National Institute of Informatics News ISSN 1883-1974 (Print) ISSN 1884-0787 (Online)

NII Today

55
Oct. 2015

National Institute of Informatics News

NII Interview

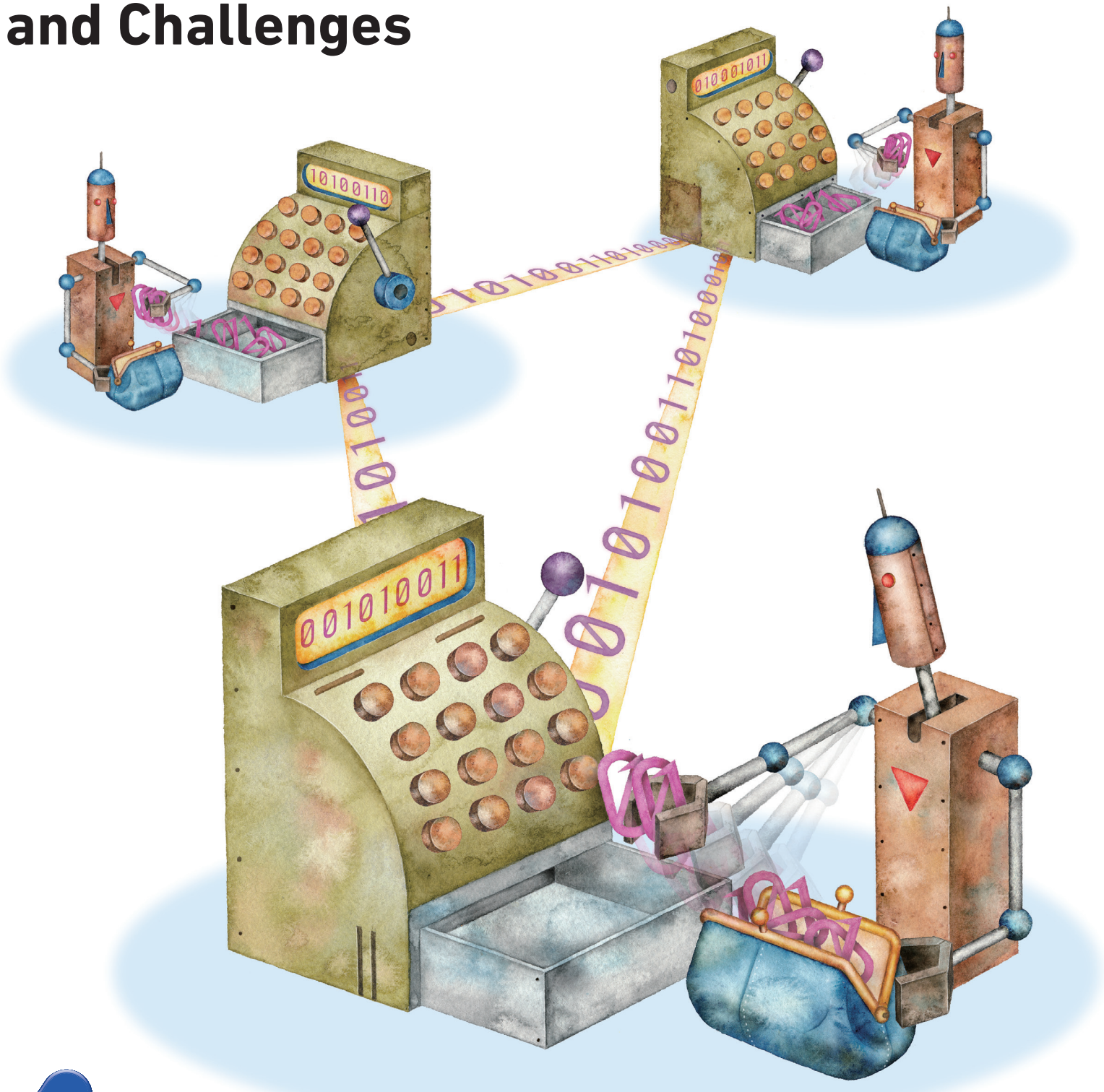
How Should We View the Rise of Virtual Currency?

The Block Chain Technology that has caused a Technological Leap in Virtual Currency

What is the Byzantine Generals Problem?

Feature

Virtual Currency Technologies and Challenges



This English language edition NII Today corresponds to No. 69 of the Japanese edition

How Should We View the Rise of Virtual Currency?

The world of virtual currency technology

Hitoshi Okada (Associate Professor, Information and Society Research Division, National Institute of Informatics / Associate Professor, School of Multidisciplinary Sciences, The Graduate University for Advanced Studies)

Interviewer: Katsuyuki Ohkawara (Journalist)

Virtual currencies such as Bitcoin are attracting attention worldwide. However, problems remain to be solved both technologically and socially. Virtual currency has not been widely evaluated in a positive way, due to problems such as the possibility for use as a means of unlawful cash transfer and the bankruptcy of some exchanges. Meanwhile, the technology behind virtual currency is progressing steadily and the legal system can be expected to develop further, which indicates that its use has the potential to become a major trend in the future.

Why is virtual currency attracting attention? As a researcher on information public policy, among other things, Associate Professor Hitoshi Okada has studied topics such as e-money and e-commerce, which are not fully covered by the existing legal system, since 1995. He says, "The environment surrounding virtual currency is similar to the dawn of the Internet around 1995." We asked Associate Professor Okada about the problems and challenges of virtual currency, as well as the supporting technologies and structures.

Hitoshi Okada

The risks surrounding virtual currency

Ohkawara: It seems as though the scandal surrounding Bitcoin in Japan has meant that the image of virtual currency as something dangerous precedes peoples' correct understanding of what it actually is. Is virtual currency dangerous?

Okada: Lumping virtual currency together in discussions can lead to the wrong conclusions. The first aspect is how risky the technology itself is. The second aspect is the degree of risk existing in the exchanges handling the virtual currency and the current structures and rules. Risk has to be looked at from at least these two perspectives. With regard to the former, many people may feel uneasy about the fact that decentralized virtual currencies such as Bitcoin are not endorsed by the state and have no issuing entity, so their structures are very different from previous currencies.

Ohkawara: Taking Bitcoin as an example, transactions are protected by encryption technology where all participants have keys, which come in the form of pairs of private and public keys. Also, unlike centralized e-money, the structure guarantees the correctness of payment information using the records of all participants using a method called a "block chain" (details on pp. 6–7). In that regard, as long as the private key is not destroyed or lost, the environment is capable of securing the Bitcoin held by a user. In the case of Mt. Gox, that kind of scandal would never have happened if the security of Mt. Gox as an exchange was secure and there had been robust management of access from inside the company.

