.

Additionally, entanglement refers to the phenomenon where two or more qubits remain connected as a single state, even when they are separated by large distances. This allows for instantaneous information transfer between entangled qubits. Quantum computing leverages the superposition of qubits to perform parallel processing, enabling the simultaneous handling of problems that classical computers must address sequentially.

Quantum computing is recognized as an innovative technology capable of addressing critical global issues such as environmental challenges, agriculture, health, energy, climate, and materials science, based on its immense

performance capabilities. Quantum Chain promises to solve major problems facing our generation by combining the advantages of blockchain and quantum computing technologies. The mission of Quantum Chain is to transcend technological and universal human challenges through the harmonious application of blockchain and quantum computing.

The era of quantum computers is already upon us. IBM is a leader in the field of quantum computing, offering various sizes of quantum processors through the cloud. They provide an open-source framework called Qiskit to support the development of quantum algorithms. Additionally, companies like Microsoft and Amazon are also supporting the development of quantum computer-based applications through their cloud services. The field of quantum computing is poised to reach a level of commercialization within a few years, and it is expected to emerge as a game-changer in the existing Web 2.0 and 3.0 domains due to its high computing performance.

Quantum computing is both a solution to existing computing problems and a disruptor of established rules. In particular, the blockchain industry predominantly relies on algorithms such as RSA and ECC, which are vulnerable to quantum computers. Another mission of Quantum Chain is to establish itself as the most secure blockchain mainnet that can serve as a foundation in a future where quantum computing is implemented.

To achieve this mission, Quantum Chain proposes the adoption of quantum-resistant encryption algorithms standardized by NIST (e.g., Kyber, Dilithium). It emphasizes the necessity of applying these algorithms to the encryption processes of on-chain data. Additionally, by implementing post-quantum cryptography (PQC), Quantum Chain aims to provide a blockchain system that is secure against quantum computer attacks, ensuring the protection of core information and users within the industry.

02-1 The Significance of Quantum Computers in Blockchain

Integrating quantum computers into blockchain systems for data validation represents a groundbreaking advancement in improving the performance, scalability, and security of decentralized networks. By leveraging the unique computational capabilities of quantum computers, many limitations faced by traditional blockchains can be overcome. While the current generation of quantum computers is still in its early stages due to the limited number of qubits, continuous technological advancements will lead to a steady increase in qubit numbers. As a result, blockchain networks will evolve into faster, more scalable, and more secure systems. QUANTUM CHAIN aims to lead these technological advancements, realizing next-generation blockchain performance improvements powered by quantum computing.

1. Revolutionary Improvement in Blockchain Performance

Quantum computers, based on the principles of superposition and entanglement in quantum mechanics, can process data exponentially faster than classical computers. Although their parallel processing capabilities are currently constrained by the limited number of qubits, they are sufficient to meet the requirements of early-stage blockchain networks.

Parallel Validation: Quantum computers can validate multiple transactions simultaneously, maximizing network processing speed.

Efficient Consensus Formation: By optimizing the data validation process, quantum computers reduce consensus formation time and ensure stable network operation, even in high-transaction environments.

Exponential Computational Power: As the number of qubits increases, the parallel computational capabilities of quantum computers grow exponentially. For instance, increasing qubits from 50 to 100 results in a dramatic rise in the number of states, from 2^{50} to 2^{100} .

Improved Transaction Processing Speed: With a higher number of qubits, quantum computers can validate more transactions simultaneously, significantly enhancing blockchain speed and scalability.

2. Supporting Blockchain Ecosystem Scalability

As blockchain use cases and network participants grow, traditional systems face scalability challenges. Quantum computers offer a powerful solution to address these issues.

Large-Scale Data Processing: Quantum computers can perform complex computations simultaneously, enabling seamless large-scale transaction processing and block validation. Also, Quantum validation reduces the computational burden on traditional nodes, increasing network efficiency and reducing energy consumption.

3. Strengthening Security

While blockchain security traditionally relies on classical cryptography, advancements in quantum computing pose a growing threat to these methods. However, integrating quantum computers into blockchain validation processes enhances security.

Quantum Encryption and Validation: Quantum computers provide new encryption algorithms and data validation techniques that surpass traditional methods, ensuring the integrity of the network.

Enhanced Network Resilience: Quantum validation nodes reduce network vulnerabilities and strengthen defenses against malicious attacks.

4. Building a Sustainable Blockchain Environment

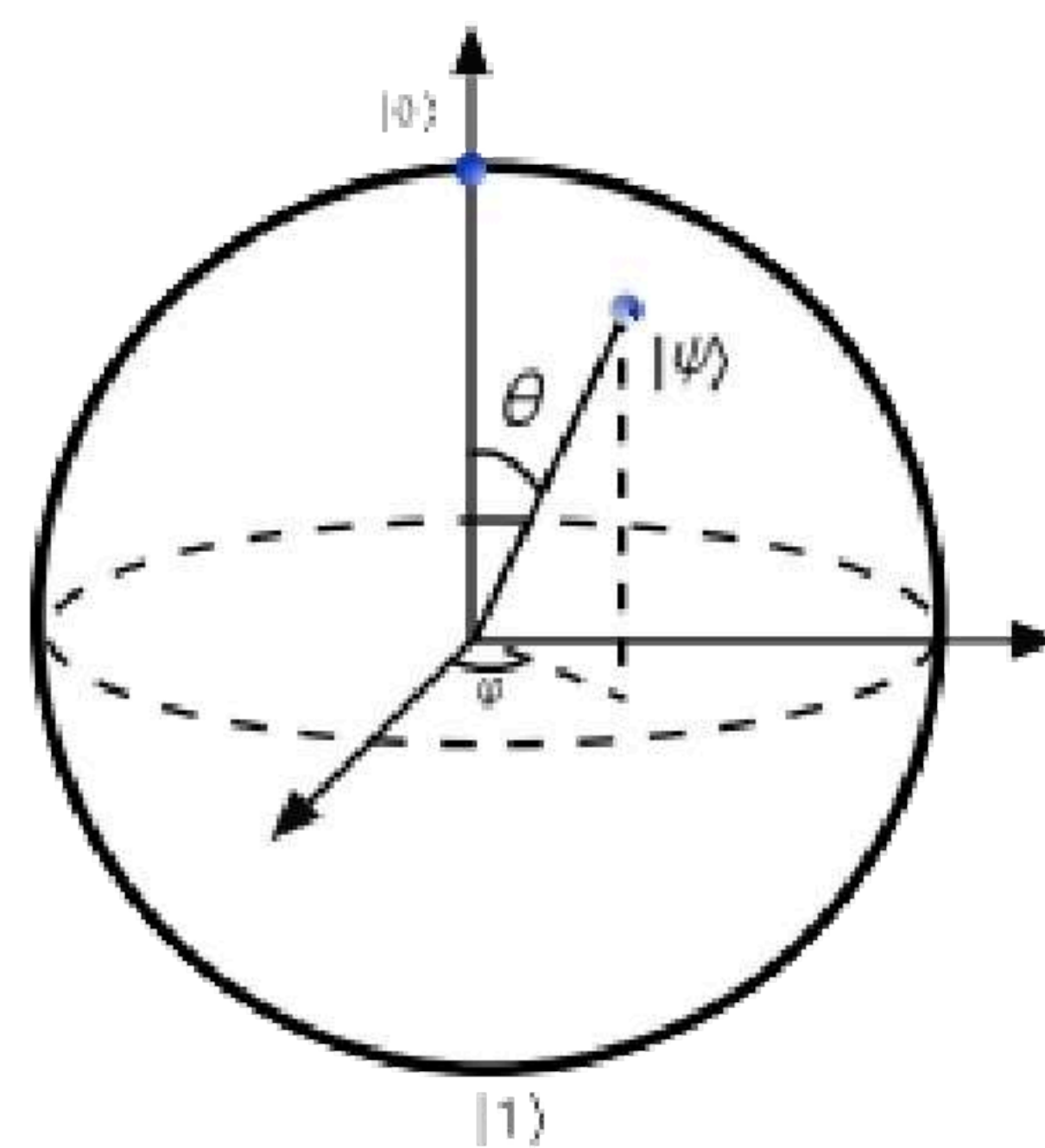
Quantum computer-powered data validation creates an energy-efficient blockchain environment. Unlike the traditional Proof of Work (PoW) model, quantum computers validate significantly more transactions with fewer resources, contributing to environmental sustainability.

