November, 2018
Payment and Settlement Systems Department
and Institute for Monetary and Economic Studies
Bank of Japan

Summary of Discussion of the FinTech Study Group

The Bank of Japan set up an interdisciplinary study group on FinTech (hereafter, "FinTech Study Group") in 2016. The FinTech Study Group was comprised of professionals in the fields of law, economics, and informatics. It met a total of five times to discuss the impact of FinTech on the financial sector (Secretariat: The Payment and Settlement Systems Department and the Institute for Monetary and Economic Studies).

The financial sector is undergoing a technological revolution called "FinTech" in which information technology (IT) is used to create and develop new financial services. While the financial sector has long embraced IT, the recent FinTech revolutions has the potential to bring about fundamental changes to the financial sector through the use of distributed ledger technologies (DLTs), the emergence of cryptocurrencies embodying such technologies, diversification of financial service providers, or expansion of financial access via smartphones and other types of mobile devices.

The use of information technologies for payments and other financial services has long been discussed, and studied from the legal, economics and informatics viewpoints. However, the development of new technologies such as DLTs has the potential to bring about fundamental changes to the financial system, and has sparked new debate.

The FinTech Study Group discussed issues, from an academic standpoint, that need to be addressed for the practical use of these advanced technologies for financial sector; i.e., (1) economic analysis of FinTech's impact on the financial system and central bank policy, (2) design of legal and regulatory frameworks, and (3) the robustness of these technologies.

This paper, prepared by the secretariat of the FinTech Study Group, summarizes the main points discussed at the Group's final meeting held on June 12, 2017. Personal opinions expressed in this paper are those of the members of the FinTech Study Group, and do not necessarily represent the official views of the member’s organization or the Bank of Japan.

Member of FinTech Study Group

-- The titles are those at the time of the Study Group

Hitoshi Okada	Associate Professor, Information and Society Research Division, National Institute of Informatics
Yoshihiro Kataoka	Lawyer, Partner, Kataoka & Kobayashi
Akira Kamo	Associate Professor, Graduate Schools for Law and Politics, The University of Tokyo
Yukinobu Kitamura	Professor, Research Division of Economic Measurement and Statistics, Research Centre for Information and Statistics of Social Science, Institute of Economic Research, Hitotsubashi University
Shouichirou Kozuka	Professor of Law, Gakushuin University
Yutaka Fujiki	Professor, Faculty of Commerce, Chuo University
Masaki Honda	Professor, Faculty of Economics, Tokyo International University
Kanta Matsuura	Professor, 3rd Department, Institute of Industrial Science, The University of Tokyo
Shin'ichiro Matsuo	Research Affiliate, Director's Liaison for Financial Cryptography, Director's Office, MIT Media Lab
Tsutomu Matsumoto	Professor, Faculty of Environment and Information Sciences Division of Social Environment and Information, Yokohama National University
Noriyuki Yanagawa	Professor, Graduate School of Economics, The University of Tokyo
Secretariat	The Payment and Settlement Systems Department and the Institute for Monetary and Economic Studies, Bank of Japan

[Overview]

Discussions at the FinTech Study Group focused mainly on distributed network systems in comparison to centralized network systems. The Study Group discussed such issues as: (1) theoretical analysis of centralized and distributed models, (2) consensus algorithms, (3) the legal nature of cryptocurrency, (4) differences between digital currencies by different issuers, and (5) information security aspects of distributed network systems.

With the emergence of FinTech, innovative payment services have been introduced. While new payment services generally develop in a distributed manner, such financial services also have "network externalities", often resulting in distributed network systems gradually shifting to centralized network systems. On the other hand, payment and settlement systems are composed of both centralized and distributed aspects. Such characteristics of payment and settlement systems could result in facilitating a switch from distributed system to centralized one, and from centralized system to distributed one. From another viewpoint, whether distributed or centralized system is favored may differ on each "layer" of the payment and settlement systems; for example, the "technology layer" may tend towards distributed system while the “service layer” may tend towards centralized system.

DLT requires a verification process. There are two models regarding this verification process: (1) consortium, in which the verification participants are limited, and (2) public, in which the verification participants are not limited. For each model, there are issues that need to be considered to ensure sustainability. With consortium-type verification, the issue is how to secure a sufficient number of verification participants over the long term. With public−type verification, the issue is the excessive maintenance cost participants are forced to bear if there are security vulnerabilities in widely-used technologies.

