2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)
Bari, Italy. October 6-9, 2019

A Blockchain-based Random Number Generation Algorithm and the Application in Blockchain Games

Mingxiao Du, Qijun Chen, Lietong Liu, Xiaofeng Ma

Abstract—**Blockchain technology has developed rapidly and has been applied in various areas. Blockchain technology has the features of decentralization, transparency, autonomy and tamper resistance etc. The blockchain, with its unique features, can address some problems in traditional areas. In traditional games area, especially the gambling game, we learn that there is a strong requirement for fairness and random numbers. But traditional games are centralized and cannot meet this requirement. Hence, we propose a blockchain-based random number generation algorithm that can provide a "true random number". This algorithm allows all the participants to take part in the generation of a random number, which ensures that the random number will not be manipulated by anyone. We as well design a blockchain game platform adopting this random number generation algorithm. Traditional games can be deployed on this platform with a simple adaptation. Finally, we deploy a poker game on the platform to verify the algorithm and performance. The experimental results show that the algorithm is effective and the platform has good performance.**

I. Introduction

The blockchain is born as the underlying technology of Bitcoin. Blockchain, as a new distributed infrastructure and computing paradigm, uses the encrypted chain-block structure to store data and uses consensus algorithms to generate blocks. Some blockchains contain smart contracts for developing blockchain-based applications. The blockchain can realize peer-to-peer transaction, coordination and collaboration based on decentralized credit, which effectively solves the problem of reliable value trading on the Internet. The blockchain has the characteristics of decentralization, transparency, autonomy, and tamper resistance.

In recent years, with the rapid development, blockchain technology has quickly attracted the attention of researchers, governments, financial institutions and technology companies. The blockchain has become a hot topic among governments and enterprises around the world. The blockchain is a so-called revolutionary technical framework [1]. Many researchers gradually focus on researching blockchain applications. Blockchain has been applied in the Internet of Things [2-4], transportation services [5, 6], energy Internet [7, 8], medical data storage [9], and supply chain finance [10, 11]. For example, Guo et al. proposed that the blockchain is expected to radically change the payment method and the bank's credit system, and improve the efficiency of banking business [12]. Zyskind et al. described a decentralized personal data management system that uses a blockchain as an automated access control manager [13].

Blockchain games currently occupy a large proportion of the blockchain applications. Blockchain games can be divided into two categories, one is a completely decentralized "on-chain game". CryptoKitties, which was unveiled at Ethereum in November 2017, is the originator of these games [14]. These games do not rely on the game provider, all the processes are completed through smart contracts on the blockchain. However, these games have some disadvantages compared with traditional games, such as simple game rules, poor interactivity, and a relatively short life cycle. Moreover, such games are limited by the performance of the blockchain, and the transaction cost of this game is high.

The other type of blockchain game is to execute part of the traditional game process with the smart contract and record some important game data on the blockchain. The players' accounts are associated with the blockchain accounts (or addresses) and the players own the assets which are recorded on the blockchain accounts (addresses). This process can prevent centralized game providers from tampering with the players' data. In addition, it also provides transparency and convenience for the circulation of game assets. Overall, the current blockchain game is in its infancy stage.

In the field of gambling and lottery games, online gaming platforms are destined to have low transparency because they are centralized. In the gambling and lottery games, "luck" explains a large portion of a victory. However, the game providers could directly manipulate the player's "luck" by cheating, which is unsupervised. Some researchers have tried to solve the fairness problem with blockchain. For example, Liao et al. designed a blockchain-based lottery system to protect the lottery number's fairness [15], and Marcin et al. constructed protocols for secure multiparty lotteries using the Bitcoin [16]. The other blockchain gambling games, like Fomo3D on Ethereum, are entirely based on smart contracts [17]. These games are relatively simple, and there is still the possibility that the game providers could cheat by exploiting the loopholes in the contract or attaching the blockchain.

The traditional gambling game usually just record some important game data on the blockchain. But this solution can only solve the problem of data tampering, and cannot prevent the game provider from cheating in the game process. Players have to choose the game providers who have a good reputation and believe that the game providers can remain fair in the game.

Mingxiao Du, Qijun Chen, Lietong Liu and Xiaofeng Ma are with the Department of Control Science and Engineering, Tongji University, Shanghai, China (e-mail: dumingxiao@hotmail.com).

