QTUM

DEFINING THE BLOCKCHAIN ECONOMY

Qtum Blockchain New Whitepaper

2020/02/24

QTUM.ORG

Preface

Before the birth of Bitcoin, global information transmission was achieved through the Internet's TCP/IP (Transmission Control Protocol / Internet Protocol) protocol to achieve high-speed and low-cost transmission. But as the communication technology developed (Internet, IoT, VR / AR), people and devices interaction methods have become more diversified and more assets are digitized or tokenized. Simply sharing and transmission of information cannot meet the demands of economic and social development, so when assets are digitalized or tokenized, people pay more and more attention to value transfer and how to transfer these assets and value point-to-point.

On October 31, 2008, Satoshi Nakamoto published the first Bitcoin white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System", and proposed the value transfer through the decentralized Bitcoin network. In the Bitcoin system, participants throughout the network directly control the transactions, and both parties to the transaction can complete the transaction without establishing a trust relationship. Blockchain technology has changed the way we acquire and share information, creating a new distributed, peer-to-peer ecological society.

Since the Bitcoin code was open-sourced in 2009, many blockchain projects have appeared in the community. Some projects are committed to becoming a universal smart contract and decentralized application platform, and the blockchain industry is developing these new technologies also with an industry application perspective. The growth of blockchain faces many challenges, which are mainly reflected in the following aspects:

1. There is insufficient compatibility between different blockchain platforms. For example, the Bitcoin ecosystem based on the UTXO (Unspent Transaction Output) model is not compatible with the Ethereum ecosystem based on the Account model, and the interoperability between blockchains is not strong;
2. On-chain governance of critical technical parameters is difficult to achieve. For most decentralized platforms, once the mainnet deployment is completed, upgrade and governance of the blockchain is a major problem;
3. The consensus mechanism lacks flexibility. The Proof-of-Work consensus mechanism has certain limitations in terms of energy requirements and incentives for miners and currency holders, and there is a risk of centralization in mining computing power;
4. Lack of new smart contract platforms. Most blockchain projects lack a connection to the real world, limiting the wide application for various industries.

1

Design Rationale

In response to various problems in blockchain technology and industrial applications, the Qtum Chain development team united the community development forces, dug into the underlying technology, and developed and implemented a series of technologies through the "Value Transfer Protocol" upgrade and other innovative solutions to build a sustainable public blockchain.

By creating the AAL (Account Abstraction Layer) the UTXO model and the smart contract Account model ecosystem were integrated, effectively solving the problem of insufficient compatibility between different blockchains;

Innovative research and development of the Qtum x86 virtual machine further enriched the programming development capability, decoupled the operating system from the virtual machine, and pushed the development of smart contracts to the mainstream;

Innovatively launched the PoS (Proof-of-Stake) consensus mechanism, with PoS nodes spread all over the world, enabling the effective collaboration of global PoS peer-to-peer networks;

Developed the first DGP (Decentralized Governance Protocol) system for on-chain governance to maintain the stable operation of the entire system.

To meet the operating system and development needs of different users, and keep truly open source, Qtum Chain provides different versions of the Qtum system, including mobile terminal services, launching commercial path modules to encourage third-party developers and create an influential worldwide open source community ecology. The ultimate goal is to integrate the blockchain into different industries such as finance, social networking, gaming, and the Internet of Things.

As the most promising blockchain ecosystem, the Qtum Chain perfectly combines the advantages of Bitcoin and Ethereum and solves the inherent shortcomings of existing blockchain systems. Qtum Chain will continue to build a basic platform, as well as the development and iteration of various product development and commercialization projects, to gradually form a blockchain economy, improve industry efficiency, and promote the efficient and coordinated development of the blockchain economy.

Qtum Chain — Defining the Blockchain Economy.

2

Governance Mechanism

As a decentralized public chain, the Qtum Chain regards blockchain governance as an important aspect of achieving sustainable development. The governance model of the Qtum Chain includes two main aspects. One is on-chain governance which uses DGP, the other is off-chain governance, which established the non-profit Qtum Chain Foundation. Through the introduction of DGP and the establishment of the Qtum Chain Foundation, Qtum Chain applies both human governance and code governance to the public blockchain, thereby realizing the decentralization of blockchain governance and effective governance decision-making.

