A Survey on Blockchain Incentive Mechanism

Jiyue Huang[1], Maoyu Du[2], Hongting Zhao[2], and Kai Lei[1,*]

Shenzhen Key Lab for Information Centric Networking & Blockchain Technology (ICNLAB)

School of Electronics and Computer Engineering, Peking University, Shenzhen, China

{huangjiyue,mydu}@sz.pku.edu.cn

leik@pkusz.edu.cn

Abstract. The current research on the blockchain can be divided into the study on network architecture and on the incentive. This paper begins with the introduction on the architecture of information technology and illustrates the goal and research status of the incentive layer of blockchain with digital economy development as the backdrop. It elaborates the existing issuance of token from computation, storage and transmission, three core facets of network technology. We analyzes the development of the token allocation and the path to confirm its rationality and discusses the possible directions and challenges of the future research on blockchain incentive, hoping to provide ideas for related research.

Keywords: Blockchain · Incentive mechanism · Digital economy

1 Introduction

Information technology architecture has been growing from large-scale centralized [11] to client/server (C/S) architecture, and to cloud computation [18]. During the progress, although the centralized architecture remains a shared feature of these three sectors, it is still entangled with the high maintenance cost and doubt on its security and reliability. As a key technology of distributed decentralized system and aiming to alleviate security risk caused by centralization, the blockchain has shown promising prospects on academic and industrial application and attracted widespread attention. Blockchain can be defined as a novel distributed infrastructure and computing paradigm [32]. It uses blockchain data structure as storage tool, generates and updates data through distributed node consensus algorithms [20], secures data transmission and access via cryptography, and programs and can manipulates data through the smart contract composed of automated scripts.

As the entity integrating p2p network and asymmetric encryption, blockchain is characterized by its decentralization, traceability, anti-counterfeiting, anti-tampering, and automatic execution of contacts, but the decentralized

consensus and reliable basis for providing fine-grained distribution of network by tokens at the data level actually serve as the two key features distinguishing it from other systems. The consensus organizes a large scale of consensus nodes to implements the data validation and accounting of shared ledgers. In the decentralized system, it is essentially a crowd-sourcing process between consensus nodes [16] [7] [26], and as the consensus node itself is self-interested, maximizing its own interest is the fundamental goal of its participation in data verification and accounting [33].

Focusing on the incentive of blockchains, as the foundation of the number of consensus nodes in the network and a key sector of the prospective development of network ecosystem, main contributions of this paper are as follows:

1. To abstract the essence of blockchain and to encourage readers to have a clearer understanding on blockchain.

2. Systematically overviewed the existing work of the blockchain incentive mechanism and analyze the basic principles and key issues on basis of mechanisms of issuing and allocating.

3. To summarize and forecast the challenges and opportunities of the research on blockchain incentive to provide enlightenment and reference for future research.

2 Economics of blockchain

2.1 Digital economy

As early as in 1976, Hayek, a rugged liberalist, analyzed the fragility of currency system based on public credit in his book of Denationalization of Money [30], argued merits of issuing currencies by different entities (banks) and forecasted a prospect that issuing money is independent from government authority. Since the beginning of 21st century, with the advancement of computer and Internet communication technology, decentralized P2P communication technology and blockchain technology have emerged. The successively emergency of blockchain currencies such as Bitcoin, filecoin, and Ripple XRP provides denationalized money forecasted by Hayek with technological feasibility.

The basic economics of blockchains concerns why distributed solutions that is technically feasible may become more cost-effective than centralized solutions [6]. And the answer is that they run along three index cost curves: 1) Moore's Law - the cost of tackling digital information, namely speed, will be halved every 18 months; 2) Kryder's Law - the cost of storing digital information, namely memory, will be halved every 12 months; 3) Nielsen's Law - the cost of transporting digital information, namely bandwidth, will be halved every 24 months (Wiles 2015). The blockchain establishes reliable trust between nodes in the network, which frees the value transferring process from the interference of the intermediary, improving the efficiency of

value interaction and reducing the cost, and becoming the cornerstone of building the value Internet.

However, existing blockchain currencies (such as Bitcoin) are issued by non-official organizations and gain no government credit endorsement. Most of them are characterized by decentralization, deflation, long transaction delay, low transaction security, and large primary participation [31], which is significantly different from other existing currencies, so the blockchain technology under the digital economy will inevitably contain the differentiation and improvement in terms of technological setups [28].

