Front. Comput. Sci., 2024, 18(2): 182813
https://doi.org/10.1007/s11704-023-3113-x

REVIEW ARTICLE

The governance technology for blockchain systems: a survey

Guocheng ZHU[1], Debiao HE (✉)[1,2], Haoyang AN[1], Min LUO[1], Cong PENG[1]

1 School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
2 Shandong Provincial Key Laboratory of Computer Networks, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China

Abstract After the Ethereum DAO attack in 2016, which resulted in significant economic losses, blockchain governance has become a prominent research area. However, there is a lack of comprehensive and systematic literature review on blockchain governance. To deeply understand the process of blockchain governance and provide guidance for the future design of the blockchain governance model, we provide an in-depth review of blockchain governance. In this paper, first we introduce the consensus algorithms currently used in blockchain and relate them to governance theory. Second, we present the main content of off-chain governance and investigate two well-known off-chain governance projects. Third, we investigate four common on-chain governance voting techniques, then summarize the seven attributes that the on-chain governance voting process should meet, and finally analyze four well-known on-chain governance blockchain projects based on the previous research. We hope this survey will provide an in-depth insight into the potential development direction of blockchain governance and device future research agenda.

Keywords blockchain governance, off-chain governance, on-chain governance, voting

1 Introduction

As the underlying technology for digital currencies such as Bitcoin [1] and Ethereum [2], blockchain [3] has gained widespread attention from scholars due to the explosive growth of digital currencies. The characteristics of decentralization, immutability and traceability make it play a significant role in various fields such as healthcare [4], IoT [5], cloud computing [6], electronic voting [7], and others. However, in the rapid development of blockchain technology, the lack of a systematic and perfect governance process is gradually exposed.

In fact, most of the blockchain systems lack a mature and standardized governance model. In 2015, Bitcoin faced the problem of Internet congestion. Miners want to increase block capacity to accommodate more transactions, while core developers support the Bitcoin Lightning networks [8] and SegWit to solve the problem. Finally, due to the lack of a proper governance model, Bitcoin underwent a hard fork [9] on August 1, 2017, split into the BCH [10] and BTC.

The DAO, based on Ethereum, is a crowdfunding project. At that time, The DAO project crowdfunded 12 million ETH, about 150 million dollars. However, since there is no standardized governance process in Ethereum, on June 17, 2016, a hacker attacked a loophole in the smart contract and stole 3.6 million ETH [11], with a total value of about 60 million dollars. Then, Ethereum forked into ETH, Ethereum classic [12] (ETC) chain to recoup losses, and the price of ETH plunged. After this incident, more and more people have begun to pay more attention to blockchain governance.

Due to its decentralized organizational structure, Blockchain governance makes its governance process different from the centralized IT system governance. So the existing IT governance framework [13,14] and data governance evaluation models [15,16] cannot be directly used to analyze the governance model. The purpose of blockchain governance is to design a set of standardized rules and procedures, define the development direction of blockchain at the macro level, ensure the healthy development of blockchain, and solve the errors that happen in the operation of the blockchain system at the micro level. An excellent governance process can reduce data and behavior inconsistency between different nodes on the blockchain and reduce the occurrence of forks.

Blockchain governance can be categorized into two types: off-chain governance and on-chain governance. Off-chain governance primarily involves decision-making by core developers and experts. Governance decisions are typically made through community discussions and meetings, without a standardized process. Although off-chain governance can be efficient, it suffers from a lack of transparency, fairness, and a high degree of centralization.

In contrast, on-chain governance relies on voting mechanisms to make decisions. Token holders can participate in the governance process by voting on proposals, with the voting process being enforced through code to reduce the impact of human factors. This approach provides a high degree of decentralization and fairness. However, on-chain governance may also suffer from low efficiency and low participation.

Received February 13, 2023; accepted July 30, 2023

E-mail: hedebiao@163.com

1.1 Our contributions

As far as we know, the existing literature on blockchain governance primarily focuses on the conceptual understanding of blockchain governance [17], the frameworks of blockchain governance [18], and the attributes that governance must fulfill [19,20]. However, there is a lack of comprehensive coverage on the technical aspects of on-chain governance voting. This paper addresses this gap by exploring the relevant issues about on-chain governance voting. The main contributions of this paper are as follows:

1. We explain the relationship between blockchain governance and consensus mechanism and present some consensus algorithms. Then we compare these consensus mechanisms with governance theory and classify the popular blockchain platforms according to their consensus algorithms and social governance.
2. We summarize the four voting methods of existing on-chain governance and explain the process of each voting method in detail. Then we compare their advantages and disadvantages and classify some blockchain systems according to the on-chain voting methods.
3. We use the model [21] for evaluating blockchain governance to analyze Bitcoin. Then we summarize the governance process of Ethereum. Besides, we give the attributes that on-chain governance should meet and analyze three popular on-chain governance blockchain platforms.
4. We summarize the challenges of designing a blockchain governance model and propose the research direction of blockchain governance in the future based on the conclusions of this paper.

1.2 Organization of this paper

The rest of this article is structured as follows: In Section 2, we present an overview of blockchain technology and voting in blockchain governance. In Section 3, we introduce four voting methods used in on-chain governance. In Section 4, introduce the off-chain governance process of Bitcoin and Ethereum. Then we give the seven attributes of on-chain governance voting should meet and use them to analyze four on-chain governance platforms. and In Section 5, we summarize the challenges of blockchain governance and provide some broader perspectives on blockchain governance. Finally, we conclude this article in the last section.

1.3 Explanation of symbols

We have summarized all abbreviations and symbols used in this article in Table 1.

Here, the n, m, in $CS_i, i = 1,\ldots,n$, $GC_i, i = 1,\ldots,m$, mean the n numbers of cryptocurrency system and m numbers of smart contracts.

Table 1 The symbols used in this paper

Notation	Description
IoT	Internet of Things
Segwit	Segregated Witness
BCH	BitcoinCash
BTC	Bitcoin
PoW	Proof of Work
PoS	Proof of Stake
PoA	Proof of Activity
PoSe	Proof of Service
DKG	Distributed key generation
DPoS	Delegated Proof of Stake
LPoS	Liquid Proof of Stake
TPS	Transaction Per Second
EIP	Ethereum Improvement Proposal
DKG	Distributed Key Generation
CSUG	A cryptocurrency system under governance
$CS_i, i = 1,\ldots,n$	The ith well-established cryptocurrency system
$GC_i, i = 1,\ldots,m$	The ith governance smart contract on $CSUG$
$VG_i, i = 1,\ldots,n$	The voting group on CS_i that holds tokens of $CSUG$
$RC_{i,j}, i = 1,\ldots,n, j = 1,\ldots,m$	The registration smart contract on CS_i for the voting choices in the governance smart contract GC_i
$VC_{i,j}, i = 1,\ldots,n, j = 1,\ldots,m$	The voting smart contract on CS_i for the governance smart contract GC_j
$CSC_i, i = 1,\ldots,n$	The light client of CS_i
VCR	The vote counting routine
CG	The consensus group of $CSUG$
GPR	The governance proposal registry

2 Preliminaries

2.1 Blockchain structure

As shown in Fig. 1, blockchain is a chain structure where data is stored in units of blocks. The block is connected to the end of the chain in chronological order. The immutability is guaranteed by cryptography. The hash value of the previous block data points to the next block, if one changes, others change.

The blockchain contains all the transactions that have occurred since the genesis block. These transactions are transformed into a fixed-length value through a hash algorithm. The Merkle tree is built layer by layer, and finally, the root of the Merkle tree is stored in the block header to verify subsequent transactions.

2.2 Blockchain fork

Blockchain fork refers to the data and behavior of blockchain on different nodes appearing inconsistent, eventually from a chain bifurcation into two chains, so that computing power and users are dispersed, and the application running in the original chain produces errors. Currently, blockchain forks can be divided into hard forks and soft forks and we can see them in Fig. 2.

Hard fork: Hard fork means a permanent divergence in the blockchain. At the beginning of a hard fork, the system will generate many blocks according to the new specification. The unupgraded nodes can not verify these blocks and discard them. Due to the different consensus mechanisms, the hard fork will cause unupgraded nodes to continue mining on the old chain and upgraded nodes on the new branch, respectively.

