
QuarkChain
www.quarkchain.io

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

QuarkChain Foundation

Version 0.3.4

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

NOTICE AND DISCLAIMER

NOTHING IN THIS WHITEPAPER CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER QUARKCHAIN FOUNDATION LTD. (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS WHO HAVE WORKED ON THE QUARKCHAIN NETWORK (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE QUARKCHAIN NETWORK IN ANY WAY WHATSOEVER (THE QUARKCHAIN TEAM), ANY DISTRIBUTOR/VENDOR OF QKC (THE DISTRIBUTOR), 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 WHITEPAPER, THE WEBSITE AT HTTPS://WWW.QUARKCHAIN.IO (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

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. Where this Whitepaper includes information that has been obtained from third party sources, the Foundation and/or the QuarkChain team have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that this Whitepaper may become outdated as a result; and the Foundation is under no obligation to update or correct this document in connection therewith.

This Whitepaper does not constitute any offer by the Foundation, the Distributor or the QuarkChain team to sell any QKC (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. 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 Network. The agreement between the Distributor and you, in relation to any sale and purchase of QKC is to be governed by only the separate terms and conditions of such agreement.

By accessing this Whitepaper or any part thereof, you represent and warrant to the Foundation, its affiliates, and the QuarkChain team as follows:

(a) in any decision to purchase any QKC, you have not relied on any statement set out in this Whitepaper;

(b) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that QKC may have no value, there is no guarantee or representation of value or liquidity for QKC, and QKC is not for speculative investment;

(d) none of the Foundation, its affiliates, and/or the QuarkChain team members shall be responsible for or liable for the value of QKC, the transferability and/or liquidity of QKC and/or the availability of any market for QKC through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to purchase any QKC if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of QKC would be construed as the sale of a security (howsoever named) or investment product and/or (ii) in which access to or participation in the QKC token sale or the QuarkChain Network is prohibited by applicable law, decree, regulation, treaty, or administrative act, and/or (including without limitation the United States of America, Canada, New Zealand, People's Republic of China and the Republic of Korea).

The Foundation, the Distributor and the QuarkChain team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of this Whitepaper or any other materials published by the Foundation). To the maximum extent permitted by law, the Foundation, the Distributor, their related entities and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of this Whitepaper or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of QKC should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the QKC token sale, the Foundation, the Distributor and the QuarkChain team.

The information set out in this Whitepaper is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of QKC, and no virtual currency or other form of payment is to be accepted on the basis of this Whitepaper. The agreement for sale and purchase of QKC and/or continued holding of QKC shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of QKC (the Terms and Conditions), which shall be separately provided to you or made available on the Website. In the event of any inconsistencies between the Terms and Conditions and this Whitepaper, the Terms and Conditions shall prevail.

All contributions will be applied towards the advancing, promoting the research, design and development of, and advocacy for blockchain technology and networks which are able to handle large scale TPS capacity, expand the usability of blockchain technology without sacrificing its core features of security and decentralisation, to achieve a network which is free of congestion and affordable for all usage scenarios that demand speed and volume. The Foundation, the Distributor and their various affiliates would develop, manage and operate the QuarkChain Network.

This is only a conceptual whitepaper describing the future development goals for the QuarkChain Network to be developed. This Whitepaper may be amended or replaced from time to time. There are no obligations to update this Whitepaper or to provide recipients with access to any information beyond what is provided in this Whitepaper.

All statements contained in this Whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation, the Distributor and/or the QuarkChain team may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date of this Whitepaper and the Foundation and the QuarkChain team expressly disclaims any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

The use of any company and/or platform names or trademarks herein (save for those which relate to the Foundation or its affiliates) does not imply any affiliation with, or endorsement by, any third party. References in this Whitepaper to specific companies and platforms are for illustrative purposes only.

This Whitepaper may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of this Whitepaper, the English language version shall prevail. You acknowledge that you have read and understood the English language version of this Whitepaper.

Executive Summary

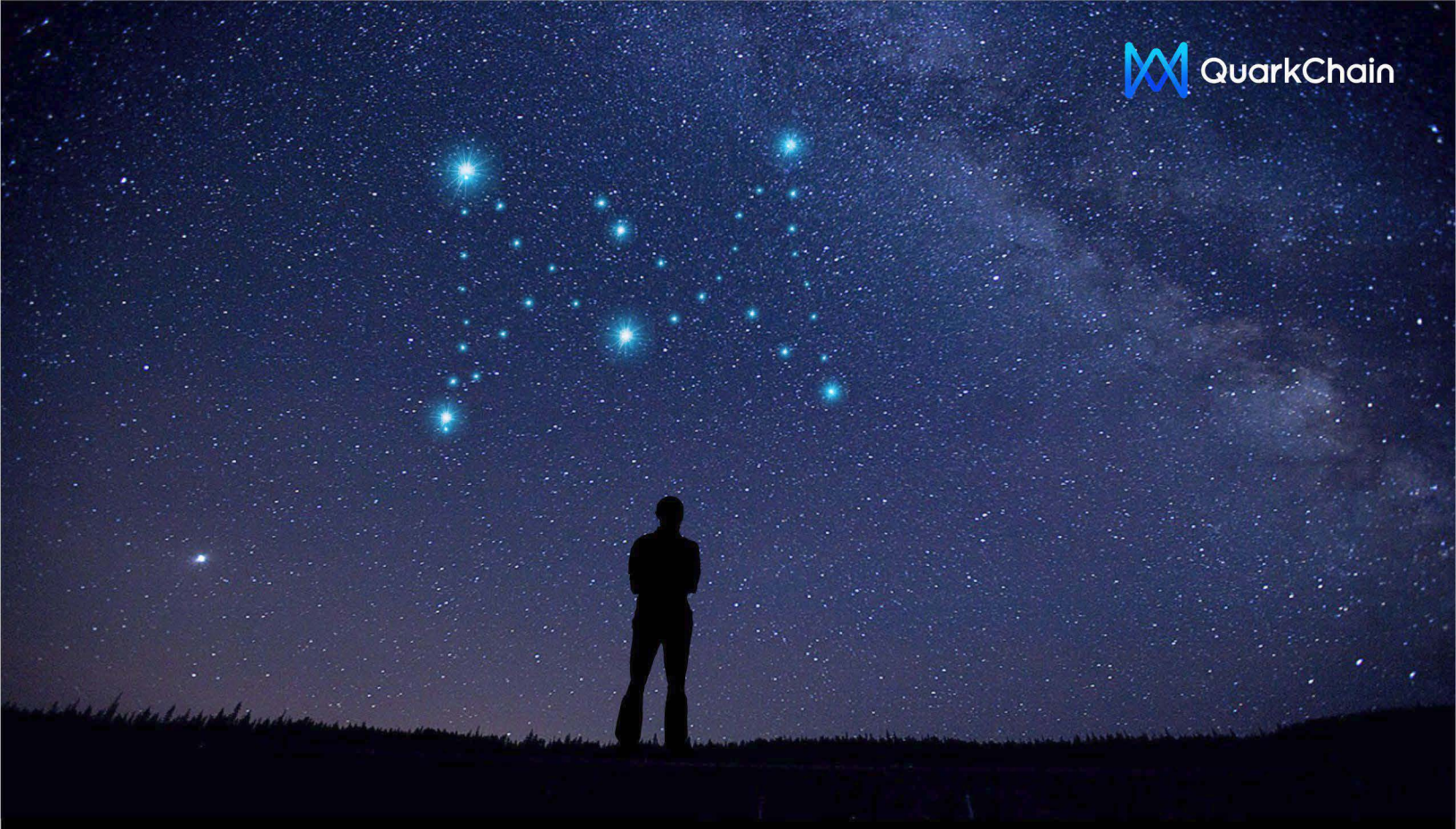
Recently, distributed ledger technologies - decentralized and trustless blockchains (e.g. Bitcoin, Ethereum), have started rewiring the nature of our current economy, communications, and knowledge. As the global financial transaction volume in all electronic payments grows, the low capacity of the current 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 100,000+ 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 first 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.
6. Turing-complete smart contract platform: the QuarkChain network supports Turing-complete smart contracts and has adopted the Ethereum Virtual Machine (EVM) to allow for easy migration of existing EVM decentralized Apps onto the QuarkChain platform.

