Journal of Digital Convergence
Vol. 16. No. 8, pp. 193-200, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.8.193

Blockchain Evaluation Indexes and Methods to Vitalize a Blockchain-based Digital Sharing Economy

Il-Gu Lee
Assistant Professor, Department of Convergence Security Engineering, Sungshin University

블록체인 기반 디지털 공유경제 활성화를 위한 블록체인 평가지표 및 평가방법에 대한 연구

이일구
성신여자대학교 융합보안공학과 조교수

Abstract Recently, there are high expectations of a society benefitting from a digital sharing economy. However, to establish a digital sharing economy, one needs to first create a reliable social structure. Transparency is recognized as the most important measure of value in not just politics or economics, but also in all domains of our lives. Although all nations strive to create "societies based on credit and trust," in truth, rigidity, irregularity, corruption, and inefficiency are widespread in all aspects of society. Thus, there is a growing interest in blockchain technology, also called the "second Internet revolution," seeking trust in digital environments, although it is difficult to obtain trust in such environments. However, the principles and methods of evaluating blockchain technologies are still unclear and not standardized. This study addresses the evaluation indexes such as transaction per second, maximum data size per one transaction, accuracy and blockchain technology application methods in the digital sharing economy and suggest ways to safely vitalize a blockchain-based digital sharing economy.

Key Words : Blockchain, Evaluation indexes, Evaluation method, Digital sharing economy, Vitalization strategy

요 약 최근 디지털 공유 경제가 사회에 가져다 줄 혜택에 대한 기대가 높다. 디지털 공유 경제가 정착되려면 신뢰할 수 있는 사회 구조가 우선 마련되어야 한다. 투명성은 정치나 경제 영역뿐 아니라 우리 삶의 모든 영역에서 가장 중요한 가치 척도로 인정받고 있고, 모든 국가가 '신용과 신뢰기반의 사회'를 지향하지만 현실 사회 곳곳에선 불투명과 부정·비리·비효율이 만연해 있다. 그러므로 신뢰하기 어려운 디지털 환경에 신뢰를 구축하기 위해 '제2의 인터넷 혁명'으로 불리는 블록체인 기술에 대한 관심이 고조되고 있다. 그러나 아직도 블록체인 기술을 평가하는 기준과 방법이 명확하지 않고 표준화되어 있지 않다. 본 연구에서는 디지털 공유 경제에 블록체인을 활용하기 위한 처리속도, 데이터량, 정확도 등의 블록체인 평가지표와 평가방법을 짚어보고, 블록체인 기반의 안전한 디지털 공유 경제 활성화 방안을 제시한다.

주제어 : 블록체인, 평가지표, 평가방법, 디지털 공유경제, 활성화 전략

1. Introduction: Digital Sharing Economy

Which is cleaner, a public bathroom or a private bathroom? The obvious answer to this question confirms the so-called tragedy of the commons, which states that "public goods that can be used by everyone

*This work was supported by the Sungshin University Research Grant of 2018-1-29-015/1
-본 연구는 성신여자대학교 연구과제 (2018-1-29-015/1) 지원으로 수행하였음.
*Corresponding Author : Il-Gu Lee (iglee@sungshin.ac.kr)
Received June 11, 2018 Revised July 2, 2018
Accepted August 20, 2018 Published August 28, 2018

at no cost will be soon destroyed" [1]. This is an unfortunate case where, as a result of every individual doing their best for their own benefit, there is total destruction.

Privatization, the recognition of private property rights, is one way to solve the tragedy of the commons problem. In this structure, every individual marks their property, manages it, and takes all the benefits that arise from it. Private property is the foundation of capitalism.

However, privatization cannot solve all problems. Privatization has led to imbalances and unequal social structures in the world, where, the more you have, the more the power and wealth you accumulate. This is the so-called tragedy of privatization [2]. Individuals do their best for personal benefit, but, ultimately, this renders society more unstable. The government has strengthened its management and imposed regulations in an effort to solve the tragedy of the commons and tragedy of privatization problems, but the results are not satisfactory.