Okada: In that respect, the problem now is not the structure or the technological challenges of the virtual currency itself, but the

Structure of Bitcoin
— the leading virtual currency

The origin of Bitcoin was an essay ("Bitcoin: A Peer-to-Peer Electronic Cash System", November 2008, https://bitcoin.org/bitcoin.pdf) written by an unidentified figure going by the name of Satoshi Nakamoto. Bitcoin is a virtual currency that is traded electronically and has a P2P structure (peer-to-peer: a type of system in which all participants act as both servers and clients to form a network). It is a method of payment that is circulated via networks, without endorsement from the state. The network technology on which Bitcoin is based ensures "independence", allowing the currency to be sent and received over the network, "safety", making it impossible to replicate or forge the currency, and "privacy", in that it does not specify users or usage history. It can be argued that it is an ideal form of electronic currency. Particularly significant is the fact that, although Bitcoin has no issuer or central administrator, it has features that are similar to real money such as "unrestricted negotiability", allowing it to be transferred directly between parties, and "divisibility", allowing face values to be divided. These features set Bitcoin apart from the e-money currently used in Japan.

Another important characteristic of Bitcoin is that the currency is generated by "mining". Mining involves storing several hundred most recent transactions in a ledger called a "block", adding the hash information of the preceding block, then adding a random number and running a hash function. The calculation is repeated until a certain number of zeros are aligned in the value obtained from the hash function (details on pp. 6–7). The mining (calculation) takes approximately 10 minutes, and only the winner who succeeds in deriving (mining) the calculation result gains the right to add the new record to the Bitcoin transaction record. Currently, 25 BTC can be obtained in one mining operation (this value will halve every 4 years). Transactions are validated by participants approving the calculation results. Sending a received virtual currency to someone else requires a digital signature using a private key stored in an electronic wallet and a public key that verifies the signature.

Thus, even without a central administrator, the unrestricted negotiability of Bitcoin is secured and transactions are validated by a combination of technologies, and this is what makes Bitcoin so fascinating for many researchers.

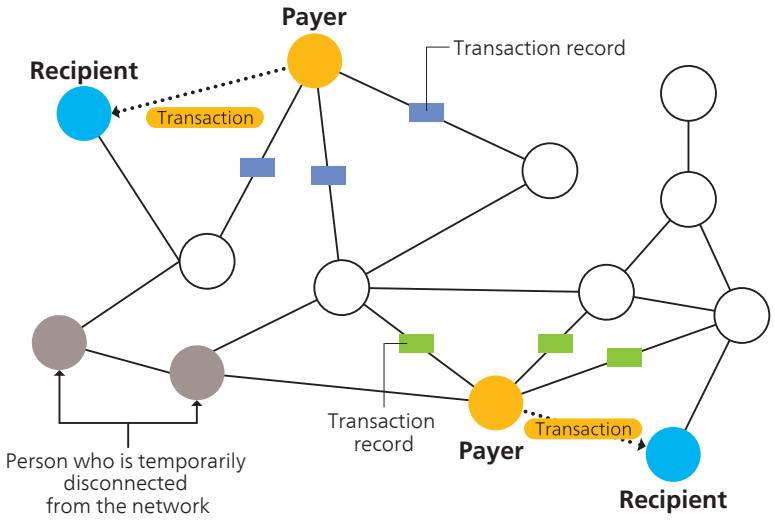


Figure A **Generating a Bitcoin transaction**
When the Bitcoin software is launched, it automatically connects the user to the P2P network. When a new transaction is generated, the payer broadcasts the transaction data to all participants.

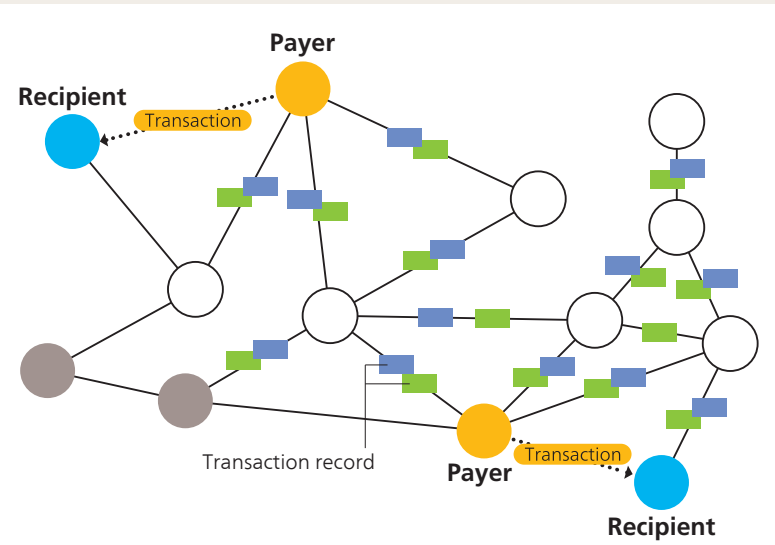
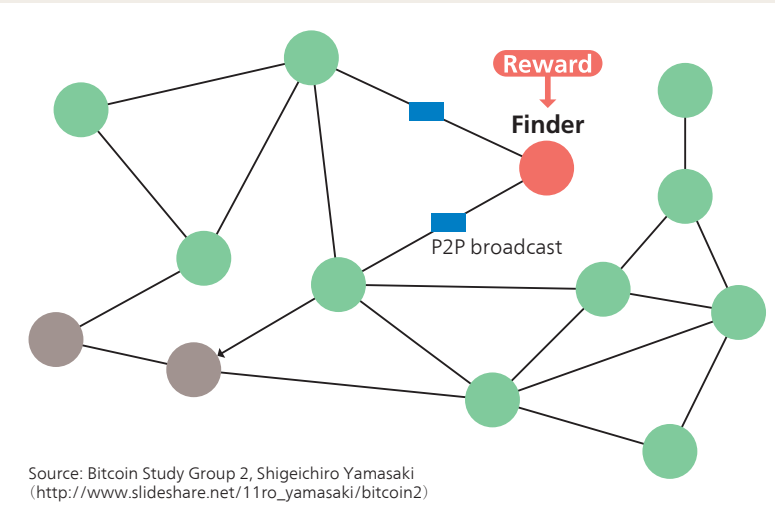


Figure B **Broadcasting on P2P network**
The nodes (relay points) in the P2P network pass the received transaction data to other nodes. The data are passed using a "bucket brigade" method and are eventually transmitted to all nodes.



Source: Bitcoin Study Group 2, Shigeichiro Yamasaki
(http://www.slideshare.net/11ro_yamasaki/bitcoin2)

Figure C **Finding proof of work**
Nodes participating in mining repeat a calculation until they discover a value with a certain number of zeros aligned. The node that finds the value first broadcasts the discovered value to all nodes.