QuarkChain

Table of Content



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 several years, many companies have been looking into blockchain technology. Almost every major financial institution in the world is doing blockchain research at the moment. Fig. 1 shows that since late 2017, there is a huge jump of the number of transaction requests in Ethereum system. The transaction volume demanded is projected to 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

First generation of blockchain is represented by bitcoin, which has started the digital currency technology revolution in the financial world. The second generation of blockchain technology is led by Ethereum. Ethereum 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 65 billion dollars (source: https://coinmarketcap.com/).

One important breakthrough 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 electrical power) these days and is not so energy efficient. In contrast, the POS systems assign the block rewards to the holder of tokens proportionally, which significantly reduce the amount of energy to mine a block and is much more economically efficient.

Blockchain visionaries imagined that this technology would spark innovation in every industry and set off a massive restructuring of communications and transactions, but this is not possible in its current state. As the demands increase, as shown in Fig. 1, another issue facing blockchain is scalability. Currently, major blockchains cannot even securely handle the volume of financial transactions that occur on centralized payment systems like Visa which claims to have 56,000 TPS on its network. Bitcoin's and Ethereums 10-20 TPS are many orders of magnitude away from this and even further from the TPS that IoT micropayments would require. The blockchain systems which do have this capacity have often sacrificed security and decentralization which are the key features that blockchain technology has to offer. For the speculation around blockchain to turn into real, widespread adoption, a network that can handle a large volume of transactions without compromising on security and decentralization must be developed.

1.3 QuarkChain Vision

The QuarkChain Network introduces a novel sharding-based blockchain architecture that aims to meet the global commercial standard. The technology behind the QuarkChain Network was inspired by the team's extensive experience in developing large-scale distributed systems in the centralized world that can handle billions of transactions per second. The mechanisms from these experiences have been applied to blockchain to create a unique solution to its scalability problem. This approach aims to greatly expand the usability of blockchain technology without sacrificing its core features of security and decentralization.

The QuarkChain Network is helping move blockchain into the next generation by increasing the current TPS capacity several-thousand fold of what it is now, to a projected about 100,000 TPS. The network being built is project to be free of congestion, making it affordable for all usage scenarios that demand speed and volume. We envision such a network applied to industries that demand higher TPS. Ultimately, the QuarkChain Network aims to build a high-throughput network to support applications such asdistributed social media, high frequency trading, Internet of Things (IoT), gaming, and payment.

2. The Challenges of Blockchain

The three main challenges of a blockchain: security, decentralization, and scalability.

2.1 Security Issue

As a transactional platform, the first priority is always security. A blockchain, as the name implies, is a chain of digitally connected "blocks". Blockchain was generated to provide means of security by doing a "decentralized ledger". Even though blockchain has some inherent properties for security, there still exist vulnerabilities, ill intentions, and malicious attacks that need to be considered when one selects the platform.

In fact, blockchains are decentralized across peer-to-peer (p2p) networks that need to be continually updated and kept in sync with a specific consensus algorithm (e.g. POW or POS). A POW-based blockchain would require at least 51% hash power of the network to perform double-spend 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 it is for the attack to 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).

2.2 Decentralization Issue

Since 2013, many decentralized trading platforms have been developed. Different from the 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 aforementioned, decentralization also gives blockchain security. However, decentralization is also being challenged these days. For example, a lot of mining pools are formed for POW-based blockchain so that a weak miner is able to collect its proportional share of block 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 for decentralized POW blockchains. For example, as of 2013 the top six mining pools consist of 75% of overall Bitcoin hash power.

2.3 Scalability Issue

In the following subsections, the existing approaches for scalability issue are reviewed.

2.3.1 Multiple Blockchains

One approach to scaling is splitting up different transactions across multiple blockchains (e.g. Bitcoin, Litecoin, Ethereum, etc.). But while this makes for lower transactional demand on each blockchain, it also means a lower hash power operating each blockchain. On smaller chains, it is easy for someone to gain enough of the hash power to perform a double-spend attack. While it offers some degree of scalability, it sacrifices security for scalability and is not a long-term solution. Having multiple blockchains also limits cross-chain transactions to cryptocurrency exchanges which charge trading fees, have long processing times, and are notoriously unsecure. Additionally, users need to maintain an address in each of the networks 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 the question of whether it is necessary to build another centralized payment method when there are already many out there.

2.3.3 Sharding

Originally, sharding technique from database means partitioning data in a large database into smaller parts. It is one of the most common ways in centralized systems to address the scalability problem. For instance, BigTable and Cassandra are two examples in the non-blockchain world to be born to solve large throughput issues. Notably, Ethereum has adopted sharding technology to scale out, 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 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 a 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) (Source: Danny Yang, Jack Gavigan, Zooko Wilcox, "Survey of Confidentiality and Privacy Preserving Technologies for Blockchains," R3, Nov. 2016)

3. The Technology of The QuarkChain Network

3.1 Design Principle

QuarkChain's design is based on the following principles:

- Enhancing the scalability while ensuring 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 ecosystem

Some blockchain designs trade off security with scalability. For example, OmniLedger claims to reach about 100,000 TPS by only handling 1% adversarial power (Source: Fig. 6 in "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding" from https://eprint.iacr.org/2017/406.pdf).

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.

