**A Stable-aware Blockchain Consensus Protocol for Wireless Blockchain Systems**

**Abstract-** Blockchain can solve security and trust challenges in wireless networks. Most previous studies of blockchain consensus protocols in wireless network rely on efficient and stable transmissions and correct leaders. Nevertheless, nodes in wireless blockchain have limited physical resources, unreliable channels, and varying bandwidths influenced jamming attacks or environments. In this paper, we propose a novel Byzantine fault-tolerant consensus protocol SWIB (**S**tability-aware **Wi**reless **B**lockchain) for blockchain in wireless networks, which do not rely on reliable communications. SWIB selects a block proposer randomly to prevent adversary corrupting the block proposer, and uses a threshold signature scheme as block proposal voting mechanism to improve the performance of blockchain system. Because only one block will be confirmed in per round, SWIB protocol can avoid the occurrence of conflicting blocks and blockchain forks. Moreover, it can guarantee security while tolerating at most faulty nodes among consensus nodes. Extensive simulation results show that SWIB is resistant to jamming attack, double-spending attack, and Sybil attack.

# Introduction

With the rapid development of wireless communication and blockchain technologies, much work has been carried out to apply blockchains in wireless applications, such as mobile edge computing [1], intelligent 5G technology [2], the Internet of Vehicles [3], etc. Applications for wireless networks face with significant challenge of security and trust. Resources constrained mobile devices are vulnerable to various attacks. Meanwhile, the open communication of wireless networks is heavily impacted by environment. Both channel bandwidth and jamming attacks make the communication in wireless networks become unstable and unreliable. Blockchain has received great attention from both academia and industry. With salient properties of decentralization and persistence as well as traceability, blockchain provides a new way to solve security and trust problems. This means that blockchain technology can provide reliable and secure resource sharing services in wireless networks. In this case, secure, trust, and efficient services of data interaction, secure access control, data traceability, identity authentication in wireless field can be supported by integration of blockchain and wireless networks.

Blockchain is emerged as a core technology of Bitcoin, which is known as a decentralized digital cryptocurrency and appears in 2008. Blockchain offers many benefits, such as decentralization, security, transparency, data integrity, and so on. Therefore, blockchain technology is being explored in many innovative applications, such as crypto currencies, smart contracts, Internet of Things, etc.(放在Introduction)

Currently, much work on wireless blockchain systems is to directly enable popular blockchain protocols in the global Internet to wireless network environment. Consensus protocols adopted by these blockchain protocols usually require massive resources consumption (e.g., Proof of Work [4]) and complicated design (e.g., Proof of Stake [5]), or rely on reliable communications (e.g., Practical Byzantine Fault Tolerant [6]). However, the limitation of wireless network makes these classical blockchain consensus protocols difficult to be deployed in wireless networks. This motivates research on design of blockchain protocols for wireless networks.

Recently, some scholars proposed blockchain consensus protocols for wireless networks. Considering the high dynamics of mobile ad-hoc network, Jiao et al. [7] designed a PoW-based stability-aware consensus protocol, whose leader election is based on node information and Proof of Work. This novel design can make sure wireless blockchain system work efficiently and steadily. But nodes running this consensus protocol require to consume massive resources, which is a heavy burden for wireless devices. In order to decrease computation power consumption, some research on wireless blockchain systems leverage the characteristics of wireless networks to design efficient wireless blockchain consensus protocols. Considering the low-power wireless devices and instability of wireless transmission, Xu et al. [9] proposed an efficient and fair Proof-of-Communication consensus protocol for wireless blockchain systems. Zou et al. [10] proposed a fast consensus protocol for permissioned wireless blockchain systems, which can achieve *k*-times consensus in unreliable and multi-access wireless environment. Besides, to overcome the interference of wireless broadcast communication, Xu et al. proposed a single-hop wireless blockchain consensus protocol under an adversarial SINR model based on a Proof-of-Channel consensus algorithm [11]. In [12], Xu et al. designed a fast fault-tolerant protocol for multi-hop wireless blockchain network wChain. To accelerate data aggregation, this protocol constructs communication spanner by maximized independent set. However, these consensus protocol cannot tolerate Byzantine failure, which is the common phenomena in wireless networks. Leveraging the transmit signal of wireless networks, Jiang et al. [8] proposed a Sybil-proof-based Byzantine fault-tolerant consensus protocol, which can achieve real-time consensus in wireless networks by selected group of nodes. This consensus protocol requires quadratic message reliable exchange to achieve consensus. Actually, all these consensus protocols work under assumption of reliable message transmission, and not consider the impact of message loss for consensus process in wireless networks.