Conclusion

Using quantum computers for data validation in blockchain systems holds immense technological, economic, and environmental significance. It stands as a cornerstone of next-generation blockchain technology, unlocking new

possibilities for decentralized networks. With quantum computing, blockchains will evolve into systems that are more scalable, secure, and efficient than ever before.

03 Quantum Technology for Main net Performance Enhancement1 : BlochSuperposition



In quantum mechanics and computing, the Bloch sphere is a geometric representation of the pure state space of a two-level quantum mechanical system (qubit), named after physicist Felix Bloch. The use of the Bloch sphere to represent superposition states is a useful tool for visualizing the state of a qubit in quantum computing.

$$|\psi\rangle = \cos(2\theta)|0\rangle + e^{i\phi}\sin(2\theta)|1\rangle$$

The superposition state of a qubit is generally expressed in the following form. By visually understanding the state of the qubit through the Bloch sphere, it becomes easier to grasp how quantum gates and operations change the state of the qubit. Additionally, quantum computers leverage the phenomenon of superposition, allowing qubits to exist in multiple states simultaneously. A qubit can represent both 0 and 1 at the same time, and this superposition state enables parallel operations, significantly increasing computational speed.

Unlike classical particles, in quantum mechanics, if two states $|A\rangle$ and $|B\rangle$ are valid quantum states, then any linear combination of these states is also a valid quantum state. This linear combination is referred to as a superposition state. If we denote the probability amplitudes for states $|A\rangle$ and $|B\rangle$ as α and β , respectively, the superposition state can be expressed as $\alpha|A\rangle + \beta|B\rangle$.

$$P(A) = |\alpha|^2 = \alpha \cdot \alpha^* = \alpha \times \text{conj}(\alpha)$$

$$P(B) = |\beta|^2 = \beta \cdot \beta^* = \beta \times \text{conj}(\beta)$$

Here, the magnitudes squared of α and β , denoted as $|\alpha|^2$ and $|\beta|^2$, represent the probabilities of measuring the respective states, and the sum of these probabilities equals 1. This superposition effect can maximize operational efficiency within blockchain networks, playing a crucial role, especially in processing complex

smart contracts. The Quantum Chain mainnet is designed to leverage these characteristics of quantum computing, providing superior performance compared to traditional blockchain systems.

04 Quantum Technology for Mainnet Performance Enhancement 2 : Quantum Entanglement

One of the most fascinating phenomena in quantum computing is the ability of two or more quantum systems to become entangled. Entanglement refers to the quantum correlation between quantum systems. When qubits are entangled, the quantum states of the individual subsystems cannot be independently described, resulting in a global system. Two systems are considered entangled if the state of the global system cannot be expressed as a combination of the states of the subsystems. Specifically, if the state of the global system cannot be written as a tensor product of the subsystem states, the two systems are entangled. This indicates that there is a correlation between the systems. Only quantum systems, such as ions, electrons, or superconducting circuits, can exist in superposition states that utilize quantum computing.

Quantum particles like electrons have an intrinsic property of "spin," which can be oriented either "up" or "down." Therefore, the quantum state of an electron is a superposition of these states. Generally, when a quantum system can exist in two quantum states, these states are often referred to as the 0 state and the 1 state to relate more closely to conventional binary computing. Additionally, we can explore examples of quantum entanglement through Bell states. Bell states represent four specific states where two qubits are entangled. These states can be expressed in the following forms.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Quantum computers perform operations using qubits. A qubit can exist in a superposition state, allowing it to simultaneously hold both 0 and 1 states. However, the true potential of quantum computing arises from the entanglement between qubits. Entanglement interlinks the states of multiple qubits, so that when the state of one qubit changes, the states of the entangled qubits change instantaneously as well.