978-1-7281-4569-3/19/$31.00 ©2019 IEEE

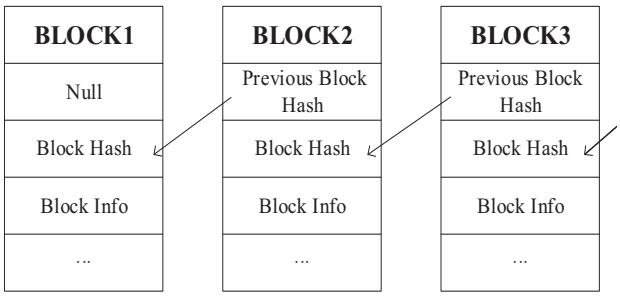

Fig. 1 data structure of the blockchain

To address the problem of the game providers' manipulation of data, we designed a blockchain-based random number generation algorithm to prevent human manipulation. This algorithm allows all the participants to be involved in the generation of a random number, which ensures that the random number could not be manipulated by anyone. Additionally, we as well proposed a blockchain game platform solution based on this algorithm for transferring tradition games to the blockchain. The platform uses a consortium blockchain and makes it possible that classical gambling games could be deployed in this platform with a simple adaptation. With the true random number and recording the game process on the blockchain, the fairness and transparency of the games in the platform are truly guaranteed.

The remainder of this paper is organized as follows. In Section II we introduce the blockchain's structure and features. In Section III, we propose the blockchain-based random number generation algorithm. In Section IV we describe the blockchain game platform and deploy a poker game on the platform to verify the algorithm and performance. In Section V we conclude the paper with some future research directions.

II. BLOCKCHAIN

A. Structure and classification

The blockchain's data structure is mainly composed of transactions and blocks. A transaction is the smallest operating unit in the blockchain. The block generally includes information such as version number, previous block hash, transaction hash, etc. Each block can contain several transactions. From the data structure, the record of blockchain is a linear chain. The chain can only add content at the end, and it is not allowed to delete or modify the previous content in the chain. As shown in Fig. 1, the linked chain is composed of sequence blocks. Each block contains a hash of the previous block, which forms a chain relationship [18]. Depending on the participants and openness, blockchains can be divided into the public blockchain, private blockchain and consortium blockchain [19].

Bitcoin, Ethereum and Hyperledger Fabric are the most popular blockchains. Bitcoin and Ethereum are public blockchains, whereas Hyperledger Fabric is a consortium blockchain [20]. Smart contracts came from Ethereum and make blockchains useful for any applications. A smart contract is a program that can automatically perform, and nodes can manipulate blockchain by this smart contract.

B. Features of the blockchain

Decentralization: Decentralization is the most basic feature of the blockchain. Blockchain applications can record, storage and update of data without relying on centralized organizations. The nodes in the blockchain network have equal rights and obligations. The nodes in the whole blockchain network jointly record the data. Blockchains have the characteristics of redundant backup, and the behavior of a single node cannot cause a system crash.

Transparency: Transactions in blockchains are open and transparent. Any operation that changes data records is transparent to the whole network. The source code of blockchains are often open and cannot be tampered with. Blockchains' records and operating rules can be reviewed and tracked. Transparency is the basis of the blockchain.

Tamper-resistance: There are two cryptographic mechanisms in blockchains to prevent tampering with records. The first is to use Merkel Tree (Merkel Tree) to index transaction records. When the original transaction is changed, the root hash value of Merkel tree will change. The second is to record the hash value of the previous block when creating new blocks. If anyone wants to change the transaction in a block, he or she must reconstruct the transaction records and hash values of all the blocks behind this block.

III. RANDOM NUMBER GENERATION ALGORITHM

A. Problems of tradition games

centralization: The traditional online gambling uses a centralized system, while the mobile app or website serves as a user interface to connect players with the back-end. Players can only passively participate in a game and accept the game rules and data. The game providers control the whole processes. In this mode, the players have to default that the providers of the game are trustful. The players must choose to accept passively otherwise leave the game.

Low transparency: The centralization interest of traditional gambling platforms leads to low transparency. Taking poker games as an example, players do not know which algorithms are used to determine the cards and whether game providers modify the data during the game. The fairness of the game is questionable. In addition, as long as the benefits are attractive enough, game providers can tamper with a game easily. The players have no tool available to supervise the game's process.

Security: Game providers are vulnerable to external attacks and the providers' availability and security are questionable. To reduce costs, the data storage and execution of the game are concentrated on a limited number of servers. Players' game data such as coins, points, items, etc. are stored on these servers. If the hackers control these servers, they can modify the game data and control the game results. This will trigger devastating disasters to the system.

