

Blockchain-based Lightweight Transaction Process Modeling and Development

Tae-Shin Kang**, Moon-Il Joo*, Beom-Soo Kim*, Tae-Gyu LEE**

* Institute of Digital Anti-Aging Healthcare, Inje University, Korea; cmki@nate.com

** Pyeongtaek University, 3825 Seodong-daero, Pyeongtaek-si, Gyeonggi-Do 17869, Korea

Corresponding Author: tglee@ptu.ac.kr, Fax: +82 31 659 8011, Tel: +82 31 659 8370

Abstract— Recently, blockchain systems are being applied in various application fields by combining blockchain with existing legacy systems. In particular, the cryptocurrency payment transaction system to support digital financial transactions is emerging as an important issue. Nevertheless, the development and valuation of blockchain-based cryptocurrency transactions and application services are fluctuating. With the advent of the Untact era due to Covid-19 recently, the commercialization of cryptocurrency is becoming more focused. In addition, as technical constraints for the spread of commercialization, there are problems of reaching a fast consensus in a large-scale blockchain network, consuming excessive energy for calculation, and storing the entire blockchain for verification. We propose a lightweight blockchain transaction process modeling to overcome these problems and to enhance blockchain applicability in an application environment where computing resources are weak. In addition, we propose a lightweight transaction-based blockchain application model optimized for areas with weak computing and network resources such as vending machines and ATMs.

Keywords— Blockchain, Cryptocurrency, Lightweight Transaction, Distributed Process, Vending Machine

I. INTRODUCTION

Since Satoshi Nakamoto proposed Bitcoin, there is active research in various fields to converge with blockchain technology [1]. Active research is being conducted in areas such as application in financial application system [2] and development and establishment of fair electronic election system [3]. These studies focus on how to combine blockchain technology with existing systems rather than focusing on the application process of blockchain-based cryptocurrency, which is the background of the original blockchain's appearance in various fields. Nevertheless, there are many technical challenges to overcome in order to apply cryptocurrency to real life. In order to continuously strengthen the scalability of blockchain applications, it is necessary to ensure the rapid and stable operation of the blockchain in an embedded environment where computing resources are weak. Many studies are being conducted to optimize the resource consumption of the blockchain. For example, K. Karlsson proposed Vegvisir, a DAG-structured blockchain that allows branching suitable for a power-limited environment with limited network connectivity [4]. Ellul et al proposed AlkyVM, a partitioned virtual machine that can integrate devices with blockchain technology [5].

However, these proposed systems are insufficient to lighten the resource consumption of the blockchain system [6].

The problems we face in applying blockchain and cryptocurrency to real life can be summarized into four issues as follows.

First, since the operation of mining blocks can bring profits such as mining rewards and fees, nodes with abundant capital continuously improve computing power, but most of the participants cannot keep up with the change in computing power. The longer the blockchain, the more centralized the computing power of the P2P network. This increases the cost of creating blocks, so the value of the cryptocurrency to be mined will increase due to environmental and technical factors.

Second, in order for the blockchain to achieve decentralized consistency, individual nodes must preserve large amounts of block data generated by numerous network participants. All past data will be permanently stored locally without compression, requiring large storage space.

Third, in order to feel the advantage of using cryptocurrency from the user's point of view, it must have at least the same convenience and processing speed as existing payment methods. In other words, the speed at which the user perceives that the transaction has been normally processed must be fast. The average time that a transaction is processed normally in Bitcoin is 60 minutes, which can be fatal in application services that need to react immediately.

Fourth, in order to improve the centralization of the value of coins, if the generation cycle of coins is excessively shortened, the number of orphan blocks increases and the stability of the blockchain system can be drastically reduced.

In this paper, in order to overcome the above-described problems, we propose a *lightweight transaction* concept that ensures the normal operation of the blockchain process even in low-performance devices by minimizing the use of system resources between the blockchain and nodes. In addition, a new coin parameter based on lightweight transaction is designed to be applied to various blockchain application systems. The *lightweight transaction* dualizes the blockchain model to form a lightweight blockchain without mining on the lightweight node network, collects transactions occurring in participating lightweight nodes, and broadcasts a new set of lightweight blocks collected on the heavyweight blockchain on a regular basis. This process can improve the resource and speed constraint problems of each of the second and third presented

Satoshi to achieve consistency and security in a blockchain network. Participating nodes solve complex puzzles such as calculating a hash value less than a randomly changing target value. It is a system that competes for. Nodes that have solved the computing problem wait for verification of other nodes before adding blocks to the existing blockchain. At this time, if several nodes cause a fork in the network, more than one valid block may be generated. In such cases, both are allowed, which leads to the branching of a single chain. However, since all nodes adopt the method of accommodating the longest chain, the lifespan of some forked nodes is short and does not significantly affect the blockchain consensus algorithm [11]. The coin proposed in this paper also uses a consensus algorithm of the proof-of-work method.

