

An Efficiency Evaluation Model for Designing Optimal Scheduling Mechanisms in N+X Hybrid Blockchain

Peipei Wang*, Kun Meng**, Shuqin Li**

* School of Computer, Beijing Information Science and Technology University, China

** Joint Lab of Sensing and Computational Intelligence, Beijing Information Science and Technology University, China
scarlett_jian@163.com, mengkurt@bistu.edu.cn, Lishuqin2005@bistu.edu.cn

Abstract— With the widespread of Bitcoin, blockchain has been focused by researchers from many fields, such as digital cryptocurrencies, finance security exchange, decentralized trade platform and so on. However, the operation efficiency (about 10min/per block) has limited its practical application except of Bitcoin. In this paper, we conduct further research based on the existing hybrid blockchain architectures, say N + X Hybrid Blockchain, which may significantly improve blockchain efficiency with the negligible cost of security. Moreover, we gave an evaluation model for the feedback process of nodes in the N+X Hybrid Blockchain and obtained optimal strategies. For the application of Energy Internet (EI), we proposed a scheduling mechanism based on the above evaluation model, and given an algorithm to implement it.

Keywords— Blockchain, Efficiency Optimization, Energy Internet, N+X Hybrid Blockchain

I. INTRODUCTION

The Blockchain technology is an emerging technology, it has been focused by researchers from many fields for its characteristics of decentralization, transparent and trustless since it was first proposed in the article “Bitcoin: A Peer-to-Peer Electronic Cash System” [1]. However, the blockchain is not an omnipotent technology. While it provides a fair platform for various industries, it is inevitable that the low transaction efficiency of blockchain-based applications [2]–[4]. The efficiency is crucial for most time-sensitive areas, therefore, it also limits its application and promotion in areas with strong timeliness such as energy and finance [5].

The blockchain can be divided into public blockchain, private blockchain and alliance blockchain by the principle of participation mechanism. The difference of characteristics determines their different application scenarios, and the core difference lies in the degree of access authority (see Table 1 for details). The public blockchain focuses on the decentralization of storage and verification. The participants are completely independent of each other in this chain, so their participation or withdrawal is not controlled by third-party organizations. The private blockchain is a weakly centralized or multi-centralized system, compared with the full distributed

system of the public blockchain, it has strict restrictions on participating nodes. The access authority of the alliance blockchain is between the public blockchain and the private blockchain, which achieves partial decentralization of the nodes. Currently, most of the blockchain applications are based on the above three chains.

TABLE 1. COMPARISON OF THREE CHAINS

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Centralization	Decentralization	Partial Center	Multi-center
Participant	Everyone	Controlled by the center	Pre-setting
Bookkeeping	All participants	User Defined	Formed by consultation
Consensus	PoW, PoS	N/A	PBFT [6], PoS
Typical Case	Bitcoin, Ethereum	Settlement System	R3, Hyperledger

The Bitcoin is a typical case of incipient public blockchain, and nodes participate in the transaction and verification process anonymously in this network, they ensure the data consistency by the Proof of Work (PoW) consensus mechanism and the economic incentives. In this application, the security will not be destroyed unless the power of cooperative attack in the whole network exceeds 51% of the total power, while it is difficult to converge so much computing power in distributed systems [7]–[9]. This security mechanism that utilizes the distributed structure of nodes and the unpredictability of network computing power, which makes the low transaction efficiency. For example, the 10 minute/block generation rate, i.e. the transaction efficiency of 7 transactions per second in Bitcoin, is far away from the actual demand, which limits its practical application [10]. Considering the inefficiencies and waste of resources brought by using PoW in Bitcoin, the Ethereum uses a hybrid consensus mechanism with improved efficiency, Casper, which is an improved mechanism for the PoW by combines PoW and Proof of Stake (PoS) and ultimately switches the

consensus mechanism to PoS [11]. The PoS consensus mechanism is different from the high energy-consuming mining of the PoW, it completes the trustiness of nodes by the amount of money held in the wallet rather than violent calculations of nodes [12], and the transaction efficiency increased to 20 transactions per second in Ethereum. Although the efficiency has improved compared to Bitcoin, it is still far smaller than VISA's average of 50,000 transactions per second and Alipay's peak value of 200,000 [13]. There is no doubt that the efficiency problem is still a major problem in the development of the current blockchain technology, and it is inevitable to sacrifice transaction efficiency for the reasons of the technical limitations of the "impossible triangle" in the blockchain (i.e. it cannot meet the three requirements of "efficient, low energy consumption", "decentralization" and "safety" at the same time) and its requirements of "decentralization" and "safety". So, the improvement of transaction efficiency must also be achieved on the basis of weakening the two conditions of "decentralization" and "security" [14].

