# A Master-Slave Blockchain Paradigm and Application in Digital Rights Management

**Zhaofeng Ma[1], Weihua Huang[2], Wei Bi[3,4], Hongmin Gao[1], Zhen Wang[1]**

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Shenzhen Datong Industrial Co..Ltd, Shenzhen 518000, China
[3] SeeleTech Corporation, San Francisco, 94107, USA
[4] Zsbatech Corporation, Beijing 100088, China

**Abstract:** Upon flaws of current blockchain platforms of heavyweight, large capacity of ledger, and time-consuming of synchronization of data, in this paper, we proposed a new paradigm of master-slave blockchain scheme (MSB) for pervasive computing that suitable for general PC, mobile device such as smart phones or PADs to participants in the working of mining and verification, in which we separated traditional blockchain model in 2 layer defined as master node layer and a series of slavery agents layer, then we proposed 2 approaches for partially computing model(PCM) and non-computing of model(NCM) in the MSB blockchain, Finally large amounts of simulations manifest the proposed master-slave blockchain scheme is feasible, extendible and suitable for pervasive computing especially in the 5G generation environment, and can apply in the DRM-related applications.

**Keywords:** master-slave blockchain; proof of equivalent work; proof of contribution; pervasive computing; DRM application

## I. INTRODUCTION

The original and core motivation of blockchain is to build up a cryptography-based decentralized digital currency system for self-organization transaction in an anonymous. Current blockchain platforms such as Bitcoin, Ethereum or Hyperledger provide a new and promising technology for digital cryptocurrency, distributed trusted data management or supply chain manangement[1-4]. However either Bitcoin or Ethereum and HyperLdger needs to synchronize the lager capacity of ledger, once the host is used as blockchain node for mining or verification, the whole computing memory and resource is occupied for computing, synchronizing, storing data by the blockchain system, in fact,current blockchain system is heavyweight and is difficult for extendible. In general case, blockchain is a decentralized trusted p2p platform which provides a cryptography-based trusted computing paradigm that all the transactions are constructed in a merkle-tree, and the specific transactions are organized under a unique

merkle-root, then in a proper time interval, then creates a block that include block header and block body, and the block header usually include timestamp, previous block hash, difficulty, version and reward.

As the first implemented blockchain appliciaiton, Satoshi Nakamoto first proposed the famous Bitcoin system in his paper “a peer-to-

Received: Mar. 21, 2018
Revised: Apr. 10, 2018
Editor: Luoyi Fu

peer electronic cash system" as the genesis innovation of decentralized digital cash system [1], in which the Bitcoin uses a proof-of-work mechanism to ensure the fair work of the computing and security[2], if someone try to modify the blocks existing in the blockchain, the proof-of-work consensus can ensure the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks[1-3]. Upon the peer to peer network, when constructing the block, new transactions are broadcast to all nodes, then each node collects new transactions into a block, each node works on finding a difficult proof-of-work for its block, When a computing node finds a proper difficult by proof-of-work, it then broadcasts the block to all p2p nodes, thosed nodes accept the block only if all transactions are valid and not already spent. nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Bitcoin is an innovative payment network and supports for rewards for mining or verification, however, Bitcoin is not so efficient for real-time transaction, and it is difficult and complex to developers, to solve the problems, Vitalik Buterin first proposed the kernel of Ethereum blockchain system which attempt to solve the efficiency and extendibility of the blockchain[5-7]. The Ethereum is a Turing-complete language which generally can solve the problem if there's enough time and storage space(whereas bitcoin is not Turning-complete), which supports Ethereum externally owned accounts (EOAs) and smart contract accounts, which is defined by its internal unique address, that can execute any possible user-defined codes according to user's needs and requirements via ERC20, the smart contract is executed in the Ethereum Virtual Machine(EVM). Ethereum is more flexible, extendible, easy and simple for users to build up variant blockchain by creates unique Token(defined by unique address)[3].

While Hyperledger fabric[4] provides a new, secure and enterprise consortium blockchain platform, which supports for manage node, verification node, each user should connect each other by certificates, and Hyperledger fabric is suitable for consortium blockchain for secure data management. The fabric is based on the most main source code from IBM, which does not support mining but is available for constructing consortium-based blockchain for authorized blockchain members.

In fact, the blockchain is defined as a cryptographic-based p2p distributed ledger with high-level security, credit, consensus and reward, which can build up variant application such as digital cryptocurrency, supply chain management, digital rights management[5-13]. in [14], the authors innovated a scheme of de-anonymizing social networks with overlapping community structure, and proposed a well-justified cost function minimizing the expected number of mismatched users over all possible true mappings. In fact, the efficiency, blockchain capacity and computing node, especially the computing ability restricts and limits general terminal and endpoint computing device joining into the mining and computing. If considering the computing and availability of mobile device, such as mobile phones, PAD, and personal computer, it need to consider flexible and extendible computing paradigm for blockchain for personal computing devices as light-weight blockchain nodes with fair consensus[9-10,13].

We proposed a new paradigm of master-slave blockchain scheme (MSB) for pervasive computing that suitable for general PC, mobile device such as smart phones or PADs to participants in the working of mining and verification, in which we separated traditional blockchain model in 2 layers defined as master node layer and a series of slave agents layer, and we proposed 2 approaches for partially computing model(PCM) and non-computing of model(NCM) in the MSB blockchain.

## II. Related Work

### 2.1 Current popular blockchain technology

#### 2.1.1 Bitcoin and its extendible blockchain platform

As the first successfully implemented blockchain application, Bitcoin[1-2] innovated the peer-to-peer electronic cash system as the original blockchain implementation, which proposed the cryptocurrency in a self-organi-

zation mode in P2P network, which verifies, constructs, synchronizes and stores the blockchain data permanently. However the Bitcoin is considered as low-efficient in TPS( only 7 TPS), and the average amount of the block is nearly 1MB, and the Bitcoin is not so efficient and is difficult to extend the architecture such as capacity, efficiency and instance of the transaction verification. Upon the Bitcoin-class blockchain, such as LiteCoin, Lighting Network are innovated and tried to solve the problem. Upon the efficiency, it is heavy-weight and cannot be separated the mining module into layered subsystem to enhance the efficiency, which limited the extendibility of the Bitcoin-like blochchain.

#### 2.1.2 Ethereum blockchain and its Token-based Innovation

To implement an extendible and reliable blockchain, Mr Butlin innovates a flexible blockchain Ethereum[3] and ERC20, in which Ethereum implements the paradigm in a generalized manner. And it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. Ethereum designed, implemented, and issued the flexible, useful, extendible platform for a new and flexible blockchain paradigm, especially it innovated the ERC20 protocol, which can make it easy to define a new token-based digital currency in public blockchain.

#### 2.1.3 Hyperledgerfabric consortium blockchain platform

Hyperledger fabric[4] provides a new, secure and enterprise consortium blockchain platform, which supports for authentication node, manage node, verification node, Hyperledger fabric is suitable for consortium blockchain for secure data management, such as supply chain management, traceability of source management, and public beneficence management[4-6, 12].