3.2 System Architecture

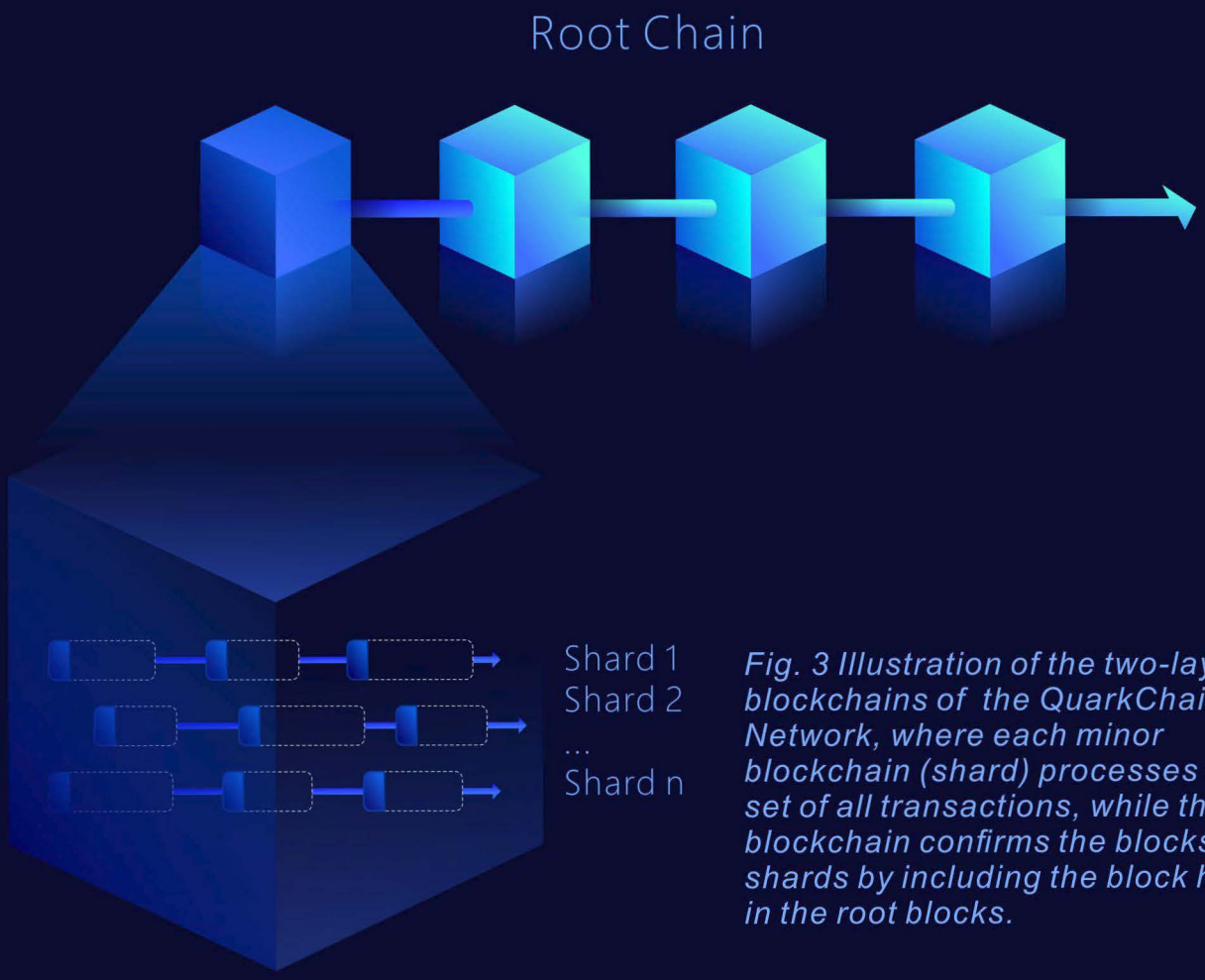


Fig. 3 Illustration of the two-layered blockchains of the QuarkChain Network, where each minor blockchain (shard) processes a sub-set of all transactions, while the root blockchain confirms the blocks in all shards by including the block headers in the root blocks.

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

- Ledger, which includes current ledger 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, the QuarkChain Network 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.

- The QuarkChain Network 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.

- The QuarkChain Network 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.

- The QuarkChain Networkis 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 the QuarkChain Network

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-spend attack, and a malicious miner needs at least 50% * 50% = 25% power to perform an attack.

Note that a network using the system of the QuarkChain Network has several minor blockchains (shards) and one root blockchain. Each blockchain offers different incentives 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. It is desirable that a marketing model is designed with features ensuring that though each party in the market pursues their own interests, the collective behaviors of each party can benefit all.

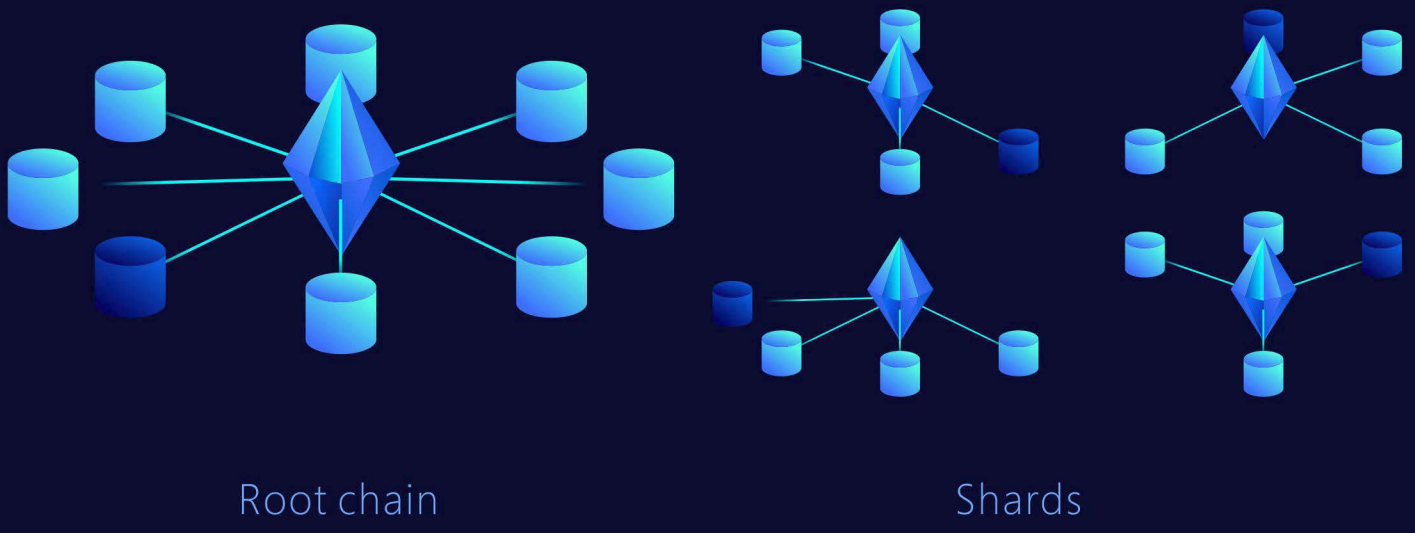


Fig 4. Illustration of collaborative mining, where the blocks in root chain have sufficiently large incentive and difficulty to protect the blocks (and thus transactions) in all shards, while all shards are incentivized to have even hash powers.

