IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 26, 2020, accepted August 10, 2020, date of publication August 18, 2020, date of current version September 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3017549

A New Consensus Protocol for Blockchain Interoperability Architecture

YAN PANG, (Member, IEEE)
Department of Analytics and Operations, National University of Singapore, Singapore 119245
e-mail: jamespang@nus.edu.sg

ABSTRACT Blockchain is widely recognized as a potential disruptive technology that has gained much popularity recently. Despite many promising results, the current blockchain landscape is fragmented, in which many blockchain systems exist in silos. Interoperability becomes a critical functionality to facilitate broad blockchain adoption and starts to attract attention in both industry and academia research. In this paper, we propose a new consensus protocol, Multi-tokens Proof of Stake (MPoS), for blockchain interoperability architecture. The MPoS protocol is able to strengthen the token network effects in a cross-chain ecosystem and grow the user base of blockchain systems dramatically. We also provide an analytical model to analyze and prove that the MPoS protocol can offer better security than traditional single-token PoS consensus protocols.

INDEX TERMS Blockchain, interoperability, cross-chain, consensus protocol, Proof of Stake (PoS), tokens, cryptocurrency, token network effects, bootstrapping, security.

I. INTRODUCTION

Blockchain is well recognized as one of the revolutionary technologies in the past decade. Its evolution from the initial ''Blockchain 1.0'' in 2008 to today's chain technology amidst the fourth industrial revolution. The implementation of version 1.0 mainly applies blockchain for decentralized cryptocurrencies in the capital market [1]. Subsequently, in Blockchain 2.0, the decentralized functionality was extended to the general market in the form of smart contracts. In the next generation 3.0, the focus was on potential applications and efficiency coordination beyond currency, economics, and markets. Currently, the succeeding technology referred to by Yang Lu as ''Extensive Blockchain'' will enable features of scalability, integration, and interoperability [2].

At present, the main challenge in the blockchain ecosystem is characterized as ''balkanization'' by blockchain software company ConsenSys, where each system and application operates in a silo without communication of data or compatibility between separate protocols [3]. This difficulty is exhibited by differences in consensus models, transaction schemes, and smart contract functionality. To be more specific, the majority of blockchain industry applications concentrate on solving fragmented problems that are confined within their own value chains and vision statements, which introduces difficult interoperability issues such as incompatible standards, asymmetric access to information, and lack of communication among different systems. For example, in the foreign exchange and transaction space, a financial institution utilizes its private blockchain to reduce inefficiencies in payment netting to another bank. However, the sending entity would face a predicament of distrust and non-standardization throughout the peer-to-peer payment channels. Ideally, in the long run, interoperability technology enables public, private, or consortium blockchains to connect with fiat currency banking systems. This simplified illustration indicates the importance of resolving chain interoperability in order to propel into a future ''Internet of Blockchains'', in which ''homogeneous and heterogeneous blockchains can communicate to facilitate cross-chain transactions of value, data, and state transition'' thereby serving as the future pillar of the internet [4].

Interoperability in the realm of blockchain represents the ability to share both digital assets and transaction data across distinct networks, without any reliance or restriction by trusted third-party exchanges. While there is no single de facto definition of blockchain interoperability, The National Institute of Standards and Technology defines interoperability in blockchain architecture as the following [5]:

The associate editor coordinating the review of this manuscript and approving it for publication was Hongbin Chen.

"An interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a unique distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable, verifiable and referenceable by another possibly foreign transaction in a semantically compatible manner."

Interoperability technology enables seamless and secure execution of smart contracts among different public permissionless, private, or consortium permissioned blockchains. It is commonly examined from three broad levels, including (i) Foundational, (ii) Structural, and (iii) Semantic [6]. Foundationally, data can be transferred smoothly among different systems. Structurally, the above-mentioned exchange takes place if and only if there is a well-defined data format. And at the semantic level, the transaction data across systems is interpretable by end-users.

Researches in blockchain interoperability only start recently [7], and they are highly concentrated on specific technical fields summarized below.

- *How to ensure that cross-chain transactions satisfy the atomicity property?*
  Atomicity is fundamental to highly usable and secure blockchain architecture. Transactions are either executed successfully and completely, or not implemented at all. In other words, should one operation in the network fails, then any outstanding operations will simultaneously fail.
- *How to confirm transactions that are made off-the-chain?*
  Off-chain transactions that occur without being broadcasted to the main chain helps address the scalability issue since a limited block size translates to higher transaction fees. At the same time, increasing the size of each block results in difficulties of network propagation and hardware system requirements.
- *How to guarantee that the total amount of token assets remains constant on the main chain?*
  In this case, the total amount of token assets on the main chain should not increase or decrease due to cross-chain transactions. One consequence of a reduction in total tokens is that assets can only traverse in one direction, rather than bi-directionally towards the parent blockchain. Additionally, an increase in the number of tokens on the main chain is considered to be a nominal growth. In fact, the token that has traversed off-the-chain has been accounted for twice. This circumstance violates the principle of bookkeeping and ought not to be accepted by the end-user. As a result, once a token crosses the original chain via an off-chain transaction, it is required to enter into a locked state. Meanwhile, when the token is ultimately reconciled back on the main chain, those in locked states can now be released.
- *How to ensure the network security of both implicated chains?*
  In the case of interoperability between public and private blockchains, network security is an underlying risk since the former is permission-less, and the latter is permission-based. Hence, the privacy and security requirements are differentiated and may pose additional challenges when connecting among distinct zones. It is critical to ensure the integrity of both the assets and transaction data. Furthermore, state transitions should be continuously monitored and validated to prevent double-spending incidents during cross-chain transactions.
- *How to achieve cross-chain communication and connection between multiple blockchains?*
  This challenge refers to the requirement to customize different peg zones in order to achieve cross-chain transactions with a number of external blockchains. For example, an Ethereum peg zone is needed to transmit data from the network to the Ethereum chain.

There is no doubt that these research questions are essential. However, another aspect of the blockchain interoperability, i.e., token network effects in the cross-chain ecosystem, is a lack of research. At present, most of the well-known blockchain networks only have several thousand daily active users (DAU). For example, Ethereum, as the most active DApp ecosystem in all blockchain platforms, only has an average of 16,840 DAU in Jan 2020 [8]. In contrast, popular internet platforms can have billions of users. For example, Facebook and WeChat reported over 1.73 billion and 1 billion DAU during the first quarter of 2020, respectively. User acquisition is especially difficult for a new blockchain network. During the bootstrapping phase of a new blockchain project, the actual utility the new blockchain network can deliver to users is limited by its small scale, and network effects work against users switching from existing alternatives. This requires an effective mechanism to quickly attract early adopters and investors with positive expectations about the project's future value. To resolve these pain points, we propose a new consensus protocol for cross-chain architecture to boost token network effects and quickly grow the user base. The major contributions of this paper are summarized below.

- To the best of our knowledge, this is the first sophisticated analysis of blockchain interoperability from cross-chain user traffic redirect and token network effects points of view.
- We propose a new consensus algorithm, i.e., Multi-token Proof of Stake (MPoS), for the blockchain interoperability architecture. Unlike traditional PoS consensus protocols that only support a single token for staking, MPoS supports the staking mechanism with multiple crypto tokens in a cross-chain ecosystem.
- We provide a comprehensive analysis of token network effects and the bootstrapping problem in blockchain systems. We also study why MPoS consensus protocol is able to strengthen the token network effects and grow the users base for parachain sub-ecosystems quickly.