#### 2.1.4 Other new blockchian technologies

As for the efficiency, capacity, and security, the other new blockchain technologies such as lighting network, cross-blockchain, muli-blockchain technologies have been studied for more efficient and high-performance transaction capacity[5-12]. And there still exists DAG, EOS[18] public blockchain technologies, which will try to provide a more efficient and effective transaction process ability in TPS, transaction fee.

### 2.2 Existing problems and flaws of current blockchain

#### 2.2.1 Lacks of extendible architecture of blockchain[9-10]

Current blockchain technologies such as Bitcoin, Ethereum and hyperledger provide a cryptography ensured P2P distributed ledger, to ensure the fair and secure transactions, its supports kinds of consensus such as PoW, PoS, DPoS, PBFT. However, current blockchain is difficult to extend to a flexible, reliable and efficient computing paradigm that allows more and more computing units join in the computing and verification.

#### 2.2.2 Heavy-weight but low efficiency of TPS[1-3]

Current blockchain provides a distributed and trusted leger with blocks and transaction, but current blockchain node is not so efficient in TPS, not so flexible especially in a heavy-weight mode, it cannot extend for distributing the task to other computing unit such as general PC, mobile smart phones or PADs to participants the work of computing.

#### 2.2.3 Lack of consensus for new blockchain paradigm[12,15-17]

Current consensus such as PoW, PoS, DPoS, PBFT[1-5], are very limited for variant consensus supporting, such as PoW is low efficient for mining, while PoS is not still not so high performance for transaction confirmation. Current blockchain should considering more practical and efficient consensus for high TPS and DAPPs[12-17].

## III. The Proposed Master-Slave Blockchain Scheme

### 3.1 The proposed master-slave blockchain model

Upon flaws of current blockchain platforms of heavyweight, large capacity of ledger, and time-consuming of synchronization of data, in this paper, we proposed a new paradigm of master-slave light-weight blockchain architecture(MSB) for pervasive computing that suitable for general PC, mobile device such as smart phones or PADs, in which we separated traditional blockchain model into master-slave model, in which the master node responsible for transaction collection, computing task distribution, and the slave agents responsible for independently computing and commit result to the master node. The slave computing device may be personal computer, mobile phones. The master-slave blockchain model is described as follows in figure 1, which showed a hierarchical model of master-slave blockchain computing paradigm.

### 3.2 The master-slave blockchain architecture

In the master-slave blockchain scheme, we proposed 2 approaches for partially computing model(PCM) and non-computing of model(NCM) in the MSB blockchain, and in the PCM blockchain model we proposed the consensus defined as proof of equivalent work(PeW), and in NCM, we proposed proof of contribution(PoC). In PCM model, as for a given amount of transactions, the master node dispatches partial computing task(includes but not limited difficulty, timestamp, hash, and version et.al parameters) to the slave agents for distributed computing with high concurrency, when the slave agent computed and found the Nonce that satisfied the mining condition, once the result of the Nonce is verified as true for the partially computing, then the master node gives a reasonable reward to the slave agent.

And in NCM model, the master node works directly as usual, but it related a series of slave agent for service-related contribution such as providing advertisement, service flow, page view(PV), unique visitor(UV), visit view(VV), independent IP address(IP), when the master node works and gains the rewards from the whole blockchain network, then it distributes rewards to the slave agents according to their service related contribution(PoC). Finally we evaluated the MSB scheme based on Bitcoin system, large amounts of simulations manifest the proposed MSB scheme is feasible, extendible and suitable for pervasive computing, the master-slave blockchain architecture is described as in figure 2.

## IV. Security Infrastructure of MSB Blockchain Scheme

As for the blockchain technology, SHA256, SHA3, RIPEMD160 and ECC-based public cryptosystem ECDSA are the infrastructure of the security algorithms[24-28]. and the public address of most blockchain is based on BASE58. Such as in Bitcoin, the ECC algorithm in blockchain system uses secp256k1 elliptic curve which is different to the standard ECDSA[26-27].