At present, it is difficult to consider private cryptocurrencies (e.g., Bitcoin) as "money" from a private law perspective. In determining the possible legal protection of the holder of a cryptocurrency, it would be an issue whether the holder’s right is a real right, a claim, or some other type of right. Cryptocurrencies may have characteristics that give rise to a real right since it has a generally assertable property value. However, it is necessary to consider whether adequate protection can be achieved by taking such a real right approach. Alternatively, a consensus algorithm could be considered as a kind of "agreement" among participants, but it is necessary to further determine what rights and obligations such "agreements" give rise to.

Digital currencies can be categorized into three types in light of their issuers: (1) no issuer, (2) private entities, and (3) central banks. For each type, it is necessary to consider the following: (1) the *de facto* concentration and centralization of no issuer-type digital currencies, (2) how to ensure suitability of the issuer (if applicable), and (3) how to ensure universal access.

Some people argue that "distributed systems are secure", or that "distributed systems are less expensive than centralized systems". This, however, may not necessarily be the case. In a distributed system, the cost of system security is passed on to each node. Therefore, it is necessary to evaluate the cost burden of the system as a whole. In addition, the security cost of the distributed systems needs to be compared to the same security level cost of the centralized systems.

1. Scope of Discussion

The use of new technologies is not a new phenomenon in the financial sector. The financial sector has long applied and utilized IT for the provision of financial services. The growing interest in "FinTech" reflects the development of distributed network systems which have different characteristics from existing centralized systems.

Members of the FinTech Study Group discussed how distributed network systems differ from existing centralized networks, especially focusing on: (1) theoretical analysis of centralized and distributed models, (2) consensus algorithms, (3) the legal nature of cryptocurrency, (4) differences between digital currencies by different issuers, and (5) information security aspects of distributed networks.

2. Theoretical analysis of centralized and distributed models

New FinTech services generally develop in a distributed manner. In the early stage of FinTech markets, many startup companies enter the market and provide various kinds of services. However, in the process of seeking efficiency, the services often tend toward centralization. In particular, with regard to payment and settlement systems, centralization tends to dominate due to the benefits of scale and networking.

In that sense, whether a certain payment and settlement system is in a distributed or centralized state might be considered as simply reflecting the development stage of the system. From another viewpoint, it could reflect a "philosophical" difference as to whether a specific payment and settlement system migrates towards distributed system or centralized system. For example, some argue that Bitcoin was designed to avoid being controlled by a centralized authority and is supported by those who embrace similar ideologies.

While centralization may be natural from an efficiency perspective, some participants may want to avoid being centrally managed. Therefore, participants seeking distributed structure and those seeking centralized efficiency may arrive at a tense compromise situation, which could lead to the coexistence of a distributed and centralized structure.

Payment and settlement systems tend to be composed of both centralized and distributed aspects. Settlement tends to be executed in a centralized manner in light of its network effect. On the other hand, payment can be affected by the agreement between the payer and the payee, and thus is executed in a distributed manner. Hence, "payment and settlement" comprises centralized "settlement" and distributed "payment". Such characteristics of payment and settlement systems could result in facilitating a switch from distributed system to centralized one and from centralized system to distributed one.

It is also important to keep in mind that each "layer" of the payment and settlement system may differ as regards to whether distributed or centralized system is favored. For example, the "technology layer" may tend towards distributed system while the “service layer” may tend towards centralized system.

Those who exploit new technologies or service models can mainly financially benefit in one of two ways: (1) by obtaining rights to monopolize such technologies or service models (e.g. patents), or (2) by obtaining first-mover advantages through the broad use of such technologies and service models. The most suited way to obtain value may differ depending on the “layer”. For example, in relation to DLT, those who build DLT platforms obtain value by exploiting as many users as possible. On the other hand, those who develop service models using DLT platforms obtain value by monopolizing the rights.

3. "Public goods" vs. "club goods" in consensus algorithms of DLT

There are two types of DLTs with respect to verification work (mining) needed to confirm the transaction history: (1) public (such as Bitcoin), which has an unspecified number of miners (those who verify the transaction) and (2) consortium (or private), which has a limited number of miners. In a public-type ledger, a consensus algorithm based on the expenditure of a large amount of resources (such as Proof of Work in Bitcoin) is used, assuming the lack of mutual trust among verification participants. In a consortium-type ledger, a consensus algorithm could incorporate a centralized element (such as a verification process based on a certain proportion of participants) on the premise of a certain degree of trust among the participants.

