Survey on Blockchain Technologies and Related Services

FY2015 Report

March 2016

Nomura Research Institute

(This report is the result of the survey contracted by
Japan's Ministry of Economy, Trade and Industry (METI))

Contents

1 Background and Objective of the Survey

Compared with conventional centralized systems, blockchain technologies used for transactions of value records, such as bitcoins, structurally have the characteristics that

(i) enable the creation of a system that substantially ensures no downtime

(ii) make falsification extremely hard, and

(iii) realize inexpensive system.

Blockchain technologies are expected to be utilized in diverse fields including IoT.

Japanese companies just started technology verification independently, and there is a risk that the initiative might be taken by foreign companies in blockchain technologies, which are highly likely to serve as the next-generation platform for all industrial fields in the future.

From such point of view, this survey was conducted for the purpose of

- comparing and analyzing details of numbers of blockchains and advantages/challenges therein;
- ascertaining promising fields in which the technology should be utilized;
- ascertaining the impact of the technology on society and the economy; and
- developing policy guidelines for encouraging industries to utilize the technology in the future.

This report compiles the results of interviews with domestic and overseas companies involving blockchain technology and experts.

The content of this report is mostly based on data as of the end of February 2016. As specifications of blockchains and the status of services being provided change by the minute, it is recommended to check the latest conditions when intending to utilize any related technologies in business, etc.

2 Terms and Abbreviations Used in This Report

Terms and abbreviations used in this report are defined as follows.

Terms	Explanations
BTC	Abbreviation used as a currency unit of bitcoins
FinTech	A coined term combining Finance and Technology; Technologies and initiatives to create new services and businesses by utilizing ICT in the financial business
Virtual currency / Cryptocurrency	Bitcoins or other information whose value is recognized only on the Internet
Exchange	Services to exchange virtual currency, such as bitcoins, with another virtual currency or with legal currency, such as Japanese yen or US dollars; Some exchange offers services for contracts for difference, such as foreign exchange margin transactions (FX transactions)
Consensus	A series of procedures from approving a transaction as an official one and mutually confirming said results by using the following consensus algorithm
Consensus algorithm	Algorithm in general for mutually approving a distributed ledger using Proof of Work and Proof of Stake, etc.
Digital signature	⇒ p.7
Token	Virtual currency unique to blockchains; Virtual currency used for paying fees for asset management, etc. on blockchains is referred to as a token.
Node	A relay point, branch point, terminal in a communication network; In this report, a node refers to a terminal in a blockchain network.
Hash value / Hash function	⇒ p.7
Public **Consortium** **Private**	Blockchains are classified depending on whether the participation in a consensus (a process for network participants to approve the same ledger) is open to anybody (public), restricted (consortium), or limited to a certain body (private) ⇒ p.25
Bitcoin	The entirety of the mechanism composed of virtual currency,

	bitcoins; When referring to individual elements, an expression specifying each element is added, such as “bitcoins as virtual currency” or “value of bitcoins.”
Proof of Concept (PoC)	To build a simple system to examine new services and systems and carry out the confirmation using said system
Blockchain	This term refers to a blockchain as a general noun, including a distributed ledger, such as Ripple; When referring to that of the Bitcoin or other individual blockchains, clearer expressions are used, such as the “Bitcoin blockchain” or the “Ethereum blockchain.” ⇒ p.11

Abbreviations	Original terms
BTC	→ See the above explanation of the term
IoT	Internet of Things
P2P	Peer to Peer ⇒ p.9
PoC	Proof of Concept → See the above explanation of the term
PoI	Proof of Importance ⇒ p.24
PoS	Proof of Stake ⇒ p.24
PoW	Proof of Work ⇒ p.9

3 History of the Bitcoin and Bitcoin Blockchain

This Chapter outlines Bitcoin, from which blockchains were originated, as well as the Bitcoin blockchain, while compiling how blockchains have been created in the process of the development of the mechanism of Bitcoin.

3.1 Thesis by Satoshi Nakamoto

At the end of November 2008, a thesis was posted by a person named Satoshi Nakamoto on a US mailing list where cryptographers exchange information. This is the very beginning of Bitcoin.[1] In his thesis titled "Bitcoin: A Peer-to-Peer Electronic Cash System," Nakamoto cited the following as the characteristics of Bitcoin:[2]

- Enable direct transactions without the need for trusted third parties;
- Enable non-reversible transactions;
- Reduce credit cost in small casual transactions;
- Reduce transaction fees; and
- Prevent double-spending.

After discussions held on the mailing list for a while, the first block was created in January 2009 and the operation of Bitcoin and Bitcoin blockchain was commenced.

Since then, the Bitcoin system has never been suspended (called no/zero downtime, etc.),[3] and users have been increasing worldwide, not only in the United States. In Japan, the collapse of an exchange in early 2014 attracted people's attention, but people also came to be interested in blockchains in 2015 amid increasing momentum for FinTech.

[1] http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
[2] https://bitcoin.org/bitcoin.pdf
[3] Consistency was once lost temporarily. https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

3.2 Characteristics of Bitcoin

Bitcoins are called virtual currency or cryptocurrency and are distributed while discovering value in the data itself managed by the software.

Fig. 3-1 shows the comparison between bitcoins, legal currency (coins and bills), and electronic money (prepaid payment instruments for third-party business under the Payment Services Act). In the case of bitcoins, for which there is no clear issuer, unlike legal currency and electronic money, the trust in the Bitcoin system itself supports the value of bitcoins. Furthermore, the fact that transaction records are disclosed, although under anonymity, and are traceable is another unique feature of bitcoins.

Fig. 3-1 Bitcoins, legal currency and electronic money

Characteristics		Bitcoins	Legal currency (Japanese yen)	Electric money (prepaid payment instruments for third-party business)
Issuance / Management	Issuer	■ Automatically issued by the system	■ Government of Japan (currency) ■ Bank of Japan (bills)	■ E-money service providers (Issuers of prepaid payment instruments for third-party business)
	Manager	■ Managed by P2P network participants	■ Government of Japan ■ Bank of Japan	■ E-money service providers (Issuers of prepaid payment instruments for third-party business)
Value	Issuance cap	■ Specified (21 million BTC)	■ None	■ Issued within the amount (Japanese yen) deposited in advance
	Grounds for value	■ Trust in the system	■ Trust in the Government of Japan	■ Deposited Japanese yen (1/2 of the deposited amount) ■ Trust in relevant e-money service providers
Money transfer	Transfer direction	■ Two-way	■ Two-way	■ One-way (Users ⇒ Member stores)
	Required time	■ Create a block every ten minutes ■ Considered to be finalized in approximately 60 minutes[4]	■ Immediately in the case of direct receipt ■ It may take time when transferring a large amount of money to a distance	■ Several days to 1.5 months until payments to member stores are completed
	Transfer fees	■ Small amount[5] ■ Borne by senders	■ Expensive ■ Borne by the both sides as the case may be	■ Borne by receivers (member stores)
Anonymity	Anonymity of transactions	■ Transaction records are clear but anonymous	■ High anonymity	■ Low anonymity (records are managed by relevant e-money service providers)
	Disclosure of transaction records	■ Disclosed	■ Undisclosed	■ Generally undisclosed

[4] Some say that the transfer of bitcoins is fast, which is only true when compared with international money transfer between banks, etc. When compared with general settlement means, it is rather slow.

[5] Transfer fees are decided based on the volume of data to be sent, instead of the amount of money to be transferred. Therefore, fees may be more expensive in the case of transferring small amount of money.

By the end of February 2016, approximately 15.26 million BTC of bitcoins were issued,[6] which is equivalent to 6.66 billion US dollars.[7] The value of 1 BTC hit a record high exceeding 1,100 US dollars in December 2013. However, after that, due to external factors, such as regulations introduced by respective countries and the abovementioned collapse of an exchange, the value declined and bitcoins were traded at below 450 US dollars as of the end of February 2016.

[6] https://blockchain.info/ja/charts/total-bitcoins
[7] https://blockchain.info/ja/charts/market-cap

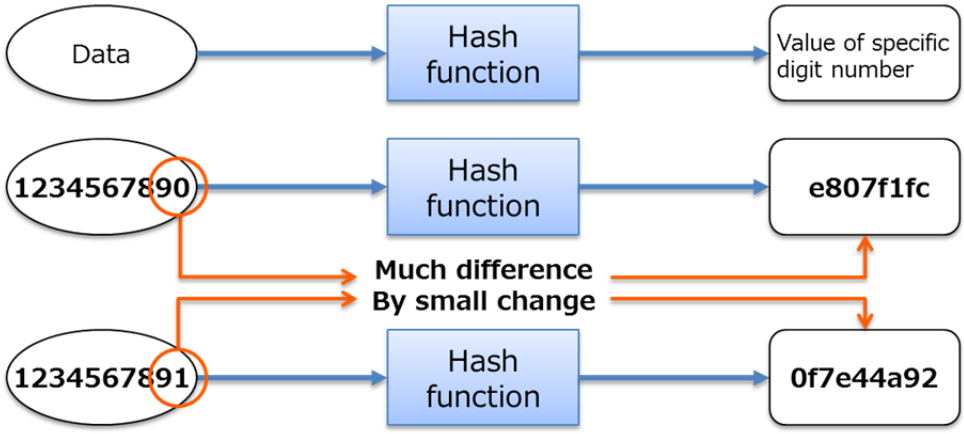
3.3 Main Technologies Constituting Bitcoin

Bitcoin is considered to have created new functions by combining existing technologies. In order to operate a system like the one for electronic money, without any central authority, it is indispensable to put in place measures to prevent falsification of data and duplicate payments, as well as a mechanism to maintain the system against any attacks by malicious users. Major technologies constituting Bitcoin (hash, public-key cryptography and digital signature, P2P, Proof of Work) are outlined below.

3.3.1 Hash

Inputting data into a hash function causes the output of a hash value with a certain number of digits. This mechanism is characterized by the fact that the same hash value is obtained from the same data but only a slight difference in the original data results in a completely different hash value. It is extremely difficult to infer the original data based on a hash value. Taking advantage of such characteristics, this mechanism is used for the detection of falsification of data, and in the Bitcoin system, it is used for the verification and guarantee of the continuity of blockchain data and the creation of blockchains through Proof of Work utilizing the calculation of hash values.

Fig. 3-2 Mechanism of hash

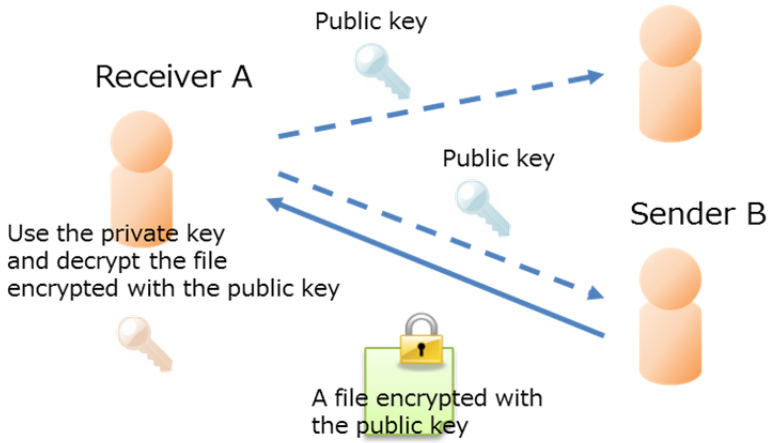


3.3.2 Public-key cryptography and digital signature

Public-key cryptography is a cryptographic method using different keys for encryption and decryption. The problem of handing over keys was solved by dividing the key into one for private

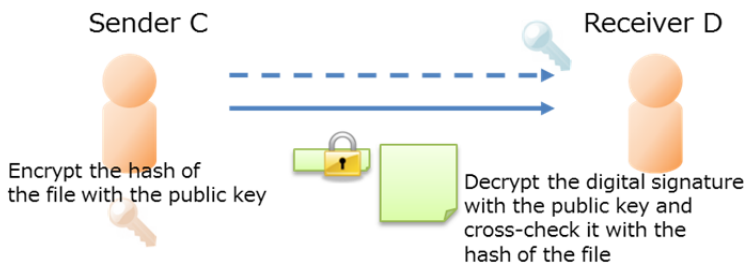
use (private key) and one available for anyone (public key). In the case of symmetric-key cryptography using the same key for encryption and decryption, various safety measures for delivering the key only to the relevant counterparty are required. In contrast, public-key cryptography enables safe delivery and receipt of files only if a receiver prepares a pair of a private key and a public key and delivers the public key to the sender in advance. Safety can be maintained even though other persons use the public key as long as the receiver properly manages his/her private key.

Fig. 3-3 Mechanism of public-key cryptography



A digital signature refers to a mechanism to prove the authenticity of the data sent via a network and a pair of keys used in public-key cryptography is also used here. Generally, a digital signature, which is made by encrypting the hash value of a file to be sent to a receiver with the sender's private key, is sent to the receiver together with said file. The receiver uses the same hash function as the sender to create the hash value of the file by him/herself and cross-checks the created hash value with the hash value obtained through decrypting the sender's digital signature with the sender's public key, thereby confirming that the sender's digital signature is authentic.

Fig. 3-4 Digital signature



In the Bitcoin system, public-key cryptography and a digital signature are used for identifying a creator of transaction data (data of a bitcoin transaction) and as an address[8] of a bitcoin wallet.[9]

3.3.3 P2P

In a general client-server network, a server takes charge of preservation and provision of data while a client requests the server for data and gains access to them, and their roles are thus fixed. In contrast, in a P2P network, all participating nodes (referring to computers for communication; also called "peers") hold data respectively and create an autonomous network wherein data are requested and provided among these nodes on an equal footing. In a P2P network, roles of respective nodes as a server or a client are not fixed, unlike the case of a client-server network.

When adopting a P2P network, it is necessary to consider search methods and data transmission methods. Search methods are the means to manage locations of nodes and data, and representative examples include conducting management only with a P2P network, installation of an index server, and nodes with high processing power (super nodes) conducting management. Data transmission methods are means of transmitting data between nodes, and are divided into direct transmission between nodes and relayed transmission via another node.[10] In the P2P network used for Bitcoin, a P2P method is adopted as a search method, while data transmission is conducted by relaying respective nodes.

P2P networking technology has contributed to developing a base for a complete distributed network and eliminating single point of failure in Bitcoin. Furthermore, regarding blockchain data, which are explained later, all nodes that participate in the P2P network of Bitcoin and conduct mining are supposed to have the same data.

3.3.4 Proof of Work

Proof of Work (PoW) generally refers to a mechanism to confirm a person's innocence (or to discourage him/her to act wrong) by having him/her do a certain work: which is simple but troublesome, and his/her having actually done said work can be easily verified.[11] For example, a

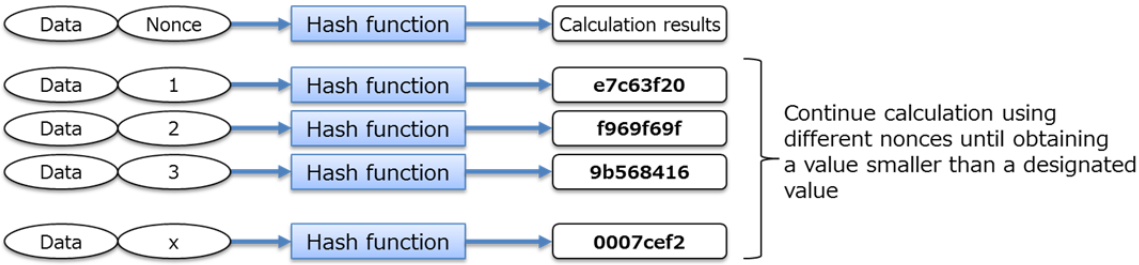
[8] ID number designated as an address to deliver bitcoins
[9] Sofware for managing bitcoins
[10] Materials for the "Working Group on Ideal P2P Network, Network Neutrality Committee" (Computer Communications Division, Ministry of Internal Affairs and Communications)
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/network_churitsu/pdf/wg2_061129_1_si_1_2.pdf
[11] Concrete examples of PoW include the one using hash, which is explained below, or CAPTCHA using images.

PoW algorithm called Hashcash[12] is adopted for sending emails. A certain hash calculation is obliged at each time of sending an email, thereby excluding spammers (those intending to deliver a large volume of emails generally want to cut time and cost as much as possible).

PoW is a work called mining in Bitcoin. Network participants calculate a hash value by adding a nonce (any given value) to the collection of transaction data delivered to them.[13] It is required to obtain a value smaller than a certain value,[14] and the participants have to continue calculations by using different nonces until they obtain the value as required. When anybody obtains the relevant value, network participants mutually confirm the correctness of the value and the collection of transaction data used for the calculations is approved to be official transaction results as a new block. Then, bitcoins are granted as a reward to the person who succeeded in obtaining the correct value through the calculations.[15] After that, all participants go on to the next mining using transaction data that were not included in said block and the newly created transaction data.

Bitcoin employs PoW to create a mechanism that can prevent falsification of data and duplicate payments without a central authority and can maintain the system against any attacks by malicious users.

Fig. 3-5 Hash calculations in a Proof of Work algorithm



[12] http://www.hashcash.org/

[13] When sending bitcoins, relevant transaction data are sent targeting the entirety of the P2P network. Therefore, transaction data that have reached each node may be different at a certain point in time, depending on the status of the P2P network.