3.4 Consensus Algorithm

To protect all transactions, the root chain and the shards in systems of the QuarkChain Network run the following consensus algorithm:

- The root chain runs the POW algorithm, which is the same as Bitcoin and Ethereum. This means when two forks happen on root chain, the fork with the longest length (or total difficulty) will survive.

- Each shard runs a consensus called root-chain-first POW algorithm. Given two forks on a shard, to determine which fork to survive, a node would compare their corresponding root chains before comparing the forks. If a fork has longer root chain, then the fork will survive no matter how long another fork is. With such consensus algorithm, a double-spend attacker has to create (see Figure 5):

  (a) the minor blocks that revert the transaction; and
  (b) a longer root chain fork that includes the minor block headers.

Such attack is much harder to perform because the attacker must acquire at least 50% (hash power on root chain) * 51% = 25% hash power of overall network .

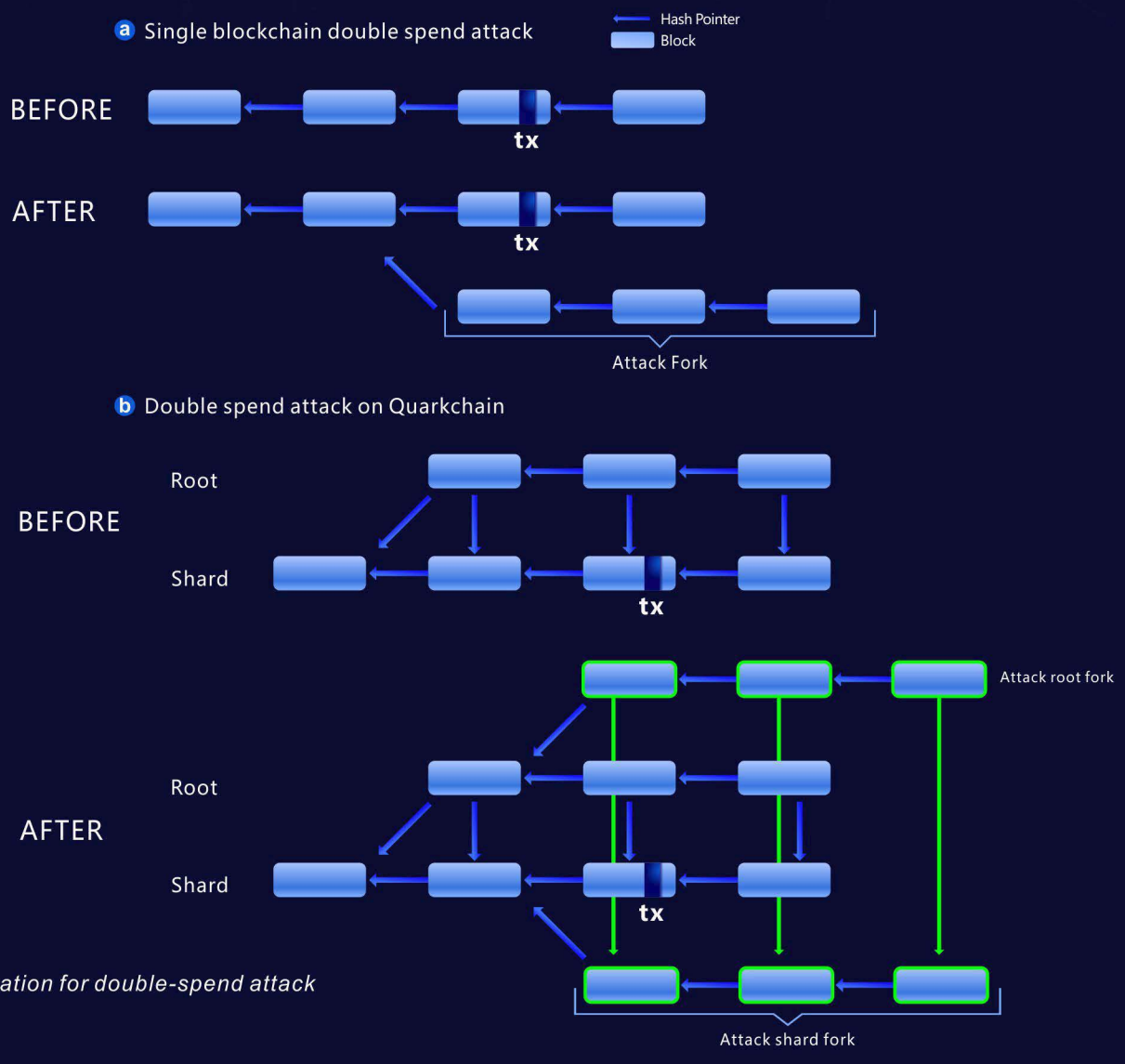


Fig. 5 Illustration for double-spend attack

3.5 Early Verification of the QuarkChain Network

Since the system of the QuarkChain Network is sophisticated and highly dynamic, an analytic solution could be hardly available. To design such a system to achieve the targeted goals, the QuarkChain team has resorted to using network simulation to simulate a 18-node and 8-shard network. This potentially allows verification of the 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. 6 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 system of the QuarkChain Network 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 wor of the root blockchain is about 1.6M, which is close to the expected value 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. The Positioning of the QuarkChain Network in Blockchain Society

The QuarkChain Network reveals a brand new path for blockchain design. This section discusses its relationship with other existing blockchains and positions it in the blockchain society.

4.1 Relationship with Single-Blockchain or Multiple-Blockchain Systems

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

- If the hash power of the root chain is 100%, then the system of the QuarkChain Network 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 system of the QuarkChain Network becomes a multiple independent blockchain system. Each shard of the QuarkChain Network 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 dilutionof hash power, e.g., a malicious attacker could easily perform a double-spend attack on one of the blockchain in a 100-shard system with only 1/200 hash power of overall network.