- We propose an approach to quantify and measure the security risk in PoS blockchain systems. We also prove that MPoS blockchain systems are more secure than the single-token PoS blockchain systems.

The paper is organized as below. Section 2 reviews the technologies of blockchain interoperability solutions. Section 3 discusses the ''Hub-paprachain'' architecture in sidechain and relay technology, and proposes MPoS consensus algorithm supporting multiple tokens staking in the main chain in hub. Section 4 researches the token network effects and bootstrapping problem in blockchain systems and studies how the MPoS consensus protocol can boost the token network effects and solve the bootstrapping problem. Section 5 analyzes the security mechanism in the MPoS blockchain system and the single-token PoS blockchain system. Section 6 concludes the paper and future works.

II. LITERATURE REVIEW

There were four primary categories of design models to address the blockchain interoperation problem, namely notary schemes, sidechains and relays, hash locking, and distributed private key control [9].

- *Notary Schemes*
  In a notary scheme, transactions highly depend on a trusted third-party notary. A group of trusted distributed nodes executes an action on blockchain A when a specific event is taken place on another blockchain B. Subsequently, the trusted individual or group agrees through a consensus mechanism and issues a signature that finalizes the transaction. From a technical point of view, notary schemes are the simplest interoperability solution. As explained by Liping Deng *et al.*, this method allows parties to ''actively listen to and respond to events as well as passively listen and respond to events when they are requested.'' [10]
  The most representative example using the notary mechanism is the interledger protocol by Ripple Labs. According to its whitepaper, the core architecture design is heavily influenced by the internet protocol and consists of independent hosting systems called ''Connectors'' and a separate ledger-provided escrow that eliminates the need for trust as a precondition [11]. While notary schemes are advantageous for its atomic process, ease of implementation, supporting capabilities for different blockchain systems, there are several main drawbacks: inefficiency, lack of flexibility, and the risk of centralization.
- *Sidechain and Relay*
  Sidechains are secondary blockchains that steer alongside the main chain like Bitcoin, Ethereum, etc. They are chains pegged to the main chain, enabling reading data, interpreting data from the main chain, and the exchange of assets from the main chain to sidechain and back. Sidechains can have their own consensus algorithms and tokens. Sidechains have to be maintained by their own miners, and miners on the main chain are not responsible for the maintenance of sidechains.
  The idea of sidechain first appeared in 2012 at the BTC chat room when the core development team of Bitcoin was considering how to upgrade the Bitcoin protocol to add new functions safely. This technology allows developers to attach new functions to other blockchains, but these blockchains are still attached to existing Bitcoin blockchains. These new functions in the blockchain can make full use of the existing Bitcoin network's characteristics without causing harm to it. In 2014, Adam back, Matt Corallo, and other core developers of Bitcoin jointly initiated and established Blockstream company. In October of the same year, a white paper ''enabling blockchain innovations with pegged sidechains'' was released [12]. For the first time, the concept of sidechain and its protocol implementation scheme were clearly proposed.
  Through the sidechain, new functions such as transaction privacy protection technology and smart contract can be added on the main chain, so that users can access a large number of new services and have no impact on the work of the existing main chain. Besides, the side chain also provides a more secure way to upgrade the protocol. When the side chain has catastrophic problems, the main chain is still safe. The technical foundation of sidechain implementation is two-way peg technology, which can be realized through the following modes: single hosting mode, alliance mode, SPV mode, drive chain mode, and hybrid design. The two-way anchoring technology can temporarily lock the digital assets in the main chain and release the equivalent digital assets in the side chain. Similarly, when the equivalent digital assets are locked in the side chain, the digital assets in the main chain can also be released. The most serious difficulty of implementing two-way anchoring is that the protocol transformation needs to be compatible with the existing main chain. That is, it cannot affect the work of the existing main chain.
  Relay model is the extension of sidechains and suitable for linking two heterogeneous or isomorphic blockchains, which is a more direct way to achieve the interoperability of blockchains. This model does not rely on the verification judgment of the trusted third party completely, only through the intermediary to collect the data state of the two chains for self-verification. The sidechain and relay protocol abstracts a cross-chain operation layer from each sidechain to avoid too many technical constraints of the main chain, keep neutrality, and accumulate value for its own project. Also, it provides a unified language, which can reduce the security risks of communication between links. The sidechain and relay are the most popular design for many cross-chain solutions, e.g., BTC relay, Rootstock, ElementChain, Polkadot, and Cosmos, etc.
- *Hashed Time Lock Contracts (HTLCs)*
  HTLCs utilize a combination of hash locking and time locking techniques and require the payment recipient to

reveal a secret hash function prior to the allotted time window. Otherwise, the payment will be automatically refunded to the sender, which is particularly beneficial in ensuring end-to-end security among multiple parties. According to Christian Decker and Roger Wattenhofer, HTLC is mainly used for off-blockchain transactions, despite its ability to operate directly on the blockchain [13].

Proposed by Joseph Poon and Thaddeus Dryja, the Bitcoin Lightning Network made headway in applying HTLC techniques to multi-hop payment channel networks [14]. As highlighted by Giulio Malavolta *et al.*, HTLCs are advantageous in circumstances of partial updates, which could potentially lead to payment losses [15]. HTLCs are primarily beneficial since they do not rely on a centralized and trusted third party to implement transactions. As a result, neither the sending nor receiving participant incurs counter-party risk and uncertainty.

- *Distributed Private Key Control (DPKC)*
  DPKC controls the private keys of various assets through the distributed nodes and maps the original chain assets to the cross-chain to ensure the interconnection of various assets in the blockchain system.
  The distributed control right management is to separate the ownership and use the right of the assets, and transfer the control right of the digital assets in the original chain to the decentralized system safely. Taking the blockchain project Fusion as an example, its implementation is completed through two basic steps of digital assets: lock in and lock out. In the process of lock in, the key is partitioned and stored in a distributed way. The asset is then transferred to the designated account on the original chain and verified by the fusion node to realize the distributed management of control rights. The same is true for the lock out process. First, check the data in the fusion mapping account, and then initiate the transaction after meeting the specific conditions. Each fusion node verifies by its own saved partition key to release the distributed control right management and asset mapping. After the handover of the distributed control right, the smart contract will synchronously update the account status data in the fusion mapping account to reflect the completion of lock in and lock out. The accounting process is actually the process of issuing or recovering an equal amount of digital assets to the mapping account through the fusion system.
  DPKC is similar to the notarial mechanism, but users always have the right to control the assets, only using the distributed storage method to store the key of digital assets, which, to some extent, avoids the centralized risk under the notarial man-machine system. In addition, account locking does not need to adopt two-way anchoring. All transactions are transferred into the original chain network after the verification node is reconstructed, without changing the characteristics of the original chain. Each chain can access the original chain freely and with a low threshold, reducing the cost of cross-chain access, so it is widely applicable and easy to realize. However, due to not changing the original chain's characteristics, cross-chain development needs to be adapted to the characteristics of the original chain. Hence, the development is difficult, and waiting for the confirmation of the original chain for a long time, resulting in low operating efficiency. Distributed private key control projects include Fusion, EKT, etc.

III. PROPOSED CONSENSUS PROTOCOL FOR BLOCKCHAIN INTEROPERABILITY ARCHITECTURE

The research work of this paper focuses on a new consensus protocol to enhance the current sidechain and relay technology for blockchain interoperability.