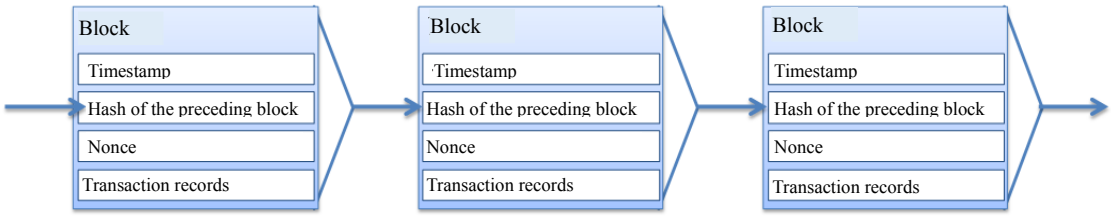
[14] It is automatically set in a manner that someone can obtain the correct value in ten minutes or so.

[15] The amount of a reward is now set to be 25BTC plus the sum of the fees for transactions incorporated in the relevant block. The reward (the abovementioned 25BTC) is to be halved once in every four years or so, and the next reduction is scheduled in approximately the summer of 2016.

3.4 Blockchains

A series of blocks created through PoW is a blockchain. Blocks compiling transaction data for a certain period of time (for approximately 10 minutes for Bitcoin) are linked into a chain and each block contains a timestamp, hash value of the preceding block, nonce, and information on transaction records included in the relevant block.[16]

Fig. 3-6 Blockchain



A fork may be generated temporarily in the Bitcoin blockchain in such cases as multiple nodes in a P2P network almost simultaneously succeed in PoW. In such a case, a chain that becomes longer thereafter is judged as the authentic one (Fig. 3-7). Therefore, in order to finalize a transaction, it is necessary to confirm that the relevant blockchain does not fork after the transaction data is incorporated in the block and multiple blocks are created thereafter. Generally, when approximately six blocks are additionally created, the relevant blockchain is considered to be the authentic one (such practice is often incorporated as a judgment system in a wallet that manages bitcoins).[17]

Blocks are thus linked into a chain in a manner that they keep past information. Therefore, in order to conclude an illegal transaction in the Bitcoin blockchain, it is necessary to continue creating blocks faster than the authentic fork or re-create all past blocks, which requires a 50% or larger percentage of the machine power (computing capacity) of all computers participating in PoW.[18] This mechanism is considered to have solved the Byzantine Generals Problem, which is explained later, to the extent practicable.

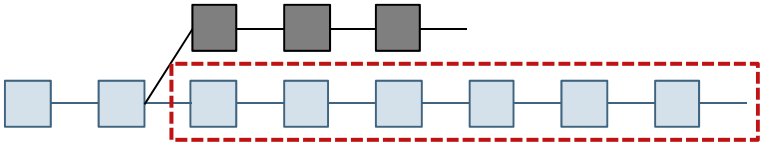
---

[16] More accurately, each block contains technical data, previous block hash, Merkle Root, PoW target, nonce, and timestamp, in addition to transaction data.
https://bitsonblocks.files.wordpress.com/2015/09/bitcoin_blockchain_infographic1.jpg

[17] It takes approximately 10 minutes to create one block. Therefore, creating six blocks requires approximately one hour.

[18] The percentage is often indicated as "51% or larger," but this is not accurate, just indicating the percentage of 50% or larger in a whole number. However, the term "51% attack" is generally used when referring to an attack to a blockchain, and therefore will be used hereinafter.

Fig. 3-7 A fork in a blockchain



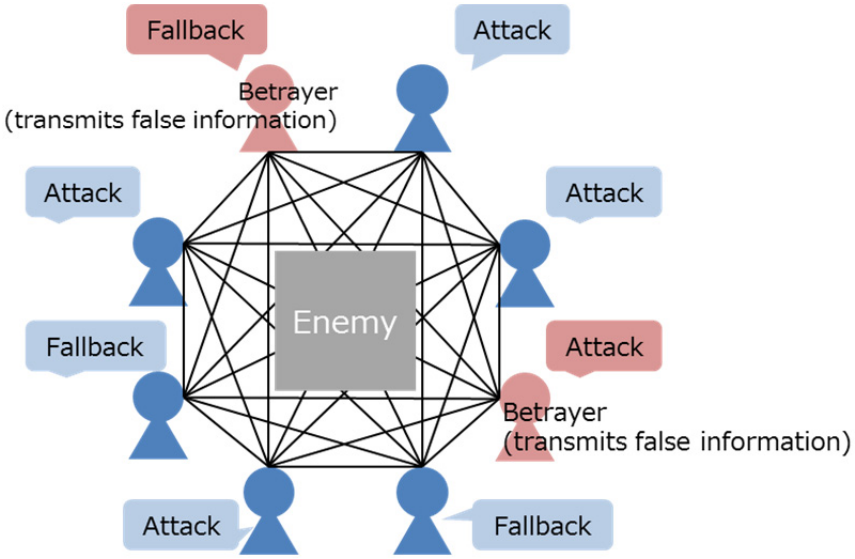
A longer chain is judged to be authentic.

3.4.1 Byzantine Generals Problem

The Byzantine Generals Problem is discussed in a thesis titled "The Byzantine Generals Problem,"[19] which was publicized by Leslie Lamport, et al. in 1982. This problem relates to the reliability in a group of components[20] in a distributed system.

Based on the idea whether generals of the countries that surround a hostile country can reach an agreement on strategies only through communicating with each other under circumstances where some of them are betrayers transmitting false information, it is questioned whether a proper consensus may be built when any group of components in a distributed system transmits false information.

Fig. 3-8 Byzantine Generals Problem



[19] http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf
[20] Meaning almost the same as a node or peer; This term is used here as in the relevant thesis.

According to Lamport et al., when the number of components transmitting false information is less than one-third of the total, a solution is obtained, or in other words, a proper consensus may be built as a whole. The percentage of participants who transmit false information among all participants decides whether a consensus may be built or not.

In the Bitcoin blockchain, a consensus or a decision of an authentic blockchain is made through PoW and mutual approval of the results thereof. As explained above, blocks are linked into a chain in a manner that they keep past information, and therefore, in order to conclude an illegal transaction as a consensus in the Bitcoin blockchain, it is necessary to continue creating blocks faster than the authentic fork or re-create all past blocks. This requires a 50% or larger percentage of the machine power of the entirety, and enormous computational resources are necessary. It is much more economically rational to obtain rewards through proper mining, which discourages people from conducting illegal transactions. This mechanism is said to have solved the Byzantine Generals Problem to the extent practicable.

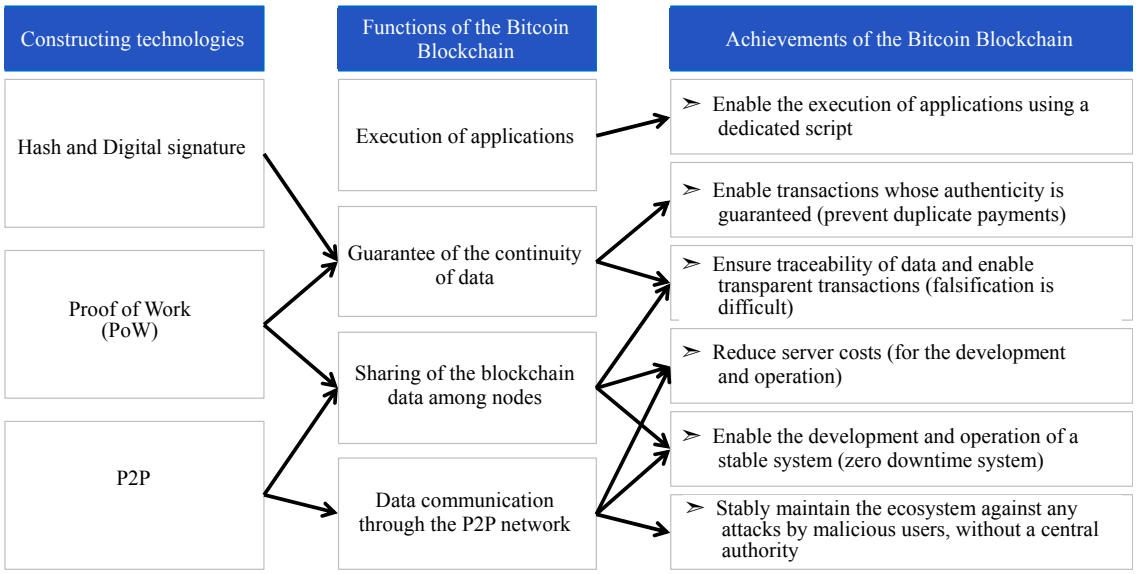
3.4.2 Functions and achievement of the Bitcoin blockchain

Bitcoin consists of major technologies, such as hash and digital signature, PoW, and P2P. Individual technologies are not novel, but the combination of existing technologies has created new functions in the Bitcoin blockchain.

Such combination has built a mechanism to prevent falsification of data and duplicate payments, as well as a mechanism to maintain the system against any attacks by malicious users, which are indispensable for operating a system like the one for electronic money, without any central authority.

Functions of the Bitcoin blockchain are roughly classified into four categories; “execution of applications,” “guarantee of the continuity of data,” “sharing of the blockchain data among nodes,” and “data communication through the P2P network.” Fig. 3-9 shows the outline of these functions and constructing technologies.

Fig. 3-9 Functions of the Bitcoin blockchain



In the Bitcoin blockchain, each node is connected to the P2P network, which works to ensure higher fault tolerance than a client-server system. Each of these nodes connected to the P2P network holds the blockchain data for which a consensus has been built through PoW.

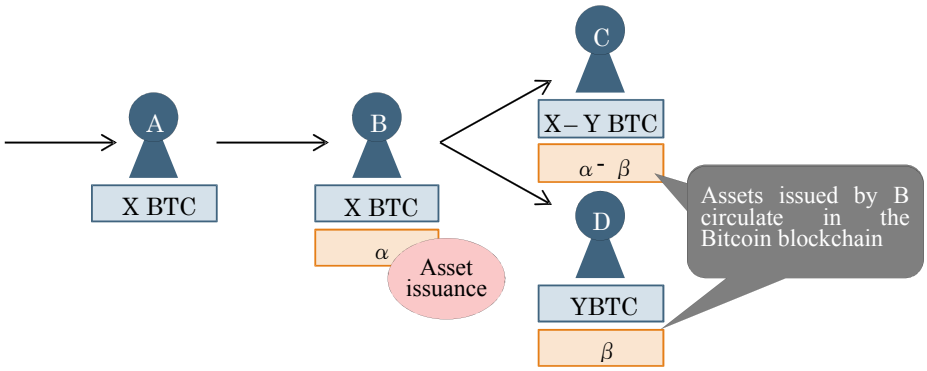
In the Bitcoin blockchain, blocks (and data in each block) are related to each other through continuing hash calculations and digital signatures. Furthermore, consensus building for each block through PoW enables follow-up and verification of the data in the Bitccoin Blockchain.

Thanks to these functions, the Bitcoin blockchain can maintain the ecosystem stably against any attacks by malicious users even without a central authority, realizing the development and operation of a stable system. As a result, server costs (for the development and operation) are said to be reduced generally, although depending on the system. Furthermore, these functions have enabled transactions whose authenticity is guaranteed and highly transparent transactions that can be verified afterward.

In the Bitcoin blockchain, a dedicated script enables the execution of various processing procedures. Representative applications include Colored Coins.[21] Colored Coins is a technology to color bitcoins as asset information (such as computerized claims, digital contents, and information on rights on computerized real assets) and circulate them in the Bitcoin system. Open Assets Protocol, which originated from Colored Coins and has general versatility, enables users of the Bitcoin blockchain to distribute arbitrary assets on their own initiative. Open Assets Protocol and Colored Coins allocate IDs for distinguishing respective colors.

[21] http://coloredcoins.org/

Fig. 3-10 Outline of the Open Assets Protocol



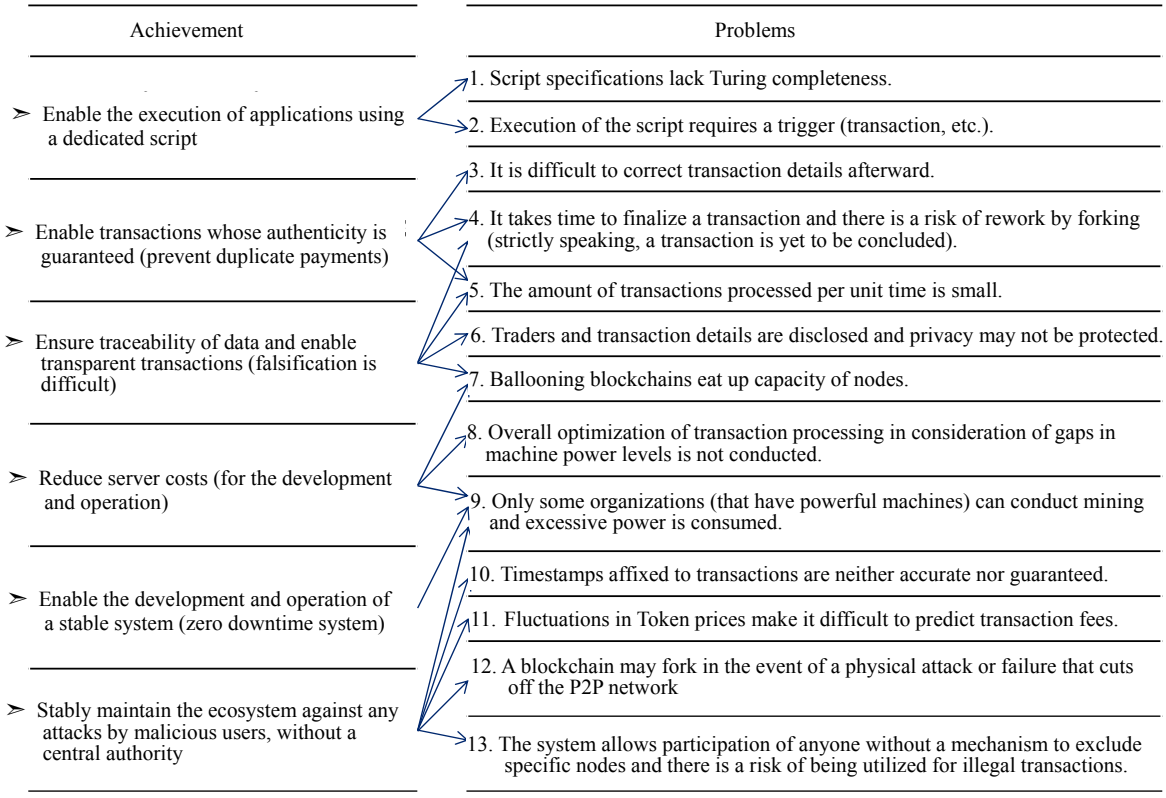
3.5 Problems of the Bitcoin Blockchain

The Bitcoin blockchain is an innovative idea that has achieved a mechanism functioning effectively without a central authority by combining existing technologies. However, increasing use of the system has revealed various problems. Those problems inherent to functions of the Bitcoin blockchain are compiled below.

The following 13 problems can be cited regarding the abovementioned achievement of the Bitcoin blockchain, each of which has been brought about by its four major functions.

Correlation between the achievement and problems revealed through widespread use is as shown in Fig. 3-11.

Fig. 3-11 Problems of the Bitcoin blockchain



The above 13 problems can be categorized into three; “problems arising from specifications and implementation of the system,” “problems arising from gaps with actual business practices,” and “mathematical and information science-related problems of the Bitcoin blockchain.” Problems arising from specifications and implementation of the system are wide-ranging and they are further divided into “problems arising from implementation of a script,” “problems arising from finality,”

and “problems arising from the P2P system.”

3.5.1 Problems arising from specifications and implementation of the system

i. Problems arising from implementation of a script

In the Bitcoin blockchain, a script (a string of letters ordering certain processing) to order automatic processing of part of a transaction can be entered, which enables an expanded use of the blockchain for the management of diverse assets, not limited to the delivery and receipt of virtual currency. However, while general computer languages need to satisfy the logical capacity called Turing completeness,[22] it is known that the Bitcoin blockchain cannot satisfy Turing completeness. Therefore, there are restrictions different from those for general scripts in such procedures as loop processing. Loop processing means to continue specific processing in succession until certain conditions are satisfied (the simplest example is to sequentially add up from 1 to 10), but this cannot be done within a single block in the Bitcoin blockchain. (Problem 1)

ii. Problems arising from finality

The Bitcoin blockchain requires 10 to 60 minutes until each block is approved by participants and a consensus as an authentic transaction record is built. Specific time required varies depending on the status of the mining in each block. In particular, when a block forks (multiple blockchains are created simultaneously), approximately 60 minutes are required for eliminating these forks. When a transaction was approved by participants as an authentic one, this is expressed as “a transaction was finalized” and this process as a whole is called “finality.”[23] The fact that a certain time is required for finality may restrict the application of Bitcoin to actual business. In actual transactions of bitcoins, the creation of following six blocks is deemed as finality of the relevant transaction, although it depends on the setting by wallet managers. This practice is adopted in consideration of a risk of rework due to blockchain fork. However, no matter how long a blockchain continues, a risk of fork cannot be eliminated strictly and therefore an extremely small risk of transaction cancellation remains.

As a thought experiment, application of the blockchain technology to vending machines can be considered. An existing vending machine promptly puts out a product when the amount of money inserted is equivalent to or higher than the product price. In the case of a vending machine controlled by a blockchain, the input of cash is first recorded in the blockchain and any following procedures

[22] When a machine can describe and calculate all problems that can be calculated with a Turing machine (a virtual abstract machine invented by Alan Turing; http://kitchom.ed.oita-u.ac.jp/jyo/proh09/mkiribu/kaisetu.html) if its memory is infinite and there is no limit for computation time, it is said that the machine satisfies Turing completeness (http://www-hiraki.is.s.u-tokyo.ac.jp/lectures/prog_giho/3.pdf).