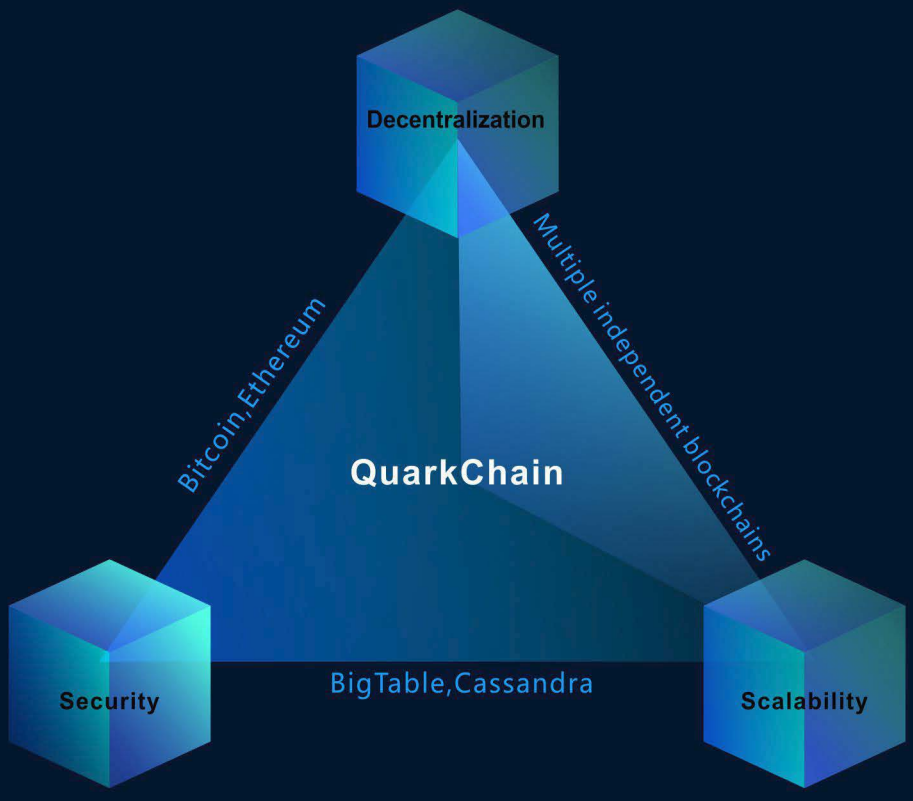
4.2 Security, Decentralization, and Scalability Position of The QuarkChain Network

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

- Dramatically scale the throughput of the network. Advanced sharding technologies have been used 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 incentives in a timely manner. This greatly encourages centralization and hurts the core value of a blockchain. The QuarkChain Network is designed to be more decentralized because a weaker miner does not 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-spend attack requires at least 25% hash power. This is smaller than single-blockchain' s 50%, but since the QuarkChain Network is more decentralized, a miner will be much harder to collect 51% hash power in our network than that of single-blockchain.



5. The Core Features of the QuarkChain Network

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

5.1 Anti-Centralized Horizontal Scalability Expansion

To build 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 the QuarkChain Network that validates all minor blocks and root chain blocks is called super-full node. If every node in the QuarkChain Network runs as super-full node, the QuarkChain Network 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.

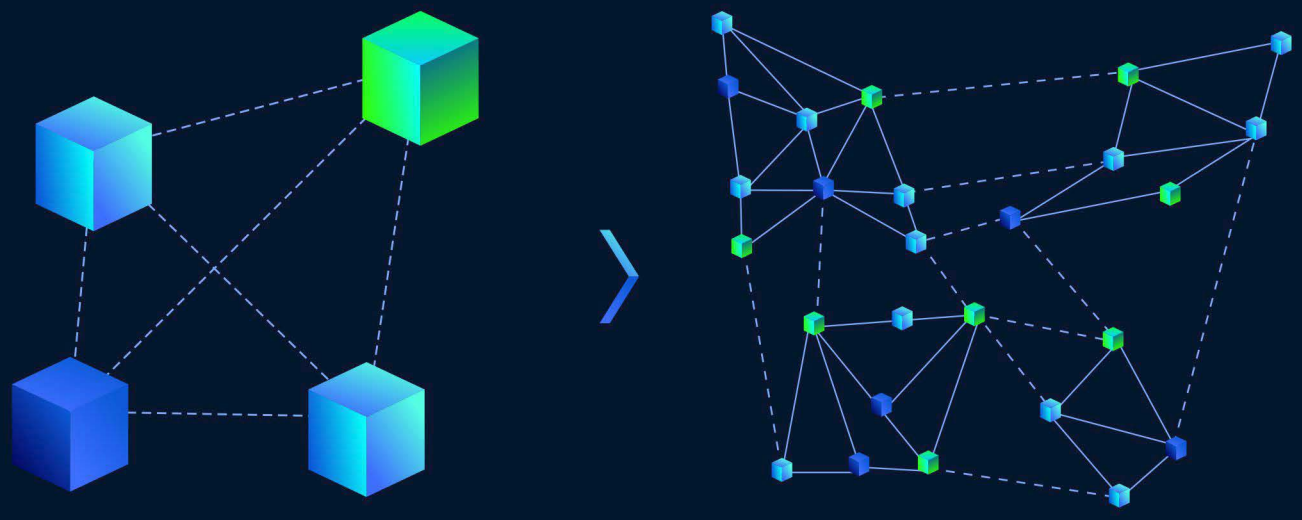


Fig. 7(A) illustration of horizontal scalability of the QuarkChain Network, where four super-full nodes (left) are replaced by four clusters of nodes (right), where the nodes in each cluster are honest to each other. (Solid line indicates honest connections, and dash line indicates unreliable connections)