Will the digital economy, which has grown beyond the analog economy, be able to solve these issues?

Initially, the vision for the Internet was, "free and equal use of information and secure sharing through perfect decentralization." However, the tragedy of the commons problem arose here as well. Because forgery is easy and duplication can be freely implemented digitally, false information has increased and distortion has worsened.

The tragedy of privatization occurred as well. The cross-border digital economy has created an imbalance that is more severe than that in the offline economy [3, 4]. All power is concentrated with those having data and technology. They monitor those who do not have data and technology and this has affected freedom and rights. The speed and level of power concentration and pursuit of self-interest have become much faster and worse than those in the offline economy.

As futurist Jeremy Rifkin has stated, "the age of ownership has gone, and we have entered the age of the shared economy" [5]. A sharing economy has been recently gaining attention as a potential solution to the tragedy of the commons and tragedy of privatization problems brought on by the digital economy [6]. Can a sharing economy solve these issues?

In this study, we apply blockchain technology to vitalize the digital sharing economy and the evaluation indexes and suggest some blockchain technology methods. In Chapter 2, we explain blockchain-based smart contracts and the digital sharing economy. Chapter 3 suggests some evaluation indexes and methods of blockchain technology, while Chapter 4 suggests methods that can safely vitalize the blockchain-based digital sharing economy. Finally, Chapter 5 concludes the study.

2. Standardization of Blockchain evaluation indexes and methods

Traditional technologies are often replaced by disruptive innovation technologies. However, innovation technology can be complementary to traditional technologies and pave the way for mutual growth. Blockchains are such a path for mutual growth and can become an innovative technology for shared growth.

First-generation blockchains were designed with heavy focus on autonomy rather than effectiveness. Therefore, it is difficult to apply them to large transactional systems. An increase in number of blockchain participants can lead to improved security, but as the volume of transactions increases, more time would be required to reach an agreement. As of now, it is difficult to apply blockchain technology to services that require speed. Because blockchains are connected in a series like a chain, it is slower than traditional centralized servers, which can implement parallel transactions.

Centralized relational databases and blockchain-distributed ledgers have advantages and disadvantages that complement each other.

For the blockchain to function as an actual "circulatory system," tremendous effort needs to be put in, not unlike how the WiFi evolved over 20 years through numerous version upgrades.

Thus, blockchain technology is considered to be the second industrial revolution, which will change the existing paradigm and order. However, the blockchain revolution will be a challenge until the resulting technical, managerial, and legal limitations are overcome.

Technically, there are no international standards for blockchain data and service compatibility, and therefore blockchains are inefficient in terms of user convenience and development verification costs. Furthermore, although the security of virtual money is excellent, there are no protective devices for individual users and exchanges. Not many specialists have a high understanding of blockchain technology, and there is a need to improve the security consciousness of users and administrators. The current laws and policies do not clearly define the roles and responsibilities of blockchain technologies in terms of effects of distribution systems, where participants are the main agents. Furthermore, the obligation to destroy transactional records and information protection regulations, such as the Financial Transaction Act, the Credit Information Act, and the Personal Information Protection Act, is difficult to apply to blockchains, where it is impossible to cancel or correct data recorded on the block and transparent data sharing is a key characteristic.

The competition to develop blockchain technology is accelerating domestically and internationally, but the technology is still in the introductory stage. Thus, for our country to be a leader in the blockchain global market, our current technological, managerial, and legal limitations must be addressed and we must have strategies to develop differentiated blockchain technology for the intelligent Internet of Things (IoT) platform, which is frequently used in the main industrial sectors.

The "Public Key Infrastructure" used in blockchain technology follows an old encryption model. In other words, it is sufficiently verified since it has already been applied in many sectors. In fact, the key to innovation in blockchain technology is the establishment of a "trust network" that can combine the well-known cryptography (public key cryptography), game theory (Byzantine Generals Problem), and software engineering (distributed policy).

