
QuarkChain
www.quarkchain.io

QuarkChain - A High-Capacity Peer-to-Peer Transactional System

QuarkChain Foundation

Version 0.3.2

Executive Summary

Recently, distributed ledger technologies -- decentralized and trustless blockchains (e.g. Bitcoin, Ethereum), has started rewiring the nature of our current economy, communications, and knowledge. As the global financial transaction volume in all electronic payments grows, the low capacity of the current blockchain-based networks cannot cover the world's commerce anytime. However, a simple pursuit of scalability usually sacrifices decentralization and security. Therefore, the ultimate goal of blockchain is to extend the scalability as high as possible while keeping security and decentralization in an appropriate level.

QuarkChain is an innovative permissionless blockchain architecture that aims to meet the global-wise commercial standard. It provides a secure, decentralized, and scalable blockchain solution to deliver 1,000,000+ on-chain TPS. The main features of QuarkChain are:

1. Reshardable two-layered blockchain: QuarkChain consists of two layers of blockchains. We apply elastic sharding blockchains (shards) as the first layer, and a root blockchain as the second layer that confirms the blocks from the first layer. The second layer is flexible to be resharded as needed without changing the root layer.

2. Guaranteed security by market-driven collaborative mining: To ensure the security of all transactions, a game-theoretic framework is designed for incentives, where at least 50% of overall hash powers are allocated to the root chain to prevent double spending attack on any transactions.

3. Anti-centralized horizontal scalability: In any blockchain network with a high TPS, a super-full node can be extremely expensive, which encourages centralization. In contrast, QuarkChain allows multiple cheap nodes forming a cluster to replace a super-full node.

4. Efficient cross-shard transactions: Cross-shard transactions in QuarkChain can be issued at any time, and confirmed in minutes. The speed of cross-shard transactions increases linearly as the number of shards increases.

5. Simple account management: There is only one account needed for the entire blockchains (shards) in QuarkChain. All cryptocurrencies from different shards are stored in one smart wallet.

Table of Contents

1. Motivations and Vision

1.1 Overview of Blockchain

Back to 1990's, Kevin Kelly already alerted the world to the advent of widespread encryption -- "crypto-anarchy: encryption always wins." "Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy." said by Tim May, a retired Intel physicist (cited from Out of Control). Just as May and Kelly predicted, since the word "blockchain" was coined in the original source code of Bitcoin in 2008, the crypto-era has broken out.

In the past two years, many companies have looked into blockchain technology. Almost every major financial institution in the world is doing blockchain research at the moment. For example, in 2016, the Sony Global Education division of the company has developed technology that uses the blockchain to house educational data that can be securely shared with other services and third parties. Fig. 1 shows that since late 2017, there is a huge jump of the number of transaction requests in Ethereum sytem. This demands actually will keep increasing since more and more applications are/will be developing in the near future.

Fig.1 Transaction fee per day in Ethereum rises sharply (47 times higher than six months ago), due to a huge number of transaction requests.(source:etherscan.io).

Harvard Business Review

"We're now in the midst of another quiet revolution: blockchain"

Said by Vinay Gupta in Harvard Business Review.

1.2 The Generations of Blockchain Technology

Bitcoin is the first major currency experiment of blockchain. Although its market cap hangs around $166 billion dollars, it has been using by millions of people for payments and remittances market. The blockchain technology under bitcoin is called the first generation.

The second generation of blockchain technology is led by Ethereum. Ethrereum developed "smart contract" which made blockchain allow not only the cash-like tokens but also financial instruments, like loans or bonds. The ethereum smart contract platform now has a market cap of around 84 billion dollars.

Another cutting edge innovation of blockchain is called "proof of stake (POS)". Current generation blockchains are mostly secured by "proof of work (POW)," which requires significant amount of hash power (and thus electricity) these days and is not energy efficient. In contrast, the POS systems assign the block reward to the holder of tokens proportionally, which significantly reduce the amount of energy to mine a block and is much more economically efficient.

As the demands increase, as we have shown in Fig. 1, another issue facing blockchain is scalability. At the beginning, in the blockchain world, every computer in the network processes every transaction. Although the decentralized and trustless blockchain protocols (e.g. Bitcoin, Ethereum) encompass the global financial transaction volume in all electronic payment today, its low capacity, more specifically 10-30 transactions per second (TPS), cannot cover the world's commerce anytime. In contrast, Visa claims to have 56,000 TPS on its network, while Alipay has achieved 200,000+ peak TPS in November 2017. The scalability problem of the current blockchain-based networks poses significant limits for their extensive applications. How to scale up blockchain TPS without compromising its security and decentralization remains elusive.

1.3 QuarkChain Vision

QuarkChain introduces a groundbreaking innovative permissionless blockchain architecture that aims to meet the global-wise commercial standard. The main idea of QuarkChain was inspired by our extensive experience in developing powerful large-scale distributed systems in centralized world that handles billions of TPS. We manage to apply the technologies on blockchain to create our unique solution on blockchain scalability problem. The solution aims to largely expand the boundaries of blockchain usability without damaging its safety and decentralization features.

We are helping to move blockchain into the next generation by increasing the current TPS thousands to millions folds higher while maintaining security or decentralization. The network we are building is free of congestion, and thus affordable for everyone with different purposes. We envision such a network applied to every industry that demands higher TPS, and encourage these industries to recognize our blockchain tool as a game-changer in the near future. Ultimately, QuarkChain aims to build a seamless platform to support distributed social media, high frequency trading, Internet of Things (IoT), gaming, and financial payments.

2. The Challenges of Blockchain

The three main challenges of a blockchain: security, decentralization, and scaling-out.

2.1 Security Issue

As a transactional platform, the first priority is always the security. A blockchain, as the name implies, is a chain of digitally connected "blocks". This makes it have some inherent characteristics that provide means of security.

First, the blocks are linked. This makes it difficult to tamper with a single record because a hacker would need to change the block containing that record as well as those linked to it to avoid detection.

Second, the transactions/records on a blockchain are secured through cryptography. Network clients have their own private keys that are assigned to the transactions they make and act as a personal digital signature. If a record is altered, the signature will become invalid and the peer network will know right away that something has happened. Early notification is crucial to preventing further damage.

Third, blockchains are decentralized and distributed across p2p networks that are continually updated and kept in sync with a specific consensus (e.g. POW or POS). A POW-based blockchain would require at least a 51 percent hash power of the network to perform double-spending attack that could revert any transaction. Such an attack highly depends on how decentralization the network is, i.e., the more the blockchain is decentralized, the harder the attack can be performed. If the blockchain is sufficiently decentralized, reaching more than 51% hash power will be extremely costly for a single entity (a miner or an owner of a mining pool).

Even though blockchain has these inherent properties that provide security, there still exist vulnerabilities, ill intentions, and malicious attacks that need to be considered when one selects the platform.

2.2 Decentralization Issue

Since 2013, many decentralized trading platforms have been developed. Different from centralized case, decentralized storage and trading allow for drastic reductions in pricing, so that any company or even person, not just the big ones, can leverage the technology. As we mentioned, decentralization also gives blockchain security. However, decentralization is also being challenged these days. E.g., a lot of mining pools are formed for POW-based blockchain so that a weak miner is able to collect its proportional reward in a timely manner instead of waiting for a long period to collect a block reward. The mining pool encourages centralization and becomes a risk of decentralized POW blockchain. For example, as of 2013 top six mining pools consist of 75% of overall Bitcoin hashing power.

2.3 Scalability Issue

In the following, we review the existing approaches for scalability issue.

2.3.1 Multiple Blockchains

One approach to tackle the scalability problem is to run multiple blockchains independently (e.g., Bitcoin, Litecoin, BCH, Ethereum), and thus the system capacity is enhanced as the number of blockchains increases. There are several limitations of doing this. If two blockchains use the same hash algorithm, the hash power can be unbalanced and will make them vulnerable to double-spending attack, reverse transaction and strategic mining attacks. Having multiple blockchains will also limit cross-chain transactions. A centralized cryptocurrency exchange is a common way to make cross-chain transactions. Yet it becomes possibly the least secure place for cryptocurrency, as numerous cyberattacks on exchanges have been reported. Also, transactions on exchange come with additional transaction fees and longer processing time. Users would also need to maintain several accounts or/and addresses for cross-chain transactions, which introduces private key management issues and further security concerns.

