# Models and Related Technology

We describe the preliminaries of SWIB, including network model, blockchain setting, communication model, and attack models. Network model is the fundamental infrastructure running the blockchain consensus protocol. Blockchain is the data architecture of distributed ledger used in SWIB. We leverage threshold BLS signature scheme to improve the performance of blockchain consensus protocol. Besides, communication model is the precondition of performance analysis in consensus protocol. In addition, we analyze the attack-resistance of SWIB under attack models.

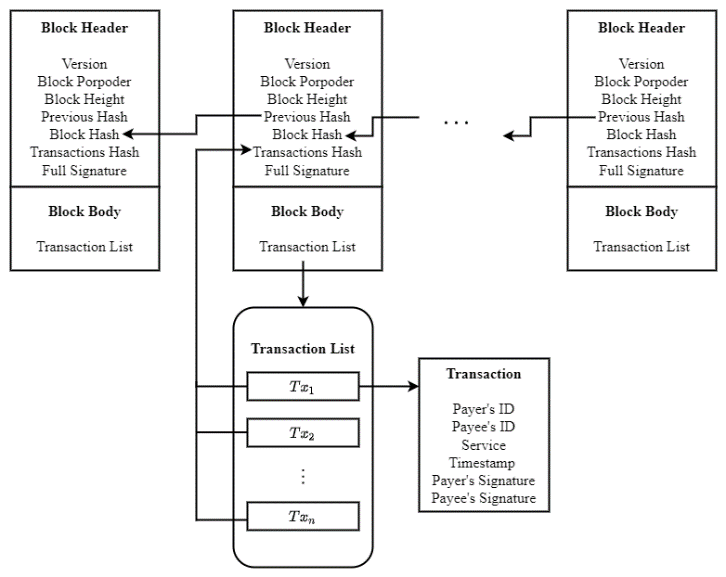
## 3.1 Network Model

Blockchain consensus protocols are designed according to network models. Consensus nodes achieve consensus on blocks through networks transmitting messages. We 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 Model

In blockchain 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 Signature Scheme

We utilize a threshold Boneh-Lynn-Shacham (BLS) signature scheme [29] to improve the performance of consensus protocols. Consensus protocols can adopt the threshold BLS signature scheme as a voting mechanism to confirm the validity of proposals. A partial signature generated by a node for a proposal is the vote of the node for the proposal. Since several partial signatures can be aggregated into a special signature, nodes can verify multiple votes in an operation. In addition, the termination of a consensus process not relies on the leader of consensus system. Any consensus node can terminate a consensus process when it has constructed the special signature. Therefore, threshold BLS signature scheme can help consensus nodes quickly and steadily achieve consensus.

Threshold signature scheme [34] aims to allow 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. In a threshold signature scheme, all participants use a share of a main private key as their private keys. To sign a message, multiple participants can execute an interactive signature generation algorithm, which uses their shares of the main private key and the message as inputs, and outputs a signature of the message. The signature can be verified by anyone using the unique main public key. The security for threshold signature scheme requires that no adversary that corrupts some participants can learn any information about the main private key or can forge a valid signature on a message. There are two important properties of threshold signature scheme: robustness and proactiveness. The former one requires that a valid signature can be generated even some malicious participants deviating from the scheme. The later one is also name periodic refreshment of shares of a main private key. The goal proactiveness is to protect a system from an adversary that obtains the information of a main private key.

Boneh-Lynn-Shacham (BLS) signature scheme [30] is closely related to bilinear maps and Gap Diffie-Hellman (GDH) groups. The signature is based on bilinear maps on elliptic curves. In GDH groups, Decision Diffie-Hellman problem is easy on certain elliptic-curves groups, but Computational Diffie-Hellman problem is hard. The BLS signature scheme based on GDH groups consists of key generation algorithm, signature generation algorithm and signature verification algorithm. Let be a GDH group pair of prime order , and be the generator of and , respectively. The signature scheme makes use of a secure hash function . In key generation, each participant has a key pair , where is private key that used to compute public key . Given a private key and a message signer can compute a digest and a signature Given a public key , a message and a signature , verifiers can compute and verify whether the Diffie-Hellman tuple is a valid.

Threshold BLS signature scheme [29] is the combination of threshold signature scheme and BLS signature scheme. The signature share generation of threshold BLS signature scheme concurs with the BLS, and the aggregation of group signature is congruent with threshold signature scheme. 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. Let be a GDH group pair of prime order , and be the generator of and , respectively. The signature scheme makes use of a secure hash function . The key generation algorithm outputs a private-public key pair for participant and a main public key , where is a share of a main private key and the public key is calculated as . The signature generation algorithm contains a partial signature generation method and a full signature recovery method. The former one is similar to the signature generation algorithm of BLS signature scheme. Given a message a signer running signature share generation method can compute a digest and a partial signature The full signature of the message can be recovered if participants aggregate a sufficient number of partial signature and execute the full signature recovery method. The full signature should be the Lagrange interpolation polynomial of these partial signatures, i.e., . The verification algorithm of threshold BLS signature scheme uses the main public key to verify the validation of the full signature. Given a main public key , a message and the full signature , verifiers can compute and verify whether the Diffie-Hellman tuple is a valid.

## 3.4 Communication Model(放在分析里面)

(加一些过渡的话)通信是分析的基础

Nodes running the SWIB can achieve consensus on proposals. For simplicity, we assume that the consensus processing is divided into synchronous rounds, each of which contains multiple slots. A slot is the time unit for nodes to transmit or receive a packet.(放在分析中)

We consider a wireless communication model with p-persistent carrier-sense multiple access (CSMA). where nodes continuously sense and transmit message with probability when detecting channel idle. We assume that the wireless channels follow the Rayleigh fading model [32]. In detail, the wireless channel between nodes and experiences path-loss is modeled as

where is the path-loss at reference distance , and is the distance between nodes , and is path-loss exponent. Let be the channel gain from to , following the complex normal distribution with zero mean and variance (i.e., ). When a signal is transmitted from to with transmission power , the Signal-to-Noise (SNR) ratio at receiving node is formulated as

where is the additive white Gaussian noise.

Messages losses can lead to consensus failure. In addition, 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 same transmit probability . Only if one node transmits in a time slot can the node transmit message successfully. Let be a variable that denotes the number of nodes, transmission contention success probability can be expressed as

Even a node competes successfully, it may fail to transmit a message due to channel fading. The SNR between nodes varies with the time-variant communication environment. When SNR is less than a given target threshold, the communication between nodes is interrupted. Since is exponentially distributed, the the SNR outrage probability between nodes and is expressed as follows

Both collision and channel fading can result in message losses. 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

为什么要考虑这个，纯粹文字性描述

We assume that an arbitrary adversary can control no more than of the total voting power and corrupt nodes. The malicious behaviors of adversary are as follows

* 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, （对共识过程的影响） by transmitting faulty messages to other nodes or doing nothing in consensus process(发送错误消息，不发送消息，或者);
* Adversary can launch jamming attack to interfere with the message transmission in wireless networks.（对共识过程的影响） Without loss of generality, we assume that the attack capability of adversary is - bounded, i.e., in any interval of consecutive slots, adversary can jam no more than slots, where and 0 < ≤ 1.(放在性能分析)