2.1 On-chain Governance Based on DGP

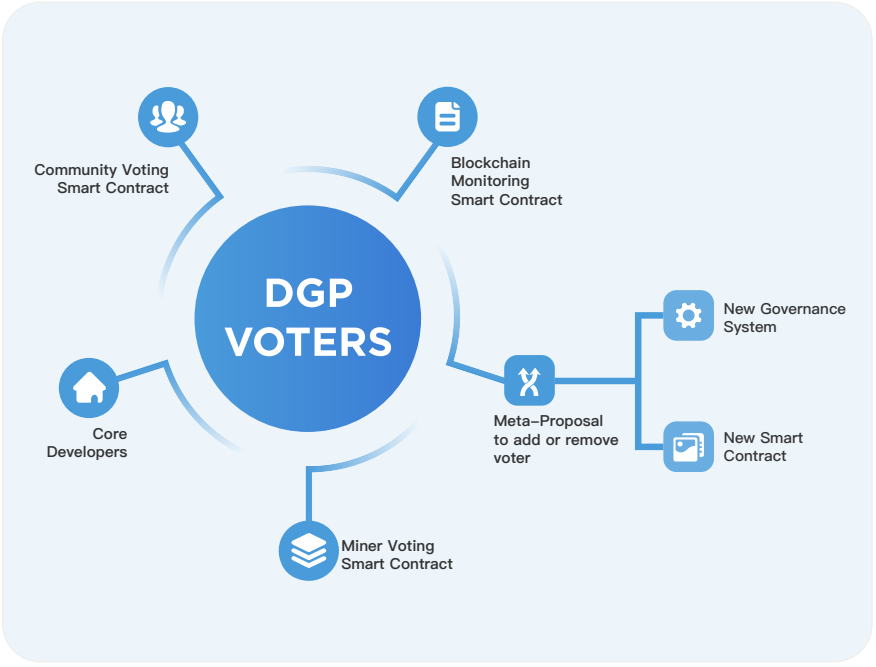
On-chain governance is the negotiation and execution process of the blockchain network update protocol embedded in the Qtum blockchain system. Qtum Chain provides a new on-chain governance model for blockchain networks by the design of DGP.

2.1.1 Multi-Party Involved On-chain Governance

The core character of DGP is that in addition to allowing QTUM token holders to participate in the voting and negotiation of the upgrade and iteration of the blockchain network, it also introduces a way for other participants in the ecosystem, including developers, community member representatives, miners, and other multi-party participants to propose and vote for on-chain governance proposals.

2.1.2 Smart Contract as the Carrier of On-chain Governance

DGP manages the parameters of the blockchain network through smart contracts embedded in the genesis blocks and clarifies the governance seats and proportion of governance participants for each party. Any participant can initiate a proposal, and the type of proposal includes the increase of management or governance seats, deletion, modification of common network parameters, etc. Participants with governance seats vote on the proposal, decide whether the proposal is approved, and execute the approved proposals through smart contracts.



2.1.3 Public and Transparent On-chain Governance

The on-chain governance mechanism on the DGP is compulsory and automatic. It can realize the automatic upgrade and continuous update iteration of the Qtum blockchain system through real-time effective decision-making and execution mechanisms. At the same time, the on-chain governance process is public and transparent, and the process is easy to audit and traceback, which helps to ensure the fairness of the entire governance process and improves decision-making efficiency without worrying about the impact of the soft and hard forks on the network and the community.

