RIETI Policy Discussion Paper Series 19-P-029

Creation of a Blockchain and a New Ecosystem

YANO, Makoto
RIETI

DAI, Chris
Leland Capital / Recika

MASUDA, Kenichi
Anderson Mori & Tomotsune

KISHIMOTO, Yoshio
Organization for Small & Medium Enterprises and Regional Innovation, JAPAN

RIETI
Research Institute of Economy, Trade & Industry, IAA

The Research Institute of Economy, Trade and Industry
https://www.rieti.go.jp/en/

RIETI Policy Discussion Paper Series 19-P-029
November 2019

Creation of a Blockchain and a New Ecosystem*

Makoto Yano
Research Institute of Economy, Trade and Industry
yano-makoto@rieti.go.jp

Chris Dai
Leland Capital / Recika
chris@recika.jp

Kenichi Masuda
Anderson Mori & Tomotsune
kenichi.masuda@amt-law.com

Yoshio Kishimoto
Organization for Small & Medium Enterprises and Regional Innovation, JAPAN
kishimoto-yo@smrj.go.jp

Abstract

This study points out issues towards a better use of blockchain technology. It first identifies the role of data as the third major productive resources next to labor and capital in the digital economy and explains that block chain technology may facilitate an efficient and fair use of this important production factor. Blockchain technology may fundamentally change the current economy in three respects: (1) Data ownership, (2) money, and (3) data industry.

Keywords: headquarter, centralization, decentralization, information network, TFP
JEL classification: D23, L22, L25, M10

* This paper is a joint product of the two research projects at RIETI titled "Blockchain and Society 5.0-The Creation of a New Marketplace based on Distributed Consensus" and "Evidence-based Policy Study on the Law and Economics of Market Quality." All the authors are grateful to all the participants in the first project; the first author is indebted to the participants in the second project for discussions over many years even before the project started.

Creation of blockchain and a new ecosystem
Makoto Yano, Chris Dai, Keiichi Masuda, and Yoshio Kishimoto[1]

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 Society5.0, in which cyber space and physical space are integrated to support an affluent and human-friendly society. Computer scientists regards the entire industry or society interconnected by information technologies and 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.

The terms like the Fourth Industrial Revolution, Society5.0, and cyber ecosystems seem so colorful and might appear rather farfetched. However, if they are put in the context of current state of economy and technology, one 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 process of a new type of productive resource being introduced into our economy. That is 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 volume of data that can 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 become 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 the economic viewpoint, this difference between past industrial revolutions and the Fourth Industrial Revolution is large. In other words, the ownership of oil was assigned to the owner of the land containing oil just as that of coal had been assigned to that containing coal before people started using oil as a major energy source. In the case of data, we have not established a clear agreement on who owns data. As a Nobel Prize laureate Ronald Coase (1910-2013) points out, the assignment of proper ownership rights is a prerequisite for the formation of a market.

In these circumstances, blockchain technology opens important ways to make efficient and fair use of data. In a broader sense, this technology is also called

[1] The first author gratefully acknowledges financial support by the Grant-in-Aid for Scientific Research (A) #16H02015.

"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 technology such as AI, IoT, and Big Data with our life. 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 Resources

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). Smart phones are all recognized as “IoT” terminals, identified by their unique ID 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 you acquire through your smart phone is provided through the Internet. At the same time, we have become an important source of information. Buying goods through Amazon or Rakuten is like offering part of your household account book. If you use Facebook and press “like,” you will express your preference towards society. Sending emails also implies providing information to society.

It is not just humans that are just about to be connected with the cyberspace through IoT. If you embed computer sensors on cows and horses on a pasture, you can keep track of their health and nutritional needs. If sensors are attached to trees and every square meter of a farm land, you can know the growth conditions of one tree and vegetables in every square meter of a field. In such a way, a new ecosystem of human beings and living things, with information technology as an infrastructure, is going to be created. Sensors on a car can keep track of your driving, which would be useful to enhance driving safety. Sensors in a hospital room can report the state of each patient and give useful signals to care takers. In this way, we are just about to 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, by collecting a lot of data and analyzing it scientifically, it is possible to gain insight various phenomena much deeper and clearer that even 10 years ago. Results from data analysis have started to deeply influencing our society.

