Chapter 1
Creation of Blockchain and a New Ecosystem

Makoto Yano, Chris Dai, Kenichi Masuda and Yoshio Kishimoto

The Japanese Ministry of Economy, Trade, and Industry regards the process of incorporating new information technology, such as artificial intelligence (AI), Internet of Things (IoT), and big data analysis into society as the Fourth Industrial Revolution. This view is reflected in the Fifth Science and Technology Basic Plan. The plan advocates Society 5.0, in which cyber space and physical space are integrated to support an affluent and human-friendly society. Computer scientists regard the interconnection of industry and society through information technologies, with people creating and using such technologies, as a single ecosystem. They have actively participated in the design and discussion of such an integrated ecosystem. Blockchain is considered to be at the core of such a cyber ecosystem.

Terms like the Fourth Industrial Revolution, Society 5.0, and cyber ecosystems seem colorful and might appear rather farfetched. However, when placed in the context of the current states of the economy and technological development, one

The original version of this chapter is written as a part of our final report to the study group "Blockchain and Society 5.0—The Creation of a New Marketplace based on Distributed Consensus" at the Research Institute of Economy, Trade, and Industry (RIETI). The authors are grateful to all the participant in the study group; the first author gratefully acknowledges the financial support of a Grant-in-Aid for Scientific Research (A) (#16H02015) from the Japan Society for the Promotion of Science.

M. Yano (✉)
Research Institute of Economy, Trade and Industry (RIETI), Tokyo, Japan
e-mail: yano-makoto@rieti.go.jp

C. Dai
Recika Co., Ltd, Tokyo, Japan
e-mail: chris@recika.jp

K. Masuda
Anderson Mori & Tomotsune, Tokyo, Japan

Y. Kishimoto
Ministry of Economy, Trade and Industry, Tokyo, Japan

M. Yano et al. (eds.), *Blockchain and Crypto Currency*,
Economics, Law, and Institutions in Asia Pacific,
https://doi.org/10.1007/978-981-15-3376-1_1

realizes that the new concepts are rather persuasive. This is because the technological innovation that is about to start is very unique in the long history of technological advancement since the First Industrial Revolution.

Today, we are witnessing the introduction of a new type of productive resource into our economy—data. Data is a new productive resource that had no economic value in the past. Until a few years ago, there was no way to gather large volumes of data that could capture daily life accurately, nor were there any computing technologies that made it possible to analyze an extremely large volume of data to explain complicated human interactions on both production and consumption sides of an economy. This has changed all of a sudden. Many productive resources, such as coal and oil, suddenly became valuable during past industrial revolutions. However, they merely replaced already existing resources. Coal replaced firewood and charcoal; oil replaced coal. Data, in contrast, does not replace any existing resources but is born as a completely new type of productive resource.

In short, industrial revolution in the past meant destroying existing resources and replacing them with new resources. Sitting in the middle of the Fourth Industrial Revolution, in contrast, data does not replace any existing resources.

From an economic viewpoint, this difference between past industrial revolutions and the Fourth Industrial Revolution is large. Previously, the ownership of oil was assigned to the owner of the land containing the oil, just as the ownership of coal was assigned before oil was utilized as a major energy source. In the case of data, we have not established a clear agreement on who owns the data. As Nobel laureate Ronald Coase (1910–2013) pointed out, the assignment of proper ownership rights is a prerequisite for the formation of a market.

In these circumstances, blockchain technology opens important avenues to make efficient and fair use of data. In a broader sense, this technology is also referred to as a "decentralized ledger," which can involve a large number of unspecified people to contribute to the effective and fair use of data in a decentralized manner.

In summary, blockchain is expected to play an important role in connecting information technology and technologies such as AI, IoT, and big data with our lives. From this point of view, this book investigates the roles that blockchain plays in a virtual ecosystem from various angles, in particular, from the following three viewpoints: (1) data ownership, (2) data transactions, and (3) data industry.

1 Data: A New Productive Resource

If you are a smart phone user, it must be impossible to think of a day without access to the Internet. A mechanism to assign unique numbers to various things and integrate them into the Internet is called the Internet of Things (IoT). Smartphones are all recognized as IoT terminals, identified by their unique identifiers called telephone numbers, and, now, play a central role in data storage on the Internet.

With the exception of the phone function, almost all the information acquired through smartphones is provided through the Internet. At the same time, we have

become an important source of information. Buying goods through Amazon is like offering part of your household account book. When using Facebook and the "like" function is used, some sort of preference is expressed toward society. Sending emails also implies providing information to society.

It is not only humans that can be connected with cyber space through IoT. Computer sensors can be placed on livestock in pasture to keep track of their health and nutritional needs. If sensors are attached to trees and every square meter of farmland, the growth conditions of trees and vegetables in every square meter of the field can be monitored. In this way, a new ecosystem of human beings and living things, with information technology as infrastructure, can be created. Sensors on a car can keep track of driving habits, which is useful to enhance driving safety. Similarly, sensors in a hospital room can monitor and report the state of each patient and give useful information to carers. In this way, we can create a new ecosystem based on information and communication technology.