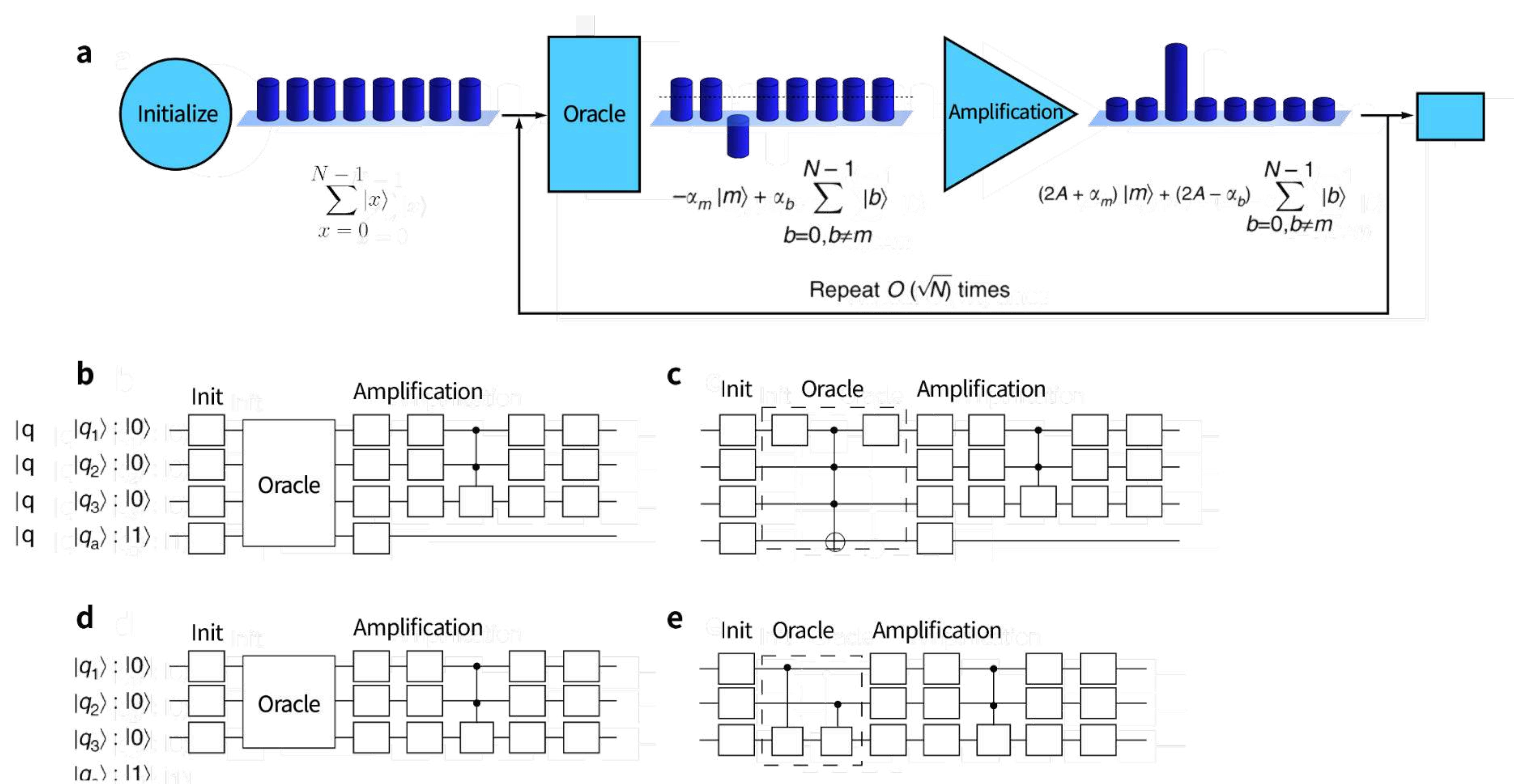
Through this entanglement, quantum computers can perform large-scale calculations in parallel. For example, if (n) qubits are entangled, a quantum computer can simultaneously process (2^n) states. This parallel processing capability is a crucial reason why quantum computers can solve complex problems very quickly. Notable algorithms that leverage entanglement include the following.

04-1 Shor's Algorithm

This algorithm is a quantum algorithm that efficiently performs the factorization of large numbers, a task that would take classical computers billions of years to complete, but can be done by a quantum computer in just a few minutes. By maintaining a strong correlation between qubits through entanglement, the algorithm maximizes its efficiency.

04-2 Grover's Algorithm

This algorithm is a quantum algorithm that efficiently performs the factorization of large numbers, a task that would take classical computers billions of years to complete, but can be done by a quantum computer in just a few minutes. By maintaining a strong correlation between qubits through entanglement, the algorithm maximizes its efficiency.



Grover's algorithm is designed to solve the problem of searching for a specific item in a database, performing the task at a much faster rate than classical methods. It achieves this by allowing parallel exploration of the state space during the search process, thereby increasing the search speed.

In a quantum computer, operations are carried out through quantum gates. Quantum gates are similar to classical logic gates but can maintain and manipulate the superposition and entanglement states of qubits.

For example, the CNOT gate (Controlled NOT gate) is used to create entanglement between two qubits or to manipulate entangled qubits. Various quantum gates, including the CNOT gate, perform complex quantum operations by entangling qubits or manipulating entangled qubits. Through qubits, quantum computers demonstrate computational capabilities that classical computers cannot match.

05 Why a Quantum Mainnet?

The Technological Foundation of a Quantum Mainnet

This article discloses the technical design of Quantum chain, a cryptocurrency that supports a token ecosystem and a decentralized application infrastructure that can perform significant computing operations using quantum superposition and entanglement effects. It provides a decentralized computing infrastructure that enables mutual data exchange between various digital ecosystems on a proprietary blockchain platform, giving mining rights to infrastructure providers and founders who act as verifiers within the network, and a mainnet designed to allow a variety of applications to interact.

Blockchain systems involve two types of participants: users who issue transactions and users who approve transactions. In a simplified environment, the system's design can create inevitable discrimination against certain participants, which in turn generates another conflict that consumes resources for conflict resolution among all elements. These conflicts often arise from the lack of sufficient computing resources. The issues mentioned earlier justify the exploration of solutions that are fundamentally different from the blockchain technology underlying Bitcoin and several other cryptocurrencies. Over the past six years, the rise and success of Bitcoin have demonstrated that blockchain technology holds real value. However, this technology has several drawbacks that prevent it from being used as a universal platform for cryptocurrencies worldwide. Key issues include the performance of the mainnet, whether the encryption methods remain secure in an era where quantum computers are becoming mainstream, and whether it possesses adequate scalability.

The two main issues with blockchain systems are performance degradation and security threats. The scalability problem of blockchain is one of the critical challenges that this technology must address to achieve widespread global adoption. Current blockchain networks experience a rapid decline in throughput when transaction volumes surge, significantly impacting the overall performance of the network. These performance issues pose obstacles to the establishment of blockchain as a global financial and commerce system. Therefore, the future of blockchain technology needs to be redesigned while considering the following factors.

1. Quantum-resistant Cryptography

The development of new cryptographic algorithms that can withstand attacks from quantum computers is essential. This will help maintain the security of blockchain networks and establish a foundation to respond to future technological advancements.