B. Algorithm

In this paper, we design an algorithm to generate random numbers. All participants, game providers, and blockchains are involved in the execution of the algorithm. First, the game provider generates a random number and records the encrypted random number on the blockchain, ensuring that the game provider cannot manipulate the result of the final

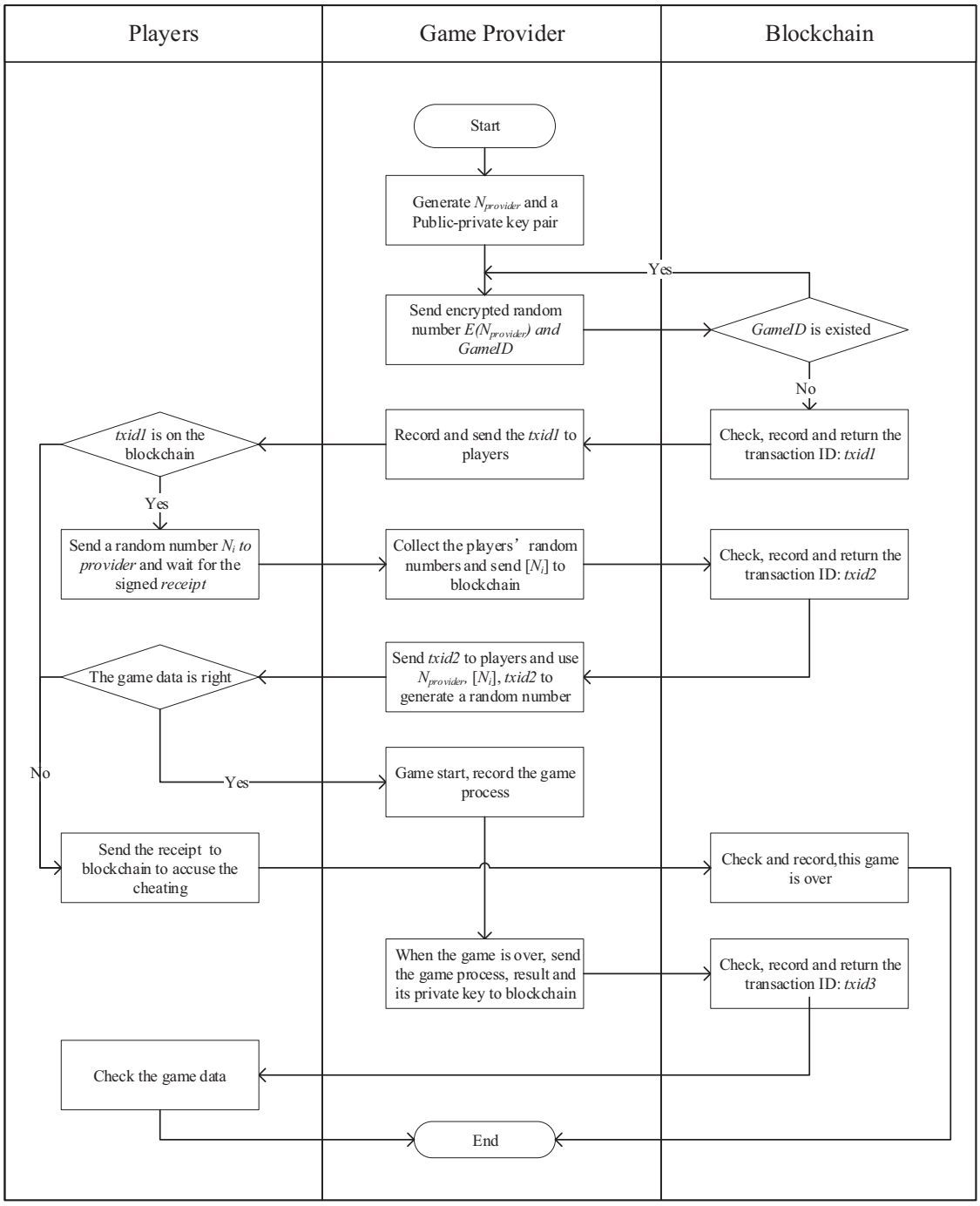

Fig. 2 process of the random number generation algorithm

random number. The players then generate their own random numbers and send them to the game provider after verification on the blockchain. The provider generates a random number according to a pre-announced algorithm by using the players' random numbers, the chain random number and its own random number. Then the game provider can use this random number to start a game.