2.3.2 Lightning Network

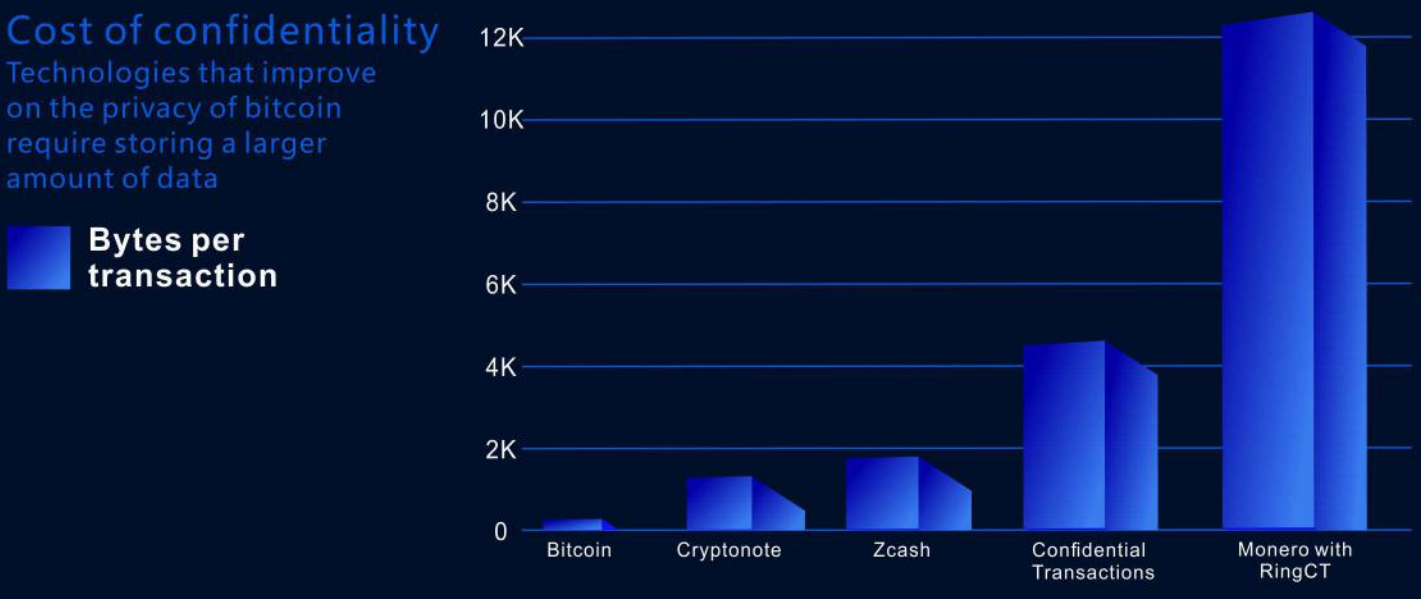
Another approach to alleviate the blockchain scalability problem is by Lightning Network. The basic idea is to defer frequent transactions among a fixed group of parties until all parties are finalized with the transactions. Then one of the parties would just post the final result without incurring multiple historical transactions on chain. A lightning network generally requires two transactions to create/destroy a payment channel, which accepts off-chain transactions. The number of off-chain TPS could be infinite in theory. However, the Lightning Network is only suitable for frequent transactions among a fixed group of parties, while it is inefficient if a user's transaction target is random and happens sporadically. Transparency is another concern because transactions are tracked through lightning channels rather than the main blockchain. Some off-chain solutions rely on trusted third parties, such as Paypal or Alipay with blockchain features. This prompts us to ask if it is necessary to build another centralized payment method because there are already many out there.

2.3.3 Sharding

Sharding refers to horizontal partition of data to break a database into smaller parts. It is one of the most common ways in centralized systems to address the scalability problem. For instance, BigTable and cassendra are two examples in the non-blockchain world to be born to solve large throughput issues. Notably, Ethereum has adopted Sharding technology to scale up, and its phase one development is near completion. However, to adopt sharding on an existing blockchain is complicated, and it is estimated to have 3 to 5 more years to go before Ethereum can fully support other fundamental sharding features, such as cross-shard transactions. The main challenges for sharding include cross-shard transactions, security issues like single shard take-over, and further scalability issues. There are also different proposals such as OmniLedger which claims to reach about 100,000 TPS by introducing intricate consensus protocols. In some other cases, a user' s account is partitioned by introducing sharding; as a result, users may end up having multiple accounts in order to make transactions with others.

2.4 Tradeoffs

Although security, decentralization, and scalability are all important for blockchain, there are some tradeoffs among them. As shown in Fig. 2, if one wants to increase the security/privacy, a larger amount of data are needed for each transaction. This means lower transaction speed and larger storage.



Source:Danny Yang,Jack Gvigan,Zooko Wilcox,"Survey of Confidentiality and Privacy Preserving Technologies for Blockchains,"R3,Nov.14,2016

Fig. 2 Illustration of the tradeoff between security and scalability (TPS)

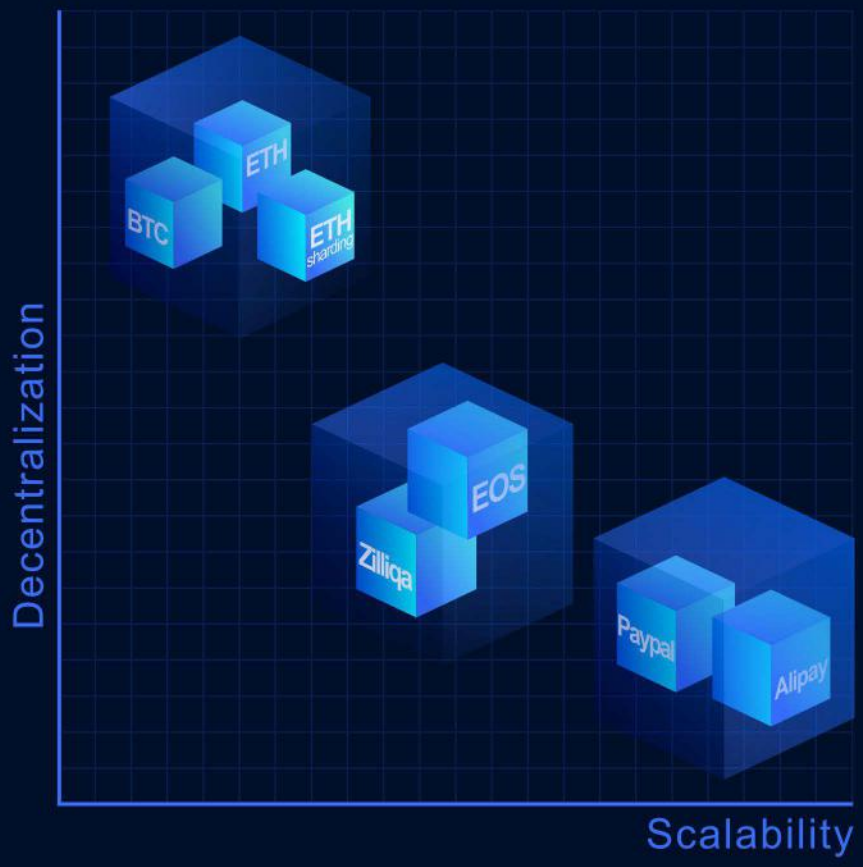


Illustration of tradeoffs between decentralization and scalability

Since the demands have increased tremendously, the ultimate goal of blockchain is to extend the scalability as high as possible while keeping security and decentralization in an appropriate level.