2.2 Governance-centered approach of organization

As discussed in the previous section, the value of blockchain is not only enboded in the innovation of information and communication technology (ICT). As a distributed ledger, data in blockchain circulates throughout the network and transactions are broadcasted over all nodes, making blockchain naturally integrates the distributed system and system value more enmboded in a new type of economic organization and governance model, which provides reliable evidence to the fine-grained economic distribution system that is non-repudiation, difficult to falsify, and based on the data value.

Blockchain is building a novel institution, making new types of contracts and organizations possible. More detailedly, this new organizational model is an implementation of transaction cost economics (TCE). Douglass C. North argues that institutions, understood as the set of rules in a society, are the key to determining transaction costs [23]. In this sense, institutions that facilitate low transaction costs, boost economic growth. Therefore, organizations and markets serve as the alternative economic systems of economic coordination. Williamson [27] believes that the form of organization largely depends on the necessity of controlling opportunism. The ultimate reason for opportunism lies on the intent and ability of agents to use trust which is called "pursuit of self-interest" by Williamson.

According to Williamson's opportunistic ideas, the consensus mechanism of the blockchain controls opportunism to some extent by establishing the trust between strange nodes. Opportunism is inversely related to the degree of the market. When opportunism is controlled to a certain boundary, the organizational field will shrink, and the market will grow to a true distributed autonomous organization. And, of course, the formation of the organization must depend on the technical architecture of the blockchain system.

2.3 Incentive layer of blockchain systems

The common intelligent transportation systems (ITS) blockchain system architecture consists of seven layers. From the bottom up, they are [21]: 1. Physical layer: It encapsulates various physical entities involved in ITS (equipment, vehicles, assets, and other objects). The key technology is the

Internet of Things [29], which has enhanced device security and data privacy when integrated with the blockchain. 2. Data layer: It encapsulates the chain structure of the underlying data block, and related asymmetric public and private key data encryption and time stamp technology, serving as the basic security guarantee; 3. Network layer: It includes the P2P networking mechanism, data transmission mechanism and data verification mechanism, which means the blockchain can network automatically [24]. 4. Consensus layer: As the core of the blockchain, it encapsulates various consensus mechanism algorithms of network nodes, determining the security and reliability of the whole system. 5. Incentive layer: It integrates economic factors including the issuance mechanism and distribution mechanism of economic incentives into the blockchain technology system and promotes the development of the system in a virtuous circle; 6. Contract layer: It encapsulates various scripts, algorithms, and smart contracts and works as the foundation of the blockchain programmable feature [8] [3]; 7. Application layer: It is used to deploy various scenarios and cases of the blockchain .

The incentive layer is located between the consensus layer and the contract layer, especially closely related with the consensus system [2]. Two major goals of incentive layer are: 1. To attract as many nodes to become data nodes in the network. Data flow in the network works as a foundation. Only when there are more data nodes included in the network, frequent network transactions, and real and rich transaction data, can the value of blockchain acts as a "distributed ledge" be reflected; 2. To encourage more nodes to enter the "mining circle" as a miner and participate in the consensus to win the bookkeeping right. As the best among current consensus algorithm in terms of tackling double-spending issue, the PoW also has to run with the consensus of more than 51% of honest nodes and more nodes means higher reliability. A example more detailedly, Eyal et al. describes miners are motivated to (1) include transactions in their microblocks [9] , (2) extend the heaviest chain, and (3) extend the longest chain. Unlike in Bitcoin, the latter two points are not identical. Eyal et al. mainly trade-offs between throughput and latency.

3 A taxonomy of incentive focus

It turns out that the incentive economy model of digital currency is the core of the blockchain industry ecology. Two goals of the incentive mechanism are based on the token of blockchain system, which is achieved by the following two strategies: One focus on the issue mechanism of the token. It assesses what behaviors of the network node deserve newly issued coins and directly demonstrates the major functional application scenarios and development directions of the blockchain system. The incentive mechanism of the issuance responds to the main ecological demands of the networks . The other focuses on the allocation mechanism of the token. It restricts the

distribution of existing tokens in the system though evaluating the nodes contributing to the network, the contribution of each node and the random factors that guarantee fairness. This one puts more emphasis on creating a good ecosystem among the participating network nodes, thereby indirectly enhance the network value, attracting nodes to participate in the network and in the consensus, and improving network reliability and the quality of the consensus.

The issuing and allocating mechanism of economic incentives are mainly considered in public chain scenarios. In public chains, it is of great significance to motivate the nodes that follow the rules to participate in the accounting and to punish the nodes violating the rules, ensuring the whole system develops into a virtuous circle. However. in the private chain, incentives are not that necessarily, because the nodes participating in the accounting often complete the game outside the chain, and participate in accounting through coercion or voluntary.

