

## **Blockchain Technology and Its Applications: Case Studies**

Jin-whan Kim <sup>1</sup>

<sup>1</sup>School of Computer Engineering, Youngsan University, 288 Junam-ro, Yangsan city, Gyeongnam 50510, South Korea

*kjw@ysu.ac.kr*

**Abstract.** Blockchain technology is expected to bring about exciting developments across a variety of fields, such as politics, economy, culture, industry, and business model. Blockchain is no doubt one key infrastructure technology to lead the Fourth Industrial Revolution. This paper is a general overview of the main features of blockchain technology. Three types of blockchains (public, private, and consortium) will be presented within a discussion of their major case studies. In addition, the latest trends and developments in blockchain technology will be briefly reviewed. The terminology of blockchain infrastructure technology has the potential to foster technological innovation across various industrial sectors as well as improve mutual harmony and understanding of complex structures and diverse phenomena in human society, especially antagonism, confrontation, and ideological conflict. With such progress in social innovation, blockchain technology will result in a fairer and more transparent human society. Greater attention will also be given to a blockchain-based mobile voting system that will enable the realization of direct democracy in a representative democracy. Furthermore, this paper offers solutions to a trilemma of problems (scalability, security, decentralization) in blockchain.

**Keywords:** blockchain, application case studies, distributed ledger, consensus algorithms, smart contracts.

## 1. Introduction

Blockchain is a distributed computing-based technology on a trusted network in which data blocks to be managed are stored in distributed databases hosted on peer-to-peer (P2P) networks. Chains are formed between the blocks so that the blocks cannot be arbitrarily revised, and the results of any changes can be accessed. In other words, blockchain is a Distributed Ledger Technology (DLT). The ledger (all the data to be managed) stores and manages transaction information on the computers of participants connected to the P2P network instead of on a centralized server of a certain organization (Kim, 2019; Lin, 2017; IRS, 2019; Nomura Research Institute, 2016).

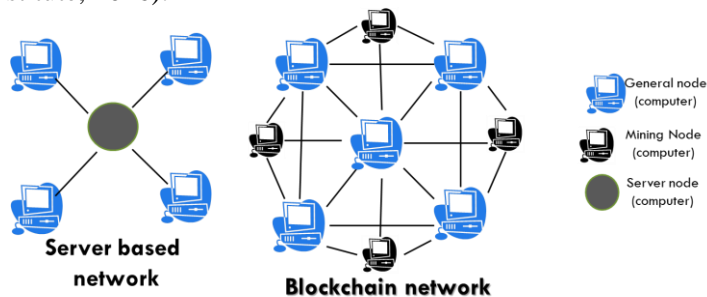


Fig. 1: Server based network and blockchain network

The left image in Figure 1 illustrates a current and traditional computer network on Internet; the right image shows a blockchain network.

Major features of blockchain technology include decentralization, invariance, reliability achieved through consensus processes in untrusted environments, security, economic efficiency, agility, decentralization, the absence of intermediaries, transparency, efficiency, and scalability. Security is achieved as data are commonly owned by multiple participants to prevent hacking. The use of open software and cost reduction related to system development and maintenance, database operations, and security creates economic efficiency. Decentralization is achieved by storing and managing transaction histories on distributed computers to prevent forgery or illegal use. Non-intermediacy is achieved by enabling transactions between individuals without certification of any specific third party, and this reduces complexity caused by intermediation and the burden of intermediary fees. When inquiries are allowed to access all information, this results in transparency, which in turn enhances reliability. Last, scalability is achieved by enabling changes in the blockchain system to fit the use case. Open sources are employed so that the blockchain system can be easily reconstructed and utilized.

Blockchains can be divided into three types: public blockchain, private blockchain, and consortium blockchain. Each type has its own characteristics, and they differ slightly in their functions and structures (Public Blockchain vs Private

Blockchain 2018).