Experts argue that the greatest advantage of the blockchain is that "it is impossible to be tampered with" and "almost impossible to hack." Encryption technology is largely responsible for this evaluation. "Reliability is determined by a mathematically proven method through coding, and the robustness of verification is enhanced through strong encryption."

Thus, the blockchain sends money or data to the address created using the public key, digitally signs it with a secret key, and then notifies all of the blockchain network participants of the transfer of ownership, but the individual who used the public and secret key cannot be identified. The fact that an unidentified someone has sent a certain amount of money to someone else is transparently publicized, but the personal information of the parties to the transaction is not disclosed.

Furthermore, as long as you have the individual key to verify the public key and ownership rights that act as the account address, a transaction is possible anywhere and anytime. Every time a transaction is made, if a new public key and secret key pair is generated for the transaction, it would be difficult to find the correlation of each transaction. Thus, it is also used as a means of black market payment, such as ransom for Ransomware or the sale of drugs or illegal weapons.

This does not mean that virtual currency trading can hide behind complete anonymity by using blockchains. It can be traced from the recorded IP address used in the process. However, tracing can be difficult if several IP addresses are used or if the IP address used is

hidden during the transaction. In any case, this is not impossible.

Furthermore, a blockchain itself can guarantee perfect anonymity, but because the exchange account uses real names, complete anonymity is impossible. If one can find the blockchain transaction address associated with an exchange account used by a criminal suspect and the transaction information within the exchange, it would be possible to find the transaction amount recorded in the blockchain. If the stock exchange is hacked, the anonymity of the blockchain would be disabled, and because of transparency, all transactions may pass to the hacker.

Many scientists foresee the blockchain as a disruptive innovation surpassing the potential impact of the Internet on our lives and all industries [7]. If the problem of data monopolization could be solved through the Internet revolution, the problem of trust can be solved by making all data transparent through the blockchain revolution, at the same time improving anonymity and minimizing the unnecessary disclosure of personal information.

However, the transparency and anonymity of blockchains can be misused in crime or abused by influential organizations, and, in the process, there could be well-intentioned victims. If the blockchain is to be used to create a more convenient and safe Internet world, we need the technology to quickly and accurately seek out the criminal activities that are growing by the day and the technology to allow individuals to identify and manage their personal information as well as tracking usage.

3. Ways to vitalize a blockchain-based secure digital sharing economy

3.1 Vitalization of the digital sharing economy by building a blockchain-based FinTech environment

Blockchain technology has been very actively introduced in the FinTech sector. FinTech is the combination of “finance” and “technology.” A new paradigm differentiated from the traditional financial service has been provided by combining financial services and IT technology. Electronic currency, electronic payment systems, financial investment platforms, etc., which began in the remittance, payment, and investment sectors, are now affecting our everyday lives.

FinTech, along with blockchain technology, is the focus in the financial market today. Kakao Bank began FinTech services as Internet banking in July 2017, opening 5 million accounts within the first 6 months [8]. Their international remittances are quite popular, reaching almost 76,000 transactions [9]. The success of Kakao Bank brought the “catfish effect” to the existing financial market, and banks are now busy updating the user interface of their mobile financial applications (app), improving the ease of use, and lowering their interest rates and fees.

What were the consumer complaints against financial services? The world has moved quickly into the high-speed mobile era, whereas financial services are still locked in a closed and rigid old-fashioned infrastructure. Each use takes a lot of time, involves complicated procedures, and overall everything is inconvenient and the threshold is high. Banks force customers to choose either “security” or “convenience.” If you chose security, you need to go through several steps, such as a passwords, graphic authentication, security card, SMS, ARS, and OTP, all for security reasons. If you require quick and convenient transactions, you are left with “weak security.” Furthermore, you have to pay high fees every time you transferred funds to another bank, sent money abroad, used the ATM, etc. Even if you tried to use the latest financial app on your smartphone in a high-speed Internet network, you are stuck in the large and outdated financial core system of the financial infrastructure and a lot of time is required to complete a transaction.