A. "HUB-PARACHAIN" ARCHITECTURE

In the sidechain and relay technology, the "Hub–parachain" is a mainstream architecture for blockchain interoperability systems (Figure 1). The Hub, e.g., Cosmos hub, Polkadot relay-chain, is a central main chain that manages many independent parallel blockchains call "parachain" in Polkadot [16] or "zones" in Cosmos [17]. These parachains can be existing heterogeneous blockchains, e.g., Ethereum, EOS, ZCash, etc., or new isomorphic blockchain systems developed using the same technology framework as the Hub. The main chain at Hub hosts a multi-asset distributed ledger. A parachain is an independent blockchain that exchanges cross-chain messages with the Hub. A constant stream of recent block commits from parachain posted on the Hub allows the Hub to keep up with the state of each parachain. Cross-chain information is then communicated from one parachain to another by posting Merkle-proofs as evidence that the information was sent and received. Because the isomorphic parachain and Hub adopt the same technology architecture, the communication between them can be handled easily by the native cross-chain communication protocols, e.g. Inter-Blockchain Communication (IBC) protocol at Cosmos [18], or Cross-Chain Message Passing (XCMP) at Polkadot [19]. To connect the heterogenous parachains with the Hub, a special adaptor module has to be introduced, e.g. pegzone at Cosmos, or bridge at Polkadot. This adaptor module is usually a specially designed blockchain that serves a distinct purpose as consensus-adaptors between the Hub and external heterogenous parachain.

Hub and each parachain can have their native crypto tokens. These tokens can be moved from one parachain to another through cross-chain communication protocols. The Hub is responsible for preserving the global invariance of the total amount of each token across the parachains. Cross-chain transactions must be committed by the sender, hub, and receiver parachains.

In the "Hub-parachain" model, all the cross-chain transactions are usually validated and recorded in the main chain at Hub. Validators secure the main chain by staking

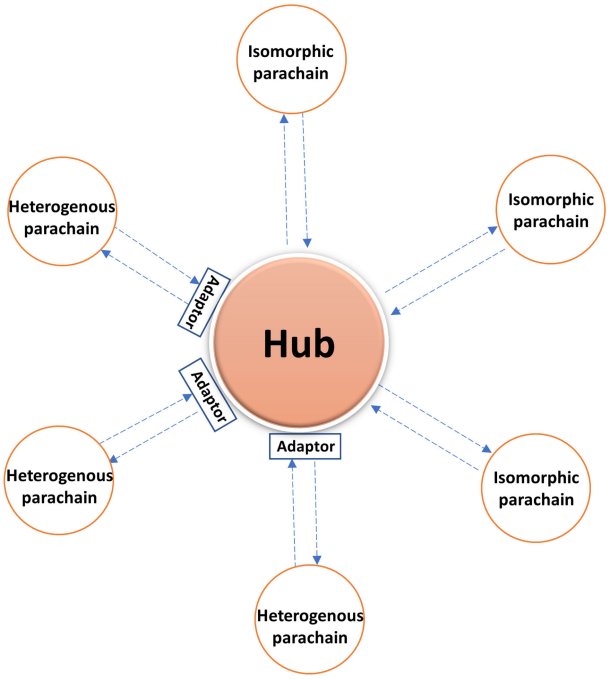


FIGURE 1. "Hub-parachain" model.

native crypto tokens of the Hub. They participate in the consensus protocol by broadcasting cryptographic signatures, or votes, to agree upon the next block in the Hub. Validators will receive block rewards (including mining reward and transaction fee) in the form of native tokens in exchange for their activities, e.g., verifying the transactions, participating in the consensus mechanism to produce the next block, etc.

B. CONSENSUS PROTOCOL

The consensus protocol is a critical component in the blockchain network. A consensus protocol is a procedure through which all the peers of the blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus protocols achieve reliability in the blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the blockchain is the only version of the truth that is agreed by all the active nodes in the network. From the data perspective, a consensus protocol will decide: 1) who has the authority to add a new block of data; 2) what are the data added in the new block. Among all the blockchain consensus protocols, Proof of work (PoW) and Proof of Stake (PoS) are the most popular ones.

- *Proof of Work (PoW)*
  The PoW consensus protocol is used to select a miner, i.e., a node in the blockchain network, for the next block generation. Bitcoin uses this consensus protocol. The main idea of PoW is to let the active nodes in the network compete to solve a complex mathematical puzzle. This mathematical puzzle requires a lot of computational power, and thus, the node who solves the puzzle the earliest gets to mine the next block. PoW is simple and effective in reaching a decentralized consensus on the next block producer. However, many people criticize it because of the high energy cost, the increasing centralization of mining operations, and low transaction throughput.
- *Proof of Stake (PoS)*
  The PoS consensus protocol is the most common alternative to PoW. In this type of consensus protocol, instead of investing in expensive hardware to solve a complex mathematical puzzle, validators invest in the tokens of the system by locking up some of their tokens as stake. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block that they think can be added to the chain. Based on the actual blocks added in the blockchain, all the validators get a reward proportionate to their staking value. In the end, a validator is chosen to generate a new block based on their economic staking value in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement. Also, there isn't a need for the entire network to be involved in the transaction validation process, which improves scalability.
  Compared to PoW, the PoS protocol provides a more scalable architecture with higher transaction throughput, and most of the cross-chain projects to address the blockchain interoperability, e.g., Cosmos, Polkadot, etc., have adopted PoS consensus protocol. However, the PoS protocol is usually less secure than the completely decentralized PoW protocol. In a PoS network, it is possible to buy a majority of the tokens, become the staker of choice, and validate wrong transactions as part of an attack.

C. PROPOSED MULTI-TOKEN PROOF OF STAKE (MPoS) CONSENSUS PROTOCOL

In the current cross-chain systems using "Hub-parachain" architecture, there are different variants of PoS implemented in the main chains. Polkadot Hub (Relay Chain) uses Nominated Proof of Stake (NPoS) to select validators using the sequential phragmen algorithm. In Polkadot design, validators and nominators work together to maximize chain security. Actors who are interested in maintaining the network can run a validator node. The system encourages the holders of Polkadot native token, i.e., DOT, to participate as nominators. Nominators may back up to the validators as trusted validator candidates. The Cosmos Hub uses Bonded Proof of Stake (BPoS) to elect validators. Stakers must bond tokens and submit a delegate transaction to each validator they would like to support with the number of tokens to delegate.

In the "Hub-parachain" model, Hub will issue its own native token, e.g., ATOM, DOT, etc., and parachains also can issue their tokens, e.g., IRIS, KAVA, etc. Although there are

multiple tokens available in a cross-chain ecosystem, current PoS variants discussed above are all using single-token staking mechanics, in which the PoS ''staking'' is only based on the native tokens issued by the main chain. For example, in the Cosmos Hub, the ''staking value'' is computed based on ATOM token, and in the Polkadot relay chain, the ''staking value'' is calculated in terms of DOT token. In this paper, we proposed a new variant of PoS consensus protocol, in which not only the native tokens of the main chain but also the parachain tokens can be staked in the central Hub. The mining rewards will be offered in the form of the native token of the main chain.

The computation of staking value is based on the real-time price of different crypto tokens from exchanges(1).

$$S = \sum_{i=1}^{n} P_i X_i \tag{1}$$

where

X_i is the real-time price of a token i in the staking whitelist, which will be updated in every block cycle. These tokens include the native token in the Hub and tokens from the parachains.

P_i is the number of token i staking at the current block cycle.

n is the number of tokens eligible for staking in the central Hub.