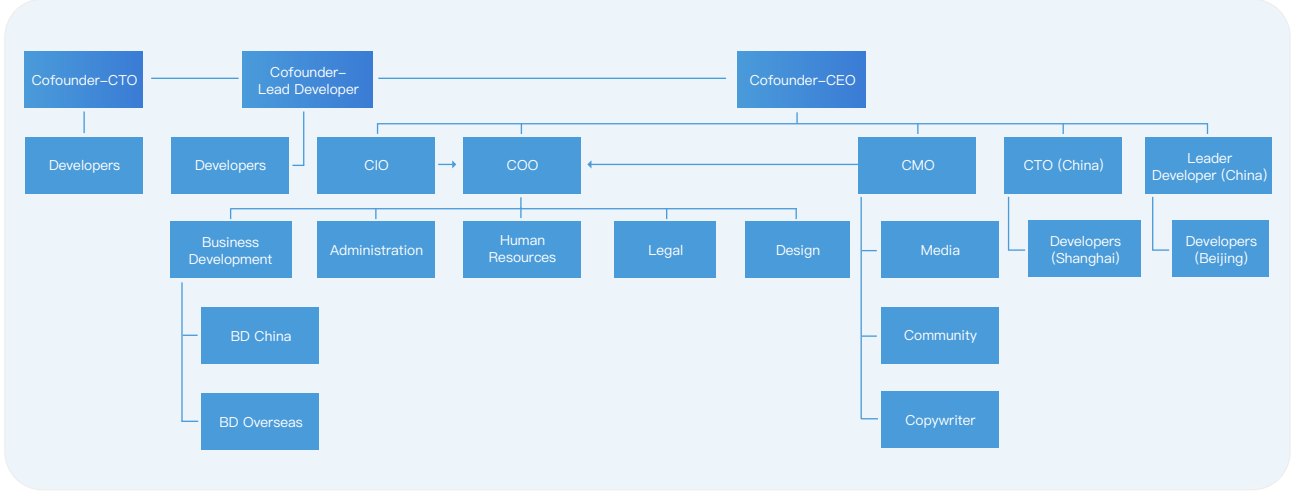
2.2 Qtum Chain Foundation

The Qtum Chain Foundation is a non-profit company officially registered in Singapore in November 2016. The Qtum Chain Foundation helps to manage the general development, progress, and privileges of open source community projects through the development of good governance mechanisms. It is committed to the development and construction of the Qtum blockchain project and the advocacy and promotion of governance transparency to promote the safe and harmonious development of the project.

The design goals of the Qtum Chain Foundation governance structure mainly consider the sustainability of open source community projects, the effectiveness of management, and the safety of raised funds.

2.2.1 Qtum Chain Foundation Governance Structure

The Qtum Chain Foundation governance structure includes operational procedures and rules for daily work and special situations. The organization structure of the Qtum Chain Foundation is as follows:



The Qtum Chain Foundation has three Cofounders, holding the positions of Chief Executive Officer, Chief Technical Officer, and Lead Developer. The three Cofounders are responsible for the overall strategic planning of the Foundation, the design and technical management of the technical framework, the Foundation's security audit, code management, leadership development of key components, overall progress supervision, and jointly determine the direction of the Foundation's development.

Under Cofounders, the Foundation has positions such as COO, CIO, China CTO, and China Lead Developer, CMO– to ensure the normal operation of the Foundation. The specific functions are as follows:

COO

Chief Operating Officer – responsible for the construction and standardization of the Foundation's management system and work processes; follow up the various plans of the Foundation, conduct follow–up supervision, inter–department coordination, summary and evaluation; conduct industry and market research.

CIO

Chief Information Officer – cooperate with the strategic planning of the foundation, carry out implementation and follow–up supervision; connect and follow up with overseas partners; carry out industry and market research.

China CTO and China Lead Developer

Lead Qtum's technical team, participate in the formulation of research & development plans and implementation; conduct technical research in related fields; manage the developer community.

CMO

Chief Marketing Officer — formulate and implement work plans of the Foundation’s global public relations management; responsible for the Foundation’s market expansion and advertising, including events and conferences, community management, media relationship maintenance, information release, etc.; responsible for handling crisis public relations and assessing third–party public relations agencies.

The foundation has design, human resources, public relations, business development, management, and other departments to carry out work in the corresponding areas.