### **1.1. Public blockchain**

A public blockchain is a decentralized distributed system in which an unspecified number of participants can share and mutually verify transaction information occurring in the system. There is no separate managing entity. Anyone can participate anonymously, and there is no restriction on authority. One current application of the public blockchain lies in the foundational technology behind Bitcoin, a well-known cryptocurrency (i.e. virtual money) currently in circulation around the world. Naturally, public blockchains are being actively researched in finance (Ripple Labs Inc 2018, S. Nakamoto 2008). DLT is at the core of public blockchains. Public blockchains may be effectively used in the financial sector through transactions such as cryptocurrencies and overseas remittances but also in other areas such as crowdfunding and transportation. This is because a public blockchain enables the authentication process to be carried out without a trusted, third party. Additionally, public blockchain is an open blockchain that enables anyone to create transactions and participate as a node. It also provides high reliability and integrity through the verification of participants' work. Despite these strengths, however, there is a disadvantage: recording and processing speeds may decrease as the transaction records of all participants are stored and shared.

### **1.2. Private blockchain**

A private blockchain is related to a public blockchain; yet, it differs in that it limits participation to only those individuals that the service provider (enterprise or organization) has approved. A private blockchain is a centralized blockchain. This type employs blockchain technology in a centralized structure as a method to enhance security and transaction speed. Unlike a public blockchain, the private type is managed independently by one entity. Only the nodes that have been verified through the authentication method created on the network can participate in this type of blockchain. Thus, to access transactions, each participant must have received appropriate permissions. In a private blockchain, only those entities that take legal responsibilities can create transactions, and only approved and verified entities may validate transaction histories and data as well as approve transactions. In private blockchains, the time for block creation cycles or verification is short because only authorized nodes participate. This renders the approval and verification progress of other unauthorized nodes unnecessary. However, since the users of private blockchains must depend entirely on the service provider, the reliability of private blockchains is limited in comparison to public blockchains.

### **1.3. Consortium blockchain**

A consortium blockchain is one in which only those users who satisfy certain requirements or have been agreed on in advance (e.g. companies, organizations) may participate. The levels of authorization assigned to users in this blockchain type

differ: for example, allowing only some participants to see all or part of transaction information or performing transactions with the authority to add new blocks to some other participants. It is a semi-centralized blockchain composed of many companies or organizations as joint entities. As with private blockchains, only the nodes (computers) of authorized users can participate in this type of blockchain.

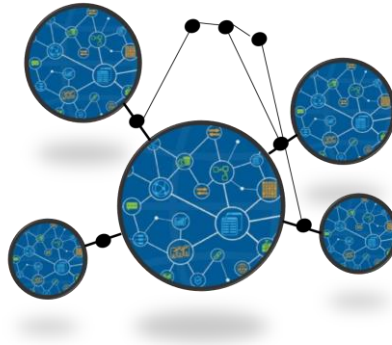


Fig. 2: Ideal blockchain network

What might an ideal blockchain network look like? Figure 2 represents an ideal blockchain network. One sees that the various blockchain networks are interconnected.

## 2. Major Technologies in Blockchain

In blockchain, transaction histories (“blocks”) are stored and managed in a chain where a cryptographic technique links all past transactions into one sequence.

### 2.1. Peer-to-peer (P2P) network system

A P2P network is a distributed computer network in which multiple computers communicate directly with each other in a one-to-one manner. Information is distributed, stored, and managed on all computers connected to the network. It is a very reliable system because even if several computers were to crash, the entire system is not affected.

### 2.2. Digital signatures using private keys and public keys

Secret keys in the form of passwords grant users the authority to access the blockchain system, and public keys are used to secure safe, anonymous transactions.

### 2.3. Hash Function Encryption

This is a core technology used to rapidly detect data manipulation or damage to data using hash values from “hash functions” that map data of arbitrary lengths with fixed data. Put another way, it is a technology that always creates the same hash values when the input data are the same.

It is possible to use the site <http://www.blockchain-basics.com/Hashing.html> for a simple test and the site <http://www.convertstring.com/ko/Hash/SHA256> to view

the SHA256 hash algorithm.

#### **2.4. Decentralized system**

This is a system that can reduce the risk of external hacking attacks because it uses distributed computers instead of a centralized server computer.

#### **2.5. Disintermediation**

This is a system that requires no intermediary because all transactions are done automatically through smart contracts.