[23] Meaning the completion of the settlement

need to wait until said block is approved. This consensus process requires at least 10 minutes in the Bitcoin blockchain. Then, a purchaser pushes a button after the amount of money thrown into is approved, and recording of this order in the blockchain also requires time in the same manner. If a consensus needs to be built for each of the procedures, regarding such matters as whether the order is correctly followed or how much the change is, requiring 10 minutes or longer each, such transaction would be impossible in actual business situations. The Bitcoin blockchain is thus not suited to transactions requiring promptness. (Problem 2 and Problem 4)

In actual business practices, it is often important to specify and record the date and time of transactions accurately. However, a timestamp affixed to a transaction recorded in the Bitcoin blockchain shows the time when a new block was created, not the time when the transaction was commenced. The time when a new block is created depends on timing of the creation of preceding blocks and responses from respective nodes and it is highly likely that a time different from the actual transaction time is recorded. Furthermore, respective nodes are not obliged to follow the Time-Stamping Authority (TSA)[24] or the Time Assessment Authority (TAA),[25] and timestamps do not always indicate accurate time. (Problem 10)

iii. Problems arising from the P2P system

As the Bitcoin blockchain stores information in a P2P distributed system, each node keeps blockchains that contain all past transaction data (as of the end of February 2016, each node had over 60GB of data in the Bitcoin blockchain[26]). Under a mechanism like the current Bitcoin blockchain, where all transaction data are to be stored, a considerable portion of each node's capacity is used up and this hinders the participation of mobile terminals and other nodes with smaller capacity. It is pointed out that the current Bitcoin blockchain may not be adaptable to a future network where nodes with smaller capacity and processing power, such as IoT, are supposed to be widely used. (Problem 7)

Furthermore, as there is an upper limit for the number of transactions each block of the Bitcoin blockchain can store (up to approximately 1,000 transactions)[27] and the interval of the creation of a new block is roughly set at around 10 minutes, only 5 to 7 transactions can be processed per second. Problems have yet to become obvious with the amount of bitcoins currently used, but when the use expands in the future, the possibility of delay in transaction processing due to insufficient capacity is pointed out.[28] For reference, the settlement system of VISA, one of the major credit-card networks,

[24] An authority that certifies time and issues a timestamp as a reliable third party
[25] An authority that delivers time; A timestamp server audits whether the relevant time synchronizes with the Coordinated Universal Time (UTC) within a prescribed accuracy.
[26] https://blockchain.info/ja/charts/blocks-size
[27] In reality, the capacity of each block is arranged to be approximately 1MB.
[28] Some say that the delay is already occurring.

processes 3,600 transactions per second on average[29] and has the peak capacity of processing 65,000 transactions or more per second.[30] (Problem 5)

The Bitcoin blockchain composing a P2P system always has a risk of attacks intending to cut off a network between respective nodes. When a network is cut off, synchronization of the blockchain data between nodes may be suspended or delayed. If new blocks are continuously created under such circumstances, there is a possibility that some blockchain data found authentic by one node may be found unauthentic by another. This is known as the problem with Eclipse Attack on a distributed system, and it is said that no solution has been made for the Bitcoin blockchain. (Problem 12)

Each node participating in Bitcoin has different machine power. A distributed system consisting of nodes with mostly the same machine power can introduce a mechanism to optimize the processing allocation depending on the status of each node, but it is difficult for the Bitcoin blockchain to optimize the entirety of the network consisting of nodes with different machine power. Therefore, there may be certain loss such as calculation duplication. (Problem 8)

The current Bitcoin blockchain adopts a mechanism that requires enormous machine power for building a consensus on transactions in each block. Nodes participating in PoW are called "miners," most of which are professional businesses that have computers dedicated for bitcoin mining. These professional businesses now almost exclusively conduct PoW of the Bitcoin blockchain.[31] Resources used for PoW are computers for calculation and electricity required for those computers, and power cost per day is estimated to be 0.15 million dollars as of 2013. Such a waste of resources is also a worry.[32] (Problem 9)

Additionally, any node can participate in the current Bitcoin blockchain, but conversely, the system has no mechanism to eliminate specific nodes. Therefore, the system cannot eliminate: ahead or afterwards, even a node intending to cut off the network as mentioned above. It is theoretically possible that a node with machine power exceeding a certain level (such as that exceeding 50% of the total power of all nodes participating in the network) chooses to illegally rewrite data in a block, but the system also cannot eliminate such node intending to conduct unlawful transactions. (Problem 13)

3.5.2 Problems arising from gaps with actual business practices

The Bitcoin blockchain is highly resistant to falsification, but it is extremely difficult to rewrite

[29] Average between October and December 2015
http://s1.q4cdn.com/050606653/files/doc_financials/2016/Q1/Visa-Inc.-Q1-2016-Financial-Results-Conference-Call-Presentation.pdf
[30] http://s1.q4cdn.com/050606653/files/doc_financials/2016/Q1/Visa-Inc.-Q1-2016-Financial-Results.pdf
[31] https://blockchain.info/ja/pools
[32]
http://www.bloomberg.com/news/articles/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster

any transaction data once stored in a block. When transaction details are recorded utilizing the Bitcoin blockchain and the relevant transaction is once finalized, it is difficult to correct the details retrospectively. Due to such characteristics, the Bitcoin blockchain is not suited to record transactions whose details may need to be corrected afterwards, and careful responses are required when handling any information such as personal data that should be kept confidential. (Problem 3)

In relation to this, it is another problem of the current Bitcoin blockchain that the details of transactions recorded in each block can all be checked by anyone. Although anonymous addresses are used for senders and recipients, transaction details are all disclosed (data such as the time and how much was sent from address A to address B are all disclosed). Disclosure of all transaction records may discourage the use of the system by those who want to conceal some transaction content for business purposes or to conduct privacy-related transactions. For example, even a transaction for which a company does not want to disclose the specific order amount to competitors may not be concealed in the Bitcoin blockchain.[33] Such data as payments of medical fees to hospitals are not kept confidential, and even if the use of anonymous addresses is the prerequisite, there remains a possibility that individuals can be specified through their long-term medical history, which also generates concerns from the viewpoint of privacy. (Problem 6)

In general transactions, accompanying fees, such as bank charges and exchange fees, are often required but these fees are mostly at fixed amounts or fixed rates and are predictable. However, in the case of a transaction using bitcoins, transaction fees are hard to predict due to fluctuations in the value of bitcoins (fluctuations in the value as a Token). Such fluctuations in transaction fees may have other adverse effects like making taxation procedures more complicated. (Problem 11)

3.5.3 Mathematical and information science-related problems of the Bitcoin blockchain

As a more fundamental problem, there is an information theory proof that "in a distributed system where time is not consistent among nodes, it is impossible to build a consensus to confirm the accuracy of certain information," and the Bitcoin blockchain is also subject to this proof. The current Bitcoin blockchain should be considered to achieve a consensus under an environment partially easing the conditions of this proof.[34]

Similarly, there is the CAP Theorem that the consistency, availability and partitioning tolerance cannot be simultaneously satisfied in a distributed system. According to this theorem, the Bitcoin

[33] There is a possibility that a user can be specified by following up a history of many transactions of a single bitcoin address (or multiple bitcoin addresses used by a single IP address) in chronological order.

[34] A consensus in a distributed system is premised on the FLP Impossibility Theorem (the theorem that no consensus algorithm that leads to 100% consensus exists in an asynchronous system as long as there is any possibility of suspension of any single node; Propounded by Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson in 1985). Therefore, it is considered that a consensus is built by specifying conditions.

blockchain is unable to satisfy the consistency.

CAP Theorem

The CAP Theorem was first propounded by Eric Brewer in 2000 at the Symposium on Principles of Distributed Computing and was proved by Seth Gilbert and Nancy Lynch in 2002. This is a theorem on distributed systems consisting of multiple nodes that handle common data and shows that distributed systems can completely satisfy only two properties out of the following three.

- C (Consistency: The status where all nodes have the latest data at the same time; Therefore, readout by each node is the returning of the data entered most recently)
- A (Availability: The status where any failure of a specific node does not affect other nodes; Therefore, each node is in a state of being able to surely respond within a time limit)
- P (Partition-tolerance: The status where nodes can continue operation even with a failure in the network; Therefore, each node is in a state of being operational even if the network is cut off)[35]

The Bitcoin blockchain, which is one of the distributed systems, can satisfy the availability and partition-tolerance, but cannot satisfy the consistency. Instead, as long as the partition of the network is eliminated within a time limit, the system is considered to maintain the eventual consistency.[36] Eventual consistency is the idea to find it acceptable if the consistency is maintained eventually even with some time lags.

[35] Cited from the reference materials for the members at the second review session

[36] As the Bitcoin Blockchain does not have a mechanism to verify network partition, preservation of the eventual consistency is not necessarily assured.

4 Application of Blockchain Technologies

As compiled in Chapter 3.5, the current Bitcoin blockchain has various problems. However, there are active attempts to adopt the system in diverse business fields, while solving or avoiding these problems. This chapter explains such moves from the viewpoint of the application of blockchain technologies.

With regard to problems arising from implementation of a script out of the problems arising from specifications and implementation of the system, a blockchain with a script ensuring the Turing completeness has been developed. For problems arising from finality, efforts have been made for increasing efficiency and speed of finality through devising algorithms related to consensus. Furthermore, for problems arising from the P2P system, solution of the abovementioned problems by selecting and limiting participants is now being discussed.

In the meantime, as gaps with actual business practices were recognized, the versatility of blockchain technologies has come to be reviewed more calmly. Active discussions now focus on how to bridge those gaps, while carefully ascertaining effects and limits of blockchain technologies.

There remain mathematical and information science-related problems of blockchains. The measures being taken and required for solving these problems will be briefly discussed below and mainly compiled in Chapter 6.

4.1 Application of Blockchain Technologies

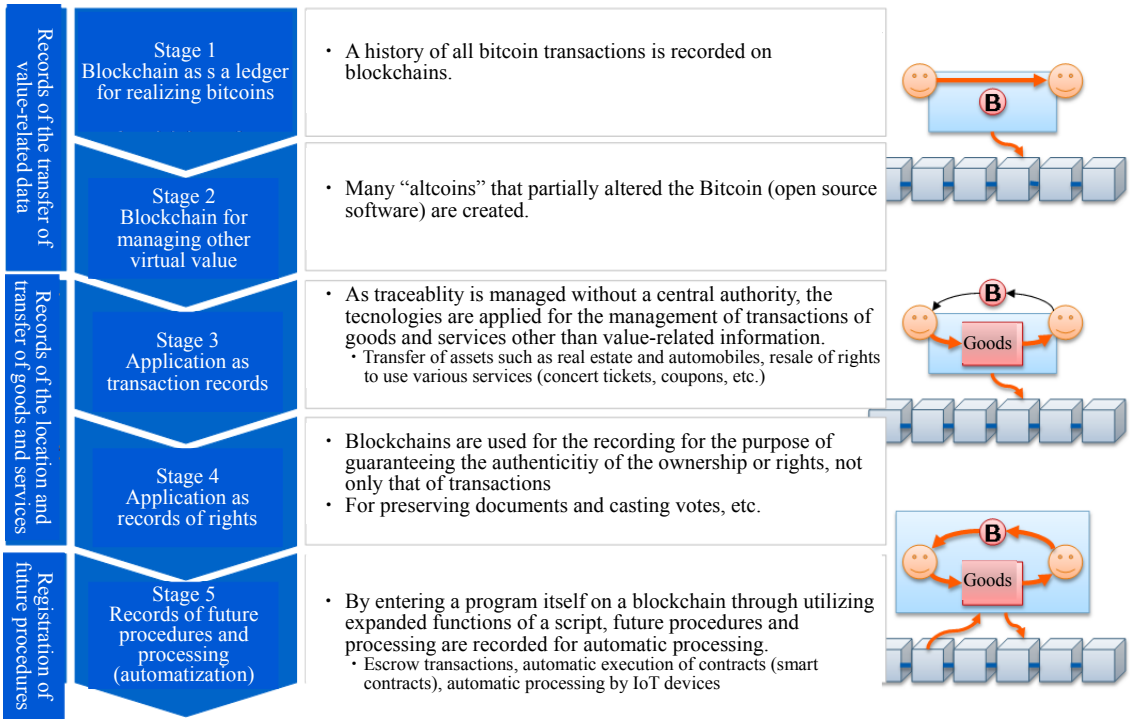
Starting from Bitcoin, diverse blockchains have been proposed. In the process of solving various problems as mentioned in Chapter 3.5, functions of blockchain technologies have been expanded and have come to be utilized for diverse usage.

Blockchain technologies have been expanded mainly centering on the three axes. First is the expansion of the scope of recording and exchange on blockchains and wider utilization of blockchain technologies, or a move to apply blockchain technologies more widely for the transfer and proof of ownership of various goods and rights to receive (provision of) services (ownership, right to use, etc.) not limited to those of value-related information. Second is the revision and improvement of performance of consensus algorithms, or a move to adopt new consensus algorithms in response to problems of PoW in Bitcoin. Third is the enhancement of the reliability of participants by limiting participation in the network, aiming to increase efficiency in building a consensus and speed up the processing of transactions by imposing certain limitations instead of allowing the participation of many and unspecified people.

4.1.1 Expansion of the scope of recording and exchange on blockchains and wider utilization of blockchain technologies

New ideas are being developed, such as managing various transaction records and diverse rights and claims, not limited to exchanges of virtual value, on blockchains by utilizing functions to ensure traceability or guarantee authenticity or functions of a script.

Fig. 4-1 Expansion of the scope of recording and exchange on blockchains and wider utilization of blockchain technologies



i. Stage 1: Blockchain as a ledger for realizing bitcoins

As seen in Chapter 3, the Bitcoin blockchain records a history of all bitcoin transactions. At this stage, the Bitcoin blockchain only functioned as a ledger for virtual currency, bitcoins.

ii. Stage 2: Blockchain for managing other virtual value

Bitcoin was developed as open source software. Therefore, once its effectiveness and potential were recognized, many “altcoins” were created by altering various parameters and encryption algorithms of Bitcoin. Such “altcoins” are more than 600 in number.[37]

[37] https://coinmarketcap.com/currencies/views/all/

iii. Stage 3: Application as transaction records

Once recognizing the fact that blockchains enable the management of transaction records without a central authority, people came to work on applying them for managing transactions of goods and services themselves and not only information on value such as that on virtual currency. They came up with ideas to apply blockchain technoloties to the transfer of assets such as real estate and automobiles, and the resale of rights to use various services (concert tickets, coupons, etc.).

iv. Stage 4: Application as records of rights

This is the stage where blockchains are used for the recording for the purpose of guaranteeing the authenticitiy of the ownership or rights, not only that of transactions. They are supposed to be utilized for preserving documents and casting votes, etc.

v. Stage 5: Records of future procedures and processing (automatization)

Moves are being actively conducted to seek means for achieving automatic processing by entering a program itself on a blockchain through utilizing expanded functions of a script and recording future procedures and processing.

The possibilities of escrow transactions, automatic execution of contracts (smart contracts), automatic processing by IoT devices, etc. are being considered.

4.1.2 Revision and performance improvement of consensus algorithms

Alternative algorithms have been proposed in response to the following out of various problems of the Bitcoin blockchain:

- PoW is conducted for every ten minutes in Bitcoin and the system is not suited to data processing that requires promptness;
- The capacity of each block is approximately 1MB, falling short of being able to process a large volume of transactions;
- The Bitcoin blockchain requires enormous machine power and its energy efficiency is low; and
- Exclusive use of machine power larger than 50% of the total of all network participants causes a risk of control (falsification, etc.) of the blockchain.

i. Proof of Stake (PoS)

PoS refers to a method to assign priority in hash calculations, in accordance with the holding ratio of virtual currency, etc.

This is based on the idea that a dishonest act committed by a node holding a large amount of virtual currency results in reducing the reliability and value of the currency and this fact works as an incentive for any participant to avoid dishonest acts. However, several means to illegally control blockchains are pointed out and countermeasures are necessary.[38] PoS is adopted in Ethereum, Bitshares, and NXT, etc.

ii. Proof of Importance (PoI)

PoI refers to a method to cluster[39] nodes through transaction graph analysis[40] using transaction amounts and balances of individual nodes as indicators, calculate the significance of each node, and assign priority in hash calculations (assign easier hash calculations) to more significant nodes. Clustering is supposed to make it possible to detect nodes that are likely to commit unlawful transactions. PoI is adopted in NEM.

iii. Practical Byzantine Fault Tolerance (PBFT)

PBFT is an algorithm for solving a Byzantine Fault resulting from a failure in building a consensus caused by the Byzantine Generals Problem. It was considered to be difficult to put a theoretical algorithm to practical use due to the enormous calculation amount being required. In 1999, a practical algorithm that can avoid a Byzantine Fault by adding a minor lag at the time of judging consensus formation was propounded,[41] and efforts to apply this algorithm to blockchains are now being made.

However, the total number of nodes must be known and the maximum number of illegal nodes should be set, and such requirements make it difficult to apply this alborithm to public systems. PBFT is now adopted in Ripple and Stellar and is also scheduled to be adopted in Orb.

4.1.3 Enhancement of the reliability of participants by limiting participation in the

[38] https://blog.ethereum.org/2014/07/05/stake/
[39] Clustering refers to an analysis method to classify analysis targets into groups (clusters) according to their characteristics through analyzing diverse data.
[40] Transaction graph analysis refers to an analysis method to clarify the influence of analysis targets and the strength of collaboration among them through analyzing the strength and frequencies, etc. of the relationships among them. Here, the influence and closeness, etc. among nodes are analyzed.
[41] http://pmg.csail.mit.edu/papers/osdi99.pdf

network

A consortium-type or private-type mechanism is proposed, which enables enhanced transaction processing through reducing PoW load by limiting participation in the network to enhance reliability of participants and adopting a simplified consensus algorithm that does not require a reward for building a consensus. However, some point out that the very significance of blockchain technologies (use without any central authority) cannot be fully realized under either a consortium-type mechanism or a private-type mechanism.