3. QuarkChain Technology

3.1 Design Principle

QuarkChain's design is based on the following principles:

- Enhancing the scalability while guaranteeing security and decentralization
- Enabling seamless cross-shard transaction for user quality of experience (QoE)
- Simple account management for clients
- Open standard to support various Dapp
- Incentive-driven eco-system

3.2 System Architecture

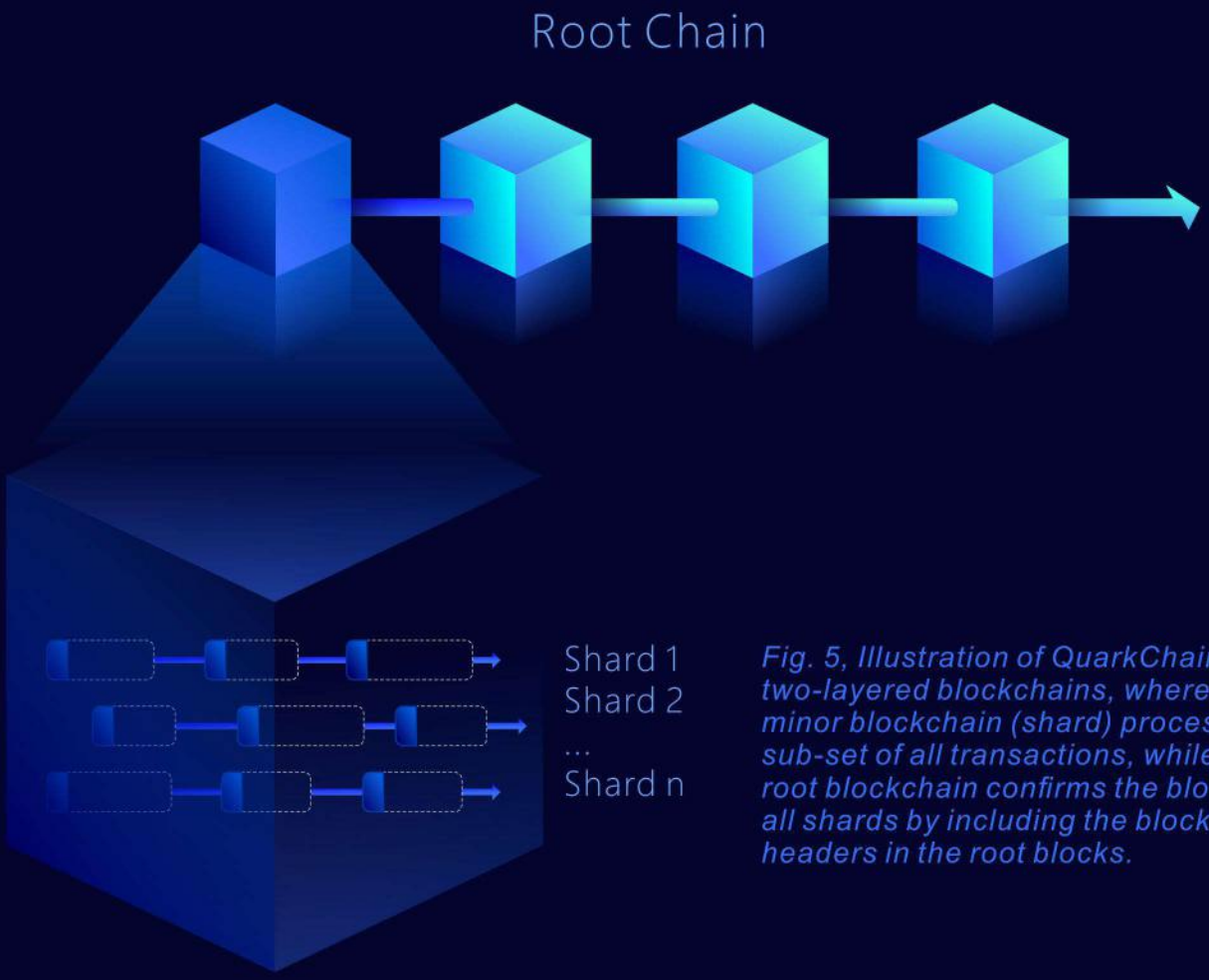


Fig. 5, Illustration of QuarkChain's two-layered blockchains, where each minor blockchain (shard) processes a sub-set of all transactions, while the root blockchain confirms the blocks in all shards by including the block headers in the root blocks.

For current blockchain technology, there are two basic functionalities in each block within the chains:

- Ledger, which includes current ledge state, performs transactions, and records results. To be data-intensive is the key property of a ledger – both current ledger and transactions details including source, destination, amount, execution code, etc, need to be maintained. The limited size of data that can be packed into a block is one of the bottleneck of current blockchains.

- Confirmation, which confirms the result of the transactions from ledger and then mines the block to reach desired difficulty (PoW). This ensures an attacker is economically inefficient to revert a transaction by mining another fork. Confirmation itself is a computational-intensive task.

Based on the observation, QuarkChain adopts the divide-and-conquer idea to separate the two main functions in two layers and thus enhance the scalability while guaranteeing the security. The detailed design is given as follows.

- QuarkChain contains an elastic sharding blockchain layer, which contains a list of minor blockchains (shards). Each shard processes a sub-set of all transactions independently, Therefore, as the number of shards increases, shards can process more transactions concurrently. As a result, the system capacity increases as the number of shards increases.

- QuarkChain has a root blockchain (rootchain) that confirms all blocks from sharded blockchains. The root blockchain does not process any transactions (since it is not economically efficient), but its block has sufficiently strong difficulty so that reverting any transaction, i.e., the transactions in root blockchain, is not economically efficient.

- QuarkChain network is also designed to support additional shards in an active network. Adding more shards is easy and fast, while users barely sense this (the users may feel faster processing of transactions if the network is congested before adding shards).

	Chain Name	Block Name	Interval	Main Functionalities
Rootchain layer	Rootchain	Root block	In minutes	Confirmation
Sharding layer	Shard	Minor block	In seconds	Ledger

Table 1, Structure of QuarkChain

3.3 Collaborative Mining

The goal of collaborative mining is to design incentive mechanisms and difficulty algorithms so that

- Hash powers are incentivized to distribute evenly among shards. This ensures that all shards are mined evenly and thus the system throughput (i.e., TPS) increases as the number of shards increases.
- The root chain has a significant large portion (over 50%) of hash power over the whole hash power of the network. This prevents double spending attack, and a malicious miner needs at least 50% * 50% = 25% power to perform an attack.

Note that a QuarkChain network has several minor blockchains (shards) and one root blockchain. Each blockchain offers different rewards and difficulties. Miners could choose any blockchain at an optimal price of their hash power. This creates an open market economic model, where a blockchain is a seller with goods being the block reward, while a miner is a buyer with hash power being their currency. We would like to design a marketing model so that even though each party in the market pursues their own interests, the collective behaviors of each party could benefit all.

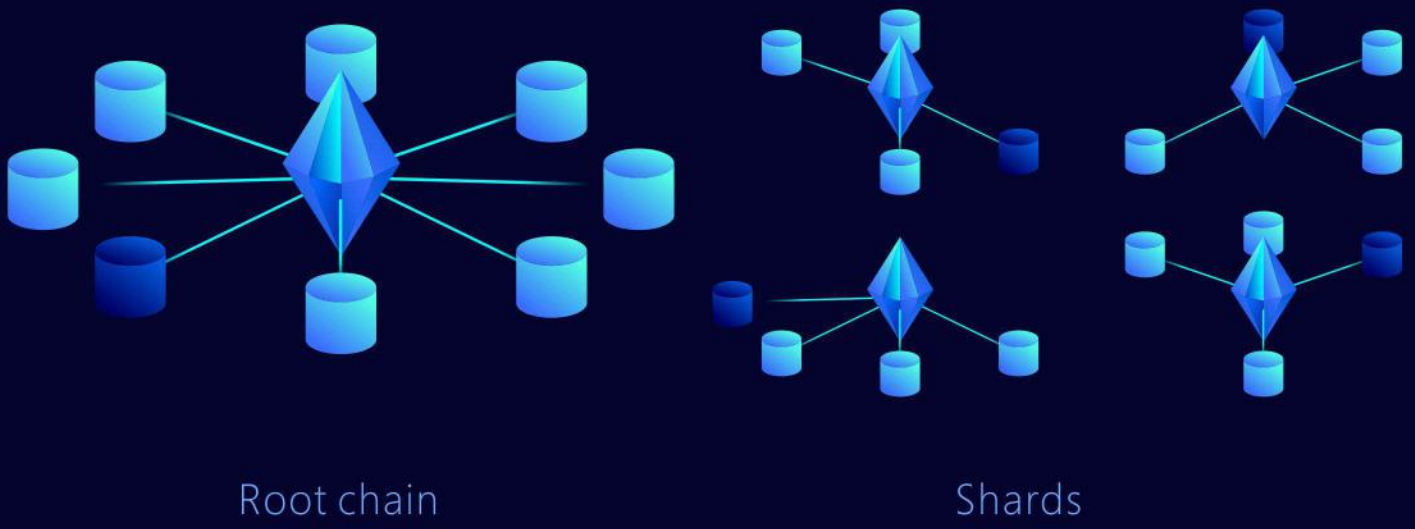


Fig 3. Illustration of collaborative mining, where the blocks in root chain have sufficiently large reward and difficulty to protect the blocks (and thus transactions) in all shards, while all shards are incentivized to have even hash powers.