In the ecosystem, all information is digitized and recorded as numbers. This is why the information exchanged in IoT is called data. With modern computer technology, huge volumes of data can be collected and scientifically analyzed in detail to gain insights into various phenomena much deeper and clearer than possible only 10 years ago. Results from data analysis have started to profoundly influence our society.

This has transformed data into a new type of productive resource, by which we can manage production processes in a much more precise manner. With data on people's medical histories, doctors will be able to diagnose a patient's illness much more accurately and give better or more appropriate treatments. With data on car driving, insurance companies will evaluate driving risks much more accurately, thus allowing them to reduce insurance fees where appropriate. With data on purchases in stores, both manufacturers and retailers have increased ability to market attractive products to customers. All these possibilities are brought about by the data-gathering capability of the Internet and the data-processing capabilities of modern computers.

2 Blockchain Technology

Blockchain may still be a new term for many readers. It is, therefore, appropriate to start with a discussion on the definition of blockchain.

A ledger is a book of permanent record. The record must be correct and tamper-free. A blockchain is a ledger that is put together on the Internet in a decentralized manner by an indefinite number of contributors.

Blockchain is a chain of files containing whatever needs to be permanently recorded. A basic blockchain connects files to form a simple string of chain. A more sophisticated blockchain connects files to form a net-like structure.

2.1 Blockchain and Data Ownership

A database is like an address book in which many data elements are stored systematically and organized for easy use. Blockchain is a new technology that allows us to record data and sources and recipients of data exchanged on the Internet, thereby creating an accurate, permanent, and very inexpensive database.

The first application of blockchain technology was the virtual currency called Bitcoin. Functionally, a virtual currency is much the same as a deposit currency that is based on bank accounts. Each bank account records debits to and credits from other accounts, which the bank keeps to be absolutely accurate and tamper-free. Because the record shows who owes how much to whom, and because people trust that the records are absolutely reliable, it can be used to transfer money through wire transfers; debit cards are a major means of payment nowadays. A virtual currency is a similar collection of accounts (called wallets) that record debits and credits. The difference is that the virtual currency accounts are on the Internet. Blockchain technology has made it possible to keep this record absolutely reliable by using algorithm without relying on a central authority like a bank.

Blockchain accounts record digital data, which plays the role of money because people trust that they are accurate and tamper-free. As this shows, blockchain can assign the ownership of each data piece to an account holder. This is the innovation that blockchain technology has brought to society.

2.2 Distributed Computing

Distributed computing is a revolutionary innovation in computer networks, which allows many terminal computers to perform complicated tasks independently (Holohan and Garg 2005). One good example is a category of games called "massively multiplayer online games" in which many different players participate and try to achieve their respective goals, which may vary from car racing to shooting to role playing. Blockchain technology is built on this idea of distributed computing and adds decentralization to enable individual participants to maintain a secure record of transactions, ownerships, and promises.

The initial design of a computer network, which connects many computers to share resources, is centrally managed. In building a centralized network, a network administrator is chosen, a large server computer is set up, a network connecting many computers is designed, and software is installed on the server and made available for network users. The administrator centrally manages users' network connections, and only users with connection permission can use the network. The networks of companies and universities are designed in this way, and the same is true for online banking systems that connect automatic teller machines (ATMs). In a centrally managed network, the terminal computers perform very minimal tasks. For example,

a bank ATM terminal recognizes the account number and the password, and then performs simple tasks such as deposits and withdrawals.

As a network becomes larger, it becomes more and more difficult to maintain a centralized network. The load on the central server increases, and the cost of managing the server becomes very large. Central servers can also become very attractive targets for malicious attacks, and once these servers are compromised, the entire system can be destroyed.

A distributed network is built by connecting various independent servers and computers. Various tasks are distributed to different servers, and altogether a single goal can be achieved. A large volume of tasks are assigned to terminal computers. As long as basic rules for connecting to the network are set and those rules are followed, any server and any computer can join the network.

Such rules are called protocols. In the most immediate example, the email address is separated by the at-mark, @; the part after the "at mark" is an address indicating a particular computer group; the part before is an individual in that group. This rule is a very small part of the large Internet protocol.

A distributed network makes it possible to utilize a large portion of the computing power of the computers in a network. The various computers connected to the network perform large tasks by computing independently while coordinating tasks through exchange of data. Having a large number of computers work independently can achieve great goals at very low cost.

2.3 Blockchain: Decentralized Ledger

Distributed computing has evolved as a computer network construction method. Blockchain is a technology that builds a ledger based on distributed computing in a decentralized manner. This might sound simple, but, in reality, it is not. To create a decentralized ledger, it is necessary to devise a totally new algorithm, and such work led to the creation of Bitcoin.

To create and maintain a secure decentralized ledger, it is not enough to use a security program; such security measures can be easily breached by experienced hackers. Even if many independent computers maintain ledger together with good intentions, they are still vulnerable to attacks by computers with malicious intentions. This is especially so if such a ledger maintains records that function as money or virtual currency, where absolute accuracy and permanence are required.