Behind Kakao Bank's popularity were the customers' complaints. Kakao Bank provided both security and convenience. Their essential security technologies were internalized for easier use, and they chose private certification over accredited certification. Certification was saved in the security hardware domain and hacking became difficult. Because security functions operate organically within the system, users face no inconvenience at all.

The key is to develop technologies that maximize convenience but maintain security based on minimum security features that are essential from the early days of product and service development. While the loan interest rates and fees were lowered, the deposit interest rates were raised. Kakao Bank allowed money to be sent with just a few items of information about the receiver along with Kakao Talk. Thus, Kakao Bank could provide a new alternative to the existing banks.

However, does that mean that the procedure of Kakao Bank is perfect?

No doubt the procedure of Kakao Bank is more convenient and faster than those of existing banks. However, the bank still has the fundamental drawbacks of a centralized system. In many situations, it was difficult to guarantee stable service quality as use increased exponentially. There is also a limit to continual innovation in the existing financial system that closely follows every innovation.

When data is centralized, security issues become very important and vulnerable. Serious malfunctioning and performance degradation of the central server have a huge impact on the entire network. In the IoT financial transaction environment that is soon to arrive, centralized systems will be expensive, inconvenient, and vulnerable.

Eventually, the centralized FinTech technology will find it increasingly difficult to ensure stable and effective financial transactions in the era of Big Data and IoT. Leading companies in FinTech are aware of these limitations, and research is underway to internalize next-generation security technologies, such as blockchains, in FinTech technology. Financial experts predict that the "era of FinTech 2.0, which uses blockchain technology" will fundamentally change the infrastructure of the financial services industry.

The blockchain-based FinTech platform can solve the constraints of the existing FinTech with a distributed financial system approach. Most financial transactions in the blockchain-based distributed FinTech will not require the other person's personal information or credit information. The data of all transactions will be recorded in the distributed ledger and forgery will be impossible. Because blockchains have no national boundaries, global interoperability is possible and funds can be transferred at a low fee. Furthermore, in the past, banks were at the center of loans, but in the future, individuals will be able to make loans safely and cheaply (peer to peer), and cloud funding can be done quickly and effectively.

In the blockchain-based FinTech environment, consumption behavior will not be different from production behavior. Any information generated during product use will be recognized as an asset of the buyer. Any processed information that cannot be identified as personal data is automatically delivered to a third party, and a value will be returned in cryptocurrency in real time. If you are not using Internet devices that collect or relay data, such as sensors and WiFi, you will be able to automatically rent it to the public and collect rental income in real time.

In the IoT era, things with intelligence are paid in accordance to a program under the smart contract. Currently, we use automatic payment systems programed like an automatic vending machine, but the scope of use and the subject of financial actions will depend on the IoT.

Blockchain technology is necessary for financial innovation, but it is like a piece in a puzzle that is missing. Blockchain technology provides security, transparency, trust, global interoperability, low fees, and high-speed requirements, all absolutely necessary to successfully commercialize FinTech and Internet

technologies in distributed networks. Bill Gates, the creator of Microsoft, predicted that "FinTech and blockchain technology will threaten banks' profitability models and narrow banks' positions," and that "finance is necessary, but banks will disappear" [7, 10]. It seems that his predictions could become reality soon. The blockchain-based FinTech technology will first supplement deficiencies rather than replace the financial system all at once. However, we expect the financial paradigm to change as our forces expand into differentiated areas.

In order to use Blockchain technology for digital sharing economy, transaction per second and maximum data size per one transaction are important parameters as shown in Table 1 because scalability has been an critical issue with crypto currencies when they are applied for FinTech. Payment network of Visa achieved 4,000 peak transactions per second on its network, and average around 2,000 transactions per second [11]. It has a peak capacity of aroun 56,000 transaction per second. Transaction throughput is limited by block size. Furthermore, O2O (online-to-offline) authentication error rate and Bio-metric generation accuracy are required for secure usage of Blockchain [12, 13].