When the game is over, the game provider must announce its random number and the private key. The players can use the game provider's private key to decrypt to determine whether the random number is correct, and finally, verify whether there is cheating in the game. Fig. 2 illustrates the process of this algorithm. The detailed steps of the random number generation algorithm are as follows:

1) The game provider generates a random number and a public-private key pair for a new game. Then the game provider encrypts this random number with the newly generated public key and sends ***message***$\{E(N_{provider}) || GameID\}$ to the blockchain. In this message, *GameID* is the new game's number.

2) The blockchain smart contract checks the *GameID*. If it's a new game, the message will be recorded on the blockchain in the form of a ***record*** *{txid1 ||E($N_{provider}$) ||GameID}*. And then return this transaction's number(*txid1*) to the game provider.

3) The game provider sends the *txid1* to all the players. The players can use the *txid1* to check the game info on the blockchain. If the game information is correct, the player *i* need to send her/his own random number to the game provider with a signed message ***random*** *{GameID ||N_i}*. Here the random number is sent to the game provider instead of the blockchain because the transaction speed of the blockchain is the bottleneck of the whole system. We try to minimize direct communications with the blockchain. Sending random numbers to the game provider is also sufficient to ensure the security of the algorithm.) The game provider replies player *i* with a signed message ***receipt***{***random***} The game provider collects all the players' random numbers and sends the message {*E($N_{provider}$) ||GameID ||*[N_i]} to the blockchain. [N_i] is the collection of these random numbers.

4) The smart contract checks the message. Then it generates a new ***record*** *{txid2 ||txid1 ||E($N_{provider}$) ||GameID ||*[N_i]*}* and return *txid2* to the game provider.

5) The game provider broadcasts the txid2 to the players. If any player's random number is tampered with, he or she can refuse to start the game and send the **receipt**{**random**} to the blockchain to accuse the cheating. If all the players agree with this txid2, the game can start. The game provider uses the random number $block_{txid2}$ *hash, txid2,* $N_{provider}$, and [N_i] as the inputs of function *f(x)* and gets a number k as output. The function *f(x)* could be an arbitrary predetermined function such as bitwise XOR operation. In the algorithm, we use $block_{txid2}$ *hash*, and *txid2* as inputs to prevent collusion between the game provider and any player.

6) Then the game provider can use *k* as a random number and start the game following the game rule. When the game ends, the game provider uploads the record and the result.

7) The smart contract generates a new *transaction {txid3 ||txid2 ||txid1 ||E($N_{provider}$) ||GameID ||*[N_i] *||Result ||Operation ||Private* $Key_{provider}$*}*. The game provider must declare the private key and *txid3* to the players.

IV. Blockchain Game Platform

A. Structure

We use a consortium chain as the underlying chain of the platform and redesign the consensus algorithm by using sharding. The consensus mechanism is designed to ensure the accuracy and consistency of stored information. The choice of consensus mainly determined by business requirements. The platform mainly serves the game field and requires high decentralization, low verification delay and high fault tolerance. In response to these needs, we design a mixed Byzantine fault tolerance (MBFT) consensus algorithm for the platform by using sharding technology. Fig. 3 shows a example structure of MBFT. MBFT can add new consensus groups with a random election mechanism to help process transactions when the number of transactions increases. The consensus groups process different transactions and smart contracts separately. Then the high-level consensus group verifies the verified transactions packages (mini-block) submitted by low-level consensus groups and generate the new block. The entire network has high scalability. We will introduce this algorithm in detail in future papers.