III. MODELING AND DEVELOPMENT OF LIGHTWEIGHT TRANSACTION ARCHITECTURE

There are two main contents described in this chapter. First, it describes what lightweight transaction is and how to lighten the transaction. Second, we propose a new coin based on lightweight transaction architecture to secure the problems of existing cryptocurrency.

A. Modeling of lightweight transaction architecture

The purpose of this study is to make the blockchain network operate normally even in an embedded environment with poor computing resources.

The embedded environment has poor computing power and cannot use a large-scale storage space, so the existing blockchain model cannot be applied as it is. The lightweight transaction architecture proposed in this paper dualizes the blockchain model to maintain the verification of the blockchain while reducing the weight of the blockchain. The dualized blockchain model is defined as a lightweight blockchain and a heavyweight blockchain, respectively, and the heavyweight blockchain has the same logic as the existing blockchain model. A lightweight blockchain is formed between each lightweight node, and a heavyweight blockchain is formed between normal nodes with power computing.

Lightweight blockchain does not perform mining to verify generated blocks, and each lightweight participating node collects transactions that occur between nodes inside the lightweight blockchain network. The nodes in the lightweight blockchain also form a blockchain network that contains the hash value of the previous block in the current block, so it is possible to guarantee the integrity corresponding to transaction forgery. Even if it is not synchronized with the heavyweight blockchain in real time, transactions within the lightweight blockchain are performed normally. Lightweight nodes regularly broadcast the collected transactions to the heavyweight blockchain, and light weight blocks are verified by participating nodes. Normally verified lightweight blockchain transactions can be deleted from the lightweight blockchain after a certain period. Even if a lightweight transaction is deleted on the lightweight blockchain, the original transaction cannot be forged anymore because the transaction has been verified and reflected normally in the

heavyweight blockchain. Therefore, even if the storage space of the system running the lightweight blockchain is not large, normal transaction processing can be guaranteed.

Heavyweight blockchain performs the same functions as existing blockchain systems. The difference from the existing model is that branching and combining modules are added to communicate with the lightweight blockchain.

The operation process of the lightweight blockchain transaction is as follows. First, the initial block of the lightweight blockchain branches off and receives the last verified block of the heavyweight blockchain network. Second, transactions occurring in the lightweight blockchain network are sequentially collected and stored in a lightweight block. Third, when the number of blocks of the lightweight blockchain is more than a certain number or the execution time of the lightweight transaction reaches the synchronization time limit, the blocks of the lightweight node are broadcast to the heavyweight blockchain to join the blockchain network. Fourth, in the heavyweight blockchain, if the blocks of the lightweight blockchain are properly verified and reflected, all blocks in the lightweight blockchain are deleted after a certain period of time, and the subsequent lightweight blockchain creation process is continuously performed. Figure 3 shows a lightweight transaction-based blockchain structure.

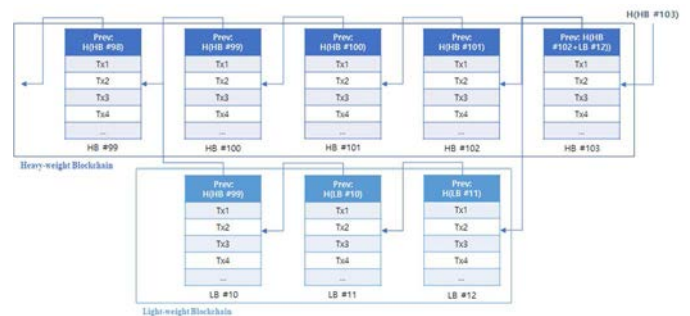


Figure 3. Lightweight transaction based blockchain structure

B. Lightweight transaction architecture based new coin: PTC

A newly created coin based on a lightweight transaction architecture is designed by changing some of the heavy parameters used in existing Bitcoin. There is already a Litecoin that has been distributed with several modifications to the part that was pointed out as a problem in Bitcoin's Coinbase. Litecoin adopts the scrypt algorithm [12], not the SHA-256 algorithm as a mining algorithm and is characterized by lower block generation time and lower power consumption than the SHA-256 algorithm. In addition, the maximum issuance of coins is 4 times that of Bitcoin. The new coin accepts part of Bitcoin and Litecoin, and the part that does not match the lightweight transaction of the new coin is designed by improving it. The direction of the new coin based on lightweight transaction is as follows.