The amount of token value S staked towards a validator defines the frequency by which the validator may propose a new block and its weight in votes to commit a block. In MPoS, the consensus nodes are known as validators, which is similar to miners in PoW. Validators secure the central Hub by validating and relaying transactions, proposing, verifying and finalizing blocks. Validators can stake their own tokens or be delegated tokens from other token holders. Each validator's voting power, or weight, amounts to the proportion of staking value that is self-funded or delegated to them. Like other PoS protocols, MPoS uses an efficient block proposer election and validation process to replace the mining process in PoW. This eliminates the need to solve a complex cryptographic puzzle, so that we can reduce the energy consumption greatly and improve transaction throughput. In addition, since not all nodes are required to be involved in the validation process, the MPoS network has higher scalability and transaction throughput than the PoW network.

As discussed early, MPoS consensus protocol might be under risk if attackers control the majority of the staking value. Therefore, it is crucial to building a governance mechanism to evaluate the parachain systems carefully before accepting their tokens in the staking whitelist. The proposed governance process includes several steps (Figure 2).

- *Submitting a new token proposal*
  Parachain can submit a proposal of adding their token into staking whitelist for voting. The proposal will be published in the cross-chain community, and the current whitelist token holder can deposit the tokens to support it. To ensure the proposal's quality, a minimum number of current whitelist tokens are deposited before the proposal is accepted for voting. If a proposal does not reach the minimum threshold within a period, e.g., 3 weeks, the proposal will be revoked. The supporters who contribute tokens to the proposal will be able to collect their deposit when the proposal is accepted or revoked.
- *Voting for the proposal*
  When the minimum deposit for a specific proposal is reached, the voting process begins. During the voting period, the current whitelist token holders are able to evaluate the new token parachain ecosystem using well-established evaluation frameworks for blockchain systems, e.g., Coindesk Crypto Economics framework [20], 7Ms framework [21], T3CG framework [22], etc. Based on the evaluation results, they can decide whether to cast their vote on the proposal. Voting power is measured in terms of stake, which can be computed by the number and the price of tokens.
- *Tallying*
  A threshold of voting stake, e.g., 67%, is set to decide whether the proposal is accepted or rejected. If the proposal is accepted, the new token will be added to the staking whitelist.

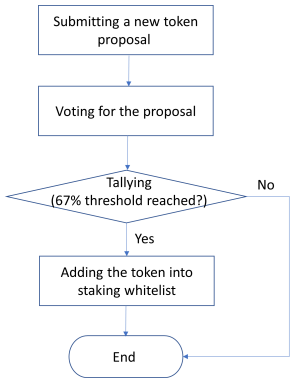


FIGURE 2. Governance process of accepting tokens in the staking whitelist.

Through implementing the governance mechanism, we can prevent the Hub from accepting high rick tokens from parachains. This will be helpful to improve the MPoS blockchain security because the staking values affect the block proposer election and validation. The two advantages of MPoS consensus protocol compared to other PoS variants are discussed below.

- Because MPoS supports multi-token staking, users of the parachains are incentivized to learn about other parachains' sub-ecosystems whose tokens are in the staking whitelist. Therefore, we can overcome the ''balkanization'' phenomenon and strengthen the token network effects and grow the user base of these sub-ecosystems exponentially.

- MPoS consensus protocol can provide better security in the main chain compared to the single-token PoS protocols.

IV. TOKEN NETWORK EFFECTS IN MPoS CROSS-CHAIN NETWORK

A. BOOTSTRAPPING PROBLEM AND TOKEN NETWORK EFFECTS

Thanks to the great effort of the forward-thinking pioneers in the past ten years, many blockchain systems have been developed, e.g., BTC, ETH, EOS, etc. These blockchain projects have already started to make impacts in the real world. However, these impacts are very limited compared to traditional internet platforms, e.g., Facebook, Alibaba, Amazon, etc., due to the much smaller user base. Therefore, increasing the user base is one of the most critical tasks for all blockchain networks in the current stage. To achieve this, we can learn from the network effects of the internet. A network effect is a positive effect whereby increased numbers of participants improve the value of a good or service, and therefore also encourage new participants as they look to benefit from the network (Figure 3). The internet is an example of network effects. For example, as more users post content on Facebook, such as links and media, the platform becomes more valuable to the public. The network effect has created exponential growth rates for internet platforms such as Facebook, YouTube, and Twitter.

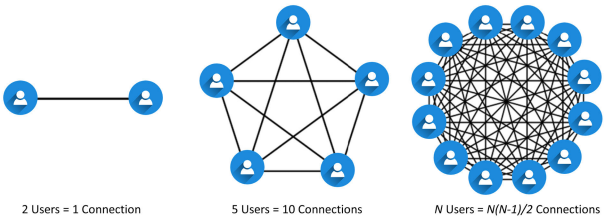


FIGURE 3. Network effects.

Blockchain is a decentralized network similar to the internet. Likewise, it is possible to leverage the network effects to grow the user base exponentially. Compared to the internet, the value of a blockchain network is even easier to measured because of the introduction of crypto tokens. Tokens represent the intrinsic value of a blockchain network. Thus, some researchers named the network effects in blockchain networks as ''token network effects'' [23]. The basic concept of token network effects is simple: the value of token increases when more people use it, and this will incentivize more participants to join the blockchain network as they are able to own some of the tokens through the participation in the blockchain network activities.

In a blockchain network, there are two major markets, i.e., application market and financial market, and three types of participants, i.e., developers, users, and investors (Figure 4). The application market focuses on value creation. Developers created DApps on the blockchain network based on business requirements. Users use the functions offered by DApps to complete different business activities, e.g., purchase goods, transfer assets, anti-counterfeit product verification, etc. These application use cases endow intrinsic value to the tokens. The more use cases of a token, the more valuable the token. In the financial market, investors discover the price of tokens through purchasing the tokens and crypto financial products [24], e.g., crypto ETF, crypto futures, etc. Because of token network effects, these participants work together toward a common goal – the growth of the network and the appreciation of the token.

Token network effects occur when the growth of the network aligns with the appreciation of the token. As the network grows, the token adds value to the platform and accelerates network effects. The most successful blockchain projects tie the token to the core activities of the network's growth. By aligning incentives across all stakeholders, projects can reach escape velocity and leapfrog centralized organizations.

In the network effect phenomenon, we have to overcome the ''bootstrapping problem'' before fully enjoy the benefits from network effects. Bootstrapping problem refers to that network effects only become significant after a certain subscription percentage has been achieved, called critical mass (Figure 5). As the value of the good is determined by the user base, this implies that after a certain number of people have subscribed to the service or purchased the good, additional people will subscribe to the service or buy the good due to the value exceeding the price.

Similarly, a key business challenge in token network effects is how to attract participants and quickly reach critical mass. This is especially crucial to a new blockchain network. In the traditional practice of internet platforms, one way to resolving the bootstrapping problem is to rely on extrinsic motivation, such as a payment, a fee waiver, or a request for friends to sign up. A more natural strategy is to build a system that has enough value without network effects, at least to early adopters. Then, as the number of users increases, the system becomes even more valuable and is able to attract a wider user base. In a blockchain tokenized network, the cost of bootstrapping might be reduced compared to traditional internet platforms, because a native token can be used to create incentives for adoption of the new network by having mining rewards or by raising capital through an initial coin offering (ICO).

However, the contribution from early adopters attracted by ICO is usually not enough to reach the critical mass of the token network effect. In addition, the ''balkanization'' phenomenon of the current blockchain ecosystem makes the token network effects even more difficult because the silo blockchain systems do not communicate with each other and the interaction among the users from different silo systems is very minimum. The proposed MPoS consensus protocol tends to overcome these problems and strengthen the token network effects.