This problem was overcome by the first blockchain, known as Bitcoin. In most blockchain, the database is shared by a large number of servers. Each server stores the entire blockchain record and carries out similar jobs in parallel. These servers are called full nodes of a blockchain. A new server that wants to join a blockchain network is free to copy the blockchain record and download the necessary software to store the records. Once in a while, the records on participating servers are synchronized so that only one record is produced. With more nodes, the number of copies of

the blockchain's ledger throughout the world increases, which makes it extremely difficult for malicious computers to attack the blockchain.

The decentralized ledger database is linked with user accounts called wallets. A wallet is a record of a particular user's transactions, which is kept on the user's terminal computer. Once a transaction between two accounts is agreed upon, the account owners apply to the blockchain to record the transaction. In most of the existing blockchains, recorders of transactions are different from users who use a blockchain as a currency. In some blockchains, users of a blockchain record their transactions by themselves.

2.4 Mining

The Bitcoin blockchain uses "mining" to maintain the accuracy and reliability of transaction records.[1] Mining in the context of blockchain technology is to present a computer-generated crypto puzzle to individuals (computers), to give a prize (in Bitcoin) to the individual who solves the puzzle first, and to let the individual record the transaction. In competing for the prize, many people (computers) engage in solving the crypto puzzle to create transaction records. With only one individual out of many competitors receiving the prize, this process is similar to mining; and individuals engaging in solving puzzles are called miners.

As soon as a mining computer solves the existing puzzle, a new file (block) is created and attached to the existing chain of blocks. The new block creates a new puzzle to be solved. At the same time, the solution is announced to the network of mining computers. Mining computers check if that solution is correct. If the solution is in fact correct, mining computers start working on solving the new puzzle created by the block that they have just validated.

In this entire process, it is important that there is no single individual who is in charge of checking the validity and uniqueness of records on blockchain. Instead, many independent individuals check the validity of records, which produces a unique record (ledger). This process is completely decentralized.

For Bitcoin blockchain, on one hand, simple records of several transactions are put together and recorded as a new block. On the other hand, for Ethereum blockchain, user-executable computer programs and resulting transactions of executing the programs can be written into a new block by a mining node.

A problem with blockchains is that mining consumes computer resources not directly related to records. Many miners work on solving the puzzle posed by the blockchain. Because this puzzle can be solved by a sequence of computations, anyone can find an answer so long as he/she is prepared to spend enough computing resources.

As a result, if there are 1,000 miners, the computational resources used by 999 miners (i.e., electricity to run computations) will be wasted. As the value of virtual currency soars, the number of miners has increased dramatically, and it is said that

[1] For the technical side of mining, see Omote and Yano.

about 10,000 miners are active around the world. Given that the average time required to solve the puzzle is 10 min, it is possible that a huge amount of electricity is being wasted. To maintain the accuracy of the blockchain, a certain number of miners must be involved. Whether electricity is wasted is related to the number of miners required to maintain accuracy.

2.5 Advancement of Blockchain Technology

The Bitcoin blockchain proved that a secure ledger can be created in a decentralized manner without using a trusted authority who is specialized in managing a ledger. Since then, different types of blockchains have been created.

A blockchain called IOTA creates a blockchain model that is not based on mining, hence does not consume a large amount of electricity. The IOTA blockchain is not a linear chain of files as used by the Bitcoin blockchain. Instead, it has a very complicated network structure, which itself is impossible to replicate. This structure is called a directed acyclic graph (DAG). Each transaction file (block) is given two arms, each of which randomly grabs another file (directed from grabbing to grabbed files). As the number of files becomes larger, the number of arms increases by the power of 2, which soon becomes an extremely complicated structure. In this structure, a sequence of files is created in which a particular file grabs another file, which will grab the next, and so on. It has been shown that if such a sequence never contains a circle (acyclic), the structure can serve as a blockchain, which can dispense with the requirement for mining.

A few years after Bitcoin was introduced, a new blockchain called Ethereum was developed. It was able to execute any program and to create execution records, as well as record transactions.

Not only does Ethereum provide its own virtual currency, called Ether, it also works in conjunction with Ether to provide a "platform" for loading and executing programs. These programs are called smart contracts, which can program the execution of a promise between users with various contingencies.

Once a business can be run on a blockchain, business developers seek funding to further develop the business or for future businesses. Such funding is also carried out over the Internet in a manner similar to crowd funding. This method of funding is called ICO (initial coin offering), and it sells and collects funds for business vouchers called tokens.

3 Building a People-Friendly Ecosystem

Information technologies such as AI, IoT, and big data are expected to contribute greatly to the realization of a new human-friendly ecosystem. However, it is a mistake to think that such an ecosystem will be built if technological innovation is realized.

The modern economy faces major problems of data monopoly and data abuse. Society 5.0 can be formed only after overcoming these problems.

3.1 Society 5.0

The blueprint of Society 5.0 as advocated by the Japanese government is based on the following loop: collection of data from every part of society by IoT, creation of big data, data analysis by AI, and injection of results of data analysis back to society.