This has transformed data into a new type of productive resources, 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 to give much better treatments. With data on car driving, insurance companies will evaluate driving risks much more accurately, thus able to reduce insurance fees. With data on purchases in stores, both manufacturers and retailers can provide much more attractive products to customers. All these are brought about by the Internet’s data gathering capability and the computer’s data processing capability.

2. Blockchain Technology

Blockchain may still be a very new term for many readers. It may, therefore, be

useful to start with a discussion on what blockchain is.

According to Webster (unabridged, 1961), 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 Internet in a decentralized manner by an indefinite number of contributors.

Blockchain is a chain of files containing whatever needs to be recorded permanently. 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 a lot of data 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. Such a database is a ledger that a blockchain creates.

The first application of blockchain technology is a 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 serve as money through wire transferring; debit cards are major means of payment nowadays. A virtual currency is a similar collection of accounts (called wallets) that records debits and credits. Only the difference is that those accounts are on Internet. Blockchain technology has made it possible to keep this record absolutely reliable by using algorism 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 the society.

2.2. Distributed Computing

Distributed computing is a revolutionary innovation in computer networks, which makes it possible for many terminal computers to perform complicated tasks independently.[2] 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 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 trustable record of transactions, ownerships, and promises.

The initial design of computer network, connecting many computers to share

[2]Anne Holohan, Anurag Garg, Collaboration Online: the Example of Distributed Computing, Journal of Computer-Mediated Communication, Volume 10, Issue 4, 1 July 2005, JCMC10415, https://doi.org/10.1111/j.1083-6101.2005.tb00279.x

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; software is installed on the server and made available for network users. The administrator centrally manages the users' network connection, and only the users who have the connection permission can use the network. The network of companies and universities is designed in this way. The same is true for a bank's online system that connects 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 minimal jobs 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 will increase, and the cost for managing the server will become very large. The central server will become a very attractive target for malicious attacks; once the server is broken, the entire system can be broken.

A distributed network is built by connecting various independent servers and computers. Various tasks are distributed to different servers, and altogether a single goal is achieved. A large volume of tasks are assigned to terminal computers. As long as basic rules for connecting to the network is 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 tasks while performing independent task, and achieve a large job. Having a large number of computers work independently will allow you to achieve great goals at a very small cost.

2.3. Block chain: Decentralized Ledger

Distributed computing has evolved as one of computer network construction methods. Blockchain technology brings the idea of decentralization into distributed computing.

Blockchain is a technology that builds a ledger based on distributed computing in a decentralized manner. This might appear easy; but it is actually not. To create a decentralized ledger, it is necessary to come up with a totally new algorithm, which lead to the creation of Bitcoin.

In order to create and maintain a decentralized ledger securely, it is not enough to use a security program; such security measure will be easily breached by experience hackers.. Even if many independent computers maintain a ledger together with good intentions, they are still vulnerable to attacks by computers with malicious intents. Especially if such a ledger maintains records that function as money or virtual currency, you need absolute accuracy and permanence.

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. Those 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. The more nodes there are, the more copies of the blockchain's ledger throughout the world, which makes it extremely difficult for malicious computers to attack the blockchain.

The decentralized ledger database are linked with the user accounts called wallets. A wallet is a record of a particular user's transactions, which is kept in the user's terminal computer. Once a transactions between two accounts is agreed on, the account owners apply to the blockchain for recording that 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's adopts what is called mining to keep the accuracy and reliability of transaction records. 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. Competing for the prize, many people (computers) engage in solving the crypto puzzle to creating transaction records. In that only one individual gets the prize out of many competitors, 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.

What is important is that in this entire process, 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 on their own wills, which produce a unique record (ledger) in the end. This process is completely decentralized.

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

The problem with blockchains is that mining consumes computer resources not directly related to records. Many minors 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 1000 minors, the computational resources used by 999 minors (i.e., electricity to run computations) will be wasted. As the value of virtual currency soars, the number of minors has increased dramatically, and it is said that about 10,000 minors are active around the world. Also, since the average time required

to solve the puzzle is 10 minutes, it is possible that a huge amount of electricity is being wasted.