The hard fork has only backward compatibility, which ensures validation of previous transactions. It creates two legal blockchains, and users can choose only one of them. You can change the block structure and call for extensive upgrades in

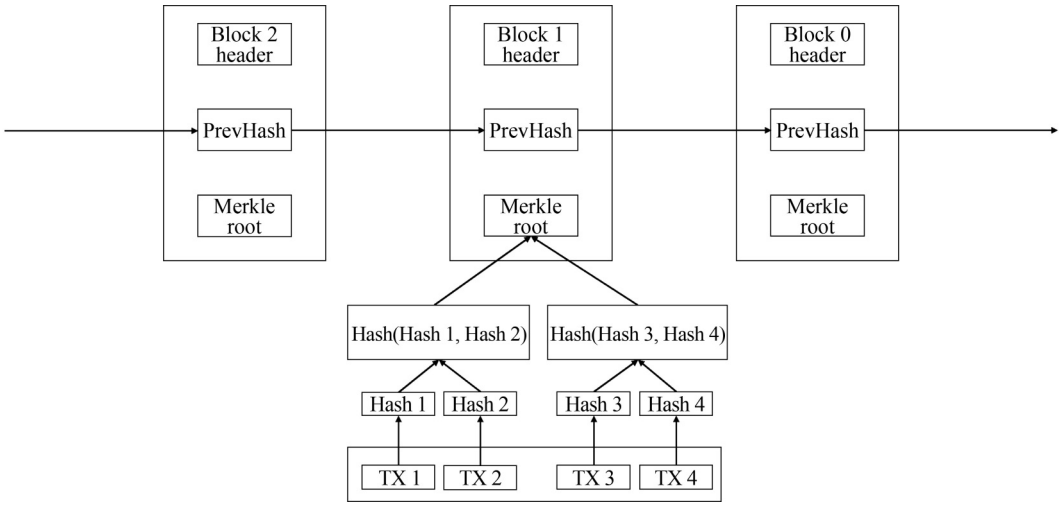


Fig. 1 The structure of blockchain

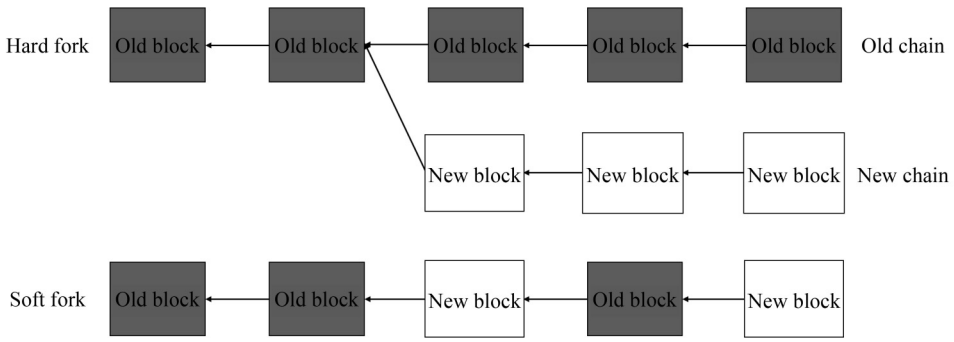


Fig. 2 Hard fork and soft fork

the hard fork. But it can split the community and scatter the number of users. If we do not take action to prevent the hard fork, there will be fewer users on the main chain, resulting in less computing power, and the security of the blockchain will be compromised.

Soft fork: Soft fork is not the real fork but a bidirectional compatible specification design. It refers to when the transaction data structure of blockchain changes, the old nodes ignore this change and can accept and verify the block produced by the new version. Two chains will not be generated after the soft fork, which is a relatively gentle way to upgrade. So it is very suitable for minor specification and protocol changes. When the soft fork happens, Miners working on the old version will gradually upgrade and slowly move to the new blockchain.

Compared to hard forks, soft forks support both backward and forward compatibility. We can not add new fields to the block but modify them under the existing structure, limiting the upgrade space. Besides, the technical implementation is complicated and unsuitable for future code maintenance.

2.3 Consensus mechanisms

The consensus mechanism is to decide how participating nodes can reach an agreement on specific data (including governance proposals) according to the design principle of "minority follows majority" in a decentralized scenario.

Different consensus mechanisms will lead to different blockchain governance models. For example, Bitcoin uses PoW give miners the power to package blocks, so they are responsible for maintaining the security and immobility in blockchain governance. Ethereum uses PoS. Bitshares, Steemit, and EOShave adopted DPoS that will allow users to delegate their governance voting rights to experts, improving the professionalism of governance proposals. Tezos has adopted LPoS.

The consensus mechanism mainly solves the problem of decision rights in the governance field, which is very important to designing an on-chain governance model. We summarize the consensus mechanisms and government type of some famous blockchain platforms in Table 2.

- PoW: PoW is a complex and time-consuming calculation that the node needs prove it has done enough work to become the block producer. In the blockchain, each node in the blockchain network can directly take part in solving the complex hash problem. Anyone solving this problem can be the block producer to package transactions and receive rewards.
- PoS: In PoS, the decision rights are determined by currency age. $currency\ age = currency\ numbers \times time$. The election of block producers relies on currency age. The higher your currency age, the more chance you have to be a block producer. The currency age decreases when a node is successfully selected as a block producer. In PoS, a small number of elites control the decision rights.

Table 2 The government type of cryptocurrency

	Launch time	Governance type	Consensus mechanism	Governance feature
Bitcoin [1]	2009	Off-chain	PoW	Decentralized
Ethereum [2]	2014	Off-chain	PoW+PoS	Decentralized
Bitshares [22]	2014	On-chain	DPoS	Representative
Dash [23]	2014	On-chain	PoW+PoSe	Decentralized
Steemit [24]	2016	On-chain	DPoS	Representative
Decred [25]	2016	On-chain and off-chain	PoA	Decentralized
Tezos [26]	2018	On-chain	LPoS	Representative
EOS [27]	2018	On-chain	DPoS	Representative

- PoA [28]: PoA combines PoW with PoS. the consensus process is as follows: First, an empty block is produced through PoW. This new block only contains the header information and the miner's reward address. Then, N verifier nodes are selected through PoS. If one of the N nodes is not online at this time, the block becomes invalid and will be abandoned. The verification signature is performed when all the N nodes receive the complete block. A legitimate block is obtained if the final verification signature passes. The miner and the N verifier nodes can share block rewards.
- PoSe: PoSe is a consensus algorithm adopted by Dash. Every master node is set to a maximum PoSe score in this algorithm. The number of registered masternodes determines the maximum PoSe score. The current PoSe scoring algorithm increases the PoSe score by 66% of the maximum score for each failed DKG session. And the score decreases by 1 per successfully mined block. The master node will be banned (the payment eligibility of the master node will be excluded) if the score exceeds the maximum threshold. Once banned, the master node can only be restored by sending a Provider update service special transaction.
- DPoS: DPoS is a robust and scalable consensus mechanism. DPoS verifies the transaction's validity by a certain number of block producers. These block producers are elected on an equal and democratic basis by the token holders. Voters are weighted by shares based on the number of tokens they own. DPoS has a faster consensus speed and higher TPS. In a blockchain system, token holders vote on block producers to select legitimate block producers to package and validate transactions. DPoS has been adopted by several blockchain projects such as Steemit, EOS, Tron, Lisk, Bitshares.
- LPoS: This consensus mechanism is used in Tezos to allow token holders to transfer verification rights to other token holders without transferring token ownership. Note that this is only an authorization. The token remains in the wallet of the consignor and can still be circulated. There is a penalty if the validator makes a security error (e.g., double-endorsing or double baking). LPoS is considered to be an upgraded version of the DPoS. We can compare them in three aspects:
  (a) Delegation purpose: In DPoS, the purpose of delegation is to elect block producers to produce blocks. While in LPoS, it is to aggregate tokens to ensure the democratic governance of these *"poor"* token holders and increase the participation of the entire community in the governance process.
  (b) The number of validators: In DPoS, the number is fixed. For example, the EOS only has 21 validators, and Lisk [29] has 101 validators. While in LPoS, the number is dynamic. In Tezos, it is up to 80000.
  (c) Design priorities: In DPoS, the design priorities are scalability and usable consumer applications. In LPoS, the design priorities are decentralization, accountable governance, and security.

3 Voting methods in on-chain governance

Voting is the way for a group to reach a consensus on an issue, usually obeying the majority rule. When a governance proposal (upgrade of the underlying protocol, modify parameters, roll back transactions, fix errors, etc.) is proposed, it requires the consent of a majority to be implemented.

If there is no standard process to express the majority's opinion, the governance process is easily manipulated by a few authoritative experts. Some users will refuse to implement the proposal when the content is not satisfied with their interests, which results in the forking of the blockchain. Voting, which can be coded into the blockchain system as a standard process, is the easiest way to solve this problem. Therefore, voting is chosen to make decisions for on-chain governance.

In this section, we will summarize and introduce the existing on-chain governance voting schemes. The comparison of the four governance voting methods is shown in Table 3.

3.1 Proxy voting

Proxy voting allows each qualified token-holder to delegate his/her voting rights to an expert. They can also cancel the proxy and vote for themselves if they are not satisfied with the

Table 3 The comparison for four governance voting methods

Voting methods	Advantages	Disadvantages	Current use
Proxy voting	Professional, flexible high participation	Accountability, centralized	Tezos, Difinity [30], Bitshares
Quartic voting	Professional, reliable high participation	Centralized, costly	Dursun et al. [31] Gitcoin [32], Kickflow [33]
Cross-chain voting	High development speed high participation, Safe	Complex, costly	MULTAV [34]
Token-lock voting	Safe, efficient	Deflation	Ping Pong [35], Decred

experts' choice. In this way, it can significantly improve the participation of blockchain governance and the professional degree of decision-making. The process of proxy voting is in Fig. 3.

The advantages of proxy voting process are as follows:

- Professionalism: The vote cast by an expert will be more professional than ordinary voters. The proposal endorsed by the experts is largely an effective proposal for the future development of the blockchain platform, which will help the system make more effective decisions.
- High participation: For those who can not understand the content of professional governance proposals, proxy voting allows them to delegate their voting rights to experts, increasing participation in the governance process.
- Flexibility: The token holders can freely choose their entrusting experts or cancel the delegate. Delegates are multi-level and can re-delegate their voting rights to someone else. This improves the flexibility of voting governance and makes voting more responsive to the collective will.