1) **Low unit amount:** The value of the unit amount of the new cryptocurrency must be low. For example, if the new unit of money is called PTC, 1PTC should be close to 1 dollar. To

realize a low unit amount, the block reward must be set high, and the total issuance of coins must be increased.

2) **Fast transaction time:** For new cryptocurrencies, the transaction time should be close to the credit card approval time. However, if the block creation time is too shortened, the stability of the blockchain system due to the Fork problem is degraded, so it is impossible to recklessly reduce the time. Therefore, within the range of stable operation of the blockchain logic, the block generation cycle is set short, and the shortcomings are handled using smart contract technology. The smart contract is a technology also called blockchain 2.0 and was proposed by Nick Szabo. Nick Szabo defines “smart contracts to formulate and secure relationships through public networks by combining protocols, user interfaces and promises expressed through interfaces” [13].

When the buyer succeeds in a double payment attack by writing a script that transfers the price of goods from the buyer's wallet to the seller's wallet using smart contract technology, the block containing the normal transaction is an orphan block. When this happens, the smart contract works, preventing the seller from getting money. Smart contract is not triggered during normal purchase situations and is triggered only when the buyer succeeds in a double payment attack or when the transaction is not normally conducted due to problems such as unexpected forks. It is known that there may be cases in which smart contracts attempt to withdraw money from the purchaser's wallet due to a malfunction of the smart contract even though the transaction was normally performed.

3) **Half-life:** Most existing coins have a half-life. The half-life is the time it takes for a certain amount to become half of the initial value, and when a coin with an initial mining amount of 50 passes through the half-life, it is reduced by half to 25, and the same process is repeated, and the mining amount converges to zero. Therefore, as the half-life passes, the supply of coins decreases by half, and when the coin mining is finally finished, that is, when the mining amount of the coin reaches zero, the supply of coins no longer occurs. As a result, the price of cryptocurrency has been steadily rising, and speculative capital has flocked due to the scarcity of limited supply, creating an unusual market as it is now. Therefore, it is set not to have a half-life, so that coins are constantly supplied until the end of the final mining, and the price increase is suppressed until the end of mining.

Table 1 below shows the differences between the new coins, PTC, BTC, and LTC, based on the orientation of the lightweight transaction architecture.

TABLE 1. DIFFERENCES FROM OTHER COIN

Metrics	Coin Name		
	BTC	LTC	PTC
Block Generate Time	10min	2.5min	1min
Max Block size	1MB	4MB	1MB

Total Issuance	21,000,000	84,000,000	10,612,000,000
Initial Mining Rewards	50	50	1000
Half-life	210,000	840,000	Non-existent
Process	The First of Cryptocurrency	Coinbase Forked from BTC	Coinbase Forked from LTC
Amount per cost	High	Medium	Hold Down to 1\$

PTC has reduced the block generation cycle to 1 minute to shorten the minimum verification time of the blockchain and has the intention to reduce the value of the unit amount as much as possible by increasing the mining reward and total issuance. Also, since there is no half-life, it prevents the price of coins from rising rapidly every half-life.

IV. LIGHTWEIGHT TRANSACTION FOR APPLYING VENDING MACHINE

One of the places suitable for use of cryptocurrencies based on lightweight transactions is a vending machine. According to a report from Vending Market Watch published in 2019, “The number of locations where vending machines are offered has increased, but the number of expected vending machines has declined significantly since 2016. The decrease in the number of vending machines seems to be due to the rapid growth rate of the micro market.” [11] Here, the micro market can be seen as an unmanned convenience store as a market with automated self-checkout technology. It is estimated that the automation market will accelerate further as Covid-19 spreads rapidly and social distancing is encouraged worldwide. Due to the impact of the accelerated automation market, the size of the micro market will grow and grow, replacing the existing vending machine market and convenience stores, and the vending machine market will have to target a niche market that cannot be digested as a micro market. Therefore, the vending machine market must target a market that cannot be digested as a micro market, and in this situation, cards are burdensome due to fees, and cash and coins are increasingly not used by people.