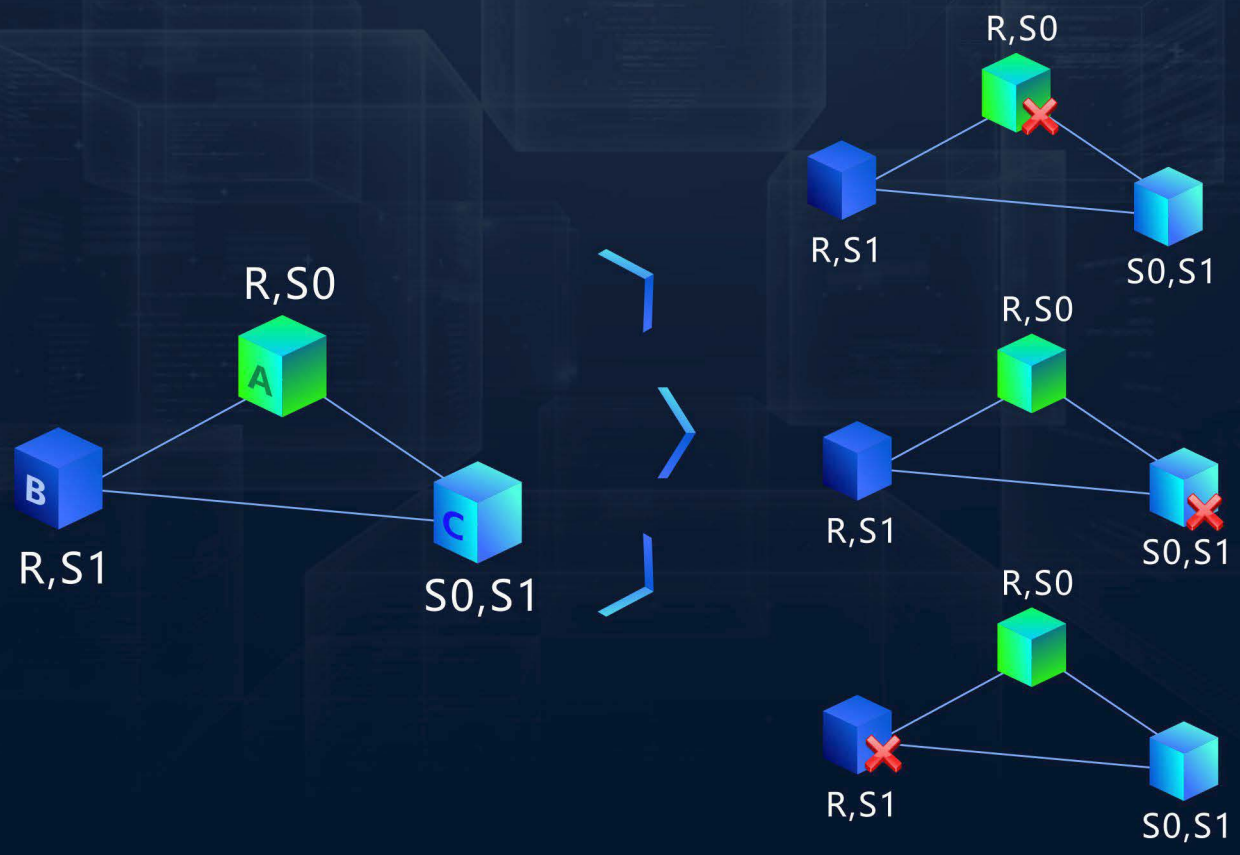


Fig. 7(B) illustration of high availability of a cluster with 2 shards run on the QuarkChain Network, where the cluster could still fully validate the network even any single node is crashed (right). For example, suppose there are 2 shards in the system, A validates shards 1-2 , B validates shards 2 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.

The QuarkChain Network 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, it can be shown 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, the QuarkChain Network 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 the system of the QuarkChain Network, the transactions can be classified 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 Network 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

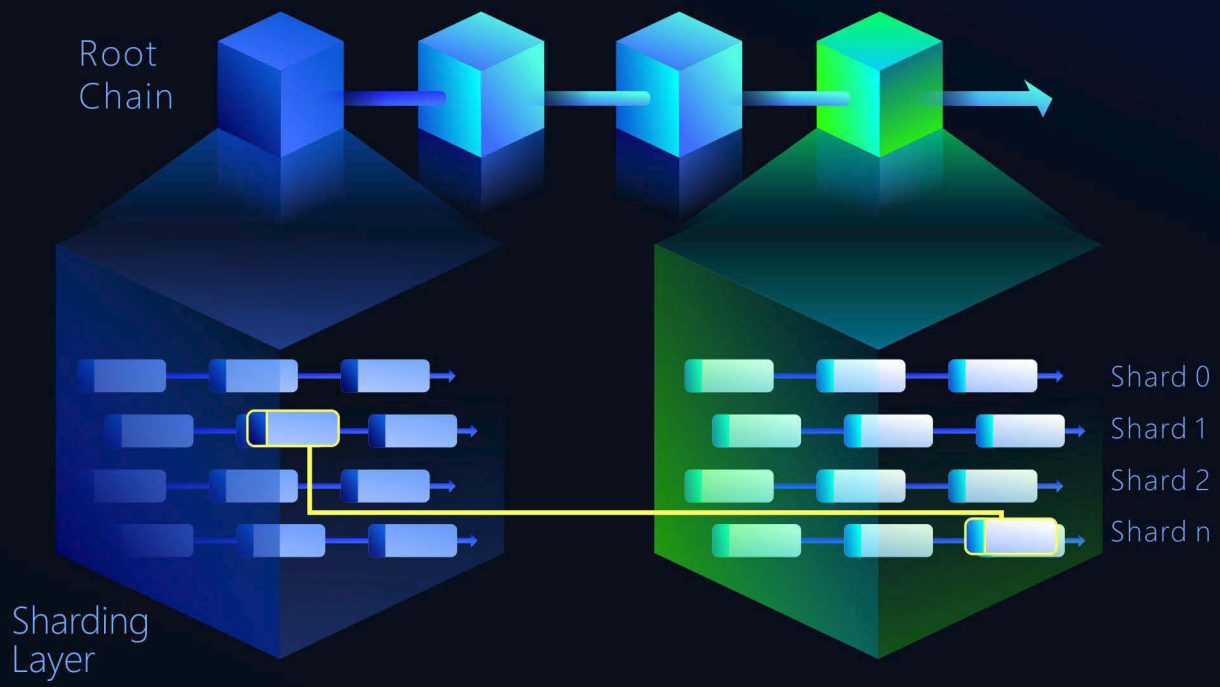


Fig. 8 Illustration of cross-shard transactions, where the output of the transaction can be spent as long as the cross-shard transaction is confirmed by the root chain.

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

5.3 Simple Account Management

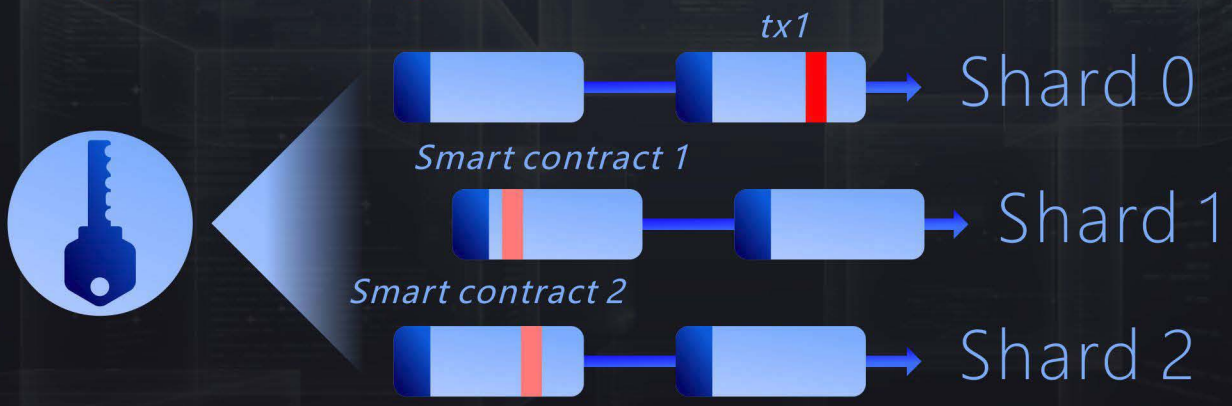


Fig. 9 Illustration of simple account management, where an account with a private key is able to perform transaction on any shards.

Unlike other sharding solutions in which a user may need to create multiple accounts in different shards in order to interact with all users/smart contracts in the network, the system of the QuarkChain Network 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, a smart wallet application will be created 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 Transaction

With this design architecture, cross-chain transaction becomes approachable. Since the QuarkChain Network only maintains 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 the point of view of the QuarkChain Network side. Another way is to accommodate the other chain as a subchain (or shard) so that cross-chain becomes cross-shard transaction.

6.The System Operational Aspects of The QuarkChain Network

6.1 On-Chain and Off-Chain Transactions

Even as the QuarkChain Network 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 two-layer sharding structure of the QuarkChain Network makes this on-chain and off-chain handling very flexible. This opens more opportunities and applications.