The disadvantages of proxy voting process are as follows:

- Accountability: Since token holders can freely choose agents and cancel delegating, and delegating process can be conducted several times, it is challenging to trace delegating process precisely.
- Centralization: Most ordinary token holders will delegate voting rights to a small number of experts in the system, and the decision-making rights are concentrated in the hands of a small number of experts.

3.2 Quartic voting

The theory of quadratic voting originated from economic research in 1977 [36], a new way of governance voting. The quadratic vote will enable voters to get as many votes as they want by paying the sum of the squares of the votes cast: 1^2 token for the 1 vote, 2^2 tokens for the 2 votes, …, n^2 tokens for the n votes.

In quadratic voting, voters need to pay more to get more votes for the proposal that maximizes their benefits. It is a high-risk, high-return investment, so the governance proposals passed tend to be high quality. The process of quartic voting is in Fig. 4.

The research suggests that quadratic voting may lead to higher Pareto efficiency [37]. It can also solve issues such as collusion [38] and Sybil attacks [39] in voting related to traditional blockchain.

The advantages of quartic voting are as follows:

- High participation: Ordinary votes can vote once with little cost. As for wealthy voters, the quadratic vote allows them to spend more to increase their vote share. It encourages small groups with strong preferences to actively participate in the governance process.
- Professionalism: Voting with more cost will make votes think more carefully. The proposal thus adopted is largely valid for the future development of the

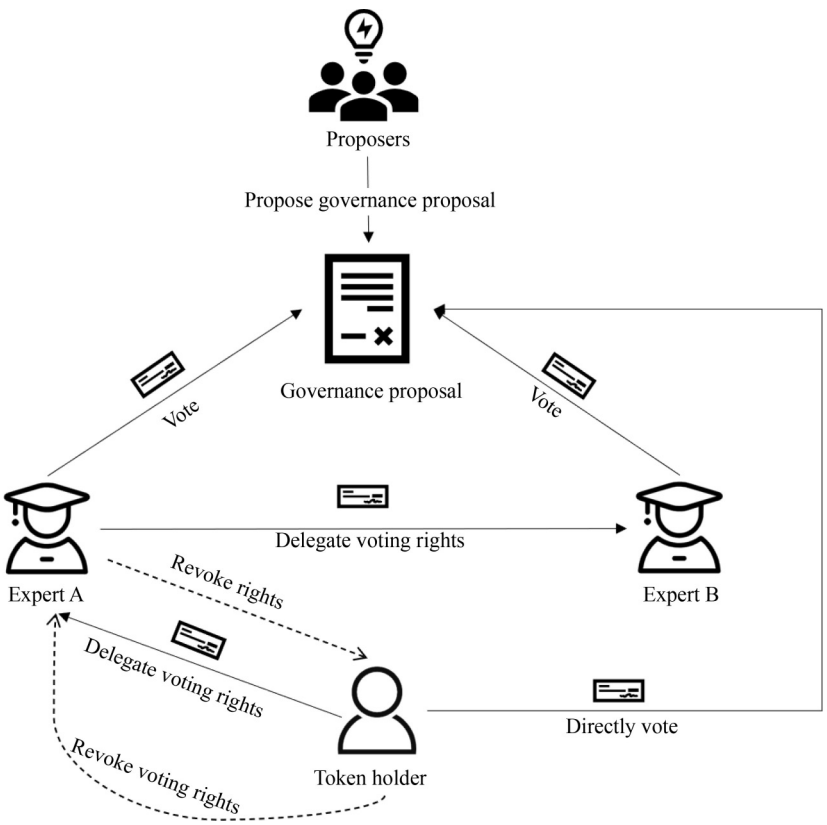


Fig. 3 Proxy voting

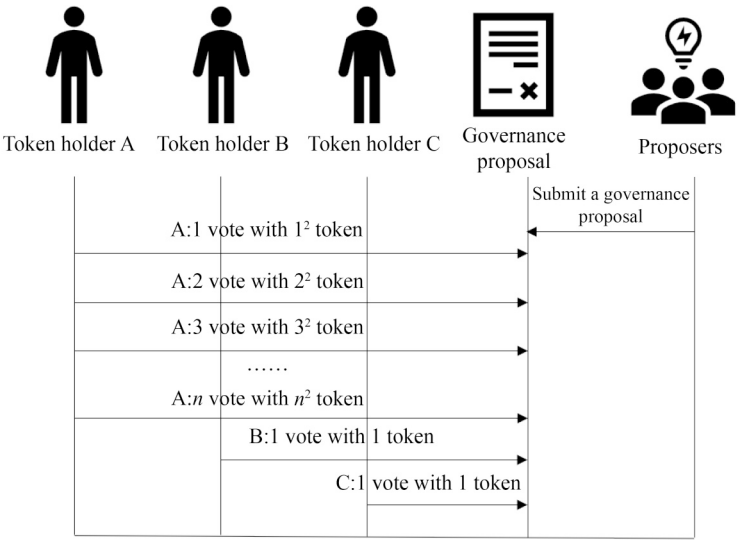


Fig. 4 Quartic voting

blockchain platform.

- Reliability: The high cost of voting reduces the malicious people's desire to manipulate the voting process.

The disadvantages of quartic voting are as follows:

- Centralization: Although there is a quadratic voting cost protection mechanism, the super-rich stakeholders who do not care about the cost can still manipulate the voting process.

3.3 Cross-chain voting

The core concept of cross-chain voting is to migrate the governance voting procedure to a well-established blockchain platform. The chosen blockchain platforms can guarantee the security and credibility of the voting results because of their robust computing power. There are four steps for implementing cross-chain voting and we can see them in Fig. 5:

1. The project manager selects the mature blockchain platform and converts the tokens of the original platform into voting tokens on a proportional basis.
2. The project developer deploys the voting smart contract on the chosen blockchain platform.
3. The proposal initiator proposes the governance proposal on the original chain, initiates the governance voting process on the selected chain, and waits for the voting result.
4. Count the votes and determine if the total approval votes pass the threshold, the governance proposal will be deployed, otherwise do nothing.

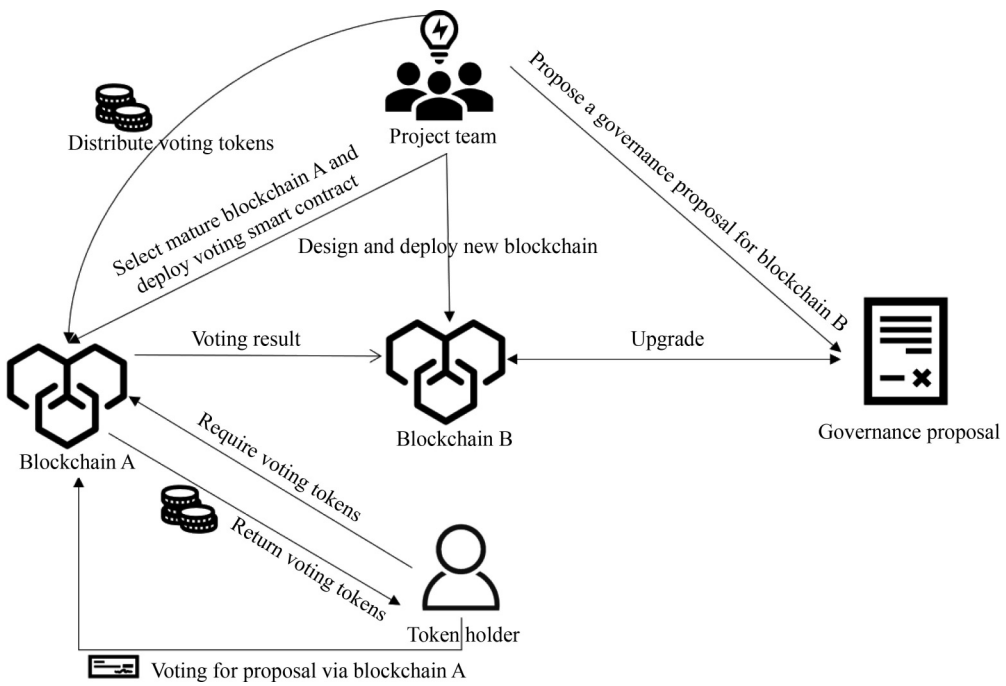


Fig. 5 Cross-chain voting

The advantages of cross-chain voting are as follows:

- Security: The mature blockchain platform has abundant computing power, so it is difficult to launch 51% attacks. The voting process is pretty safe.
- High participation rate: Token holders of the chosen blockchain platforms may be attracted to participate in the governance process of the new blockchain, which will increase the participation rate.
- Development: Token holders attracted from chosen blockchains are generally experienced users. They usually have great ideas about the development of the new blockchain and will make more professional decisions in governance.

The disadvantages of cross-chain voting are as follows:

- Complex: It is difficult and complex to design and deploy smart contracts on chosen blockchain platforms.
- High cost: There are high transaction fees for a vote on a mature blockchain like Ethereum. Initiating a transaction on Ethereum requires a gas fee, averaging $15.31 per transaction by the time of this paper. Besides there are costs associated with developing and deploying voting smart contracts.

3.4 Token-lock voting

During the on-chain voting process, a token locking mechanism can be set up to reduce malicious behavior. When stakeholders want to participate in the voting process, they need to lock a portion of the tokens to change for proposals or voting rights. If the malicious behavior is detected, the tokens will be burned (transferred to the address without the private key). Otherwise, the tokens will be returned. In this way, the malicious users will be punished for their bad behaviors. The process of token-lock voting is in Fig. 6.