Take the Bitcoin as an example. The nodes joining the network win the billing rights through the proof of work (PoW). The Bitcoin rewards make them proactive "miners" , and under the incentive mechanism, the competition for computing power drives miners to constantly optimize their "mining machines". This definitely promotes the further optimization of blockchain systems.

Obviously, the incentive mechanism encourages the nodes to participate in the maintenance of the safe operation of the block chain system and protects the general ledger from tampering through the means of economic balance. It strongly correlates with the consensus mechanism is a strong correlation and is the long-term impetus to maintain the operation of the blockchain networks.

3.1 On issuing mechanism

As mentioned above, the true meaning of the token is to encourage the nodes to maintain the reliability of the system consensus and to improve the ecological value of the blockchain system. Existing researches on issuance mechanism of the blockchain token aim at the three major issues of computer network: computation, storage and transmission, and have made great progress.

Calculation The most typical example of calculating the contribution is the bitcoin system using the PoW consensus mechanism. The network solves the hash function of the specific difficulty through each miner node, and evaluates the power contribution of the node when participating in the consensus. The computing power at the single node does not exceed the total system budget. At 51% of the force, the system can effectively alleviate the very important double flower problem in the digital currency. Although the bitcoin system has aroused heating attention over the computer science field and

the economic and financial circle, as a prototype of the blockchain economy proposed by Nakamoto, scholars have optimized and adapted this in later research.

Eyal et al. [10] shows that the Bitcoin mining protocol is not an incentive for an attack: the collaborating miners receive more than their fair share. Rational miners prefer to join selfish miners [1] [4], and the size of the collusion group will increase until it becomes a majority. It prohibits selfish mining by pools that command less than 1/4 of the resources. This threshold is lower than the wrongly assumed 1/2 bound, but better than the current reality where a group of any size can compromise the system. Similar improvements are generally made in the trade-off of efficiency, safety and fairness [13] [1].

Storage Compared with the computing power used to calculate the contribution to solving hash function in the PoW system, with the development of centralized cloud storage, more shared storage resource in the blockchain network can be utilized, and the contribution can be evaluated based on the provided storage service.

Compared with the computing power used to calculate the hash contribution in the PoW system, with the development of centralized cloud storage, the shared storage resource utilization in the blockchain network is higher, and the contribution can be evaluated based on the provided storage service. . A typical example of a storage-based blockchain system is filecoin [1], which is built on a blockchain and a decentralized storage network with native tokens. Customers spend tokens to store data and retrieve data, while miners earn tokens by providing storage and retrieval data to form a supply and demand trading platform for storage and retrieval.

Three major roles in the Filecoin network are the customer, storage miner and search miner. When the customer publishes the demand for storing and retrieving data, the storage miner who is required to provide collateral priced in proportion to storage space provides storage and earns Filecoin,. Then the network will use the Proof-of-Space-time (PoSTs) to confirm whether the miner has complied with the commitment to store the data of the customer, while the search miner offers the data retrieval service and earns Filecoin without providing collateral. The market is operated by a network that uses PoSTs (Proof-of-Space-time) and PoRep (Proof-of-Replication) to ensure that miners properly store the data as they promised.

Transmission The incentive on transmission aims to encourage data nodes (such as IoT devices) in the network to share real data and encourage intermediate nodes to forward data actively and honestly [14] [25]. For example, CreditCoin [19], trading and accounting information is tamper-proof

[1] https://filecoin.io/

and oriented to the vehicular announcement network, encourages users to share traffic information. It implements conditional privacy that allows its Trace Manager to track the identity of the malicious user in an anonymous announcement of a related transaction. Therefore, CreditCoin can encourage users to forward announcements anonymously and reliably. Similarly, to tackle potential selfish behaviors or collusion through distributed P2P applications, He et al. [14] propose a type of secure verification and pricing strategy to balance energy and bandwidth consumption by nodes forwarding files, delivering messages or uploading data.

In fact, giving incentive to transmission aims to keep nodes honest and active. On the one hand, to make efforts on honesty is to construct good economic conditions, ensuring nodes cannot change the effective transmission of the network for personal will, which is one of the core issues of decentralization to a certain extent. On the other hand, to reward active nodes is based on the "self-interest" principle so that the nodes can achieve the approximate balance between pay and benefit as much as rules permit, which requires the Nash equilibrium to find and prove the balance point.