Source: Bitcoin Study Group 2, Shigeichiro Yamasaki(http://www.slideshare.net/11ro_yamasaki/bitcoin2)

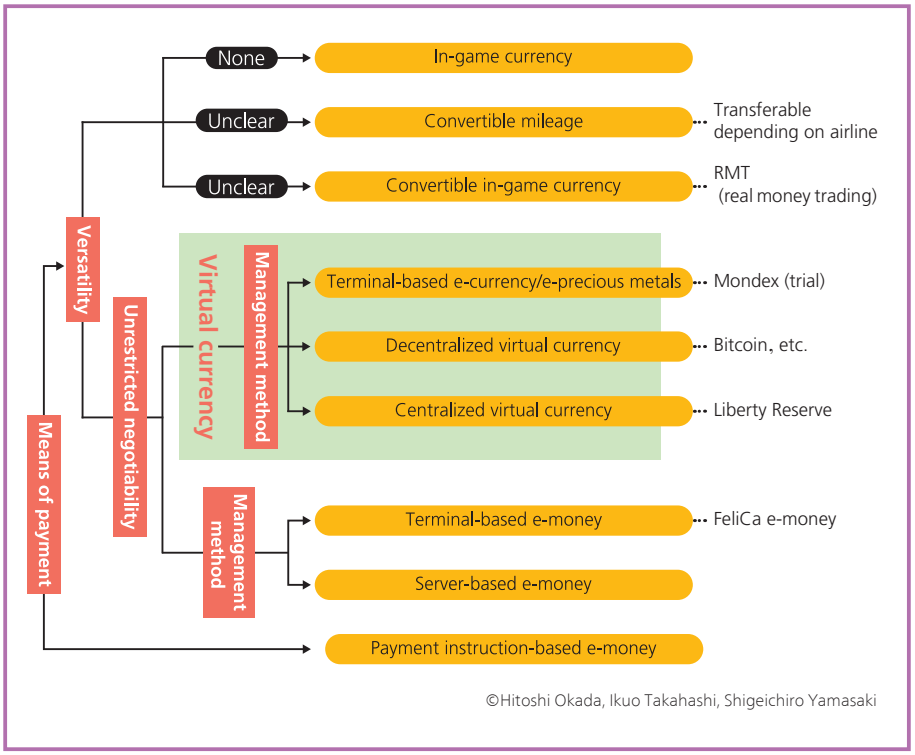


Figure **Classification of virtual currency and e-money**

technological challenges of the exchanges and their management systems, which is the second of the two aspects of risk that I mentioned earlier. Banking services can only be conducted by companies authorized by the Banking Act, but there is no regulation for virtual currency. It has been reported that the Financial Services Agency has started considering a license or registration system for exchanges. Such a structure is necessary to support a system of trustworthy exchanges.

In June of this year, the Financial Action Task Force (FATF), an international organization that polices money laundering, sought to tighten regulations on virtual currency by recommending the introduction of a license system for exchanges, and the State of New York, USA, has already begun operating a license system for virtual currency businesses. These kinds of systematic provisions will have a huge effect on the spread of virtual currency. However, license and registration systems must take into consideration the characteristics of virtual currency. It will not be sufficient to simply extend the existing Banking Act and approve exchanges based on them having financial industry know-how. Virtual currencies are used in ICT environments, and so having sufficient ICT knowledge and expertise and implementing secure environments are essential. In that sense, I think that information security audits will be a more important factor in the popularization of virtual currency.

Will virtual currencies become widespread?

Ohkawara: Currently, virtual currencies are only being used by a certain group of people known as "early adopters". Will virtual currencies become widespread in Japan?

Okada: Domestically, we may not really feel the need for virtual currency. Japan has a financial infrastructure, and we have only ever used currency issued by trusted entities, whether coinage, gift certificates, or e-money. Also, in most cases, we have been rescued when risk has occurred. Moreover, seeing the extent to which e-money has spread and how it can be used with ease throughout Japan, including in convenience stores and railways, there may be no real need to use virtual currency.

However, a response to virtual currency may be unavoidable in achieving the government's objective of increasing foreign tourists to 20 million in the run-up to 2020. The first problem facing foreign tourists upon arrival at Narita Airport is getting their first cup of coffee (laughs). In Japan, there tends to be an unwillingness to accept small payments by credit card, and so foreign tourists can't even buy a cup of coffee without first exchanging some money into Japanese yen. If they could buy the coffee using virtual currency, they would just need to have a smartphone. There are already stores accepting Bitcoin in places like Roppongi and Ginza, but in the run-up to 2020, further consideration may be given to establishing environments for using virtual currency in the retail and service industries.

Another aspect is the use of virtual currency by companies for international transactions. This is expected to increase, as it allows transactions to be made using a common currency value without being influenced by exchange rates, and it involves hardly any commission charges. International transactions are predicted to increase in Japan as a result of the TPP (Trans-Pacific Partnership), and I think that there will be moves to use virtual currency for these transactions.

Ohkawara: I don't get the feeling in Japan that virtual currencies will become particularly widespread.

Okada: That may be true, but the use of virtual currencies is quietly spreading in Europe and the US. The major American travel booking site Expedia and the major computer company Dell are starting to use virtual currency for payments. Also, in developing countries where many people do not have bank accounts, the use of virtual currencies is expected to spread with the popularization of the Internet and smartphones. Conducting financial transactions from a smartphone with a virtual currency account has the potential to spread very quickly. The combination of the Internet, smartphones, and virtual currency may be an effective approach to establishing a financial infrastructure in developing countries, and may mean that those countries come from behind to suddenly take the lead in this area. Clearly, once the high degree of convenience of virtual currency is recognized, its diffusion will accelerate further.

In fact, in terms of its similarity to cash, Bitcoin somewhat resembles the e-money Mondex that was trialled in Swindon, UK, in 1995, and initiatives that even involve banks in various countries are finally being implemented because requirements such as Internet payments and the spread of de-

vices have been met. It is also interesting that people who remember that trial have high hopes for Bitcoin and are trying to encourage improvements directed towards promoting its use. Incidentally, the main difference between existing e-money and virtual currency is that virtual currency has "unrestricted negotiability", meaning that it can be used as a means of payment between unspecified people and a transferee can transfer virtual currency to a third party. In this sense, virtual currency can possess characteristics that are closer to real currency.

Ohkawara: The Massachusetts Institute of Technology (MIT) has announced that it is establishing a state-of-the-art research institution aimed at popularizing Bitcoin, with MIT Media Lab Director Joichi Ito playing a central role. What influence will this have?

Okada: The structure of Bitcoin has a certain reputation, and many researchers and companies have paid attention to it because of that. However, one problem has been that real movements in new technology have not followed. That was the responsibility of the Bitcoin Foundation, but a more technology-neutral research institution is required. If MIT becomes able to support the evolution of core technologies from a neutral standpoint, it will further promote technical research into virtual currency.

Virtual currency resembles the Internet

Ohkawara: Do you mean virtual currency has the potential to change global financial systems?