The government states, "In the information society (Society 4.0), cross-sectional sharing of knowledge and information was not enough, and cooperation was difficult."[2] It continues, "Social reform (innovation) in Society 5.0 will achieve a forward-looking society that breaks down the existing sense of stagnation, a society whose members have mutual respect for each other, transcending the generations, and a society in which each and every person can lead an active and enjoyable life."

The government argues, "Society 5.0 achieves a high degree of convergence between cyberspace (virtual space) and physical space (real space)…In the past information society, the common practice was to collect information via the network and have it analyzed by humans. In Society 5.0, however, people, things, and systems are all connected in cyberspace and optimal results obtained by AI exceeding the capabilities of humans are fed back to physical space. This process brings new value to industry and society in ways not previously possible." However, it is a mistake to assume that so long as technological innovation progresses, the image of Society 5.0 will naturally be realized without any effort.

3.2 Industrial Revolution and Market Quality

Since the First Industrial Revolution, industrialization has brought about the concentration of resources in specific industries and companies. Yano (2009) views this process as a dynamical system of technology and market quality.[3] According to Yano, massive technological progress lowers market quality. This brings about various social problems; essentially, the concentration of resources causes fundamental changes in lifestyle and social structure. Once market quality falls to a certain level, however, demand will increase because of accumulated knowledge and experience, which will stimulate new innovation (Yano and Furukawa 2019).

The First Industrial Revolution (1760s to the 1840s) began with the invention of steam engines in England. The textile industry underwent major technological

[2] https://www8.cao.go.jp/cstp/english/society5_0/index.html.

[3] For a further analysis on market quality, see Yano (2019).

innovation, many workers were hired, capital was invested, and production expanded. Instead of engaging in in-house production activities, people were hired in large factories. Capital was accumulated by companies rather than by individuals. This resulted in the exploitation of workers, which Karl Marx (1818–1883) criticized harshly (Marx 1867). The Second Industrial Revolution came with steel production, railways, large-scale iron and steel production, electricity, telegraphs and telephones, and machinery. Major companies became enormous, and were perceived as a menace to society (Hilferding 1910).

3.3 Data Monopoly and Data Abuse

Yano's theory applies to the recent progress brought about by the technological revolution in information and communication technology (ICT revolution). One of the most successful groups of companies after the turn of the century is GAFA, which represents the initials of Google, Amazon, Facebook, and Apple. These companies were very successful during the ICT revolution, and, in doing so, have collected large volumes of data.

This concentration of resources realized economies of scale and production efficiency. Nevertheless, many people are worried about data concentration on GAFA (Radingsky 2015).

This worry is not imaginary but real, as shown by the recent abuse of data collection by Cambridge Analytica. Cambridge Analytica is alleged to have collected the personal data of 230 million Americans through Facebook accounts and used it to influence voters in favor of Donald Trump in the 2016 US presidential election (Cadwalladr 2018).The original method of data collection, which was developed by two psychologists, was to offer an Internet-based psychological test for anyone interested, and, at the end of the test seek permission to access the respondent's Facebook profile. According to Cadwalladr (2018), 40% of the respondents gave permission. By using the data, the psychologists were able to measure personality traits and to correlate scores against Facebook "likes" for millions of people. This method was adopted by Cambridge Analytica, which obtained personal data and then devised methods to influence important votes such as the US presidential election and the Brexit referendum.

This is a clear warning that data can be badly abused by monopolizing it. Unless these problems are resolved, the integration of cyber and physical spaces may end up with a rather dark society that is far from the image presented by the Society 5.0 initiative. Avoiding the emergence of such a dark society is a pressing issue that we now face (Economist 2018).

3.4 Small to Medium-Sized Enterprises

Many people say that in the digital economy, data is a production factor equivalent to oil. Data needs to be shared and distributed throughout society if it is to be used effectively in the digital age. So far, however, data has accumulated in the hands of large companies trying to establish competitive advantage. As a result, data is just stored, and it is becoming more difficult for small and medium-sized companies to use data for innovation.

For small to medium-sized enterprises, an even bigger problem is that they do not have good access to human resources specialized in handling data. This has created an egg-or-chicken paradox. To break such a vicious cycle, we require a good ecosystem that allows everyone to own and trade data and utilize the results of data analysis.

To resolve these problems, blockchain technology is ideal. It can be expected to release data to every productive sector, thereby enhancing the productivity of the economy as a whole.

4 Organization of This Book

As discussed above, the integration of cyber space and physical space will not automatically lead to the creation of a human-friendly society unless a sound interface is created between such a society and data as a new economic resource. The main purpose of this book is to investigate the role of blockchains as such an interface. In particular, we focus on the roles of blockchains from three viewpoints: (1) data ownership, (2) data transactions, and (3) the data industry.

4.1 Data Ownership

Many people think that as the IoT becomes more important in the production process, data will become an increasingly important production factor. To make good use of these new resources, it is necessary to start with setting ownership. In Chapter 2, Steven Pu and Makoto Yano cover this issue in the context of market quality theory.