3

Technical Characteristics

3.1 Account Abstraction Layer

To achieve the interoperability and combine the UTXO model and the smart contract Account model, and decouple the value transfer layer from the contract execution layer, Qtum created the Account Abstraction Layer (AAL).

Qtum developed optimizations for the interface and conversion between smart contract operations and UTXO operations, and developed four new opcodes:

OP_CREATE: create a smart contract
OP_CALL: call smart contract (send QTUM to the contract)
OP_SPEND: spend QTUM in smart contract
OP_SENDER: allow address other than contract call sender to pay for Gas

When the Qtum blockchain generates new blocks, in addition to making regular checks on transaction scripts, it also needs to check whether transactions contain the above-mentioned opcodes. OP_CREATE is used to pass the contract bytecode to the virtual machine. OP_CALL sends data, gasPrice, gasLimit, VMversion and other key parameters required to run smart contracts through transaction scripts, and finally passes them to the virtual machine. Relying on this design, the Qtum x86 virtual machine can run on the blockchain in parallel with the EVM (Ethereum Virtual Machine), without the need to significantly modify the underlying protocol and retaining good functional scalability. In the future, any virtual machine based on the account model can be adapted to run on the Qtum blockchain.

In addition to a large number of adaptations and improvements in functionality, the Qtum also borrowed the concept of Gas from Ethereum, used the Gas model in the contract operation, and optimized the Gas model of the EVM. Use of the Gas model can prevent endless loops caused by errors and malicious attacks, can allow miners to get rewards for performing calculations based on actual workload, and encourage contract designers and users to make reasonable use of on-chain resources. Normally the address of the contract call sender pays the Gas, but the OP_SENDER opcode allows a third-party address, such as a distributed application service provider, to pay the Gas. Similar to EVM, there is also a state rollback for “out of Gas” and a refund of remaining Gas after successful execution. In response to these situations and some rare boundary use cases, Qtum has appropriate processing to ensure the normal and efficient operation of smart contracts.

3.2 x86 Virtual Machine

Based on the strong scalability of the AAL, the Qtum Chain can implement multiple virtual machines running in parallel without changing the underlying architecture. Qtum is developing a new design Qtum x86 virtual machine. The x86 virtual machine uses Von Neumann computer architecture, which means that the code is data, which conforms to the mainstream contemporary programming model. The basic principles of the x86 virtual machine ensure that it is possible to write smart contracts that run on the Qtum blockchain by making simple modifications and using many existing compilers and programming languages. Almost all compilers currently support the x86 architecture instruction set, so the actual bytecode and architecture support is very complete.

Qtum's x86 virtual machine will support the i686 instruction set and will initially support the Rust language. Therefore the x86 virtual machine will automatically inherit the support of this upper–level language and development tools so that Qtum can get rid of the limitations of EVM computing limitations and Solidity language issues, and can implement features more efficiently, such as variable–length key values, linear memory, and bring real–time on–chain data analysis.

The use of x86 virtual machine can also provide developers with more standard libraries. These standard libraries will exist like pre–compiled contracts, and their fees and prices can be managed through DGP, which will greatly reduce the difficulty of developing smart contracts and development operating costs. In addition to the kernel of the virtual machine, the Qtum x86 virtual machine includes the design of a storage lease model and a new state storage model to solve the problem of excessive growth for the blockchain.

3.3 Mutualized Proof-of-Stake Consensus Mechanism

Another innovation of Qtum is the MPoS (Mutualized Proof-of-Stake) consensus mechanism. The general Proof-of-Stake mechanism does not have the problem of competition in computing power, and the hardware threshold requirements are low, so it is more conducive to the decentralized distribution of nodes. Qtum's MPoS algorithm is improved from PoS 3.0, but the combination of the traditional PoS consensus mechanism and smart contracts will bring security risks such as "junk contract" attacks and cannot be used directly in Qtum. In this regard, Qtum increases the cost of attacks by sharing the block reward among block-producing nodes and delaying the payments. Each new block reward is divided equally between the block producing miner and 9 previous miners (10% of the reward to each), and the remaining 90% of the rewards are delayed by 500 blocks. The improvement of this revenue mechanism does not change the core logic of PoS 3.0 and makes it impossible for attackers to predict how much block rewards can be obtained, nor to obtain block rewards immediately, thereby greatly increasing the cost of launch "junk contract" attack. (There is only a theoretical possibility, and it is impossible to achieve in practice).