Table 1. Blockchain Evaluation Indexes

Index	Unit	Requirement examples
Transaction per second	TPS	>5,000
Maximum data size per one transaction	Giga Bytes (GB)	>20
Channel latency	ms	100
O2O authentication error rate	%	<3%
Bio-metric generation accuracy	%	>95%

3.2 Blockchain-based secure digital sharing economy framework

It is difficult for digital contracts written in a program to have legal status[14]. At the current technology level, it could be difficult to perfectly program all the complicated and subtle relationships between people in a digital contract. However, this problem can be solved if Artificial Intelligence (AI) is used to develop and adjust the terms of the contract to suit the trading partner and mediate subtle conflicts [15].

Furthermore, for building the smart contract platform, we need secure coding and security internalization of decentralized applications. If the coding is not secure or security is not internalized, reverse engineering might attack the weak points of the distribution app. Furthermore, the hacker may find out the malfunction patterns of the distribution app through fuzzing and neutralize the system.

The smart contract is a technology with potential to combine blockchains and create tremendous added value. In order to maximize the conveniences and efficiencies that smart contracts can bring in, we need to improve the legal status of digital contracts and develop secure distributed application technology with security internalization.

The blockchain can thus serve as a ladder to overcome the many barriers that the digital economy faces. Ultimately, the digital economy will overcome the limitations of the offline economy, and the tragedy of the commons and tragedy of privatization problems of the digital economy will be solved by a shared economy. Furthermore, the blockchain can be a breakthrough for the shared economy.

In particular, if blockchains are applied to the Internet, the ownership of all transaction data will become transparent, forgery will become impossible, and one will be able to record and track forgery and falsification. Also, smart contracts will enable the transfer of ownership and permission for use, and the compensation that follows can be provided clearly. Currently, various attempts are underway and it is expected to soon have open platforms to implement knowledge sharing, such as Wikipedia, open source software, and Linux, as a blockchain.

We can build an objective reputation measurement system that can improve the quality and accuracy of information provided by the open platform participants.

For example, a sponsor may grant an amount to an escrow (separate) account, and a participant may create a system to increase the number of blockchain accounts while building reputation. Then, the position of the participants who fabricate information will naturally decrease, and the contribution to community development will increase reputation and rewards.

Furthermore, if blockchain technology is applied, the personal information included in Big Data can be accessed only by the owner of the data with a private key. Anyone can see the contents of the blockchain, but anonymity is maintained. The pursuit of gains by individuals will maintain public value and improve the efficiency of the whole group. As the blockchain community grows, diversifies, and becomes complicated, public value will become greater and more secure, and this will lead to an ideal mechanism where an individual's selfish efforts will naturally lead to high efficiency of the whole group.

4. Conclusion

Sharing economy creates new markets and products [16, 17], and digital sharing economy has been powered by digital technologies. Blockchains are evolving into personalized, programmable enterprise systems for transaction authentication in an open public mechanism such as the bitcoin. In the future, blockchains will evolve like an innovative object-oriented Internet platform that combines with distributed computing technology using the cloud to meet the various IoT requirements and constraints[18, 19]. Furthermore, once the blockchain is fully internalized on the IoT, it can become a key technology that drives key industries such as public infrastructure, finance, communications, health care, transportation, trade, and energy.

Blockchains secure the ownership rights of data and everyone has the equal opportunity to use data through sharing. An equitable reward distribution is also possible. Blockchains break up rights through a distribution network not controlled by anyone and allows for economic gains and technical convenience to reach not just a small group of people, but everyone. We anticipate blockchain technology to become a key factor in actualizing a digital sharing economy and distributed capitalism, which could not be created under the traditional capitalism and the Internet.

It is only a matter of time for true sharing economy platforms like Uber and Airbnb to emerge. As further work, blockchain models will be implemented and demonstrated in an emulation testbed with the suggested evaluation indexes.

REFERENCES

[1] O. Elinor. (2008). The New Palgrave Dictionary of Economics: Palgrave Macmilan.
DOI : 10.1057/9780230226203.1729.