The advantages of token-lock voting are as follows:

- Security: Malicious proposals and voting behavior will cause economic losses. This will reduce the frequency of malicious behavior and improve the system's security.
- Efficient: There will be a deadline for locking tokens, which requires voters to vote quickly before the deadline.

The disadvantages of token-lock voting are as follows:

- Deflation: The number of permissionless blockchain platform tokens is fixed (like 21 million tokens for Bitcoin). Burning tokens will lead to deflation in the blockchain platform.

4 The analysis of blockchain governance

4.1 Off-chain governance and analysis

Off-chain governance refers to one or more influential organizations or individuals making decisions on issues about upgrading the system, modifying the consensus mechanism, or fixing bugs in blockchain through discussion and negotiation. These decisions usually affect the overall direction of blockchain development.

The advantages of off-chain governance are as follows:

- Efficient: Off-chain governance does not need a lengthy on-chain voting process. Just a few meetings through some experts can make it.
- Professionalism: The majority of people involved are experts and core developers.
- Flexibility: Any users can initiate proposals in the community for discussion, experts can discuss by email, phone, or meeting, and core developers can communicate by Github.

The disadvantages of off-chain governance are as follows:

- High centralizetion: Only a few elites (experts and Core developers) have the right to make decisions, and most users do not directly participate in the governance process.
- Untransparent: The process and data in governance are not recorded in the blockchain.
- Incentives: Participants in off-chain governance process often have asymmetric incentives. For example: In Bitcoin, miners have a direct financial incentive (block rewards). While developers receive nothing from BIP implementation. This reduces developers' desire to

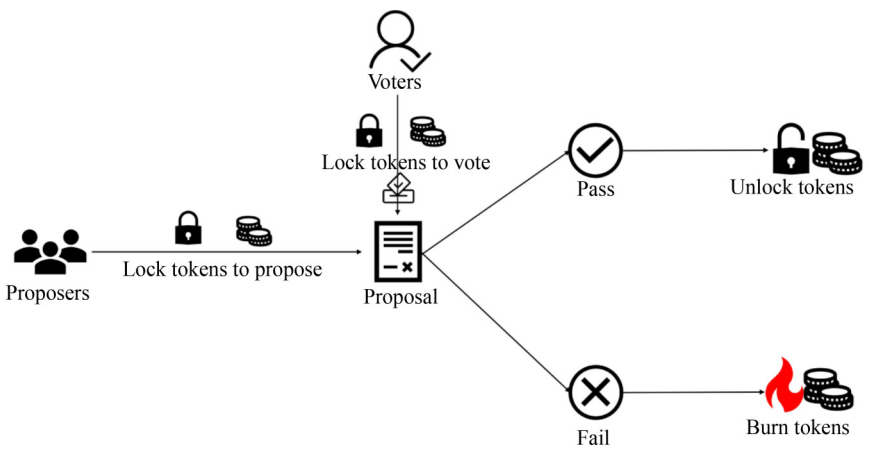


Fig. 6 Token-lock voting

participate in off-chain governance.

In the early stage of a new blockchain platform, it is better to adopt the off-chain governance method and return the governance power to the core developers and experts of the blockchain. With the increase in user numbers, we believe that the governance type can gradually transfer from off-chain to on-chain (like the transition process from PoW to PoS in Ethereum).

In this Section, we choose Bitcoin and Ethereum for the off-chain governance analysis due to the following reasons:

- Pioneering Status: Bitcoin and Ethereum are the two most well-known and widely adopted cryptocurrencies in the world. This dominance ensures that any off-chain governance mechanisms developed for these platforms would have a significant impact on the overall crypto industry.
- Community Support: Both Bitcoin and Ethereum have large and active communities of developers, experts, and normal users. This community support is crucial for implementing and testing off-chain governance mechanisms.
- Technical Maturity: Bitcoin and Ethereum have robust consensus algorithms and a long history of development, making them reliable platforms for exploring and implementing off-chain governance mechanisms

4.1.1 The analysis of Bitcoin

In the blockchain governance analysis model [21], the governance layers can be categorized into three distinct components: 1) Off-chain community governance, 2) Off-chain development governance, 3) On-chain protocol governance. Here, we provide a concise overview of each layer. The precise introduction can be referred to [21].

- Off-chain community: This layer encompasses the governance matters taking place in the real world.
- Off-chain development: This layer encompasses the governance matters taking place in the real world with an explicit focus on the software development process.
- On-chain protocol: This layer comprises all the governance matters taking place on the blockchain through its underlying protocol.

In the three layers of the blockchain governance evaluation model, we need to analyze off-chain governance projects from five dimensions: 1) Roles, 2) Incentives, 3) Membership, 4) Communication, 5) Decision making.

Now, we use the framework [21] to analyze the various elements of Bitcoin in off-chain governance.

Governance layer 1 Off-chain community:

- Roles: Token-holders, Bitcoin Foundation, Community figureheads, Online moderators.
- Incentives: All participants in the community are stakeholders, and they are shareholders in Bitcoin. The rise in the price of Bitcoin will lead to an increase in wealth for all.
- Membership: The Bitcoin community is an open community. Anyone who owns BTC can become a token-holder. There is no threshold to participate in the discussion in the community. Anyone with ideas, including opinions on the existing structure of the block, loopholes, and future developments, can freely discuss them. It is difficult to become a forum moderator. You need to be active, provide constructive suggestions for the development of Bitcoin, and gain recognition and respect from other community members. There is no fixed application process.
- Communication: Off-chain communication occurs via the Bitcoin talk, Reddit, Twitter, etc.
- Decision making: Anyone can freely express their opinions within the community. There is no fixed voting process. When an idea is inspiring, the community moderators will post it to let more involved together. Users can initiate a vote for a proposal without official regulations. In the Bitcoin community, everything is liberty.

Governance layer 2 Off-chain development:

- Roles: Core developers, Contributors, Maintainners (miners), BIP editors.
- Incentives: Ordinary contributors are mainly motivated by their passion for coding and establishing a social reputation. They do not receive direct financial rewards. The Bitcoin Foundation funded the core developers from 2012 to 2015 and by MIT's DCI program after 2015. There are also other Bitcoin-supporting organizations like Blockstream, Chaincode Labs, etc.
- Membership: It is difficult to become a core developer who requires a lot of code capability and contribution to Bitcoin. No one cares about your background; the only thing that matters is your work quality. There is no threshold for ordinary developers and contributors. Anyone who wants to contribute to Bitcoin can become a contributor.
- Communication: Bitcoin developers communicate via e-mail lists and the annotation system on Github. They can share through Bitcoin-talk, Twitter, QQ, Reddit, etc.
- Decision making: When developers update Bitcoin, it is through the BIP process on Github. Anyone can propose an updated proposal, but only the core developers have the right to confirm a BIP proposal. Any BIP proposal needs to go through the 7-step life cycle: thinking, suggestion, formal proposal, code implementation, activation setting, release version, activation.

Governance layer 3 On-chain protocol:

- Roles: Miners, Full nodes, Lightweight nodes.
- Incentives: The miner's earnings are divided into block rewards and transaction fees. At the time of writing, the block bonus per block is 6.25 BTC. The transaction fee determined by the initiators will influence the speed of

packaging. For full nodes, there is no economic incentive. However, if there is a hard fork in the blockchain, the full nodes have the right to verify the blockchain's rules. The incentive to run full nodes can be an indirect vote to let miners know which rules their users support. There is no extra incentive to run light nodes. Users can participate in the Bitcoin network by running light nodes.

- Membership: Anyone can run a mining node, a full node, or a light node. The actual situation is that if you want to be a miner in Bitcoin, there are high requirements for equipment, and Application Specific Integrated Circuit (ASIC) chips are generally required. Running a full node requires large memory of the computer. Light nodes can run on mobile devices with lower requirements.
- Communication: The communication between nodes is through the P2P network, and the propagation of transactions adopts the Gossip protocol [40]. After a transaction is created, it is first sent by the source node to its neighbor nodes, which forward the transaction to their neighbor nodes. At this time, the full node updates the ledger information of the entire network, and when receiving the transaction, it verifies the validity of the transaction. A light node is a normal node in the P2P network and does not have all the ledger information of the entire network. It needs to connect to the full nodes when communicating.
- Decision making: The consensus mechanism in Bitcoin is PoW. There is no voting mechanism in Bitcoin. The longest chain principle is applied to solve transaction conflict. A transaction requires six-block confirmations to be considered legitimate in the Bitcoin system.

4.1.2 The analysis of Ethereum

Ethereum governance is primarily done through EIP [41], a designed document providing information to the Ethereum community. As is shown in Fig. 7, EIP can be divided into 3 types:

- Standards Track EIP: This kind of EIP describes changes to underlying technical details, such as network protocols, block structures, and transaction rules.
- Meta EIP: This kind of EIP describes a change to (or an event in) a process. Meta-EIPs apply to areas other than the Ethereum protocol itself. They may propose an implementation, but not to Ethereum's codebase; they often require community consensus.
- Informational EIP: This kind of EIP describes an Ethereum design issue, or provides general guidelines or information to the Ethereum community, but does not propose a new feature.