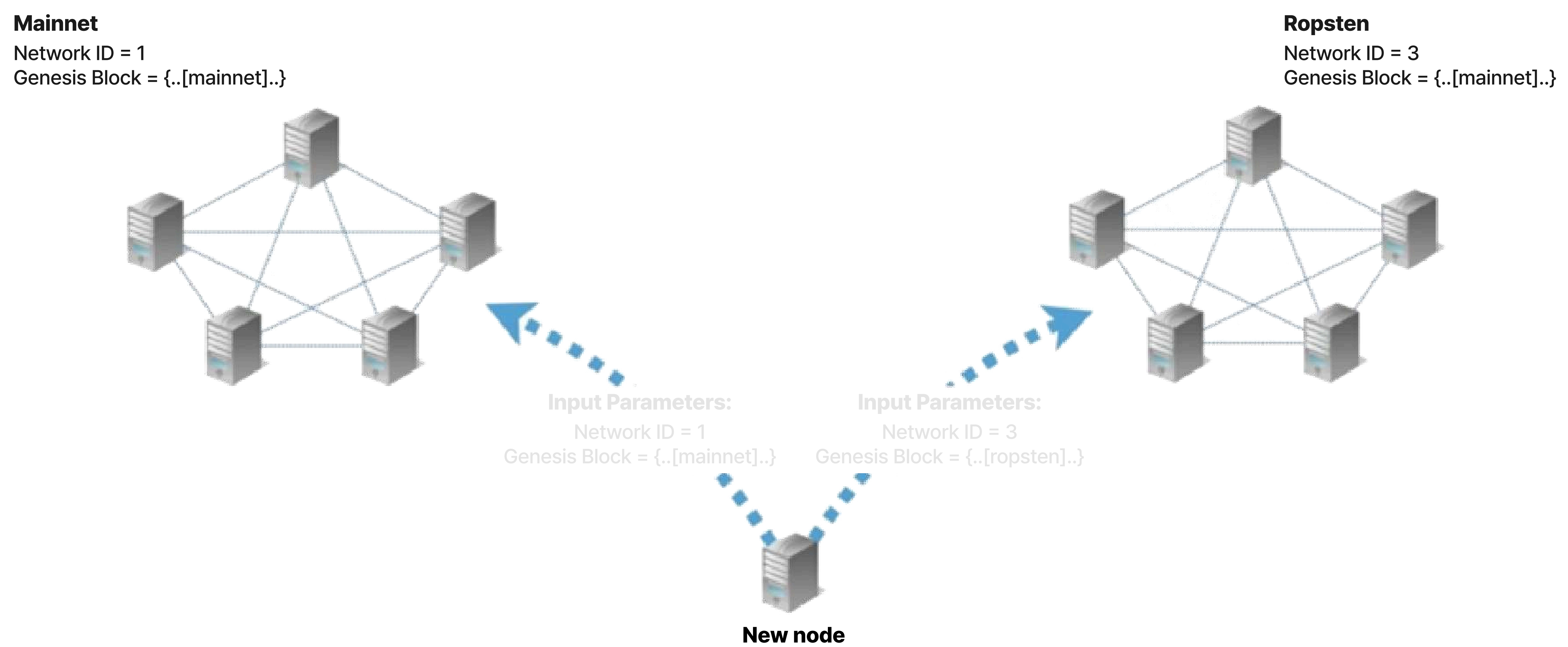
2. Scalability

It is necessary to improve the structure of the blockchain to allow the network to process more transactions quickly. This can be achieved through various technical approaches, such as sharding and off-chain solutions.

3. Energy Efficiency

Current blockchain networks, particularly the Bitcoin network, consume a massive amount of energy. This has been identified as a factor threatening environmental sustainability. Therefore, the development of consensus algorithms

that can enhance energy efficiency is crucial.



4. Governance Model

There is a need for a more efficient and fair governance model to resolve conflicts within the blockchain community and to determine the direction of the network's development. Although it is a decentralized system, transparency and trust must be ensured in the coordination of opinions and decision-making processes among participants.

Ultimately, the advancement of quantum computers poses new threats to existing encryption methods. Most of the encryption techniques currently in use are designed with classical computing environments in mind, and therefore cannot guarantee their safety in an era where quantum computers are widespread. Quantum computers have the ability to quickly decrypt existing encryption algorithms, which presents a serious issue that could undermine the foundations of blockchain systems.

To address these challenges, blockchain technology must evolve to establish itself as a core message in global finance, developing into a future-oriented technology that possesses stability and scalability as a financial asset. This concern and technological challenge have been inspired by the "Chain Network" (SA SEUL) mainnet, and one of the primary goals is to advance and solve the technical challenges previously faced by the Chain Network through quantum computer-based technologies.

This system inherits the philosophy and core principles of the Chain Network, aiming to resolve the scalability and security issues encountered by earlier networks while establishing a more robust and flexible blockchain environment. In particular, it actively leverages improvements in quantum computing to maximize block generation speed and the efficiency of smart contract processing, laying the groundwork for handling more complex computations swiftly.

Through the parallel processing capabilities and entanglement phenomena of quantum computing, this system offers exponentially higher processing speeds compared to existing blockchain networks while emphasizing the maintenance of security. Thus, it aims to realize the ideals of the Chain Network and establish the foundation for next-generation blockchain technology.