6.2 Smart Contract

The QuarkChain Network 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 the platform of the QuarkChain Network. In addition, to utilize high-scalability feature of the QuarkChain Network, an additional scalability-aware interface will be provided with features such as which shard the contractis being executed and 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. The account management of the QuarkChain Network has been further simplified 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 of the addresses of the user in the rest of the shards.

To simplify management, most transactions of a user will be initiated from the primary account, temporarily move to an address in the secondary account if the transaction requires it (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 on the QuarkChain Network:

- 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 primary account of a user, smart wallet will automatically transfer the token to the secondary account of the user 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 primary account of the user.

7. The Ecosystem of The QuarkChain Network

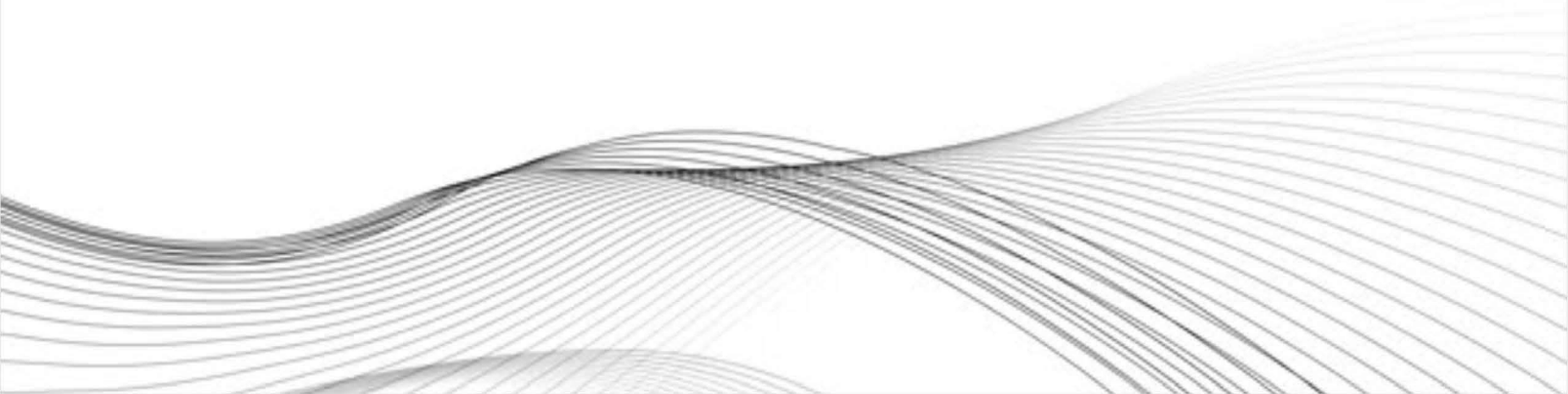
7.1 Token Economics

7.1.1 Properties and Usages of Token

The native digital cryptographically secured utility token of the QuarkChain Network (QKC) is a major component of the ecosystem on the QuarkChain Network, and is designed to be used solely as the primary token on the network. QKC will initially be issued by the Distributor as ERC-20 standard compliant digital tokens on the Ethereum blockchain, and these will be migrated to tokens on the blockchain of the QuarkChain Network when the same is eventually launched. As discussed above, the main goal of the QuarkChain Network is to solve scalability problem of the current blockchain based systems.

QKC is a non-refundable functional utility token which will be used as the unit of exchange between participants on the QuarkChain Network. The goal of introducing QKC is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on the QuarkChain Network. QKC does not in any way represent any shareholding, participation, right, title, or interest in the Foundation, its affiliates, or any other company, enterprise or undertaking, nor will QKC entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. QKC may only be utilised on the QuarkChain Network, and ownership of QKC carries no rights, express or implied, other than the right to use QKC as a means to enable usage of and interaction with the QuarkChain Network.

The key application scenarios of the QuarkChain Network will focus on financial tech areas and game industries. The Token of the QuarkChain Network (QKC) will play very important roles, as the medium of exchange for the QuarkChain Network. There are several detailed areas of application for QKC.



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

Transaction currency
QKC is required as virtual crypto "fuel" for using certain designed functions on the QuarkChain Network, providing the economic incentives which will be consumed to encourage participants to contribute and maintain the ecosystem on the QuarkChain Network. Computational resources are required for running various applications and executing transactions on the QuarkChain Network, as well as the validation and verification of additional blocks / information on the blockchain, thus providers of these services / resources would require payment for the consumption of these resources (i.e. "mining" on the QuarkChain Network) to maintain network integrity, and QKC will be used as the unit of exchange to quantify and pay the costs of the consumed computational resources.
Similar to Ethereum, each transaction on the QuarkChain Network needs to pay transaction fee. Since the QuarkChain Network has powerful transaction processing capability, transaction fee will be very low. Transaction fee only can be paid by QKC. The QuarkChain Network supports smart contracts. A smart contract transaction of the QuarkChain Network is completed by sending a message to the contract address.

Contribution incentives
As a peer-to-peer system, using economic means to produce positive feedback can promote the continuous development of the system. QKC will be distributed as incentives to incentivise the community to make continuous contributions towards the system. Users of the QuarkChain Network and/or holders of QKC which did not actively participate will not receive any QKC incentives.

QKC is an integral and indispensable part of the QuarkChain Network, because without QKC, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on the QuarkChain Network.

7.2 Business Development

7.2.1 Mobile Decentralized Applications (DApps2go)

The QuarkChain Network is built according to the belief that a DApp built upon on mobile devices is more applicable and has more ecosystem value, based on the fact that 4.47 billion people are using mobile phones and there is 68% mobile phone internet user penetration worldwide in 2018. Mobile based DApps are very limited today due to the low capacity of mobile networks which cannot deal with blockchain data flow.

The QuarkChain Network has robust infrastructure to fully support mobile DApps (Dapps2go), and its infrastructure design is mobile-oriented. Furthermore, on-chain developer tools will be provided to create an Android-friendly environment, making DApps2go development as simple as possible. A significant amount of QKC as incentives for developers who adopt and build their DApps on the QuarkChain Network. 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 the QuarkChain Network. 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 removing the ride sharing central authority to lower the cost of using ride sharing for customers. The QuarkChain Network is projected to be an ideal platform to build sharing economy businesses.

7.2.2 Minimum Viable Products with Onchain Fast Evolution

The QuarkChain Network aims to shorten product development cycles by adopting build-measure-learn feedback loop from the lean startup methodology. Thus, developers have been allowed to run minimal viable products on-chain. With great support from the high transaction processing capability of the QuarkChain Network, developers can deploy and test their products on the main-net with quick feedback collection. An Onchain Demo Show zone on the main-net of the QuarkChain Network 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

The QuarkChain Network 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 the decentralized ledger and advanced cryptographic protected private key of the QuarkChain Network it is believed that there can be DApps to support small business owners by providing an affordable and easy handling anti-counterfeit solution. This solution can also be used for education systems for validating diplomas and laboratory raw data. The QuarkChain Network will always be open and collaborative with such businesses, and will partner with them to leverage and scale up their business.

