Lei YU, Xiao-fang ZHAO, Yan JIN, Heng-yi CAI, Bo WEI, Bin HU, 2019. Low powered blockchain consensus protocols based on consistent hash. *Frontiers of Information Technology & Electronic Engineering*, 20(10):1361-1377. https://doi.org/10.1631/FITEE.1800119

Low powered blockchain consensus protocols based on consistent hash

Key words: Blockchain; Consensus protocol; Consistent hash; Low energy consumption; Decentralization

Corresponding author: Lei YU
E-mail: yulei2008@ict.ac.cn; yulei@ncic.ac.cn
ORCID: Lei YU, http://orcid.org/0000-0003-4316-1763

Motivation

- The value of blockchain technology has been widely recognized, but consensus protocols for blockchain technology still face challenges. The consensus protocol of the public blockchain cannot achieve the goal of simultaneous optimization of decentralization, low energy consumption, and security.
- The strong privacy guarantee limits the promotion of blockchain technology, and in most industry scenarios, proper supervision is necessary.

Running scenario

Assumption 1 The asymmetric cryptographic algorithm is public. In the case of a known public key, it is not feasible to solve the private key through algorithm inversions, or randomly to search for possible private key space. It is not feasible to fake the digital signature.

Assumption 2 The hash digest algorithm cannot be inverted.

Assumption 3 The percentage of honest nodes in the blockchain network exceeds 50%. If the percentage of non-honest nodes is more than 50%, the blockchain system will be worthless.

Assumption 4 The consistent hash algorithm contains enough space to hold enough nodes on the hash ring. It ensures that any node's mappings on the hash ring do not overlap, and it is impossible to reverse.

Main idea

- The consistent hash algorithm can provide a random election mechanism to determine the node of the creating block, which can avoid the computational competition behavior of honest nodes. The validation of new block is still simple, but the malicious node forging new block requires high computational power.
- Limited regulation is needed in most industrial scenarios. Digital certificate-based registration mechanism is the premise of public blockchain applications.

