



Prospect Analysis for Utilization of Virtual Assets using Blockchain Technology

Jeongkyu Hong* , Member, KIICE

School of Electrical and Computer Engineering, University of Seoul, Seoul 02504, Republic of Korea

Abstract

Blockchain is a decentralized network in which data blocks are linked. Through a decentralized peer-to-peer network, users can create shared databases, resulting in a trustworthy and aggregated database known as a blockchain that enhances reliability and security. The distributed nature of the blockchain enables data to be stored on multiple nodes, eliminating the need for a central server or platform. This disintermediation significantly reduces the transaction and administrative costs. The blockchain is particularly valuable in applications where reliability and stability are critical because it establishes an open database that ensures data integrity, making it virtually impossible to tamper with or falsify data. This study explores the diverse applications of the blockchain technology in virtual assets, such as cryptocurrency, decentralized finance, central bank digital currency, nonfungible tokens, and metaverses. In addition, it analyzes the potential prospects and developments driven by these innovative technologies.

Index Terms: Blockchain, Virtual Asset, Decentralization, Smart Contract, Cryptocurrency, CBDC, NFT

I. INTRODUCTION

In a blockchain, blocks, which are storage units of data, are chained according to specific sort-order rules. A connected database (DB) becomes a distributed transaction ledger stored in distributed nodes (such as individual computers) rather than in a specific location. Therefore, a blockchain can be viewed as a decentralized, distributed DB aggregate, and if the internet is the “sea of information,” the blockchain is the “sea of trust.” This is because the DB of the blockchain is created in a peer-to-peer (P2P) network manner among participants who have configured nodes according to the protocol for verifying new blocks. Blocks must be manipulated before new blocks are created. In other words, numerous blocks need to be manipulated within a certain period of time, which is virtually impossible; therefore, security and reliability are high.

The blockchain algorithm records all the transaction information that occurs during a certain period in block units and transmits this record to all the node members; when the validity of a block is secured, a new block is added to the existing block. In this case, each block includes a hash pointer (a means of checking for forgery and alteration), which is a link to the previous block, time display, and transaction data. Thus, the blockchain technology can solve the problem of double spending, such as fraud, by providing an efficient, open, and distributed ledger that can record transactions in a verifiable manner, so that each new unit of value is transacted only once [1,2].

Consequently, the blockchain has become the basis for cryptocurrency operations, such as Bitcoin and Ethereum, and can be used in various fields, such as ID management, electronic voting, personal health record management, smart contracts, fund transfer, trade finance, real estate registration,


Received 7 September 2023, Revised 20 October 2023, Accepted 23 October 2023

*Corresponding Author Jeongkyu Hong (E-mail: jhong@uos.ac.kr)

School of Electrical and Computer Engineering, University of Seoul, 02504, Republic of Korea

Open Access <https://doi.org/10.56977/jicce.2024.22.1.64>

print ISSN: 2234-8255 online ISSN: 2234-8883

 This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Copyright © The Korea Institute of Information and Communication Engineering

securities issuance and trading, overseas remittance, and the activation of high-value items (e.g., diamonds). It has unlimited innovation and growth potential. In particular, efforts are being made to create a new financial ecosystem using the blockchain technology in the financial district, and a new direction for the fintech industry is being sought [3,4].

Recognizing this situation, this study examines various utilization methods, particularly in the field of virtual assets, among various application fields using the blockchain technology and analyzes future development directions accordingly.

II. BLOCKCHAIN TECHNOLOGY ANALYSIS

To understand the blockchain technology, the following aspects need to be understood: what information is contained in a block, who makes a block, how the stability and reliability of a block are secured, how a chain is constructed, whether a chain can be composed by anyone, what is mining, how to do it, why blockchains and cryptocurrencies coexist, and what the hash functions are. An overall configuration diagram showing the connection and flow of each node using a blockchain is shown in Fig. 1 [5].