With the lean start-up 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 The QuarkChain Network for Internet of Things

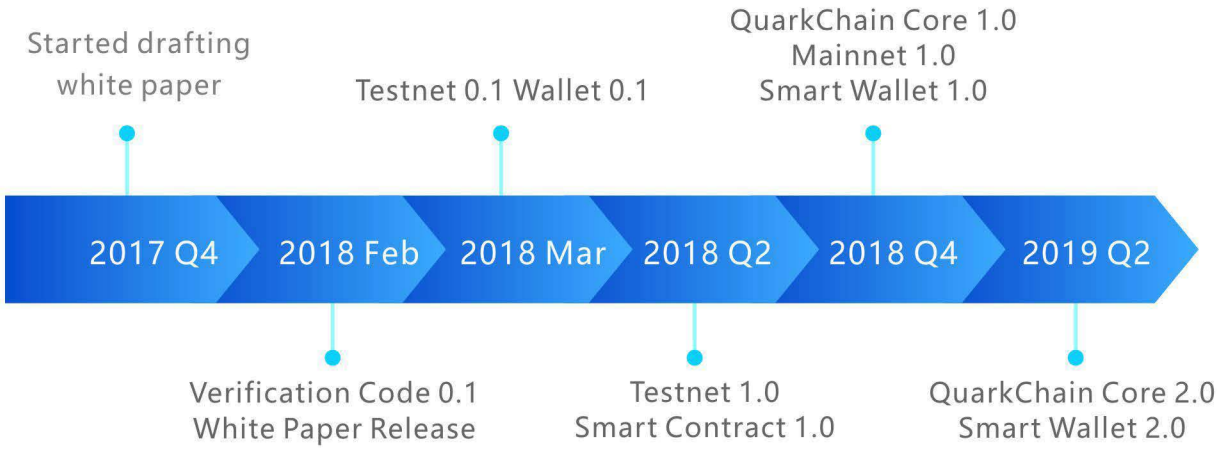
Although it is still under investigation, blockchain has shown a great potential to be applied for Internet of Things (IoT). Using blockchain can reduce the cost of money transfer and also helps the rapid realization of the value of IoT transfer. However, IoT usually contains a large number of devices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

7.2.5 The QuarkChain Network 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 the blockchain design to include the reshardable functionality and the QuarkChain Network 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 the platform of the QuarkChain Network , many data mining algorithms can be developed and economic models can be developed. The QuarkChain Network 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 the design of the QuarkChain Network with higher efficiency.

8. Roadmap and Timeline



Q4 2017: Started drafting white paper;

Feb. 2018: Delivered a version of white paper and developed verification code 0.1 which mainly serves as proof of concept for our system;

Mar. 2018: Released Testnet 0.1 with Wallet 0.1. Testnet 0.1 supports basic transactions including both in-shard and cross-shard transactions. (Projected plans below)

Q2 2018: Release Testnet 1.0 with smart contract support.

Q4 2018: Release QuarkChain Core 1.0, Mainnet 1.0, together with Smart Wallet 1.0. QuarkChain Core 1.0 will provide basic functionalities of the QuarkChain Network and basic optimization. There is a plan to launch the mainnet at the same time.

Q2 2019: 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 of small scale 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 with 6 years work experience at Facebook and Google.
•Build 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
•Expert in signal processing for wireless systems, big data, IoT

Yaodong Yang / Research Scientist
•Professor at Xianjiao Tong Univ.
•Partner of Demo++
•PhD from Virginia Tech
•Dedicated on Blockchain development and research

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

Operation Team

Ting Du / Business Development and Eco-system
- Founder of incubator Demo++, Incubator of Ink, Ziggurat
- Geek in Product Management
- Committee of Liuhe Capital Shanghai
- Dedicated on Blockchain productization and business application

Anthurine Xiang / Marketing and Community
- 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
- Extensive experience in startup, crypto investments and building up ecosystem

Patrick Mei / Creative and Content
- Founder of investment firm, 3 years experience in financial investment
- Crypto media writer
- Bachelor from Fudan University

Julianne Zhu / Social Media Broadcasting
- MBA from Rutgers University,
- Former BD Director from Roboterra
- expertise in business development and marketing

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

10. Risks

You acknowledge and agree that there are numerous risks associated with purchasing QKC, holding QKC, and using QKC for participation in the QuarkChain Network. In the worst scenario, this could lead to the loss of all or part of the QKC which had been purchased.

10.1 Uncertain Regulations and Enforcement Actions

The regulatory status of QKC and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of virtual currencies has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including QKC and/or the QuarkChain Network. Regulatory actions could negatively impact QKC and/or the QuarkChain Network in various ways. The Foundation (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, the Foundation will apply a cautious approach towards the sale of QKC. Therefore, for the token sale, the Foundation may constantly adjust the sale strategy in order to avoid relevant legal risks as much as possible. For the token sale the Foundation is working with Tzedek Law LLC, a boutique corporate law firm in Singapore with a good reputation in the blockchain space.

10.2 Inadequate disclosure of information

As at the date hereof, the QuarkChain Network is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to the QuarkChain Network, it is not absolutely complete and may still be adjusted and updated by the QuarkChain team from time to time. The QuarkChain team has no ability and obligation to keep holders of QKC informed of every detail (including development progress and expected milestones) regarding the project to develop the QuarkChain Network, hence insufficient information disclosure is inevitable and reasonable.

10.3 Competitors

Various types of decentralised applications are emerging at a rapid rate, and the industry is increasingly competitive. It is possible that alternative networks could be established that utilise the same or similar code and protocol underlying QKC and/or the QuarkChain Network and attempt to re-create similar facilities. The QuarkChain Network may be required to compete with these alternative networks, which could negatively impact QKC and/or the QuarkChain Network.

10.4 Loss of Talent

The development of the QuarkChain Network depends on the continued co-operation of the existing technical team and expert consultants, who are highly knowledgeable and experienced in their respective sectors. The loss of any member may adversely affect the QuarkChain Network or its future development. Further, stability and cohesion within the team is critical to the overall development of the QuarkChain Network. There is the possibility that conflict within the team and/or departure of core personnel may occur, resulting in negative influence on the project in the future.

10.5 Failure to develop

There is the risk that the development of the QuarkChain Network will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or QKC, unforeseen technical difficulties, and shortage of development funds for activities.

10.6 Security weaknesses

Hackers or other malicious groups or organisations may attempt to interfere with QKC and/or the QuarkChain Network in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Foundation or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of QKC and/or the QuarkChain Network, which could negatively affect QKC and/or the QuarkChain Network.

Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to QKC and/or the QuarkChain Network by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

10.7 Other risks

In addition, the potential risks briefly mentioned above are not exhaustive and there are other risks (as more particularly set out in the Terms and Conditions) associated with your purchase, holding and use of QKC, including those that the Foundation cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Foundation, its affiliates and the QuarkChain team, as well as understand the overall framework, mission and vision for the QuarkChain Network prior to purchasing QKC.