06 Consensus Algorithm : Quantum Random Sampling (QRS)

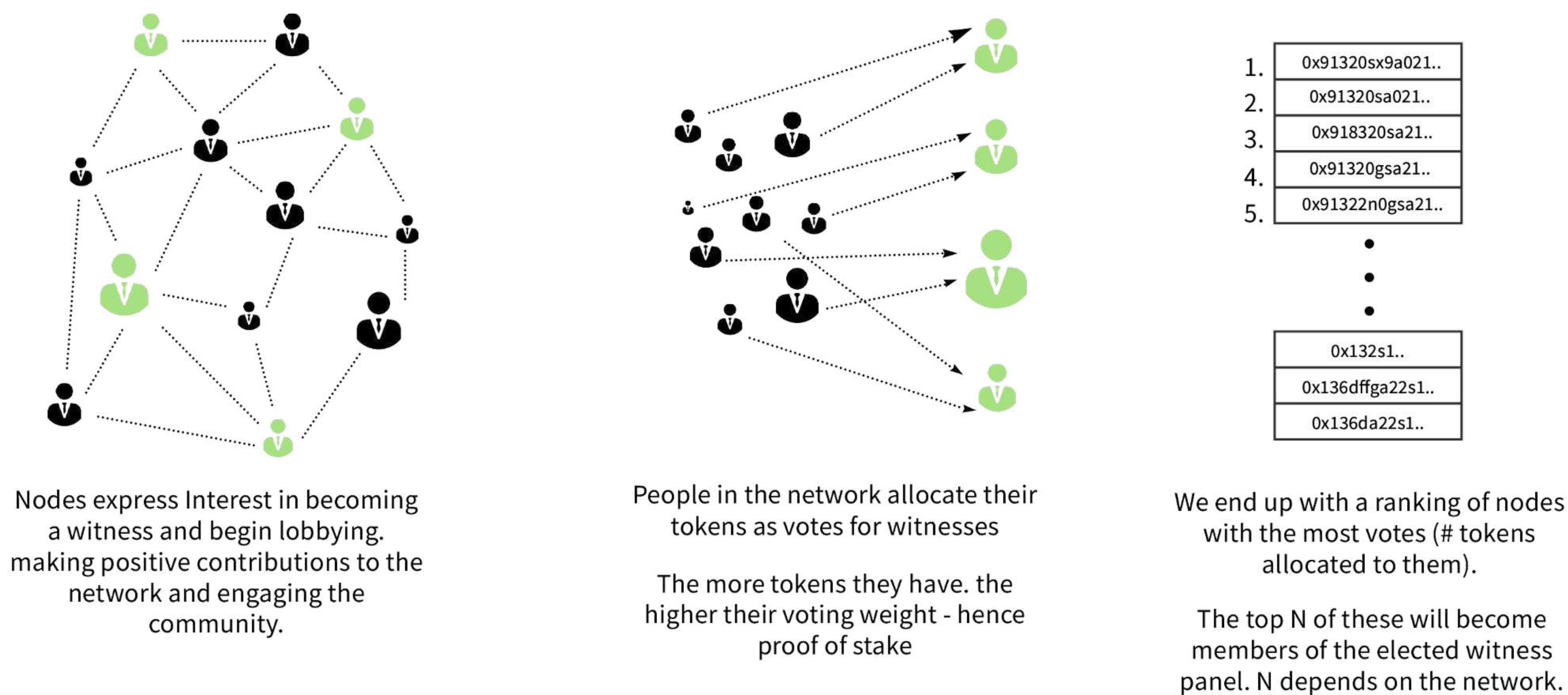
It is a widely proven fact that achieving complete safety (known as finality in the blockchain field) and liveness is impossible. This is the challenge posed by the FLP Impossibility theorem. Safety means that "if consensus has been reached among nodes, any node reviewing the consensus data will find the same value." Liveness signifies that "if there are no issues with the transaction data (transaction or block in the blockchain), consensus will be reached as much as possible within the environment." As the structures of safety and liveness are reinforced, the network consensus algorithm becomes less practical. Therefore, the Practical Byzantine Fault Tolerance (PBFT) algorithm secures safety from a minimal commercialization perspective while allowing for some inefficiency in liveness, enabling consensus to be achieved in various network environments.

Even if there are some nodes that persist in malicious decision-making, the PBFT algorithm ensures the reliability of the consensus reached within the network. Based on this PBFT, we designed the mainnet by adjusting the number of validator nodes to establish a stable consensus method and increase the speed of transactions. The delegated proof-of-stake system can process blockchain transactions more quickly than other consensus algorithms. The proof-of-stake method is overwhelmingly faster than the proof-of-work method and has the potential for broader applications.

Introducing QRS, a result of this exploration: Quantum Random Sampling leverages the unique random sampling capabilities of quantum computers to select validators in a fair and unpredictable manner within the blockchain network, forming an innovative consensus algorithm that is efficient and secure. QRS maximizes block generation and transaction validation by fully utilizing the parallel processing capabilities of quantum computing while focusing on enhancing the security of the network.

1. Network Initialization

The network implemented with the QRS algorithm is designed based on quantum-resistant encryption technology. Each node (participant) is assigned a unique Quantum Key Pair generated by a quantum computer when joining the network. This key pair plays a crucial role in transaction signing, verification, and the consensus process.



2. Random Sampling Process

Whenever a block is generated, the QRS algorithm randomly selects a small number of nodes as validators within the network. This process is carried out as follows:

a. Quantum Sampling

Whenever a block is generated, the QRS algorithm randomly selects a small number of nodes as validators within the network. This process is carried out as follows:

b. Validator Selection

Sampling occurs through the generated random numbers, and the selected nodes participate as validators in transaction verification and block generation. This process is conducted fairly for all nodes in the network, and the unpredictability enhances the security of the network.

3. Transaction Verification and Consensus Formation

The selected validators use a quantum computer to verify transactions. This process is referred to as Proof of Replication (PoR), a concept originally introduced in Filecoin, which proves that data is stored at a specific location. Solana utilizes this concept to verify that data has indeed been stored. Proof of Replication Streaming is a technique used in the Solana blockchain to efficiently handle data storage and verification. This technology focuses on ensuring data integrity within the network while optimizing storage space and reducing resource burdens among nodes. The Quantum chain incorporates parts of this algorithm to operate as a more robust core logic.

a. Proof of Replication (PoRep)

PoRep is a concept originally introduced in Filecoin, which proves that data is stored at a specific location. Solana uses this concept to verify that data has actually been stored.

b. Streaming Method

Subsequently, Solana introduced a streaming method to make the PoRep verification process more efficient. Data is encrypted, and the encrypted data is hashed, followed by random sampling to verify that the data is correctly stored at a specific point in time. This method is designed to handle large volumes of data while increasing verification speed.

c. Signature Verification

The validity of the transaction's signature is verified through the QRS algorithm. Balance verification and double-spending prevention: It checks whether the sender's balance is sufficient and verifies that the transaction has not been used twice.

d. Consensus Formation

Validators transmit the verification results to the network as messages, and consensus is formed when a majority of validators reach the same conclusion through the Quantum Majority algorithm.

4. Block Generation and Propagation

Once consensus is reached, the verified block is added to the blockchain and propagated throughout the network. In this process, the validators who generated the block receive rewards according to the network's incentive structure.