Okada: If we consider the environment surrounding virtual currency now, it closely resembles the dawn of the Internet around 1995. One similarity is that there is no central administrator for either the Internet or Bitcoin. At the dawn of the Internet, there were discussions about what kind of technology it was and whether it was really safe and trustworthy. Many people were skeptical about the unknown technology then. On the other hand, its merits were also widely discussed. Looking at things today, we see that the Internet has changed the world greatly. Hardly anyone worries about its structure nowadays. People use it, knowing the risks. Similarly, attention is now focused on the structure, risks, and merits of virtual currency. Like the Internet, if many people feel there are benefits, virtual currency will spread naturally.

Ohkawara: The question of whether Bitcoin ownership rights will come into existence is under discussion, but should virtual currency be treated as property?

Okada: In Japan, this question was raised in the National Diet in March of last year, and a debate developed around the two alternatives of Bitcoin being currency or property. The government's response confirmed that Bitcoin does not fall into the category of currency, but it did not define it as property. First, it is necessary to discuss how virtual currency is positioned as currency.

Virtual currency is used in international transactions, and so Japan's system must be built with an eye on movements in Europe and the United States. In the US, currency is defined as something that has the power of legal tender, possesses negotiability, and is customarily used, but virtual currency is not regarded as having the power of legal tender. In other words, if you choose to accept a virtual currency, it holds true as payment, but it does not possess all the attributes of a currency. Similarly, in Japan, I think that it is appropriate to recognize virtual currency as a voluntary currency that can be used as compensation for a transaction upon obtaining the agreement of the other party. However, the position of currency in Japanese law and US law is different, and so legal consistency must be considered.

We must first clarify the systemic and technological risks of virtual currency, and then start preparing for those risks with a full understanding of the technologies and structures. Looking ahead, it is essential that Japan accumulate cutting-edge technology and expertise relating to Bitcoin's core technology—the block chain.

(Photography: Yusuke Sato)

A Word from the Interviewer

Virtual currencies with no issuing entities differ greatly from our conventional systems of currency, and so it is natural for there to be voices of concern. However, perhaps now is the time for a change in thinking. In an age when the Internet and mobile environments have become established as social infrastructure, the use of virtual currencies is inevitable. Especially in developing countries that are unfettered by the past, the spread of virtual currencies may happen very quickly. I am concerned that Japan may lose its competitive edge in international transactions if Japanese people are slow to change their way of thinking. It is important that people gain a correct understanding of virtual currency, rather than holding a preconceived notion that it is risky.

Katsuyuki Ohkawara Journalist

Born in Tokyo in 1965. After working as editor-in-chief of an IT industry journal, became a freelance journalist in 2001. Has interviewed and written extensively in areas centering on the IT industry for more than 25 years. Currently writing for business magazines, PC magazines, and web media.

The Block Chain Technology that Has Caused a Technological Leap in Virtual Currency

Potential application to transaction support technologies

Shigeichiro Yamasaki
(Professor, Department of Information and Computer Sciences,
Faculty of Humanity-Oriented Science and Engineering, Kinki University)

Various technologies and systems aimed at enabling the circulation of currency as electronic information over networks have been explored. Bitcoin virtual currency, in particular, has attracted researchers' interest due to its clever structure and technology that ensures soundness without either an issuing entity or an administrator. What is the "block chain technology" behind the soundness of Bitcoin transactions? Professor Shigeichiro Yamasaki of Kinki University, who researches block chain application systems, explained the technology.

Virtual currency is "a method of payment that is circulated via networks, without endorsement from the state." For currency to be circulated as electronic information over networks, it must possess "unrestricted negotiability", similar to real money. This is a combination of two elements: "negotiability" that allows it to be used for payments between many unspecified people, and "successive transferability" that allows it to be transferred by the person who receives it to a third party. For a currency to be fit for practical use, there must also be measures in place to prevent fraud such as falsification of transaction details and double spending.

When there is a centralized management system that involves a trusted third party, unrestricted negotiability and prevention of fraud can both be achieved. However, ensuring the credibility of a third party involves operational costs and creates problems such as escalating commission charges.

A structure that elaborately combines technologies

Bitcoin has skillfully resolved these issues. The concept of this virtual currency, described in an essay published in 2008 by a mysterious figure calling himself Satoshi Nakamoto, allows unrestricted negotiability via the Internet while preventing fraud using only software and a distributed network system.

The individual component technologies are not actually new, but are proven technologies in practical use. The Bitcoin structure brilliantly combines these reliable technologies based on an elaborate concept, and has brought about a technological leap forward in virtual currency.

The foundation is a P2P (peer-to-peer) network in which terminals with equal status are connected directly and exchange data with each other. When the Bitcoin software is installed and launched, it automatically connects the user to the network.

There is no central server or central storage in a P2P network. Transaction data are stored in each user's terminal. When sending Bitcoins, the sender transmits data called a "transaction" to all users connected to the network, not just to the recipient. Then, the transmitted transaction is stored in a database called a "block chain".

What is block chain technology?

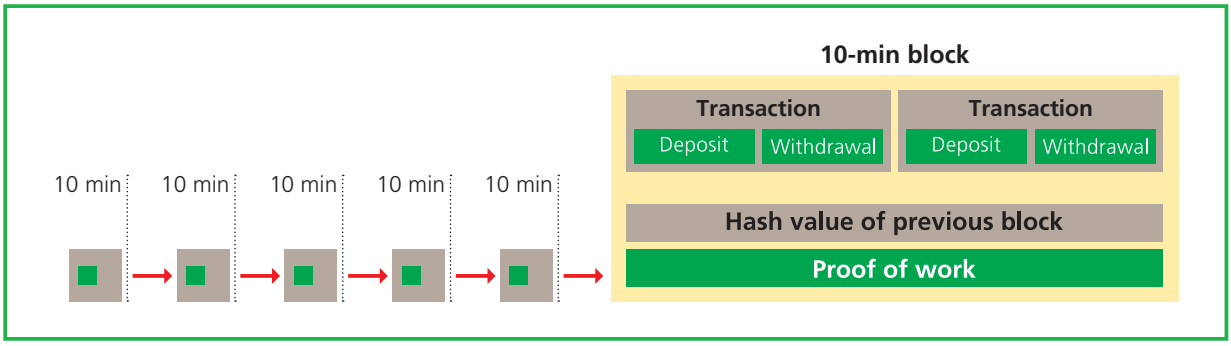
This system of storing data in a block chain is at the heart of Bitcoin.

Bitcoin users can participate in a calculation competition that uses cryptographic hash functions. The concept can be explained by likening it to a contest in which players throw a pair of dice and the first player to throw lower than a specified value is the winner.

The winner of the calculation competition verifies the transactions within approximately the last ten minutes, creates a "block" of data that includes the calculation solution (proof of work), and sends it to all Bitcoin users. The users receiving the block each verify its contents, and if they decide that it is all in order, the block is connected to the existing blocks and saved.