3.4 Decentralized Governance Protocol

Blockchain communities often split and generate new blockchains through contentious hard forks because of different opinions about the development direction of a project. These different opinions can be roughly divided into three categories:

·Disagreements in the development direction of project algorithms and functions;
·Fix key loopholes and rollback successful attacks;
·Disagreements on certain parameters of the blockchain.

The first two must be solved using a hard fork in most cases, but the third type of problem can be solved more gently. DGP's framework is implemented through several smart contracts deployed in the genesis blocks. The basic governance structure is that miners (stakers), developers, and QTUM holders within the entire ecosystem are involved in blockchain governance. The process of governance is completed by voting, and the blockchain can realize self-management, upgrades, and iteration.

The implementation of DGP core logic is composed of a series of smart contracts (including framework contracts and feature contracts). The Qtum nodes contain code that incorporate these smart contract parameters to control Gas pricing and block size. These critical consensus parameters can be modified by the DGP process for an on-chain software update which does not require a hard fork.

3.5 Qtum 2.0

After two years of stable operation of the main network, the first Qtum hard fork upgraded a consensus algorithm and added new opcodes. To adapt to the ever-changing application scenarios of blockchain technology, Qtum will gradually upgrade the underlying protocol and launch Qtum 2.0. In addition to upgrading and optimizing the underlying block spacing algorithm, Qtum 2.0 also included a series of new features to expand the boundaries of the use of the blockchain and enrich the functions of the Qtum blockchain. Future features will include confidential assets, offline staking, and chain-cloud integration.

Confidential assets

Qtum plans to support the issuance and circulation of private assets through smart contracts, and to reduce the development and use costs of private asset-related contracts on the Qtum blockchain by deploying pre-compiled contracts and optimizing the privacy certification data structure. In the recent upgrade of Qtum 2.0, btc_ecrecover pre-compiled contracts have been deployed. In the future, more pre-compiled contracts on secp256k1 elliptic curves and Schnorr signatures will be deployed to further reduce the deployment and operation costs of privacy asset solutions.

Offline staking

In the standard Qtum PoS system, the nodes participating in staking must stay online, and online stakers improve the security and operations of the network, but this design has limitations for ordinary holders. The offline staking mechanism that Qtum is developing can solve the above problems well. Ordinary users can delegate the rights of staking to special online staking nodes, so there is no need to keep their nodes online, and they always have control of their tokens which can be safely held offline and spent at any time.

Chain–cloud integration

The development of the blockchain to this day still does not depart from the logic of Bitcoin's block–by–time plus global synchronization verification. This is not a big problem for the use of low–interaction actions such as value transfers, but it may not be the best for application platforms. It can be seen that some simple small games can block Ethereum, EOS and other platforms, so in large–scale commercial applications, the existing public blockchain platform is inadequate. The Qtum team believes that the most important feature that blockchain brings to applications is not "decentralization", but rather the following three "blockchain features":

·"Four in one" authority management mechanism for accounts, addresses, funds, and identities;
·Comes with a natural clearing and settlement network;
·High–speed growth brought by incentives and liquidity.

These are the features that are lacking in all existing Internet applications. Most of the existing Internet applications are deployed on the cloud, and in the foreseeable future, applications deployed on the cloud will remain mainstream. The Qtum team believes that the fusion of the above–mentioned blockchain characteristics with applications deployed on the cloud will generate new application forms and promote the true adoption of blockchain.