#### **2.6. Distributed ledger**

All transaction information is stored and managed on individual computers participating on a P2P network instead of being stored and managed on a centralized server computer.

#### **2.7. Smart contracts**

This is a system in which contracting parties preprogram contents agreed upon in advance. The parties then register electronic contracts whose contents are automatically executed when the contract conditions are met so that certain transactions are automatically processed according to the previous arrangements.

#### **2.8. Consensus algorithms**

To properly form agreements among an unspecified number of participants, there are consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Importance (PoI), Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), and so on.

### **3. Cases of Blockchain Use**

#### **3.1. Banking sector**

Bank services such as deposits and loans may see an increase in their reliability as distributed ledgers and smart contracts available with blockchain technologies are used. In addition, the same technologies can be applied to foreign exchange businesses. International remittances and issuances of letters of credit and management in trade can proceed at lower cost and higher speeds. For example, Ripple coin (XRP) effects within blockchain technology are considered to be substantial. Ripple is a real-time gross settlement system as well as a currency exchange and remittance network created by Ripple Labs, a US-based technology company.

#### **3.2. Crowd sourcing**

Blockchain technology can also be applied to matching services that connect ordering and receiving businesses as well as job seekers and clients on the Internet to solve various problems. These problems include accuracy of matching, speed of results, or high commission fees. In addition, the use of blockchain technology in

crowd funding is increasing. The ability of individuals or companies to generate public financial support for a product or service is a major advantage of crowd funding. This process allows investors to participate through small financial contributions that carry little burden. In other words, crowdsourcing is a structure in which individuals and companies are directly connected without the use of intermediaries, and this dovetails well with the characteristics of blockchains.

### **3.3. Insurance sector**

With blockchains a new type of collateral management system can easily identify and utilize the massive amounts of information that insurance contracts contain. In this process, the blockchain integrates real data and smart contracts. Various projects are currently exploring these advancements. In one notable case, an insurer at American International Group has applied blockchains to the insurance business in cooperation with IBM.

### **3.4. Licensing and payment system sector**

Blockchain-based cryptocurrencies are used in a variety of payment systems. In addition, these cryptocurrencies can be widely used in areas where licenses granted to access certain content (e.g. music, films) for a set number of times or a set duration of use.

### **3.5. Medical treatment and healthcare sector**

Hospitals and clinics have challenges to manage, maintain, and repair medical treatment systems, resulting in the allocation of massive financial and human resources. It is estimated that the introduction of blockchains can remarkably reduce the costs that medical institutions incur. One important contribution would be the recording of medical records on blockchain so that patients' unique medical records can be easily accessed from anywhere within the industry (Pirtle, 2018; Dan et al., 2016).

### **3.6. Copyright management sector**

The use of blockchain technology will foster great change in copyright management as it tracks ownership and prevents forgery. For example, blockchain technology can digitize concert tickets to prevent scalping, the unauthorized resale of tickets. In the same way, it can prevent the illegal copying and sharing of computer and video game software. Both instances further reinforce copyright protections for a variety of creative works.

### **3.7. Electronic government, public sector**

Central and local governments can employ blockchain-based administrative services for a variety of tasks: official record keeping, online electronic voting, education, taxation, national defense, new and renewable energy management and related transactions. For real estate specifically, the services that will benefit from such improvements are sale and registration, transfers of ownership, and records of

reconstruction and repair. In all cases, blockchain technology will play a great role in cost reduction. With such administrative changes, society can become fairer and more transparent, leading to greater convenience and quality of life for all citizens (Kim, 2018; Lee, 2019; Islam et al., 2019).

### **3.8. Supply chain management, logistics, and distribution systems fields**

Logistics systems have stages in which products are transported from producer to consumer. The recording and management of these changes and the conditions in which such changes may occur necessitate a solution for rapid information delivery and enhanced transparency. The agricultural, fishery, livestock industries may use blockchain technology to manage detailed records that track the distribution and consumption routes of goods, rare minerals, and artifacts produced.

### **3.9. Eco-friendly management system sector**

By using artificial intelligence and big data technologies running on Internet of Things (IoT) blockchain platforms, it is possible to refine current methods of managing and improving water and air pollution indexes. One such promoted use of blockchain technology interlocks sensors for light, air temperature, humidity, and environmental pollutants such as fine dust, greenhouse gases, soil contaminants, and wastewater (Lee, 2018).