3.2 On allocating mechanism

The blockchain is not only the innovation of network technology, but also the innovation of new economic ecology. In the blockchain, the "transparent" data transmission coordinates with the distributed general ledger. Compared to the conventional architecture where IP end-to-end slave connection to transmission, this is capable to assess the contribution of the nodes more clearly. Generally, the distribution mechanism recognized by most people needs to follow three rules: 1. To ensure the reasonable evaluation on the data provider and revenue is still valid after forwarding. 2. The reward for the maintenance of real data and active forwarding by the intermediate routing node. 3. The requesting node obtains real data and the value is reasonably evaluated.

Take the bitcoin allocation as an example. In the original allocation model proposed by Nakamoto, the first miner succeed in digging for the right to accounting can get a bitcoin, while the rest all fail and can only expect the next turn although they paid the computing power too. Because of this, many small nodes have a low probability of receiving rewards. Even with the network publishing transaction data, these nodes are not motivated enough to be a miner node, which appears to contradict the reciprocal economic structure equipped with multi-accessed network and fine-grained sharing in the future. Currently, there are more than a dozen of enhanced fine-grained distribution [17] based on bitcoin [22]. The combination of ByzCoin and PBFT [5] is stuck to the transaction fee of BitCoin so that more miners can get participated and share mining reward through dynamic formation representing the recently successful block miners' hash capability ratio consensus group to achieve the Byzantine consensus while retaining the open

membership of Bitcoin. Its incentive mechanism focuses on motivating intermediate nodes, and each node involved in the transaction transfer receives a portion of the transaction fee. In addition, the combination of incentives and intelligent routing can reduce communication and storage costs.

4 Challenges and Opportunities

Conventional IP network architecture can only met the demand of end-to-end data transmission. Its inconsistency causes many problems. And the exchange of data between various types of networks suffers most. The Internet with TCP/IP as its core is confronted increasingly serious technical challenges, exposing inadequacy in terms of scalability, security, reliability, flexibility and mobility. Blockchain is not an original technological innovation, but an alloy of P2P networking, digital encryption and distributed storage. In the existing network architecture, there are identity being bound to location, control being bound to transmission and security (identity) being unbound to data. The merit of the blockchain lies on that the network is equipped with the freedom to get real data, value, identity, and transaction which is credible, distinguishable, and traceable meanwhile. This is the advanced nature of the network architecture, and it is a new economic model from the data value level.

Although the text above divide the incentive into the issuance of token and allocation on the basis of the focus of previous work, the two segments are both indispensable and run jointly. For conducting solid reform on economic structure, the incentive still requires research on these fields: 1. To build quantified link between data and its value. With the support of economics and Game Theory, data value can become market-oriented. 2. To study the incentive on basis of consensus compatibility that works as its indispensable core [15]; 3. Based on the mathematics, to quantify token allocation in a fine-grained path and to balance the fairness stimulus brought by random fators and the rule-guided consensus orientation.

Research on the incentive of blockchian is still in primary stage and confronted various challenges in noted areas including evaluation on data value, the balance between random factors and allocation rules, and how to conduct valid confirmation with real transaction data still inadequate in the system [12]. It is hoped that more favorable results can be worked out with the improvement of blockchain and network structure and increasing emergence of real data. Integrating old-fashion technologies, blockchain is illuminating the future.

5 Conclusion

This paper starts with the novel economic organization model in the era of digital economy and focuses on the objectives and existing researches on the incentive layer of the blockchain. For the incentive, it begins with

the three aspects that the network pays most attention to: calculation, storage and transmission, introduces cases on the token issuance , analyzes how the issuance impacts the orientation of the blockchain application, and illustrates the optimization on the distribution and rationalization mechanism. Finally, we illustrates that the research on the blockchain incentive is still in a primary stage and look into possible developments, opportunities and challenges of future research, hoping to provide reference and ideas for the later research.