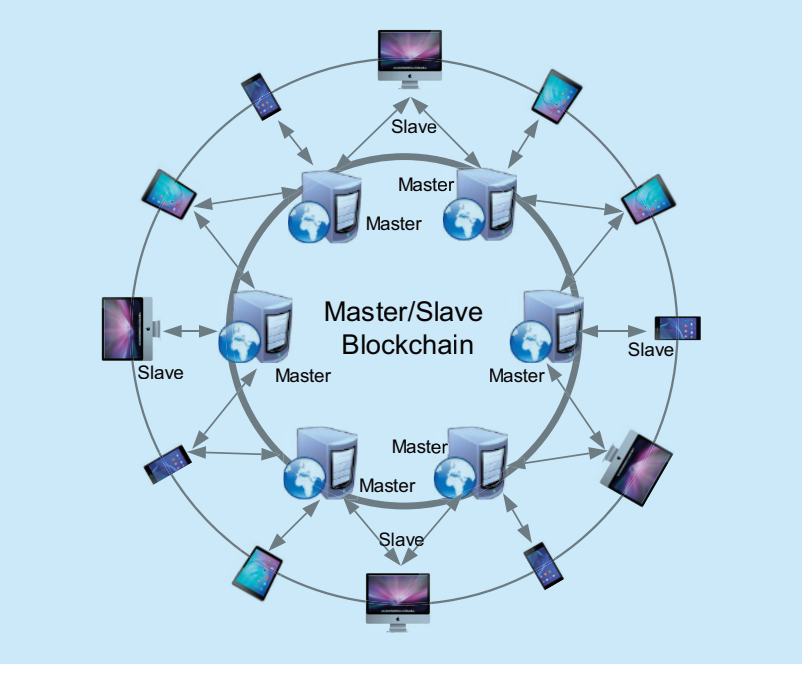


**Fig. 1.** *The master-slave blockchain model.*

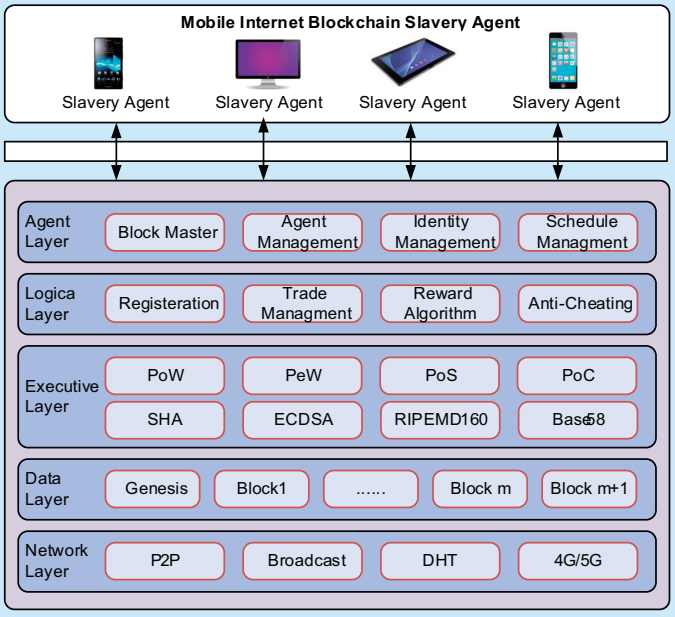


**Fig. 2.** *The master-slave blockchain architecture.*

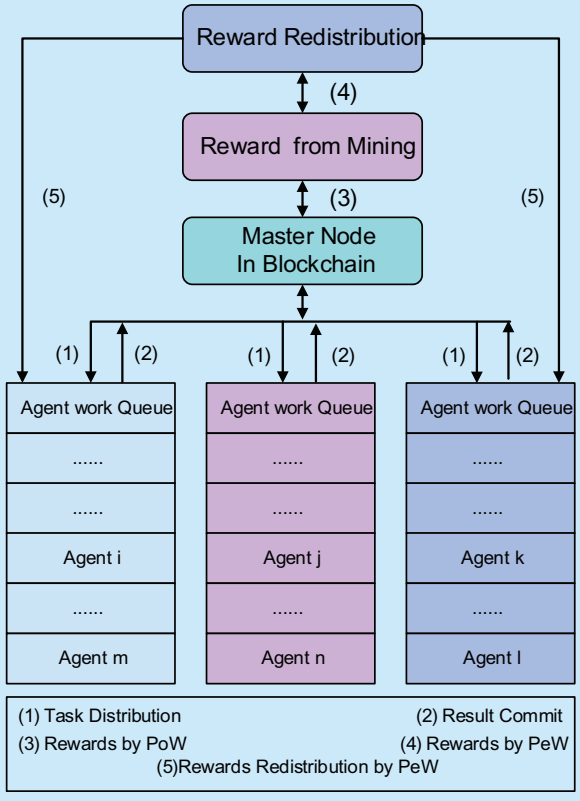


**Fig. 3.** *The master-slave blockchain execution procedure.*

## V. Master-Slave Blockchain Execution and Consensus

### 5.1 Master-slave blockchain execution process

In the PCM blockchain model we proposed the consensus defined as proof of equivalent work(PeW), and in NCM, we proposed proof of contribution(PoC). In PCM model, as for a given amount of transactions, the master node dispatches partial computing task(includes but not limited difficulty, timestamp, hash, and version et.al parameters) to the slave agents for distributed computing with high concurrency, when the slave agent computed and found the Nonce that satisfied the mining condition, once the result of the Nonce is verified as true for the partially computing, then the master node gives a reasonable reward to the slave for the computing of the slave computing work(PeW). And in NCM model, the master node works directly as usual, but it related a series of slave agent for service-related contribution such as providing advertisement, service flow, page view(PV), unique visitor(UV), visit view(VV), independent IP address(IP), when the master node works and gains the rewards from the whole blockchain network, then it distributes rewards to the slave agents according to their service related contribution(PoC). The master-slave blockchain execution process is described in figure 3.

### 5.2 New Consensus of master-slave blockchain scheme

The main consensus mechanisms[19-21] include proof of work(PoW), proof of stack(-PoS), distributed POS(DPoS) and practical Byzantine Fault Tolerance(PBFT), other consensus mechanisms include Paxos, Raf, which can satisfy different applications of blockchain scenes.

In the proposed MIB consensus, we proposed proof of equivalent work(PeW), proof of contribution(PoC):

5.2.1 Proof of Equivalent Work(PeW)

In the Proof of equivalent work consensus, the mobile internet agent computes the Nonce as partial computing unit in the slave side.

**(1) PeW Algorithm of MIB Slave User-Agent AID[i]**

**Input:** AID, $y_0$= $T_0$, blockHeader

where,

$T_0$ is the target difficulty value

blockHeader is composed as follows:

$$blockH = \{ version, prevHash, merkleRoot, timeStamp, bits, extdField \} \quad (1)$$

**Output:** Nonce

(1) the slave mobile internet UserAgent AID node computes:

$$f(x_i) = Sha256(Sha256(m(x_i))) \quad (2)$$

(2) if the condition is satisfied:

$$f(x_i) < y_0 \quad (3)$$

(3) Then AID node stops to compute, and set to $N_i$

AID set: Nonce=$x_i$

(4) AID node signs the Nonce as follows:

$$k_{SA}G = (x_{SA}, y_{SA}) \quad (4)$$

$$r_{SA} = x_{SA} \ mod \ n \quad (5)$$

$$e = h(Nonce) \quad (6)$$

That is:

Then the server B computes:

$$s_{SA} = r_{SA}k_{SA} + ed_{SA} mod \ n \quad (7)$$

$$Sig_{SA} = (r_{SA}, s_{SA}) \quad (8)$$

(5) Finally, the Slave Agent AID return Nonce and its signature $Sig_{SA}$ to master node;

(6) End.

**(2) PeW Algorithm of MSB Slave Agent AID[i]**

**Input:** AID, Nonce, blockHeader,

where,

$T_0$ is the target difficulty value

blockHeader is composed as follows:

$$blockH = \{ version, prevHash, merkleRoot, timeStamp, bits, extdField \} \quad (9)$$

$N_i$, the nonce as the goal value for mining.

**Output:** blockHeader, blockBody, $R_{success}$, $R_{unSuccess}$

(1)After received the Nonce Ni, then MIB Master Node

firstly verifies the validation of the Nonce.

$$e = h(Nonce) \quad (10)$$

$$u = r_{SA}^{-1}s, \ v = r_{SA}^{-1}e \quad (11)$$

$$X = uG - vQ = (x_1, y_1) \quad (12)$$

$$r_1 = x_1 \bmod n \quad (13)$$

If r=$r_{SA}$ it manifests the signature is true.

(2) The MIB Master Node broadcasts the block data to all candidate blocks to verify its correctness and validity. Generally, supposing that there are $M_0$ blocks participant the verifying and the verification result is true, that is :

bVeriResult[i]=Veri(Blocks([i], BlockHeader, Nonce)), i=1,2,…$M_0$

such as in Bitcoin $M_0$=6, and in Ethereum $M_0$=12

if all the bVeriResult[i] is true, i.e:

bVeriResult[i]=True, i=1,2,…$M_0$

(3)The MIB Master Node constructs and outputs:

$$blockHeader = \{ version, prevHash, merkleRoot, timeStamp, bits, nonce, extdField \} \quad (14)$$

(4) The MIB Master Node then constructs :

Blocks={ BlockHeader, BlockBody}

Where

BlockBody={$Trans_1$, $Trans_2$, …,$Tran_n$}

(5) The MIB Master Node dispatches Reward to the successfully mining or verifying Agent AID[i]:

$R_{Success}$=R[ AID[i]]

(6) To encourage those who participate the working of mining or verifying agent, the MIB Master Node still give reward to the Successfully mining AID[j](i!=j)

$R_{unSuccess}$=R(AID[j], CP[j])

CP[i]=CPF( time, freq, eff)

where(CPF means contribution Percentage Function)

t is the time the AID[j] took for the working of mining or verifying.

freq is the frequency of the AID[j] working.

eff is the efficiency value of the AID[j] working.