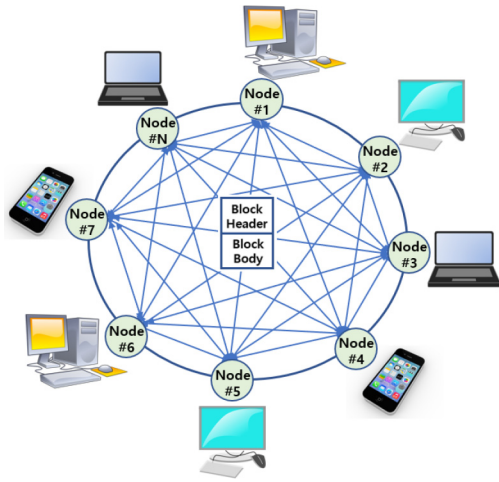


Fig. 1. Overall flow and structure of a blockchain

A. Configuration of Block

As shown in Fig. 2, a block is divided into two components: block header and block body. In Fig. 2, the hash of the block contains information about the name of the block and information, such as the version corresponding to the header information of the block, the hash of the previous block, Merkle tree root, difficulty target, and nonce. This is the result of converting to SHA256 after obtaining the sum by adding all values. The version refers to the version of the

block; the previous block hash is the address value of the previous block among connected blocks; the Merkle tree root is the hash tree of the transactions stored in the body of the block; the time is the creation time of the block; the difficulty is the complexity of the goal value; and the nonce is an index necessary for obtaining a hash value in the process of generating a block [6,7].

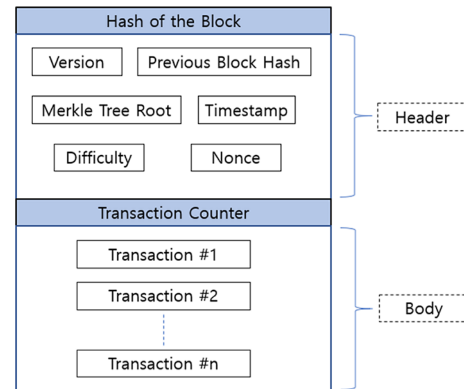


Fig. 2. Components of a block

B. Generation of Block

To create a block, the value obtained by hashing the transaction history and the nonce value in the block first, that is, the hash value of the block, is generated. The hash value is larger than a specific boundary value (hash value leading index) determined by the difficulty algorithm of the system. If the value is small, it is considered valid. For example, in the case of Bitcoin, the first block (block #0, called the genesis block) has a hash value starting at 10 zeros, and recently, it has had a hash value starting at more than 20 zeros. Participants change the nonce value and repeat the hashing operation along with the transaction details to determine a hash value smaller than a certain boundary value, which is called mining. At this time, the miner who finds the valid hash value the fastest is said to have “mined (created) a block” and is given a reward accordingly, and from the next block, a chain including the hash value of the previous block is formed, as shown in Fig. 3 [6,7].

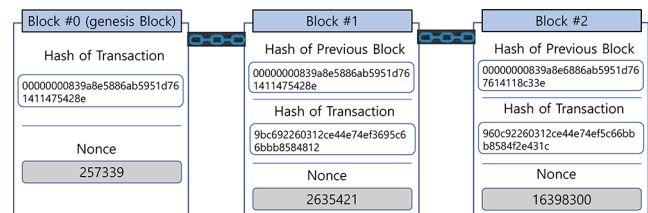


Fig. 3. Example of block creation and connection

C. Consensus Algorithm

A consensus algorithm is a process in which numerous nodes connected to a P2P network create a mutual agreement on which block is legitimate; this is called mining. For example, in the case of cryptocurrency, this algorithm proves that the operation (mining) of adding a new block to a chain that has built trust is completed by recording the details of financial transactions. It is designed to reward coins to the miners who first complete the task. In addition, the transaction fee generated by the node requesting the transaction is given to the miner; thus, the profit of the miner is the sum of the reward and fee [6,7].

All the nodes in the P2P network induce consensus on the sharing, verification, and addition of new records so that all the nodes in the P2P network can finally hold the same transaction details through mutual communication. Furthermore, as the transaction details are transparently disclosed, this is called the public transaction ledger or a trust protocol. Consensus algorithms include proof of work, proof of stake, proof of elapsed time, Byzantine fault tolerance, and proof of authority.

III. UTILIZATION ANALYSIS FOR VIRTUAL ASSETS OF BLOCKCHAIN TECHNOLOGY

A. Cryptocurrency

A cryptocurrency is an electronic currency that uses encryption technology to secure transactions within a P2P network. It is a digital asset that creates and maintains a unit of currency in a decentralized distributed environment and records transaction information in a distributed ledger. It is a different concept from virtual currency, which is issued and managed by a developer in a specific institution and is centralized and distributed online only in a specific community.