There is an N + X Hybrid Blockchain architecture proposed in [15] to compensate for the shortcoming of blockchain efficiency. In this structure, N stands for a high-confidence private nodes and X represents public nodes participating in the transaction, they are the representatives of authoritative grid agency and the consumer who participates in energy transactions respectively. It advocates the combination of public blockchain and private blockchain, the public blockchain is used for the secure storage of transaction information because of its features of decentralization, while the private blockchain takes advantage of the high credibility and the limited number of nodes for transaction verification and supervision, meanwhile, the mining mechanism of high energy consumption and low efficiency can be eliminated with the addition of the private nodes to the hybrid chains, it ensures the chains security and effectiveness by exploiting the independence and randomness of the nodes. What more, a reasonable scheduling mechanism of verification nodes can substantially improve the transaction efficiency.

In this paper, we further explore and optimizes the scheduling strategies of verification nodes involved in N+X Hybrid Blockchain structure transactions. To solve the problem of verification nodes selection in energy trading, there are gave a verification node feedback model for the feedback process of nodes, and this model is implemented by an algorithm. Ultimately, the optimal verification node selection strategy that takes into account the security and transaction efficiency is obtained.

II. SECURITY GUARANTEE OF N+X HYBRID BLOCKCHAIN

In the following table 2, we give a characteristic comparison of public blockchain, private blockchain and N+X Hybrid Blockchain. The conclusion shows that all of them retain the characteristics of decentralization, transparency and security even though they have different implementations of

blockchain techniques in their respective application scenarios. And the degree of decentralization makes them slightly dissimilarity in the realization mechanism of their respective characteristics.

TABLE 2. THE CHAINS IMPLEMENTATION MECHANISMS

Feature	Public Blockchain	Private Blockchain	N+X Hybrid Blockchain
Centralization	P2P	Private network	P2P+Private network
Transparent	Hash, Merkle Tree	Hash, Merkle Tree	Hash, Merkle Tree
Security consistency	Timestamp Anonymous nodes	Timestamp Trusted nodes	Timestamp Randomness nodes
effectiveness	Low	High	High

The public blockchain is oriented to the entire P2P network, each node has the same status, and there is no special central node or hierarchy in the network. The Hash encryption algorithm of the transaction ensures the security of the plaintext and the transparency of the processed data. At the same time, the Hash-encrypted ciphertext transaction set is stored in the Merkle Tree structure, which reduces the storage information capacity in the block and satisfies the requirements of quickly searching and verifying transaction information. Meanwhile, the transaction information is signed through an asymmetric encryption mechanism so that the transaction cannot be easily falsified. The data consistency of the chain in the distributed system is guaranteed by the blockchain consensus mechanism, take the popular blockchain applications such as Bitcoin and Ethereum as examples, some of the consensus mechanisms resist the attacks of saboteurs by forming a powerful computing power such as PoW, while others such as PoS take advantage of the fair competition from participating nodes to ensure security, most of the above mining activities waste a lot of CPU computing resources. In addition, the transaction set in the block must be verified by all node before being recorded in the chains, what brings about inefficiency while ensuring security, and it is one of the main reason of blockchain efficiency issues. Since its confidentiality and trust of nodes in the private blockchain, it is not necessary to achieve unified data in the system through mining. On the other hand, considering the existence of faulty nodes and malicious nodes in the cluster, consensus algorithms such as PBFT and Raft are usually adopted, which makes the storage efficiency of private blockchain is higher than public blockchain.