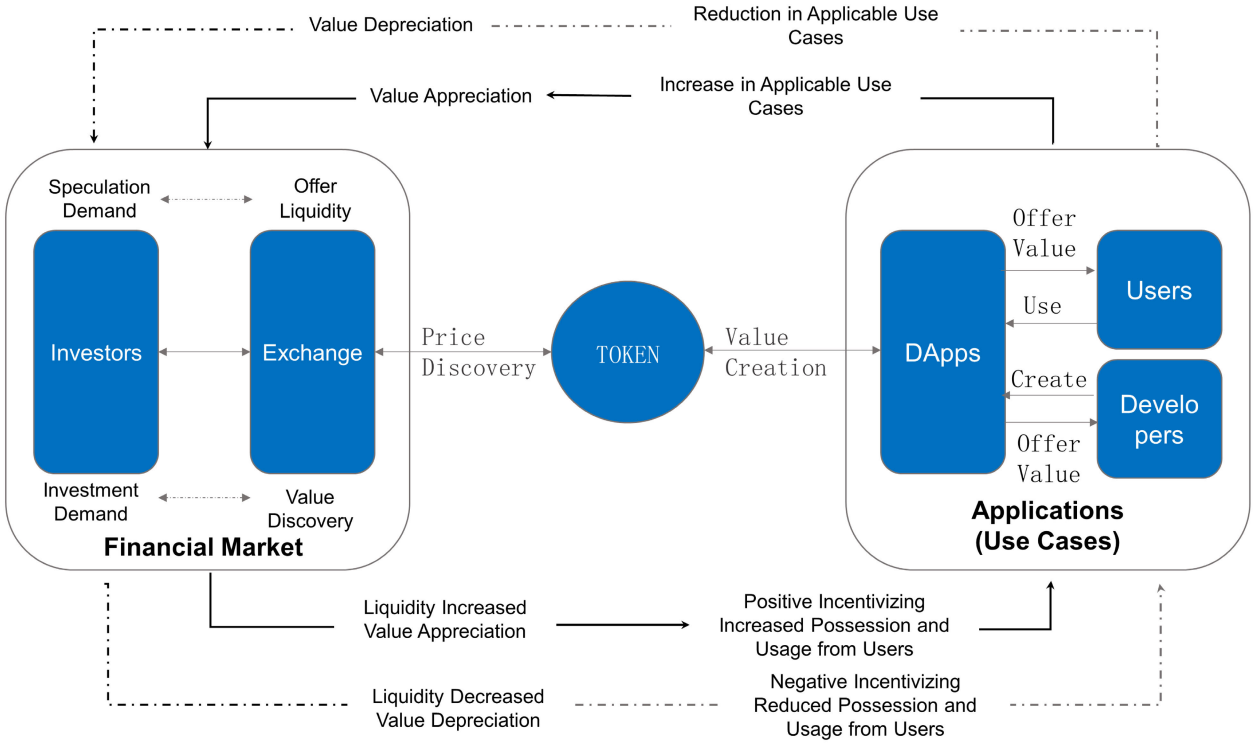


FIGURE 4. Ecosystem of token network effects (customized from [24]).

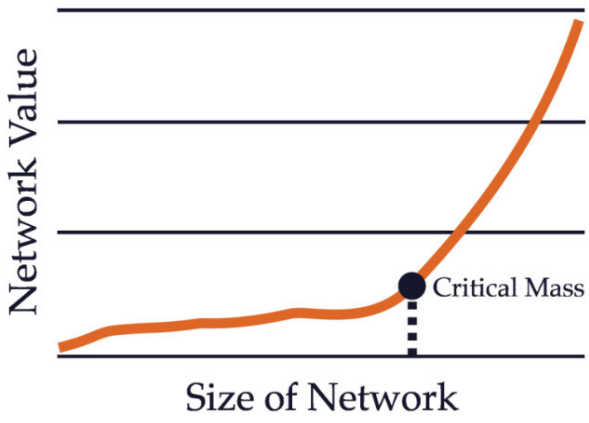


FIGURE 5. Critical mass in network effect [25].

B. TOKEN NETWORK EFFECT ANALYSIS IN MPoS CROSS-CHAIN NETWORK

In the proposed MPoS consensus protocol, both mature blockchain systems, e.g., BTC, ETH, EOS, and new blockchain startups, can join the MPoS cross-chain ecosystem and become parachains (Figure 6). If the tokens from a mature parachain system, e.g., ETH, EOS, etc., is used in the MPoS "staking pool", users from other parachain systems will be interested in learning more about this parachain. This will help direct user traffic from other parachains to this parachain system, which will increase the user base dramatically.

The PoS consensus protocol is the most common alternative to PoW. In We can further quantify the network value of MPoS brings to a blockchain network using Metcalfe's law in network effect theory. We assume that there are parachain A and B, which have M and N users respectively before joining a MPoS cross-chain system. Based on Metcalfe's law, we can measure the total network value of A and B is asymptotically proportional to M^2 and N^2. After joining a MPoS cross-chain system, both tokens A and B are used for MPoS staking in the main chain. As both tokens can be used to mine the rewards, users in parachains in A and B will have a strong motivation to learn about the other parachain ecosystem. If we are able to effectively attract P users from A to B and Q users from B to A (Figure 7) by MPoS consensus protocol, the total network value of A and B will increase to $(M+Q)^2$ and $(N+P)^2$, respectively. Therefore, we are able to increase the network value of mature parachains through MPoS consensus significantly.

The cross-chain user traffic created by MPoS consensus protocol is even more important for a new blockchain network because of the bootstrapping problem discussed early on. If a new token is listed in the whitelist of MPoS "staking pool", users in the whole cross-chain ecosystem are aware of the new chain. Some of the participants of the central Hub and other mature parachains may become the early adopters of the new token. They are willing to dedicate time and effort to support a new blockchain network because they want to increase the value of the token and get more returns from the investment of the new token. Therefore, through introducing MPoS in

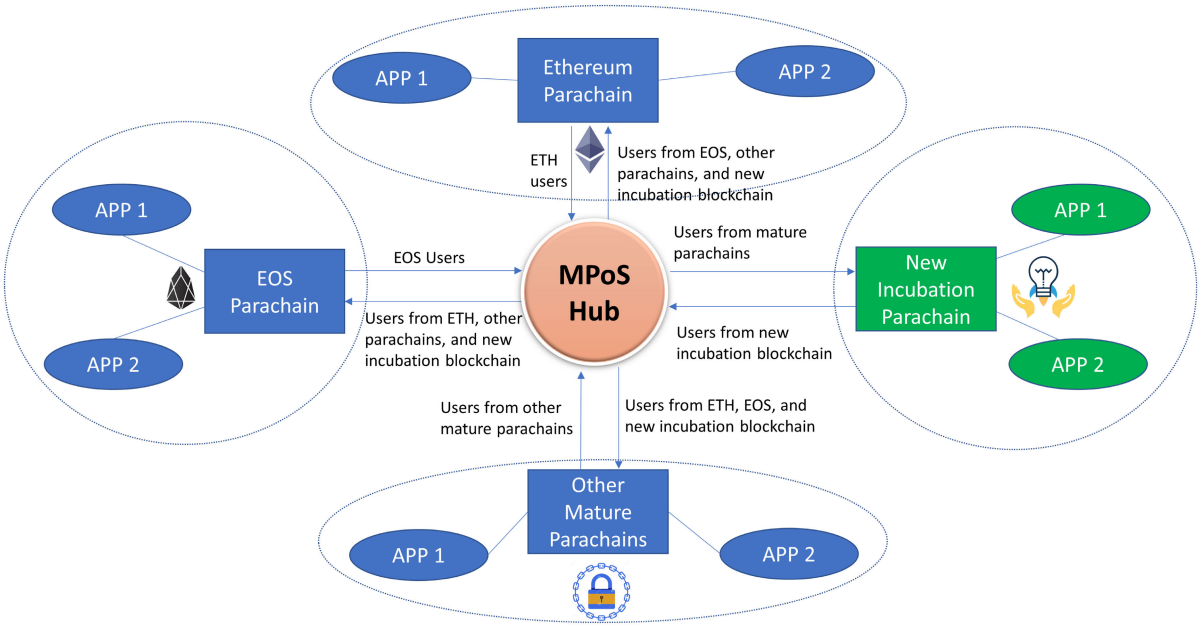


FIGURE 6. Share user traffic in an MPOS ecosystem.