Then MIB Master Node gives the final rewards R as above:

(7) End.

### 5.2.2 Proof of contribution

In the non-computing of model(NCM), the master node works directly as usual, but it related a series of slave agents for service-related contribution such as providing advertisement, service flow, page view(PV), unique visitor(UV), visit view(VV), independent IP address(IP), when the master node works and gains the rewards from the whole blockchain network, then it distributes rewards to the slave agents according to their service related contribution, we defined the consensus as proof of contribution (PoC).

**(1) Definition of PoC Algorithm in the non-computing of model(NCM)**

**Definition:** Proof of Contribution(PoC) is the consensus algorithm that supports for non-computing model in master-slave blockchain environment, the reward and the consensus is defined as following the compound function f:

$$\mathrm{C(x,y)} = f(R(x), CF(y)) = R(x) \cdot CF(y) \quad (15)$$

Where R(x) and CF(y) represent the reward function and control factor function:

$$\mathrm{R}(x) = \mathrm{Comp}(\mathrm{x_{PV}}, x_{UV}, x_{VV}, x_{IP}) \quad (16)$$

$$CF(y) = CtrlFactor(\mathrm{y}_{Auto}, \mathrm{y}_{\mathrm{Re}peat}) \quad (17)$$

And the parameters in R(x) represent service flows, which include page view(PV), unique visitor(UV), visit view(VV), independent IP visiting(IP), advertisement hit(AH). Generally, the parameters often has the following relationship:

$$PV > VV > UV > IP \quad (18)$$

While the CtrlFactor(y) represents the control factor function to control invalid or deliberate cheating behavior, the PoC consensus function C(x,y) is defined as the following formula:

$$\mathrm{R}(x) = \mathrm{Comp}(\mathrm{x_{PV}}, x_{UV}, x_{VV}, x_{IP}) = (\frac{1}{2} * (\sqrt{\frac{x_{PV} \cdot x_{UV}}{\alpha^2 + x_{PV}^2 + x_{UV}^2}} + \sqrt{\frac{x_{VV} \cdot x_{IP}}{\beta^2 + x_{VV}^2 + x_{IP}^2}})) \quad (19)$$

$$CF(y) = CtrlFactor(\mathrm{y}_{Auto}, \mathrm{y}_{\mathrm{repeat}}) = \sqrt{\frac{\mathrm{y}_{Auto} \cdot \mathrm{y}_{\mathrm{repeat}}}{\gamma^2 + y_{Auto}^2 + y_{repeat}^2}} \quad (20)$$

As the parameters such as page view(PV), unique visitor(UV), visit view(VV) are natural numbers, thus the factors $\alpha, \beta, \gamma$ parameters is defined as natural number, $\alpha \geq 1, \beta \geq 1, \gamma \geq 1$, then there exists the following property of PoC:

$$\begin{aligned} &\mathrm{C(x,y)} = f(R(x), CF(y)) = R(x) \cdot CF(y) \\ &= (\frac{1}{2} * (\sqrt{\frac{x_{PV} \cdot x_{UV}}{\alpha^2 + x_{PV}^2 + x_{UV}^2}} + \sqrt{\frac{x_{VV} \cdot x_{IP}}{\beta^2 + x_{VV}^2 + x_{IP}^2}})) \cdot \\ &\sqrt{\frac{\mathrm{y}_{Auto} \cdot \mathrm{y}_{\mathrm{repeat}}}{\gamma^2 + y_{Auto}^2 + y_{repeat}^2}} \\ &\leq (\frac{1}{2} * \sqrt{\frac{x_{PV} \cdot x_{UV}}{x_{PV}^2 + x_{UV}^2}} + \sqrt{\frac{x_{VV} \cdot x_{IP}}{x_{VV}^2 + x_{IP}^2}})) \cdot \sqrt{\frac{\mathrm{y}_{Auto} \cdot \mathrm{y}_{\mathrm{repeat}}}{y_{Auto}^2 + y_{repeat}^2}} \end{aligned} \quad (21)$$

Then in the proof of contribution consensus(PoC), we can give proper reward as the above definition. And in real application system, it is reasonable and fair for different users to visit and contribute to the service-related system.

**(2) PoC Algorithm in the non-computing of model (NCM)**

**Input:** user behavior vector R(x) and R(y) to the destination objects as defined as the above definition.

**Output:** The contribution awards share C(x,y) to the user

(1) the system daemon monitors and records each client's behavior, the system counts each parameter in R(x), which includes page view(PV), unique visitor(UV), visit view(VV), independent IP visiting(IP), advertisement hit(AH).

(2) For each parameter of R(x), the system counts and calculates the summary of the specific time period(such as a day):

$$X_{PV} = \sum_{i=1}^{n} x_{pv}^{i} \quad (22),$$

$$X_{UV} = \sum_{i=1}^{n} x_{uv}^{i} \quad (23)$$

$$X_{VV} = \sum_{i=1}^{n} x_{vv}^{i} \quad (24),$$

$$X_{IP} = \sum_{i=1}^{n} x_{ip}^{i} \quad (25)$$

(3) For each parameter of R(x), the system merge the repeat parameter as one valid behavior:

$$X_{PV} = \sum_{i=1}^{n} x_{pv}^{i} - \sum_{i=1}^{m} x_{pv}^{j}(t_0) \quad j < i, m < n \quad (26)$$

$$X_{UV} = \sum_{i=1}^{n} x_{uv}^{i} - \sum_{i=1}^{k} x_{uv}^{j}(t_0), \quad j < i, k < n \quad (27)$$

In which $t_0$ is the specific time window, such as in 10 minutes the system monitored a user accessed the specific page view 100 times, which is obviously a machine behavior, then the PV counter should be NOT accepted in the system.

(4) Not only the repeat counter such as PV or VV should be viewed as invalid, and the system should punish the machinery automatic behavior as follows:

$$CF(y) = CtrlFactor(\mathrm{y}_{Auto}, \mathrm{y}_{\mathrm{repeat}}) \quad (28)$$

Where $y_{auto}$ and $y_{repeat}$ represents the the machinery page view (PV) counter and visit view( VV) counter.

(5) The system then calculates the contribution as follows:

$$R(x) = \frac{1}{2} * \left( \sqrt{\frac{\sum_{i=1}^{n} x_{pv}^{i} \cdot \sum_{i=1}^{m} x_{uv}^{i}}{\alpha^2 + (\sum_{i=1}^{n} x_{pv}^{i})^2 + (\sum_{i=1}^{m} x_{uv}^{i})^2}} + \sqrt{\frac{\sum_{i=1}^{k} x_{vv}^{i} \cdot \sum_{i=1}^{l} x_{ip}^{i}}{\beta^2 + (\sum_{i=1}^{k} x_{vv}^{i})^2 + (\sum_{i=1}^{l} x_{ip}^{i})^2}} \right) \quad (29)$$

$$CF(y) = CtrlFactor(\mathrm{y}_{Auto}, \mathrm{y}_{\mathrm{repeat}}) = \sqrt{\frac{\sum_{i=1}^{n} \mathrm{y}_{auto}^{i} \cdot \sum_{i=1}^{m} \mathrm{y}_{repeat}^{i}}{\gamma^2 + (\sum_{i=1}^{n} \mathrm{y}_{auto}^{i})^2 + (\sum_{i=1}^{m} \mathrm{y}_{repeat}^{i})^2}} \quad (30)$$

In the above R(x), the parameters $x_{pv}$ and $x_{uv}$ is the valid counter that had be dealt without machinery automatic behavior.