In this paper, we propose a stability-aware wireless blockchain consensus protocol SWIB. This protocol is analogous to the Proof-of-Stake consensus protocol in the way that nodes can achieve consensus without consuming massive resources for mining. SWIB adopts a randomized election scheme and a secure threshold signature scheme to ensure that all nodes in the wireless blockchain system can reach consensus in a random and steady manner. It operates in a round by round fashion. Each consensus round contains block proposer election phase, block proposal generation phase, block verification phase, and block finalization phase. A single block proposer is randomly and non-interactively selected according to nodes' probability in block proposer election phase. This probability depends on nodes' stability, which is a function of nodes' active time and the number of recently generated blocks. The unpredictability of leader election can reduce the corruption risk of adversary. In addition, we adopt the threshold BLS (Boneh-Lynn-Shacham) signature scheme to improve the efficiency of consensus reaching in blockchain system. Using such a scheme can greatly reduce the system communication overhead of consensus process. Decoupling block proposer from block verification and finalization can increase the stability of consensus termination. Consensus termination can be achieved by any node who has obtained sufficient votes, without relying on correctness of block proposer. Thus, our protocol can improve the stability and efficiency of consensus process, and also reduce the risk of faulty consensus caused by faulty nodes or unstable wireless channels. Our contributions in this paper are summarized as follows:

* We propose a new blockchain consensus protocol SWIB, which combines random election algorithm with threshold BLS signature scheme. It can ensure stable generation of blocks in wireless blockchain systems and reaching consensus in unreliable and unstable one-hop wireless networks.
* We propose a random block proposer election algorithm, which is suitable for wireless networks. Consequently, a high-quality node can be elected as block proposer in a randomized way, which can reduce the corruption risk of adversary and improve the chance of generating valid block.
* To improve the robustness of SWIB, we use threshold BLS signature scheme as voting mechanism to improve the efficiency and stability of consensus process. Even the block proposer fails after broadcasting a block, block finalization can still be completed through one round of partial signatures exchanges. Moreover, our protocol design satisfies strong consistency that can efficiently prevent blockchain forks.
* We analyze the consensus success probability and expected consensus latency of SWIB protocol, and discuss the consensus security and attack resistance of SWIB when adversary controls less than 50% of voting power. Finally, extensive simulation results validate the correctness of our theoretical analytical results.

The rest of this paper is organized as follows. Section 2 introduces related work on state-of-the-art blockchain protocols, wireless consensus algorithms. In Section 3, we introduce various models and assumptions in this study. In Section 4, we present the details of the stability-aware wireless blockchain consensus protocol. Security and performance analyses are conducted in Section 5. Extensive simulation results are presented in Section 6 for performance evaluation, and conclusion is given in Section 7.

# Related Work

In this section, we give a brief review of existing work for consensus protocols in blockchain. We will first introduce state-of-the-art blockchain consensus protocols and then consensus protocols for wireless networks.

## 2.1 Blockchain Consensus Protocols

In this subsection, we briefly introduce popular blockchain consensus protocols, and divide into two categories: resource-proof-based and communication-based. For a comprehensive overview in this aspect, please refer to [13].