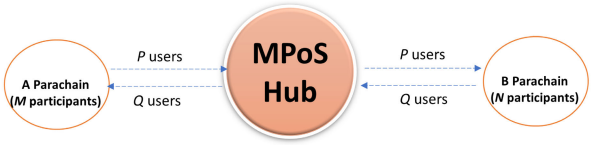


FIGURE 7. Direct user traffic in MPoS cross-chain system.

the cross-chain central Hub, the user traffic of other mature parachains can be redirected to a new parachain, and quickly reach the critical mass of token network effects. Therefore, it creates a bandwagon effect as the new parachain becomes more valuable and more people join, resulting in a positive feedback loop.

V. SECURITY ANALYSIS IN MPoS CROSS-CHAIN NETWORK

A. ADVERSE ATTACK TO PoS SYSTEMS

One of the vital security risks of PoS is adverse attack. In a PoS system, the attacker can execute an attack while controlling a majority, e.g., 2/3, of the total pool of tokens staked by validators. Traditionally, most industry practitioners and academic researchers consider that the adverse attack on PoS systems is unlikely for two reasons.

- To launch an attack on PoS systems, attackers would have to risk of depreciation of their entire stake amount. Even if an attack succeeds, the value of PoS-based crypto token will fall, and the attackers with the most stake will eventually lose the most. Therefore, those who attempt to attack the PoS blockchain will not be easily motivated.
- The market economy has a natural safety valve for the PoS systems because the price of the token will rise significantly when someone tries to buy such a massive amount of token to launch an attack. This will make the attackers' job far more difficult.

However, recent research shows that attackers can make a profit from an adverse attack on the PoS blockchain systems using the traditional stock market's short selling concept [26]. Besides, the cryptocurrency market is highly volatile due to the following reasons, which makes the PoS adverse attack easier and cheaper.

- *Lack of mature regulation framework*
  Blockchain and cryptocurrency are new and fast-growing areas, and current government regulations are far behind industry development. The limited regulation allows for market manipulation, which introduces high volatility in the market.
- *Speculation and herd mentality*
  As cryptocurrency is still an emerging market, many early adopters are millennials and do not have much investment experience in cryptocurrency. They are usually speculators without a long-term investment mindset. When the market goes down, these inexperienced speculators literally cannot afford to lose so that they will dump at the first sign of trouble. This is a reactionary behavior, and they will generally lose money before getting out of the market. When the market is booming, they will buy crazily without considering the reasonable price. As a group, this appears to be coordinated en

masse, but it is just the motivations of many single entities that propagate into a herd mentality. This speculative behavior causes even more volatility in an already choppy market.

- *Media impact*
  Because cryptocurrency is a relatively small digital asset market with tons of speculation, the media has a substantial impact on the cryptocurrency prices. Speculators and investors are constantly eyeing the headlines for the next big news story that will launch or crash the market. When something does emerge, everyone knows it's a race to buy or sell, and the fastest will profit the most, while the slowest will lose the most.

In such a volatile market, attackers can purposely circulate negative news of a specific token, and quickly buy a large amount of token to complete the attack in a PoS network. In contrast, as there are multiple tokens used in MPoS staking, it is almost impossible for the attackers to manipulate the price of all these tokens in the staking whitelist at the same time. What's more, the analytical model proposed in the next section proves the security risk of MPoS systems is lower than single-token PoS systems.

B. ANALYSIS OF SECURITY RISK IN SINGLE-TOKEN PoS AND MPoS SYSTEMS

To quantify the security risk of PoS blockchain systems, we need to define a right approach to measure the risk.

1) MEASUREMENT OF THE SECURITY RISK IN PoS BLOCKCHAINS

As discussed early on, to carry out an attack, attackers need to purchase a large amount of tokens from the market and control the majority of the staking value. If attackers have the capital to buy enough tokens at price p to launch an attack successfully, they can do the same when the token price is less than p. Therefore, the security risk of PoS blockchains is corresponding to the attacking price p. We can measure this security risk using the probability of token price equal to or less than p. Because token price can not be a negative number, the security risk can be represented as $P(0 \leq X \leq p)$ (Figure 8). If we know the distribution of the crypto token price, we can compute the security risk $P(0 \leq X \leq p)$ based on the probability density function (PDF).

2) THE SECURITY RISK IN SINGLE-TOKEN PoS SYSTEMS

Figure 9 shows the daily opening price distribution of BTC and ETH in the past one year (16 July 2019 16 July 2020) based on the data provided by CoinMarketCap (www.coinmarketcap.com). From these price histogram charts, their prices can be approximated as a normal distribution. Therefore, we assume the crypto token price follows a normal distribution with mean μ and standard deviation σ, $X \sim N(\mu, \sigma^2)$. The PDF of $N(\mu, \sigma^2)$ is given by Equation (2).

$$f_X(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left\{-\frac{(x-\mu)^2}{2\sigma^2}\right\}. \quad (2)$$

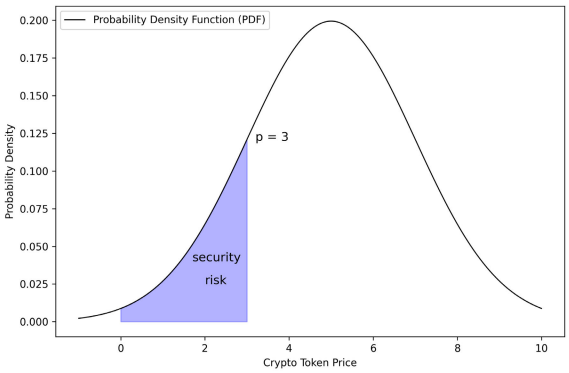
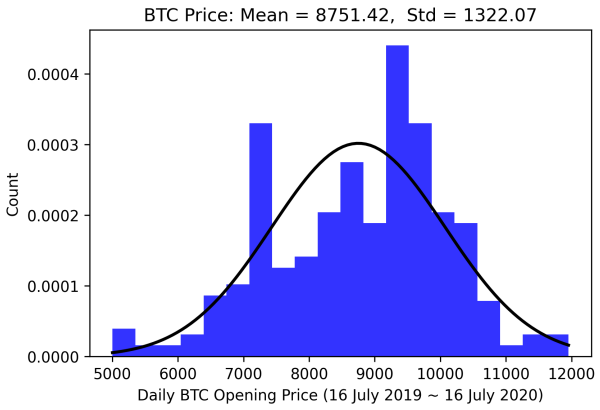
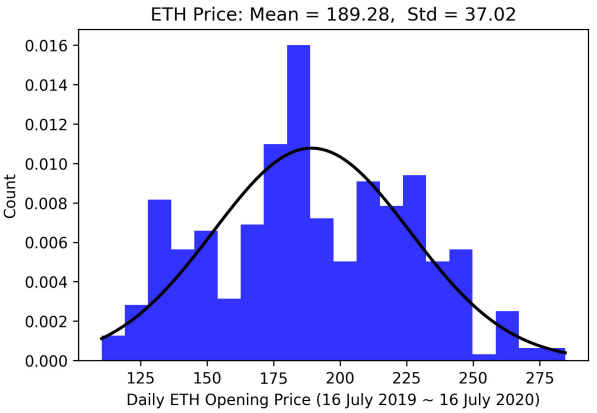


FIGURE 8. Measurement of security risk in PoS blockchain system.