The first decentralized cryptocurrency was Bitcoin, which was published in October 2008 by Satoshi Nakamoto in a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." Since then, altcoins (i.e., all cryptocurrencies except Bitcoin) that follow Bitcoin have been issued for use in various applications. Ethereum, the most famous altcoin, provides scalability to transparently operate various applications, such as contracts, SNS, e-mail, and electronic voting, in addition to its monetary function; however, Bitcoin can only function as a currency, such as payments or transaction [8,9].

B. Decentralized Finance (De-Fi)

Decentralized finance (De-Fi) is a financial system that uses blockchains and cryptocurrencies to perform all the functions provided by real finance, such as loans, transac-

tions, and asset management, without intermediaries or third parties. In De-Fi, all the transactions are performed using smart contracts and a liquidity pool. The liquidity pool acts as a medium to connect two tokens, and transactions based on stable coins are provided. Almost all De-Fi applications are provided using the Ethereum platform [10].

For example, if an individual invests \$1,000, buys 500 stable coins (BUSD), and buys nonstable coin (ETH) with the remaining \$500, BUSD and ETH are stored in the liquidity pool. If someone has BUSD and wants to buy ETH, they use the liquidity pool and pay a fee. All the contracts and transactions are made using the blockchain software; therefore, no one can intervene. Fig. 4 shows the De-Fi transaction process.

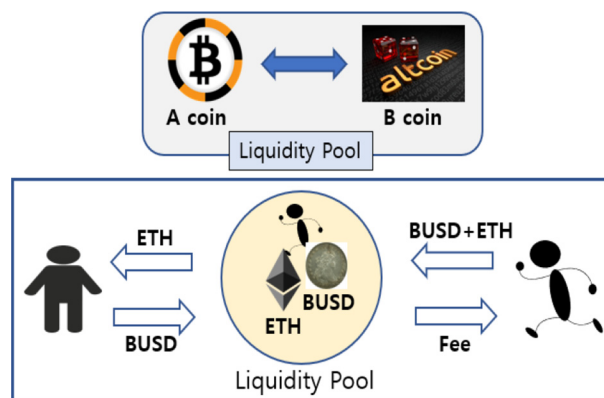


Fig. 4. De-Fi transaction procedure

Additionally, if the insurance company codes the contents of the contract and stores them in a blockchain, there is nothing for humans to do in the settlement process when making an insurance claim. When the hospital creates an electronic document and uploads it to the blockchain network, it checks whether it satisfies the conditions for the payment of insurance money, such as the period and validity conditions of the contract stored in the blockchain. If approved, the insurance money is automatically paid, and this record is also stored in the blockchain, and all complex processing processes are automated.

C. Central Bank Digital Currency

Central bank digital currency (CBDC) is a legal currency issued directly by the central banks of each country based on the blockchain technology and is called "digital cash." As shown in Fig. 5, there is almost no price volatility as guaranteed by the central bank, and it can be used even if the Internet is cut off using near-field communication; hence, the fee is low, and improved accessibility is provided to the financially underprivileged without a bank account. It has advantages, such as the rapid promotion of financial and monetary policies, including fiscal targets; the expansion of tax reve-

nue through tracking illegal funds; and the minimization of currency issuance costs [11].

However, there are disadvantages, such as a reduction in the business area of existing private banks owing to the central bank's concentration of financial power, the decline of innovation engines in cards and similar fintech areas, and the infringement of personal information owing to the exposure of personal information, such as tracking transaction details. CBDC services are underway in China, and research and experimentation are underway in most countries.