4

Economic Model

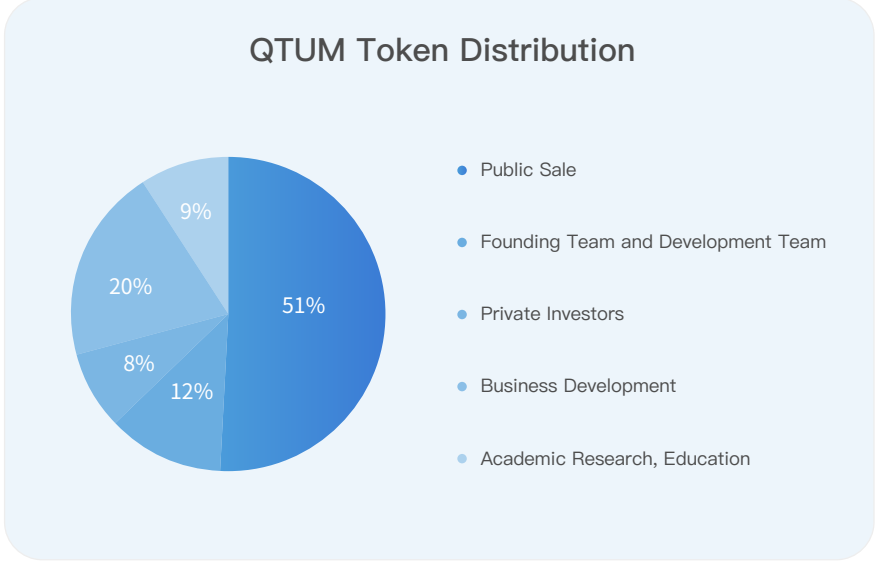
4.1 Initial QTUM Token Distribution

The initial supply of QTUM was 100 million, which was generated in the coinbase transaction at 20,000 QTUM per block for the first 5,000 blocks of the Qtum blockchain.

Of the initially created tokens, 51%, or 51 million QTUMs, were sold to the public in March 2017. Revenue from this public sale funds the operation of the Qtum Chain Foundation, including system development, marketing, financial and legal consulting.

20%, or 20 million QTUMs, will be allocated to the founding team, private investors, and development teams. Among them, 7% –8% will be allocated to private investors, and 12% –13% will be allocated to the founding team and development team.

29%, or 29 million QTUMs, will be used for commercial and community development, academic research, education, and market expansion. Of this, 20% will be used for business development, including expansion of industry–related applications, supporting DApp (Distributed Application) development, business expenses (legal, compliance, accounting, consulting), marketing and public relations, and token swaps. The remaining 9% will be used to support academic research, developer education, promotion of Qtum chain technology, and cooperation with the open–source community.



To protect the interests of investors and ensure the healthy long-term operation of the project, in addition to the regulations on the use of the QTUM tokens, the Qtum Foundation also designed a lock-up mechanism for some development funds. The details are as follows:

Entity	Percentage	Amount	Lock-up
Qtum Community	51%	51,000,000	No lock-up
Early Supporter	8%	8,000,000	No lock-up
Team	12%	12,000,000	Distributed in four years
Academic Research, Education and Market Extension	9%	9,000,000	4-year lock-up. From March 2017 to 2021, each March unlock a quarter (2.25 million QTUM).
Business Development	20%	20,000,000	4-year lock-up. From March 2017 to 2021, each March unlocks a certain part. The unlock amounts for each year are 7 million QTUM 6 million QTUM 3.5 million QTUM 3.5 million QTUM respectively.

4.2 Staking Reward

As mentioned earlier, the incentive of block rewards for stakers (miners) are given in three parts: a subsidy of newly minted QTUM, transaction fees from QTUM token transfers, and Gas fees from using smart contracts.