(6) Then the final reward contribution is computed as:

$$\mathrm{C(x,y)} = f(R(x), CF(y)) = R(x) \cdot CF(y) \quad (31)$$

(7) Finally, the system returns the C(x, y) as the final contribution reward for the proof of contribution(PoC).

## 5.3 Blockchain management and reconstruction

When the master-slave blockchain procedure is verified as valid, then when constructing the correct block in the whole blockchain system, the blockchain management includes for 4 stage operations: (1) download blockchain data;(2) receive blockchain data;(3) verify the blockchain data; (4)reconstruct bllockchain.

### 5.3.1 Whole blockchain data downloading

When the node first runs the blockchain network, it need to download the whole blockchain data. The efficient stratagem of the blockchain download is header first, that is the system firstly download the block header(only 80bytes), when download all the blockheader, then the system can download the whole blockdata from different peers in P2P network.

### 5.3.2 Blockchain receiving

After downloaded the blockchain data from peers, then the current node will load the whole index from LevelDB,which may be a tree rather than a single chain, that is each block has only one parent block, but has more than one sub-blocks.

### 5.3.3 Blockchain verification

Once the node first runs the blockchain network, it need to download the whole blockchain data. The efficient stratagem of the blockchain download is header first, that is the system firstly download the block header(only 80bytes), when download all the blockheader, then the system can download the whole blockdata from different peers in P2P network.

As well known, the blockchain data structure of the block data is listed as follows:

BlockData= (BlockHeader| BlockBody)

where the

BlockHeadr=[ Height, Timestamp, Difficulty, Bits,

Version,Nonce, CurrentBlockHash,

PreviousBlockHash, MerkleRoot ]

BlockBody = [UnlockingScript, LockingScript]

1） Then the peer firstly verify the data in-

tegrity and the correctness of data format.

2) The blockchain peer transfers the blockdata to the receiver and signs the block as follows:

$$k_p G = (x_p, y_p) \tag{32}$$

$$r_p = x_p \ mod \ n \tag{33}$$

$$e = h(blockData) \tag{34}$$

And then the peer computes:

$$s_p = r_p k_p + ed_p mod \ n \tag{35}$$

$$Sig_p = (r_p, s_p) \tag{36}$$

Thus $Sig_p = (r_p, s_p)$ is the signature from the peer p.

3) each other peer received the blockdata, and can verify the correctness as follows:

$$e = h(BlockData) \tag{37}$$

$$u = r_p^{-1} s_p, \ \ v = r_p^{-1} e \tag{38}$$

$$X = uG - vQ = (x, y) \tag{39}$$

The signature is valid if and only if the following formula exists:

$$r_p = x \bmod n \tag{40}$$

In fact, it's easily to verify that the signature is valid in and only if the following equation is correct:

$$\begin{aligned} X &= uG - vQ \\ &= uG - vd_p G \\ &= r_p^{-1} s_p G - r_p^{-1} ed_p G \\ &= (r_p^{-1}(r_p k_p + ed_p) - r_p^{-1} ed_p) G \\ &= r_p^{-1} r_p k_p + r_p^{-1} ed_p - r_p^{-1} ed_p) G \\ &= k_p G \\ &= (x_p, y_p) \end{aligned} \tag{41}$$

Then there must exist:

$$r_p = x \bmod n \tag{42}$$

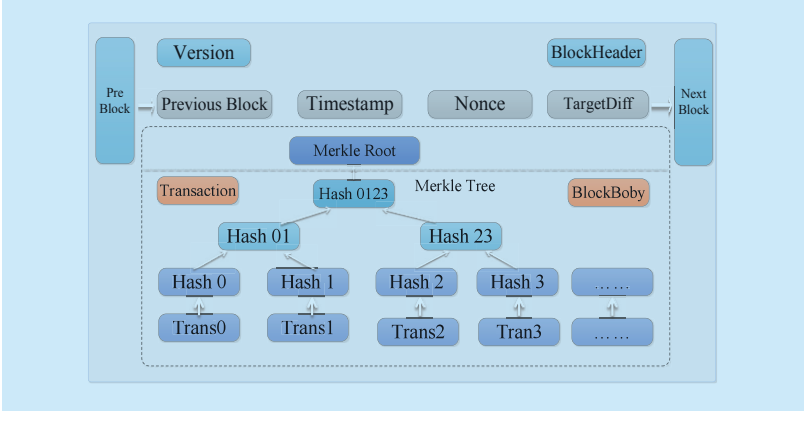


**Fig. 5.** *The Blockchain block and transaction data structure.*

Thus its manifests the peer verifies the signature of the blockdata as true, then the blockchain management system then check the transcation is a UTXO or not.

#### 5.3.4 Blockchain reconstruction

When the peer finds a longer chain than current exist chain, it needs to reconstruct the blockchain, most reconstruction is just for one block data reconstruction, only occurs when different miners computes the same valid block.

### 5.4 Block and transaction data construction

After pass the verification, the blockchain platform then build Up the blocks and transactions in time-order with tamper-resistance and security, the block data and transaction data is constructed and included block header and block body. The blockchain will permanently stores the data in the P2P network and cannot allow it be modified or deleted in a tamper-resistance mode, which can provide strong and high level reliability and security. Even some blockchain nodes deliberately announced or the nodes truly corrupted, the most other nodes can provide strong and trusted service for evidences. The block and transaction data structure are defined as bellows which is easy to convert to JSON format. The blocks and transaction data are organized in figure 5 and figure 6.

In the master-slave blockchain mode, the slave agent only acts as the light-weight client of computing nodes, which computes and finds the proper nonce that satisfy the condition, thus gets the rewards according to the consensus methods such as proof of equivalent work or proof of indirect contribution.

## VI. Evaluation of Master-Slave Blockchain Scheme

### 6.1 Evaluation environment of master-slave scheme

To evaluate the availability and efficiency, we

built up the master-slave blockchain simulation environment based on Bitcoin v0.10.99.0-unk, in which we simulated the task redistribution thread and receiver thread from slave agents, and when the slave agents received the computing task(including mining computing and verification computing), then do the computing work according to the related computing parameters. The master-slave blockchain simulation environment is listed as table1.

We deployed 4 master nodes and each nodes serves 3 slave agents include general personal computer, android mobile phones and Pads for task receiving and computing and verification.

## 6.2 Experiments of master-slave blockchian scheme

In the deployed 4 bitcoin blockchain system, the master-slave bitcoin platform, we used variant kinds of PCs. Android mobile phones or Pads joined into to 4 master nodes, and then evaluated the performance and scalability of the master-slave blockchain scheme. The simulation of master-slave blockchain parameters are listed in table 2-3, algorithm 1 is the genesis initialization in CMainParams function, algorithm 2 is the blockchain data created from genesis block.