[2] B. Wade. (2005). A New Tragedy for the Commons: The Threat of Privatization to National Parks (and Other Public Lands), *The George Wright Forum, 22(2).*

[3] R. Iannela. (2017). Tragedy of the Digital Commons: Amplified Zombies, *IEEE Technology and Society Magazine, 36(3).*
DOI: 10.1109/MTS.2017.2738081

[4] U. Huws. (2015). iCapitalism and the Cybertariat Contradictions of the Digital Economy. *Monthly Review, 66(8),* 42-57.
DOI : 10.14452/MR-066-07-2015-01_7

[5] J. Rifkin. (2000). The Age of Access: The New Culture of Hypercapitalism. *Penguin Putnam.*

[6] J. Hamari, M. Sjoklint & A. Ukkonen. (2016). The Sharing Economy: Why People Participate in Collaborative Consumption, *Journal of the Association for Information Science and Technology, 67(9),* 2047-2059.
DOI : 10.1002/asi.23552

[7] D. Tapscott & A. Tapscott. (2016). Blockchain Revolution: How the Technology Behind Is Chaining Money, Business, and the World, Portpolio.

[8] N. Y. Kwak, H. Yoo & C. C. Lee. (2018). Study on Factors Affecting Financial Customer's Switching Intention to Internet only bank: Focus on Kakao bank. *Journal of Digital Convergence, 16(2),* 157-167.

[9] Kakao bank report 2017. kako website. https://www.kakaobank.com/Corp/IR/Announcement/Business/pages/1 (last access: 2018.05.22.)

[10] A. Machenzie. (2015). The Fintech Revolution, *London*

Business School Review, 26(3), 50-53.

[11] Bitcoinwiki. https://en.bitcoin.it/wiki/Scalability (last access: 2018.05.22.)

[12] L. Fridman, S. Weber, R. Greenstadt & M. Ka. (2017). Active Authentication on Mobile Device via Stylometry, Application Usage, Web Browsing, and GPS Location, *IEEE Systems Journal, 11(2),* 513-521.

[13] J. R. Pinto, J. S. Cardoso, A. Lourenco & C. Carreiras. (2017). Towards a Continuous Biometric System Based on ECG Signals Acquired on the Steering Wheel, *MDPI Sensors, 17(10).*

[14] M. Giancaspro. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective, *Computer Law & Security Review, 33(6),* 825-835.

[15] Y. P. Lin, J. R. Petway, W. Y. Lien & J. Settele. (2018). Blockchain with Artificial Intelligence to Efficiently Manage Water Use under Climate Change, *MDPI Environments, 5(3).*

[16] J. Y. Yoon & S. I. Kim. (2017). A Study on Development of Fashion Sharing Platform for Shared Economy - Focusing on fashion rental service case, *Journal of the Korea Convergence Society, 8(7),* 199-205.

[17] S. H. Kim & D. M. Lee. (2018). A study on the ways for differentiation of domestic car sharing service, *Journal of the Korea Convergence Society, 9(3),* 181-186.

[18] S. Hong & S. Park. (2017). The Research on Blockchain-based Secure IoT Authentication, *Journal of the Korea Convergence Society, 8(11),* 57-62.

[19] S. Hong & S. C. Rong. (2018). Developing a Blockchain based Accounting and Tax Information in the 4th Industrial Revolution, *Journal of the Korea Convergence Society, 9(3),* 45-51.

이 일 구(Lee, Il-Gu) [정회원]

- 2003년 2월 : 서강대학교 전자공학과 (공학사)
- 2005년 2월 : 한국과학기술원 정보통신대학원 (공학석사)
- 2012년 2월 : 한국과학기술원 지식재산대학원 (경영학석사)
- 2016년 2월 : 한국과학기술원 정보보호대학원 (공학박사)
- 2017년 2월 ~ 현재 : 성신여자대학교 융합보안공학과 조교수
- 관심분야 : 정보통신, 정보보호, 지식재산
- E-Mail : iglee@sungshin.ac.kr