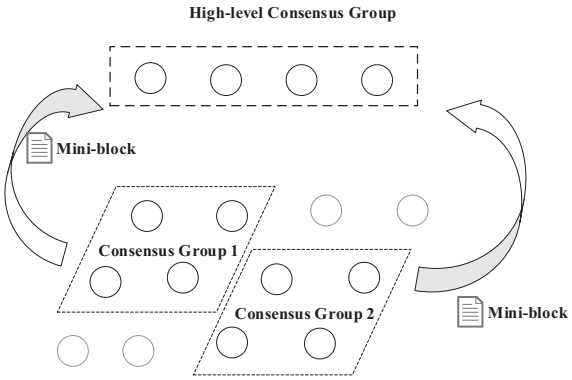

Fig. 3 consensus groups of the blockchain

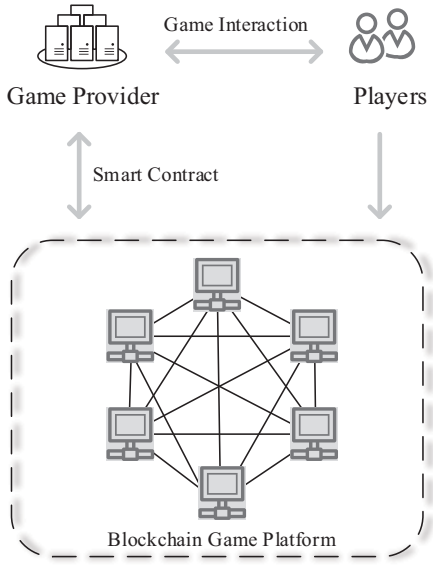

Fig. 4 participants' interaction in the platform

In this consortium chain-based game platform, the nodes participating in the transaction verification and block producing are maintained by some authorized institutions. The game providers can develop game contracts on the blockchain, and record game data to the blockchain through the game contracts. These contracts are open to all users and are associated with the corresponding games. The players can use a client to query the game data which have been stored on the blockchain. The platform interaction is shown in Fig. 4.

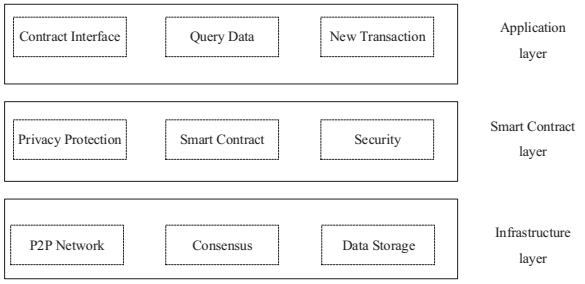

Fig. 5 layers of the blockchain

The game platform consists of three layers: the infrastructure layer, the smart contract layer, and the application layer. Fig. 5 shows the blockchain's layers and modules.

Infrastructure layer: The infrastructure layer is the foundation of the game system, including data storage, peer-to-peer (p2p) network, and consensus mechanisms. This layer is responsible for recording data and communication among nodes. Data synchronization is accomplished among nodes through a consensus mechanism. The consensus mechanism ensures consistency and tampers resistance of stored data

Smart contract layer: The smart contract layer links the platform layer and the application layer. On the one hand, smart contract layer must provide flexible interfaces, such as random number generation interface, data logging interface for the application layer. In addition, smart contract layer also needs to manage the application access rights; on the other hand, it needs to interact with the infrastructure layer to save the application data, and ensure that the data on the blockchain cannot be tampered with.

Application layer: The application layer acts as a window of the platform and is responsible for interacting with the client. The application layer responds to the clients' operations on the platform by calling smart contracts. The application layer can also provide some applications and smart contract interfaces for third-party companies to develop new games.

B. Experiment

We deployed a poker game on the platform to test the design. The poker game uses gRPC APIs to connect with blockchain. The smart contracts are programmed by Golang and running in Dockers. We deployed 12 computers as blockchain nodes, 1 computer as the game platform and 1 computer as the game provider. There are 1 high-level consensus group and 2 low-level consensus groups, and each group contains 4 nodes. We use different processes to simulate the players in 5 computers.

In the experiment, the game provider first starts enough games. Then the players simultaneously execute the algorithm in section 3.2. We record the average latency between the player sending out its random number and the game provider sending back *txid2*. This latency is approximately equal to the load time that a player has to wait to start a game. Every two players play a game together. The result is shown in Fig. 6. When the number of players is less

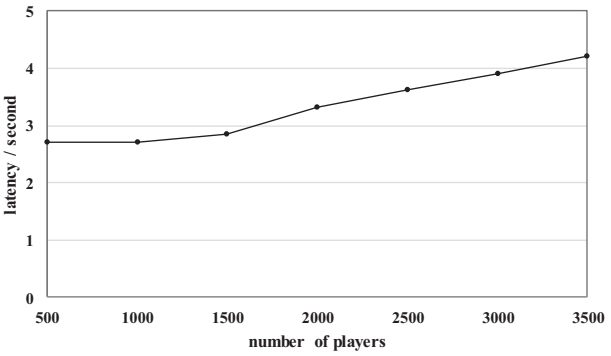

Fig. 6 latency of the poker game

Fig. 7 a game record queried from the blockchain

than about 2000, there is only one consensus group. Due to the limitation of block size and package speed, when the number of players continues to increase, if there is still only one consensus group, the latency will double when the number of players doubles. However, when a new consensus group was added at this time. Although transaction allocation and mini-block verification increased some time, the original delay was greatly reduced. The final record of one of the games is shown in Fig. 7. The record is queried from the blockchain with *txid3*.