5. Security and Efficiency

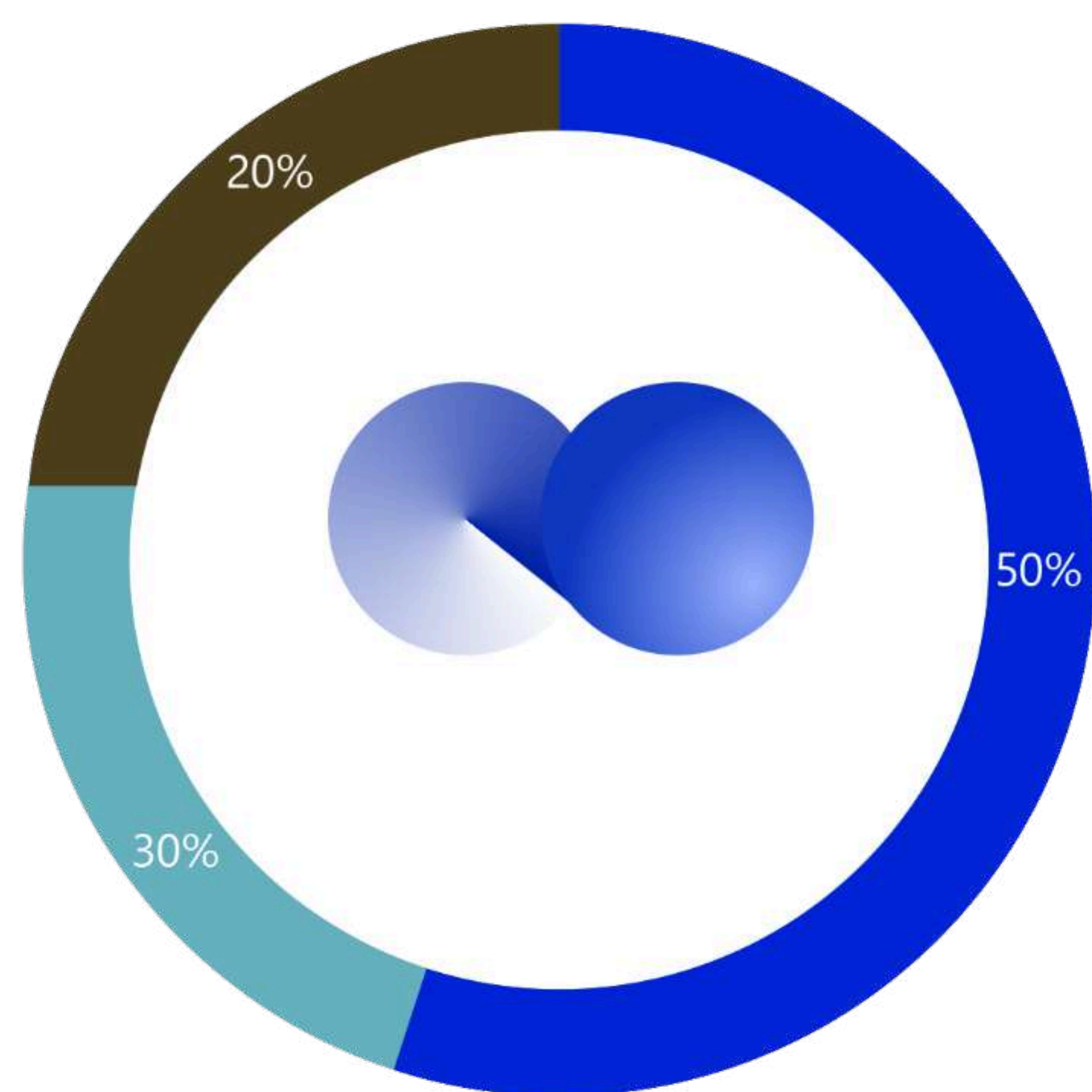
The QRS algorithm maximizes network security by selecting validators in an unpredictable manner through the powerful random sampling capabilities of quantum computers. Communication is protected through quantum-resistant encryption, providing security suitable for the era of quantum computing. Additionally, parallel processing allows for more efficient transaction verification and block generation.

07 QUANTUM CHAIN Distribution

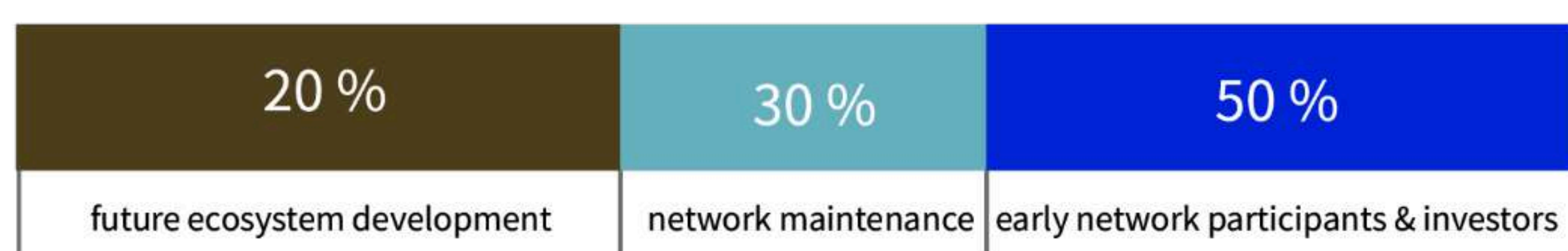
The total issuance of QUANTUM CHAIN is set at 3.5 billion tokens. This fixed supply has been determined since the initial stages of the network and is one of the key elements supporting the token economic model of QUANTUM CHAIN. With a fixed supply, the scarcity of the tokens is ensured, and as the network grows, the value of the tokens will adjust according to the principles of supply and demand.

A total of 3.5 billion coins will be issued, of which 100 million coins will be distributed for ecosystem expansion to activate the initial ecosystem. The remaining 3.4 billion coins will be distributed to users through mining. This distribution is broadly categorized into portions allocated to initial network participants and investors (50 million coins), portions needed for network maintenance and operation (30 million coins), and portions reserved for future ecosystem development (20 million coins).

The goal is to enhance security with a quantum-resistant algorithm and ensure stable network operation in the long term. The issuance and distribution policy of QUANTUM CHAIN follows the fundamental principles of token economics and will adjust liquidity in line with the growth of the blockchain ecosystem.



- early network participants and investors (50 million)
- network maintenance and operations (30 million)
- future ecosystem development (20 million)



QUANTUM CHAIN plans to use 100 million tokens for the initial ecosystem building and activation. This initial supply will be strategically allocated to promote the project's growth and network activation. First, we will list on major cryptocurrency exchanges to secure liquidity in the global market, allowing initial investors and users to trade tokens smoothly.