Because blocks are successively created, confirmed, and connected in chronological order like this, the database is called a block chain (Figure). The block chain serves as a time stamper, as well as a transaction

Figure **Block chain structure**



ledger. Changing the transaction details retrospectively is practically impossible because of the enormous amount of work required to recalculate the proof-of-work contained in each block. This structure supports transaction irreversibility and prevention of double spending, which are essential elements in practical application of a virtual currency.

Taking advantage of human desire

The incentive for taking part in the calculation competition is the Bitcoin reward. Every time the competition takes place, a certain amount of Bitcoins (currently, 25 BTC) are newly issued and awarded to the winner together with the commission charges for the transactions made within approximately the last 10 minutes. This is similar to mining for gold, and so the calculation competition is called “mining”.

The Bitcoin software continues to set competition problems, while adjusting the degree of difficulty so that a solution is derived approximately every 10 minutes. Anyone can participate in data mining, but in order to win, you must have the ability to throw the dice more often than anyone else in approximately 10-minute intervals. This means that participants with greater computing power have an advantage. Enhancing computing power requires substantial investment and power costs, but the winner gets the Bitcoin reward.

In a system without an issuing entity or administrator, it might seem possible for misconduct to occur if a user with overwhelming computing power were to appear or a group of users collude together. However, the value of Bitcoins is only secure if the Bitcoin economy is sound, and it makes no sense for users to bring the system down by committing fraud.

Of course, appropriate technology to prevent fraud is provided, including robust public key encryption and digital signature technologies, and a ledger system that makes it possible to verify the integrity of all transactions. On top of that, making human desire the driving force behind the entire system through the process of mining and block chain technology, and using it to ensure soundness as well, is a truly clever idea.

In distributed networks, the problem of forming a correct consensus without being misled by false information is known as the Byzantine Generals Problem (details on pp. 8–9), and Bitcoin can be said to be an example of attempting to solve that difficult problem through block chain system design.

Giving authenticity to electronic information

By accumulating electronically recorded events to create chronicles called blocks, as described above, block chain technology has made it impossible to corrupt information. The technology has succeeded in giving authenticity to electronic information, which had been considered almost impossible. Furthermore, the technology has a time stamping function and so can prove the chronology of events.

These characteristics make block chain technology applicable not only to community currency systems but also to public application/notification systems and to social information infrastructure that handles official documents. This technology has the potential to bring about major changes in society as a means of proving the genuineness of records, the grounds for chronological priority, transfer of ownership, and so on, in the cyber world.

(Written by: Akiko Seki)

Shigeichiro Yamasaki

Professor, Department of Information and Computer Sciences, Faculty of Humanity-Oriented Science and Engineering, Kinki University. Areas of expertise include mobile agents and public key infrastructure. Currently researching the application of block chain technology as a social information infrastructure.

What is the Byzantine Generals Problem?

A solution was vital to Bitcoin becoming a currency

Fraudulent use of virtual currency and the Byzantine Generals Problem

For Bitcoin to be usable as a virtual currency, fraud such as falsification of transaction details and double spending had to be prevented. This kind of fraud resembles a problem known as the Byzantine Generals Problem, which is a famous problem in distributed algorithm studies.

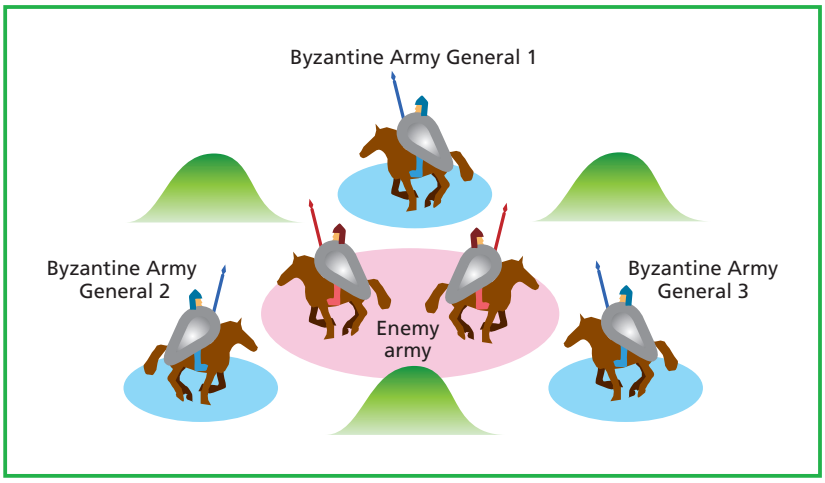
The Byzantine Generals Problem is a problem involving reliability in distributed systems devised by mathematician Dr. Leslie Lamport, winner of the 2013 Turing Award [1]. Dr. Lamport is well known as the author of LaTeX (a macro-package for preparing research papers for use with the electronic typesetting system TeX), but his area of expertise as a researcher is distributed algorithms in computer science.

The setting for the Byzantine Generals Problem is a battlefield where generals of the Byzantine Empire, each commanding their own unit, encircle an enemy (Figure 1). Each unit is separated from the others and can communicate only by sending messengers to each other. The battle can be won if all of the generals give the order to launch an attack simultaneously, but will be lost if only some of the units attack. In other words, the generals must all agree whether to attack or retreat. However, among the generals, there may be traitors who have switched allegiance to the enemy. When a traitor receives a proposal to attack from another general, he might change it to a proposal to retreat and pass it on to a different general. This could mean that some generals will receive orders to both attack and retreat. The worst-case scenario is that just some units will start to attack, and the battle will be lost.

In Figure 2-A, a general proposing attack (or retreat) sends that proposal to the other generals. The generals receiving the proposal transmit it to the other general. However, if General 2 is a traitor, he changes attack to retreat (or retreat to attack) before sending the message to General 3. In this case, General 3 does not know whether the original proposal was to attack or retreat. A scenario like Figure 2-B can also be imagined, in which the general who proposes attack (or retreat) is a traitor. In this case, he sends different messages of attack or retreat to different generals.

Thus, the Byzantine Generals Problem is a problem of devising a method that enables honest generals (that is, not traitors) to unanimously agree to attack or retreat, or in other words, a method that guides the generals to the correct consensus. Research conducted by Dr. Lamport and his team showed that, when there are N traitorous generals, the decision of the honest generals can agree if the number of honest generals is at least 2N + 1. Figure 3 shows a situation where there is one traitor among four generals.

Figure 1 **Byzantine army surrounding an enemy army**



The challenge of fault-tolerant distributed systems

Dr. Lamport viewed this Byzantine Generals Problem as a consensus problem in a fault-tolerant distributed system. Here, "distributed system" means a system in which multiple computers work together to carry out processing and storing that could not be done by a single computer. The currently topical cloud computing is simply a form of distributed system. In this context, "consensus" means that the same value is held by multiple computers.