Method

1. Blockchain data structure of CHB-consensus

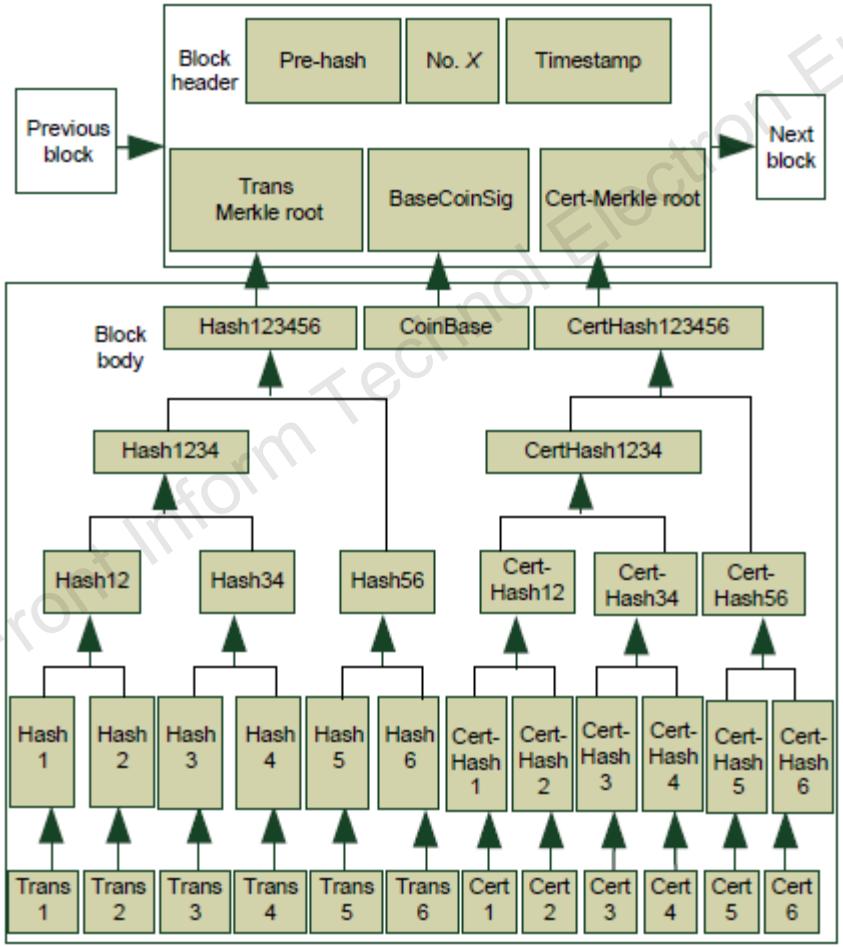

Fig. 4 Blockchain data structure of CHB-consensus

Method

2. Determination of the creator of a new block based on a consistent hash algorithm

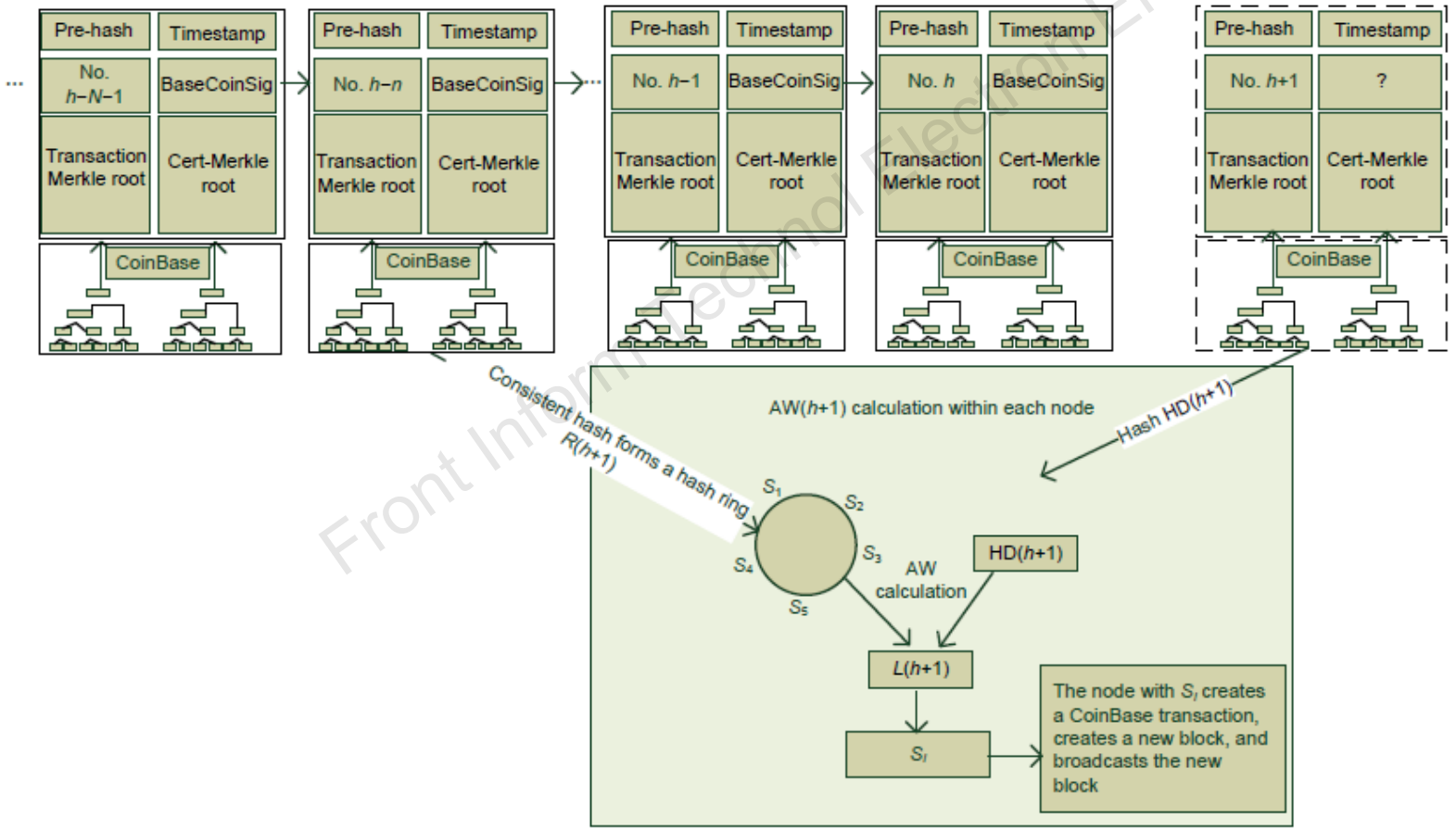

Fig. 5 AW calculation process when a block is created

Method

3. The creation process of a CHBD-consensus protocol

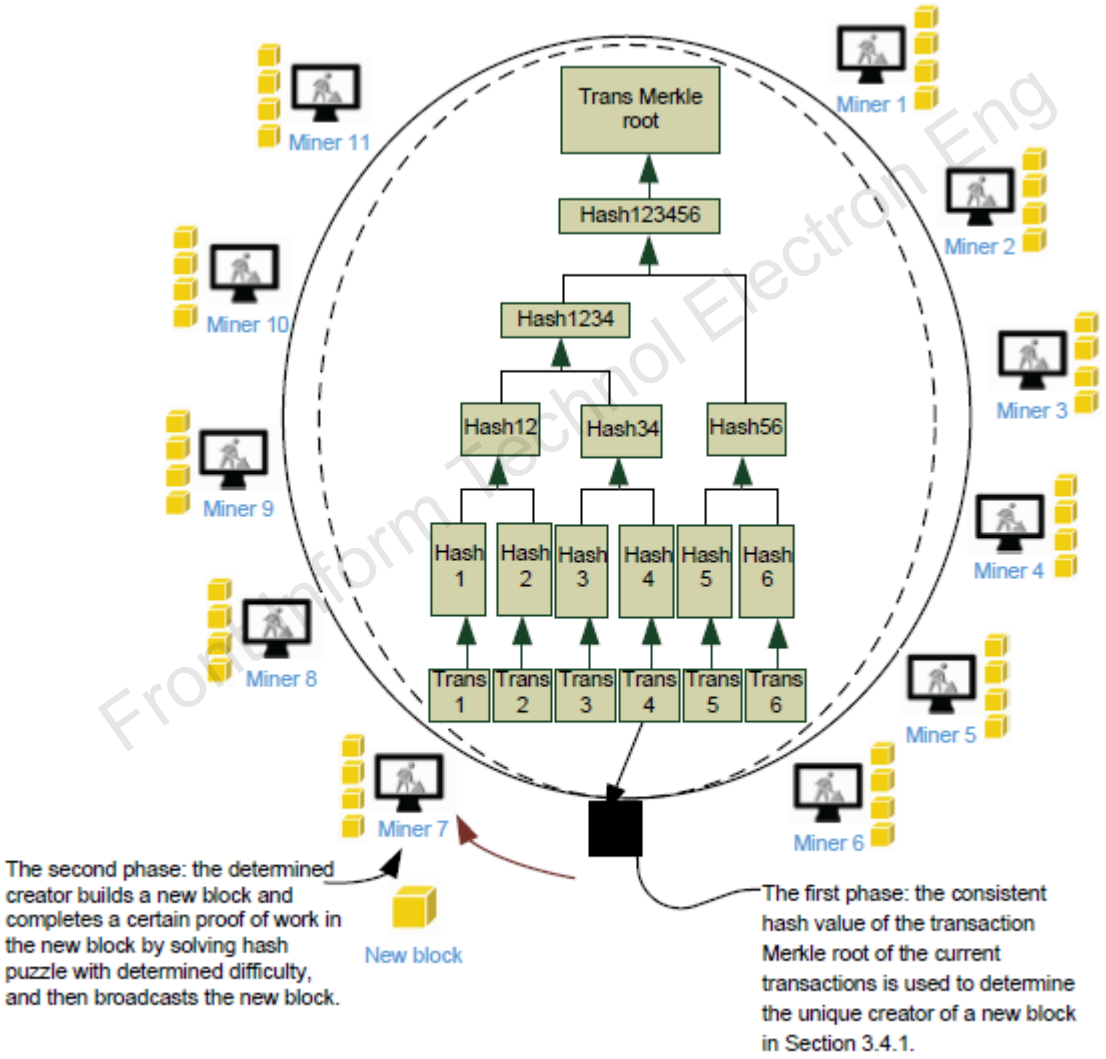

Fig. 6 Basic process of CHBD-consensus

Method

Validation 1 The previous block referenced by the new block exists, and is valid.

Validation 2 The block contains the correctness of transactions.

Validation 3 Correctness and completeness of other data items exist in the block header and block body.

Validation 4 The output of the token reward transaction is pointing to an address which is different from that of the output token reward transaction contained in block h (to avoid aggression, two consecutive reward transactions sent to the same public key address are not allowed).

Validation 5 Recalculate HD(h+1), $R(h-N)$, and mapping position $L(h-N)$ on the corresponding hash ring, and validate the consistency with the calculation result of the current node in step 3.

Validation 6 Validate that the output of the token reward transaction in block h+1 is consistent with the public key address of S_i corresponding to the digital certificate serial corresponding to $L(h-N)$.

Validation 7 Validate that the digital certificate number S_j of this node is contained in the body of block h+1.

Validation 8 Validate the consistency of the digital signature BaseCoinSig in the header of block h+1 with the token reward transaction in the body of block h+1. When all the validations are passed, the node accepts the new block h+1 and links it to the end of the current blockchain.