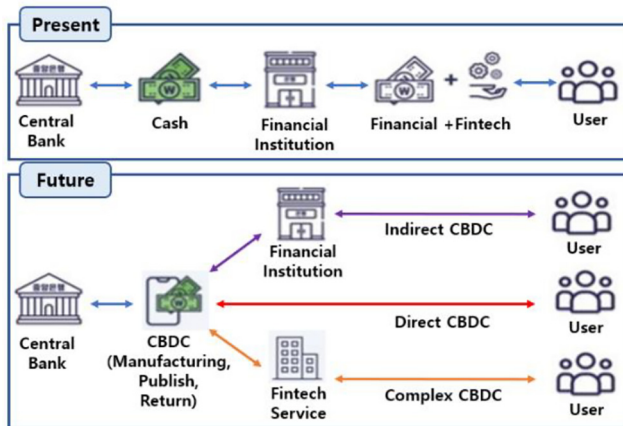


Fig. 5. Conceptual diagram of current cash and future CBDC distribution methods

D. Non-Fungible Token (NFT)

Unlike existing virtual assets, non-fungible tokens (NFTs), which are scarce and unique, use the blockchain technology to provide unique recognition values to digital assets. That is, by issuing only one token for each digital asset object, only one token exists in the world and cannot be replaced. By converting related information, such as the ownership and sales history of digital assets, into a blockchain DB, the original issuer and owner can be checked at any time, and illegal copying or forgery is prevented, resulting in the absence of ownership disputes. NFTs are expected to play the role of a game chain that creates revenue models and jobs by applying them to all objects with inherent value (e.g., artwork, game items, collectibles, movies, music, sports goods) [12]. A representative example of an NFT is “Everydays: the First 5000 Days,” a digital artist who bundled 5,000 digital paintings drawn every day since 2007 and compiled them into a single digital painting. It was sold at an auction at Christie’s for \$6,930 and is currently displayed at the Metapurse Digital Museum.

E. Metaverse

This has recently become a popular topic in the era of the

Fourth Industrial Revolution, and the metaverse (meta-universe) has been mentioned as a growth engine for new industries. Metaverse is a compound word of “meta,” which indicates fabrication or abstraction, and “universe,” which indicates the real world and a three-dimensional virtual world. This concept is more advanced than the existing term virtual reality (VR), and is a form in which the virtual world, such as the web and the Internet, is absorbed into the real world. As the Internet evolves into a 3D network, the metaverse is expected to become a crucial keyword in the future IT industry and a new gamechanger. Existing VR is unidirectional, but the metaverse can experience the real world in virtual reality in both directions. The ownership of virtual assets within the metaverse is guaranteed by the blockchain technology, such as NFTs [13].

A metaverse can be applied to all objects to the extent that it is also used as a new term, metaverse of things (MoT), and is recognized as an innovative technology for virtualization and immersion. In particular, it will be possible to realize a virtual world close to reality in Web 3.0, which is called the next-generation Internet. The metaverse is expected to be applied to various fields, such as digital twins, virtual spaces, and experience sharing.

IV. DEVELOPMENT PROSPECTS OF BLOCKCHAIN AND VIRTUAL ASSETS

The blockchain can be applied and utilized in various fields to improve reliability, stability, and decentralization based on mutual agreement and security. This is gradually becoming a reality, and its importance is further expanding. Several virtual-asset-related services, such as digital finance, smart contracts, decentralized platforms, metaverses, NFTs, and trust data sharing, based on the blockchain technology are already being provided or are in progress. The views on cryptocurrencies as virtual assets differ depending on likes and dislikes. However, it is expected that some major cryptocurrencies, including Bitcoin, will be recognized as virtual assets and circulated as currency in the future. De-Fi has been recognized as a necessity because of the financial crisis caused by the bankruptcy of Lehman Brothers, a global investment bank, in 2008, and the bankruptcy of Silicon Valley Bank, a venture investment bank, and Credit Suisse Bank, a global bank, in 2023. Its use has become widespread in recent years [14].

The service timing of the central bank’s digital currency has not yet been confirmed, but the need for it is recognized, and each country is competitively promoting it; thus, the introduction of the service appears to be a matter of time. NFTs will become a much larger market in the future, as a service that must be considered a matter of course in the digital platform era. The metaverse has already begun to perme-

ate our lives. In the future, it will be used in almost all fields and will develop to a point where we cannot imagine a world without metaverse services. VR devices and platforms for games using metaverse technology, exercise and healthcare platforms linked with robots, video conferencing platforms using avatars, and products and technologies of several start-up companies, particularly linked to metaverses and Web 3.0, are expected to be developed, and it is expected that various technologies for building metaverse content and economic ecosystems using the blockchain and Web 3.0 technology will be introduced in the future.

In addition, the current circulating currency will evolve into a digital currency, and cryptocurrency, which is highly volatile but recognized as a virtual asset, will be self-sustaining, focusing on coins with clear applications. NFTs will spread from the current introduction stage to the rapid development stage. Particularly, a metaverse based on NFTs will establish itself as a major service that will lead the new Web 3.0 era. Therefore, it is judged that the blockchain will transform offline finance into online finance and fundamentally change the industrial infrastructure to innovate the future society.

The blockchain technology has features, such as trust enhancement, security enhancement, and efficiency improvement; hence, it will be used in various newly derived virtual asset application fields. The blockchain will accelerate the second Internet revolution era, the Internet will bring equalization, and the blockchain is predicted to bring equalization of value.