As pointed out by Ronald Coase, a resource cannot be put on a market unless proper ownership is assigned to the resource. Many people say that data in a coming digital economy is a production factor equivalent to oil for the existing economy.

To whom should ownership be assigned for such an important production factor? It is our view that the ownership of data should belong to the originator of data so

as to avoid inefficient and unfair use of data, which may result from monopoly and abuse of data.

Currently, most data that we produce is collected and accumulated by large Internet data companies, as presented by GAFA. Such data is kept in a black box, and there is no way for ordinary people to know how it is used. For the oil industry, on the one hand, everyone has a relatively clear understanding on the supply chain from producers to consumers. In the case of data, on the other hand, how it is used is kept under a veil.

For data to play an equally important role as oil in digital society, it must be shared and used by many people. Nevertheless, an increasing number of large companies are monopolizing data to establish a competitive advantage. Being stored in large companies, it is becoming increasingly difficult for small and medium-sized companies to use data for innovation. On the other hand, for large companies, there is no strong incentive to use data; it is adequate to hold the information to deter challenges from competitors. How can we improve this situation?

The first step is to return ownership of the data to the individual who produces it. Blockchains make it possible to record data ownership at a low cost. Once the ownership of data is decided, data can be traded. To assign proper ownership of IoT data and put it on a market, it is necessary to develop a new blockchain technology. In Chapter 3, Steven Pu explains the development of this technology.

4.2 Data as Money

As an increasing number of people accept Bitcoin and other virtual currencies, a number of associated problems have arisen, such as money laundering, transactions of illegal drugs, and speculative activities. If these problems are not resolved, virtual currencies may not circulate widely. At the same time, however, blockchain technology itself has shown that data can be used as money. It can create a reliable record (ledger) of transactions in a decentralized manner without a central administrator. In Chapter 4, Makoto Yano investigates the possibility that such a decentralized ledger currency can take over the conventional deposit currency and paper money, once the existing problems are overcome.

4.3 Data Industry

As noted above, Ethereum is a technology that makes it possible to run any program and to record the results on blockchain. This opens up an infinitely large possibility for blockchain business.

The market in which data is traded on blockchain is often called a marketplace. In a marketplace, anything can be traded from candy to golf club memberships. These transactions are made by software applications called decentralized applications (DApps). In Chapter 5, William Metcalfe explains the role of smart contracts in Ethereum and the current state of DApp technology and their applications.

In a blockchain marketplace, all transaction records are made public. In exchanges for virtual currencies, in contrast, they are not made public; in this respect, they are similar to marketplaces such as Amazon. For this reason, a virtual currency exchange can be called a centralized marketplace. Centralized marketplaces present themselves as a single point of failure, and, therefore, are prone to malicious attacks. Moreover, they lack transparency such that the actions of the organizer of a centralized market cannot be monitored by outsiders.

A bottleneck of the current virtual currency system is the time needed to carry out transactions. To overcome this problem and to provide more convenient transactions, an exchange market for virtual currency has been developed. However, the existing virtual currency exchanges are centrally controlled by exchange organizers. As a result, they are prone to malicious attacks, and in fact, a number of hacking incidents on exchange has been reported.[4]

The decentralized exchange (DEX) is a new DApp that has been developed to cope with this weak points of centralized marketplaces. DEX allows a seller and a buyer of crypto assets to make a direct exchange in a decentralized manner on blockchain. Data (crypto assets and transaction records) is held in a decentralized manner so that DEX does not present itself as a single point of failure to attackers. Furthermore, because the system is open to the public, transactions can be made in a much more transparent fashion. It is offered in exchange for investments in DApp development. In Chapter 6, Chris Dai explains DApps and DEX and explains the current state of token business.

A token is a device to raise funds for developing blockchains and blockchain applications (DApps). A token can be thought of as a ticket for using the services that a DApp promises to offer. It is offered in exchange for investments in DApp development.

The introduction of fundraising by token issuance may be a result of the decentralized nature of blockchain technologies. Because of decentralization, the start-up process of blockchain businesses is significantly different from that of conventional businesses. In the current state of society, in which blockchains are not yet established, it may be desirable to treat start-up blockchain businesses like venture investments. However, once the technology is established, a new decentralized financial system will become necessary. From these perspectives, in Chapter 7, we consider the desirable designs for a decentralized financial system for both short-term and long-term scenarios.

The main message of this study is that it is important to build an ecosystem in which the new technology (blockchain), laws and institutions, including data ownership,

[4]For a list of hacking incidences, see SELFKEY (2019), https://selfkey.org/list-of-cryptocurrency-exchange-hacks/,downloaded.

and markets for digital assets are harmonized. Market quality theory suggests that the ownership of big data collected through the Internet should be assigned in such a way to support high-quality digital data markets. See Chapters 2 and 7 for a discussion on desirable designs of the decentralized financial system from these perspectives.

In Chapter 8, Kazumasa Omote and Makoto Yano discuss the blockchain technology on which Bitcoin is based.

