ISSN 2951-2727

치안과학기술리뷰

Police Science Technology Review

통권 4호 | 2023. 6. VOL.01

법과학융합연구 특집

Forensics Study Edition

경찰대학 치안정책연구소
Korean National Police University Police Science Institute

Change in Security Paradigm: Blockchain Security

Dongguk University Graduate School of International
Affairs and Information Security,
Director of Research Center of Blockchain,
Sung Jun Park

deb_blockchain@anduschain.io

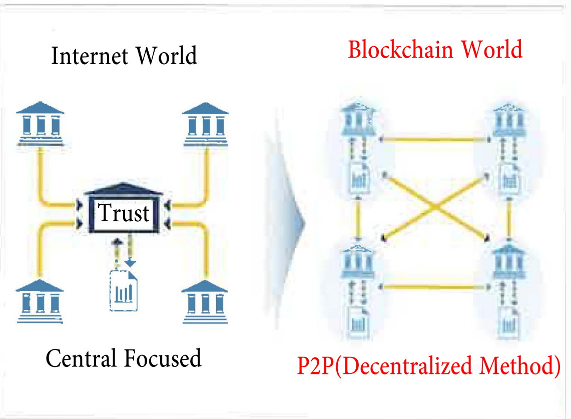
I Study's Background and the Necessity

Currently, we are at a point of rapid transition from the Internet world, following the trends brought about by technological advancement, to a blockchain-based world built on the philosophy of 'mutual coexistence.' In the past, the author emphasized the need for preparedness in cybersecurity, stating opinions about the potential for various types of cybercrimes that were not previously considered. This was due to the rapid increase in internet usage among criminals and information security issues in the cyber world as the internet revolution (information revolution) dawned in the 1990s. his meant that we needed to go beyond the simple concept of cybersecurity and also introduce the concept of cyber security. Already, our response capabilities towards cybersecurity have been continuously developing and becoming more sophisticated. Just like the experiences from these precedents, at this current moment of rapid transition from the internet world to the blockchain world, we now need to thoroughly prepare for blockchain security, moving beyond just cybersecurity.

In relation to this, as one of the various considerations, we have explained in the appendix a five-step process for sound judgment of cryptocurrency, particularly to prevent cryptocurrency scams in advance.

1. The Birth of Bitcoin

Generally, when people think of blockchain, they think of cryptocurrency (virtual assets or digital assets), and when they think of cryptocurrency, they associate it with Bitcoin. However, while Bitcoin is the first P2P cryptocurrency created using the concept of a distributed ledger, the clear fact is that it is not based on blockchain. What is important here is that the essence Bitcoin shows us is not a world of centralization, but the existence of a decentralized P2P world. Of course, the existence of a P2P world here means a reliable P2P ecosystem (business models, etc.) (see Figure 1).



<Diagram 1> Internet World and Block Chain World

2. The Birth of Bitcoin

By demonstrating that Bitcoin exists in a decentralized P2P world, we have opened the possibility of transitioning all currently centralized ecosystems into decentralized P2P ecosystems. However, Bitcoin had an issue transitioning all ecosystems into a P2P ecosystem because its sole purpose was to be a P2P cryptocurrency. The concept of blockchain, which improved these drawbacks of Bitcoin, made it possible to transition all current ecosystems into a P2P ecosystem, which led to the birth of Ethereum. Ultimately, the concept of blockchain, speaking specifically as the computers we know, is that the definition of Ethereum is a global trust computer, and this is exactly the definition of blockchain. That is, to give a simple example of the difference between Bitcoin and Ethereum, it can be understood as the innovative evolution that occurred from a simple telephone to a smartphone.

3. The Purpose of a Blockchain Computer

To understand the vision and purpose of a blockchain computer, one must understand its four functions. Those functions are as follows:

① Cryptocurrency issuance: Issuing a cryptocurrency with various characteristics and functions

② Smart contract: Software that manages/controls digital assets

③ Digital assets: Assets whose ownership of digital assets is managed/controlled by a smart contract

④ DAO (Decentralized Autonomous Organization): An equal P2P horizontal organization where everyone is equal.

1) Cryptocurrency:

As can be seen, the existence of a cryptocurrency issuance feature allows anyone to easily issue a cryptocurrency with any characteristics. There are many misconceptions about cryptocurrency among the general public. To be clear, the cryptocurrency discussed in blockchain has the following three goal-oriented characteristics:

① Decentralization (distribution) concept: A P2P method, not a centralized approach

② Application of cryptographic technology: The safety of cryptocurrency relies on cryptography

③ Digital representation of value: Representing the value and rights of digital assets

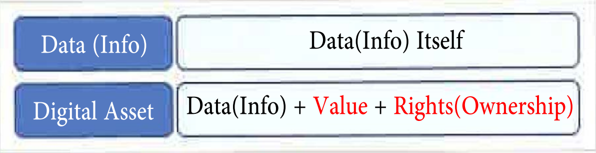
2) Smart Contract:

The smart contract mentioned in blockchain is the 'software' we know. However, a smart contract is a special-purpose software, specifically a software whose purpose is to manage and control digital assets.