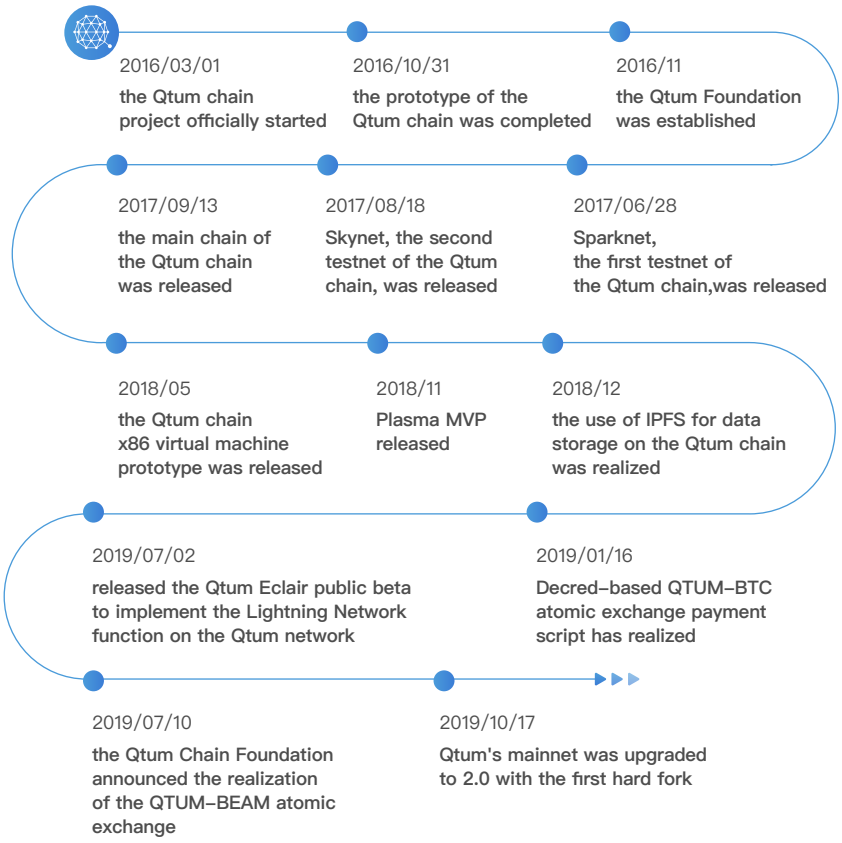
In addition to the initially issued tokens, newly minted QTUM will be issued with block rewards. The initial block reward subsidy is 4.0 QTUM per block, which is halved every 4 years with no subsidy by 2045. Therefore, in the first four years, the annual issuance ratio (inflation rate) is about 1% of the total supply. With the increase of the issuance and the halving of block rewards, the issuance ratio will gradually decrease until there is no additional issuance.

According to the Qtum node code, every 985,500 blocks (for code see qtum/src/chainparams.cpp), the block reward subsidy will be halved. Calculated at the design block interval of 128 seconds, the block reward of Qtum will be halved every 4 years, a total of seven times and then set to zero.

5

Implementation and Iteration

5.1 Milestones



Appendix

Terminology

Bitcoin

The first successful peer-to-peer electronic cash system, the global community expects to become an electronic gold system in the future.

Cryptocurrency

In the '90s of the last century, the continuation of the spirit of crypto punk, to build a cryptocurrency that minimizes trust, and serves all Internet users who value privacy and personal rights. BTC (Bitcoin) is a type of cryptocurrency.

Blockchain

IBM is a contributor to this concept. In 2015, IBM vigorously promoted the concepts of Permission Blockchain and Blockchain for commercial purposes, which is a general reference concept.

Public chain

Starting from Ethereum, it is hoped that a network can provide different object-oriented services in addition to a standard symbol system. An ideal public chain platform needs to join network nodes without thresholds and service access without thresholds. Besides, the services operated above must be valuable. According to this standard, the industry has no public chain for the mass market. But there are many different "symbol" distribution networks.

Blockchain core technology

The original meaning was specific to the bitcoin blockchain, but currently refers to the entire industry. Refers to the key technologies involved in maintaining a distributed peer-to-peer network. Such as cryptography, consensus algorithm, virtual machine technology, game mechanism, peer-to-peer network, and other technologies.