Appendix

As shown in Fig. 1, modern networks can be divided into three types: centralized, distributed, and decentralized. The Internet is a revolutionary technology that has transformed centralized networks into distributed and more decentralized networks. Blockchain is a technology that has made it possible to build a completely decentralized network on the Internet. However, the Internet is far less decentralized than a blockchain, meaning that a government can block Internet access for computers, as has been done in China. The network system of a blockchain, in contrast, cannot be directly interfered with by a government.

When creating a network there are three topologies to choose from: centralized, distributed, and decentralized. As mentioned above, a computer connected on a network is called a node. In a centralized network, a computer called a central node owns and manages the entire network. The central node is a single point of contact for information sharing, controlling access to all calculations and data, and storing data.

The biggest problem with centralized networks is that the central node becomes a single point of failure. In other words, if the central node is broken, the entire network will crash. Attackers can break the entire network by bringing down the central node. Also, because the network workload is concentrated on the central node, the larger the network, the greater the load on the central node.

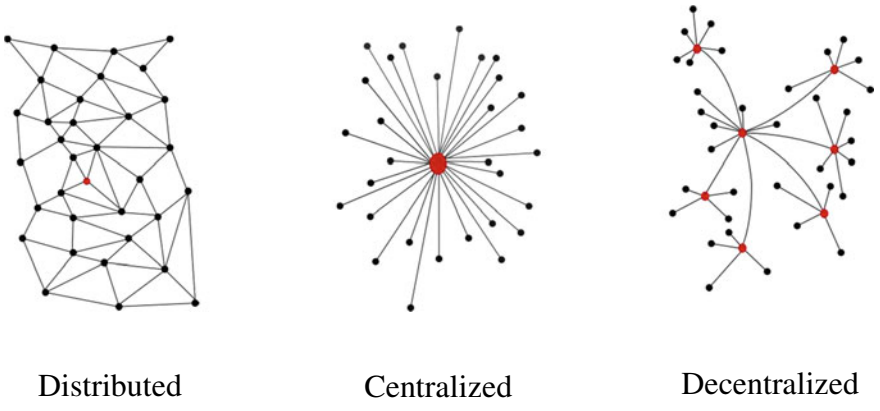

Fig. 1 Different types of networks

A distributed network is based on the concept of distributed computing. The Internet is a representative example. In a distributed network such as the Internet, each participating node performs computation and data storage independently but *appears to its users as a coherent system.* This eliminates the problem of single point of failure that can occur in centralized networks. Because nodes are independent, even if a particular node fails, information can be accessed from other nodes.

In a distributed network such as the Internet, there is no single central node. However, many nodes are similar to the central node of a centralized network and are located to perform management tasks. Such management nodes control the distribution of workload on the network and authenticate network participants. As a result, the work of the network is optimally distributed among the nodes and calculation processing is performed. Some distributed networks also have peer-to-peer networks, with only completely identical nodes without a central node. However, in this case, network-wide sharing of the same data is very difficult.

If a distributed open network is chosen to maintain a universal ledger instead of a centralized network, we need to eliminate the participation of malicious nodes. In this case, it is necessary to develop a special protocol to protect data and computations from spamming and incorrect data sent from malicious nodes. Blockchain technology makes this possible by utilizing an algorithm that protects data and computations from malicious nodes by majority vote of participating nodes. A calculation procedure (algorithm) based on blockchain technology is called a decentralized consensus formation algorithm or simply a "consensus algorithm." Such a network is called a decentralized and distributed network in the sense that it fully addresses malicious attacks based on majority agreements, and is distinguished from distributed networks that do not synchronize data across the network.

Consensus Among Blockchain Nodes

Public blockchain is a type of decentralized network. Nodes participating in the network independently execute software based on the same algorithm and maintain coordination throughout the network. The good thing about decentralization is that there is no central node, so there is no single point of failure and it is resistant to hacking and single node failure. Instead, there is a need to maintain common awareness of data across all nodes in the network. It is very difficult to synchronize data on a network where independent nodes are unstable (sometimes attackers can take control of some nodes). In blockchain protocol, the algorithm for achieving this synchronization is called the consensus algorithm. Consensus means that the data agreed upon across the network (majority of the nodes) will be reviewed and a copy will be stored at each node. This data agreement is similar to the political election system. The difference is how to count one vote. In a political election system, normally one person can cast one vote. However, there is no concept of "number of people" in the network of nodes (computers).To prevent the same person from voting more than once, the unit of voting must be such that a network of computers

can understand and quantify. For consensus algorithms such as proof-of-work (PoW) computational power is the unit of vote. For proof-of-stake (PoS), the unit of vote is the number of tokens you own or "stake." Unlike political elections, blockchain consensus (voting) is run much more frequently and automatically. For example, in the case of Bitcoin, consensus is reached at 10-minute intervals with the creation of a new block.

Sharding

Given that complete blockchain data is recorded on all full nodes as a feature of blockchain, it takes considerable time to synchronize and create new blocks (data) with a consensus algorithm on all nodes. As a result, blockchains like Bitcoin and Ethereum can only record about 7–26 transactions per second for the entire network. This is too slow for many applications. One solution designed to increase blockchain data recording/processing throughput is sharding. Even before the invention of blockchain, sharding was used to speed up database access by dividing the database to several parts and distributing the parts to several separate servers. Applying the same concept to a blockchain, rather than obtaining consensus from all nodes and then adding a new block (synchronization), groups (shard) of nodes can be created and if consensus can be reached within the group of nodes then a new block can be added.