In this experiment, we only make a simple modification to the random number generation function and the data storage function of a tradition poker game. Then the poker game can be deployed on the platform. This experiment shows that with only two low-level consensus groups, the system still has low game latency in the case of thousands of concurrent requests. The actual blockchain game experience is not much different from the centralized one.

V. CONCLUSION

In this paper, we propose a blockchain-based true random number generation algorithm. This algorithm combines players, game providers and blockchains to generate random numbers. It solves the problem of "pseudo-random" and manipulation problem in traditional gambling games. Then we design a blockchain game platform based on this algorithm. The game platform is based on the consortium

chain, which can provide better performance than traditional public chains and solve the forking problem. The blockchain game platform provides an interface, and the traditional games can connect to the platform without any changes. The game process is recorded on the blockchain so that the whole process of the game can be supervised. The platform solves the problem of cheating and manipulating game data artificially by game providers. Besides, the random number generation algorithm can be used in many other application scenarios to ensure fairness.

Considering the insufficient performance and the data privacy protection problem of the blockchain, we do not use smart contracts to execute all the complex game logic. We still retain the role of game provider in the random number generation algorithm and game platform. Next, we are going to optimize the platform in three aspects: (1) Add a credit evaluation module to the blockchain to monitor the game providers' behavior. The credit evaluation module can help the game players to choose reliable game providers. (2) Use secure multi-party computation (SMPC) in the blockchain. We will design an SMPC-based random number generation algorithm and SMPC-based game process to prevent the joint cheating between game providers and some players. (3) Continue to optimize the consensus algorithm and design a blockchain with high performance and low latency. Relying on this high-performance blockchain, the game logic process can be executed entirely using the smart contract. With this solution, the blockchain game platform will be completely transparent and fair.

ACKNOWLEDGMENT

Thanks to the support of the research topic "The possibility and breakthrough of blockchain application" from China Center for International Economic Exchanges (CCIEE).

This work was supported in part by the National Natural Science Foundation of China (Grant No. 61573260, 61733013), and Basic Research Project of Shanghai Science and Technology Commission (Grant No. 18DZ1200804).

REFERENCES

[1] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and Energy-Efficient Handover in Fog Networks Using Blockchain-Based DMM," IEEE Communications Magazine, vol. 56, pp. 22-31, 2018.

[2] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," IEEE Communications Magazine, vol. 56, pp. 50-57, 2018.

[3] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, p. S0308596117302483, 2017.

[4] Z. Yu and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, pp. 983-994, 2017.

[5] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, pp. 119-125, 2017.

[6] L. Hong, Z. Yan and Y. Tao, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," IEEE Network, vol. 32, pp. 78-83, 2018.

[7] N. Zhang, Y. Wang, C. Kang, J. Cheng, H. E. Dawei, and H. District, "Blockchain Technique in the Energy Internet: Preliminary Research Framework and Typical Applications," Proceedings of the Csee, 2016.

[8] X. Tai, H. Sun and Q. Guo, "Electricity Transactions and Congestion Management Based on Blockchain in Energy Internet," Power System Technology, 2016.

[9] J. M. Romanbelmonte, C. R. De and E. C. Rodriguezmerchan, "How blockchain technology can change medicine.," Postgraduate Medicine, pp. 00325481.2018.1472996, 2018.

[10] P. Treleaven, R. G. Brown and D. Yang, "Blockchain Technology in Finance," Computer, vol. 50, pp. 14-17, 2017.

[11] I. Eyal, "Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities," Computer, vol. 50, pp. 38-49, 2017.

[12] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," Financial Innovation, vol. 2, p. 24, 2016.

[13] G. Zyskind, O. Nathan and A. S. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in IEEE Security and Privacy Workshops, 2015, pp. 180-184.

[14] U. W. Chohan, "The Leisures of Blockchains: Exploratory Analysis. SSRN,", 2017.

[15] D. Liao and X. Wang, "Design of a Blockchain-Based Lottery System for Smart Cities Applications,", 2017, pp. 275-282.

[16] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin,": IEEE, 2014, pp. 443--458.

[17] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," IEEE Access, vol. 6, pp. 53019--53033, 2018.

[18] F. M. Ametrano, "Bitcoin, Blockchain, and Distributed Ledger Technology," Social Science Electronic Publishing, 2016.

[19] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in Systems, Man, and Cybernetics (SMC), 2017 IEEE International Conference on, 2017, pp. 2567-2572.

[20] C. Cachin, "Architecture of the hyperledger blockchain fabric,", 2016.