Blockchain value

Building a division of labor and collaboration infrastructure in the information age. Real assets and marketable securities will first be circulated and traded on the currencyless blockchain. Because of its credit, it still comes from real-world credit injection. What does not rely on real-world credit injection is the coined blockchain network, which is still in its very infancy and it is currently very difficult to become a true public infrastructure, but this direction is constantly evolving and innovating. Public infrastructure here means, for example, putting all the goods and financial information of a city on this network.

Account Abstraction Layer (AAL)

The account abstraction layer connects the bottom layer of the UTXO model's account with the smart contract layer. Supports a variety of virtual machines in a lightly coupled manner to implement smart contracts running on the UTXO model.

Decentralized Governance Protocol (DGP)

Achieve dynamic governance using smart contracts and without requiring hard forks. Through DGP, users can dynamically modify network parameters on the chain, and implement permission management and voting.

References

1. A.M Antonopoulos. Mastering bitcoins, 2014.

2. I. Bentov, A. Gabizon, and A. Mizrahi. Cryptocurrencies Without Proof of Work, pages 142–157. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016. 3. A. Biryukov and D. Khovratovich. Equihash: Asymmetric proof-of-work based on the generalized birthday problem. Proceedings of NDSSˆa˘ A´Z16, 21–24 February 2016, San Diego, CA, USA. ISBN 1-891562-41-X, 2016.

4. B. Bisping, P.D. Brodmann, T. Jungnickel, C. Rickmann, H. Seidler, A. St¨uber, A. Wilhelm-Weidner, K. Peters, and U. Nestmann. Mechanical verification of a constructive proof for flp. In International Conference on Interactive Theorem Proving, pages 107–122. Springer, 2016.

5. Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pages 23–26. IEEE, 2017.

6. O. Bussmann. The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation, pages 473–486. Springer International Publishing, Cham, 2017.

7. C. Cachin. Architecture of the hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.

8. Krishnendu Chatterjee, Amir Kafshdar Goharshady, and Arash Pourdamghani. Hybrid mining: exploiting blockchain's computational power for distributed problem solving. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pages 374–381. ACM, 2019.

9. K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. IEEE Access, 4:2292–2303, 2016.

10. Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin G¨un Sirer, et al. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security, pages 106–125. Springer, 2016.

11. P. Dai, N. Mahi, J. Earls, and A. Norta. Smart-contract value-transfer protocols on a distributed mobile application platform. URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf, 2017.

12. Daniel Ferreira, Jin Li, and Radoslawa Nikolowa. Corporate capture of blockchain governance. Available at SSRN 3320437, 2019.

13. Johannes G¨obel and Anthony E Krzesinski. Increased block size and bitcoin blockchain dynamics. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), pages 1–6. IEEE, 2017.

14. A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov. A provably secure proof-of-stake blockchain protocol, 2016.

15. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pages 254–269. ACM, 2016.

16. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008.

17. A. Ouaddah, A.A. Elkalam, and A.A. Ouahman. Towards a Novel PrivacyPreserving Access Control Model Based on Blockchain Technology in IoT, pages 523–533. Springer International Publishing, Cham, 2017.

18. Fahad Saleh. Blockchain without waste: Proof-of-stake. Available at SSRN 3183935, 2019.

19. P. Serguei. A probabilistic analysis of the nxt forging algorithm. Ledger, 1:69–83, 2016.

20. Voshmgir Shermin. Disrupting governance with blockchains and smart contracts. Strategic Change, 26(5):499–509, 2017.

21. P Vasin. Blackcoin's proof-of-stake protocol v2, 2014.

22. M. Vukoli´c. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In International Workshop on Open Problems in Network Security, pages 112–125. Springer, 2015.

23. M. Vukoli´c. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, pages 112–125. Springer International Publishing, Cham, 2016.

24. Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7:22328–22370, 2019.

25. G. Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014.

26. Xiwei Xu, Ingo Weber, and Mark Staples. Architecture for blockchain applications. Springer, 2019.

27. Matthew A Zook and Joe Blankenship. New spaces of disruption? the failures of bitcoin and the rhetorical power of algorithmic governance. Geoforum, 96:248–255, 2018.