In order to maintain the accuracy of the blockchain, a certain number of minors need to be involved. Whether or not the electricity bill is wasted is related to the number of minors required to maintain accuracy.

2.5. Advancement of Blockchain Technology

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

A blockchain called the IOTA creates a new type of a blockchain that is not based on mining, which consumes a large amount of electricity. The IOTAis not a linear chain of files as in the Bitcoin blockchain. Instead, it has a very complicated net 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 power of 2, which will soon become an extremely complicated structure. In this structure,a sequence of files is created in which a particular file grab 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 without mining.

A few years after Bitcoin was introduced, a program called Ethereum was developed that was able to execute any program and to create execution records, as well as simply recording transactions.

Not only does Ethereum provide its own virtual currency, called Ether, but also it works in conjunction with Ether to provide a platform (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 for funding to develop or their future businesses. Such funding, too, is carried out over the Internet in a manner similar to cloud 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 technology such as AI, IoT, and Big Data is expected greatly to contribute 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 is something that can be formed only after overcoming those problems.

3.1. Society 5.0

Collect data from every part of a society by the IoT, create bigdata, analyze it with AI, and feed results of data analysis back to the society. An ecosystem realizing this loop is the blueprint of Society 5.0 advocated by the Japanese government.

The government states, “In the information society (Society 4.0), cross-sectional sharing of knowledge and information was not enough, and cooperation was difficult.”[3] 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 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 have brought about the concentration of resources in specific industries and companies. Yano (2009) views this process as a dynamical system on technology and market quality.[4] According to him, a massive technological progress lowers market quality. This brings about various social problems; the concentration of resources contributes a fundamental change in life style and social structure. Once market quality falls to a certain level, however, the demand will increases due the accumulation of knowledge and experiences, which will stimulate new innovation.[5]At the same time, it also lowered market quality and caused major social problems.

The first industrial revolution began with the invention of steam engines in England from the 1760s to the 1840s. The textile industry has undergone major technological innovation, many workers have been hired, capital has been invested, and production has expanded. Instead of engaging in in-house production activities, people were hired in large factories. Capital was accumulated in companies rather than individuals. This resulted in the exploitation of workers, which Karl Marx (1818-1883) criticized harshly.[6]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, which was perceived to be a menace to the society.[7]

3.3. Data Monopoly and Data Abuse

Yano’s theory applies to the recent technological 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 so successful during the ICT revolution that they have succeeded in

---

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

[4] Yano, M, 2009,

[5]Yano, M., and Y. Furukawa, 2019, “Two-dimensional Constrained Chaos and Time in Innovation: An analysis of industrial revolution cycles,” RIETI DP19-E-008.

[6]Marx, K., 1867, Capital, Volume 1.

[7]Hilferding, R., 1910, Financial capital.

collecting a large volume of data.

This concentration of resources realized economies of scale and production efficiency. Nevertheless, many people are worried about data concentration on GAFA.[8]

This worry is not imaginary but real, as is shown by the recent abuse of data collection by the Cambridge Analytica. The Combridge Analytica is said to have collected 230 million American's personal data through Facebook account and accused to using data to influence voters in favor of Donald Trump when he was a U.S. presidential candidate.[9]The original method of data collection, which was developed by two psychologists, was to offer an Internet service for psychological test for anyone interested and, at the end of the test in exchange for a permission to the respondent's Facebook profiles. According to Cadwalladr (2018), 40 percent of the respondents gave a permission. By using this data, the psychologists were able to measure personality treats and to correlate scores against Facebook "likes" for millions of people. This method was adopted by the Cambridge Analysica, which obtained personal data and came up with a way to influence such important votes as the U.S. presidential primaries and Brexit.

This is a clear warning that data can be badly abused by monopolizing it. Unless these problems are be resolved, the integration of cyber and physical spaces may end up with a rather dark society, which 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 face with.[10]

3.4. SMEs

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 they are 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 size enterprises, even the 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. In order to break such a vicious cycle, a good ecosystem is necessary in which everyone can own and trade data and utility the results of data analysis.