In addition, while the rate of use of coins and money as a payment method of existing vending machines is lowering, and the use rate of credit cards and debit cards is increasing, the failure rate of coins and money slots and maintenance costs are continuously increasing. In this situation, cryptocurrency will be quite attractive in the vending machine industry. This is because the fee is lower than that of a card, and there is no need to carry it like cash. However, it is not an easy problem to use blockchain logic in a system with poor hardware such as a vending machine. Each vending machine becomes a node and requires considerable computing power and storage space to process and verify blockchain transactions.

Therefore, we propose the application of a new currency applying the lightweight transaction architecture to the vending machine. By installing the aforementioned light client on the vending machine, the burden on storage space is reduced, and the fast consensus time and low unit price are realized, so that

consumers can use it without burden. The following figure 4 is an example implementation of a new cryptocurrency applied to a vending machine.

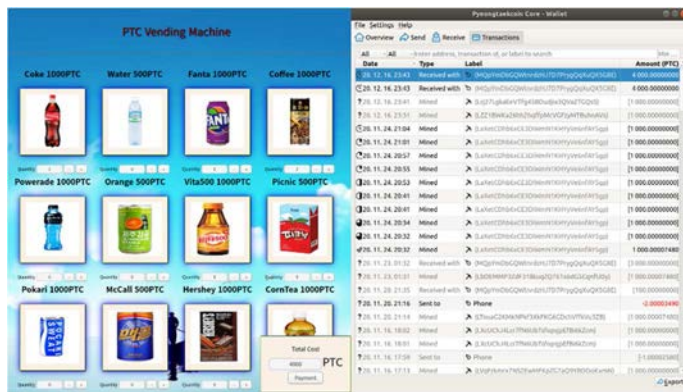


Figure 4. Apply lightweight transaction for vending machine

The following figure 5 shows the cryptocurrency-based vending machine service algorithm.

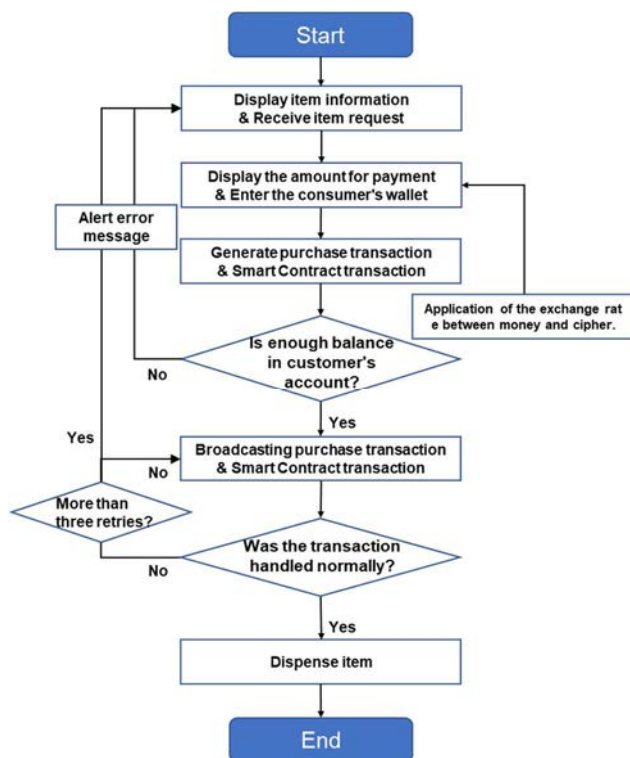


Figure 5. Cryptocurrency based vending machine service algorithm

The biggest difference from the existing vending machine service algorithm is that a module for cryptocurrency transactions similar to card transactions is added for cryptocurrency transactions, and the exchange API to synchronize the market price must be included inside the vending machine due to the nature of cryptocurrency that the market price changes from time to time. In order to check whether the transaction was successful at the vending machine, first check the buyer's wallet address with a QR code through a

QR code reader before the transaction. After that, a script is created in the vending machine, a transaction that transfers money to the seller's wallet address, and a smart contract that operates when the transaction is not performed normally, and broadcasts it to the blockchain network. If it is normally broadcast on the blockchain network, the product is delivered to the buyer.