Fig. 4-2 Comparison among public-type, consortium-type, and private-type mechanisms[42]

Public	Consortium	Private
■ Participation in a network (building a consensus and conducting mining) is open to anyone. ■ Methods of building a consensus are important in order to eliminate malicious participants.	■ A blockchain is used while building a consensus only among members who can be trusted with each other to some extent, such as members of a specific company group. ■ Building a consensus is easier as participants are all identified.	■ A blockchain is used only within a specific organization. ■ Building a consensus is quite easy as the mechanism is open only to the relevant organization.

[42] This table shows one example, as there are no established definitions of public-type, consortium-type, and private-type mechanisms.

4.2 Responses to Problems of the Bitcoin Blockchain

Some of the problems of the Bitcoin blockchain compiled in Chapter 3.5 have been solved by other blockchain infrastructure providers. Proposed solutions are indicated below for each of the three types of problems arising from specifications and implementation of the system. Fig. 4-3 compiles responses to each problem taken by various other blockchains.

4.2.1 Responses to problems arising from specifications and implementation of the system

i. Responses to problems arising from implementation of a script

These problems are addressed mainly in the aspect of the expansion of the scope of recording and exchange on blockchains and wider utilization of blockchain technologies, out of the three core directions for the application and expansion of blockchains.

The Bitcoin blockchain fails to satisfy the Turing completeness as mentioned above, but Ethereum, another blockchain system, satisfies it. Ethereum enables the implementation of a script that is impossible on the Bitcoin blockchain and is expected to be applicable to a wider range of use cases. (Problem 1)

Sidechain and Counterparty also implement Turing-complete scripts, and the Bitcoin blockchain is considered to be able to conduct diverse processing by expanding its functions with them.

ii. Responses to problems arising from finality

These problems are addressed mainly in the aspect of the revision and performance improvement of consensus algorithms, out of the three core directions for the application and expansion of blockchains.

Blockchains other than the Bitcoin blockchain are said to be able to avoid excessive power use by reducing mining costs through the adoption of consensus algorithms, such as PoS and PoI. Nevertheless, there remains the problem that PoS enables only certain organizations with high balances to conduct mining. (Problem 9)

Some consortium-type or private-type blockchains determine conditions for finality on the side of the blockchain developer or adopt PBFT or other consensus algorithms, thereby enabling the reduction of time required for using the Bitcoin blockchain (approximately 10 to 60 minutes). On the other hand, although the time required for finality can be shortened, it is difficult to reduce the time by milliseconds. Therefore, such blockchains are not suited to transactions requiring promptness and are particularly unsuitable for transactions with severe time constraints. (Problem 4)

As a means to ensure the accuracy of the time of a timestamp, one option is to collect and statistically analyze time records recognized by each node connecting to the P2P network of the

relevant blockchain and use the accurate time derived through the analysis as time for a timestamp. It is also possible to obtain accurate time information through the collaboration with the TSA or the TAA. (Problem 10)

iii. Responses to problems arising from the P2P system

These problems are addressed mainly in the aspect of the enhancement of the reliability of participants by limiting participation in the network, out of the three core directions for the application and expansion of blockchains.

As mentioned above, gaps in machine power of nodes participating in the Bitcoin system make it difficult to optimize the network as a whole, and the possibility of duplication of calculations or other types of loss is pointed out. Participation in consortium-type or private-type blockchains is on a permission basis, and such blockchains are considered to be able to align machine power levels and speed up transaction processing by introducing multicore CPUs and GPU computing. (Problem 8)

Some consortium-type or private-type blockchains can create an environment that enables reduction of data sizes by such means as compressing data stored in blocks in each node or uploading such data to another server. Furthermore, they can increase the amount of transactions processed per unit time by using an original data management format that can reduce transmission load. (Problem 5)

Public-type blockchains that allow free participation of nodes have high risks of receiving a 51% attack especially at the time of establishing a system, as the overall machine power is not large. Therefore, it can be possible to limit participation of nodes only at the initial stage and build a system only with reliable participants to reduce such risks. Consortium-type or private-type blockchains have smaller risks of being attacked as they limit participants from the beginning and malicious nodes cannot participate easily. In order to prevent illegal transactions by malicious participants, it is technically possible for public-type blockchains to conduct a cluster analysis of transaction volume and balances of respective nodes and detect suspicious nodes that may make unlawful transactions in advance. Consortium-type or private-type blockchains have managers and such managers can eliminate suspicious nodes that may make unlawful transactions. (Problem 13)

It is pointed out that the block size of Bitcoin is becoming insufficient as the transaction volume increases, and means to solve the problem of capacity shortage of the blockchain has been discussed mainly among core developers. At present, this problem is planned to be solved by first implementing Segwit (Segregated Witness) and then releasing the capacity to officially incorporate the input data into the system. Segwit is an idea to compress the current data capacity by 25% at the maximum by removing signature-related data from transaction information to be stored in a block. In addition to Segwit, the implementation of an idea called Bitcoin Classic is also discussed. Bitcoin Classic is an idea to increase block size from the current 1MB to 2MB, aiming to solve the problem

of capacity shortage in a method different from that of Segwit.[43] If both ideas are put into practice, the volume of transaction data that can be stored in one block will increase by eight times, and the problem relating to block size may be solved for the time being. (Problem 7)

4.2.2 Responses to problems arising from gaps with actual business practices

As mentioned above, it is difficult to correct the details entered in a block of the Bitcoin blockchain retrospectively. On the other hand, some other blockchain systems like Ethereum have publicized the possibility of retrospective correction of a preceding block in the event of a failure in building a consensus due to the entry of a program by a specific script, at such timing as the creation of a new block. Consortium-type or private-type blockchains can incorporate a mechanism under which the manager side arbitrarily takes procedures to correct erroneous transactions.

In order to protect privacy in transactions, some public-type blockchain offers services to conceal transaction data by adding an untraceable property to the system.[44] Consortium-type or private-type blockchains are available only among limited participants in the first place, and there is no need to worry about the infringement of privacy.

Fluctuations in the value of bitcoins make it difficult to predict transaction fees, but it is possible that a company prepares and issues tokens free from price fluctuations that are not linked to legal currency and are not associated with the market price.

4.2.3 Responses to mathematical and information science-related problems of the Bitcoin blockchain

There are no complete solutions for the FLP Impossibility Theorem and the CAP Theorem, but it is said to be possible to take measures by setting some conditions. However, in-depth theoretical discussions have yet to be carried out.

[43] The method of Bitcoin Core is to transfer data to a new blockchain incompatible with the current blockchain (called hard forking), but many express concern over the possibility of failure in smooth transfer.

[44] For example, Zcash adopts a zero knowledge interactive proof protocol. This is one of the methods of proof, which was proposed in 1985, or a protocol by which a person proves that his/her proposition is true to another person by transmitting no other knowledge than the fact that the proposition is true.; http://pdf.landfaller.net/80/80-4.pdf

Fig. 4-3 Responses to problems of the Bitcoin blockchain

Problems	Solutions by other BCs		Remaining problems
1. Script specifications lack Turing completeness.	Pub	Arbitral processing may be entered on a script as the Turning completeness is satisfied. (Ethereum)	-
	C/Pri	-	There are services that are building an environment enabling automatic execution of a script (it is necessary to check whether they satisfy Turing completeness). (mijin, etc.)
2. Execution of the script requires a trigger (transaction, etc.).	Pub	-	Execution of the script requires a trigger (transaction, etc.).
	C/Pri	-	Execution of the script requires a trigger (transaction, etc.).
3. It is difficult to correct transaction details afterward.	Pub	Retrospective correction is made at such timing as the creation of a new block in the event of a failure in building a consensus due to the entry of a program by a specific script. (Ethereum)	-
	C/Pri	C/Pri blockchains can decide procedures to correct erroneous transactions.	-
4. It takes time to finalize a transaction and there is a risk of rework by forking (strictly speaking, a transaction is yet to be concluded).	Pub	-	It takes time to finalize a transaction.
	C/Pri	Introduction of super nodes may shorten time for finality and a risk of rework by forking. (Orb) C/Pri blockchains can solve the problem by setting conditions for finality.	Time required for finality can be shortened, but it is difficult to reduce the time by milliseconds, and such blockchains are not suited to transactions requiring promptness.
5. The amount of transactions processed per unit time is small.	Pub	-	An idea to increase block sizes to increase the processible transaction amount is proposed but there are mixed reactions.
	C/Pri	Through the adoption of an original data management format that can reduce transmission load, the amount of transactions processed per unit time has been increased. (mijin, etc.)	-
6. Traders and transaction details are disclosed and privacy may not be protected.	Pub	Services adding untraceable property have been developed by adopting a zero knowledge interactive proof protocol. (Zcash, etc.)	-
	C/Pri	Blockchains are available only among limited participants in the first place, and there is no need to worry about the infringement of privacy	-
7. Ballooning blockchains eat up capacity of nodes.	Pub	-	Segwit realizes a method to reduce the use of the capacity of a block by separating the signature from the transaction structure.
	C/Pri	It is possible to create an environment that enables reduction of data sizes by such means as compressing data stored in blocks in each node or uploading such data to another server. (mijin)	-
8. Overall optimization of transaction processing in consideration of gaps in machine power levels is not conducted.	Pub	-	Overall optimization of transaction processing in consideration of gaps in machine power levels is not conducted.
	C/Pri	Participation is on a permission basis, and it is possible to align specifications of hardware and speed up transaction processing by introducing multicore CPUs and GPU computing. (mijin, etc.)	-
9. Only some organizations (that have powerful machines) can conduct mining and that excessive power is consumed.	Pub	Adoption of PoS/PoI reduces mining costs and prevent excessive power use. (Ethereum, NEM, etc.)	In PoS, only some organizations with high balances can conduct mining.
	C/Pri	Adoption of PoS/PoI reduces mining costs and prevent excessive power use. (Orb, mijin, etc.)	In PoS, only some organizations with high balances can conduct mining.
10. Timestamps affixed to transactions are neither accurate nor guaranteed.	Pub	It may be possible to complement the timestamp function by collecting and statistically analyzing time records recognized by each node via the P2P network. (NEM)	-
	C/Pri	The accuracy of the time is to be ensured by affixing a timestamp, while linking to a time server.	-
11. Fluctuations in Token prices make it difficult to predict transaction fees.	Pub	It is possible to independently prepare tokens free from price fluctuations caused by changes in the market price. (Colored Coins, etc.)	-
	C/Pri	It is possible to independently prepare tokens free from price fluctuations caused by changes in the market price. (Orb, mijin, etc.)	-
12. A blockchain may fork in the event of a physical attack or failure that cuts off the P2P network.	Pub	As a risk of receiving a 51% attack is high especially at the time of establishing a system, a trusted environment is sometimes ensured at the initial stage.	A risk of receiving a 51% attack is high especially at the time of establishing a system.
	C/Pri	There is little risk of being attacked as the environment does not allow participation of malicious nodes. (mijin, etc.)	-
13. The system allows participation of anyone without a mechanism to exclude specific nodes and there is a risk of being utilized for illegal transactions.	Pub	It is possible to detect suspicious nodes that may make unlawful transactions by conducting a cluster analysis of transaction volume and balances of respective nodes. (NEM, etc.)	-
	C/Pri	As the environment is centralized, it is possible to eliminate suspicious nodes that may make unlawful transactions. (Orb, mijin, etc.)	-

4.3 Classification of Blockchains and Use Cases

As seen in Chapter 4.2, various blockchains have been developed for solving challenges of the Bitcoin blockchain, and diverse services are provided on respective blockchains. Fig. 4-4 compiles such services based on the three axes explained in Chapter 4.1.

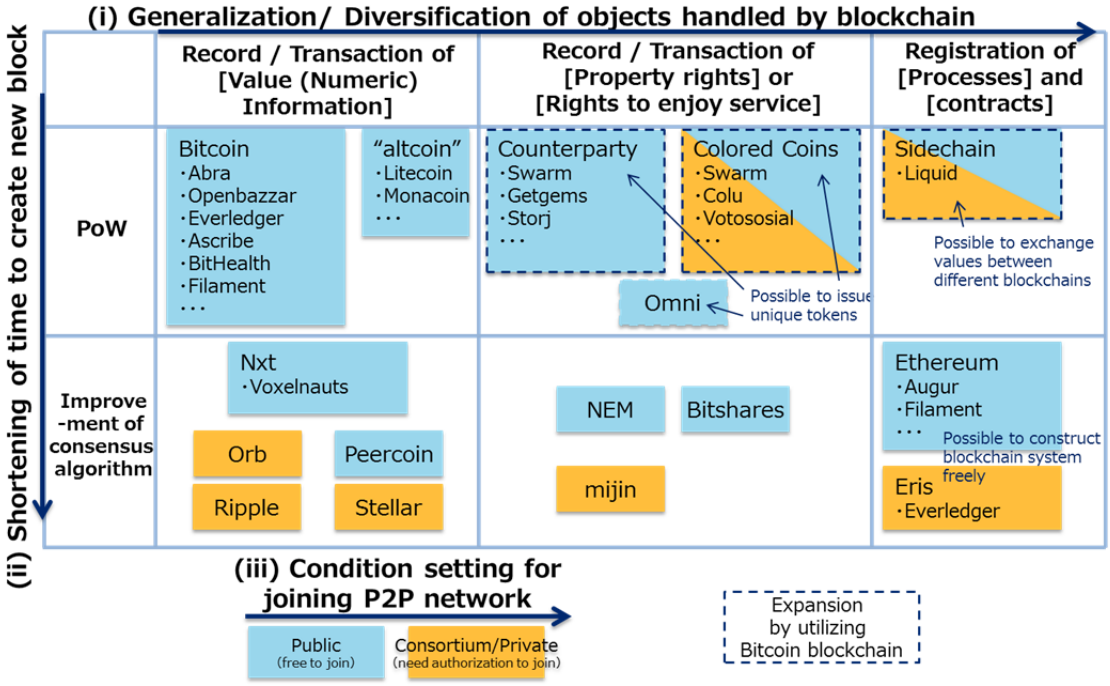
The major function of Bitcoin and the “altcoins” which were derived from the former is to record transfers of value information and they use PoW. There are already various services using the Bitcoin blockchain, such as Abra (remittance to Islamic countries), Openbazzar (marketplace), and Everledger (proof of ownership).

One example of blockchains developed from the Bitcoin blockchain by expanding its range of use is Omni. Furthermore, Counterparty, Colored Coins, Sidechain, etc. are now being used as methods to expand the functions of the Bitcoin blockchain, although they are dependent on Bitcoin blockchain. Counterparty provides such services as Swarm (cloud funding), Getgems (SNS), and Storj (storage), Colored Coins provides such services as Swarm, Colu (proof of ownership), and Votososial (electronic voting), and Sidechain provides Liquid (settlement between exchanges).

As blockchains that have been developed from the Bitcoin blockchain by altering consensus algorithms, there are Nxt, Peercoin, and Orb, etc., which adopt Proof of Stake, and Ripple and Stellar, etc., which adopt original algorithms. Among these, Orb, Ripple, and Stellar were developed as consortium-type or private-type blockchains with limited participants and can conduct faster processing.

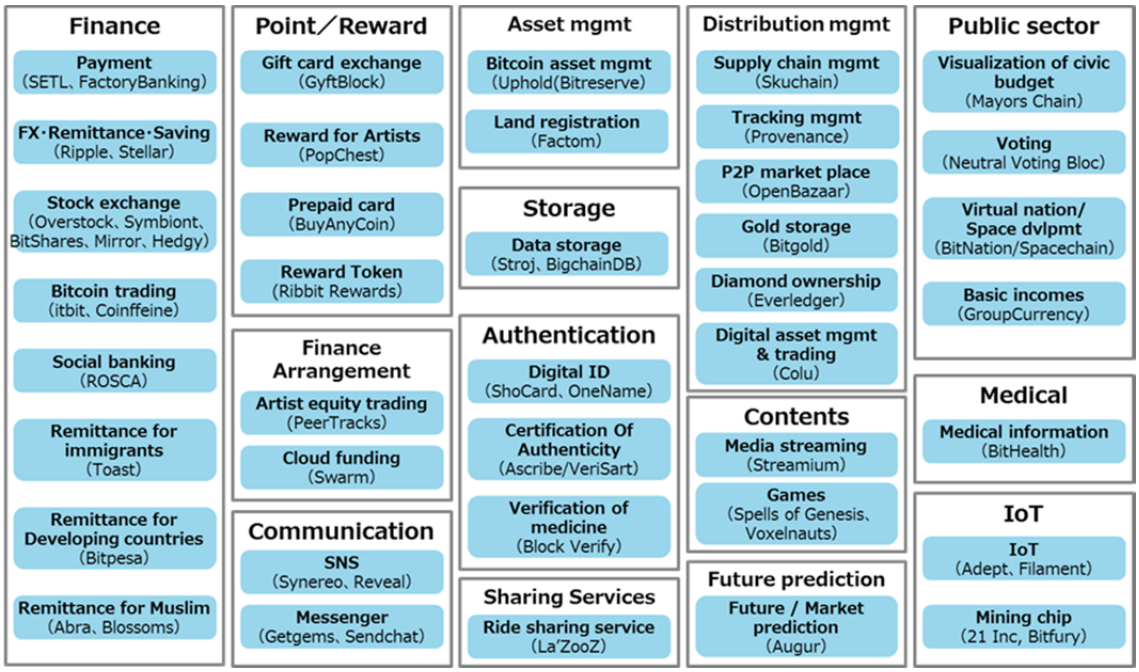
As examples of blockchains seeking to further expand the range of use to cover rights on goods or services, there are NEM and Bitshares, as well as mijin, which is a consortium-type or private-type version of NEM. Additionally, Ethereum and Eris, etc. were developed on the premise of incorporating future procedures through the smart contract mechanism in a blockchain and automating processing. Ethereum provides such services as Augur (prediction market) and Filament (sensor network), and Eris provides Everledger, etc.