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

4.Organization of the Book

---

[8] Radingsky, K., 2015, "Data monoplists like Google are threatening the economy," Harvard Business Review, 02, March 2015.

[9]Cadwalladr, C., 2018, "'I made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," Guardian, 18 March, 2018.

[10]Economist, 2018, "How to tame the tech titans - The dominance of Google, Facebook and Amazon is bad for consumers and competition," The Economist, 18 Jan., 2018.

As is 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 new economic resources. The main purpose of this book is to investigate on 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) data industry.

4.1. Data Ownership

Many people think that, as the IoT becomes more important in the production process, data will become a more and more important production factor. In order to make good use of those new resources, it is necessary to start with setting ownership. Pu and Yano (2019) cover this issue in the context of market quality theory.[11]

As is pointed out by the Nobel Prize laureate Ronald Course, a resource cannot be put on a market unless a 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 ownership should be assigned for such an important production? It is our view that the ownership of data should belong to the originator of data so as to avoid the inefficient and unfair use of data, which may resulting from monopoly and abuse of data.

Currently, most of the data that we produce are collected and accumulated by large internet data companies, as presented by GAFA. Those data are kept in a black box, and there is no way for ordinary people to know how they are used. For the oil industry, on the one hand, everyone has a more or less 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.

In order 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 more 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 just enough to hold on to it so as 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 the data. Blockchains make it possible to record data ownership at a low cost. Once the ownership of data is decided, data can be traded. In order to assign proper ownership to IoT data and put them on a market, it is necessary to develop a new blockchain technology. Pu (2019) explains the development of this technology.[12]

4.2. Data as Money

As an increasing number of people accepts Bitcoin and other virtual currencies, a number of problems has 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

---

[11] Pu, Steven, and Makoto Yano,

[12] Pu,

that data can be used as money. It can create a reliable record (ledger) of transaction in a decentralized manner without a central administrator. Yano (2019) investigates the possibility that whether or not such a decentralized ledger currency can take over the conventional deposit currency and paper money, once the existing problems are overcome.[13]

A bottleneck of the current virtual currency system is a time that is needed to carry out transactions. In order to overcome this problem and to provide more convenient transactions, an exchange market for virtual currency has been developed. Kobayashi (2019) discusses the functions and issues associated with an exchange.[14]

4.3. Data Industry

As is 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 are traded on blockchain is often called a marketplace. On a marketpalce, anything can be traded from candies to golf club memberships. These transactions are made by software applications called decentralized application (DApp). Metcalfe (2019) explains the role of smart contracts on Ethereum and the current state of DApps technology and their applications.[15]

On 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 such market places as Amazon; for this reason, they 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, and what the organizer of a centralized market does cannot been monitored by outsiders.

The decentralized exchange (DEX) is a new DApp that is developed to cope with these weak points of centralized market places. The DEX makes it possible for a seller and a buyer of crypto assets directly to make an exchange in a decentralized manner on blockchain. Data (crypto assets and transaction records) are held in a decentralized manner so that a DEX does not present itself as a single point of failure to attackers. Because, moreover, it 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. Chris Dai (2019) relates DApps and DEX and explain the current state of token business.[16]

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 fund raisings by token issuances may be a result of the

[13] Yano (2019)
[14] Kobayashi (2019)
[15] Metcalge (2019)
[16] Dai (2019)

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 blockchain is not yet established, it may be desirable to treat the startups of blockchain businesses like venture investments. Once, however, the technology is established, a new decentralized financial system will become necessary. From these perspectives, Yano, Dai, Masuda and Kishimoto (2019) the editor of this book will study desirable designs for the decentralized financial system from both short and long run perspectives.[17]

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, and markets for digital assets are harmonized. Market quality theory suggests that the ownership of bigdata collected through Internet should be assigned in such a way to support high quality digital data markets. See Pu and Yano (2019) and Yano, Dai, Masuda, and Kishimoto (2019) for a discussion on desirable designs of the decentralized financial system from these perspectives.