Additionally, to activate the QUANTUM CHAIN ecosystem early, we will provide incentives to developers and partners to promote the development of various decentralized applications

(DApps) and support the activation of diverse services on the network. Furthermore, we aim to implement a reward program for early community members to encourage user participation and build a decentralized community, thereby expanding the network.

08 DeFiand Quantum Superposition Token Swap System

DeFi has led the dapp revolution since the summer of 2020 and continues to be the most dominant force in terms of held value. In November 2021, the total value locked in DeFi across all blockchains exceeded 204billion. The top 10 DeFi protocols achieved a10–fold expansion with an annual growth rate of 1,700%, 2.6 billion, and the cumulative revenue of the top 10 major protocols reached \$40 million in daily revenue for dapps.

This represents an increase of nearly 30 times compared to 2020. The dApp industry showed significant signs of organic growth in 2021. At the time of writing, over 2.7 million unique active wallets (UAW) connected daily to blockchain dApps hosted on more than 30 blockchain protocols tracked by DappRadar. The number of UAW interacting with dApps increased by 592% compared to 2020. The growth has been steady and sustained.

To concretize the value of DeFi and provide liquidity, a new solution is proposed. This swap is named Quantum Superposition Swap. The Quantum Superposition Swap is a solution that meets demand based on probability when effective demand arises on the supply and demand curve, securing the liquidity of assets by sharing incentives. It overlays asset data from each blockchain and waits in a superposition state where transactions may or may not occur until a transaction takes place. In this state, it generates trades in the form of auctions and creates a pool of assets in a superposition state at the point where demand exceeds supply, adjusting the probabilistic supply rate to be close to 1 over a period. When the probabilistic supply rate reaches 1, the demander acquires the asset, and the providers engage in incentive trading of the frozen bid amount as soon as it becomes available from the pool. Of course, not all

assets in the virtual world are traded in the SWAP. Only those from virtual worlds that can guarantee sufficient trust can deposit assets to prove their "trustworthiness." Initially, the foundation will be responsible for measuring trustworthiness based on criteria, and by the time the beta version is released, it will be refined through community feedback with quantifiable standards.

09 On-chain Data Exchange and Multi-chain Integration on the Mainnet

Multichain is a technology that allows multiple blockchains to interact within a trusted network environment. There are two sophisticated models of multichain. First, there is the digital transaction exchange model, which simply facilitates the interaction of specific transactions on the blockchain. Second, it involves a method of exchanging data by integrating the stored block data and processes within the blockchain. Quantum Chain is convinced that both blockchain interaction technologies are essential for building a trustworthy data-driven ecosystem. The overview is as follows.

Like all other blockchain-based virtual worlds, Quantum Chain utilizes the characteristic of blockchain to record all activities occurring on the network, thereby creating a reliable virtual world. The comprehensive record-keeping and inherent security of blockchain ensure the safety of the virtual world against both internal misconduct and external attacks. Assets in this trustworthy virtual world should not become exclusive privileges that only a few can monopolize. To connect the world in a virtual computing space, it must be an open world that is more accessible, available to everyone, and capable of infinite expansion.

Quantum Chain addresses this by introducing multichain technology. With multiple chains operating simultaneously, security is further enhanced, and Quantum Chain provides interoperability among various chains and the virtual worlds built upon them. As a result, Quantum Chain will serve as a bridge between reality and a trustworthy virtual world, functioning as a decentralized protocol that guarantees value based on real-world assets. It will act as a standard and benchmark for the value of the virtual world and, furthermore, will serve as a connecting point for virtual worlds based on multiple ecosystems. The simultaneous operation of multiple chains strengthens security, while Quantum Chain facilitates interoperability among these chains and the virtual worlds above them.

10 QUANTUM CHAIN Project Roadmap

From the third quarter of 2024, the QUANTUM CHAIN project will begin to implement key stages in order to establish an innovative blockchain ecosystem.

1. Initial Phase (Q3 2024 - Q4 2024)

Primary Quantum Epoch Launch

In the third quarter of 2024, we will initiate the first major development stage of the QUANTUM CHAIN network through its core theme, "Primary Quantum Epoch." During this phase, we will activate the first quantum computer

Completion of Project Concept and Design

We will finalize the core concept of QUANTUM CHAIN and complete the technical design and token economics model. This will clarify the project's vision and goals.

White Paper Release

We will publish a white paper in Q3 2024 that details the vision, technical structure, token distribution, and economic model of QUANTUM CHAIN. This will publicly disclose the project's roadmap and objectives.

Mainnet Beta Launch

In the fourth quarter of 2024, we will launch the mainnet beta, allowing us to test the fundamental features of QUANTUM CHAIN and validate the network's stability and performance. This will enable us to identify and address any technical issues prior to the official mainnet launch.

2. Mainnet Launch and Expansion Phase (Q1 2025 - Q3 2025)

Official Mainnet Launch

In the second quarter of 2025, we will officially launch the QUANTUM CHAIN mainnet. This mainnet will serve as a new blockchain network that utilizes quantum computing to perform validator roles, providing an infrastructure that offers high performance and security simultaneously.

Integration of Quantum-Resistant Algorithms

Alongside the mainnet launch, we will integrate quantum-resistant algorithms into the network to address security threats posed by quantum computers, thereby enhancing the integrity and safety of the network.

Ecosystem Expansion

We will initiate a developer support program to assist in the development and operation of various dApps and smart contracts on the QUANTUM CHAIN network. This will expand the practical usability of the network and invigorate the ecosystem.

Multichain Integration and Swap Function Implementation

Starting in the second quarter of 2025, QUANTUM CHAIN will enhance interoperability with various blockchain networks to support a multichain environment. This will enable asset swaps with other blockchain networks, allowing users to seamlessly move assets across different chains. The swap functionality on QUANTUM CHAIN will provide a platform for rapid and secure asset exchanges.

3. Global Expansion and Community Enhancement (Q4 2025 - Beyond)

Expansion of Global User Base

Starting in the fourth quarter of 2025, we will launch a global marketing campaign to increase awareness of QUANTUM CHAIN in various regions and build a global ecosystem.

Introduction of Community Governance

From 2026 onward, we will implement a governance system that allows the community to participate in key decisions of the network, strengthening the user-centric decentralized network.

Ongoing Technical Upgrades

We will continuously improve performance and security through regular network upgrades that reflect advancements in quantum computing and blockchain technology.