The N+X Hybrid Blockchain structure in the EI is partially decentralized in practical application. It consists of a public blockchain of fully decentralized public user nodes and a private blockchain managed by private nodes familiar with the grid business. The public node is used for secure storage of transaction information because of its decentralization feature, private node used to verify and supervise transaction data for

its characteristic of high trust, which solves the problem that verification by all nodes in the public blockchain. At the same time, taking advantage of the high trustworthiness of the private blockchain and the randomness of the nodes in the system, the data consistency requirement can be achieved without wasting a lot of effort, and the transaction efficiency can be improved.

In the BSS (Block Static Storage) system [15], a public node (i.e. energy consumer) broadcasts energy transaction requests, and the other nodes of the system give feedback by determining whether they meet the request conditions after receiving the request. On the other hand, it will receive corresponding economic reward to maintain the ecological balance of the system after becoming a verification node [16]–[17]. When the transaction information is generated, the transaction set and the block information are verified by nodes in the network. In the Bitcoin system, the verification of transaction is to select all nodes in the network as verification nodes to ensure the consistency and security of the data, which greatly affects the transaction efficiency. while in the N+X Hybrid Blockchain of EI, it is not necessary to select all nodes for block verification when considering the large number of decentralized public nodes in the energy system, and the verification nodes can be obtained through a node scheduling strategy.

The largest difference from the conventional blockchain is that there is no consensus mechanism in the N+X Hybrid Blockchain, the trust problem between nodes in this mode is guaranteed by the randomness feature by the selected verification node, which avoid the waste of resources. Currently, the hybrid chain structure employs a strategy of selecting a specified number of nodes (two-thirds of the public nodes) for block information verification. However, With the increasing number of the public nodes in the BSS system, the number of verification nodes in the above verification mechanism will become increasingly large, and the time-consuming of the verification process will remain one of the bottlenecks for efficiency.

III. ESTABLISHMENT OF FEEDBACK NODE MODEL

In this hybrid chain structure (Figure 1), the public node is used for security assurance of block information, and the private node occupy the status of managers for its unique write permissions and the high credibility of the nodes. At the same time, the delay of transactions between private nodes is smaller, so its transaction efficiency is much larger than that of public nodes. Take into account of the strengths and weaknesses of this two kinds of nodes, in this paper, there are adopts the linear combination of public and private node for the block verification in the hybrid chain. The public node guarantees security and the private node is used to improve efficiency [19].

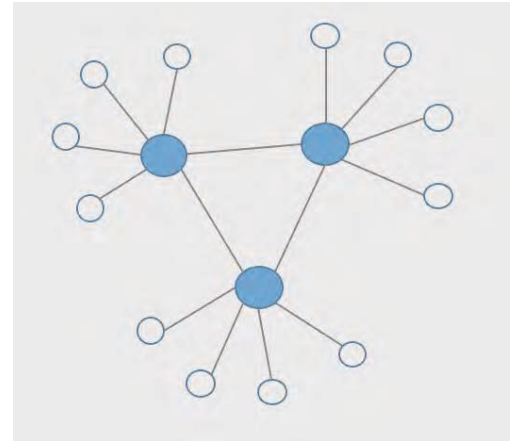


Figure 1. Network topology structure for N+X Hybrid blockchain

A complete block verification process includes the verification of transaction set, the fast verification of block information and return the verification results to the VTCN. Due to the differences of routing and logical distance between nodes in the network, the waiting time of nodes in the verification process, i.e. the verification feedback delay, is not uniformly distributed. In a very short time after the VTCN sends out the transaction verification request, the number of feedback nodes is almost unchanged, which is a small probability event. While during a specific period of time, the number of feedback nodes reaches a peak. What more, the verification feedback process of verification nodes is random and independent from each other.

The Poisson process is one of the most widely-used counting processes, it is usually used in scenarios where we are counting the occurrences of certain events that appear to happen at a certain rate, but completely at random. Thus, we conclude that the Poisson process might be a good model for verification feedback nodes [20]. The Poisson distribution is the probability distribution of a random variable X (called a Poisson random variable) such that the probability that X equals k is given by:

$$P(X = k) = \frac{\lambda^k}{k!} e^{-\lambda}, k = 0, 1, 2, \dots \quad (1)$$

Where k denotes the number of feedback nodes within a specified time S and the parameter λ equals the expected value of X which determines the shape of the distribution.

