# Models and Related Technology

We describe the preliminaries of SWIB, including network model, blockchain setting, communication model, and attack models. When designing a blockchain consensus protocol, we first require to determine a network model that is the fundamental infrastructure running the protocol. Then, we should consider the data architecture of distributed ledger used in our protocol. To improve the performance of blockchain protocol, we use a threshold BLS signature scheme as voting mechanism to reduce consensus latency. Since computing time is negligible small, we can analyze the performance of consensus protocol by giving a communication mode. In order to discuss the attacks-resistance of consensus protocol, attack models should be predefined.

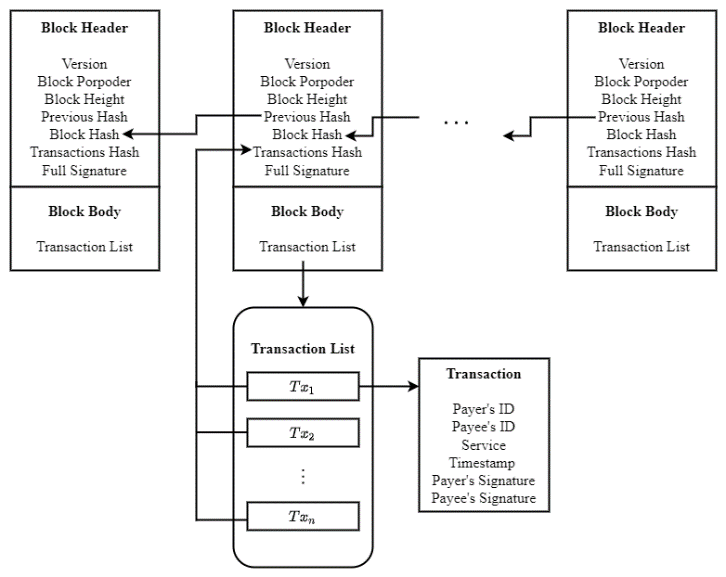
## 3.1 Network Model

Blockchain consensus protocols are designed according to network models. Consensus nodes achieve consensus through networks transmitting messages. We only consider a wireless broadcast network consisting of nodes, which are located within communication range of each other, and communicating with each other by transmitting messages. All nodes have same functions. Each node equipped with transceiver works in a half-duplex manner. This means that nodes can transmit or receive messages, but not both simultaneously. In practice, such a network can be formed by a group of unmanned aerial vehicles or intelligent vehicles.

Nodes adopting digital signature technology can achieve node identity confirmation and the verification and integrity of communication messages. In digital signature, each node has its key pair, which used to message encryption and decryption, and generate signature. We assume that each node can get its private-public key pair and a main public key by independently running a secure distributed key generation protocol. Each node can obtain the public keys and identities of other nodes by exchanging messages. Thus, each node knows the identities and public keys of all other nodes.

## 3.2 Blockchain

Blockchain is a public electronic ledger, which similar to a relational database. This ledger is openly and simultaneously shared among various nodes in system. Blockchain uses a consensus protocol to ensure the dependability and integrity of blockchain system. Therefore, blockchain can only be updated when consensus is reached on a new block between nodes in the system. Each node maintains a local blockchain, which is composed of blocks chronologically linked to create a chain. Each block contains a block header and a block body. The block header records blockchain version, block proposer, block height, previous hash, block hash, block full signature, and transactions hash root, etc. The block body stores transaction recodes, which consist of payer's information, payee's information and other necessary contents. Figure 1 shows the data structure of a blockchain.



**Fig. 1 Blockchain**

## 3.3 Threshold BLS Signature Scheme Technology

Threshold Boneh-Lynn-Shacham (BLS) signature scheme [29] is the combination of threshold signature scheme [34] and BLS signature scheme [30]. The signature share generation of threshold BLS signature scheme concurs with the BLS, and the aggregation of full signature is congruent with threshold signature scheme. BLS signature scheme is closely related to bilinear maps and Gap Diffie-Hellman (GDH) groups, where the Computational Diffie-Hellman problem is hard but the Decision Diffie-Hellman problem is easy. Threshold signature scheme allows multiple participants securely reconstruct a secret (i.e., a main private key) and perform computation (i.e., signature generation or decryption) even an adversary has corrupted some participants. Threshold BLS signature scheme includes key generation algorithm, signature generation algorithm and verification algorithm. The key generation algorithm adopts a discrete log-based distributed key generation method [31] to distribute private-public key pair and a main public key to participants. In threshold BLS signature scheme, participants jointly sign a message through the signature generation algorithm. The full signature of the message can be obtained when a sufficient number of participants sign the message. All participants can use the main public key to verify the full signature by the verification algorithm.