You might think it sufficient to simply send the value you want agreed on to the other computers, but computers fail, and when there are multiple computers, the number of computers that may fail increases. Failure can be dealt with if the computer stops working, but if it continues to operate and starts communicating or processing erroneously, it becomes an extremely troublesome problem. Basically, the Byzantine Generals Problem involves finding a method and conditions for multiple normal computers having the same value, by likening computers that fail but continue operating erroneously to traitorous generals and the other normal computers

Figure 2 Three Byzantine generals (including one traitor)

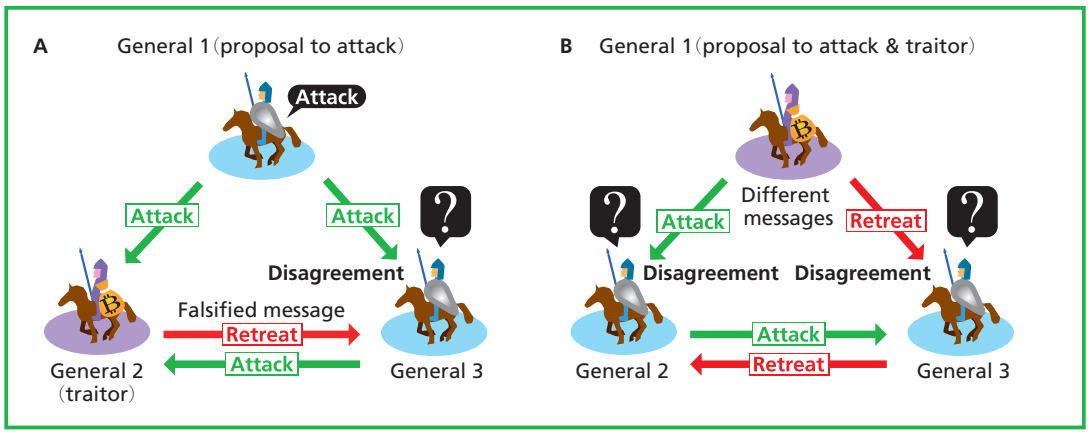
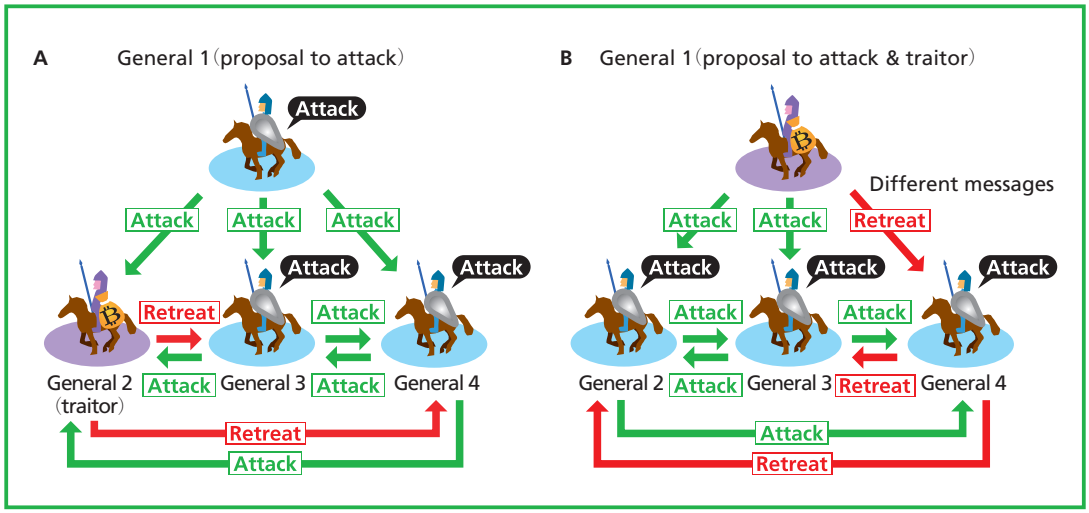


Figure 3 Four Byzantine generals (traitor N = 1, 4 ≥ 3N + 1)



to honest generals.

The Byzantine Generals Problem is a popular topic that usually comes up in textbooks on distributed systems because the problem corresponds to typical faults in real distributed systems. When failure causes unpredictable faults, it is sometimes called a Byzantine failure, and this is the most troublesome example of computer failure.

Bitcoin would not exist without a solution to this problem

Regarding the relationship between the Byzantine Generals Problem and Bitcoin, falsification of transactions and double spending is comparable to traitorous generals in the Byzantine Generals Problem. In fact, Bitcoin would not exist as a currency without a solution to the Byzantine Generals Problem. Bitcoin has introduced a mechanism that detects and inhibits fraud (see pp. 6–7). This mechanism requires an enormous amount of calculation work to create a 10-minute transaction record called a "block chain", and provides an incentive to create these records by transferring Bitcoins to the fastest person to calculate the block chain. The mechanism is also designed so that an enormous amount of calculation work is required to alter the block chain retrospectively, and the difficulty of changing transactions ensures Bitcoin's continuity as a virtual currency.

Looking at it from a different perspective, Bitcoin's block chain mechanism can be seen as a countermeasure for dishonest generals in the Byzantine Generals Problem, and may lead to new solutions to this problem in situations limited to virtual currency transactions.

Incidentally, Dr. Lamport is a researcher with a sense of humor, and it was that sense of humor that led him to come up the Byzantine generals as an example. As well as the Byzantine Generals Problem, he has devised a distributed consensus system called the Paxos algorithm, which he sets in a parliament on an ancient Greek island. Whereas the Byzantine Generals Problem uses traitorous generals, the Paxos algorithm uses members returning home partway through a parliament as an analogy for computer failure and recovery. Dr. Lamport submitted his first paper on this algorithm [2] to an academic journal in 1990, but it was left unpublished—perhaps because the journal's editor assumed that it was a joke due to the humorous explanation of the algorithm using an ancient Greek parliament as an example. It was eventually published in the journal in 1998—eight years after its submission!

The Paxos algorithm has subsequently been used as a core technology, such as the updating of replicated data, in most commercial cloud computing services. It may not be long before the Paxos algorithm reaches the same level of fame as the Byzantine Generals Problem.

(Written by: Ichiro Satoh [Professor, Information Systems Architecture Science Research Division, National Institute of Informatics])

References

[1] Leslie Lamport, Robert Shostak, Marshall Pease: "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol.4, No.3, pp.382-401, 1982.

[2] Leslie Lamport: "The part-time parliament", ACM Transactions on Computer Systems, Vol.16, No.2, pp.133-169, 1998.

News 1 Open House 2015

Excitement over Running Fire of Research Presentation Open Forum 2015 also held

Open House 2015 was held on June 12 and 13 with the aim of introducing NII's projects and research to a wide range of people, including the general public and researchers.

Director General Masaru Kitsuregawa gave an activity report titled "Towards a New SINET: Upgrading to 100 Gbps Nationwide/With US: e-infrastructure envisioned by NII". He talked about the significance of the upgrade of the Science Information Network (SINET) that NII provides to universities and research institutions to 100 Gbps next spring, and the influence that it will have on such prime examples as the shift to cloud computing and open science. The keynote speech was given by Tsuguhiko Kadokawa, the chairman of Kadokawa Corporation.