### **3.10. Sharing economy sector**

As key players in the sharing economy, Uber and Airbnb have both created significant changes in the transportation and accommodation industries, respectively. In like vein, one influencer on the medical industry is Folding Coin, a project in which participants exchange the processing power of their computers to help cure cancer and other diseases in return for cryptocurrency coins. From this example, it is expected that blockchain technology will catalyze the acceleration of entities in the sharing economy. For example, every individual who produces value-added goods (e.g. electric power, artwork) will become a business operator. Accordingly, it is expected that this will usher in new era of global bartering and distribution of products and goods. As more stable transaction systems are established, the necessity for cryptocurrencies will also rise (Lee, 2018; Kyu-hwang, 2018; Kim, 2018).

### **3.11. Other fields for blockchain technology utilization**

Other applications of blockchain technology include the continuous and permanent management of reliable press releases, the accelerated growth of advertisements and travel products to attract tourists, the enlargement of a trustworthy and utilizable rental industry, the minimization of exhausting and unnecessary legal disputes or ideological conflicts, and widespread donation culture.

### 3.12. Problems that must be solved

There are several problems related to the extension of blockchain technologies. They are represented in Figure 3.

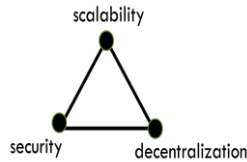


Fig. 3: A trilemma of problems related to blockchain technologies

To begin, the issues of scalability, security, and decentralization represent a three-fold challenge for the implementation of blockchain on a larger scale. In other words, focus on one issue may require modifications in relation to the other two.

Second, legal and regulatory guidelines must be considered. Current legal and institutional regulations regrettably fail to provide appropriate support for the blockchain ecosystem. Establishing the correct levels of support will be required for the blockchain ecosystem to take hold and flourish.

Third, a lack of human resources creates barriers to the full development of blockchain services.

Fourth, there is still a need for secure user authentication; thus, it is important to consider a variety of methods including multi-modal biometrics as well as identification cards or passwords that will enhance the user authentication process.

## 4. Forecast of Future Blockchain Markets

At the 2016 World Economic Forum in Davos, blockchain was chosen as a technology that will lead the Fourth Industrial Revolution. It was predicted that 10% of global GDP will be stored in blockchains by 2025. At the 2018 forum, blockchains were a core agenda item. There were heated debates among experts about how blockchains would offer reliability to digital information, create transactions between individuals, and change present society and its current systems. According to a report released by the International Data Corporation (IDC), an enterprise specialized in IT market analysis, the market for blockchains is expected to grow annually by 83%.

## 5. Developmental Trends of Representative Blockchain Technologies

### 5.1. Bitcoin Core

Bitcoin Core was the first blockchain-based technology developed by Satoshi Nakamoto and his colleagues. It was based on a paper Nakamoto published in 2009. Bitcoin Core is a source technology that enabled the distribution of bitcoins, the



most widely used cryptocurrency at present. Currently, the extension of Bitcoin's functionality and maintenance are carried out through its open source community (<https://bitcoinfoundation.org>, <https://bitcoin.org/ko>).

## **5.2. Ethereum**

Whereas Bitcoin Core specializes in payment and cryptocurrencies, Ethereum has a feature that enables users to freely define smart contracts with programming. Solidity, Ethereum's proprietary programming language, is mainly used for smart contract development. It is run on an Ethereum Virtual Machine (EVM) for the execution of smart contracts, and it is not dependent on any specific operating system, like Java Virtual Machine (JVM). In recent years, Ethereum has also provided binary codes for Raspberry Pi's IoT applications. Ethereum clients are implemented in many programming languages including C++, Go, and Python.