Threshold Boneh-Lynn-Shacham (BLS) signature scheme [29] can be used to help consensus protocols improve the performance of system. Consensus protocols can adopt the threshold BLS signature scheme as a voting mechanism to improve the efficiency of consensus. All consensus nodes use a share of a main private key as their private keys. In a consensus process, each node generates a partial signature of a proposal as the vote of the node for the proposal. The full signature of the proposal can be recovered when nodes aggregate a sufficient number of partial signature. Since several partial signatures can be aggregated into a full signature, nodes can verify multiple votes in an operation. In addition, the termination of a consensus process not relies on the leader of system. Any consensus node can terminate a consensus process when it constructs the full signature and broadcasts the full signature to others. Therefore, threshold BLS signature scheme can help consensus nodes quickly and steadily achieve consensus. In SWIB, we use threshold BLS signature scheme as mechanism to improve the performance of blockchain system. To ensure the security of SWIB, we assume that the number of honest nodes should satisfy the requirement of threshold BLS signature scheme.

## 3.4 Communication Model

In SWIB, we mainly focus on the impact of wireless communication in the performance of blockchain system. As a metric that used to evaluate the performance of blockchain system, consensus latency consists of computing time and communication time. However, the computation load of nodes in SWIB is small, which means the computing time is negligibly small. During consensus process, nodes broadcast messages over wireless channel to achieve consensus. We consider a communication model with p-persistent carrier-sense multiple access (CSMA). Nodes continuously sense channel and transmit message with a constant probability when detecting channel idle. We assume that wireless channels follow the Rayleigh fading model [32]. The channel gain between nodes follows the complex normal distribution. According to the Rayleigh fading model, the received signal-to-noise (SNR) ratio over the channel between nodes can be computed.

During consensus process, messages losses can lead to consensus failure. Message losses are mainly caused by channel collision and channel fading. Therefore, a successful transmission should satisfy two conditions: 1) if and only if there only one node transmitting in a time slot; and 2) the SNR ratio is equal to or bigger than the target one. In channel contention process, nodes compete for the channel with a constant transmit probability. Only if one node transmits in a mini time interval can the node transmit message successfully. Even a node competes successfully, it may fail to transmit a message due to channel fading. The SNR ratio over channel between nodes varies with the time-variant communication environment. When SNR ratio is less than a given target threshold, the communication between nodes is interrupted. In order guarantee communication under unreliable networks, retransmission mechanism is necessary. When communication interruption occurs, retransmissions are carried out until the lost messages are successfully delivered.

## 3.5 Attack Models

Attacks launching by adversary can halt consensus process. The attack-resistance is very important for security of blockchain system. We assume that an arbitrary adversary can control no more than of the total voting power and corrupt nodes. In SWIB, we only consider two kinds of attacks of adversary: Sybil attack and jamming attack.

* Adversary can launch Sybil attack, in which adversary can generate a large number of identities for corrupted nodes. These nodes can deviate from consensus protocol. Adversary may obtain inappropriate power in consensus process. Adversary can overwhelm other nodes through majority voting power, then control the generation of blocks and prevent other new nodes from entering system.
* Adversary can launch jamming attack to interfere with the message transmission. Jamming attack is a denial of service attack that adversary prevents other nodes from using the channel to communicate by occupying the channel they are communicating on. Consensus process can be interrupted when adversary launches jamming attack. Adversary can prevent other nodes from broadcasting their votes. A consensus process cannot be complete if the number of votes is less than the secure threshold of blockchain system. In Blockchain system adopting communication-based consensus protocols will loss liveness when consensus process is interrupted. Adversary can prevent other new nodes from entering system by jamming the requests of these new nodes. Therefore, the security of the system will be halted.

We design SWIB that can resistant both Sybil attack and jamming attack. Even an adversary launches attacks, blockchain system can still work due to adversary cannot affect the security of blockchain system.

# The Stable-aware Wireless Blockchain Consensus Protocol

In this section, we propose a stable-aware wireless blockchain consensus protocol, abbreviated as SWIB. We first give an overview of the protocol, and then present a detailed of SWIB. To ensure the security of the protocol, we propose an incentive and publishment mechanism and a synchronization mechanism.