A new initiative this year was "Running Fire of Research Presentation at NII" (see photo). One hundred studies were presented by 10 researchers, who each presented 10 studies in 7.5 minutes. In the Demos/Poster Exhibition, researchers exhibited some of their own work and answered questions from visitors. Efforts were also made to reach out to younger generations. An Informatics Workshop aimed at elementary and junior high school students was held for the first time, and there was also a "Science Life Café for Female High School Students" and "Research Lesson for High School Students" for students of Toyama High School. Next year's NII Open House will be held on May 27 and 28.

On June 11 and 12, the Academic Information Infrastructure Open Forum 2015 was also held. The theme was "Academic Information Infrastructure for Open Science", and it was aimed at teaching staff, security managers, and IT vendors targeting science. NII is promoting the development and expansion of academic information infrastructure vital to its research and educational activities. Discussions included the question of what is required of academic information infrastructure in terms of supporting open science, something inspiring high hopes in universities and other academic circles.

News 2 Start of this fiscal year's NII Public Lectures

First theme: speech synthesis technology

This fiscal year's NII Public Lectures have begun, with the first lecture held on July 29. The subject this year is "The Forefront of Informatics". In six lectures, the latest research findings will be explained in a straightforward manner using topics closely related to daily life.

The first lecture was titled "Talking Computers: The Present and Future of Speech Synthesis Technology", and Associate Professor Junichi Yamagishi (Digital Content and Media Sciences Research Division) who specializes in speech information processing gave a scientific explanation of speech synthesis, which has been a subject of research since the 1950s. A video of the lecture will be available on the NII website from mid-November.

The second lecture was held on August 20. It was titled "Creating Fast and Efficient Supercomputers: Pursuit of Low-Latency Network Topology" and given by Ikki Fujiwara, Associate Professor by Special Appointment (Information Systems Architecture Science Research Division). The lecture schedule can be found on the back cover, and details and applications can be found on the public lecture page of the NII website (http://www.nii.ac.jp/event/shimin/).

News 3 Exchanging ideas on big data

Industry–Government–Academia Collaboration Prep School

The 3rd NII Industry–Government–Academia Collaboration Prep School was held on July 22. These are open lectures geared towards industry, providing an opportunity for NII researchers and people in business and local government to meet and exchange ideas.

The subject was "What Should Be Understood Before Launching Big Data Initiatives?" In the first half, Professor Takeaki Uno (Principles of Informatics Research Division), specializing in data mining and algorithm research, explained the current state of big data and gave an overview of its handling. He also talked about the importance of collaboration between people possessing data analysis technology and on-site staff in finding business opportunities because, with the development of infrastructure, people often do not know what to do with the enormous amounts of information that they are acquiring. In the second half, participants were joined by young Assistant Professors Kazunori Sakamoto (Information Systems Architecture Science Research Division) and Takuya Akiba (Principles of Informatics Research Division) as they shared and discussed situations and challenges involving big data in their work.

The next lecture will be held on October 13 and led by Professor Isao Echizen (Digital Content and Media Sciences Research Division), who is researching measures against privacy infringement. Details, including how to participate, will be given on the NII website.

Flash

NII/NINJAL Joint Research 2015 Public seminar

Held on July 24. Part of joint research with the National Institute for Japanese Language and Linguistics (NINJAL) handled by the Center for Dataset Sharing and Collaborative Research, which was established this fiscal year. On the subject of "Problems in Developing Language Resources: Focusing on Rights Issues", initiatives by both organizations were explained and a general discussion with participants was held.

ERATO Festival Season II

Held on August 3 and 4. Presentation of research by the "JST ERATO Kawarabayashi Large Graph Project" directed by Professor Kenichi Kawarabayashi (Principles of Informatics Research Division). The presentation was limited to research findings selected this year in a meeting of senior management, and a total of 22 presentations and discussions were held over the two-day period.

Topics

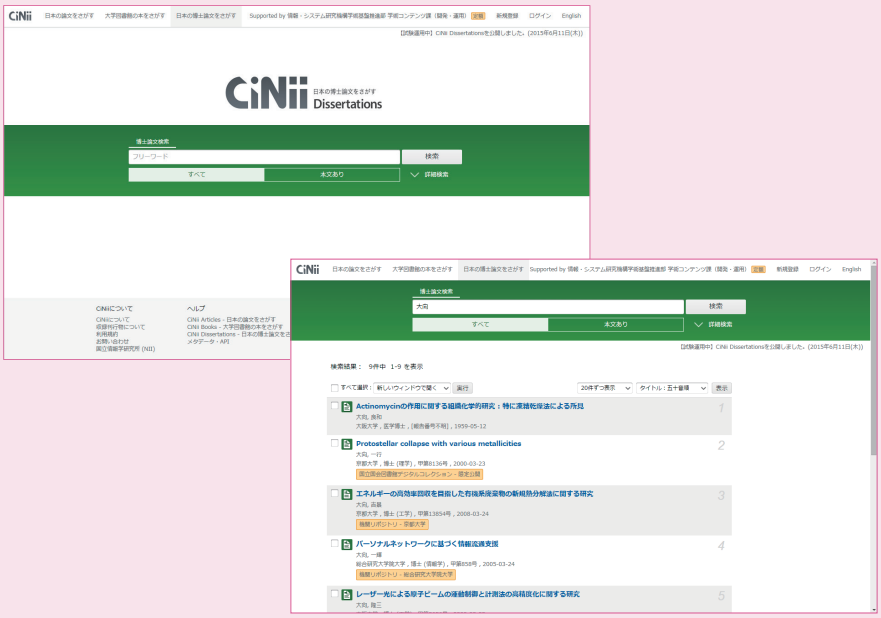
Trial Operation of CiNii Dissertations Commences Centralized retrieval of Japanese doctoral dissertations

Nii has developed a service called CiNii Dissertations that commenced trial operation in June. This is the only service in Japan capable of centralized, comprehensive retrieval of Japanese doctoral dissertations, as well as full-text display of electronically published dissertations. The service will be officially launched in October of this year. CiNii Dissertations (http://ci.nii.ac.jp/d/?l=en) is available for anyone to use.

The searchable dissertation data consist of approximately 570,000 Japanese dissertations published since September 1923 and held by the National Diet Library; approximately 130,000 dissertations (including digitized full-text data) in the National Diet Library Digital Collection, which the library received between 1991 and 2000 and digitized; and approximately 130,000 items of stored data from the institutional repositories of various universities.

Up until now, it was necessary to search each of the abovementioned collections separately in order to find dissertations. CiNii Dissertations makes it possible to conduct a comprehensive search of all the collections at once. Furthermore, if the full text has been published electronically, it can be read with just a few clicks. CiNii Dissertations provides a one-stop service that greatly improves the ease with which users can retrieve dissertations and read full texts.