Fig. 4-4 Classification of blockchains



Not limited to the above, many other services are provided using blockchains in diverse fields (Fig. 4-5).

Fig. 4-5 Use cases and exmaples of services using blockchains



i. Finance

There are many use cases in the financial field, such as using a blockchain for settlement. Bitcoins as virtual currency can be considered as one of the use cases of blockchains. Various methods of use are proposed, which include remittance, settlement, transactions of securities, claims, and other various derivatives, and Islamic finance, etc. Ripple is one of the representative blockchains in this field.

ii. Loyalty points and reward

Loyalty point services and reward are provided on blockchains. This service is close to a settlement service, but is premised on being used within a specific area by limiting usage and users.

GyftBlock, which provides an exchange service of gift cards using a blockchain, enables issuance, sending and exchange of gift cards on a blockchain, and can also control users and monitor how the service is used.

iii. Funding

This service aims to use blockchains for cloud funding and investments to artists. As managers are not necessary or only a simple management system suffices, it is expected that artists and business entities can obtain larger shares from collected funds.

Swarm provides a service to procure funds through cloud funding on a blockchain. Contributors can receive dividends under a smart contract.

iv. Communication

Messaging services and social networking services (SNS) have been made available using blockchains. These services are sometimes used in combination with a remittance service mentioned in i or a reward service mentioned in ii.

Getgems provides SNS (SNS itself is provided separately from a blockchain). It grants original virtual currency, GEMZ tokens, to its users when they browse advertisements, etc. and users can exchange tokens while communicating with each other on SNS.

v. Asset management

Ownership and transfer of assets, including land registration, can be managed on blockchains.

Factom, etc. commenced the provision of a service.

vi. Storage

This is a service to manage data on the Internet using blockchains. As storing data themselves on a blockchain significantly increases the volume of a blockchain, some blockchains adopt another means for the management of data.

Storj provides a service to manage various electronic files using a blockchain. Data themselves are encrypted and stored in a dispersed manner on a P2P network, and therefore cannot be accessed by third parties, achieving a storage service with high fault resistance.

vii. Authentication

Mechanisms to manage the authentication of validity of goods, etc. using blockchains are put in place. The applicable scope is wide, including works of art, drugs, digital contents, etc.

Ascribe provides a service to manage copyright of works of art on a blockchain. Artists who have registered their own works can manage and transfer ownership and can manage records of use of the service.

viii. Sharing

Rights to use shared cars or other goods shared in the sharing economy can be managed using blockchains.

La'ZooZ aims to provide a sharing service using a blockchain. At present, it provides a ride sharing application like Uber.

ix. Commercial distribution management

Traceability can be realized by registering all histories of processing from raw materials to final products, not only by replacing so-called EDI with blockchains. This is also applied to digital contents in the same manner as a mechanism mentioned in vii.

Everledger provides a system to manage diamonds. The serial number and carat, various commodity information, ownership and distribution record of each diamond are managed.

x. Content

Blockchains can be used for delivering contents on the Internet. Such services charging streaming broadcasting by time unit or managing items of online games are provided.

Streamium provides a service to support content delivery, having established a system to charge by the second (paid with bitcoins) for video delivery, etc.

xi. Prediction

A new service has emerged to have participants vote on predictions on various matters in the world and share rewards depending on voting results. This is sometimes called the prediction market and is what has replaced a bookmaker in the United Kingdom on a blockchain.

Augur provides a decentralized prediction market platform where participants cast votes on various events to predict the future through the wisdom of the crowd.

xii. Public

There are many trials to realize public services on blockchains, such as budget management, voting, notification management, provision of social security, etc. of local governments. In the city mayoral election in London, one candidate ran a race with a campaign pledge to introduce the use of a blockchain for budget management. Estonia, Honduras and others show interest in adopting blockchains in their public systems.

Neutral Voting Bloc (NVB) is a service provided in Australia, advocating itself as a new political party. It announces that members of the NVB will carry out actual congressional activities in accordance with the voting results on the blockchain.

xiii. Medical services

This is an idea to manage medical data, such as electronic health records and medication records, by using blockchains. Proposed methods for protecting privacy include not recording medical data themselves on a blockchain but managing only passes to medical institutions, etc. where health records are managed.

BitHealth aims to achieve its goal to enable users to safely check their own health records from anywhere in the world using a blockchain.

xiv. IoT

Blockchains can also be used in the IoT field. The expected utilization method is one where

sensors, etc. conduct predetermined processing tasks independently without involving a central server.

Such services as ADEPT by IBM and Samsung are attracting attention.

4.4 Demontration Experiments Using Blockchains

As mentioned in Chapter 4.3, various trials utilizing blockchain technologies have been made and some of them have already been launched as services. Under such circumstances, some domestic and overseas companies and organizations started to make efforts to utilize blockchain technologies. Many of such efforts are still at the demonstration or experimental stage but aim to utilize blockchain technologies to achieve the goal of creating new added value in their existing business and reduce costs, etc. In Japan, efforts are mostly made independently by each company, while cross-industry initiatives by company groups, etc. are characteristically increasing overseas. Major examples are shown in 4.4.1 and 4.4.2 below.

4.4.1 Major examples of domestic companies considering utilization of blockchain technologies

In May 2015, NTT Service Evolution Laboratories publicized the results of their study on content licensing management utilizing a blockchain. This technology has been developed as part of NTT's project to develop immersive telepresence technology "Kirari!," and is positioned as one of the solutions ensuring simple and convenient video licensing management to enable worry-free use of various video works. The company considers that community activities for dissemination, not only the high level of technology, are important to have such content management mechanism accepted in society, and plans to advance efforts in collaboration with diverse stakeholders including content producers and manufacturers.[45]

Nomura Research Institute started demonstration experiment in October 2015, aiming to utilize blockchain technologies in the securities business. Furthermore, in December 2015, it started the preparation of a work scenario utilizing blockchain technologies and sorting out of matters to be verified jointly with the SBI Sumishin Net Bank, and it plans to create a prototype for verification in line with the work scenario, verify outcomes and problems, and promote efforts to specify how to apply blockchain technologies in banking business. The company outsources the implementation of blockchain technologies to Dragonfly FinTech, etc.[46,47]

In December 2015, Sakura Internet and Tech Bureau announced their plan of free provision from January 2016 of mijin CloudChain β, a demonstration environment of mijin CloudChain by Tech Bureau, on Sakura Cloud operated by Sakura Internet. They say that it is the first trial in the world to provide a private-type blockchain environment to the general public free of charge as a practical cloud service. Through the provision of this demonstration environment, they intend to have users

[45] http://www.ntt.co.jp/journal/1505/files/jn201505010.pdf
[46] http://www.nri.com/jp/news/2015/151005_1.aspx
[47] http://www.nri.com/jp/news/2015/151216_1.aspx

recognize the potential of a private-type blockchain and thereby contribute to promoting utilization of private-type blockchains in a wide range of areas.[48]

In January 2016, Softbank announced that it will conduct R&D on a platform that enables high-reliability transactions on the Internet through the use of blockchain technologies. In this R&D, the company as a carrier aims to understand new value to be created by blockchain technologies and develop and provide concrete services utilizing such value as early as possible. As the first project, it will develop a prototype of an international fund-raising platform utilizing blockchain technologies with cooperation from Consensus Base and Appirio.[49]

In February 2016, GMO Internet and Tech Bureau announced a business alliance to jointly develop back-end engines for games. Application of blockchain technologies to backend game engines is expected to reduce the operation cost by 50% or more and realize a zero downtime environment to minimize downtime. They plan to start selling PaaS backend engines at GMO app cloud, a dedicated cloud service for game applications, around the autumn of 2016.[50]

In February 2016, it was reported that the Bank of Tokyo-Mitsubishi UFJ had been developing original virtual currency. For the time being, the bank positions such currency as in-house currency, but also has a scheme to make the currency exchangeable with the yen and issue it to customers sometime in the future. This virtual currency is named MUFG coin and the bank is said to have almost completed a trial application to incorporate MUFG coins into customers' smartphones.[51]

In February 2016, Mizuho Financial Group announced its plan to start demonstration experiments of blockchain technologies in collaboration with Information Services International-Dentsu, CurrencyPort, and Microsoft Japan. Taking advantage of characteristics of blockchain technologies and smart contracts, these demonstration experiments focus on better understanding of technologies and application in financial business: targeting syndicated loan business which involves various parties, and is considered to have much room to improve efficiency in clerical work. The bank aims to verify applicability and create a new model that may bring about innovation in the financial industry.[52]

4.4.2 Major examples of overseas companies considering utilization of blockchain technologies

R3 CEV, a US FinTech company which leads a consortium wherein 42 companies worldwide participate (as of March 2016, Nomura Holdings, Sumitomo Mitsui Banking Corporation,

[48] http://www.sakura.ad.jp/press/2015/1216_mijin_cloud_chain/
[49] http://www.softbank.jp/corp/group/sbm/news/press/2016/20160106_01/
[50] https://www.gmo.jp/news/article/?id=5146
[51] http://www.asahi.com/articles/ASJ1W4RWKJ1WULFA012.html
[52] http://www.mizuho-fg.co.jp/release/20160216release_jp.html

Mitsubishi UFJ Financial Group, Mizuho Financial Group, etc. participate from Japan), has created the Private Distributed Ledger among participating company groups, and has been conducting multiple demonstration experiments. The R3-managed Private Distributed Ledger was developed by Chain, Eris Industries, Ethereum, IBM, and Intel, and cloud computing resources to be used in the experiment are provided by Microsoft Azure, IBM Cloud, and Amazon AWS. Mr. David Rutter, CEO of R3 CEV, says that the adoption of the Private Distributed Ledger by financial institutions and companies providing technologies across their boundaries on a worldwide scale will create a significant momentum and will bring about effects, transparency, scalability, and security of the same level as merits brought about by electronic transactions in the financial industry.[53]

In April 2015, the MIT Media Lab announced its plan to start an initiative to deal with bitcoins and other cryptocurrency in general. In this initiative, with the support and participation of member companies of Media Lab, teachers and students of MIT conduct research. The company has set the following three goals:[54]

(i) Conduct research and engage more students on digital currency topics that address challenges about security, stability, scalability, privacy, and economics.

(ii) Convene governments, nonprofits, and the private sector to research and test concepts that have high social impact.

(iii) Provide evidence-based research to support existing and future policy and standards.

In October 2015, Nasdaq, together with Chain, publicized Nasdaq Linq, a trading system for unlisted shares utilizing blockchain technologies (it had already announced the development of the system as of May 2015). This is a system to be used by unlisted companies participating in the Nasdaq Private Market, the unlisted shares market operated by Nasdaq, and supplements Exact Equity, which Nasdaq had provided as a cloud-based system for enabling those unlisted companies to participate in said market. For the time being, this system is utilized by six companies, namely, Chain, ChangeTip (company relating to electronic money startup), PeerNova (company relating to encrypted ledger technology), Synack (company relating to cyber security), TangoMe (company relating to messaging applications), and Vera (company relating to messaging applications for business use).[55]

Linux Foundation is a non-profitable consortium for facilitating the growth of Linux and was established in 2000. Openledger project, a joint development project utilizing blockchain technologies, which was announced in December 2015, aims to create an industry-specific robust system for application, platform, and hardware that supports commercial transactions, build a

[53] http://r3cev.com/

[54] https://medium.com/mit-media-lab-digital-currency-initiative/launching-a-digital-currency-initiative-238fc678aba2

[55] http://ir.nasdaq.com/releasedetail.cfm?releaseid=938667

framework for an open source distributed ledger to be utilized across industry participants, and foster personnel to develop such system and framework. More than 20 companies participate in this project, including Fujitsu, Hitachi, NEC, and NTT Data from Japan.[5657]

The World Wide Web Consortium (W3C) established the Blockchain Community Group and is preparing guidelines for standardizing message formats on blockchains based on ISO20022. The group also conducts studies and evaluation of new technologies relating to blockchains.[58]

Australian Securities Exchange (ASX), which had discussed the adoption of blockchain technologies upon renewal of the existing system, announced capital contribution to and a business alliance with Digital Asset Holdings in January 2016, declaring the decision to utilize technologies of said company. ASX plans to replace its Clearing House Electronic Subregister System (CHESS) with a new system to enable near real-time settlement of equities trades and reduce system management costs.[59]

---

[56] http://www.linuxfoundation.jp/news-media/announcements/2015/12/jp_linux-foundation-unites-industry-leaders-advance-blockchain

[57] https://www.hyperledger.org/

[58] https://www.w3.org/community/blockchain/

[59] http://www.smh.com.au/business/banking-and-finance/asx-builds-blockchain-for-australian-equities-20160121-gmbic0.html

4.5 Direction of Development of Blockchains

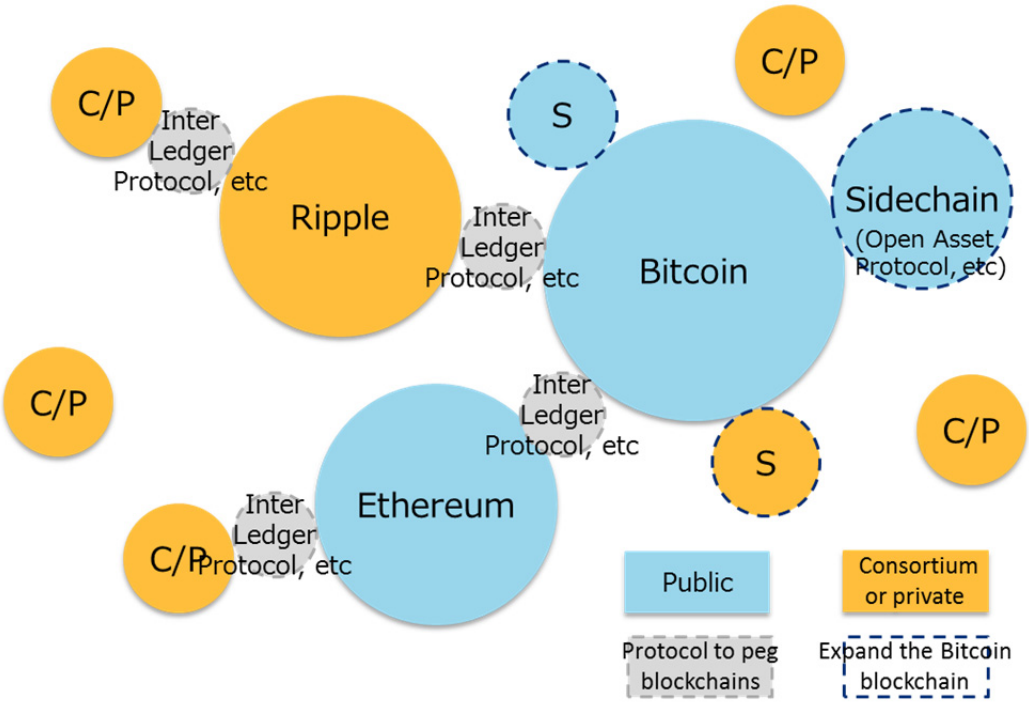
Several scenarios can be considered for future courses of the development of blockchains depending on which blockchain is mainly used. However, these scenarios are only created at the level of infrastructure, and individual services may be provided in any of these scenarios.

At present, only the Bitcoin blockchain is said to be operating stably. It is expected as one option that the Sidechain and Open Assets Protocol that record various types of value will be utilized and their scripts will be input in the Bitcoin blockchain itself. In this case, various services will be mainly provided on the Sidechain system or the Open Assets Protocol system. The Bitcoin blockchain is an open system, but the use of Sidechain and Open Assets Protocol will enable the operation of a mechanism where the openness is well-controlled in a manner similar to the relationship between the Internet and an in-house LAN.

In the meantime, there is a possibility of collaboration with Ethereum, Ripple, or other individual blockchains via Sidechain and Inter Ledger Protocol,[60] etc. As it has been explained so far, the Bitcoin blockchain has various challenges. Many new blockchains aiming to solve such challenges have been proposed, and some of those new blockchains may be evaluated as being usable and be actually used. When a closed consortium-type or private-type mechanism is mainly used, one option is to partially customize various consortium-type or private-type blockchains provided by various companies to develop an in-house system. If such option is adopted, common specifications are rarely necessary and it is highly likely that each company will build a blockchain independently and provide services utilizing such original blockchain. Furthermore, there is also a possibility that new public-type blockchains may be developed and disseminated widely.