11 Potential Attacks and Threats to the Mainnet

In a blockchain mainnet that uses quantum computing as validators, various attack vectors may exist. Some of these issues stem from the fundamental characteristics of blockchain technology, with critical concerns arising from phenomena such as the Tragedy of the Commons and Eclipse Attacks. These attacks can exploit structural weaknesses in the network or pose potential risks that lead to inefficient use of resources.

1. Tragedy of the Commons

The Tragedy of the Commons refers to a situation in a blockchain network where resources shared by nodes (e.g., network bandwidth, computing power, etc.) are overused, leading to a decline in overall network performance or resource depletion. This issue particularly arises when network participants seek to maximize their own benefits. While each node may act rationally on an individual basis, collectively, this can result in the exhaustion of network resources and a decrease in overall system efficiency.

For example, if quantum computer validators excessively utilize resources to maximize their verification capabilities while generating blocks, there is a risk of depleting the total resources of the network. Such resource consumption can negatively impact the entire network, potentially leading to transaction delays, increased verification costs, and even instability within the network.

2. Eclipse Attack

Eclipse Attack is an attack that isolates specific nodes within the network by blocking or controlling the connections of all peer nodes associated with that node. This attack can lead to the isolated node making incorrect decisions based on false information, negatively impacting the network's consensus process.

For example, a quantum computer validator may be isolated from the network, or a malicious actor may isolate such nodes, causing them to validate incorrect transactions or generate inaccurate blocks. This can undermine the consistency of the network and pose serious risks to the overall integrity of the blockchain.

3. Excessive Staking Concentration

In a blockchain network, a situation where specific nodes monopolize the validator role through excessive staking can undermine the decentralization of the network and grant excessive power to a small number of nodes. This can lead to governance attacks or security vulnerabilities.

For example, if certain validators maximize their staking using quantum computers and monopolize the majority of the network's validation, a few participants may gain control over the entire network, compromising the fairness and principles of decentralization. This can also increase the risk of a 51% attack.

4. Resource Exhaustion Attack

Attackers can deplete network resources by sending excessive transactions or executing numerous smart contracts that require complex computations, thereby exhausting the network's processing capacity. Such attacks can slow down the network's processing speed, delaying the handling of legitimate transactions and ultimately threatening the stability of the network.

For example, a scenario could involve exploiting the computational power of quantum computers to continuously request complex operations from the network or generating large amounts of transaction spam to paralyze the network. This not only reduces the efficiency of the blockchain but can also severely degrade the user experience.

5. Staking Influence Attack

In a Proof of Stake (PoS) system, if certain nodes hold excessive stakes, they can exert disproportionate influence over the network's consensus process. This can create a situation where a specific group is able to dictate network policies.

For example, if certain validators concentrate their stakes within the network, they could leverage the computational power of quantum computers to exert excessive influence in the consensus process. This can negatively impact the democratic decision-making process of the network and pose risks of centralization.

12 Mainnet Network Layer

1. Network Layer

The network layer is responsible for communication among participating nodes in the blockchain. This layer propagates transactions and blocks throughout the network and manages message delivery between nodes. The network layer consists of the following elements:

P2P Network

Composed of a decentralized peer-to-peer (P2P) network where all nodes hold equal status and exchange transactions and blocks with each other.

Node Discovery and Connection

Includes mechanisms for discovering new nodes within the network and maintaining connections with existing nodes.

Network Protocol

Defines communication protocols for the propagation of transactions and blocks, validation requests, and consensus information exchange.

2. Consensus Layer

The consensus layer is where the core consensus algorithm of the blockchain is executed. In this layer, the validity of transactions is verified, and a consensus process is carried out to add new blocks to the network. The consensus

layer of this mainnet is based on the Quantum Random Sampling (QRS) algorithm, with the following key components:

Validator Nodes

Nodes randomly selected by the QRS algorithm validate transactions and generate blocks.

Quantum Sampling

Utilizes the random sampling capabilities of quantum computers to select validators, resulting in fair and unpredictable consensus.

Quantum-Resistant Majority Voting

Consensus is formed based on the results of multiple validators, applying the principle of majority voting to finalize the consensus when it is reached.

3. Data Storage Layer

The data storage layer is responsible for securely storing all transaction and block data within the blockchain network. This layer is designed to ensure the integrity, accessibility, and scalability of the data. The main components include:

Distributed Ledger

A database of the blockchain that is distributed across all nodes, with each node holding the complete blockchain data.

Data Structure

Utilizes cryptographic data structures such as Merkle Trees to maintain the connectivity between blocks and ensure the integrity of the data.

Snapshots

Periodically saves the state of the network as snapshots to reduce data recovery and verification times.

4. Application Layer

The application layer supports smart contracts and decentralized applications (DApps) that operate on the blockchain network. This layer provides various interfaces and tools to enable developers and users to leverage the functionalities of the blockchain.

Smart Contract Engine

Supports the execution of smart contracts and efficiently handles complex computations utilizing quantum computers.

API and SDK

Provides interfaces that assist developers in building DApps on the blockchain and interacting with the blockchain..

User Interface (UI)

Includes front-end interfaces that help end users access and use blockchain applications.

5. Security Layer

The security layer is responsible for ensuring the security of data and communications across all layers of the network. In response to new security threats posed by the emergence of quantum computers, this layer implements various security mechanisms, including quantum-resistant encryption technologies.

Quantum-Resistant Encryption

Utilizes encryption techniques capable of withstanding attacks from quantum computers to protect transaction signatures and communications between nodes.

Access Control

Manages permissions and access controls to prevent unauthorized access to the network.

Intrusion Detection System (IDS)

Monitors for abnormal activities on the network and detects potential attacks in real-time.



Legal Rights

This document has been prepared by the Digital Asset Division of Quantum Chain (hereinafter referred to as the "Project") and is not intended to induce or recommend investments. It is provided solely for informational purposes to assist investors in their investment judgments. While this document is based on reliable information at the time of writing, it may contain errors and differing information. Therefore, we do not guarantee the accuracy or completeness under any circumstances. No one, including the issuer of this document, guarantees the value or payment of this digital asset. The value of this digital asset may fluctuate significantly due to market conditions, technological changes, regulatory trends, and other factors. All content in this document may differ from our official opinions. Additionally, we have not provided this document to any third party prior to its public release. Investing in digital assets may result in a loss of principal in some cases. We accept no responsibility for any investment outcomes resulting from the information provided. This document cannot be used as evidence of legal liability regarding the investment results of customers under any circumstances. The copyright of this document belongs to the Project, and it may not be reproduced, modified, or redistributed in any form without the Project's consent.