The negative exponential distributions are a class of continuous probability distributions, it describes the times between events in a Poisson process, i.e. the delay t of the verification node's feedbacks [21]–[23]. The probability density function of a negative exponential distribution is:

$$P_1(t; \lambda) = \begin{cases} \lambda e^{-\lambda t}, & t > 0 \\ 0, & t \leq 0 \end{cases} \quad (2)$$

In this model, the parameter λ means that the number of verification feedback nodes within specified time S . The expected values of node feedback delay $D = 1/\lambda$.

There is a "51% power attack" in the traditional blockchain network, and the main reason for this attack is that the nodes hope to improve the possibility of successful mining and obtain economic rewards. The "51% power attack" means that the malicious nodes aggregate more than 51% computing power of the whole network, which may modify the block information and destroy the decentralized characteristics of the blockchain. We found that the public blockchain network composed of public nodes is structurally decentralized in the hybrid chain network through analyzing the trading of BSS system. The possibility of achieving such attacks in a fully distributed network is extremely low, even if the malicious nodes attempting to tamper with block information have more than 51% of the computing resources. So the block security is guaranteed. There are also manager nodes in the BSS system besides the public nodes, it has higher authority compared with the public node. In this private chain network composed of private nodes, nodes are connected to each other and the efficiency of data exchange is high. However, the "51% power attack" is also prone to happen, its role is much smaller than that of public nodes in terms of ensuring the block information security.

The verification nodes participating in the verification process in the hybrid chains need to meet the independent and unpredictable requirements to avoid "51% power attack" for the purpose of the security verification of block information. Since the private node in the hybrid chain is more likely to be the attack target, we give the proportion of the two types of nodes in the N verification nodes randomly, it ensures the block security by the feature of randomness. It can be seen from the figure (1) that the transmission delay varies depending on the network topology and the routing path when the verification node feedback the block verification information to the VTCN. The VTCN is a private node, and the number of private nodes is limited and it is connected to each other in the network, so the delay D_{pu} of public node D_{pu} and the private node delay D_{pr} satisfy the condition that $D_{pu} > D_{pr}$. The feedback situation of nodes varies with node delay, so the delay t of the two kind nodes satisfying the negative exponential distribution of different λ parameter, respectively.

$$P_1^*(t; \lambda_u) = \begin{cases} \lambda_u * e^{-\lambda_u t}, & t > 0 \\ 0, & t \leq 0 \end{cases} \quad (3)$$

$$P_2^*(t; \lambda_r) = \begin{cases} \lambda_r * e^{-\lambda_r t}, & t > 0 \\ 0, & t \leq 0 \end{cases} \quad (4)$$

The cumulative distribution function is:

$$F_1(t; \lambda_u) = P_1^*(T \leq t) = \begin{cases} 1 - e^{-\lambda_u t}, & t > 0 \\ 0, & t \leq 0 \end{cases} \quad (5)$$

$$F_2(t; \lambda_r) = P_2^*(T \leq t) = \begin{cases} 1 - e^{-\lambda_r t}, & t > 0 \\ 0, & t \leq 0 \end{cases} \quad (6)$$

A pseudo-random number uniformly distributed on (0,1) is implemented by using a Pseudo-Random Function on the computer, and the random number q is used as the proportion of the public node in the verification node. Then, the parameters λ_{N+X} in the hybrid chain network satisfies the following conditions:

$$\lambda_{N+X} = q\lambda_u + (1 - q)\lambda_r \quad (7)$$

The above analysis shows that the verification node's delay in the N+X Hybrid Blockchain presents a negative exponential distribution. When establishing a verification node selection model based on the negative exponential distribution, the most important thing is to use the knowledge of probability and statistics to determine the relevant parameters, so as to establish a specific node selection model. There are given a simulation example to solve the parameters of this model by the simulation environment MATLAB R2017a. Given $S = 1s$, then 100 random variables which obey the negative exponential distribution are generated to represent the node delay, the 100 sets of node delay data can be obtained. We can calculate the expectation of the number of feedback node by using these actual data.