CiNii Dissertations follows on from CiNii Articles (CiNii's article retrieval service) and CiNii Books (CiNii's service for retrieving materials from university libraries) to become the third service offered by CiNii, a database service for academic information retrieval provided by NII. All three services employ a common search interface that has been perfected over the decade since the start of CiNii's services.



As materials of high academic value describing the latest research findings, doctoral dissertations have been collected by the National Diet Library and university libraries via degree-granting institutions. With the revision of rules on academic degrees in March 2013, it became a general rule for doctoral dissertations to be published on the Internet, and dissertations are now being made available through institutional repositories, which are platforms for universities and other degree-granting institutions to transmit their research findings to society.

▶ Development of ERDB-JP
A service for sharing electronic resources published in Japan

The Council for Promotion of Cooperation between University Libraries and the National Institute of Informatics, which comprises NII and the Japanese Coordinating Committee for University Libraries, has developed ERDB-JP (Electronic Resources Database-JAPAN). This is a service for sharing electronic resources published in Japan that will be built by universities and publishers working together. The Council began recruiting partners (data-generating organizations) in June.

Using ERDB-JP to compile an accurate database of electronic journal information published in Japan will make it possible to create appropriate links to full-text articles from CiNii and university library retrieval services.

The Council is currently targeting university libraries as partners, but intends to expand this to include publishers and further improve the quality of data in the future.

SNS

"Hey, this is great!"
Hottest articles on Facebook and Twitter (May–July 2015)

National Institute of Informatics, NII (official) Facebook
www.facebook.com/jouhouken/

Start of trial operation of CiNii Dissertations, a new service and the only one in Japan capable of centralized, comprehensive retrieval of Japanese doctoral dissertations
(6/24/2015)

National Institute of Informatics, NII (official) Twitter
@jouhouken

[NII NEWS] Start of trial operation of CiNii Dissertations, a new service and the only one in Japan capable of centralized, comprehensive retrieval of Japanese doctoral dissertations
(6/23/2015)

Bit on Twitter! Twitter
@NII_Bit

Assistant Professor Takuya Akiba interviewed for educational magazine. Reminisced about his high school and university days when he achieved a string of excellent results in national and international programming contests. Asked whether he would take part in any more programming contests, he said, "My battleground has changed. Now it's algorithm research!" (5/19/2015)

Essay

Finance, Information, and Virtual Currency

Akihiro Hada
Visiting Professor, National Institute of Informatics／General Manager, Technology Research & Innovation, Nihon Unisys, Ltd.

The financial industry has been called an equipment-intensive industry. The primary equipment is related to ICT. This equipment constitutes "back systems", which have existed since the beginning to receive transaction data and prepare financial statements, as well as channels between markets and customers, business/risk management and marketing support, and the hubs connecting these. Up until the 1970s, real economies and financial markets were close together, and the important thing was remote, instant, mass handling of payments and cash transactions. In other words, the information handled in finance possessed "confidentiality" associated with trading and financing, and was acted upon by the "gravity" of the real economy. "Equipment" was something that electronically processed "data", which were divorced from this confidentiality and gravity.

Subsequently, following the securitization of real assets and liberalization of financial prices, business fields, product design, and foreign transactions that began with reform of the London Stock Exchange, financial markets have grown to be many times greater than real economies. ICT has contributed to securitization and liberalization by removing the constraints of space and time from the exchange of financial transaction data by networking equipment on a global scale, and by advancing financial engineering aimed originally at hedging risks related to information. In addition, the high speed and mathematical difficulty of data processing have produced "pseudo-confidentiality".

The nature of financial instruments, which are simply amounts of money and attached conditions, and the demand for seamless, realtime processing, have meant that financial transactions have generally become increasingly automated and self-service. ICT has also served to strengthen asset management and new product development capabilities, and back systems that are robust and flexible have encouraged core functions provided by financial systems to become decentralized and independent of financial institutions.

This means that, like e-business in other industries, newcomers are appearing and bringing new business models using ICT in marginal areas. Recently, much attention has been paid to virtual currencies, personal asset management, and other FinTech innovations geared to the expectations of users of the financial services started by these new businesses, which are different from the expectations of conventional users.

Marginal virtual currencies may become mainstream in the future. In that event, will various time and space constraints be eliminated and the core of global financial transactions be shifted to virtual space while maintaining excess liquidity? Instead, themes in informatics would increase and it would be more interesting if, with the emergence of new manufacturing/distribution using the IoT (Internet of Things) and CPS (cyber-physical systems), "pseudo-gravity" were produced and a new real economy were formed with new business management goals that differed from the conventional return-on-investment approach.

Future Schedule

October 13 | 4th NII Industry–Government–Academia Collaboration Prep School, "Informatics, Manufacturing, and Regional Revitalization: From R&D of Privacy Visor to Practical Application in Society" (Professor Isao Echizen, Digital Content and Media Sciences Research Division, and others)

October 21 | 2nd SPARC Japan Seminar 2015 (Open Access Summit 2015), "Towards the New Paradigm of Science and Scholarly Communication Environment: e-Science, Research Data Sharing, and Research Data Infrastructures" (Host)

October 22 | 3rd NII Public Lecture, "Easier CG Production: Technique Combining Algorithm and UI" (Digital Content and Media Sciences Research Division, Assistant Professor Kenshi Takayama)

November 10–12 | 17th Library Fair & Forum (Sponsor/Exhibitor)

November 26 | 4th NII Public Lecture, "What Do We Know?—Ontologies and Corpus Incorporating Implicit Knowledge" (Ai Kawazoe, Associate Professor by Special Appointment, Research Center for Community Knowledge)

November 29 | Inter-University Research Institute Corporation Symposium (Exhibitor)

December 2–4 | Annual Meeting of the Academic Exchange for Information Environment and Strategy (Exhibitor)

Notes on cover illustration The motive for this scene played out by retro cash registers and humorous robots is to convey a view of the dream-inspiring world of virtual currency that could be provided by machines (= technology) in the future.

Weaving Information into Knowledge
NII

National Institute of Informatics News [NII Today]
No. 55 Oct. 2015
[This English language edition NII Today corresponds to No. 69 of the Japanese edition.]
Published by National Institute of Informatics, Research Organization of Information and Systems
Address | National Center of Sciences 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430
Publisher | Masaru Kitsuregawa **Editorial Supervisor** | Ichiro Satoh
Cover illustration | Toshiya Shirotani **Copy Editor** | Madoka Tainaka
Production | MATZDA OFFICE CO., LTD., Athena Brains Inc.
Contact | Publicity Team, Planning Division, General Affairs Department
TEL | +81-3-4212-2164 **FAX** | +81-3-4212-2150 **E-mail** | kouhou@nii.ac.jp

Bit (NII Character)

http://www.nii.ac.jp/en/about/publications/today/