## **5.3. Hyperledger Fabric**

Hyperledger Fabric is a blockchain technology developed by the Hyperledger Project (<https://www.hyperledger.org>), which is a collaborative project of the Linux Foundation. Provided through open source, Hyperledger Fabric has a characteristic which enables strict identity management and the firsthand selection of agreement algorithms. It does not have a platform specific to a particular business model, yet it does present a technology standard that can be universally employed in many industries. Hyperledger Fabric uses "chain codes" to execute transactions, and these can be implemented in programming languages such as Go and Java. More than 150 enterprises and organizations around the world such as IBM, Accenture and JP Morgan are participating in this project.

## **6. Conclusions**

This paper has provided a general overview of key features of blockchain technology and its three types: public, private, and consortium. In addition, current uses and possible future uses of blockchain technology were discussed alongside major case applications. Recent blockchain technology development trends and development methods with key programming languages (e.g. Go, C ++, Python, Java, Solidity) were also briefly reviewed.

Certainly, blockchain is a technological breakthrough that can deliver and manage critical digital assets on highly reliable network environments; however, if users employ a rudimentary security authentication scheme—such as passwords—when they want to access a blockchain network, it can cause vulnerability to leakage and illegal or fraudulent use. In such cases, trust in the network will collapse. In order to address these problems, we intend to study and present a method for enhanced user authentication security technology that incorporates other technologies such as biometric authentication. We will also pay greater attention to a blockchain-based mobile voting system that will enable the realization of direct

democracy in a representative democracy. Furthermore, we are interested in solving blockchain's challenging trilemma: scalability, security, and decentralization.

It is clear that blockchain technology is emerging as a key infrastructure technology that will lead the Fourth Industrial Revolution. Blockchain infrastructure technology is expected to become very important in promoting mutual harmony and understanding of the complex structure and various social and human phenomena. This technology will lead to a more transparent and fairer society as creators innovate developments in various fields such as politics, economy, culture, education, business, and industry.

## 7. Acknowledgements

This work was supported by Youngsan University Research Fund of 2019.

## References

Dan, et al. (2016). Blockchain in health. *Ernst & Young*, <https://www.hyperledger.org/wp-content/uploads/2016/10/ey-blockchain-in-health.pdf>.

IRS Global. (2019). Blockchain related global market and business trends. *Market Report*.

Islam, A., Kader, M. & Shin, S. Y. (2019). A blockchain-based smart and secured scheme for question sharing in the smart education system. *Journal of information and communication convergence engineering*, 17(3).

Kim, C. (2018). An online voting system based on ethereum block-chain for enhancing reliability. *Journal of the Korea Academia-Industrial cooperation Society*. 19(4), 563-570.

Kim, E. (2018). A study for the innovativeness of blockchain. *The Journal of Society for e-Business Studies*, 23(3), 173-187.

Kim, J. (2019). Latest trends and major case studies of blockchain technology. *International Journal of Hybrid Information Technology*, 12(2), 1-6.

Kyu-hwang, A. & Hwajeong, S. (2018). Donate system development using Blockchain technology. *Journal of the Korea Institute of Information and Communication Engineering*, 22(5), 812-817.

Lin, I. C. & Liao, T. C. (2017). A survey of blockchain security issues and challenges," *international journal of network security*, 19(5), 653-659.

Lee, I. (2018). A study on blockchain networking for internet of things. *Journal of Digital Convergence*, 16(8), 201-210.

Lee, I. (2018). Blockchain evaluation indexes and methods to vitalize a blockchain-based digital sharing economy. *Journal of Digital Convergence*, 16(8), 193-200.

Lee, R. & Lim, J. Electronic voting systems using the blockchain. *Journal of the Korea Institute of Information and Communication Engineering*, 23(1), 103-110.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *White Paper*, Available: <http://bitcoin.org/bitcoin.pdf>.

Nomura Research Institute. (2016). Survey on blockchain technology and related services. *FY2015 Report*.

Pirtle, C. & Ehrenfeld, J. (2018). "Blockchain for healthcare: the next generation of medical records. *Journal of Medical Systems*, 42, 172.

Public blockchain vs Private blockchain, Retrieved September 5, 2018 from <https://tokenpost.kr/terms/5822>.

Ripple Labs Inc. (2018). Ripple: A Primer. *White Paper*. Available site: <https://bravenewcoin.com/assets/Whitepapers/ripple-primer.pdf>.