3.4 Early Verification of QuarkChain Network

Since a QuarkChain system is sophisticated and highly dynamic, an analytic solution could be hardly available. To design such a system to achieve our goals, we resort to network simulation to simulate a 18-node and 8-shard QuarkChain network. This allows us to verify our incentive mechanism and difficulty algorithm in early stage.

```
====================================
Node 1, rewards 2926100
Node 2, rewards 2683100
Node 3, rewards 50600
Node 4, rewards 13500
Node 5, rewards 13300
Node 6, rewards 27000
Node 7, rewards 25800
Node 8, rewards 27700
Node 9, rewards 50100
Node 10, rewards 31300
Node 11, rewards 37200
Node 12, rewards 15500
Node 13, rewards 50200
Node 14, rewards 37600
Node 15, rewards 13100
Node 16, rewards 25300
Node 17, rewards 14200
Node 18, rewards 37900
Powerful/weak rewards ratio: 11.93
------------------------------------
Major chain height 249, reward 11400, work 1642250.81, blocks interval 147.99
Minor chain 0, height 3820, work 15352.94, block interval 9.65
Minor chain 1, height 3815, work 15371.62, block interval 9.66
Minor chain 2, height 3823, work 15287.76, block interval 9.64
Minor chain 3, height 3796, work 15117.48, block interval 9.71
Minor chain 4, height 3803, work 15202.11, block interval 9.69
Minor chain 5, height 3794, work 15223.01, block interval 9.71
Minor chain 6, height 3809, work 15293.13, block interval 9.67
Minor chain 7, height 3793, work 15245.74, block interval 9.72
====================================
```

Fig. 4 illustrates a snapshot of simulation results of collaborative mining. There are 18 miners (nodes) in the simulation, where two miners have 100x hash power than the rest of 16 miners.

The QuarkChain system has 8 minor blockchains with target block duration 10s and a root blockchain with target block duration 150s. Some interesting comments are discussed as follows:

- The heights of all minor blockchains are about 3800s, and they are very close to each other. In addition, all of them have similar work (i.e., the expected hashes to generate a block), and their block intervals are very close to 10s. This means that all minor blockchains are mined evenly and thus the system throughput is about 8x more than the single shard case.

- The root blockchain's work is about 1.6M, which is close to our expectation 1.8M (half of the hash power of the network because all minor chains have 15K work every 10 seconds, and a root blockchain block rate is about 15 times longer than the minor chains).

4. QuarkChain Positioning in Blockchain Society

QuarkChain reveals a brand new path for blockchain design. In this section, we discuss its relationship with other existing ones and position it in the blockchain society.

4.1 Relationship of QuarkChain with Single-Blockchain Systems or Multiple-Blockchain Systems

The QuarkChain's 50% hash power allocation on the root chain is reconfigurable (e.g., 25% or 75%). By adjusting the hash power, the QuarkChain can resemble existing blockchain systems.

- If the hash power of the root chain is 100%, then the QuarkChain system becomes a single-blockchain system as there is no miner on shards and all miners will only mine the root chain and weak miners may join mining pool. In addition, the root chain could include as much minor blocks as possible, and thus a root block is essentially a unlimited-sized block as single-blockchain system

- If the hash power of the root chain is 0%, then the QuarkChain system becomes a multiple independent blockchain system. Each shard of QuarkChain can be treated as an independent blockchain. It is more scalable of course, and it is also more decentralized since a weak miner may not need to join a mining pool. However, it is very insecure due to the dilation of hash power, e.g., a malicious attacker could easily perform a double-spending attack on one of the blockchain in a 100-shard system with only 1/200 hash power of overall network

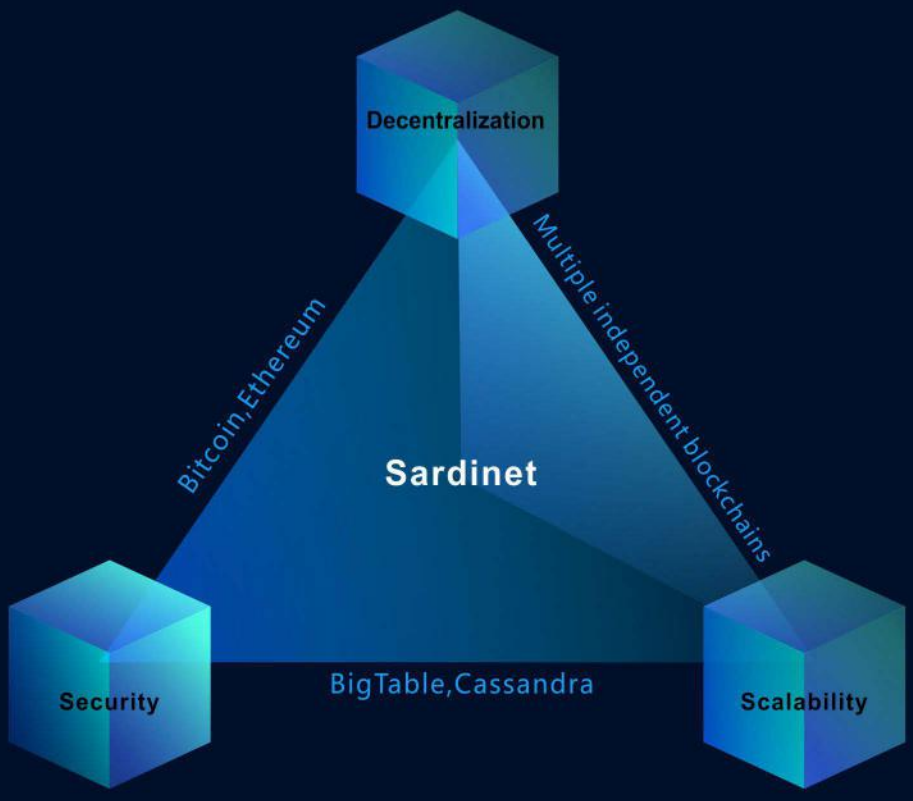
4.2 Security, Decentralization, and Scalability Position of QuarkChain

QuarkChain's 50% hash power allocation on the root chain enhances the system's security besides scalability. In addition, QuarkChain is more decentralized than single-blockchain system so that QuarkChain is also secure.

- Dramatically scale the throughput of the network. We use advanced sharding technologies to improve the system capacity and could easily increase system capacity to process more transactions per second as needed.

- More decentralized than single-blockchain network. As the hash power of a single-blockchain network increases, the expected return time of weak miners grows significantly, and they have to join a mining pool to collect their rewards in a timely manner. This greatly encourages centralization and hurts the core value of blockchain. QuarkChain is designed to be more decentralized because a weaker miner doesn' t need to join a mining pool to collect its reward.

- Security. All transactions in the QuarkChain network are protected by 50% of the overall hash power of the network, and a double-spending attack requires at least 25% hash power. This is smaller than single-blockchain's 50%, but since QuarkChain is more decentralized, a miner will be much harder to collect 51% hash power in our network than that of single-blockchain.



5. QuarkChain Core Features

Unlike many existing approaches that attempt to address the scalability problem by enhancing existing systems, QuarkChain is designed for scalability from the beginning - similar to its centralized counterpart. QuarkChain believes following important values: usability (fast, simple), decentralization (public participation), safety (reliable). Features of the QuarkChain are listed below.

5.1 Anti-Centralized Horizontal Scalability Expansion

To construct a peer-to-peer network that is impervious to malicious attack, traditional blockchain technologies require every node to fully validate all blocks and reject any block that is invalid. Similarly, the node in QuarkChain that validates all minor blocks and root chain blocks is called super-full node. If every node in QuarkChain runs as super-full node, QuarkChain could have the same safety level as traditional blockchains.