The governance process can be briefly summarized as follows:

1. Ethereum participants (users, miners, core developers) think about how Ethereum can be improved or upgraded, collect suggestions from the community, listen to user needs, summarize and submit to Github in a standardized format as an EIP;
2. After submission, the proposal goes through a life cycle of technical review, research, and discussion. In this process, the author modifies the EIP according to the modification suggestions to meet the requirements of different users. After completing the modification, the protocol will be shown to developers again and go to the next step;
3. When the EIP is approved, it will be deployed on the test network. The EIP will be activated, and the whole network will upgrade after passing testing.

The specific analysis of Ethereum can be referred to [21].

4.2 On-chain governance and analysis

In this section, we first introduce the attributes of voting in on-chain governance, then we use these attributes to analyze Tezos, MULTAV and Dash.

We choose MULTAV for our research because it represents a novel on-chain governance approach that introduces cross-chain voting, a concept that has not been previously implemented. Thus, our analysis focuses on studying and researching its unique governance mechanism.

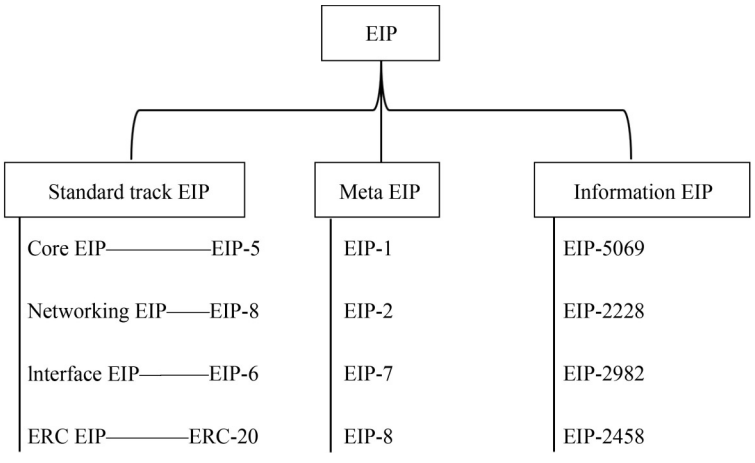


Fig. 7 EIP category

As for Tezos and Dash, the reasons are as follows:

- On-chain governance focus: Tezos and Dash are two prominent cryptocurrencies that specifically emphasize on-chain governance as a core feature. They have implemented mechanisms that allow token holders to participate in decision-making processes directly on the blockchain.
- Different approaches: Tezos and Dash take distinct approaches to on-chain governance. Tezos utilizes a liquid proof-of-stake consensus algorithm and a self-amendment process, allowing token holders to propose and vote on protocol upgrades. Dash employs a masternode system, where masternode operators participate in governance decisions and receive rewards.
- Community engagement: Both Tezos and Dash have active and engaged communities. Their communities actively participate in governance processes, providing valuable insights and feedback that can contribute to the research and development of on-chain governance mechanisms.

4.2.1 The attributes of voting in on-chain governance

An excellent on-chain governance voting method needs to meet the seven attributes: accountability, incentive mechanisms, decision making, authentication, anonymity, coercion-freeness, auditability. We can see them in Fig. 8.

- Accountability: In blockchain system, the decisions are made by different nodes together. There is no specific one to take responsibility. Moreover, there is an anonymous mechanism in the blockchain. When some nodes do evil, the accountability problem is difficult to solve. Therefore, accountability needs to be considered in detail when designing a blockchain governance mechanism.
- Incentives: In blockchain system, different people play different roles and have different interests; It is necessary to design a suitable incentive mechanism to encourage everyone to actively participate in the blockchain governance process, put forward good development governance suggestions, and punish malicious nodes.
- Decision making: Blockchain is a distributed project, there is no core authority between nodes and no unified decision deployment. The governance process is often lengthy and inefficient. It is common for some nodes to agree to upgrade and some to refuse, resulting in a fork. Therefore, it is necessary to consider the decision-making aspect to evaluate a blockchain governance method.
- Authentication: In the blockchain system, token holders cast a ballot through their accounts. These accounts, such as hash values for blockchain addresses, are usually virtual addresses. Therefore, it is easy for one to register multiple virtual addresses to vote maliciously. Virtual identities must be bonded with real ones, such as driver's license numbers, to ensure the voter's legal identity.
- Anonymity: Anonymity is the key for the voters to express their will freely. Otherwise, malicious attackers may threaten users based on the results of the real-name ballot or bribe them to change their votes. Therefore, an excellent on-chain governance voting mechanism needs to consider anonymity. Currently, mixed network [42], group signature [43], and ring signature [44] can be used to achieve the anonymity of voting.
- Coercion freeness: Coercion means an attacker requires a voter to vote for a particular candidate or abstain. This problem is challenging because it is impossible to tell whether voters have been coerced according to the voting results. Kulyk et al. [45] set voting priorities that allow users to override previously forced votes by casting higher-priority votes before the ballot ends. Clarkson et al. [46] use the fake identity to make the coercer unable to match the user's identity with the vote to achieve the purpose of anti-coercion.
- Auditability: Audibility ensures the trustworthiness of governance outcomes by enabling anyone to audit the correctness of on-chain governance voting results. As a distributed ledger, blockchain has good auditability because of its immutability. It should be emphasized that anonymity must always be maintained, and even

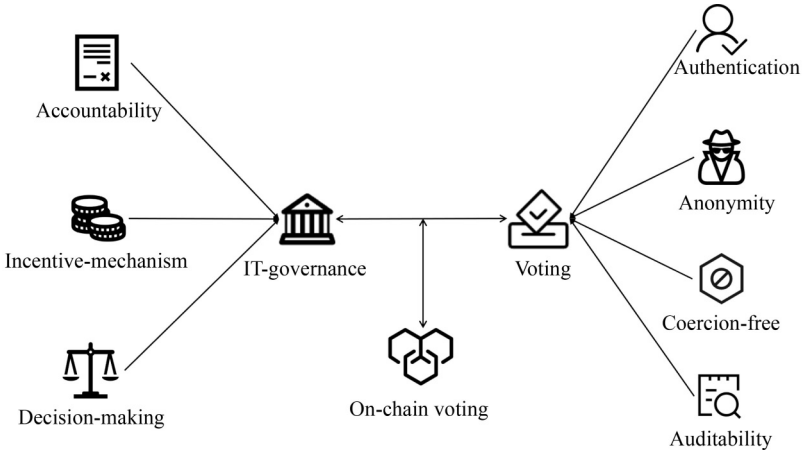


Fig. 8 The attributes of voting in on-chain governance

auditors can not obtain the true identity of voters. Decentralization also needs to be considered so that audit bodies can be designed in a distributed way, for example, through secure multi-party computing [47].

4.2.2 The analysis of Tezos

Tezos is a famous smart contract public blockchain platform that can self-upgrade and evolve through code modification. The self-evolution process is implemented through on-chain governance mechanisms. Tezos defines a set of upgrade protocols to achieve the unity of stakeholders. The upgrade's scope includes modifying the software code and the governance voting process. A suitable on-chain governance mechanism reduces the possibility of hard forks. Tezos codifies the governance process, reduces the intervention of human factors, and enhances decentralization.

In Tezos, token holders can delegate their tokens to other users, and the users with more than 8000 tokens can become bakers who can bake and validate the blocks.

- Accountability: Tezos allows delegators to change bakers at any time. The tokens are not required to be locked during the voting process, which means participants can sell their tokens after the vote and before the governance proposal is fully activated. Bakers are the only ones accountable for the amendment process in Tezos. But this is not accurate. Accountability needs to be improved.
- Incentives: There is no specific incentive for initiating proposals. At the same time, there is no reward for token holders actively participating in the voting governance process. For miners, there are the mining rewards, while for the users, there is only the investment income of the Tezos tokens. The incentive mechanism needs to be improved in future development.
- Decision making: The bakers have the right to vote for governance proposals. At the same time, ordinary users have the right to vote for bakers. The bakers have more influence in governance than ordinary users.
- Authentication: There is no central authority to authenticate voters. Allombert et al. [48] introduced this scheme.
- Anonymity: The public key of every delegate corresponds to their ballot. So anonymity is not satisfied.
- Coercion Freeness: Delegate votes are bonded with token holders' pseudo-identities, and voters can not vote multiple times to cover previous ballots. So coercion resistance needs to improve.
- Auditability: The final results are public, and the voting data are recorded on the blockchain. Thus auditability is satisfied.