Statistics the measured data of simulation experiment, the average feedback delay $E(t)$ of the public verification node is:

$$E(t) = \sum_{i=1}^{\theta} t \cdot p = 4.1900$$

so, the number of public feedback nodes obtained in 1s is:

$$\lambda_u = \frac{1}{E(t)} = 0.2387,$$

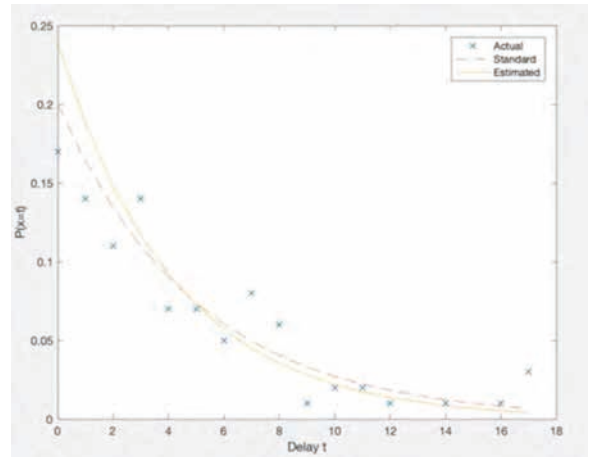


Figure 2. Delay-Probability Diagram

Substituting the above actual parameters and the obtained parameters into the above Eq. (5), drawing a curve and comparing the images with the measured data. It can be seen

that the graph curve $\lambda_u = 0.2387$ is closer to the measured data curve than the standard graph $\lambda_u = 0.2$, so the parameter $\lambda_u = 0.2387$ is determined.

Similarly, the parameter of the private node $\lambda_r = 0.6369$ is determined.

IV. AN ALGORITHM FOR SOLVING THE VERIFICATION NODE FEEDBACK MODEL

When the parameter λ_u , λ_r is determined, the value of q is given by the above Eq. (6) randomly. then the parameters λ_{N+X} are uniquely determined (see figure 3 below).

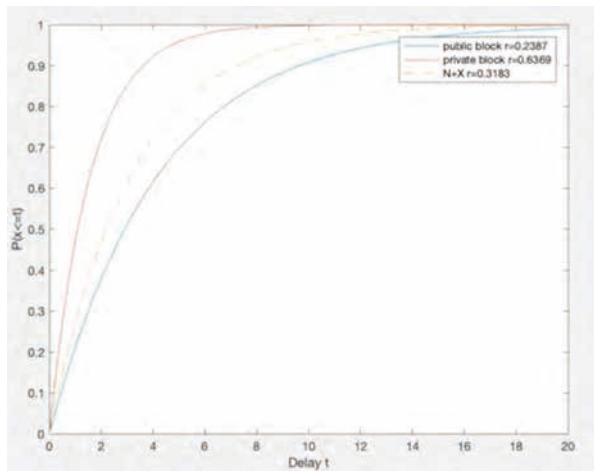


Figure 3. Cumulative Distribution of Nodes Delay

Event E: The number of feedback nodes before a certain moment S is not less than n .

To ensure the security of the block information in the hybrid chain, the number of feedback node must be at least n when select N nodes as within a specified time.

Among the selected N verification nodes, each verification node with feedback information during S time satisfies the condition $p(t \leq T)$, and the expression for the probability of obtaining n verification feedback nodes is:

$$\begin{aligned} P(x = n) &= C_N^n P(t \leq S)^n (1 - P(t \leq S))^{N-n} \\ &= C_N^n (1 - e^{-\lambda_{N+X}t})^n e^{-\lambda_{N+X}t^{N-n}} \end{aligned}$$

The relationship between the number of verification nodes N and the probability of feedback n nodes is verified. The function graph is shown in Figure 4.

The probability of occurrence of the Event E $P(x \geq n)$ is

$$P(x \geq n) = 1 - P(x < n) = 1 - \sum_{i=1}^{n-1} P(x = i),$$

Give the graph of the relationship between the number of selected verification nodes N and the probability that the number of feedback nodes is not less than n (Figure 5).