## 6.3 Simulation results of master-slave scheme

Figures 7-9 are the simulation results of the master-slave blokchain computing model. Figure 7-8 are the PeW consensus simulations in one master node and 3 slave nodes computing performance comparison, and figure 9 are the simulation results of PoC, in which α,β,γ were parameterized as 1, 2,3, to simply the whole computing complexity, in the serial data set S1, α,β,γ are parameterized as α=β=γ=1, and in serial data S2, α=β=γ=2, finally, in S3, α=β=γ=3. The results showed reasonable reward rate for variant contribution in PoC.

## 6.4 Simulation analysis of master-slave scheme

The simulation results of figure 7 and figure

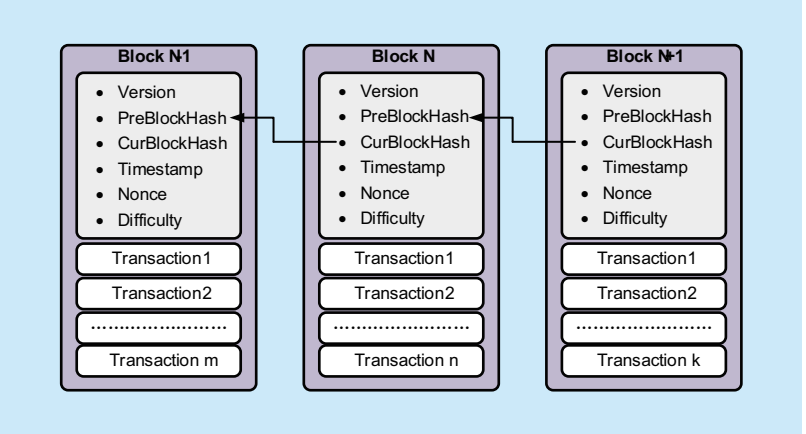


**Fig. 6.** *The general data structure of blockchain(Bitcoin).*

**Table I.** *Development environment parameters.*

| | | | |
|---|---|---|---|
| OS | Ubuntu16.04.2 X64 Server | Hardware | 8GB RAM 500GBdisk |
| RAM | 16 GB | CPU | Intel i7-8550U |
| Blockchain | Bitcoin v0.10.99.0 -unk | Develop Tool | C++ Python visual studio MinGW |
| DB | LevelDB | Nodes Amount | 4 |
| Digital Signature | ECDSA | HASH | SHA256 |
| Master Port | 10366 | Slave Port | 10365 |

**Table II.** *The network parameters of master nodes.*

| IP address | User Agent | response time(ms) |
|---|---|---|
| 118.190.152.48:9996 | /DRMNode:0.10.99 | 199 |
| 120.79.178.156:9996 | /DRMNode:0.10.99 | 169 |
| 120.79.154.159:9996 | /DRMNode:0.10.99 | 98 |
| 47.96.191.144:9996 | /DRMNode:0.10.99 | 101 |

**Table III.** *The peer node network status in master-slave platform.*

| | |
|---|---|
| Direction | Out |
| Version | 70002 |
| User agent | /DRMCoinNode:0.10.99/ |
| Service | Network |
| Height | 22293 |
| Synchronization height | 22297 |
| Forbidden score | 0 |
| Connection time | 16min 43sec |
| Last send time | 33 sec |
| Last receive | 33 sec |
| Send bytes | 2 KB |
| Receive bytes | 1 KB |
| Ping time | 217 ms |
| Time setoff | 8 sec |

**Algorithm 1.** The genesis initialization in CMainParams function.

```
//the genesis initialization in CMainParams funcitotn
    CMainParams() {
    strNetworkID = "DRMNetwork";
    ……..
    nDefaultPort = 9696;
    bnProofOfWorkLimit = ~arith_uint256(0) >> 8;
    nSubsidyHalvingInterval = 210000;
    nEnforceBlockUpgradeMajority = 750;
    nRejectBlockOutdatedMajority = 950;
    nToCheckBlockUpgradeMajority = 1000;
    nMinerThreads = 1; // 0 for all available cpus.
    nTargetTimespan = 60 * 60; // re-targeting every one hour
    nTargetSpacing = 5 * 60; // do new pow every 1minutes.
    nGenesisSubsidy = 1000;
    const char* pszTimestamp = "The DRM Blockchain is
    Created for Digital Rights Management. By Dr.
    Ma Zhaofeng, CPSec Research Team, BUPT,Jan 6,2018.";
    ……...
    genesis.vtx.push_back(txNew);
    genesis.hashPrevBlock.SetNull();
    genesis.hashMerkleRoot = genesis.BuildMerkleTree();
    genesis.nVersion = 1;
    genesis.nTime = 1517899981;
    genesis.nBits = 0x1e00ffff;
    genesis.nNonce = 20178638;
    ……
}
```

**Algorithm 2.** The blockchain information created from genesis block.

```
{// getblock by hash string
    "hash" : "0000048cb46e865c1dd6d88d2564c6926383482a70
    d18874b8ed770f866c1797",
    "confirmations" : 1927,
    "size" : 188,
    "height" : 18443,
    "version" : 2,
    "merkleroot":
        "b00c9bb237485531370a68b5f4af5291efd2a
        53041398d91ad374940f76db70a",
    "tx":
        ["b00c9bb237485531370a68b5f4af5291efd2a53041398d91ad
        374940f76db70a"
        ],
    "time" : 1517976539,
    "nonce" : 183708,
    "bits" : "1e062e8c",
    "difficulty" : 0.00063188,
    "chainwork":
        "0000000000000000000000000000000000000000000000000000
        46876c4ee8b",
    "previousblockhash":
        "00000620a91328ef5e683c8bfffe6730e890ea5a41b6cf20
        e85ed4a880a7a2a9",
    "nextblockhash":
        "00000103ef5d721efc1808569e4753d43d2d28683e00394
        f78ec5f393509d089"
}
```

8 reflex the master and slave node(s) computing resource occupation(CPU), of which the mobile phone's CPU occupation is 25.17-28.21%, and the average value is 26.36%, and the pad CPU usage rate is 22.18-24.93%, and average percentage is 23.36%, while the PC slave node's occupation is 18.21-20.03%, and the average rate is 19.05%, based on which we can found that with the hardware computing performance decreasing, the master node need much more computing CPU for the collection and waiting for the slave nodes to commit the computing and verification results.

While in PoC, it is easily found, that with the parameters $\alpha,\beta,\gamma$ increasing, the average reward rate declined from 41.53%, 40.11%, to 38.85%, this indicated that if we want to give the salve node a less reward we can parameterized $\alpha,\beta,\gamma$ to a large value, thus the reward rate can be reduced to a reasonable level.