However, running a super-full node could be very expensive in a high-throughput blockchain system. For example, 1M TPS with each transaction being 250 bytes would require 2 GBps network bandwidth, which becomes a huge barrier to many users. In addition, the traffic would generate about 20 Terabytes data per day or 7 Perabytes data per year. The high requirements on CPU, storage, memory, and network bandwidth of super-full node impose a significant barrier, and such requirements may be only acceptable by powerful parties (e.g., company uses powerful workstation in their data center). This greatly discourages decentralization and hurts the core values of blockchain.

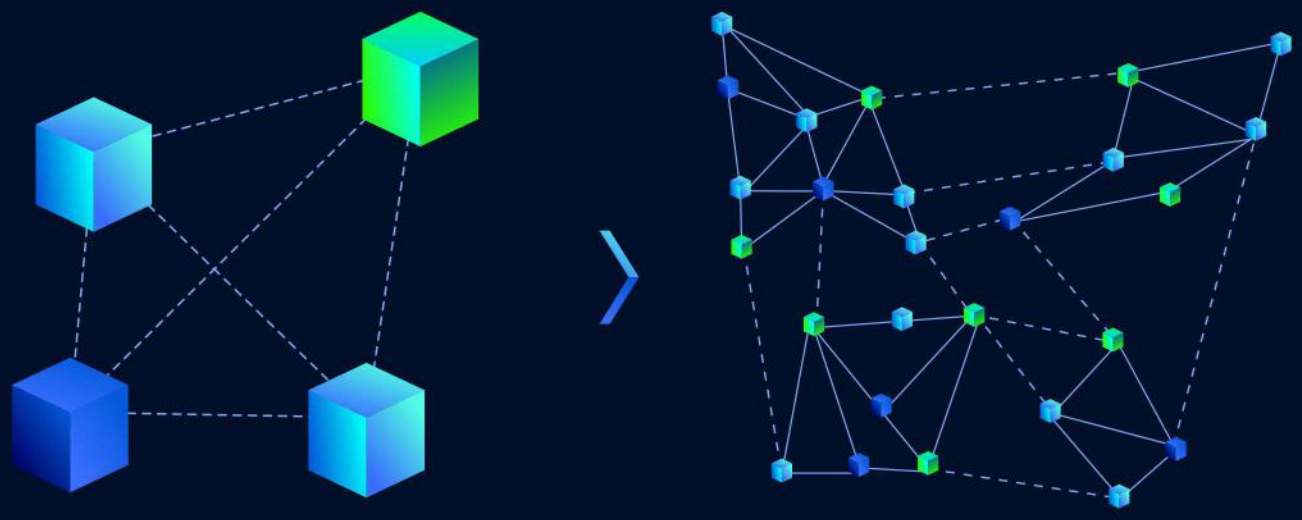


Fig. 6(A) illustration of horizontal scalability of QuarkChain network, where four super-full nodes (left) are replaced by four clusters of nodes (right), where the nodes in each cluster are honest to each other. (Solid line indicates honest connections, and dash line indicates unreliable connections)

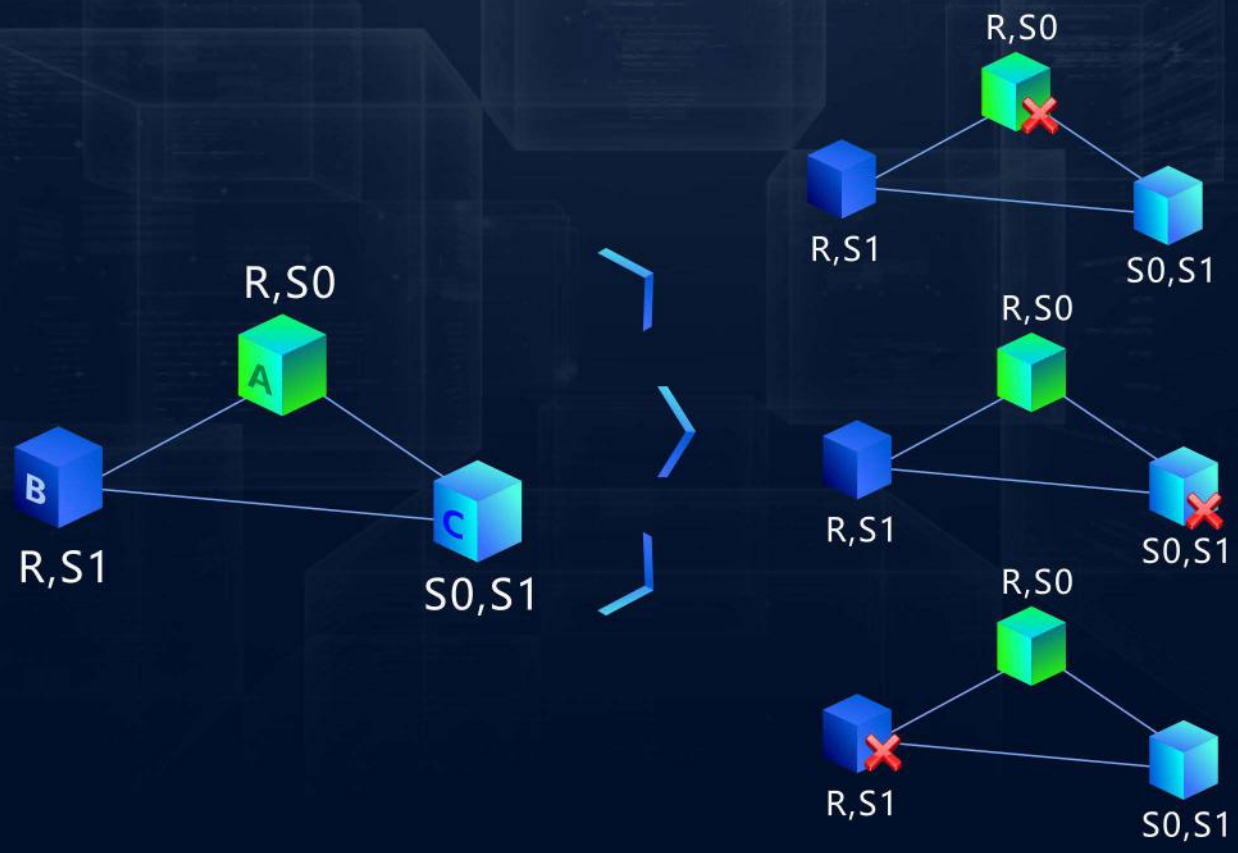


Fig. 6(B) illustration of high availability of a QuarkChain cluster with 2 shards, where the cluster could still fully validate the network even any single node is crashed (right). For example, suppose there are 2 shards in the system, A validates shards 1-2 , B validates shards 2 and root chain, and C validates shards 1 and root blockchain, and A,B,C are honest to each other, then A,B,C could form a cluster that is able to fully validate any blocks.

QuarkChain addresses the concern by allowing multiple honest nodes in a cluster to run as a super-full node. Each node in the cluster only validates a sub-set of chains. As long as the union of their sub-sets cover root blockchain and minor blockchains, we could show that they are able to fully validate the whole blockchains without acquiring an expensive machine. In addition, if one of the nodes crashes in the cluster, the rest nodes are still able to fully validate any blocks since any two of them form another cluster, enabling high availability of such clusters.

Furthermore, to encourage forming such clusters in the network, QuarkChain will have incentives for miners to answer a puzzle about the information of random blocks (e.g., 64-bit xor on random blocks in a randomly-selected shard or root blockchain). The puzzle will perform over a large amount of blocks and it is memory or storage intensive, and thus downloading the random blocks on-demand from the network will be inefficient.

5.2 Efficient and Secure Cross-Shard Transaction

In a QuarkChain system, we classify the transactions into two categories:

- In-shard transactions, where the input and output addresses of the transaction are in the same shard
- Cross-shard transactions, where the input and output addresses are in different shards.