Method

Validation 9 When a node receives each new block from the P2P network, it will determine whether a fork occurs or not. If a fork occurs, the node downloads multiple branches, and the following calculations are made for each branch by the node:

$$\mathrm{BranchWeight} = \sum_{i=h-b}^{i=h+1} \left[\frac{\mathrm{NumT}_i}{1+\mathrm{ownT}_i} \cdot \mathrm{Re}(i) \right].$$

Validation 10 Validate that the random number Nonce found by the creator makes the double SHA256 target hash value of the block header satisfy the difficulty value requirement.

Theoretical analysis

- The main energy consumption of the PoW consensus protocol comes from the double SHA256 calculation of all miners for solving the hash puzzle. In the PoW protocol, let D_{PoW} denote the difficulty value and V the target value. Then we can have

$$D_{\mathrm{PoW}}=V_{\max}/V, \tag{8}$$

- Thus, for any given Nonce, the probability p when it satisfies difficulty is given by

$$p=\frac{V}{2^{256}}=\frac{V_{\max}}{D_{\mathrm{PoW}}\cdot 2^{256}}=\frac{1}{D_{\mathrm{PoW}}}. \tag{9}$$

- For each node, the expected time to find a block is expressed as

$$E_{\mathrm{PoW}}(t)=\frac{D_{\mathrm{PoW}}}{R}. \tag{10}$$

Theoretical analysis

In the PoW protocol, n nodes perform a hash trial independently, so the expected time to find a block in the whole blockchain network is

$$E_{\text{w-PoW}}(t) = \frac{E_{\text{PoW}}(t)}{n} = \frac{D_{\text{PoW}}}{nR}. \tag{11}$$

The energy consumption in a unit time of each node is proportional to R, with a scaling factor a.

In the PoW protocol, the total energy consumption of the entire blockchain network during a creation period is

$$C_{\text{PoW}} = naRE_{\text{w-PoW}}(t) = aD_{\text{PoW}}. \tag{12}$$

Theoretical analysis

In the CHBD-consensus protocol, under the same attack difficulty as under the PoW protocol ($D_{\text{PoW}}=D_{\text{CHBD}}$), the difficulty value of the hash puzzle in the second phase is $d_{\text{CHBD-second}}=D_{\text{CHBD}}/n=D_{\text{PoW}}/n$. For each node, the expected time to find a block is

$$E_{\text{CHBD}}(t)=\frac{d_{\text{CHBD-second}}}{R}=\frac{D_{\text{CHBD}}}{nR}=\frac{D_{\text{PoW}}}{nR}. \quad (13)$$

In the CHBD-consensus protocol, there is only one node to perform the second-phase PoW in each creation period; thus, the expected time to find a block in the whole blockchain network is

$$E_{\text{w-CHBD}}(t)=E_{\text{CHBD}}(t)=\frac{D_{\text{PoW}}}{nR}. \quad (14)$$

The total energy consumption of the entire blockchain network during a creation period is

Theoretical analysis

$$C_{\text{CHBD}} = aRE_{\text{w-CHBD}}(t) = \frac{aD_{\text{PoW}}}{n}. \tag{15}$$

Through the above analysis, it can be seen that, under the same attack difficulty and in the same hardware and network environment, the expected time to create a new block using the PoW protocol or the CHBD-consensus protocol is the same. The ratio Rt of the energy consumption of the CHBD-consensus protocol to the energy consumption of the PoW protocol is

$$\text{Rt} = \frac{C_{\text{CHBD}}}{C_{\text{PoW}}} = \frac{1}{n}. \tag{16}$$

The CHB-consensus protocol does not consume any energy for hash calculation in the whole network. Therefore, there is no comparative analysis for the CHB-consensus protocol.

Conclusions

- Two new consensus protocols based on a consistent hash algorithm, CHB-consensus and CHBD-consensus, have been proposed. CHB-consensus and CHBD-consensus still use the unforgeability of hash computational power to reach a consensus across the blockchain network. They force the attack behavior of malicious nodes to pay massive computational power, while an honest node's creation block process does not require additional computational power.
- We have analyzed possible attacks in detail and gave a rigorous but adjustable validation strategy.

Conclusions

- Finally, we have analyzed the issues of fairness, security, efficiency, privacy, and energy consumption, proving the advantages of CHB-consensus and CHBD-consensus. In the same hardware environment and with the same security guarantee, compared with PoW, CHB-consensus no longer consumes computational power. CHBD-consensus power consumption is 1/*n* times that of PoW.
- The existence of CA creates a risk of privacy leakage; however, the level of risk depends on the reliability and credibility of the CA system.