3) Digital Assets:

Above all, the most crucial concept is that of digital assets. Blockchain computers are for the digital asset revolution. Digital assets, simply put, can be thought of as data with value. However, the core elements of an asset are value and ownership.

The differentiated characteristics between simple data and digital assets are determined by whether value and ownership are combined. This is a critical distinction.



<Diagram 2> Comparison of Data and Digital Asset

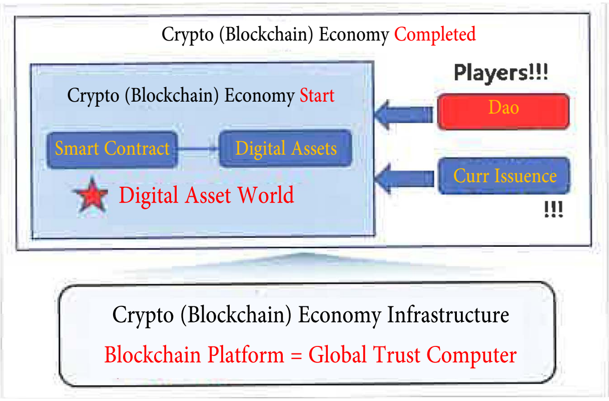
The simplest example of digital assets is personal information. In the current internet world, personal information is perceived merely as data for storage and management. However, in the world of blockchain, personal information is stored, managed, and used as a digital asset. The most crucial factor in this storage and management is the relationship between cryptocurrencies and digital assets. According to the third characteristic of cryptocurrencies, digital assets are expressed by the value and ownership given by cryptocurrencies. Consequently, digital assets and cryptocurrencies can be considered the same concept.

4) Decentralized Autonomous Organizations (DAO)

The concept of DAO, the last of the four functions of blockchain computers, can be explained as follows. If we look at the organizational relationship of a company, rather than having a hierarchical organization with ranks such as CEO, department heads, etc., it can be described as a P2P horizontal organization where everyone has equal authority and responsibility.

As explained above, through these four functions of the blockchain computer, the changing force of invisible technology-based change signals a transformation into a world where digital asset transactions are possible.

This enormous change heralds a new paradigm of digital asset trading economy, known as crypto-economy (or blockchain economy).


Crypto (Blockchain) Economy Completed
Players!!!
Crypto (Blockchain) Economy Start
Dao
Smart Contract
Digital Assets
Curr Issuence
Digital Asset World
!!!
Crypto (Blockchain) Economy Infrastructure
Blockchain Platform = Global Trust Computer

<Diagram 3> CryptoEconomics(Digital Asset Economics)

Ⅱ From Cyber Security to Blockchain Security

The currently successful cyber security is defined as the security in the cyber world, and blockchain security can be defined as security in the blockchain world. The differences between cyber security and blockchain security can be explained in two main areas. The first is the change in the characteristics of the security target, and the second is the change in the management and operation method. Above all, due to the fundamental difference between cyber security and blockchain security, it is necessary to establish a blockchain security department instead of expanding the cyber security department.

1. Changes in the characteristics of the security target

The most important objective of security in the blockchain world would probably be to analyze the digital asset ecosystem and solve security-related problems

The biggest feature of the digital asset ecosystem is P2P. This implies that digital assets move freely without borders. In fact, it is undeniable that the backdrop of Bitcoin's activation is due to the use by criminal organizations. Therefore, since 2015, the G7 and the FATF (Financial Action Task Force) have started regulatory cooperation against digital asset transactions and related actors, and in the 2019 FATF General Assembly, they stated, "In the newly applied guidelines, digital asset service providers must comply with anti-money laundering (AML) and counter-terrorist financing (CFT) regulations at the same level as traditional financial institutions" and created the recommendation as follows.

① The identity of both parties in a funds transfer must be verified.
② A process must be developed to share related information with other virtual asset handlers and the judiciary.
③ Users' identities must be identified, and appropriate inspections must be carried out to prevent illegal activities.
④ A program to alert the risks of specific businesses should be developed.

Based on this, South Korea enacted the Act on Reporting and Use of Certain Financial Transaction Information (Special Act) in 2020 and has been implementing it since September 2021. The core objective of the Special Act is to prevent money laundering and tax evasion. For this, the essence is to prepare a plan to track and manage the flow of cryptocurrencies centered on cryptocurrency exchanges (virtual asset operators), with the same concept that manages the existing financial ecosystem. Nevertheless, due to the P2P nature of cryptocurrencies, many problems arise, such as cryptocurrency transactions that do not use the regulated cryptocurrency exchanges. These issues need to be resolved promptly.