V. CONCLUSIONS

The blockchain is a data distribution processing technology that distributes and stores data, such as the transaction details of all users participating in the network. Furthermore, by establishing an open DB through sharing among participants, it is almost impossible to manipulate or forge data. Therefore, the blockchain is used in application fields where reliability and stability are important.

In this study, we examined various ways to utilize the blockchain technology in the virtual asset field and analyzed future development directions based on this technology, such as cryptocurrencies, De-Fi, CBDC, NFTs, and metaverses. Among the technologies mentioned in this paper, some have already been recognized as business models and have achieved visible results, and most technologies are either considering commercial business models or being promoted.

In the future, the field of virtual assets using the blockchain technology is expected to create new businesses as a major service in the Web 3.0 era and provide means and methods that have not been experienced so far.

ACKNOWLEDGEMENTS

This study was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (MSIT) (No. 2022R1F1A1074641).

REFERENCES

- [1] J.-Y. Lee, "Blockchain Technology Trends and Implications," *STEPI Trends*, no. 34, pp. 1-21, Jul. 2017.
- [2] J.-W. Kim, "Analysis of Blockchain Ecosystem and Suggestions for Improvement," *Journal of Information and Communication Convergence Engineering*, vol. 19, no. 1, pp. 8-15, Mar. 2021. DOI: 10.6109/jicce.2021.19.1.8.
- [3] Y. Chen and Y. J. Kim, "Challenges and Tendencies in Blockchain for SCM -Science Mapping Analysis," *Journal of KISS*, vol. 32, no. 2, pp. 55-67, Feb. 2022.
- [4] H. Y. Jeong and Y. K. Choi, *Block chain economy, Seoul: Future & Innovation 21*, ISBN: 979-11-9762-910-5, 2022.
- [5] B. J. Choi, C. S. Kim, and M. C. Lee, "Research Trends on Distributed Storage Technology for Blockchain Transaction Data," *Electronics and Telecommunications Trends*, vol. 37, no. 3, Jun. 2022. DOI: 10.22648/ETRI.2022.J.370309.
- [6] J. H. Oh, *Block chain changes the Future*, GoodWelthBooks, ISBN: 979-11-91447-24-8, 2021.
- [7] NomadCoders, "Get a good understanding of blockchain," 2021. [Online], Available: <https://youtu.be/a7Meu4z-F4list=PL7jH19IHhOLOJFXeVqjtawzNQLxOgTdqt>.
- [8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *The Cryptography Mailing List*, Oct. 2008. [Online], Available: <https://bitcoin.org/bitcoin.pdf>.
- [9] Coinbase HELP, "What is the Bitcoin Blockchain?," Coinbase 2023. [Online], AvailableFig: <https://help.coinbase.com/en/coinbase/getting-started/crypto-education/what-is-the-bitcoin-blockchain>.
- [10] R. H. Campbell, A. Ramachandran, and J. Santoro, *Defi and the Future of Finance*, New York: Wiley, ISBN: 978-1-119-83601-8, 2021.
- [11] A.-C. Cuțitoi, "Machine Vision Algorithms, Sensory Data Mining Techniques, and Geospatial Mapping Tools in the Blockchain-based Virtual Economy," *Review of Contemporary Philosophy*, vol. 21, pp. 223-238, 2022. DOI: 10.22381/RCP21202214.
- [12] M. Banerjee, J. Lee, and K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149-160, Aug. 2018. DOI: .
- [13] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the Metaverse: A Review," *Journal of Social and Information Networks*, *arXiv preprint arXiv:2203.09738*, pp. 1-17, Mar. 2022. DOI: 10.48550/arXiv.2203.09738.
- [14] S. Makridakis and K. Christodoulou, "Blockchain: Current Challenges and Future Prospects/Applications," *The Journal of Future Internet*, vol. 11, no. 12, pp. 258, Nov. 2019. DOI: 10.3390/fi11120258.



Jeongkyu Hong

received the B.S. degree from the College of Information and Communications, Korea University, Seoul, Korea, in 2011, the M.S. degree from the Department of Computer Science, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2013, and the Ph.D. degree from the School of Computing, KAIST, Daejeon, Korea, in 2017. He worked as an assistant professor in the Department of Computer Engineering at Yeungnam University from September 2018 to August 2023. He has been with the School of Electrical and Computer Engineering at the University of Seoul since September 2023, as an associate professor. His current research interests include the design of low-power, reliable, and high-performance processor architectures, and memory systems.