Theoretically, with more shards and more blocks added in parallel, the overall network throughput becomes higher. However, while throughput can be improved, sharding also presents serious challenges. For example, with more shards, the number of nodes in a shard becomes less and they are more vulnerable to attacks. In addition, because it is also possible to process transactions across shards in what is a complicated process, there are concerns about both vulnerability and throughput of transactions.

Scalability and Decentralization

Scalability in blockchain refers to the speed at which blockchain can add transaction records and reach consensus across the network. Decentralization can be thought of as a measure of how independently nodes or computers agree on a set of transactions without central direction and control. As the system becomes more decentralized, it becomes more independent and the records become more tamper resistant from external monitoring and censorship. Technically, there is clear trade-off between the three factors characterizing a blockchain—scalability, safety, and decentralization. However, regardless of the purpose for which the blockchain is used, security is usually not a feature that can be sacrificed. In most situations, what matters is

the trade-off between scalability and decentralization. Sharding, described in the previous section, is a technology introduced to improve scalability.

During the early stage of blockchain application development, emphasis was placed on decentralization. As a result, technical performance and usability were sacrificed. For example, in a blockchain Dapp, the user is only given a password for login once and if lost, the user account cannot be recovered, and, as a result, the assets stored in the account will be completely lost. This maybe acceptable for an engineer who values the fact the password is not kept on someone else's server. However, most people are used to an environment where their account can be reissued or reset if the password is lost. To appeal to the general public, Dapps must centralize the password management to a certain degree to allow for unintended user errors.

Token Price: Security or Utility

During early development of the Bitcoin program, a whitepaper and prototype protocol were released and the open-source community worked together to ensure reliability and credibility based on the good intentions of ordinary engineers interested in the program. However, in such collaboration based purely on good faith, it is also difficult to secure enough resources to commercialize a blockchain project. In recent blockchain projects, financing was obtained by ICO (initial coin offering). A typical ICO sells a ticket for a service called a token.

The ICO fundraising method is often abused as a method to evade the securities law. If a token is recognized as a means of investment, it leads to speculative purchasing. As a result, prices can soar and be higher than their actual value. For example, during 2018, when the price of Bitcoin rose, it cost $10 to transfer $100 for Bitcoin. In this case, the Bitcoin transaction fee was higher than that of bank transfer and credit card, and therefore was not suitable to be used for payment.

An even bigger problem is that the token prices of blockchain-based applications fluctuate significantly due to speculation. The price of Bitcoin rose sharply in 2017 and dropped significantly in 2018. For speculators, price fluctuations provide a profit opportunity, but for actual users who pay cash to purchase tokens to use the blockchain-based applications will be dismayed at the price fluctuation.

Those who are trying to create new blockchain applications and provide them to the market are expected to solve these problems by providing stable tokens or virtual currency. For example, it may be useful to consider automatically adjusting the supply of tokens to price fluctuations, or to introduce an institution with a central bank function. Doing so may allow users to find higher value in blockchain application services. In the future, for the blockchain industry to grow, it is essential that the quality of service improves rather than having more speculative opportunities arise.

Traceability and anonymity

As mentioned earlier, originally, in blockchain, the account and the owner of the account were not linked. Movement of funds in each account was publicized, but only the owner knew who owned the account. In other words, the owner of the account was anonymous. By exploiting the anonymity, it is possible to transfer funds while keeping the identity of the account owner secret. This is very difficult to achieve with the banking system. Thus, blockchain appears to be well suited for use in illegal transactions and money laundering. However, anonymity in blockchain is not perfect, and identities may be uncovered if the system is abused extensively.

This fact is well demonstrated by the case of Silk Road, an illegal drug e-commerce site. Silk Road was launched in February 2011 and provided a marketplace for illegal drug trading until it was closed by the FBI in October 2013. This site provided the seller's account and the buyer's account, and seller's account was able to list products; that is, illegal drugs. The buyer was able to place the order anonymously and made payment using Bitcoin. As a result, the seller and buyer were able to trade the goods anonymously. It is estimated that more than 100,000 buyers and thousands of sellers were involved and more than 1 billion USD was traded before the closure.

By the summer of 2013, the FBI had already started an investigation of Silk Road and identified the IP address (the numerical address assigned to each computer server on the Internet) of the Silk Road site. The person who was operating Silk Road was arrested on charges of money laundering, computer hacking, and illegal drug transactions, and was eventually sentenced to life imprisonment.

As this case demonstrates, the high anonymity provided by blockchain is not absolute. Even if dubious Internet activities do not occur on a largescale like Silk Road, graph/data analysis can be applied to identify and trace fraudulent transactions.