[60] A protocol propounded by Ripple for exchanging information between blockchains

Fig. 4-6 The world where various blockchains including the Bitcoin blockchain are utilized



Note) C/P: Consortium-type or private-type blockchains

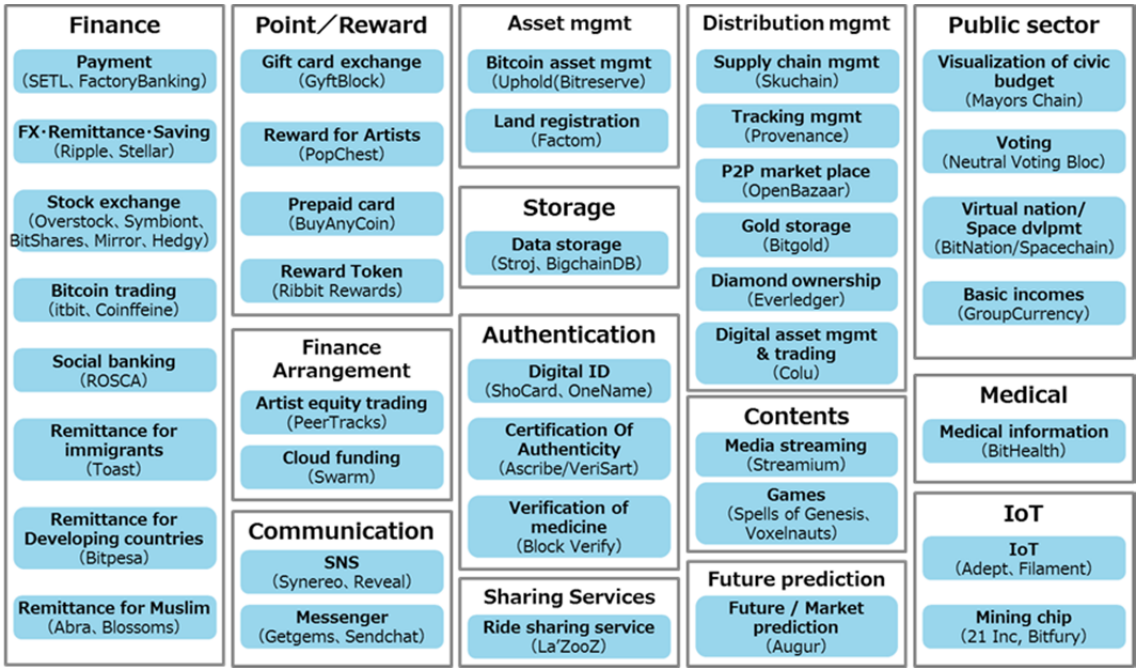
S: Blockchains based on Sidechain or Open Assets Protocol

5 Utilization of Blockchains

5.1 Functions of Blockchains and Use Cases

As seen in Chapter 4, various use cases of blockchains have already been proposed.

Fig. 5-1 Use cases and examples of services using blockchains (mentioned above)



On the other hand, as a result of interviews with domestic and overseas working-level officials, it was found that the utilization of blockchains is not indispensable or the cost for replacing the existing systems is too large in some cases.

Examination of the above use cases based on functions of blockchains compiled in 3.4.2 revealed that there are cases where not all functions are necessary. Especially unique functions of blockchains are considered to be "enabling the transactions whose authenticity is guaranteed (prevent duplicate payments)," "ensuring traceability of data and enabling transparent transactions (falsification is difficult)," and "stably maintaining the ecosystem against any attacks by malicious users without a central authority."

Regarding the function of "reducing server costs (for the development and operation)," which is often cited as one of the advantages of blockchains, it should be necessary to verify to what extent cost reduction is possible. In particular, in the case of replacing an existing client-server core system and where it is necessary to consider consistency with an information system and other peripheral systems, cost merit may not be necessarily large.

Fig. 5-2 Correspondence between use cases and functions of blockchains

	Local currency	Land registration	Supply chains	Sharing economy	Smart contracts
➢ Enable the execution of applications using a dedicated script			○		○
➢ Enable transactions whose authenticity is guaranteed (prevent duplicate payments)	○	◎		○	○
➢ Ensure traceability of data and enable transparent transactions (falsification is difficult)	○	○	○	◎	○
➢ Reduce server costs (for the development and operation)	Verification through demonstration is necessary.				
➢ Enable the development and operation of a stable system (zero downtime system)	○				
➢ Stably maintain the ecosystem against any attacks by malicious users, without a central authority		○	○	○	○

5.2 Expected Use Cases

Regarding use cases that are expected to be highly compatible with blockchains, their advantages and challenges are compiled below.

5.2.1 Local currency

It is possible to distribute and manage local currency issued by a local government, etc. on a blockchain. Local currency is issued to residents through certain procedures and is used at stores within the relevant community or for payments for public services, etc. Other possible usage include transfer of local currency among residents, use of local currency by stores that received the currency from their customers (for purchasing raw materials within the community or paying wages to employees residing in the community, etc.), and preferential tax treatment for taxpayers who paid their taxes with local currency. It is also technically possible to set expiration dates or design a mechanism under which the currency's value diminishes gradually, and to increase the amount of local currency in circulation by comprehensively combining such techniques.

i. Major information managed by blockchains

Blockchains can manage records of granting (who issued the local currency, and when and to whom the currency was granted), transfer (from whom to whom the currency was transferred), and use (when and where the currency was used for what purpose), as well as expiration dates of local currency, how fast value diminishes, and conditions for granting the currency (such as that the amount to be granted increases when a resident satisfies certain conditions (income, age, etc.)).

ii. Utilized functions of blockchains (corresponding to Fig. 5-2)

Out of the functions of blockchains, the following three are considered to be important in the provision of local currency services: “enabling the transactions whose authenticity is guaranteed (prevent duplicate payments),” “ensuring traceability of data and enabling transparent transactions (falsification is difficult),” and “enabling the development and operation of a stable system (zero downtime system).”

・Enable the transactions whose authenticity is guaranteed (prevent duplicate payments)

In issuing local currency, it must be ensured that the currency is granted correctly only once when certain conditions are satisfied. Furthermore, duplicate payments must be prevented also in the case of transferring or using local currency. In this respect, blockchains are effective in that they guarantee authenticity and can prevent duplicate payments.

・Ensure traceability of data and enable transparent transactions (falsification is difficult)

Under a mechanism allowing free circulation of local currency, it is also required to ensure that the fact of any duplicate payment can be checked, not only that duplicate payments are to be prevented as mentioned above. Under a mechanism where the total amount of local currency issued or their usage is determined, it is important that a third party can check whether the currency is issued and used correctly. In this respect, blockchains are effective in that they ensure traceability and enable transparent transactions.

・Enable the development and operation of a stable system (zero downtime system)

Local currency is supposed to be used for substituting settlement with legal currency, and high availability is required accordingly. Higher availability may be required for local currency than for loyalty point services. In this respect, blockchains are effective in that they can build and operate more stable systems.

iii. Points to note when utilizing blockchains

When utilizing blockchains for local currency, the following points need to be noted.

a Accuracy of timestamps affixed to transactions

It is necessary to ascertain the accurate time when the local currency was granted and used. Therefore, accuracy is required for timestamps affixed to transactions that are recorded on the blockchain, but in the case of the Bitcoin blockchain, for example, the time of a transaction depends on the participant who records said transaction. Accordingly, a mechanism needs to be established to enable a third party to objectively confirm the accuracy of the time.

b Finality (finalizing and completing transactions) that requires certain time

In the case of the Bitcoin blockchain, the time that a transaction is incorporated in the blockchain is unknown at the time of sending data of said transaction. Even if the transaction is incorporated in the blockchain, the parties are supposed to wait until following six blocks are created, in consideration of the possibility of a blockchain fork. Therefore, it is necessary to wait for approximately one hour at least until finality.

Some consortium-type or private-type blockchains adopt such means as forcibly determining the authentic blockchain to shorten time required for finality, but it should be noted that there still remains uncertain elements compared with centralized systems.

c Amount of transactions processed per unit time

It is said that the Bitcoin blockchain can process only five to seven transactions per second. In a local currency system, the number of transactions that need to be processed can be much larger. Therefore, it is supposed to utilize Open Assets Protocol, Sidechain, or other blockchains, etc. instead of only depending on the Bitcoin blockchain itself.

d Judgment of satisfaction of conditions for granting local currency

Conditions for granting local currency (procedures for purchasing the currency) are supposed to arise outside the relevant blockchain. It is necessary to transmit such external events to the blockchain (commence a transaction) and to make an agreement on who will take charge of that task and in what manner, in advance, for each service.

iv. Similar applications

In addition to local currency, blockchains may also be utilized for the following similar services.

- Remittance

Blockchains may be used for sending and receiving all value information including local currency and various types of virtual currency, not limited to remittance of legal currency. If a public-type blockchain is adopted, such remittance service naturally covers the whole world.

- Securities transactions

Transactions of computerized securities are easy on blockchains. It is expected that efforts for utilizing blockchains will be commenced with regard to company bonds for which transactions are less frequent.

- Loyalty point services

Companies can provide their loyalty point services on blockchains. If exchange of different types of loyalty points is made possible among users, the advantage of utilizing blockchains will become larger.

- Electronic coupons

A nearly similar mechanism may also be adopted with regard to electronic coupons issued by restaurants and retailers, etc. for managing their issuance and use. Under a mechanism allowing free circulation of coupons, in particular, the advantage of utilizing blockchains will be larger.

v. Impact on markets

If these services are provided on blockchains, this will affect markets for local currency,

remittance, securities transactions, loyalty point services, coupons, and merchandise tickets, etc. Sizes of respective markets are as follows.

- Amount of local currency in circulation: Approx. 0.3 to 1 billion yen (2015)[61]
  * Approximately 600 types of local currency are issued nationwide, each of which circulates at the amounts of 5 to 20 million yen annually.
- Remittance: 421.6 billion yen (FY2014)[62]
  * Annual amount handled by funds transfer service providers
- Securities transactions: 745 trillion yen (2015)[63] * Trading value
- Loyalty point services market: 850 billion yen or more (FY2015)[64]
- Coupons market: Approx. 40 billion yen (2013)[65]
- Premium merchandise tickets, etc.: 170 billion yen (FY2014 Supplementary Budget)

vi. Impact on industrial structure

(1) Immediate impact

It is expected that platforms for exchanging value of local currency will be established and will contribute to revitalizing local economies. Furthermore, it will be made possible to convert unused international electronic coupons into another form of value in Japan and diverse marketing tools may be developed.

(2) Future possibilities

- Conversion of various types of value into points

In the world where the fundamental infrastructure has been developed for local currency and loyalty point services using blockchains and such services are provided inexpensively, anyone can convert various types of value (including personal ideas or behavior, etc. that have not been covered so far) into points and manage them. Such points will be utilized in transactions with entities other than the issuer of the relevant points and will circulate freely.

- Blurring boundary between points and currency

As a result, points will be used in a similar manner as currency and may create an economic ripple effect larger than their issued value. For example, if energy saving points issued by the national

[61] Estimated by NRI, 2015
[62] Japan Payment Service Association
[63] Japan Exchange Group
[64] "2016 IT Navigator" by ICT Media Industry Consulting Department, Nomura Research Institute (Toyo Keizai Inc., 2015)
[65] Couponsite.jp; http://couponsite.jp/news/2014/02/2013.html

government or local points issued by shopping malls or other local entities can be directly converted to and managed with loyalty points issued by private companies or other value close to currency, etc., this will facilitate the use of points in a manner similar to currency and at the same time will stimulate consumer behavior.

With regard to public administration, if local governments can issue original points, they may find it easier to take economic revitalization measures targeting local areas or specific groups, which have been difficult due to the high cost of building required systems, etc.

- Building of trust with points

When point services have come to be used in a similar manner as general currency as mentioned above, they may have functions similar to deposit services and loan services. If so, points may also acquire a function to build trust, and there is a possibility that private companies will become able to launch some strategies similar to financial measures apart from the economic packages (financial measures) conducted by the Bank of Japan.

5.2.2 Land registration

It is possible to register, publicize, and manage information on land, such as physical status and related rights, on blockchains. Not only data on land, buildings, and owners, but also the transfer of land or other property and the establishment of a mortgage may be recorded and managed and this will improve the efficiency of related operational work.

i. Major information managed by blockchains

Information on land and buildings and records of transfer thereof can be managed. Additionally, information on the division and consolidation of land (parcel subdivision and parcel consolidation), as well as on ownership and mortgages or other related rights that is now managed on registries may also be managed on blockchains. Such information will be made available for inspection to anyone in the same manner as in the case of the current registries.

ii. Utilized functions of blockchains (corresponding to Fig. 5-2)

Out of the functions of blockchains, the following three are considered to be important in their application to land registration: “enabling the transactions whose authenticity is guaranteed (prevent duplicate payments),” “ensuring traceability of data and enabling transparent transactions (falsification is difficult),” and “stably maintaining the ecosystem against any attacks by malicious users without a central authority.”

・Enable the transactions whose authenticity is guaranteed (prevent duplicate payments)

When transferring land, appropriate procedures must be executed so that the transfer is carried out correctly only once, while avoiding the same land from being transferred to multiple persons. In this respect, blockchains are effective in that they guarantee authenticity and can prevent duplicate payments.

・Ensure traceability of data and enable transparent transactions (falsification is difficult)

It is necessary that matters registered in a registry, such as backgrounds for transfer and establishment of a mortgage, etc., are recorded correctly and past records can be checked. In this respect, blockchains are effective in that they ensure traceability and enable transparent transactions.

・Stably maintain the ecosystem against any attacks by malicious users without a central authority

At present, registries are managed by respective Legal Affairs Bureaus. This system can be replaced with a blockchain and the new system will operate stably without any central server. In this case, all nodes will be public organs and the possibility of involving malicious participants is quite low. Additionally, even in the event of a failure in a server, the system as a whole can continue operation.

iii. Points to note when utilizing blockchains

When utilizing blockchains for land registration, the following points need to be noted.

a Accuracy of timestamps affixed to transactions

When cancellation and establishment of mortgages, etc. are conducted in succession, the order of those procedures is important. The time of procedures is significant and must be accurate in order to process each of the procedures executed at multiple locations in the right order.

b Necessity to ensure the link with payments and receipts of money, etc. among parties

In the case of land transfers, payments and receipts of money will take place at the same time. Furthermore, when making loans, mortgages are often established. Such financial transactions including payments and receipts of money must be linked correctly with procedures for land transfers on blockchains. It is also possible to process payments and receipts of money themselves on blockchains.

iv. Similar applications

Blockchains may also be utilized for the following similar services.

- Patent information

Patent-related information may also be managed on blockchains. If not only the details of patents but also their ownership are managed on blockchains, the management of transactions of rights may also become possible on blockchains.

- Electronic health records

Personal medical data may also be managed on blockchains. Consistent medical treatment at multiple hospitals may become available with a due consideration to privacy by limiting information managed on blockchains to only records of individuals' hospital visits, while having respective hospitals manage details of their patients' health records.

- Document management (guarantee authenticity of vouchers)

Creating and updating histories of various documents may be managed on blockchains. On the other hand, means to prevent block sizes from ballooning such as through managing data themselves separately from the relevant blockchain (distributed DB, etc.) should be sought.

- Various notifications (notifications of birth, change of address, marriage, etc.)

Mainly various notifications to local governments may be managed on blockchains. For example, if the resident register is managed on a blockchain, a notification of change of address may be completed only with digital signatures of the relevant person and the local governments before and after the moving.

- Voting

Voting rights may also be managed on blockchains. (As long as digital signatures are safely managed) double voting can be avoided, while proxy voting, which is not allowed at present, may become possible.

v. Impact on markets

Sizes of related markets are respectively as follows.

- Land registration

Registration Information System, Ministry of Justice: 19.4 billion yen (FY2014)[66]

* Only operational cost

[66] "IT-related Investments by the National and Local Governments" (2015), Ministry of Finance

- Similar services

Patent Administration System, Japan Patent Office: 16.9 billion yen (FY2014)[67]

* Only operational cost

Electronic health records: Approx. 200 billion yen (Estimation for 2018)[68]

(Reference) Local governments' system-related budgets (FY2014)[69]

Municipalities: Approx. 520 billion yen (out of which, approx. 330 billion yen for operation)

Prefectures: Approx. 191 billion yen (out of which, approx. 127 billion yen for operation)

- Voting

The cost for the election of the House of Representatives in December 2012 was 58.7 billion yen.[70]

vi. Impact on industrial structure

(1) Immediate impact

Land registration, registration of patents and other rights, and various types of certificates, which have a counter-force, may be managed under an open distributed system at low cost and the private sector may also become able to issue certificates in lieu of the administrative authority. As a result, the land registration system by the Ministry of Justice, etc. or local governments' functions to issue certificates and manage registration will no longer be necessary, which may reduce the roles of the national and local governments.

Furthermore, management of passports, etc. on blockchains may prevent forgery.

(2) Future possibilities

- Proof and confirmation of identity

Blockchains may change or replace the culture of using seals for proving identity or procedures of document submission, etc. upon concluding contracts (such as for purchasing mobile phones or opening bank accounts). As a result, seal makers or other companies relating to proof of identity may be eliminated and procedures taken by financial institutions upon account opening, such as sending dedicated mails to relevant persons, may also be replaced.

- Proof of rights

The application of blockchains to bilateral contracts, which have not been subject to registration,

[67] "IT-related Investments by the National and Local Governments" (2015), Ministry of Finance
[68] Seed Planning, Inc., 2015
[69] "IT-related Investments by the National and Local Governments" (2015), Ministry of Finance
[70] http://www.soumu.go.jp/main_content/000235283.pdf

may enable data to be shared and traced, which will attach a counter-force to such contractual rights as well. Proof of rights may eventually have a counter-force without any supporting entity with authority or credibility, and an open and inexpensive distributed system may be able to fulfill the roles of administrative organs.

5.2.3 Supply chains

Production process of products starting from raw materials, as well as their distribution and sale may be traced on blockchains.

i. Major information managed by blockchains

Trade records (receipt and placement of orders, estimated delivery dates, etc.), processing records of processed goods, identification data of individual goods (lot number and specifications), information to guarantee authenticity, and the process from manufacturing to distribution of industrial products, etc. may be all managed on blockchains.

ii. Utilized functions of blockchains (corresponding to Fig. 5-2)

Out of the functions of blockchains, the following three are considered to be important in the provision of supply chains: “enabling the execution of applications using a dedicated script,” “ensuring traceability of data and enabling transparent transactions (falsification is difficult),” and “stably maintaining the ecosystem against any attacks by malicious users without a central authority.”

・Enable the execution of applications using a dedicated script

For example, when a manufacturing process contains a stage to assemble two types of components that were manufactured separately, a blockchain will manage the process and make it possible not to proceed to the assembling stage until the processing of the both components is completed.