In-shard transactions are simple, since a shard already contains complete ledger information of the shard. Cross-shard transactions are more difficult because of the synchronization between two shards. The QuarkChain fully supports cross-shard transactions as first-class citizen, in a sense that:

- Any user could issue any cross-shard transaction at any time
- Cross-shard transactions can be confirmed in minutes
- The throughput of cross-shard transactions could be scaled linearly as the number of shards increases

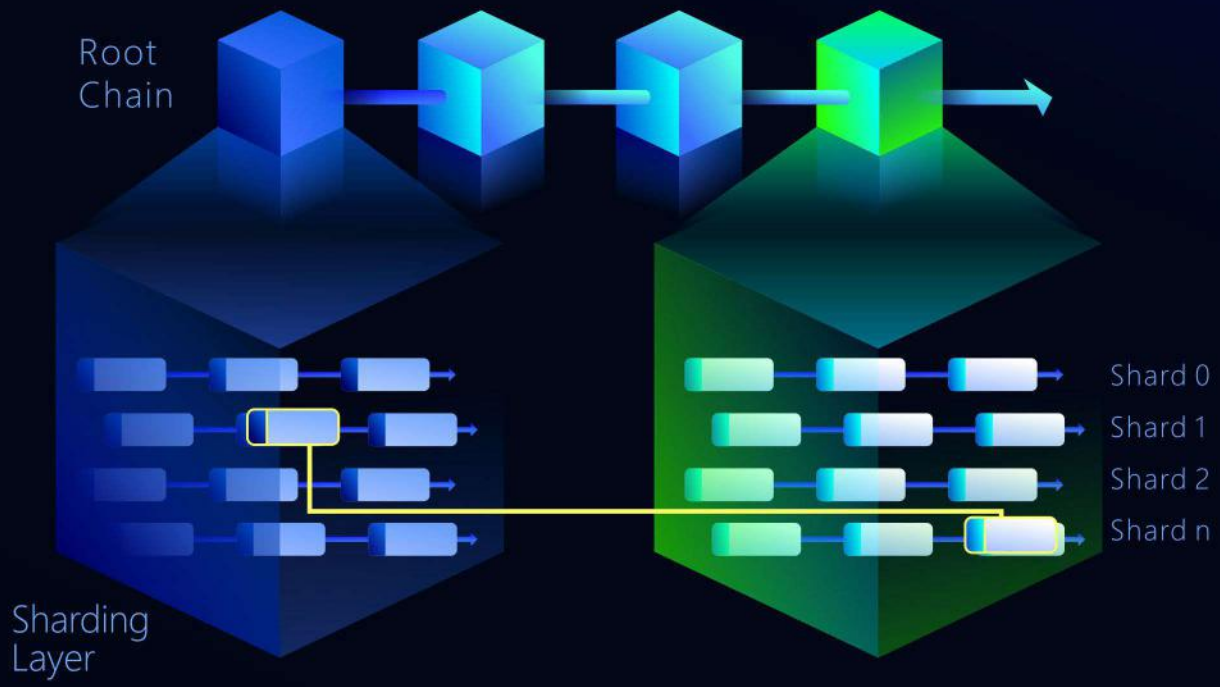


Fig. 7, Illustration of cross-shard transactions, where the output of the transaction can be spent as long as the cross-shard transaction is confirmed by the root chain.

These key features of our QuarkChain create a world in which anyone will be able to easily perform any transaction in a cost-effective manner.

5.3 Simple Account Management

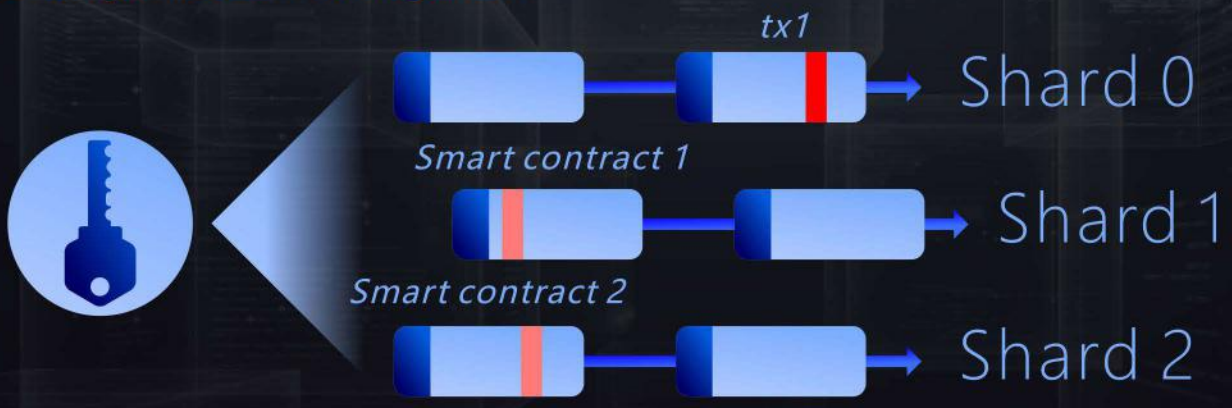


Fig. 8 Illustration of simple account management, where an account with a private key is able to perform transaction on any shards.

Unlike other sharding solutions that a user may need to create multiple accounts in different shards in order to interact with all users/smart contracts in the network, QuarkChain system greatly simplifies account management - a user only needs to have one account to manage all addresses in all shards and is able to interact with all users seamlessly. In addition, we will create a smart wallet application which will automatically perform cross-shard or in-shard transactions (including smart contract) for a user, and the user may not be even aware of sharding in the system. Some users may choose advanced way to manage their addresses, e.g., allowing payments always via in-shard transactions, and thus a merchandise is able to receive a payment from all users in seconds.

5.4 Cross-Chain Transactions

With our design architecture, cross-chain transaction becomes approachable. Since we only maintain one root chain, the transaction from another blockchain can be implemented by converting the tokens by an adapter and then performing the transaction like a cross-shard transaction from QuarkChain side. Another way is to accommodate the other chain as a subchain (or shard) so that cross-chain becomes cross-shard transaction.

6. QuarkChain System Operational Aspects

6.1 On-Chain and Off-Chain Transactions

Even QuarkChain supports high scalability, it can also accommodate off-chain transactions. Some applications need both on-chain and off-chain handling. For example, some transactions need to access external data (not on the blockchain). The QuarkChain two-layer sharding structure makes this on-chain and off-chain handling very flexible. This opens more opportunities and applications.

6.2 Smart Contract

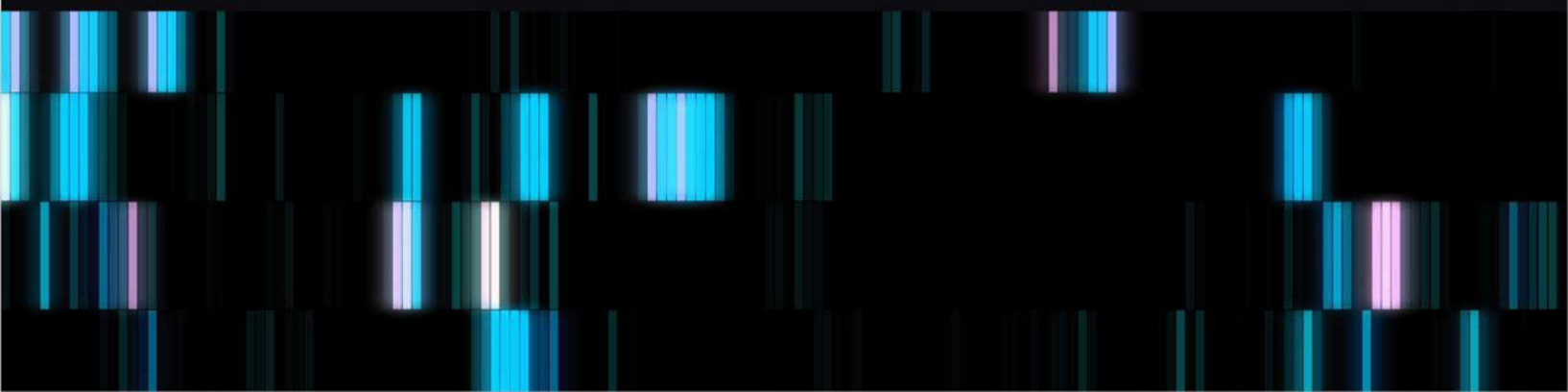
QuarkChain will support smart contracts via Ethereum virtual machine (EVM). EVM is the most widely used execution engine for smart contracts. Most of the existing dApps built on top of EVM can be directly deployed on QuarkChain platform. In addition, to utilize high-scalability feature of QuarkChain, we will provide additional scalability-aware interface such as which shard the contact is being executed, sending smart contract specific data via different shards.