Omote and Yano (2019) discuss the blockchain technology on which Bitcoin is based.[18]

Appendix

1. Networks

As shown in Figure 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. The difference is that the internet is far less decentralized than a blockchain so that a government can block internet access for computers, as has been done in China. A blockchain, in contrast, cannot directly be interfered within its network system by a government.

When creating a network there are 3 types of topology to choose from, centralized, distributed, and decentralized. As mentioned above, a computer connected on a network is called a node. In a centralized network, there are computers called central node that own and manage 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. The attacker can break the entire network by bringing down the central node. Also, since the network workload is concentrated on the central node, the larger the network, the greater the load on the central node.

A distributed network is a network 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 a collection of independent computers that appears to its users as a

[17] Yano, Dai, Masuda, and Kishimoto (2019)
[18] Omote and Yano (2019)

coherent system. This eliminates the single point of failure problem of 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 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 work 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 some special protocol to protect data and computation from spamming and wrong 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. Calculation procedure (algorithm) based on blockchain technology is called decentralized consensus formation algorithm or simply consensus algorithm. Such network is called decentralized and distributed network in the sense that they fully address malicious attacks based on majority agreements, and are distinguished from distributed networks that do not data synchronization across network.

2.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 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 1 vote. In a political election system, normally 1 person can cast 1 vote. However there is no concept of "number of people" in the network of nodes (computers). In order to prevent the same person from voting more than once, the unit of vote must be such that a network of computers can understand and quantify. For consensus algorithm such as PoW (proof of work)computational power is the unit of vote. For PoS (proof of stake), the unit of vote is the number of tokens you own or "stake". Unlike political elections, blockchain consensus (voting) is run a lot more frequently and automatically. For example, in the case of Bitcoin, consensus is reached at 10 min interval with the creation of a new block.

3.Sharding

Since complete blockchain data is recorded on all full nodes as a feature of blockchain, it takes a lot time to synchronize and create new blocks (data) with consensus algorithm reached on all nodes. As a result, blockchain 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 capabilities 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, instead of getting consensus from all nodes and then add 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, the more shards and more blocks can be added in parallel, the higher the overall network throughput. However, while throughput can be improved, sharding also has serious challenges. For one the more shards the number of nodes in a shard becomes less and more vulnerable to attacks. And since it is also possible to process transactions across shards, in that case the process is complicated and there are concerns about both vulnerability and throughput of transactions.

4. 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. The more decentralized the system the more independent and tamper resistant the records can be 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 use, 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, engineers' emphasis was placed on decentralization. As a result, technical performance and usability was sacrificed. For example, in a blockchain decentralized application often called "Dapps", the user is only given a password for login once and if he or she loses it, the user account cannot be recovered and as a result, the assets stored in the account will be completely lost. This may be acceptable for an engineer who values the fact his password is not kept in someone else's server. However, most people are used to an environment where their account can be reissued or reset if they lose the password. To appeal to the general public, Dapps must centralize the password management to a certain degree to allow for unintended user errors.

5 Token Price: Security or Utility

During early stage development of Bitcoin program, whitepaper and prototype protocol was 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 blockchain based on pure good will. In recent blockchain projects, financing is done by a method called 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 being purchased for speculative purposes. 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, therefore not suitable to be used as 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 apps 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 central bank function. Doing so may allow users to find higher value in blockchain app services. In the future, in order for the blockchain industry to grow, it is essential to improve the quality of service rather than providing more speculative opportunities.

6. Traceability and anonymity

As mentioned in the earlier section, originally, in blockchain, the account and the owner of the account are not linked. Movement of funds in each account is publicized, but only the owner know who owns the account. In other words, the owner of the account is anonymous. By exploiting the anonymity, it is possible to transfer funds but keeping the identity of the account owner secret, something very difficult to do with the banking system. So it seems to be a system that is easy to use for illegal transactions and money laundering. However, anonymity in blockchain is not perfect, and it is likely to be discovered if it 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 seller's account and buyer's account, and seller's account was able to list products, i.e. illegal drugs. The person who bought the illegal drug through the buyer account was able to place order anonymously and made payment using bitcoin. As a result, the seller and the buyer were both able to trade the goods anonymously. It is estimated that more than 100,000 buyers and thousands of sellers have been involved and more than 1 billion USD has been traded before the closure.