・Ensure traceability of data and enable transparent transactions (falsification is difficult)

When any failure is found in a product, the manufacturing process can be traced back to the raw materials and the scope of recalled products, for example, can be specified easily.

・Stably maintain the ecosystem against any attacks by malicious users without a central authority

On a supply chain involving various stakeholders, such as raw material suppliers, processors, and distributors, a system not dependent on any specific stakeholder can be operated.

iii. Points to note when utilizing blockchains

When utilizing blockchains for supply chains, the following points need to be noted.

a Necessity to manage authority to update or append records

It is necessary to manage the authority, regarding whose record, what information and what timing.

b Necessity to ensure the consistency with actual processing stages and timing

Also in relation to the above, it is necessary to ensure the consistency with actual processes to avoid such cases as where an uncompleted process is recorded as having completed.

iv. Similar applications

In addition to supply chains, blockchains may also be utilized for the following similar services.

- Merchandise trades

If bills of lading (B/L) and letters of credit (L/C) are managed on blockchains and trades are managed with scripts, procedures that have remained manual and inefficient may be executed more smoothly.

- Management of precious metals and jewels

Utilization of blockchains for managing each piece of precious metals and jewels, such as gold and diamonds, from their processing stages will enable purchasers to check the processing records of products and this may increase credibility of products.

- Certification of authenticity of works of art, etc.

If works of art and artifacts with their creators' signatures are managed using blockchains, their authenticity can be confirmed even after being circulated in the market and copyright management will become easier, which may decrease counterfeits of works of art.

v. Impact on markets

Sizes of related markets are respectively as follows.

[Supply chains]

Total sales amount of GMS: Approx. 13 trillion yen (FY2015)[71]
Total sales amount of CVS: Approx. 10trillion yen (2015)[72]
Retail market of home electronics: 7.11 trillion yen (2015)[73]
Jewelry: 972.6 billion yen (2014)[74]
Fine art: 100 billion yen[75]
Domestic SCM software: Approx. 33.9 billion yen (FY2014) [76]
Manufacturing control software: Approx. 31.8 billion yen (FY2014) [77]

vi. Impact on industrial structure

(1) Immediate impact

Efficiency improvement is expected in accounting processes such as order placements, quotation offering, delivery, inspections, and payments, as well as in traceability and quality control. Additionally, tracking will become easier when any illegal or defective goods are found and contacts with purchasers will also be made easier.

As tracking records can be referred to, information asymmetry will be eliminated and the risk in selecting clients will be reduced.

(2) Future possibilities

- Change in commercial practices of distributors and retailers

Inventory information, which is separately held by retailers (downstream), wholesalers (middlestream), and manufacturers (upstream) at present, and timely commercial information (information on hot-selling goods), which is now apt to be exclusively held by the downstream sector, may be shared and made traceable on blockchains that are neutrally operated without a central authority. This may stimulate and facilitate supply chains as a whole and may also strengthen the bargaining power of the upstream sector. Furthermore, there is also a possibility that a new supply chain system across the existing sectors may be created.

- Switch of players

A distribution platform that enables more direct connection between final consumers and upstream manufacturers may be created and large-scale intermediary distributors like Amazon may lose much of their reason for being.

---

[71] Japan Chain Stores Association; https://www.jcsa.gr.jp/public/data/tokei_H27.pdf
[72] Japan Franchise Association; http://www.jfa-fc.or.jp/particle/320.html
[73] GfK Japan; http://www.gfk.com/jp/insights/press-release/2015-it-1/
[74] Yano Research Institute Ltd.; https://www.yano.co.jp/press/press.php/001365
[75] Nikkei Business Publications, Inc.; http://business.nikkeibp.co.jp/article/manage/20091125/210545/
[76] IDC Japan; http://www.idcjapan.co.jp/Press/Current/20150804Apr.html
[77] IDC Japan; http://www.idcjapan.co.jp/Press/Current/20150804Apr.html

Regarding electric appliances, with the progress of IoT and the development of the product assurance system, their lifecycles even after being sold to final consumers can be made traceable and a shift to new sales tactics that do not end with merely selling products will be facilitated.

5.2.4 Sharing economy

Information on transfer of rights to use of assets, etc. and evaluations by providers and users may be recorded on blockchains. At present, management and transactions of rights to use on blockchains are only supposed to be carried out in a sharing economy-type service, such as the one provided on platforms operated by specific companies like Uber and AirBnB.

i. Major information managed by blockchains

Information on holders of rights to use of assets to be shared, as well as information on transfer of such rights and payments and reciepts of money is to be mainly managed. Evaluations by providers and users (word-of-mouth information) may also be managed.

ii. Utilized functions of blockchains (corresponding to Fig. 5-2)

Out of the functions of blockchains, the following three are considered to be important in the provision of sharing services: “enabling the transactions whose authenticity is guaranteed (prevent duplicate payments),” “ensuring traceability of data and enabling transparent transactions (falsification is difficult),” and “stably maintaining the ecosystem against any attacks by malicious users without a central authority.”

・Enable the transactions whose authenticity is guaranteed (prevent duplicate payments)

In the case of an accommodation service, for example, the right to stay on a specific day must not be given to multiple groups. In this respect, blockchains are effective in that they guarantee authenticity and can prevent duplicate payments.

・Ensure traceability of data and enable transparent transactions (falsification is difficult)

To enable users to confirm that the relevant right is being duly distributed will increase their comfort.

・Stably maintain the ecosystem against any attacks by malicious users without a central authority

In the current sharing services, a platform manager plays an intermediary role between lenders and borrowers, but the utilization of blockchains can create a transaction mechanism without a central authority.

iii. Points to note when utilizing blockchains

When utilizing blockchains for sharing services, the following points need to be noted.

a Necessity to manage authority to update or append records

It is necessary to manage the authority to record information on goods to be shared, such as commencement and end of use.

b Necessity to ensure the consistency with actual use or right transfer stages and timing

It is necessary to make a record on a blockchain accurately upon evacuation of a place or return of goods, and clarification of procedures is required.

c Necessity to ensure the link with payments and receipts of money, etc. among parties

In the similar manner to the item above, when payment and receipt of money takes place at the time of the transfer of the rights to use, a record on a blockchain needs to be linked with the settlement. Settlement may also be made with virtual currency on blockchains.

d Consideration to privacy

A service system should be designed not to easily disclose the privacy of providers and users. When designing data management, consideration needs to be given to the fact that users' usage histories can be traceable.

e Method of paying fees to blockchains

Some blockchains require payment of tokens in addition to service fees. In many cases, tokens are to be paid by transaction parties or by users at present. Conditions for payment of tokens need to be agreed upon in advance.

iv. Similar applications

In addition to a sharing economy, blockchains may also be utilized for the following similar services.

- C2C auctions

By using blockchains for the management of auctioned goods, records of how they have been used can be preserved.

- Electronic libraries

By using blockchains for the management of rights to read electronic books, electronic libraries may be realized.

- Smart locks and smart sockets

Diverse usage of blockchains in daily lives can be considered, for applications such as for managing the authority to unlock a key or the authority to use electricity by plugging an appliance into a socket. New business models for using blockchains for these purposes to provide sharing services may be developed.

- Digital contents

In a similar manner to the case of electronic libraries mentioned above, rights to use digital contents can be managed by blockchains. This may promote use of digital contents while protecting copyright holders.

- Ticket services

If tickets that can freely circulate in the market are issued and managed officially on blockchains, it will become possible to efficiently manage the sale of tickets, while eliminating involvement of illegal ticket brokers.

v. Impact on markets

[Sharing economy]

Market size (domestic): Approx. 2 3 billion yen (2014)[78]

* Out of which, that relating to automobiles is approx. 18 billion yen, that relating to leasing is approx. 0.4 billion yen, that relating to clothing, etc. is approx. 0.6 billion yen, that relating to personnel is approx. 2.7 billion yen, and that relating to financial services is approx. 1.1 billion yen.

The market size (domestic) for FY2018 is estimated to be 46.2 billion yen.

[Similar services]

C2C auctions: Approx. 1 trillion yen (2014)[79]

Smart locks: Approx. 50 billion yen (2014)[80]

Ticket services: Approx. 500 billion yen (2013)[81]

[78] Yano Research Institute Ltd.
[79] Nikkei MJ, October 31, 2014
[80] Photosynth Inc.
[81] The Bridge, May 12, 2014; http://thebridge.jp/2014/05/startups-trying-to-ticket-business

Digital contents: Approx. 12 trillion yen (2014)[82]

Libraries: Ordinary expenses of public libraries excluding extra expenses amount to approx. 100 billion yen (2014).[83]

* Expenses for cloud-based library management systems are approximately 9 billion yen (2012).[84]

vi. Impact on industrial structure

(1) Immediate impact

Blockchains may contribute to facilitating the growth of the sharing economy as an emerging market. For example, when consumers generally doubt the security of a sharing economy-related business, the utilization of a blockchain may enhance credibility concerning security.

Additionally, surplus funds resulting from reduced expenses on in-house systems thanks to the utilization of blockchains may increase new business investments.

If evaluations and word-of-mouth information by users of various types of sharing economy are shared among them, information asymmetry will be eliminated and may further stimulate transactions, leading to the expansion of the relevant market.

(2) Future possibilities

- Elimination of the necessity of sharing economy service providers

Expected effects include increased utilization rates of idle assets, and dramatic efficiency improvement in the management of rights to use of admission tickets, hotel rooms, rental cars, rental videos, etc. However, there is a possibility that an environment may be developed in the end where C2C transactions can be executed without the involvement of service providers currently providing sharing economy platforms.

- Emergence of prosumers

As the boundary between consumers and producers or service providers becomes blurred, prosumers may emerge as mainstream.

5.2.5 Smart contracts

Contract terms, performed obligations, and future processes, etc. may be recorded on blockchains. The idea of a smart contract was already propounded in the 1990s,[85] but emergence of blockchains

[82] "Digital Content White Paper 2015," Digital Content Association of Japan (2015)
[83] "Libraries in Japan; Statistics and Lists," Libraries Survey Committee, Japan Libray Association (2015)
[84] Fuji Chimera Research Institute, Inc.
[85] http://szabo.best.vwh.net/smart.contracts.html

has made it achievable without the involvement of third parties.

i. Major information managed by blockchains

Contract terms, performed obligations, various procedures, and work processes are recorded.

ii. Utilized functions of blockchains (corresponding to Fig. 5-2)

Out of the functions of blockchains, the following four are considered to be important in the provision of smart contracts: “enabling the execution of applications using a dedicated script,” “enabling the transactions whose authenticity is guaranteed (prevent duplicate payments),” “ensuring traceability of data and enabling transparent transactions (falsification is difficult),” and “stably maintaining the ecosystem against any attacks by malicious users without a central authority.”

・Enable the execution of applications using a dedicated script

A smart contract system automatically conducts various processing tasks, and therefore, such processing tasks need to be registered as scripts in advance. Each script is implemented sequentially when respective conditions are satisfied.

・Enabling the transactions whose authenticity is guaranteed (prevent duplicate payments)

It depends on circumstances, but a mechnism to prevent the same processing task from being conducted multiple times needs to be put in place. It is also important to ensure that the execution of a contract can be proved retrospectively.

・Ensure traceability of data and enable transparent transactions (falsification is difficult)

It is important to ensure that a script itself can be updated and processing records are traceable.

・) Stably maintain the ecosystem against any attacks by malicious users without a central authority

Contracts should be managed on an open blockchain to preserve records of contracts, instead of each company separately operating their own blockchain.

iii. Points to note when utilizing blockchains

When utilizing blockchains for smart contracts, the following points need to be noted.

a Necessity to manage authority to update or append records

The management of authority to update smart contracts is indispensable in order to prevent unauthorized rewriting of contract details.

b Necessity to manage information on holders of rights on assets, and information on transfer of rights on assets and payments and receipts of money therefor

Transfers of assets, money and goods covered by smart contracts need to be managed respectively.

c Necessity to manage information on credit cards, etc. used for payments and other information on personal assets (shares, etc.)

Prior agreements need to be made with regard to whether legal currency or virtual currency is to be used for settlements upon transfer of assets, etc.

d Difficulty in correcting data

As it is difficult to correct information once recorded on a blockchain, measures need to be put in place in preparation for any error in the details of a smart contract or any erroneous processing.

iv. Similar applications

Under smart contracts, blockchains may be utilized for the following similar services, as well as in contract-related businesses in general.

- Derivatives (derivative financial instruments)

In derivative transactions, funds are paid and received under various conditions. If such conditions are determined in advance under a smart contract, automatic judgment of satisfaction of conditions and settlement processing may become possible.

- Escrow service

A smart contract system on a blockchain may eliminate the need for third party intermediaries in transactions and thereby realize an escrow service.

- Energy control

A smart contract system may enable automatic battery charging for electric appliances (home appliances and electric vehicles, etc.) connected to blockchains depending on their utilization status, and automatic settlements by predetermined means.

- Last testaments / Will

If a last testament is prepared as a smart contract during life, automatic execution of the testament upon the death of the relevant person may become possible.

- Company liquidation

A smart contract system may enable automatic allocation of assets or various rights in the event of company liquidation.

v. Impact on markets

[Smart contracts][86]

Accounting software: Approx. 70 billion yen

Consolidated accounting software: Approx. 7.5 billion yen

Personnel management and payroll software: Approx. 54 billion yen

* The above are the total market sizes for package software and cloud services.

Electricity service: 8 trillion yen[87] * The size of the electricity retail market liberalized in April 2016

IoT: 518.5 billion yen (2015)[88]

Inheritance tax: 11.6 trillion yen (FY2013)[89] * Taxable amount

vi. Impact on industrial structure

(1) Immediate impact

A smart contract system on a blockchain may replace most of the back-office tasks of each company (execution of contracts and transactions, payments and settlements, managerial decisions and other decision-making procedures, etc.). As a third party organization supervising the execution of contracts becomes unnecessary, escrow services may no longer be needed.

Contracts are executed automatically and their details are performed without depending on the credibility of contract partners, and this may decrease breach of contract disputes and may result in the reduction of litigation costs.

(2) Future possibilities

- Automatic execution of contracts

Various transaction scenes where written contracts are not prepared at present may be reccorded on blockchains as smart contracts and a number of transactions may be executed automatically to improve transaction efficiency dramatically. For example, transactions and settlements may be completed automatically irrespective of past business relationships with relevant clients and trading of surplus power among machines and purchase of maintenance supplies may become possible. If this is realized, companies and organizations will prefer products and services corresponding to such mechanism.

---

[86] Fuji Chimera Research Institute, Inc.

[87] http://www.enecho.meti.go.jp/category/electricity_and_gas/electric/electricity_liberalization/pdf/summary.pdf

[88] "IoT in 2030" by Kotaro Kuwazu, Nomura Research Institute (Toyo Keizai Inc., 2015)

[89] National Tax Agency; https://www.nta.go.jp/kohyo/tokei/kokuzeicho/sozoku2013/sozoku.htm

- Optimization of collection of taxes and provision of public services

If a micropayment service using a smart contract system is introduced in the world of IoT, it will become possible to build a cost-sharing mechanism that reflects the benefit principle more accurately, and this may make visible the workings of the local government administration. For example, waste treatment fees can be collected based on the amount and the collection methods of inhabitant tax may be altered. In the same manner, tollgates may become unnecessary thanks to a charging system based on the length of use and collection methods of vehicle tax and gasoline tax, etc. may be altered.

- Management of IoT devices without a central authority

In the world of IoT, where sensors and other nodes increase limitlessly, there is a possibility of the emergence of middleware utilizing bockchain technologies that manages not only these many and unspecified nodes but also all processes, including communications and transactions among nodes, without a central authority and that guarantees the credibility and security of data. Innovative means of managing devices and data may be developed, such as tracking information on the rights concerning individual data and feeding it back to right holders.

6 Impact on Society and Medium- to Long-term Challenges

Here, the impact on society and medium- to long-term challenges of blockchains will be discussed from the following three aspects: (i) technologies, (ii) business and work procedures, and (iii) systems and industrial policies.

6.1 Impact on Society

As explained in Chapter 5.1, blockchains may be technically utilized based on their functions of

- "enabling the transactions whose authenticity is guaranteed (prevent duplicate payments),"
- "ensuring traceability of data and enabling transparent transactions (falsification is difficult)," and
- "stably maintaining the ecosystem against any attacks by malicious users without a central authority."

Expansively, a blockchain may be defined as a protocol in a system with a certain number of participants to mutually approve value and information on the Internet without depending on specific entities or systems.

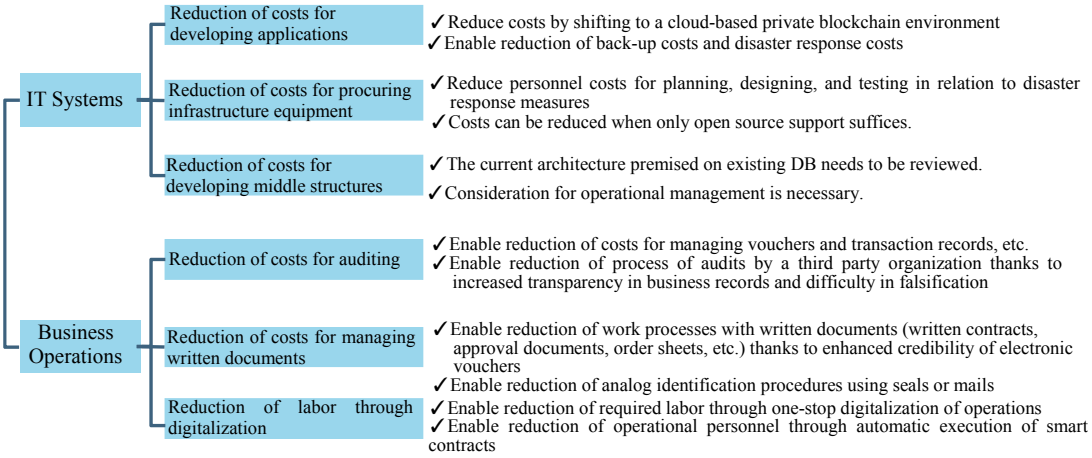
On the other hand, as a result of interviews with domestic and overseas working-level officials, it was found that the utilization of blockchains is not indispensable or the cost for replacing the existing systems is too large in some cases, as mentioned above.