Resource-proof-based consensus protocols require consensus nodes to compete for the block proposal right in each round using their physical resources (e.g., computational power, memory, etc.) or virtual resources (e.g., shares, reputation, wealth, etc.). The most classic proof-of-physical-resources consensus protocol is Proof-of-Work (PoW) [4], which is adopted in Bitcoin and Ethereum. In PoW consensus algorithm, nodes win the block proposal opportunity by solving a computational puzzle. However, this protocol cannot provide instant consensus finality of blockchain protocol [14]. Actually, even though adversary controls computing power is less than 50% of total power, multi-blocks confirmation can only guarantee probabilistic consistency of PoW-based consensus protocol. Due to the large time-varying of generate a block, the block-confirmation latency of PoW-based blockchain protocol is in general large, and transaction throughput is limited. In order to improve the performance of blockchain system, some other physical-resource-proof-based consensus protocols have been proposed. For example, consensus nodes running Proof-of-Space consensus protocol [15] compete for block proposal right through occupied memory or disk space, and achieve consensus within about 4 minutes. Proof-of-Burn consensus protocol [16] belongs to the category of physical-resources-proof-based consensus protocols. Consensus nodes obtain block proposal chance by burning another “coin” such as Bitcoin.

Physical-resource-proof-based consensus protocols consume huge physical resources of consensus nodes to pursue the block proposal chance, which leads to massive waste of physical resources. As an alternative, virtual-resource-proof-based consensus protocols can avoid such large resource overhead. Proof-of-Stake (PoS) [5] is a typical consensus protocol in this aspect. In PoS, consensus nodes are elected as block proposer according to their held stakes. The more stakes a node holds, the higher the probability it is elected. In order to solve the “Nothing at stake” problem of PoS and improve the performance of blockchain system, some consensus protocols have been proposed. Such as Proof-of-Authority consensus protocol [], in which consensus nodes passing a preliminary authentication aware the right to generate new blocks. Proof-of-Reputation [18] is also a virtual-resource-proof-based consensus protocol, in which consensus nodes with enough reputation can obtain the right to generate a new block. Virtual-resource-proof-based consensus protocols do not consume physical resources, and are friendly to environment. Therefore, more and more blockchain systems pursue to use proof-of-virtual-resource consensus protocols.

In communication-based blockchain consensus protocols, all consensus nodes reach consensus on block proposal by exchanging messages and performing local computation. Most of these protocols can tolerate Byzantine failure and provide strong consistency. The most classical communication-based consensus protocol is practical Byzantine fault tolerant consensus protocol (PBFT). In PBFT, a block proposer is elected from all consensus nodes to propose a new block, which will then be responsible for driving communication of vote phase. Because consensus nodes are not required to mortgage assets or consume resource, adversary can be malicious in consensus process with small cost. PBFT consensus protocol eliminates the influence of malicious behavior to ensure blockchain system security by cooperation mechanism. Since the communications of nodes are driven by leader/primary, the consensus security of PBFT depends on the correctness of leader. Faulty leader can lead to the interruption of consensus process. The PBFT consensus protocol achieve consensus among consensus nodes with quadratic message complexity. Thus, PBFT consensus protocol usually has low scalability due to high communication overhead. To overcome the shortage of PBFT consensus protocol, some communication-based protocols are proposed to improve performance by reducing communication overhead. In NEO [20], partial nodes of delegated Byzantine fault tolerant consensus protocol are delegated to participant consensus process to reach agreement by voting on generated block. Reducing the number of consensus nodes can decrease the number of communication messages, and further increase the performance of system. Zyzzyva [21] utilizes a modified BFT consensus protocol SBFT. The consensus protocol employs a threshold signature scheme to reduce communication overhead of consensus process. Since consensus latency decreases, the performance of system will be improved.