In Japan, a registered virtual currency exchange is obligated to confirm the identity of a customer in accordance with the Crime Revenue Transfer Prevention Act. In addition, the virtual currency exchange manages the customer's deposit wallet and can link the account number and the customer's personal identification information. In this way, as the day-to-day blockchain transactions increase, various insights can be identified from the data, which may prevent crimes and identify suspicious transactions that exploit blockchain anonymity. In the future as more people use blockchain for their transactions in both the physical and cyber world, the protection of privacy for on-chain transactions may become a bigger challenge.

References

Cadwalladr C (2018) 'I made Steve Bannon's Psychological Warfare Tool': Meet the data war whistleblower. Guardian, 18 March 2018

Economist (2018) How to tame the tech titans – the dominance of Google, Facebook and Amazon is bad for consumers and competition. The Economist, 18 January 2018

Hilferding R (1910) Financial capital

Holohan A, Garg A (2005) Collaboration online: the example of distributed computing. J Comput-Mediated Commun 10-4, JCMC10415, https://doi.org/10.1111/j.1083-6101.2005.tb00279.x
Marx K (1867) Capital, vol 1
Radingsky K (2015) Data monopolists like Google are threatening the economy. Harvard Business Review, 02 March 2015
SELFKEY (2019) A comprehensive list of cryptocurrency exchange hacks. Downloaded at https://selfkey.org/list-of-cryptocurrency-exchange-hacks/, on 11 Nov. 2019
Yano M (2009) The foundation of market quality economics. Jpn Econ Rev 60–1(1–32):2009
Yano M (2019) Market quality theory and the coase theorem in the presence of transaction costs. RIETI DP19-E-097
Yano M, Furukawa Y (2019) Two-dimensional constrained chaos and time in innovation: an analysis of industrial revolution cycles. RIETI DP19-E-008

Makoto Yano is Chairman of the Research Institute of Economy, Trade and Industry (RIETI); he is also a specially appointed professor at Kyoto University, Jochi University, and Chubu University. He is an internationally known researcher who has made a number of substantial contributions in international trade, market theory, and especially on economic dynamics. His contributions in economic dynamics, for example, are represented by articles in *Econometrica* in 1995 and the *Journal of Economic Theory* in 1996, which explained the conditions under which general economic equilibrium shows chaotic behavior. His 1998 *Econometrica* article is recognized as the latest most important work on the characterization of dynamic general equilibrium.

Besides those rather theoretical works, Prof. Yano has also provided influential insights on contemporary real-world phenomena. Those include transfer problems (*American Economic Review*, 1999), voluntary export restraints (*International Economic Review* [IER], 1995), and trade conflicts (IER, 1998), on which there have been a number of follow-up papers.

His recent research on "market quality" addresses various problems in modern economies, including the financial market crisis since 2008 and the recent nuclear accidents in Japan, from the point of view of market quality—a new economic concept that Prof. Yano has developed and is applying to Japanese and international markets. Concerning quality of competition, quality of information, and quality of products, market quality is defined as an index jointly determined by the efficiency of an allocation and the fairness of the prices that are achieved in a market. Prof. Yano received a B.A. in economics from The University of Tokyo in 1971 and a Ph.D. in economics from The University of Rochester in 1981.

Chris Dai is the CEO and co-founder of Leland Capital, Recika Co., Ltd., and CEO of LongHash Japan. He has a broad range of business management and investment experience. He was formerly the COO/CIO of Yixing SCM (an international logistics provider), a consultant at Accenture, and a co-founder of multiple ventures. Starting in 2013, Mr. Dai was one of the early investors in Bitcoin and Ethereum. To promote the understanding of blockchain's true value, he joined the Research Institute of Economy, Trade and Industry's blockchain research team. He received a B.S. in management science and engineering from Stanford University in 2004.

Kenichi Masuda has been a partner at the law firm of Anderson, Mori & Tomotsune since 1997. He graduated from The University of Tokyo in 1986. After completing work at the Judicial Research and Training Institute, he was admitted to the bar in Japan and joined the law firm in 1988. He graduated from The University of Chicago Law School in 1992 and was admitted to the bar of the State of New York in 1993.

Mr. Masuda has extensive experience in advising foreign clients and is familiar with cross-border issues, in particular, mergers and acquisitions of listed and unlisted businesses, joint ventures, and other cross-border investments, as well as corporate restructuring. The scope of his experience also includes assisting and representing venture companies and establishing venture

capital or other private equity funds. He regularly provides legal services on employment and labor union relations (including representation of client companies in court and other dispute-resolution forums), real property transactions, intellectual property issues, and general corporate and commercial matters.

Mr. Masuda currently teaches at The University of Tokyo Law School as a visiting professor.

Yoshio Kishimoto is director general of International Policy for Small and Medium-Sized Enterprises (SMEs), Ministry of Economy, International Trade and Industry. He was vice president of the Research Institute of Economy, International Trade and Industry with Professor Yano.

He has held various positions in METI including head of the Environment and Economy Office, Business Support Division of the SME Agency, and director general of the Kyushu Bureau of METI. He received his M.A. in international affairs from Columbia University in 1992 and a Bachelor of Law degree from The University of Tokyo in 1985.