4.2.3 The analysis of MULTAV

The newly launched cryptocurrency blockchain project has a small market capitalization and initial circulating supply. Thus, its governance process can be easily controlled by a malicious attacker. To solve this problem, Fan et al. [34] propose an on-chain governance framework-MULTAV. The framework of MULTAV is shown in Fig. 9. The notations are listed in Table 1. It can be divided into five steps:

1. Initial token distribution. The project managers need to investigate n mature blockchain platforms. Then they convert the new cryptocurrency tokens for voting tokens of the n $CS_i, i = 1, \ldots, n$, at market prices. After conversion,the token holders of $CSUG$ will be divided into n CS_i.
2. Proposal voting preparation. Token holders who want to submit governance proposals on $CSUG$ need to deploy GC, RC, VC. After deployment, the contract author sends transaction to GPR to start voting process.
3. Proposal (pre)-voting in action. Token-holders who want to vote need to register first. They can send transactions to the RC to complete the registration process. After that, token holders can send transactions to smart contract VC_i for voting process.
4. Proposal vote counting. CSC_i reads the VC_i status and calls the VCR to generate the vote result. There is a

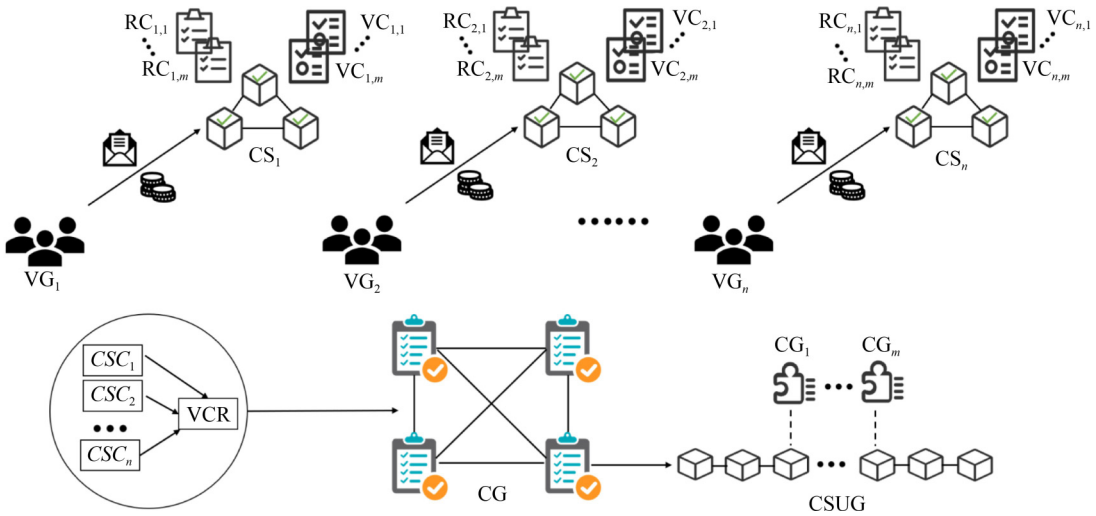


Fig. 9 The framework of MULTAV

status field for each proposal in *GPR*. Change the status field "voting" to "valid" if the number of votes exceeds a predefined threshold or "invalid" otherwise.

5. Proposal decision execution. If the results of the proposals are valid, then the voting results will be added to the blockchain and the proposal will be deployed. If the proposal is invalid, nothing will happen.

In the security analysis of this model, if the probability of each $CS_i, i = 1,\ldots,m$, being breached is p, then the whole system will be breached with a probability of p^m. But it is not true. Assume the vote result is very close to the passing threshold (e.g.,70% of the total votes). If any $CS_i, i = 1,\ldots,m$ is breached at this point, affecting 1% of the votes, it would also change the final result. So the probability of breaking the system is p, not p^m. Therefore, the security analysis in this paper is not reasonable.

The analysis of MULTAV is as follows:

- Accountability: The voting process happens in the chosen blockchain, where accountability depends. As for initiating a proposal, the proposer needs to deploy a *GC* on *CSUG*. So the accountability for the proposer is well satisfied.
- Incentives: In this model, the incentives mechanism is not clearly defined for proposing or voting. Proposers can set the rewards for voting in their governance proposals to incentivize more token holders to vote for them.
- Decision making: Token holders vote for governance proposals across different blockchains, making decisions together.
- Authentication: In step 3, the vote must be registered with the *RC* first. So the authentication is satisfied.
- Anonymity: In step 2, transaction contains the name of the proposer. Therefore, there is no anonymity for the proposer. However, anonymity in voting depends on the chosen blockchain and voting smart contract.
- Coercion freeness: It is not clear.
- Auditability: The *VCR* is defined in the model for the audit process. Moreover, in cross-chain voting, the data recorded on the chosen blockchain are publicly verifiable.

4.2.4 The analysis of Dash

Dash's on-chain governance model addresses two issues: governance and funding. Dash has created a decentralized governance by blockchain system where all governance proposals are submitted.

In Dash, only the master nodes with more than 1000 Dash can vote for governance proposals. It is a very high threshold to own 1000 dash because, by writing this paper, 1 Dash equals $87.11.

Each master node has one vote for each proposal (Yes/no/abstain). Approval occurs when yes votes minus no votes equal 10% or more of the total available votes. Any token holder can initiate a governance proposal, but it needs to pledge 5 Dash to prevent waste of system resources. Dash allocates 10% of the block award to its governance development, which is used to fund the highest-ranked governance proposal and the voters who vote for this proposal. The process of Dash governance is shown in Fig. 10.

- Accountability: Tokens locked up for voting can be unlocked before implementing proposals. There is no penalty for the master nodes that vote for malicious proposals. So accountability is not satisfied.
- Incentives: 10% of the mined block reward will be allocated to the proposals that successfully pass voting. Master nodes will be paid a bunch of Dash from mined

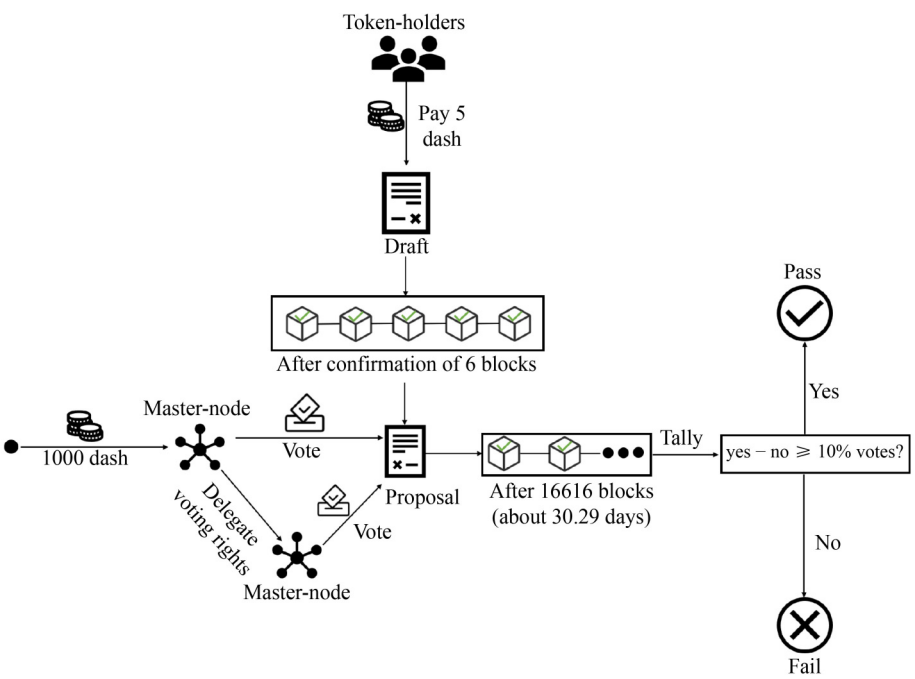


Fig. 10 Dash governance process

block reward if they positively participate in the consensus and voting process.

- Decision making: Token holders can pledge 1000 Dash to become master nodes, then have voting rights to make decisions.
- Authentication: There is no central authority to perform authentication.
- Anonymity: Masternodes only need pseudonyms to cast a vote. Normal nodes who have 1000 dash only need pseudonyms to become masternodes. The voting process does not reveal the real identity of voters, so anonymity is satisfied.
- Coercion freeness: masternode votes are bonded with its pseudo-identities, and they can not vote multiple times to cover previous ballots. So coercion resistance needs to be improved.
- Auditability: Because the final tally is public, the data about the voting will be recorded on the blockchain and cannot be tampered with. Thus auditability is satisfied.

4.3 Hybrid governance and analysis

Hybrid governance combines on-chain and off-chain governance. For the macro governance issues such as the development direction of blockchain, the use of foundation funds, and the management of project development, it is better to adopt off-chain governance. Experts, scholars, and project managers will make decisions about these issues through off-chain meetings. And as for the microcosmic governance issues, such as the parameters of consensus mechanism, block rewards, block structure change, and rollback of the error transactions, they can be handed over to all users through on-chain voting.

Hybrid governance is more suitable for blockchain. All kinds of unexpected problems may occur during the operation. The on-chain governance code cannot cover all the situations before coding. Thus it is unrealistic to rely on on-chain governance entirely. At the same time, off-chain governance, wholly controlled by elites, conflicts with blockchain's immutability and decentralization.

The advantages of hybrid governance combine the advantages of on-chain and off-chain governance. They have been listed above. The disadvantage of hybrid governance is immaturity. The development of current hybrid governance technologies is still in its infancy. There is controversy over which governance issues adopt on - or off-chain governance.

The comparison of three governannce methods is shown in Table 4.

4.3.1 The analysis of Decred

Decred adopts hybrid governance. Anybody who holds enough DCR (token in Decred) may time-lock their coins to purchase tickets and participate in governance. Validation of blocks and voting on consensus rule changes occur on-chain.

Voting on higher-level issues, such as how to spend treasury funds or significant policy decisions (amendments to the Decred constitution), occurs off-chain in Politeia. The Decred governance model is shown in Fig. 11.