## VII. Analysis of Master-Slave Blockchain Scheme

### 7. 1 Availability of master-slave blockchain

The DRMChain Scheme provides a flexible DRM approach that enables user-controlled encryption but administrator and auditor can decrypt and audit the content once the released content is suspected violation or illegal usage, in the scheme, we proposed 3 parts control model trusted and creditable content encryption, secure key management, multi-signature for violation appraisal.

### 7.2 Consensus of master-slave blockchain

The proposed master-slave blockchain scheme allows variant computing device such as personal computer, mobile phones, or Pads can join into the blockchain computing and get reasonable rewards according to their work or contribution, the proposed proof-of-equivalent (PeW), and the proof-of-indirect-contribution(PIC) innovated the existing consensus of blockchain, and are effective and efficient

mechanism that can attract more persons joint into the blockchain system without large capacity ledger data synchronization.

### 7.3 Extendibility of master-slave blockchain

With the proper connection mode such as the mining pool for cluster computing in Bitcoin, the master-slave blockchain scheme innovates the blockchain paradigm that develops the heavy-weight blockchain to light-weight layered computing mode, which can dispatch different work to slave agents for discrete time usage of mining task balance or indirect contribution for blockchain useful utilization without synchronize blockchain data synchronization.

## VIII. The Master-Slave Blockchain Application in DRM

Digital content service is mainly occupying the bandwidth rather than the computing resource, upon which the proposed master-slave paradigm is very suitable for digital right management of content service. The proposed PeW and PoC consensus is a reasonable method for DRM-related applications[19-22].

### 8.1 Scene of the PeW in DRM system

In the DRM service[19-20], when the user client daemon is idle or free time, the PeW consensus can be implemented in a master-slave mode to allow computing resource limitation device such as phones or Pads join in the partial computing work as slave, and the full-computing node organizes the valid computing piece as master, which can speed up the full-computing node for the mining work. With 5G network bandwidth and computing ability development, it's a good and promise direction for PeW application in mobile Internet computing times. In the DRM servie, when the client daemon is free or idle, the PeW is efficient and secure for master-slave blockchain paradigm[20].

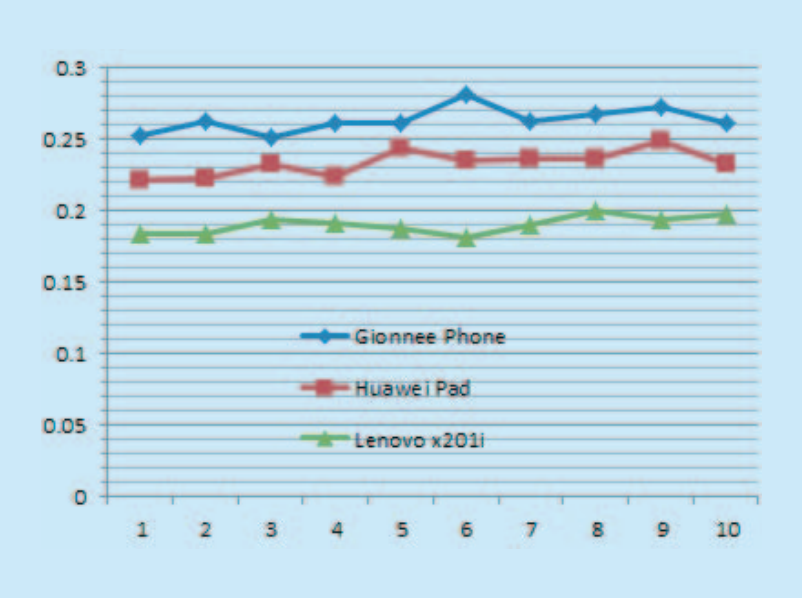


**Fig. 7.** *The simulation of CPU usage of the master node in PeW.*

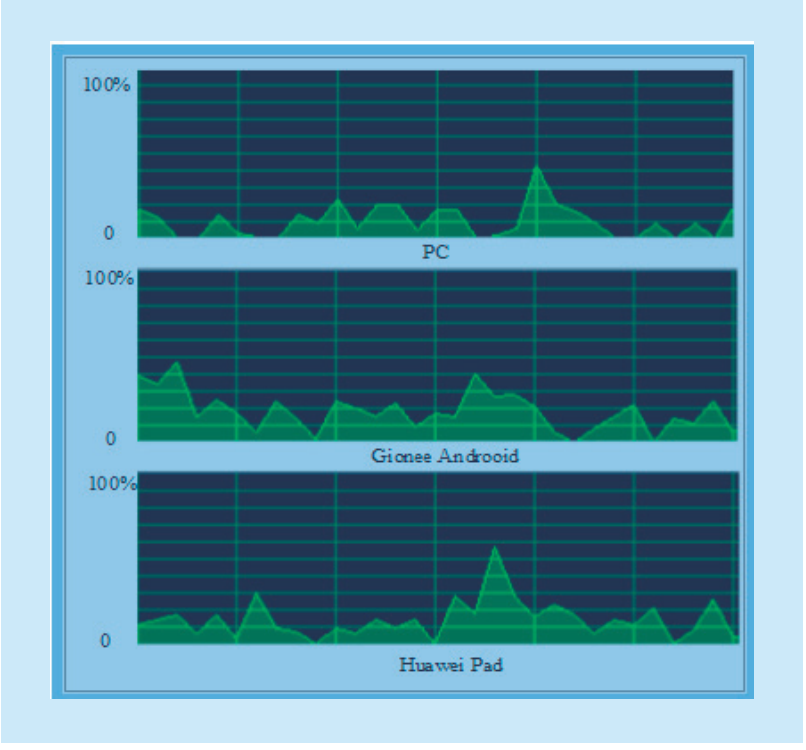


**Fig. 8.** *The simulation of CPU usage of variant slave nodes in PeW.*

### 8.2 Scene of the PoC for DRM-based content view

As for the proposed blockchain paradigm, the proof of contribution(PoC) is suitable for user to visit or consume the content, once the user

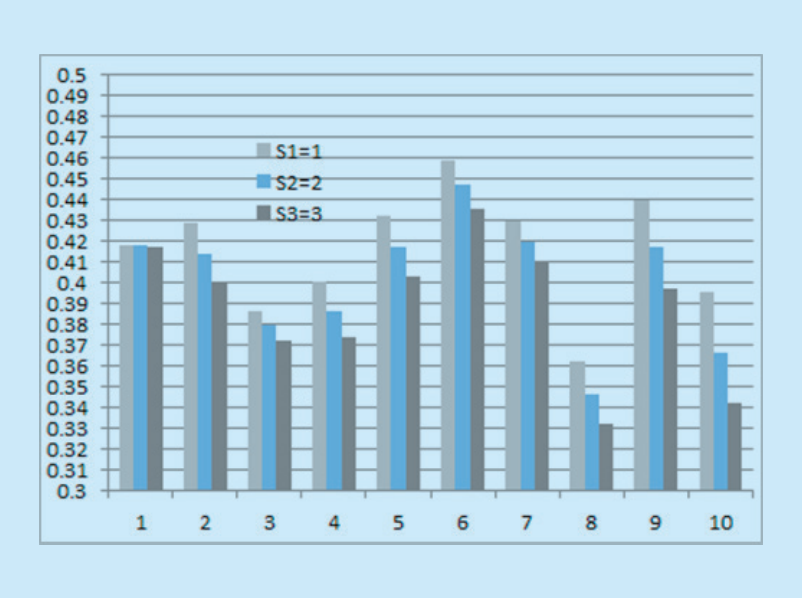


**Fig. 9.** *The simulation of awards percentage in PoC.*

visit, preview, play, or share the content, the user should be encouraged, and should give the reward according to the user's PV, UV,VV, or IP, and the valid sharing and the shared user's valid consumption, the content service provider then gives the user an active blockchain-based digital currency reward, and the user can query the reward transaction in his/her account, which is very useful for sharing economy. Especially when using DRM[21-22] and blockchain technology for content service, it is easily implemented a blockchain-based new DRM content service, that the right content serves the right user in a right way with a right reward. The users can consume the content by digital currency, which either is he/she bought independently, or is granted as a reward by his/her contribution of consumption or sharing, thus PoC consensus is a classic application for DRM-based content service scene.