The lightweight transaction process can be extended not only to vending machines, but also to cryptocurrency ATMs and micro markets, which are automatic sales systems. The logic of ATM and vending systems is also not very different from that of vending machines, and this process will be an attractive option wherever blockchain needs to be applied in a limited hardware resource environment.

V. CONCLUSION

This study presented a good alternative to the application environment where normal block hash calculation ability and electric power wasted on a large-scale blockchain network were burdensome. Nevertheless, despite the proposed lightweight transaction-based blockchain system suggesting an improvement direction for the resource constraint problem, there remains a problem of how to suppress the biased inflation of issued cryptocurrencies. Future research intends to propose a technical method to improve inflation biased in cryptocurrency based on the proposed lightweight blockchain process, and to discover and apply application cases of vending machines.

ACKNOWLEDGMENT

This research was supported by the Ministry of Trade, Industry and Energy (MOTIE), Korea, through the Education Program for Creative and industrial Convergence. (Grant Number N0000717).

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, 2008.
- [2] T. Wu and X. Liang, "Exploration and practice of inter-bank application based on blockchain," 2017 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, 2017, pp. 219-224
- [3] Hsiao JH., Tso R., Chen CM., Wu ME. (2018) Decentralized E-Voting Systems Based on the Blockchain Technology. In: Park J., Loia V., Yi G., Sung Y. (eds) Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore.
- [4] K. Karlsson et al., "Vegvisir: A Partition-Tolerant Blockchain for the Internet-of-Things," 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, 2018, pp. 1150-1158
- [5] J. Ellul and G. J. Pace, "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things," 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, 2018, pp. 1-4
- [6] Y. Liu, K. Wang, Y. Lin and W. Xu, "LightChain: A Lightweight Blockchain System for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3571-3581, June 2019.
- [7] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," in IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, July 2018.
- [8] Johnson, D., Menezes, A. & Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36-63 (2001)

- [9] Certicom research, 'SEC 2: Recommended Elliptic Curve Domain Parameters Version 2.0,' January 2010.
- [10] Bi, W., Jia, X., & Zheng, M. A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain. arXiv preprint arXiv:1808.02988, 2018.
- [11] Gupta, Suyash & Sadoghi, Mohammad, Blockchain Transaction Processing, 2018.
- [12] Percival Colin. Stronger key derivation via sequential memory-hard functions, 2009
- [13] Szabo, Nick. "Formalizing and securing relationships on public networks." First Monday 2.9, 1997.
- [14] 2019 State of the Industry Report: Operators Beat Revenue Numbers with New Locations and Services, accessed Nov 09, 2020, <https://www.vendingmarketwatch.com/reports/document/21085744/2019-state-of-the-industry-report-operators-beat-revenue-numbers-with-new-locations-and-services>



Tae-Shin Kang entered the Smart Contents major of ICT-Convergence Division at Pyeongtaek University in 2019. Currently, as an undergraduate research student in the Smart Systems Lab, he is participating in blockchain and cryptocurrency research.



Moon-Il Joo received the PhD degree in computer engineering from Inje University in

2018. He is currently working as a research professor at the Institute of digital anti-aging healthcare, Inje University, Korea. His research interests are in software engineering, human computer interaction, smart phone programming, and component based development.



Beom-Soo Kim received the bachelor's degree in computer engineering from Inje University in 2018. He is getting a master's in the Institute of digital anti-aging healthcare, Inje University, Korea. His research interests are in human computer interaction, smart phone programming, and component-based development.



Tae-Gyu Lee (BSc'92–MSc'96–PhD'06) He received the B.Sc. degree from Kunsan National University, Kunsan, Korea in 1992, the M.Sc. degree from Soongsil University, Seoul, Korea in 1996, and the Ph.D. degree from Korea University in 2006. He is currently a Professor in the ICT convergence Division, Pyeongtaek University, Gyeonggi, Korea. He has been a Professional Researcher in Advanced Convergent Technology R&D Group, Korea Institute of Industrial Technology (KITECH), Ansan, Korea for 2009-2013. He has also been a President in the JIGUNET Corporation, Seoul, Korea, from 1999. His research interests are in distributed systems, ubiquitous computing, middleware, sensor networks and computing, wearable and robot computing.