Politeia, a public proposal system launched by Decred in 2018, is an off-chain governance system that decides how to use funds. The system stores governance data transparently in

Table 4 The comparison about three governance methods

Governance methods	On-chain governance	Off-chain governance	Hybrid governance
Method	On-chain voting	Off-chain meeting	Hybrid
Participants	Token holders	Core developers, experts	Experts (off-chain) Token holders (on-chain)
Advantages	Fair Transparent	Professional efficient, flexibility	Combining both
Disadvantages	Low participation Low efficiency, Variability	High centralization untransparent	Immaturity
Main goal	Modify consensus mechanism and some governance detail	Formulate overall direction of blockchain development	Overall all governance issues of blockchain

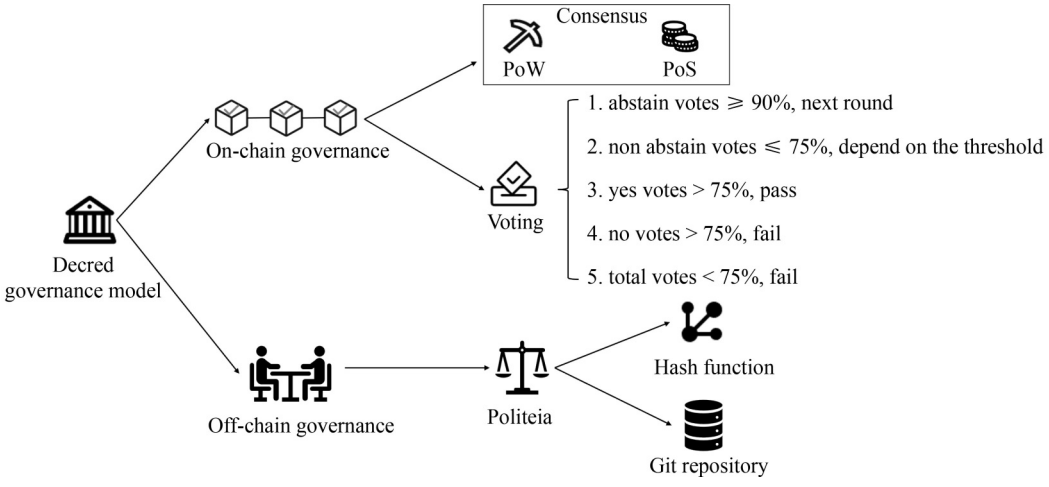


Fig. 11 Decred governance model

the Github repository and anchors it to the blockchain with Decredtime. When creating an account, the system automatically generates a public and private key pair. Users use their private keys to sign a vote for or against a proposal. So the comments under each data set can be traced back to a specific user.

Politeia's proposal submission process is as follows:

1. A user submits a proposal and sends it to the administrator for review. If the proposal is useless, it will be marked as "Abandoned," and the proposed fee will be deducted.
2. After passing the audit, the administrator initiates the vote. The voting process will last for about a week, about 2016 blocks. There is a quorum for a vote to be valid: 20% of the eligible tickets must vote "Yes" or "No". The threshold for a proposal to be approved is 60% "Yes" votes.
3. After passing the vote, the funds can begin to flow. Otherwise, nothing will happen. Decred Holdings Group will continue the payment.

We analyze the Decred governance process as follows:

- Accountability: Tokens locked will be unlocked after 256 blocks, but the proposal needs 8064 blocks confirmed to implement. It means the malicious voters can safely retrieve their tokens during this period to avoid punishment. So accountability is not satisfied.
- Incentives: There is no additional incentive for submitting quality proposals and governance of the voting process. In the consensus mechanism of Decred, voters can only get part of their reward by validating blocks, so the incentives mechanism needs to be improved.
- Decision making: Anyone can participate in voting decisions by purchasing voting rights.
- Authentication: It is not clear.
- Anonymity: Token holders are not required to reveal their real identities to participate in the voting process. Thus anonymity is satisfied.
- Coercion freeness: There are no explicit secrecy guarantees in the voting process. Thus coercion freeness is not satisfied.
- Auditability: Because the final tally is public, the data about the voting are recorded on the blockchain. Thus auditability is satisfied.

The analysis of the four on-chain governance blockchain platforms are listed in Table 5.

5 Challenges and future reasearch directions

5.1 Challenges in blockchain governance

The challenge in blockchain governance can be analyzed in three aspects:

- Smart contract: The transparency of smart contract code will allow hackers to find loopholes for attacks (e.g., 2016, The DAO attack). Besides, Everts et al. [49] believe if the smart contract is too long, it will cause a surface attack. What is more, another challenge is the unchangeable hard-coded logic of smart contracts.
- DAO: First, the accountability of DAO can be challenging. Usually, the developers of DAO are mobile. Accountability becomes complicated because the developers are uncertain. Second, the legislation of DAO is difficult. Scholars [50] believe that the initial laws on token issuance and services may become outdated before they can be enforced due to the rapid growth of DAO. The nodes of DAO can be scattered in various countries worldwide, making it challenging to implement international legislation. As a result, there is no clear law for DAO.
- Centralization: Most methods of blockchain governance are highly centralized: on-chain governance is essentially led by plutocrats, while core developers and experts dominate off-chain governance. The highly centralized governance violates the decentralized principle and reduces users' trust in the blockchain. Suppose the centrality of governance is reduced, when an emergency occurs, no one has absolute authority to stop malicious behaviors immediately, which will cause economic losses to users (e.g., 2016, the DAO attack). Therefore, it is hard to achieve a balance between decentralization and centralization.

5.2 Future research directions

In this section, based on the research findings, we present potential research directions for future research in blockchain governance, including legal issues, the appropriate scenarios of three governance models, and incentive mechanisms.

5.2.1 Blockchain governance and law issues

Blockchain governance is facing legal issues. Future legislation in blockchain governance can be focused on in detail:

First, blockchain is a decentralized system where the network consists of multiple nodes in different locations.

Table 5 The analysis of four on-chain governance blockchain

	Tezos	MULTAV	Dash	Decred (on-chain part)
Accountability	Partially satisfied	Yes	No	No
Incentives	Partially satisfied	Partially satisfied	Yes	Partially satisfied
Decision-making	Decentralized	Decentralized	Centralized	Decentralized
Authentication	Partially satisfied	Yes	No	No
Anonymity	No	Same as the chosen blockchain	Yes	Yes
Coercion freeness	No	N/A	No	Yes
Auditability	Yes	Yes	Yes	Yes

According to the analysis of the Bitnodes. IO, Bitcoin nodes are distributed in 84 countries. The top three are the United States (1880), German (1740) and France (525). Legal and value systems vary from country to country, making it difficult to reach a unified law on blockchain and its governance.

Second, there is little law to address the issues that arise in blockchain governance. Different laws about on-chain and off-chain governance are needed to govern the process.

Third, as a distributed and immutable ledger, Blockchain provides a good space for harmful information to spread. Blockchain technology is currently unable to audit uploaded information, so laws are needed to define the scope of harmful information and establish penalties based on the harm to society. The law is still in the blank stage in this field, which can be studied in depth.

5.2.2 The appropriate scenarios of the three governance methods

In blockchain system, whether to adopt on-chain or off-chain governance is the research direction in the future. We believe the governance model needs to be dynamically adjusted according to the stage of blockchain development.

In the early stage, due to the insufficient number of users and weak computing power, it is likely to cause security problems adopting on-chain governance. Malicious users can easily control the voting process without any cost. Therefore, it is more beneficial to be governed by founders and core developers off-chain in the early stage.

When the computing power reaches a large number, it becomes difficult to control the voting process. Then, it can turn to on-chain governance. On-chain governance is more suitable for the decentralized concept of blockchain, and better reflects the will of the whole participants.

Besides, we can consider the hybrid of on-chain and off-chain governance. For the macro governance issues such as the development direction of blockchain, the use of foundation funds, and the management of project development, it it better to adopt off-chain governance and leave these issues to experts.

As for the microcosmic governance issues, such as the parameters of consensus mechanism, block rewards, etc., can be handed over to all users on the chain through voting. Such division of labor ensures blockchain development and considers the characteristics of decentralization. Thus hybrid governance will be a hot research direction.

5.2.3 Incentive mechanisms

In the current blockchain governance model, there is a lack of suitable incentive mechanisms. There is no clear financial incentive for proposers or voters for on-chain governance. Although locking tokens is required in Dash and Decred to prevent malicious proposals, it is not enough to incentivize voters to vote.

In future research, economic incentives can be directly given to voters to encourage them to participate in voting. As for initiating proposals, we could consider using game theory and PoW to incentivize. The excellent proposers have more chances to be block producers and have block rewards. At the same time, the malicious proposers are restricted from mining, which can effectively improve the efficiency and participation rate of blockchain governance.

6 Conclusion

In this paper, we discussed the concept of blockchain governance and summarized four main methods of on-chain governance voting. Then, we proposed seven attributes for the on-chain governance voting, and used them to analyze four on-chain governance blockchain. Moreover, as for off-chain governance, we use the blockchain governance evaluation model proposed by Pelt to analyze Bitcoin and introduce the governance mode of Ethereum. Based on the above research analysis, we put forward some directions for further research in the future.

Acknowledgements The work was supported by the Shandong Provincial Key Research and Development Program (No. 2021CXGC010107), the National Natural Science Foundation of China (Grant Nos. 62172307, U21A20466, 62272350), the New 20 Project of Higher Education of Jinan (No. 202228017), the Special Project on Science and Technology Program of Hubei Provience (Nos. 2020AEA013, 2021BAA025) and the Fundamental Research Funds for the Central Universities (No. 2042023KF0203).