Hybrid consensus protocols can alleviate the “impossible triangle” of blockchain systems. Single consensus protocol cannot satisfy security, decentralization and scalability of blockchain systems simultaneously. Physical-resource-proof-based consensus protocols are highly decentralized and secure, but its scalability is low. Virtual-resource-proof-based consensus protocols are highly decentralized and scalable, but exist serious security problems. Communication-based consensus protocols have high scalability and security, but decentralization is low. Therefore, hybrid consensus protocols have been proposed to balance the “impossible triangle” of blockchain system. The first version of Casper [17] is a hybrid consensus of PoW and PoS, aiming to replace the PoW consensus algorithm with PoS consensus algorithm in Ethereum. This consensus protocol improves the security of blockchain system by reducing the risk of chain fork. Fruitchain [] uses a hybrid consensus protocol of PoW and DPoS consensus algorithms. This protocol can achieve high performance and low fork probability. In order to prevent chain fork and achieve high performance, some hybrid consensus protocols combining resource-proof-based and BFT consensus algorithms have been proposed. ByzCoin [] improves transaction throughput by adopting a hybrid consensus protocol of PoW and BFT consensus algorithms. This protocol can achieve strong consistency of blockchain system. These consensus protocols are not suitable for wireless networks with limited resources devices due to high computation overhead. To decrease the waste of resources, Tendermint [22] uses a hybrid consensus protocol combining PoS and BFT consensus algorithms. This protocol adopts leader rotation mechanism to avoid adversary corruption, and achieve high security and performance of system by BFT consensus algorithm. Besides, Algorand consensus protocol [23] is a hybrid consensus protocol of PoS and Byzantine agreement algorithms. This protocol uses VRF-based leader and committee election algorithm to prevent adversary knowing the information of leader and committee in advance. Byzantine agreement protocol can make sure high performance and strong consistency of system. However, these consensus protocols adopting BFT consensus algorithms rely on reliable communication model. Thus, these protocols cannot be directly utilized in wireless scenarios with unreliable and unstable communication channels. Our protocol is a type of hybrid consensus protocol combining PoS and communication-based consensus algorithms. This protocol uses PoS consensus algorithm to ensure the fairness of consensus process, and utilize a special communication-based consensus algorithm to improve the performance and security of system.

## 2.2 Consensus Protocols for Wireless Networks

Since our study is closely related to consensus protocols and wireless networks, we briefly introduce the studies on consensus protocols for wireless networks in this subsection.

There has been extensive prior research on consensus protocols for wireless networks. Santoro and Widmayer [] study consensus in the presence of unreliable communication, and show that consensus cannot be achieved if as few as of the messages sent in a round can be lost.

Many consensus protocols have been proposed to achieve consensus in wireless networks. Leveraging the natural superposition property of wireless multiple-access channels, Zheng et al. [24] proposed fast average consensus in clustered wireless sensor networks to achieve consensus within short time. In order to efficiently achieve global consensus among nodes in clustered wireless networks, Goldenbaum et al. [25] presented an iterative gossip algorithm based on the superposition property of wireless channel. Newport and Robinson [26] proposed fault-tolerant distributed consensus algorithms to solve consensus problem of wireless systems through abstract MAC layer model. These consensus algorithms can guarantee consensus termination with high probability even facing any number of failures and no network information in advance. To achieve finite-time max-consensus in a multi-agent system, Molinari et al. [27] presented a switching consensus protocol according to the superposition property of fading wireless channel. Max-consensus can be achieved under this protocol within finite number of iterations. Besides, Moniz et al. [28] proposed an asynchronous Byzantine consensus protocol for resource-constrained wireless ad hoc networks. Even some messages are lost dynamically, the protocol can still achieve consensus efficiently.

In recent years, some studies combined wireless consensus algorithms with blockchain to design blockchain consensus protocols for wireless networks. According to the intristic property of wireless broadcast communication, Jiang et al. [8] proposed a Sybil-proof-based Byzantine fault-tolerant consensus protocol, which can realize real-time consensus in wireless networks. Some studies increase consensus efficiency by making full use of wireless broadcast operations. Xu et al. [9] proposed an efficient and fair Proof-of-Communication consensus protocol in wireless blockchain systems. Zou et al. [10] proposed a fast consensus protocol that can achieve *k*-times consensus in unreliable and multi-access wireless environment. Besides, to overcome the interference of wireless broadcast communication, Xu et al. proposed BLOWN that based on a Proof-of-Channel consensus algorithm under adversarial SINR model [11]. In addition, Xu et al. designed a fast fault-tolerant wireless blockchain protocol wChain [12], which can quickly aggregate data and reach consensus in multi-hop wireless communication networks.

这里应该总结一下本文工作与上述工作的主要差别…否则读了半天，毫无感觉.