Reference

1. Andrychowicz, M., Dziembowski, S., Malinowski, D., Mazurek, L.: Secure multiparty computations on bitcoin. In: Security Privacy. pp. 76–84 (2014)
2. Anjana, P.S., Kumari, S., Peri, S., Rathor, S., Somani, A.: An efficient framework for concurrent execution of smart contracts (2018)
3. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: International Conference on Principles of Security and Trust. pp. 164–186 (2017)
4. Babaioff, M., Dobzinski, S., Oren, S., Zohar, A.: On bitcoin and red balloons. In: ACM Conference on Electronic Commerce. pp. 56–73 (2012)
5. Castro, M., Liskov, B.: Practical byzantine fault tolerance. pp. 173–186 (1999)
6. Davidson, S., De Filippi, P., Potts, J.: Economics of blockchain. Social Science Electronic Publishing (2016)
7. Doan, A.H., Ramakrishnan, R., Halevy, A.Y.: Crowdsourcing systems on the world-wide web. Communications of the Acm **54**(4), 86–96 (2011)
8. Ersoy, O., Ren, Z., Erkin, Z., Lagendijk, R.L.: Transaction propagation on permissionless blockchains: Incentive and routing mechanisms. In: CRYPTO Valley Conference on Blockchain Technology (2018)
9. Eyal, I., Gencer, A.E., Renesse, R.V.: Bitcoin-ng: a scalable blockchain protocol. In: Usenix Conference on Networked Systems Design and Implementation. pp. 45–59 (2016)
10. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: International Conference on Financial Cryptography and Data Security. pp. 436–454 (2014)
11. Feng, Y.U.: Research on it architecture of large-scale securities centralized transaction system. Computer Engineering **32**(9), 247–250 (2006)
12. Gervais, A., Karame, G.O., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: ACM Sigsac Conference on Computer and Communications Security. pp. 3–16 (2016)
13. He, Y., Chen, M., Ge, B., Guizani, M.: On wifi offloading in heterogeneous networks: Various incentives and trade-off strategies. IEEE Communications Surveys Tutorials **18**(4), 2345–2385 (2016)
14. He, Y., Li, H., Cheng, X., Liu, Y., Yang, C., Sun, L.: A blockchain based truthful incentive mechanism for distributed p2p applications. IEEE Access **PP**(99), 1–1 (2018)

15. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In: International Cryptology Conference. pp. 357–388 (2017)
16. Kittur, A., Chi, E.H., Suh, B.: Crowdsourcing user studies with mechanical turk. In: CHI '08 Proceeding of the Twenty-Sixth Sigchi Conference on Human Factors in Computing Systems. pp. 453–456 (2008)
17. Kokoriskogias, E., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., Ford, B.: Enhancing bitcoin security and performance with strong consistency via collective signing. Applied Mathematical Modelling **37**(8), 5723–5742 (2016)
18. Kumar, K., Lu, Y.H.: Cloud computing for mobile users: Can offloading computation save energy? Computer **43**(4), 51–56 (2010)
19. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., Zhang, Z.: Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems **19**(7), 2204–2220 (2018)
20. Luu, L., Teutsch, J., Kulkarni, R., Saxena, P.: Demystifying incentives in the consensus computer. In: ACM Sigsac Conference on Computer and Communications Security. pp. 706–719 (2015)
21. Modiri, N.: The iso reference model entities. IEEE Network **5**(4), 24–33 (2002)
22. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Consulted (2008)
23. North, D.: Transaction costs, institutions, and economic performance. ICS Press
24. Okada, H., Yamasaki, S., Bracamonte, V.: Proposed classification of blockchains based on authority and incentive dimensions. In: International Conference on Advanced Communication Technology. pp. 593–597 (2017)
25. Sompolinsky, Y., Zohar, A.: Secure high-rate transaction processing in bitcoin **8975**, 507–527 (2015)
26. Wang, Y., Cai, Z., Yin, G., Gao, Y., Tong, X., Wu, G.: An incentive mechanism with privacy protection in mobile crowdsourcing systems . Computer Networks **102**, 157–171 (2016)
27. Williamson, O.E.: The economic institutions of capitalism. firms, markets, relational contracting. Social Science Electronic Publishing **32**(4), 61–75 (1998)
28. Yuan, Y., Wang, F.Y.: Blockchain: The state of the art and future trends. Acta Automatica Sinica (2016)
29. Yuan, Y., Wang, F.Y.: Towards blockchain-based intelligent transportation systems. In: IEEE International Conference on Intelligent Transportation Systems. pp. 2663–2668 (2016)
30. 弗里德里希 · 冯 · 哈耶克: 货币的非国家化. 新星出版社 (2007)
31. 王晟: 区块链式法定货币体系研究. 经济学家 **9**(9), 77–85 (2016)
32. 祝烈煌, 高峰, 沈蒙, 李艳东, 郑宝昆, 毛洪亮, 吴震: 区块链隐私保护研究综述. 计算机研究与发展 **54**(10), 2170–2186 (2017)
33. 袁勇, 王飞跃: 区块链技术发展现状与展望. 自动化学报 **42**(4), 481–494 (2016)