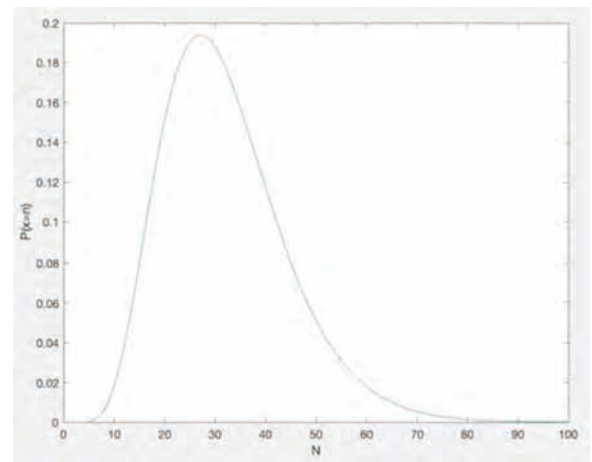


Figure 4. N-P(x=n)

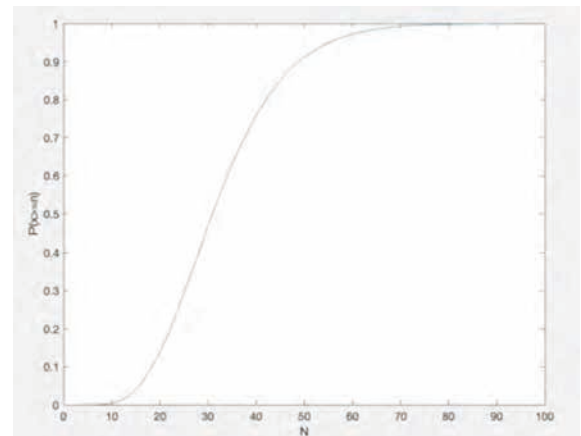


Figure 5. N-P(x ≥ n)

As can be seen from the figure above, the graph of the selected verification nodes number N and the probability that the number of feedback nodes is not less than n is monotonous and non-decreasing. Moreover, its probability will eventually be close to 1. Therefore, the number of the verification node N can be uniquely determined by the minimum probability of satisfying the Event E.

In this way, the value of N is the number of optimal authentication nodes that satisfy security and take into account the transaction efficiency.

V. CONCLUSIONS

In this paper, the verification node feedback model in the hybrid blockchain is implemented by verifying the Poisson distribution change of the nodes, and the relevant parameters of the verification node feedback model are determined through simulation experiments. Finally, the optimal strategy of the verification node that meet the security requirements of the system and the service delay of the transaction in different network environments is obtained, so that the two parties can reach the balance. It turns out that the value of N in this model is much smaller than the number of nodes in the network.

ACKNOWLEDGMENT

The authors are also deeply grateful to Dr. R. Meng, associate Professor of Beijing Information Science and Technology University, gives his numerous constructive comments and helps. In addition, there exists other teachers' help and encouragement. The authors would like to express sincere gratitude to them.

