International Journal of Hybrid Information Technology
Vol.12, No.2 (2019), pp.1-6
http://dx.doi.org/10.21742/ijhit.2019.12.2.01

# Latest trends and Major Case Studies of Blockchain Technology

Kim Jin-Whan

*School of Computer Engineering, Youngsan University, Korea*
*kjw@ysu.ac.kr*

***Abstract***

*As one key infrastructure technology to lead the Fourth Industrial Revolution, blockchain technology is expected to bring about exciting developments across a variety of fields, such as politics, economy, culture and education. This paper is intended as a general overview of the main features of blockchain technology. In addition, the latest trends and development methods of 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 render human society more transparent and fair.*

***Keywords:*** *Blockchain, Case study, Public, Private, Consortium, Bitcoin, Ethereum*

## 1. Overview of blockchain technology

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 managements transaction information on the computers of participants connected to the P2P network instead of on a centralized server of a certain organization [1][2][3].

Blockchains can be divided into three types: public blockchain, private blockchain, and consortium blockchain. Each type has its characteristics, and they are different slightly in their functions and structures [4].

## 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 (virtual money) currently in circulation around the world. Naturally, public blockchains are being actively researched in the financial field [5][6].

**Article history:**
Received (April 2, 2019), Review Result (May 28, 2019), Accepted (June 24, 2019)

Print ISSN: 1738-9968, eISSN: 2652-2233 IJHIT

### 1.2. Private blockchain

A private blockchain is a relative concept of a public blockchain. 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 introduces blockchain technology to a centralized structure as a method to enhance security. Unlike a public blockchain, the private type is managed independently by one managing entity. Only those 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.

### 1.3. Consortium blockchain

A consortium blockchain is one in which only those users who satisfy certain requirements or have agreed 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 transact while giving 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.

## 2. Major technologies in the blockchain

In the 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.

### 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. 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.

### 2.6. 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.

### 2.7. 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), Proof of Importance (PoI), and Practical Byzantine Fault Tolerance (PBFT).

## 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 business. International remittances and issuances of letters of credit and management in trade can proceed at lower cost and higher speeds.

### 3.2. Crowdsourcing

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. In addition, the use of blockchain technology in crowdfunding is increasing. The ability of individuals or companies with an idea for a product or service to invite public participation through the Internet to raise funds is a major advantage of crowdfunding.

### 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.

### 3.4. Licensing and payment system sector

Blockchain-based cryptocurrencies are used in a variety of payment systems. A representative domestic case is the pay coins of Danal Co., Ltd. In addition, these cryptocurrencies can be widely used in areas where licenses are 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 medical institutions incur. One important contribution would be the recording of medical records on the blockchain so that patients' unique medical records can be easily accessed from anywhere within the industry [7][8].

### 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.

### 3.7. Electronic government, public sector

Central and local governments have the opportunity to employ blockchain-based administrative services for a variety of tasks: official record keeping, online electronic voting, education, taxation, new and renewable energy management and related transactions [9][10].

### 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 methods of managing and improving water and air pollution indexes. One such promoted use of blockchain technology interlocks sensor devices for light, air temperature, and humidity as well as environmental pollutants such as fine dust, greenhouse gases, soil pollution, and wastewater [11].

### 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 FoldingCoin, 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. Every individual who produces value-added goods (e.g. electric power, artwork) will become a business operator [12][13][14].

## 4. Developmental trends of representative blockchain technologies

### 4.1. Bitcoin Core

Bitcoin Core was the first blockchain-based technology developed by Satoshi Nakamoto and his colleagues 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.

### 4.2. 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.

### 4.3. 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 that 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.

## 5. Conclusion

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. That is, the trust in the network will collapse. 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.

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 fair society as creators innovate developments in various fields such as politics, economy, culture and so on, as well as innovation of education and industry, business model.

But, 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.

## Acknowledgments

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

## References

[1] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," International Journal of Network Security, vol.19, no.5, pp.653-659, Sep, **(2017)** DOI: 10.6633/IJNS.201709.19(5).01

 

[2] IRS Global, “Blockchain Related Global Market and Business Trends,” Market Report, **(2019)**
[3] Nomura Research Institute, “Survey on blockchain technology and related services,” FY2015 Report, **(2016)**
[4] Public Blockchain vs Private Blockchain, Retrieved September 5, from https://tokenpost.kr/terms/5822, **(2018)**
[5] Ripple Labs Inc., “Ripple: A primer,” White Paper, Available site: https://bravenewcoin.com/assets/Whitepapers/ripple-primer.pdf, **(2018)**
[6] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” White Paper, A-vailable: http://bitcoin.org/bitcoin.pdf, **(2008)**
[7] Pirtle C. and Ehrenfeld J. “Blockchain for healthcare: the next generation of medical records?” Journal of Medical Systems, vol.42, article no.172, **(2018)** DOI: 10.1007/s10916-018-1025-3
[8] Dan Gietl et al., “Blockchain in health,” Ernst & Young, https://www.hyperledger.org/wp-content/uploads/(2016)/10/ey-blockchainin-health.pdf, **(2016)**
[9] Chul-Jin Kim, “An online voting system based on Ethereum block-chain for enhancing reliability,” Journal of the Korea Academia-Industrial cooperation Society, vol.19, no.4, pp.563-570, **(2018)**
[10] Roo-daa Lee and Joa-sang Lim, “Electronic voting systems using the blockchain,” Journal of the Korea Institute of Information and Communication Engineering, vol.23, no.1, pp.103-110, Jan, **(2019)** DOI: 10.6109/jkiice.2019.23.1.103
[11] Il-Gu Lee, “A study on blockchain networking for internet of things,” Journal of Digital Convergence vol.16. no.8, pp.201-210, **(2018)** DOI: 10.14400/JDC.2018.16.8.201
[12] Il-Gu Lee, “Blockchain evaluation indexes and methods to vitalize a blockchain-based digital sharing economy,” Journal of Digital Convergence vol.16, no.8, pp.193-200, **(2018)** DOI: 10.14400/JDC.2018.16.8.193
[13] Kyu-hwang An and Hwajeong Seo, “Donate system development using Blockchain technology,” Journal of the Korea Institute of Information and Communication Engineering, vol.22, no.5, pp.812-817, May, **(2018)** DOI: 10.6109/jkiice.2018.22.4.812
[14] Euiseok Kim, “A study for the innovativeness of blockchain,” The Journal of Society for e-Business Studies vol.23, no.3, pp.173-187, **(2018)** DOI: 10.7838/jsebs.2018.23.3.173

## Authors

**Jin-whan Kim**
Received a BS degree in computer and statistics from Pusan National University in 1989, and MS and Ph.D. in computer and science from Yonsei University, Seoul, Korea, in 1992 and Pusan National University, Pusan, Korea, in 2006, respectively. He is an associate professor in Youngsan University. His research areas are dynamic signature verification, on-line character recognition, voice processing, multi-modal biometric system, ubiquitous computing and blockchain technology.
Phone: +82-55-380-9331
E-Mail: kjw@ysu.ac.kr