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

As this case shows, the high anonymity provided by blockchain is not perfect. Even if it is not a large-scale illegal activity such as 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, virtual currency exchange manage customer's deposit wallet and able to link 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, how to protect privacy of onchain transactions maybe a bigger challenge.

References:

Cadwalladr, C., 2018, "'I made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," Guardian, 18 March, 2018.

Dai, Chris, 2019. "DEX: A Dapp for the Decentralized Marketplace," mideo. RIETI.

Economist, 2018, "How to tame the tech titans - The dominance of Google, Facebook and Amazon is bad for consumers and competition," The Economist, 18 Jan., 2018.

Hilferding, R., 1910, Financial Capital.

Holohan, Anne, and Anurag Garg, Collaboration Online: the Example of Distributed Computing, Journal of Computer-Mediated Communication, Volume 10, Issue 4, 1 July 2005, JCMC10415, https://doi.org/10.1111/j.1083-6101.2005.tb00279.x

Marx, Karl, 1867, Capital, Volume 1.

Metcalfe, William (2019). "Ethereum, Smart Contracts, DApps," mimeo. RIEIT.

Omote, Kazumasa, and Makoto Yano (2019). "Bitcoin and Blockchain Technology," mimeo. RIETI.

Pu, Steven, (2019) "Industrial Applications of Blockchain to IoT Data," mimeo. RIETI.

Pu, Steven, and Makoto Yano (2019) Market Quality Approach to IoT Data on Blockchain Big data," mimeo. RIETI.

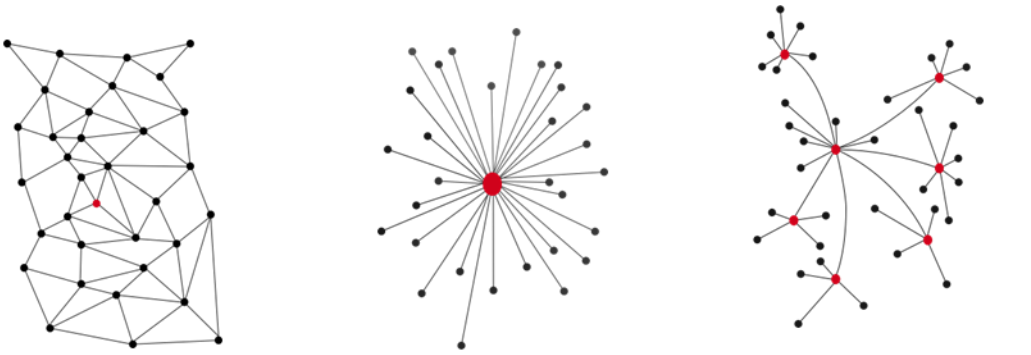
Radingsky, K., 2015, "Data monoplists like Google are threatening the economy," Harvard Business Review, 02, March 2015.

Yano, Makoto, 2009. "The foundation of market quality economics," The Japanese Economic Review 60-1, 1-32, 2009.

Yano, Makoto, 2019. "Theory of Money: From Ancient Japanese Copper Coins to Virtual Currencies," mimeo. RIETI.

Yano, Makoto, Chris Dai, Kenichi Masuda, and Yoshio Kishimoto (2019). "Blockchain Business and its Regulation," mimeo. RIETI.

Yano, M., and Y. Furukawa, 2019, "Two-dimensional Constrained Chaos and Time in Innovation: An analysis of industrial revolution cycles," RIETI DP19-E-008.



Centralized Decentralized Distributed

Figure 1: Different types of networks

https://en.wikipedia.org/wiki/Decentralised_system
https://en.wikipedia.org/wiki/Decentralization
”Decentralization: A Sampling of Definitions”, 1999, p. 13.
(http://web.undp.org/evaluation/documents/decentralization_working_report.PDF)
Johnson, Norman L. "Diversity in Decentralized Systems: Enabling Self-Organizing Solutions". Theoretical Division, Los Alamos National Laboratory, for University of California Los Angeles 1999 conference "Decentralization Two". CiteSeerX 10.1.1.80.1110.