REFERENCES

- [1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[Online], available: <https://bitcoin.org/bitcoin.pdf>, 2009.
- [2] Kokoris-Kogias E, Jovanovic P, Gailly N, et al. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing[J]. Applied Mathematical Modelling, 2016, 37(8):5723-5742.
- [3] Sompolinsky Y, Zohar A. Secure High-Rate Transaction Processing in Bitcoin[J]. 2015, 8975:507-527.
- [4] Eyal I, Sirer E G. Majority Is Not Enough: Bitcoin Mining Is Vulnerable[J]. Eprint Arxiv, 2013, 8437:436-454.
- [5] Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. Acta Automatica Sinica, 2016, 42(4):481-494
- [6] RBFT: Redundant Byzantine Fault Tolerance. Pierre-Louis Aublin, Sonia Ben Mokhtar, Vivien Quema. 2013 IEEE 33rd International Conference on Distributed Computing Systems (ICDCS). 2013.
- [7] When Bitcoin Mining Pools Run Dry. Laszka A, Johnson B, Grossklags J. Financial Cryptography and Data Security. 2015.
- [8] 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely, Tuyet Duong, Lei Fan, Hong-Sheng Zhou. <http://eprint.iacr.org/2016/716>.
- [9] Aste T. The Fair Cost of Bitcoin Proof of Work[J]. Social Science Electronic Publishing, 2016.
- [10] Swan M. Blockchain: Blueprint for a New Economy. USA: O'Reilly Media Inc., 2015.
- [11] Ethereum White Paper. A next-generation smart contract and decentralized application platform [Online], available: <https://github.com/ethereum/wiki/wiki/WhitePaper>, November 12, 2015.
- [12] Proof of Stake[EB/OL]. Bitcoin Wiki. Available: https://en.bitcoin.it/wiki/Proof_of_Stake. 2015.
- [13] Zhang Ni, Wu Qing, Zong Liang, Zhao Wei, Guo Tianyong, Wang Wen, Wu Qiang, the central bank's digital currency is evolving. [J] China Development observation, 2017 (04): 18-20+23.
- [14] Chen Yi Xi. "Impossible Triangle" of blockchain technology and issues needing attention. [J]. Zhejiang finance, 2016 (02): 17-20+66.
- [15] Wu Lijun, Meng Kun, Xu Shuo, et al. Democratic Centralism: a hybrid Blockchain architecture and its applications in Energy Internet[C]. IEEE International Conference on Energy Internet (ICEI). 2017.
- [16] N. Zhang, Y. Wang, C.Q. Kang, et al. Blockchain Technique in the Energy Internet: Preliminary Research Framework and Typical Applications. Proceedings of the CSEE, vol. 36, issue 15, pp. 4011-4022, 2016.
- [17] Schwieters N, van Hoof J, Etheridge D, et al. Blockchain— an opportunity for energy producers and consumers? [EB/OL] . (2016-11-04) Available: <http://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf>.
- [18] Dong Han, Zheng Yan, LiLei Li. Evaluation method of smart grid efficiency based on stochastic frontier model [J]. Power system technology, 2015, 39 (7): 1963-1969.
- [19] C. Lin, Y. Li, and J.X. Wan. "Optimization approaches for QoS in computer networks: a survey," Chinese Journal of Computers, Vol. 34, No. 1, pp. 1-12, 2011.
- [20] Sung Nok Chiu; Dietrich Stoyan; Wilfrid S. Kendall; Joseph Mecke (27 June 2013). Stochastic Geometry and Its Applications. John Wiley & Sons. pp. 110–111. ISBN 978-1-118-65825-3.
- [21] J. F. C. Kingman (17 December 1992). Poisson Processes. Clarendon Press. pp. 11–12. ISBN 978-0-19-159124-2.
- [22] Daley, Daryl J.; Vere-Jones, David (2007). An Introduction to the Theory of Point Processes: Volume II: General Theory and Structure. Springer. p. 26. ISBN 0387213376.
- [23] Jesper Moller; Rasmus Plenge Waagepetersen (25 September 2003). Statistical Inference and Simulation for Spatial Point Processes. CRC Press. pp. 15–16. ISBN 978-0-203-49693-0.



Wang Peipei received the B.S. degree in software engineering from Tianjin University of Commerce, Tianjin, China, in 2016.

Her is currently with under postgraduate of School of Computer, Beijing Information Science and Technology University, Beijing, China. Her research interests include energy internet and blockchain.



Meng Kun received the B.S. degree in Department of Mathematics from Zhoukou Normal University, Henan, China, in 2002, and the M.S. degree in School of Mathematics & Information Science, and the Ph.D. degree in School of Computer and Communication Engineering from University of Science and Technology Beijing, Beijing, China, in 2012.

He is currently with associate professor of School of Computer, Beijing Information Science and Technology University, Member of IEEE, ACM and China Computer Federation. His research interests include energy internet, performance evaluation and stochastic models.



Li Shuqin received the B.S. degree in computer application from University Of Shanxi, Shanxi, China, in 1985, and the M.S. degree in Computer Application from Nanjing University of Science & Technology, Nanjing, China, in 1988, and the Ph.D. degree in School of Computer from Nanjing University of Science & Technology, Nanjing, China, in 2006.

Her is currently with professor of School of Computer, Beijing Information Science and Technology University. Her research interests include artificial intelligence and multi-agent collaboration.