6.3 Account Management

Since a user can manage all addresses in all shards via a private key, a user will essentially have the same number of addresses as the number of shards. If the number of shards is large (e.g., thousands or tens of thousands), a user may have multiple balances in multiple shards, and thus managing all balance in all shards can be inconvenient. We further simplify account management by defining the following two types of accounts:

- Primary account: Primary account is the address of the user in a default shard
- Secondary account: Secondary account manages the rest addresses of the user in the rest shards.

To simplify management, most transactions of a user will be initiated from the primary, temporally move to an address in secondary account if the transaction requires (e.g., smart contract in different shards), and if there is remaining balance in secondary account after the transaction, the balance will be moved back to the primary account. This ensures that the balance of the user should be in the primary account most of time, and thus the user does not need to manage the balances in the addresses of secondary account. This feature is enabled by smart wallet, which will be provided by QuarkChain team as an open source project.



6.4 Smart Wallet

There are two typical transactions in QuarkChain:

- Transfer some tokens associated with an address to another address which may be in the same shard or not
- Execute a smart contract in a specific shard

Smart wallet will simplify account management when using these transactions so that a user does not need to be aware of the underlying detailed in-shard/cross-shard operations:

- For a transfer transaction, smart wallet will automatically detect the primary account of a user (the address of the user in a default shard) and perform the in-shard/cross-shard transaction accordingly
- For a smart contract transaction, if the smart contract does not exist in the same shard of the user's primary account, smart wallet will automatically transfer the token to the user's secondary account in the shard that smart contract belongs to. The smart wallet will perform the smart contract transaction in the shard. If there is remaining balance in the secondary account, smart wallet will (optionally) automatically transfer the balance from the secondary account to the user's primary account.

7 QuarkChain Eco-system

7.1 Token Economics

As discussed above, the main goal of QuarkChain is to solve scalability problem of the current blockchain based systems. The key application scenarios of QuarkChain will focus on financial tech areas and game industries. Token of QuarkChain (QKC) will play very important roles, which carry the value of QuarkChain. There are several detailed application fields of QKC.

Value carrier
The essence of the encrypted currency is the value carrier, which is the most important attribute of QKC.

Transaction currency
Similar to Ethereum, each transaction on QuarkChain needs to pay transaction fee. Since QuarkChain has powerful transaction processing capability, transaction fee will be very low. Transaction fee only can be paid by QKC. QuarkChain supports smart contract. Interact with contracts on QuarkChain will pass through transaction.

Contribution reward
As a peer-to-peer system, using economics means to produce positive feedback can promote the continuous development of the system. QKC will be the reward to motivate the community to make continuous contributions to the system.

7.2 Business Development

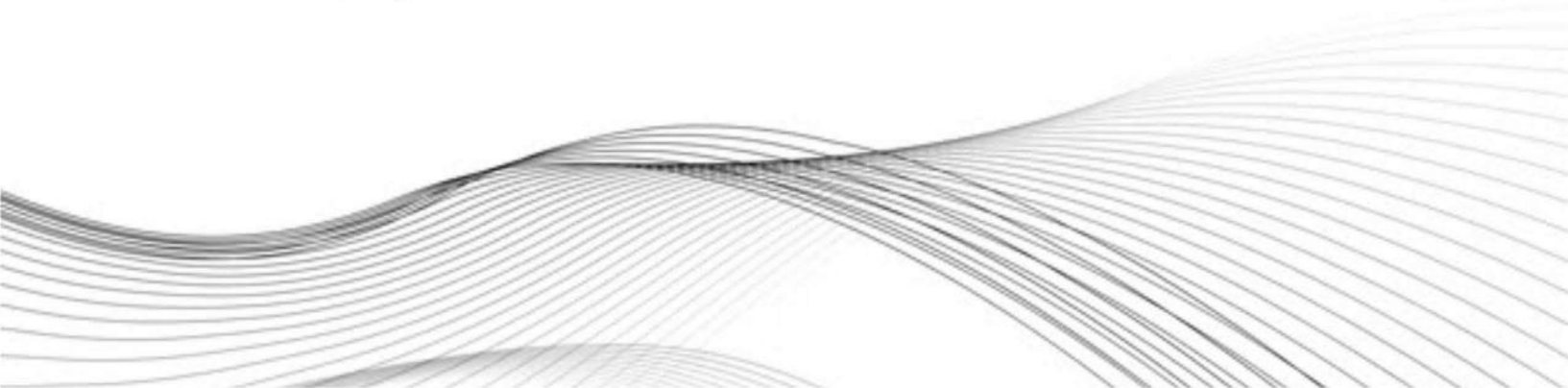
7.2.1 Mobile Decentralized Applications (DApps2go)

We believe that DApp built upon on mobile devices is more applicable and has more ecological values, based on the fact that 4.47 billion people are using mobile phone and 68% mobile phone internet user penetration worldwide in 2018. Mobile based DApps are very limited today due to the low capacity of mobile network which cannot deal with blockchain data flow.

QuarkChain has robust infrastructure to fully support mobile DApps (Dapps2go), and its infrastrucrture design is mobile-oriented. Furthermore, we will provide on-chain developer tools to create an Android-friendly environment, making DApps2go development as simple as possible. We will also allocate significant amount of QKC as incentives for developers who adopt and build their DApps on QuarkChain. Our easy scale-out blockchain technology makes social network, online storage, gaming and sharing economic platforms on blockchain possible. For instance, developers could build a completely decentralized peer to peer share riding DApp on QuarkChain. It can easily handle 7.4-billion rides per year—a number completed by the largest ride sharing company in the world in 2017—while removes the share riding authority to lower the cost of using share ride for customers. QuarkChain is an ideal platform to build shared economy businesses.

7.2.2 Minimum Viable Products with Onchain Fast Evolution

QuarkChain aims to shorten product development cycles by adopting build-measure-learn feedback loop from the lean startup methodology. Thus, we allow developers to run minimal viable products on-chain. With great support from QuarkChain's high transaction processing capability, developers can deploy and test their products on the main-net with quick feedback collection. An Onchain Demo Show zone on QuarkChain main-net will provide ultra- smooth and fast testing experience to help product managers and developers of DApps validate their ideas rapidly.



7.2.3 Demand Oriented Business Scenario

QuarkChain only brings real business into blockchain world. Such businesses must have strong needs for high throughput blockchain, and be able to solve existing customer or business demands. A good scenario is authentication, which is full of challenging and cost-inefficient. Existing technologies, such as high anti-counterfeiting technologies behind the national identification documents, can be too expensive for small to medium business to adopt. With the help of our decentralized ledger and advanced cryptographic protected private key, however, we believe that there can be DApps to support small business owners by providing affordable and easy handling anti-counterfeit solution. This solution can also be used for education systems for validating diplomas and laboratory raw data. QuarkChain will always be open and collaborative with such businesses, and will partner with them to leverage and scale up their business.

With the lean startup philosophy in mind, we carefully select business partners from 2-5 different industries where high-throughput blockchain can maximize its utilization. The current business partners are listed below:

7.2.4 QuarkChain for Internet of Things

Although it is still under investigation, blockchain has shown a great potential to be applied for Internet of Things(IoT). Using blockchain can reduce the cost of money transfer and also helps the rapid realization of the value of IoT transfer. However, IoT usually contains a large amount of devices and there may be a large number of transactions simultaneously. QuarkChain will play an important role as a platform to support IoT applications with a large number of low-cost devices and speed transactions. The use of smart contracts can also realize the automatic data collection and processing and thus build more applications.

7.2.5 QuarkChain for AI and Big Data

Blockchain provides a digital platform for economic transactions and thus it is highly related to artificial intelligence (AI). There are many aspects that blockchain can use AI technologies. For example, through reinforcement learning, sharding can be more efficient so that the common trading clients can be allocated in one shard or at least closer shards to reduce the transaction cost. However, this requires blockchain design has the reshardable ability and QuarkChain offers this function exactly.