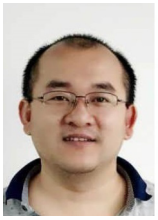
Competing interests The authors declare that they have no competing interests or financial conflicts to disclose.

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review, 2008, 2120
2. Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014, 151: 1–32
3. Bhattacharya S, Victor N, Chengoden R, Ramalingam M, Selvi G C, Maddikunta P K R, Donta P K, Dustdar S, Jhaveri R H, Gadekallu T R. Blockchain for internet of underwater things: State-of-the-art, applications, challenges, and future directions. Sustainability, 2022, 14(23): 15659
4. Nguyen G N, Le Viet N H, Elhoseny M, Shankar K, Gupta B B, El-Latif A A A. Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with resnet model. Journal of Parallel and Distributed Computing, 2021, 153: 150–160
5. Rani S, Babbar H, Srivastava G, Gadekallu T R, Dhiman G. Security framework for internet-of-things-based software-defined networks using blockchain. IEEE Internet of Things Journal, 2023, 10(7): 6074–6081
6. Mamta, Gupta B B, Li K C, Leung V C M, Psannis K E, Yamaguchi S. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA Journal of Automatica Sinica, 2021, 8(12): 1877–1890
7. Gupta B B, Mamta, Mehla R, Alhalabi W, Alsharif H. Blockchain

technology with its application in medical and healthcare systems: a survey. International Journal of Intelligent Systems, 2022, 37(11): 9798–9832
8. Lin J H, Primicerio K, Squartini T, Decker C, Tessone C J. Lightning network: a second path towards centralisation of the Bitcoin economy*. New Journal of Physics, 2020, 22(8): 083022
9. Webb N. A fork in the blockchain: income tax and the bitcoin/bitcoin cash hard fork. North Carolina Journal of Law & Technology, 2018, 19(4): 283–311
10. Bitcoin Cash. Bitcoin cash. See bitcoincash website, 2019
11. del Castillo M. The DAO attacked: Code issue leads to $60 million ether theft. See baypayforumblockchain-coins/the-dao-attacked-code-issue-leads-to-60-million-ether-theft website, 2016
12. Ethereum Classic. Ethereum classic. Ethereum Classic. See ethereumclassic.github website, 2017
13. Weill P. DonâĂŹt just lead, govern: how top-performing firms govern it. MIS Quarterly Executive, 2004, 3(1): 1–17
14. Posthumus S, Von Solms R. A framework for the governance of information security. Computers & security, 2004, 23(8): 638-646
15. Micheli M, Ponti M, Craglia M, Berti Suman A. Emerging models of data governance in the age of datafication. Big Data & Society, 2020, 7(2): 2053951720948087
16. Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. Journal of the American Medical Informatics Association, 2020, 27(3): 491-497
17. Liu Y, Lu Q, Zhu L, Paik H Y, Staples M. A systematic literature review on blockchain governance. Journal of Systems and Software, 2023, 197: 111576
18. Liu Y, Lu Q, Yu G, Paik H Y, Perera H, Zhu L. A pattern collection for blockchain governance. 2022, arXiv preprint arXiv: 2203.00268
19. Liu Y, Lu Q, Yu G, Paik H Y, Zhu L. Defining blockchain governance principles: a comprehensive framework. Information Systems, 2022, 109: 102090
20. Kiayias A, Lazos P. SoK: blockchain governance. In: Proceedings of the 4th ACM Conference on Advances in Financial Technologies. 2022, 61−73
21. van Pelt R, Jansen S, Baars D, Overbeek S. Defining blockchain governance: A framework for analysis and comparison. Information Systems Management, 2021, 38(1): 21–41
22. Schuh F, Larimer D. Bitshares 2.0: general overview. See cb-dev-platform-images.s3.eu-west-1.amazonaws.com/project/whitepaper/bitshares website, 2017
23. Duffield E, Diaz D. Dash: a privacy-centric crypto-currency. See exodus.com/assets/docs/dash-whitepaper website, 2015
24. Kim M S, Chung J Y. Sustainable growth and token economy design: the case of steemit. Sustainability, 2018, 11(1): 167
25. Jepson C. Dtb001: Decred technical brief. See decred.org/dtb001 website, 2015
26. Goodman L M. Tezos-a self-amending crypto-ledger white paper. See tezos.com/whitepaper website, 2014
27. Elrom E. EOS.IO Wallets and Smart Contracts. The Blockchain Developer, 2019, 213–256
28. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: extending bitcoin's proof of work via proof of stake [extended abstract]y. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34–37
29. Alves D. Proof-of-Concept (POC) of Restaurant's food requests in the Lisk Blockchain/sidechain. Journal of Physics: Conference Series, 2021, 1828(1): 012110
30. Hanke T, Movahedi, M., Williams D. DFINITY technology overview series consensus system, 2018
31. Dursun T, Üstündağ B B. A novel framework for policy based on-chain governance of blockchain networks. Information Processing & Management, 2021, 58(4): 102556
32. Pasquini R. Quadratic funding under constrained matching funds. SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3702318
33. Abdullah M A, Ibrahim M A R, Shapiee M N A, et al. The classification of skateboarding tricks via transfer learning pipelines, PeerJ Computer Science, 2021, 7: e680
34. Fan X, Chai Q, Zhong Z. MULTAV: a multi-chain token backed voting framework for decentralized blockchain governance. In: Proceedings of the 3rd International Conference on Blockchain. 2020, 33−47
35. Merrill P, Austin T H, Rietz J, Pearce J. Ping-pong governance: token locking for enabling blockchain self-governance. In: Proceedings of the 1st Mathematical Research for Blockchain Economy. 2020, 13−29
36. Groves T, Ledyard J O. Some limitations of demand revelaing processes. Public Choice, 1977, 29(2): 107–124
37. Berg A, Berg C, Novak M. Crypto Public Choice. SSRN Electronic Journal, 2018, doi: 10.2139/ssrn.3236025
38. Posner E A, Weyl E G. Quadratic voting and the public good: introduction. Public Choice, 2017, 172(1): 1–22
39. Weyl E G. The robustness of quadratic voting. Public Choice, 2017, 172(1): 75–107
40. Demers A, Greene D, Hauser C, Irish W, Larson J, Shenker S, Sturgis H, Swinehart D, Terry D. Epidemic algorithms for replicated database maintenance. In: Proceedings of the 6th Annual ACM Symposium on Principles of Distributed Computing. 1987, 1−12
41. Becze M, Jameson H. Eip-1: Eip purpose and guidelines. See eips.ethereum.org/EIPS/eip-1 website, 2015
42. Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84–90
43. Chaum D, van Heyst E. Group signatures. In: Proceedings of Workshop on the Theory and Application of of Cryptographic Techniques. 1991, 257−265
44. Rivest R L, Shamir A, Tauman Y. How to leak a secret. In: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. 2001, 552−565
45. Kulyk O, Neumann S, Marky K, Budurushi J, Volkamer M. Coercion-resistant proxy voting. Computers & Security, 2017, 71: 88–99
46. Clarkson M R, Chong S, Myers A C. Civitas: toward a secure voting system. In: Proceedings of 2008 IEEE Symposium on Security and Privacy (sp 2008). 2008, 354−368
47. Zhao C, Zhao S, Zhao M et al. Secure multi-party computation: theory, practice and applications. Information Sciences, 2019, 476: 357-372
48. Allombert V, Bourgoin M, Tesson J. Introduction to the Tezos blockchain. In: Proceedings of 2019 International Conference on High Performance Computing & Simulation (HPCS). 2019, 1-10
49. Everts M H, Muller F. Will that smart contract really do what you expect it to do?. Groningen: TNO, 2018
50. Khan N, Kchouri B, Yatoo N A, Kräussl Z, Patel A, State R. Tokenization of sukuk: Ethereum case study. Global Finance Journal, 2022, 51: 100539

Guocheng Zhu received the Bachelor degree in 2019 from the School of Computer Science, Xidian University, China. He is currently working toward a Master degree at the Key Laboratory of Aerospace Information Security and Trusted Computing (Ministry of Education), School of Cyber Science and Engineering, Wuhan University, China. His research interests mainly include applied cryptography and blockchain technology.



Debiao He received the PhD degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, China in 2009. He is currently a Professor of the School of Cyber Science and Engineering, Wuhan University, China. He has authored or coauthored more than 100 research papers in refereed international journals and conferences, such as IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and Usenix Security Symposium. His main research interests include cryptography and information security, in particular, cryptographic protocols. He is in the Editorial Board of several international journals, such as ACM Distributed Ledger Technologies: Research & Practice, Frontiers of Computer Science, and IEEE Transactions on Computers.

Haoyang An received his BS degree in information security from Hefei University of Technology, China in 2019 and received his MS degree in computer science (dual degree) from Central China Normal University, China and University of Wollongong, Australia in 2021. He is currently a PhD candidate at Wuhan University, China. His research interests include cryptography and blockchain.

Min Luo received his PhD degree in computer science from Wuhan University, China in 2003. He is currently a Professor at the School of Cyber Science and Engineering, Wuhan University, China. He has published papers in international conferences/journals, such as S&P, ACM TRETS, IEEE SYST J, and IEEE TVT. His research interests mainly include applied cryptography and blockchain technology.

Cong Peng received his PhD degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, China in 2021. He is currently an Associate Professor of the School of Cyber Science and Engineering, Wuhan University, China. His research interests mainly include applied cryptography and data security.