(a) BTC price distribution



(b) ETH price distribution

FIGURE 9. Cryptocurrency price distribution.

The security risk corresponding to the attacking price p can be computed by Equation (3).

$$P(0 \leq X \leq p) = \int_0^p f_X(x)dx = \frac{1}{\sigma\sqrt{2\pi}} \int_0^p \exp\left\{-\frac{(x-\mu)^2}{2\sigma^2}\right\} dx. \quad (3)$$

3) THE SECURITY RISK IN MPoS SYSTEMS

We consider there are n crypto tokens used in a MPoS system. Because the parachains and Hub are managed and operated independently by different project teams, we can assume

the price of each token (including the Hub's native token and parachain tokens) is an independent random sample X_i with a normal distribution. In the actual situation, the mean value μ and standard deviation σ of each staking token X_i could be different. To simplify the analysis, we assume all staking tokens in the whitelist follows the normal distribution $N(\mu, \sigma^2)$. In the MPoS consensus protocol, all the tokens in the whitelist can be used for staking, and the staking value is computed based on the real-time token prices and the number of tokens (Equation 1). To compute the security risk of MPoS systems, we assume the number of different tokens is the same in the staking pool and introduce a "virtual" token $\tilde{X}$, whose price is the sum of token prices in the MPoS staking whitelist (Equation 4).

$$\tilde{X} = \sum_{i=1}^{n} X_i, \tag{4}$$

where

n is the number of tokens used in the MPoS staking computation.

$X_i \sim N\left(\mu, \sigma^2\right)$ represents the price of token i in the MPoS staking whitelist.

Based on Central Limit Theorem, $\tilde{X}$ approximately follows a normal distribution with $\tilde{\mu} = n\mu$ and $\tilde{\sigma}^2 = n\sigma^2$. If attackers want to launch an attack to the MPoS blockchain system, they need to purchase enough number of $\tilde{X}$ and control the majority of staking value. The PDF of $\tilde{X}$ is given by Equation (5).

$$f_{\tilde{X}}(x) = \frac{1}{\tilde{\sigma}\sqrt{2\pi}} \exp\left\{-\frac{(x-\tilde{\mu})^2}{2\tilde{\sigma}^2}\right\}. \tag{5}$$

The security risk corresponding to the $\tilde{X}$ price p can be calculated using Equation 6.

$$\begin{aligned} P(0 \le \tilde{X} \le p) &= \int_0^p f_{\tilde{X}}(x)dx \\ &= \int_0^p \frac{1}{\tilde{\sigma}\sqrt{2\pi}} \exp\left\{-\frac{(x-\tilde{\mu})^2}{2\tilde{\sigma}^2}\right\} dx \\ &= \int_0^p \frac{1}{\sqrt{n}\sigma\sqrt{2\pi}} \exp\left\{-\frac{(x-n\mu)^2}{2n\sigma^2}\right\} dx. \end{aligned} \tag{6}$$

Realistically, attackers will most likely launch the attack at a low price point. It is reasonable to assume the attacking price p is equal to or lower than μ, i.e., $p \le \mu$. To compare the security risks of the single-token PoS and MPoS systems, we compare $P(0 \le X \le p)$ and $P(0 \le \tilde{X} \le p)$.

Proposition 1: Assume that $X \sim N\left(\mu, \sigma^2\right)$ and $\widetilde{X} \sim N\left(n\mu, n\sigma^2\right)$, if $0 < p \le \mu$ and $n > 1$, we have

$$P(0 \le \widetilde{X} \le p) < P(0 \le X \le p)$$

(Proof in Appendix)

Proposition 1 guarantees that the security risk of MPoS systems is lower than that of single-token PoS systems when the attacking price $0 < p \le \mu$. For example, in a single-token PoS system with token price $X \sim N(10, 5^2)$, the security risk at attacking price of 5 is $P(0 \le X \le 5) = 0.13591$. In a MPoS system with two tokens and $\widetilde{X} \sim N(2 \times 10, 2 \times 5^2)$, the security risk at attacking price of 5 is $P(0 \le \tilde{X} \le 5) = 0.01461$, which is much lower than the risk in the single-token PoS system (Figure 10). In other words, if the MPoS system is facing the security risk of 0.13591, attackers have to carry out the attack at the price of 12.3 instead of 5, i.e., $P(0 \le \tilde{X} \le 12.3) \approx 0.13591$. This means that the attackers have to pay a much higher cost to complete the attack.

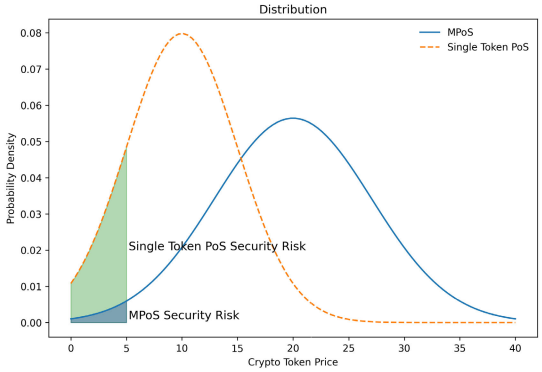


FIGURE 10. Security risk comparison between single-token PoS and MPoS systems.

VI. CONCLUSION AND FUTURE WORKS

Despite the rapid development of blockchain in the past ten years, blockchain technologies and applications are still in the early stage. One of the key challenges blockchain facing now is interoperability. Currently, blockchain systems operate in a silo without communication to each other. As a result, the user base of most of the blockchain systems is very small compared to other popular internet platforms. In this paper, we proposed a new consensus protocol, MPoS, for blockchain interoperability architecture, which can reinforce the token network effects in cross-chain ecosystems and grow the user base of parachains exponentially. The proposed MPoS can also solve the bootstrapping problem of a new blockchain network effectively. In addition, we propose a new approach to measure and analyze the security risk in PoS blockchains. The analysis shows that MPoS protocol can provide better security than other traditional single-token PoS protocols.

Blockchain interoperability is an important emerging research topic, and there are many interesting areas for further research. In the future, more factors can be added in MPoS to enhance consensus protocol, e.g., token age, node health, etc. Another area we can explore in the cross-chain ecosystem is the incubation of new blockchain projects. In this paper, we already show that the cross-chain traffic redirected by MPoS consensus protocol can help to bootstrap the new blockchain project. We can also further study how to leverage other cross-chain resources to incubate the new blockchain project in the ecosystem, e.g. raising funds through tokens in the MPoS whitelist, etc.