In the short term, a large number of services for specific purposes will emerge through the utilization of blockchains. Such services include those dealing with local currency or other types of value information, those providing sharing services, and those managing commercial distribution, etc. In the same manner, individual services will be commenced for the management of land registration, patents, and various types of certificates, respectively. What is common to these services is the fact that a business model not dependent on an intermediary third party is developed in each business field and services are provided accordingly, and the impact of such new types of services on respective markets is considered to be significant. Adoption of blockchains may reduce costs for developing and operating systems (Fig. 6-1).

Regarding the city mayoral election in London in May 2016, Mr. George Galloway, one of the candidates, has pledged to make visible the usage of city budgets by using blockchain technologies, naming the project as "MayorsChain." He explains his plan to record public expenses on the MayorsChain and build an environment allowing anyone to track budget execution, thereby reducing

city budgets by approximately 5%.[90,91] Such moves to adopt blockchains in administration systems are expected to be accelerated.

Fig. 6-1 Expected cost reduction through the introduction of blockchains



In the medium- to long-term, services developed and operated indepently may be linked with each other. Then, rights and information being distributed on respective blockchains will come to be evaluated mutually and be exchanged with other rights and information based on their value thus evaluated. For example, when a service of offering private houses as temporary lodging and a local currency service are linked with each other, it will become possible for Mr. A to pay for coupon tickets for a public swimming pool in City C with his/her right to stay overnight at Mr. B's second house, without the involvement of an intermediary agent. In other words, barter exchanges will be reinstated through the utilization of blockchains. Virtual currency and legal currency will become necessary only for making up the difference in value of exchanged goods.

In the business world, various transactions are recorded on blockchains as smart contracts and automatization and labor saving will be facilitated. Automatic tracking of individual goods, starting from the import of raw materials to their processing, sale, and after-sales services, is made possible and intermediary agents will also be eliminated in this process. In particular, in the field of distribution, manufacturers and final consumers will be able to conduct transactions directly, and such trends will be closely related to the development of IoT. Sensors connected to blockchains will automatically carry out tasks in various scenes, such as placing and receiving orders for materials and supplies, measuring the amount of services used and charging fees, sending warning letters and taking primary responses, etc.

[90] http://mayorschain.com/
[91] http://uk.businessinsider.com/george-galloway-blockchain-bitcoin-mayorschain-london-2015-7

In the same manner as in the case of services for consumers, if various assets of companies (their own shares and other companies' shares, patents, and real estate, etc.) are distributed on blockchains, value based thereon will also start to circulate and credit may be created accordingly. Creditworthy companies with enormous assets will come to have power to control finance comparable to that of a national government.

All these moves are supposed to expand globaly both in the services and business fields.

Naturally, the role of administrative bodies will also change significantly. Regarding land registration, management of patents, and registration of marriage, etc., for which paperwork should not necessarily be carried out by the administrative bodies (although they need to ascertain the situation), the management using blockchains may sequentially be introduced. A digital signature using a wallet installed in a smartphone or other device may replace a seal to be affixed on documents to be submitted to an administrative institution. Furthermore, if the taxation system is incorporated in services using blockchains in the services and business fields in the form of payments with tokens, automatic collection of taxes and efficiency improvement may be realized and a mechanism based on the benefit principle will be ensured, exerting influence on the operation of the taxation system.

6.2 Medium- to Long-term Challenges

Various measures have been taken for challenges of blockchains as explained above. However, there are also medium- to long-term challenges.

6.2.1 Challenges in terms of technologies

i. Consistency with the real world

As in the case of a vending machine cited above, there is a problem that instructions need to be issued to a blockchain from the outside on a timely basis, and the timing of incorporation of relevant data in the blockchain is not known in advance. In particular, synchronization of time on a blockchain and in the real world is extremely difficult. For example, there is no guarantee that an instruction to execute Processing A at 10 o'clock on May 1 is actually commenced at exactly 10 o'clock. Similarly, another problem is that transactions are not finalized according to the CAP Theorem. Therefore, operational adjustments are made for each service. Transactions on the Bitcoin blockchain, for example, are considered to be finalized when six blocks are created and approved. However, it should be noted that the possibility of any other fork becoming superior in the following blocks is not denied here.

ii. Correction of information

One of the significant characteristics of blockchains is that records are preserved as data that cannot be falsified, but conversely, this means that records cannot be corrected retrospectively. It is necessary to consider measures to be taken in the event of an operational error or a script bug and how to protect privacy when personal information or privacy information is disclosed on blockchains.

iii. Appropriate application of individual technologies

There are problems concerning securing of partition-tolerance, guarantee of the accuracy of timestamps, and safe management of private keys, etc., for which technical knowledge accumulated so far is not fully utilized. Close communication between developers of blockchains and existing researchers is considered to be necessary.

iv. Specific verification of the effects of cost reduction

Regarding the function of "reducing server costs (for the development and operation)," which is often cited as one of the advantages of blockchains, it should be noted that there are cases where cost merit may not be necessarily large such as where it is necessary to consider consistency with an

information system and other peripheral systems when replacing an existing client-server core system. It is necessary to verify to what extent cost reduction is possible for each case.

6.2.2 Challenges in terms of business

i. Necessity to ensure the link with transactions in the real world

In terms of business, how to ensure the link with transactions in the real world is a big issue. In particular, the fact that actions requiring promptness cannot be guaranteed to be taken as required is a challenge and this is closely related to the challenge concerning finality. Initiatives to ensure that finality is achieved within a certain period of time are roughly divided into two approaches: one is to improve or expand the functions of PoW in a consensus algorithm, or in other words, to introduce a new algorithm such as PoI or PoS; and another is to install an algorithm not dependent on PoW, like PBFT, which can achieve finality in an extremely short time. At present, the relative superiority between these initiatives cannot be decided, but they are surely essential approaches to the challenge concerning finality. On the other hand, in the case of consortium-type or private-type blockchains, a method to have a specific node forcibly eliminate forks may be adopted as seen in Orb. Another option is to determine methods to confirm finality and rules in the event of forking of a blockchain, in advance, as business rules. The latter two approaches are more practical measures.

It is preferable that the validity of these approaches be verified in the respective business fields, based on what is required for finality in actual business scenes.

ii. Development of SLAs

Development of Service Level Agreements (SLAs) is also indispensable for providing services on blockchains. At present, the meaning of downtime of a blockchain, frequency of delayed processing, time required for eliminating delays, etc. are not clear on service levels. In order to apply blockchains in actual business, performance requirements and specifications need to be clarified. For that purpose, it is necessary to classify work procedures to which blockchains can be applied and develop SLA models respectively in accordance with their materiality.

It is evident from the experience of developing SLAs in various system fields that discussions by experts among each industry and beyond the boundary of industries are also required for developing SLAs for the utilization of blockchains. In the meantime, it should be noted that blockchains have different features from those of existing distributed systems. Simple application of evaluation indicators for existing systems may fail to effectively express the features of blockchains and may result in hindering further utilization of blockchain technologies. It is indispensable to prepare a broad-based platform for information sharing and discussions among experts in the field of blockchains and experts specialized in existing systems.

Furthermore, human resources development based on well-developed SLAs is also urgently needed. Present blockchain engineers have pursued blockchain technologies on their own, instead of having been trained based on existing curricula. From now on, industry, academia, and the public sector will have to design and implement their own programs to train the blockchain engineers required in respective fields.

iii. Standardization activities for blockchain technologies

Blockchains are innovative in the area of distributed systems and have significant potential along with many challenges. However, efforts for standardization have rarely been made so far. Technical features of blockchains make it difficult for each node participating in the relevant network to decide the structure of the system on its own initiative. Therefore, efficient decision-making processes for technically improving and expanding functions of blockchains are still being sought. The predictability or controllability concerning future technical specifications is extremely significant for companies intending to utilize blockchains.

Mr. Joi Ito of the MIT Media Lab compares the development of blockchains with the early period of the Internet and points out the necessity to make efforts for international standardization while promoting active community activities for blockchains. At present, various trials are being conducted for expanding the use of blockchains, but if nothing is done regarding such voluntary activities, various incompatible and less expansive specifications may emerge. Some efforts for standardization are required for efficient development of the blockchain market.

iv. Clarification of rules for sharing transaction costs

The Bitcoin blockchain has actually brought about innovation enabling remittance at far lower fees than that through the conventional financial system. However, the current Bitcoin blockchain requires the payment of bitcoins as fees (for network transactions) when sending transaction data, which means that a person purchasing goods with bitcoins must pay fees in addition to the price of the goods.

On the Bitcoin blockchain, transaction fees are to be borne by remitters. In ordinary business transactions, it is rare to have remitters bear transaction fees, and it is necessary to consider how to ensure consistency with the current business practices.

Additionally, on the Bitcoin blockchain and other blockchains, remittance fees are determined as proportional to the amount of information, not to the amount of money to be remitted. Considering that remittance fees charged in the existing financial system are generally proportional to the amount of money, it is important to discuss remittance fees for small amount transactions on blockchains. In particular, while the application of blockchain technologies to IoT is being discussed, it will become increasingly significant to consider cost sharing rules from the perspective of a micropayment

service.

v. Clarification of the exchange rate with legal currency

The exchange rate with legal currency is not always constant for virtual currency represented by bitcoins. Accordingly, a settlement mechanism may become complicated when trading goods or services that are defined only with legal currency. For example, when a person intends to purchase shares with bitcoins or other virtual currency, a prior agreement on the exchange rate must be made among related parties.

Furthermore, in the case of virtual currency linking to legal currency, like bitcoins, price fluctuations have been very large. If such price fluctuations continue, significant fluctuations in transaction fees (or transaction amounts) heighten risks for general companies that predicting transaction amounts would become even more difficult. Solutions for these challenges also need to be considered.

vi. Anonimity, Protection of privacy, and the trade-off with identity verification

The current Bitcoint blockchain somewhat guarantees the anonymity of entities making transactions, but transaction data are disclosed and their privacy is not guaranteed in that sense. Such mechanism that discloses transaction details cannot be utlized by entities that want to conceal the details of their transactions. Discussions on how to protect contract details that need to be kept secret from competitors are important.

In the meantime, transactions can be executed on the Bitcoin blockchain without going through a process of identity verification and this causes worries over money laundering from the perspective of a financial system. Such worries may be eliminated to some extent in consortium-type or private-type blockchains, but a more extensive discussion may be required.

6.3 Expectations for Administrative Bodies

Based on medium- to long-term impact on society and remaining challenges concerning blockchains, the following are expected for administrative bodies.

i. Support for accumulation of use cases

Unfortunately, compared to foreign countries, support for blockchain technologies is said to have been smaller in Japan in terms of personnel, goods, money, and information. In particular, it is pointed out that investments in ventures are qualitatively and quantitatively at a low level in the blockchain-related area. In order to gain an understanding of the potential of blockchain technologies in a short time frame, verification of hypotheses through demonstration experiments in various fields is indispensable. How to increase trials for hypothesis verification in a timely manner is an urgent issue.

However in Japan, demonstration experiments for blockchains have been conducted sporadically with individual companies and initiatives across industries or work processes have rarely been seen. The significance of the respective initiatives of individual companies is not denied, but cross-industry core use cases need to be verified speedily for the purpose of maximizing output by the limited number of blockchain engineers. Competent government organizations and industry groups should play a leading role in urgently sorting out use cases with significant impact and building a system to verify the validity of such use cases.

ii. Support for development and accumulation of blockchain technologies

Cryptographic technologies and database technologies used in blockchains are not at all novel. Japan is not too far behind other countries in terms of the number of researchers in these technological fields. Furthermore, Japan also has strength in the field of hysteresis signature, whose significance will further increase in blockchain technologies, and in the field of cryptographic calculations. However, blockchain technologies are not at all evaluated in these fields.

As public key certificates were not considered to be necessary for digital signature at the beginning, it is often the case that challenges of a new technology unexpected at the initial stage are gradually revealed. It is possible for Japan to build a system to contribute to the international society by utilizing those engineers in the fields of cryptography and digital signature, while making use of their technological knowledge, in bulding a common understanding of the probability of the technologies and in standardizing technologies based thereon. The Japanese government may be able to offer support for the building of such system.

In order to help the development of blockchain-related business in Japan and contribute to the strengthening of international competitiveness, the govenment is expected to offer support to related

technologies proactively, upon requests from the domestic industrial arena, and should thereby maintain the presence of Japan in efforts for international standardization of blockchain technologies.

iii. Enhancement of fundamental research

Blockchain technologies are said to have various information theory related challenges. It is required to verify consistency with theoretical theorems concerning distributed systems. Supporting blockchain-related research in the mathematical aspect and the information theory aspect as a priority research field for Japan will have a significant meaning and will eventually enable Japan to make international contribution in this field.

iv. Review of the existing administrative system

Blockchain technologies may function as the infrastructure allowing mutual approval without the need of a central authority. The application of such technologies may dramatically improve the efficiency of existing administrative procedures.

However, computerization of the administrative systems is still underway in Japan. Blockchain technologies can be used for further facilitating the computerization. For example, in the private sector, issuance and transaction of shares using blockchains required the computerization of share certificates in the first place. Similarly, it is preferable that the conventional administrative architecture, where various certificates are required for proving the ownership of rights, would be changed to a new one under which ownership of rights is recorded in lists. More extensively, the creation and introduction of a public notice blockchain system that can be used for identity verification may also be possible. Possible utilization of blockchain technologies needs to be taken into account when proceeding with the computerization of the existing analog system.

v. Optimization of taxation

Many blockchains adopt a mechanism to consume tokens when executing processing, and this can be utilized for collecting taxes. Utilization of a blockchain for procedures for tax payment will enable taxpayers to pay taxes with tokens. For example, when vehicle registration numbers are to be managed on a blockchain, a mechanism may be designed to have vehicle owners to pay tokens equivalent to tax amounts (such as vehicle tax) upon registering a new vehicle or changing users, etc. Such mechanim can integrate paperwork and taxation in relation to vehicle registration. If smart contracts come to be adopted widely, collection of stamp tax upon concluding contracts may also be automatized. In this case, the whole concept of stamp tax also needs to be discussed.

vi. Review of laws and regulations in consideration of technology advancement

When considering laws and regulations concerning blockchains, the perspective of law and economy (rules, markets, architecture, and system) is necessary. For such items as share certificates and bonds that can be managed under a list system, the scope of application will be wider.

According to Article 228 of the Code of Civil Procedure, electronic data equivalent to those presumed to be authentic sealed documents (two-tiered presumption) are only those electronic certificates issued by certificate authorities under the Act on Electronic Signatures and Certification Business. It is necessary to clarify what requirements need to be satisfied by data recorded on blockchains so that such data can be found to have certain legal admissibility under the Civil Code.

It is also said that regulations governing cases of issuing assets on a token market are not clear from the perspective of protecting consumers. When sharing economy develops on blockchains, it will become possible to purchase the right to use B with the right to use A, but how to impose consumption tax in such cases need to be clarified. Adjustments not only with the Payment Services Act but also with the tax-related acts are required.

Additionally, various blockchains may come to provide services across borders, and discussions on regulations and taxation regarding such cases need to be held internationally.

7 Conclusion

7.1 What is Blockchain?

A blockchain is a mechanism using a P2P that has functions of

- “enabling the transactions whose authenticity is guaranteed (prevent duplicate payments),”
- “ensuring traceability of data and enabling transparent transactions (falsification is difficult),” and
- “stably maintaining the ecosystem against any attacks by malicious users without a central authority.”

Expansively, it can be defined as a protocol to mutually approve value information on the Internet.

7.2 Who can Utilize Blockchains for What Purposes

Private companies may be able to provide various services without the involvement of an intermediary third party. Utilization methods in various fields have already been proposed and verification of possible impact upon actual application has been commenced.

Companies and administrative organs may achieve cost reduction by replacing existing work procedures with blockchains. Some countries have started to consider the adoption of blockchains as public infrastructure.

7.3 What Kind of Impact on Socioeconomy

In various fields, new business models without an intermediary third party will be developed and more efficient services will come to be provided, which may change the ecosystem of the relevant fields.

Value will come to be understood differently and it will become possible to directly exchange various assets and information with the use of virtual currency.

Various mechanisms within or across industries will be automatized and clerical procedures will be processed more efficiently.

Introduction of blockchains as administrative mechanisms or local governments’ systems will simplify various types of paperwork and reduce costs, and as a result, will enable the administration to concentrate on more substantial work. At the same time, it may become necessary to review the taxation system, including the mechanisms to collect taxes.

7.4 Challenges of Blockchains

Theoretical verification has yet to be conducted, and application of blockchains to actual services has not been demonstrated sufficiently. The background ideas of blockchains are completely different from those of existing systems, and methodologies for ensuring service levels and security have not been established.

Therefore, detailed discussions are required both in terms of technologies and in terms of business.

7.5 Things Required for Policy

Giving incentives to apply existing Japanese technologies accumulated in such fields as cryptography will contribute to the development of blockchains. At the same time, the government can promote hypothesis verification concerning blockchains and accumulate and broadly publicize outcomes and challenges in Japan, thereby efficiently facilitaing the development of the relevant market.

Furthermore, utilization of blockchains in the administrative field may accelerate efficiency improvement and sophistication of administrative affairs. This may affect the institutional design including the taxation system.

As the diverse changes explained above are supposed to take place globally across borders, efforts should be made cooperatively with other countries.