## IX. Conclusion

The most useful contribution of the paper is that we proposed a new paradigm of master-slave blockchain scheme (MSB) for pervasive computing that suitable for general PC, mobile device such as smart phones or PADs to participants in the working of mining and verification, in which we separated traditional blockchain model in 2 layers defined as master node layer and a series of slave agents layer, and we proposed 2 approaches for partially computing model(PCM) and non-computing of model(NCM) in the MSB blockchain. Finally we evaluated the MSB architecture based on Bitcoin system, large amounts of simulations manifest the proposed MSB scheme is feasible, extendible and suitable for pervasive computing. The proposed PeW and PoC consensus is a reasonable method for DRM-related applications, and as the permanent research topic, performance and TPS enhance is the most important issues to be studied in the future work.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61272519, the Research Funds of Blockchain Joint Lab between BUPT and BCT, and the joint Blockchain and Security Lab between BUPT and CAPSTONE.

## References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] *The Bitcoin Project*. [Online]. Available: https://bitcoin.org

[3] *The Ethereum Project*. [Online]. Available: https://www.ethereum.org.

[4] *The Hyperledger Project*. [Online]. Available: http://www.hyperledger.org.

[5] M Swan. "Blockchain: Blueprint for a New Economy", O'Reilly Media, Inc., 2015.

[6] M Pilkington. "Blockchain Technology: Principles and Applications", *Social Science Electronic Publishing*, 2016.

[7] LW Cong, Z He. "Blockchain Disruption and Smart Contracts", *Social Science Electronic Publishing*, 2017.

[8] G Zyskind, O Nathan, Alex. "Decentralizing Privacy: Using Blockchain to Protect Personal Data", *IEEE Security & Privacy Workshops*, pp 180-184, 2015.

[9] Danny Bradbury. "The problem with bitcoin". *Computer Fraud & Security*, vol. 2013, no.11, pp 5-8,2013.

[10] Akif Khan. "Bitcoin payment method or fraud

prevention tool", *Computer Fraud & Security*, vol.2015, no.5, pp 16-19,2015.
[11] A. E. Kosba, A. J. Miller, E. Shi, Z. Wen, and C. Papamanthou. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *IEEE symposium on security and privacy,* pp 839-858, 2016.
[12] M. Vukolić. "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," *International Workshop on Open Problems in Network Security*, pp. 112-125, 2015.
[13] A. Dorri, M. Steger, S.S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communications Magazine,* vol.55, no.12, pp 119–125, 2017.
[14] Luoyi Fu, Xinyu Wu, Zhongzhao Hu, Xinzhe Fu, Xinbing Wang, "De-anonymizing Social Networks with Overlapping Community Structure", *IEEE International Conference on Computer Communication (INFOCOM),* Honolulu, USA, Apr. 15th-19th, 2018.
[15] Sarah Underwood. "Blockchain Beyond Bitcoin", *Communicatoin*, ACM, vol.59, no.11, pp 15–17,2016.
[16] L Luu, V Narayanan, C Zheng, et. al.. "A Secure Sharding Protocol For Open Blockchains", *ACM SIGSAC Conference on Computer & Communication*, pp 17-30, 2016.
[17] Tyler Moore. "The promise and perils of digital currencies", *International Journal of Critical Infrastructure Protection*, vol.6, no.34, pp 147-149, 2013.
[18] EOS, "The most powerful infrastructure for decentralized applications", https://eos.io.
[19] Ian Kerr, Jane Bailey, "The implications of digital rights management for privacy and freedom of expression", *Social Science Electronic Publishing*, vol.2, no.2, pp 85-95, 2005.
[20] Danny Bradbury,"Decoding digital rights management", *Computers & Security*, vol.26, no.1,pp 31-33, 2007.
[21] Ma Zhaofeng,"Digital Rights Management:-Model, Technology and Application", *China Communications*, Vol. 14 (6): 156-167, 2017.
[22] Liu Yanbing, Lu Xingyu, Jian Yi, xiao Yunpeng, "SDSA: A Framework of a Software-Defined Security Architecture", *China Communications*, Vol.13,No.2,pp.178-188,2016.
[23] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.
[24] V. S. Miller, "Use of Elliptic Curve in Cryptography", *Advances in Cryptology-CRYPTO'85, Lecture Notes in Computer Science,* vol. 218, pp. 417-426, 1986.
[25] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.
[26] ANSI X9.62. Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).1999.
[27] *IEEE P1363. Standard Specifications for Public-Key Cryptography. IEEE. Standard P1363,* 2000.
[28] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C, Second edition, John Wiley & Sons, Inc. 1995

## Biographies

***Zhaofeng Ma,*** Ph.D Degree, He engages in science research and education work in School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include blockchain, mobile Internet innovation and security, digital rights management. Email: mzf@bupt.edu.cn

***Weihua Huang,*** is the CTO of Shenzhen Datong Industrial Co..Ltd, Shenzhen, China He engages in science research and development work in information system development and innovations, now he is the leader as the CAPSTONE for blockchain research and development based consortium blockchain. Email: hwhmail@163.com

***Wei Bi,*** Ph.D Degree,Wei has a PhD degree in Vision Science from City, University of London and a Master degree in Computing from the University of Oxford. He is the chief scientist of SeeleTech corporation and Zsbatech corporation and the deputy secretary general of China Blockchain Technology Innovation and Application Alliance. Email: wei.bi@alumni-oxford.com

***Hongmin Gao,*** is a Ph.D candidate in School of Cyber Security, Beijing University of Posts and Telecommunications. His research interests include blockchain, applied cryptography and digital rights management. He finished the blockchain platform of BUPT-BCT Joint Lab. Email: gaohm@bupt.edu.cn

***Zhen Wang,*** is a Ph.D candidate in School of Cyber Security, Beijing University of Posts and Telecommunications. His research interests include blockchain, mobile Internet security and digital rights management. He participated and finished the blockchain platform of BUPT-BCT Joint LAB, and mobile interenet security projects of BUPT. Email: wangzhen@bupt.edu.cn