Blockchain genuinely relates to big data and it generates temporal and space domain data. As blockchain grows, the amount of data increases fast. No matter it is private chain or public chain, these data will generate great value for the company or the whole world's economy. Built on QuarkChain platform, many data mining algorithms can be developed and economic models can be developed. QuarkChain is open to collaborate with data analysts and economists to develop new economic models and also this analysis will bring back valuable feedback to further enhance QuarkChain design with higher efficiency.

7.3 Applications development (Case study)

7.3.1 Chihuo

Chihuo is a content-based social media that publishes reviews of Chinese food and restaurants in U.S. has over half-million subscribers in WeChat and 400K followers in its Facebook and Weibo page. The company makes revenues by selling vendors' product on its e-commerce website, and by collecting advertising fee and consulting fee from restaurants and packaging food companies. To further penetrate the market share, Chihuo is looking for a solution to increase user acquisition and retention. What we offer to Chihuo is to run Dapp on QuarkChain and supply its own token. By doing so, Chihuo will create an economic cycle shown below.

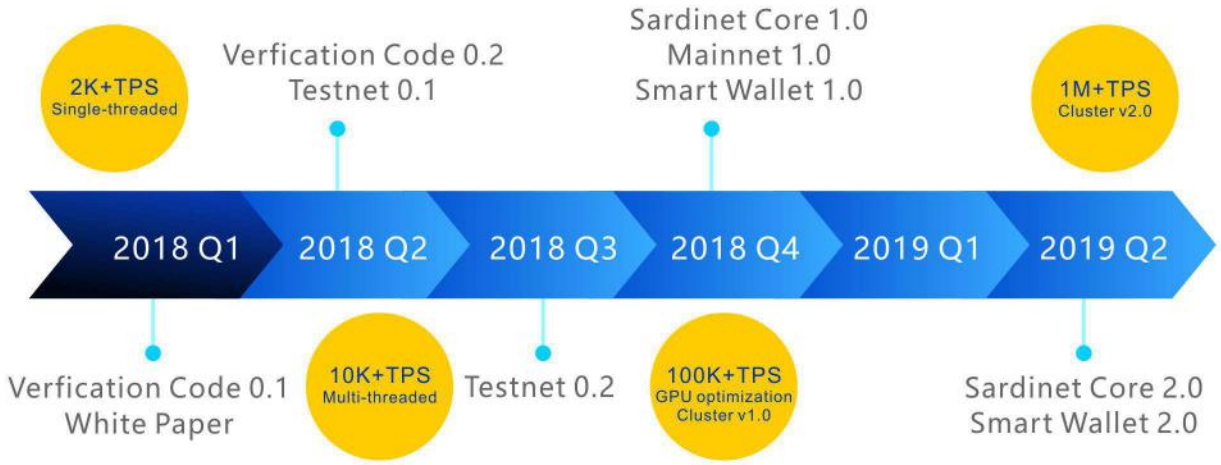
User receives token from Chihuo as registration/loyalty/referral award. The token can be spent by users as voucher for local restaurants/retailer/e-commerce platform. Restaurants/food vendors return token to Chihuo as an exchange of discounted advertising/consulting fees. This economic loop has three benefits:

- Chihuo builds a sustainable user growth model. The model covers up user acquisition, retention and referral. This allows Chihuo to penetrate and retain its market fast and sturdy.
- User benefits from this model by paying less money on food.
- Restaurants, retailers and food manufacturers, in addition to have discounted price for marketing fee at Chihuo, can quantitatively measure Chihuo's advertisement performance by analyzing token recycle. This transparency also allows Chihuo and themselves to better strategize marketing campaigns.

7.4 QuarkChain Collaborators



8. Roadmap and Timeline



Q1 2018: we focus on white paper and developing verification code 0.1 which mainly serves as proof of concept for our system;

Q2 2018: we will release verification code 0.2 and implement Testnet 0.1 with Wallet 0.1. Testnet 0.1 supports basic transactions including both in-shard and cross-shard transactions.

Q3 2018: we will release Testnet 0.2 and Wallet 0.2. Testnet 0.2 will support most features of QuarkChain such as smart contract, reshard, etc.

Q4 2018: we will release QuarkChain Core 1.0, Mainnet 1.0, together with Smart Wallet 1.0. QuarkChain Core 1.0 will provide basic functionalities of QuarkChain and basic optimization (e.g., GPU support).

Q1 2019: we will release Quarkchain Core 2.0, Mainnet 2.0, together with smart wallet 2.0. QuarkChain Core 2.0 will further optimize QuarkChain Core 1.0 and enable clustering feature so that a group cheap nodes can form a cluster and run as a full node.

9. Development Team

Development Team

Qi Zhou / Founder
Expert in high-performance systems
Former Googler and have 15+ years development experience
PhD from Georgia Institute of Technology

ZhaoGuang Wang / Senior Software Engineer
Expert in large scale distributed systems
6 years work experience at Facebook and Google building systems capable of processing millions of queries per second
Master in computer science from University of Michigan.

Xiaoli Ma / Research Scientist
Full Professor at Georgia Tech
IEEE Fellow

Yaodong Yang / Research Scientist
PhD Advisor at Xi' an Jiao Tong Univ.
Partner of Demo++
PhD from Virginia Tech
Dedicated on Blockchain development and research

Wencen Wu / Fund Manager
Assistant Professor at RPI
Expert in model simulation and verification in distributed autonomous systems
PhD from Georgia Institute of Technology

Operation Team

Ting Du / CMO for Chinese Market
Geek in Product Management
Founder of incubator Demo++, Incubator of Ink
Committee of Liuhe Capital Startup
Dedicated on Blockchain productization and
business application

Anthurine Xiang / CMO for International Market
Combined background of finance, consulting and tech,
6 year experience in both Wall street and Silicon Valley.
Lead of platform analytics at Wish, previously marketing
lead at Beepi and Linkedin
Focusing on business partnership and branding
of blockchain projects

Kyle Wang / COO
Founder and CEO of multiple international companies
Enthusiast in distributed ledger technology (DLT)
12 years experience in international trading
and supply chain finance

Julianne Zhu / Social Media Broadcasting
Former BD Director from Roboterra
(an AI & Robotics company)
Expertise in business development and marketing
MBA from Rutgers University

Patrick Mei / Community Manager
Founder of investment firm, 3 years experience in financial investment
Crypto media writer
Bachelor from Fudan University

Advisor

Bill Moore
Distinguished Engineer at Sun Microsystems
Co-led the ZFS team and served as Chief Engineer for Storage at Sun Microsystems
President of DSSD / EMC Fellow

Mike Miller
Ph.D. Physicist with 100+ publications. Founder: Cloudant (YCS08)
acquired 2014 (IBM Cloud Data Services).

Zhiyun Qian
Expert in cyber security
Discovered serious vulnerabilities in Linux, Android, and TCP/IP
Assistant Professor at UC riverside

Arun G. Phadke
University Distinguished Professor Emeritus & Research Professor of Virginia Tech
National Academy of Engineering

Leo Wang
Crypto Fund Manager. Invested in Over 50+ Project allover the world. Ontology、ArcBlock、SmartMesh、Elastos、QuarkChain、Penta、MedicalChain、AppCoin、BitGuild、Zeepin、Gifto、Iotex、UGC、Ocoin、Scry、Bluzelle、Lino、Linkeye、Fortuna、DDex.....

Kevin Hsu
Kevine has rich experience in investment and has invested over 60 blockchain companies around the world

Disclaimer:

Nothing in this article constitutes legal, financial, business, or tax advice. You should consult your own legal, financial, business, tax, or any other professional adviser before engaging in any activities mentioned or in connection herewith. Neither QuarkChain Foundation, including any member who has worked on this article or QuarkChain platform or involved in developing QuarkChain related project, nor any service provider shall be liable for any kind of direct or indirect damage or loss whatsoever which you may suffer in connection with accessing this white paper.

This Whitepaper is intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein below may not be exhaustive and does not imply any elements of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information.
Nothing contained in this Whitepaper is or may be relied upon as a promise, representation or undertaking as to the future performance of the QuarkChain.