2. Change in Security Response Method

As explained in the change in the characteristics of the security target, the blockchain world is a P2P world unlike the Internet world. It is believed that it is desirable to switch to a P2P method, not from the perspective of a centralized approach. The current cyber security is centered around the main department (Police Agency), but blockchain security needs to be transformed into a national security measure where the main department and all citizens participate in security measures together. The existing community policing measures, such as the self-policing teams in operation, can be referred to. This should be formalized and expanded so that the Police Agency and all citizens cooperate closely to develop blockchain security measures together. This means transitioning from the current centralized security management and operation (based on the Police Agency) to a decentralized security method where citizens participate together. Ultimately, we can consider a security policy and management system that involves citizen participation. Of course, sudden changes in management and operation methods can cause various problems, so a hybrid organization that combines centralized and decentralized organizations is suggested as an intermediate step.

For example, the central organization, akin to a control tower, would be managed by the Police Agency, and a decentralized method that allows as many citizens as possible to participate is suggested.

3. Establishment of a Dedicated Blockchain Security Department

Blockchain security has fundamentally different types and characteristics from cyber security. Therefore, a new organization based on the concept of a Blockchain Crime Investigation Team, capable of analyzing and resolving these characteristics, needs to be established.

The most important role of the organization under the Blockchain Crime Investigation Team concept is to focus not only on urgent blockchain security measures and policies but also on establishing medium- and long-term domestic blockchain security measures. For this, the most important thing is to recognize the important value that the Blockchain Crime Investigation Team needs to establish a close cooperation system with domestic blockchain and cryptocurrency experts.

III Urgent Blockchain Security Measures

Because the existing cyber security and blockchain security fundamentally deal with different worlds, essential innovation needs to occur in the security methods. This is because the traditional centralized security method has its limitations in achieving blockchain security. Taking these characteristics into account, even if the ultimate direction of blockchain security is to be established later, we propose several urgent blockchain security measures.

① Analysis of cryptocurrency-related crime types and characteristics
⇒ Analysis of unhealthy cryptocurrency issuance and distribution systems
⇒ Cryptocurrency price manipulation methods
⇒ Cryptocurrency hacking
⇒ Types of cryptocurrency-related fraud, etc.
② Development and application of cryptocurrency flow tracking technology
⇒ Tracking the cryptocurrency of criminals
③ Rebuilding of global cooperation for cryptocurrency-related crime both domestically and internationally
⇒ Building a cooperative system with domestic departments related to cryptocurrency
⇒ Establishing a global cooperation system for cryptocurrency-related crime with organizations like Interpol

IV Conclusion

The reality is that there is much confusion in the market due to misunderstandings about blockchain and cryptocurrencies, and many crimes related to cryptocurrencies, such as cryptocurrency fraud, are occurring because of a lack of understanding of the massive changes in the world brought about by blockchain technology and the definition of blockchain. However, the most important core is that the internet world (centralized world) is being innovated into the blockchain world (decentralized world), and at the center of it is cryptocurrency (digital asset).

Just as the concept of physical security expanded into cyber security with the transition from the physical world to the internet world, it is clear that an expansion into blockchain security is now necessary, and there is an undeniable reality that swift adoption is required. The simplest example is that hackers are now demanding cryptocurrencies such as Bitcoin instead of cash. To achieve this, a 'together' preparation through accurate and concrete understanding of blockchain and cryptocurrency (digital assets) is needed. A similar example is the 'token securities' currently being pushed by financial authorities. However, what blockchain and cryptocurrency experts are talking about here is tokenization of securities, not securitization of tokens.

While blockchain security may still sound abstract and conceptual, like the existence of cryptocurrency based on blockchain, we need to concretize each step with the blockchain philosophy and thought of 'together,' and we must prepare in advance before it's too late. In particular, what I want to emphasize is that there could be limitations to blockchain security in the new area using only the existing cyber security methods, so a new method, a blockchain operating method introduced with blockchain, is needed.

Addendum

[Five Steps for Judging a Sound Cryptocurrency]

■ **Step 1: Existence of a White Paper**

⇒ All projects must have a concrete description (a kind of business plan) of the token ecosystem innovation they wish to achieve.

■ **Step 2: Existence of the digital asset represented by the cryptocurrency**

⇒ Analyze what digital asset the issued token represents.

■ **Step 3: Rationality of the value of the digital asset and the value of the cryptocurrency**

⇒ Analyze whether the price of the cryptocurrency appropriately represents the value of the corresponding digital asset (analyze for any bubble).

■ **Step 4: Existence of a crypto-economic profit model**

⇒ This is the most important item. Analyze the balance between the rewards paid to customers and the company's profits (the profits should be larger than the rewards).

■ **Step 5: The soundness of the company (especially, the credibility of the executives, including the CEO)**

⇒ Assess the technical feasibility of realizing the token ecosystem/most importantly, judge the credibility of the CEO, etc.