APPENDIX

PROOF OF PROPOSITION 1

Assume that $X \sim N\left(\mu, \sigma^2\right)$ and $\widetilde{X} \sim N\left(n\mu, n\sigma^2\right)$, if $0 < p \le \mu$ and $n > 1$, we have

$$P(0 \le \widetilde{X} \le p) < P(0 \le X \le p)$$

Proof: For $0 \leq x \leq \mu$ and $n > 1$, we have

$$\begin{aligned}
\frac{f_X(x)}{f_{\tilde{X}}(x)} &= \sqrt{n}\exp\left\{\frac{(\text{x-n}\mu)^2}{2n\sigma^2} - \frac{(x-\mu)^2}{2\sigma^2}\right\} \\
&= \sqrt{n}\exp\left\{\frac{(\text{x-n}\mu)^2 - n(x-\mu)^2}{2n\sigma^2}\right\} \\
&= \sqrt{n}\exp\left\{\frac{\left(x^2-2nx\mu+n^2\mu^2\right)-\left(nx^2-2nx\mu+n\mu^2\right)}{2n\sigma^2}\right\} \\
&= \sqrt{n}\ \exp\left\{\frac{(1-n)x^2+\left(n^2-n\right)\mu^2}{2n\sigma^2}\right\} \\
&\geq \sqrt{n}\ \exp\left\{\frac{(1-n)\mu^2+\left(n^2-n\right)\mu^2}{2n\sigma^2}\right\} \\
&= \sqrt{n}\ \exp\left\{\frac{\left(n^2-2n+1\right)\mu^2}{2n\sigma^2}\right\} \\
&= \sqrt{n}\ \exp\left\{\frac{(n-1)^2\mu^2}{2n\sigma^2}\right\} \\
&\geq \sqrt{n} \\
&> 1.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
&P(0 \leq X \leq p) - P(0 \leq \widetilde{X} \leq p) \\
&= \int_0^p f_X(x)\,dx - \int_0^p f_{\tilde{X}}(x)\,dx \\
&= \int_0^p \left[f_X(x) - f_{\tilde{X}}(x)\right]dx \\
&> \int_0^p 0dx \\
&= 0,
\end{aligned}$$

which completes the proof.

REFERENCES

[1] S. Melanie, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, Inc., 2015.

[2] Y. Lu, "Blockchain and the related issues: A review of current research topics," *J. Manage. Anal.*, vol. 5, no. 4, pp. 231–255, Oct. 2018.

[3] Consensys. (2019). *Avoiding Blockchain Balkanization*. [Online]. Available: https://consensys.net/research/avoiding-blockchain-balkanization/

[4] H. Tam Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of blockchains: Techniques and challenges ahead," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1574–1581.

[5] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manag.*, early access, Jun. 21, 2019.

[6] S. Ray. *Blockchain Interoperability*. Accessed: Jun. 15, 2020. [Online]. Available: https://towardsdatascience.com/blockchain-interoperability-33a1a55fe718

[7] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2020, *arXiv:2005.14282*. [Online]. Available: http://arxiv.org/abs/2005.14282

[8] Fadilpasic, Sead. *Ethereum Grows on Gaming Dapps, Tron–on Gambling, EOS–Going Downhill*. Cryptonews, Available: Accessed: Feb. 12, 2020. [Online]. Available: https://cryptonews.com/news/ethereum-grows-on-gaming-dapps-tron-on-gambling-eos-going-do-5762.htm

[9] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101079.

[10] L. Deng, H. Chen, J. Zeng, and L. J. Zhang, "Research on cross-chain technology based on sidechain and hash-locking," in *Proc. Int. Conf. Edge Comput.*, Seattle, WA, USA, 2018, pp. 144–151.

[11] S. Thomas and E. Schwartz. *A Protocol for Interledger Payments*. Accessed: Jun. 15, 2020. [Online]. Available: https://interledger.org/interledger.pdf

[12] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, and J. Timón, "Enabling blockchain innovations with pegged," Ind. White Paper 5620e43, 2014. Accessed: Jun. 15, 2020. [Online]. Available: https://blockstream.com/sidechains.pdf

[13] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Proc. Symp. Self-Stabilizing Syst.* Springer, 2015, pp. 3–18.

[14] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," Ind. White Paper Version 0.5.9.2, 2016. Accessed: Jun. 15, 2020. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[15] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 2019, pp. 1–30.

[16] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," Polkadot White Paper. Accessed: Jun. 15, 2020. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf

[17] J. Kwon and E. Buchman, "Cosmos white paper," Cosmos White Paper. Accessed: Jun. 15, 2020. [Online]. Available: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

[18] IBC Ecosystem Working Group. *Inter-Blockchain Communication Protocol (IBC)*. Accessed: Jul. 21, 2020. [Online]. Available: https://github.com/cosmos/ics/tree/master/ibc

[19] Polkadot. *Cross-Chain Message Passing (XCMP)*. Polkadot wiki. Accessed: Jul. 21, 2020. [Online]. Available: https://wiki.polkadot.network/docs/en/learn-crosschain

[20] Coindesk. *Crypto-Economics Explorer–Glossary*. Accessed: Jul. 21, 2020. [Online]. Available: https://www.coindesk.com/data/glossary

[21] W. Sebastian. *A Simple Framework for ICO Due Diligence*. Accessed: Jul. 21, 2020. [Online]. Available: https://medium.com/@sebastianhrw/a-simple-framework-for-ico-due-diligence-9a4a905fe64d

[22] M. Peer. *ICO 2.0: A framework for Due Diligence*. Accessed: Jul. 21, 2020. [Online]. Available: https://medium.com/hackernoon/ico-2-0-a-framework-for-due-diligence-49b8d6eb0c58

[23] Karnjanaprakorn, Michael. (2017). *Token Network Effects*. [Online]. Available: https://www.freecodecamp.org/news/token-network-effects-a-new-business-model-for-a-decentralized-web-6cde8b4e862/

[24] K. Liu. (2019). *Why do we need Token Economics?*. https://hackernoon.com/token-economics-1-why-do-we-need-token-economics-2c0006098aea

[25] NFX. *The Network Effects Bible*. Accessed: Jun. 15, 2020. [Online]. Available: https://www.nfx.com/post/network-effects-bible/

[26] S. Lee and S. Kim, "Short selling attack: A self-destructive but profitable 51% attack on PoS blockchains," IACR Cryptol. ePrint Arch., Tech. Rep. 019, 2020. Accessed: Jul. 21, 2020. [Online]. Available: https://eprint.iacr.org/2020/019.pdf

YAN PANG (Member, IEEE) received the master's and bachelor's degrees in mechanical engineering from Zhejiang University, China, in 1999 and 2002, respectively, and the Ph.D. degree in system engineering from the National University of Singapore (NUS) joint with the Massachusetts Institute of Technology (MIT) in 2006.

He was also a Lead Architect and Senior Manager with IBM R&D Labs in charge of analytics and optimization product development. He was the Client Technical Advisor (Chief Architect) in analytics and optimization with IBM, and led the IBM Technical Solution Design, ASEAN Public Sector. He is currently an Associate Professor with the Department of Analytics and Operations, National University of Singapore (NUS), and also with the Co-Director of the NUS Business Analytics Centre. He has authored more than 30 articles, and 8 patents and invention disclosures. His research interests include big data analytics, optimization, AI, cloud computing, and blockchain.

Dr. Pang was a recipient of a number of industry and academic awards, including the IBM Outstanding Technical Achievement Award (OTAA), the IBM Invention Plateau Award, and finalist of the Andrew Fraser Prize 2007 of the Institute of Mechanical Engineers (IMechE).