A public consensus algorithm can be regarded as a "public good" with zero exclusivity in that anyone can participate in the verification work. On the other hand, a consortium consensus algorithm can be viewed as a "club good" with a limited number of participants involved in the verification work. However, Bitcoin, which uses a public-type ledger, relies on private incentives such as remuneration for mining to ensure verification is accomplished. In that regard, it can eliminate consumption by those that do not provide remuneration, and thus cannot be economically regarded as a "public good". Rather, it is a mechanism designed to provide public goods and services using personal incentives.

An important requirement for currencies is that they are sustainable in the long term. Taking Bitcoin as an example, a mechanism must be established to guarantee safety in the long term and to ensure that the verification work continues. This means that, as mining fees decrease, two issues need to be addressed: (1) how to maintain incentives for Bitcoin mining, and (2) how to construct a governance structure that eliminates excessive influence of specific users.

If a service infrastructure is developed without considering future security issues and spreads widely among the public, it will impose huge maintenance costs as well as security vulnerabilities. This is illustrated by the need to continually update the operating systems of personal computers. The same could be the case for DLTs; even if there are issues with the design, system users will have no option but to continue using the system and pay excessive maintenance costs, if the system becomes widely used due to first mover advantages. System users should be mindful that different system designs can impact the security levels that may be achieved.

4. Legal nature of cryptocurrency

It is necessary to consider the legal nature of a cryptocurrency depending on its design and characteristics. Legal aspects of a cryptocurrency not only involve private law issues that deal with the relations between individuals or institutions, but also regulatory issues, such as those introduced in Japan for cryptocurrency exchanges.

As regards private law issues, for instance, it is difficult to say that Bitcoin currently has general acceptability and is legally regarded as "money". Therefore, it seems natural to consider a delivery of a Bitcoin merely as a fulfilment of an obligation to transfer Bitcoin, rather than a fulfilment of a monetary obligation.

One hotly debated topic is whether a holder of a cryptocurrency is entitled to a real right, a claim, or another right. Some argue that cryptocurrency has characteristics that give rise to a real right, since it has a generally assertable property value. It should be noted, however, that the transfer of a cryptocurrency is realized not by the transfer of the value itself but by the disappearance and emergence of value. Such nature of cryptocurrency is similar to that of a means of payment based on claims. In considering the legal nature of cryptocurrency, it is necessary to consider whether desirable protection would be achieved by granting a real right to the holder of a cryptocurrency whereby eliminating competing rights towards the cryptocurrency. In addition, granting a real right could lead to a possible cost increase for the entire payment system. Further, from the viewpoint of safe conduct of transactions, a receiver of a cryptocurrency would be more strongly protected if the receiver can obtain the cryptocurrency free from past payment histories.

Cryptocurrencies differ from a means of payment based on claims in that a claim towards a specific person cannot be clearly conceived. It may be possible to take a view that some sort of "agreement" exists among network participants focusing on the consensus algorithm. For example, payers and payees using Bitcoin may potentially assume an "agreement" amongst themselves. However, an "agreement" in a distributed network may be a weak one, such as merely agreeing to use an existing protocol. The issue thus becomes whether such an agreement can be regarded as a legal agreement, and what kinds of rights and obligations it gives rise to.

5. "Distributed" and "centralized" system from the perspective of digital currency

Issuance of "digital currency" (here, not limited to cryptocurrency premised on the definition in the Payment Services Act in Japan) has become possible due to the advancement of IT and it has become widely discussed in various form. Digital currencies can be categorized into three types depending on the issuer: (1) no issuer, (2) a private entity and (3) a central bank. The no issuer type (i.e., distributed digital currencies) maintains trust by operating in accordance with predetermined rules such as fixing the maximum issuance amount. Digital currencies issued by a private entity or a central bank gain trust by having a central administrator (i.e. the private entity or the central bank) who controls the currency supply. Issuance of hybrid-type digital currencies has also been proposed whereby a hierarchical structure is adopted; i.e., the digital currencies issued via intermediaries situated between the central bank and the users. RSCoin, proposed by academics at the London University, is an example of this hybrid model.

One of the big concerns associated with privately issued digital currencies is trust, or the lack thereof, towards the issuer. For example, when a private entity issues currency to meet its own funding needs, the issuer may have an incentive to control the value and issuance timing for its own benefit. Since the incentive for seigniorage is substantial and the issuer faces difficulty in maintaining trust, there has hardly been any case in history where a currency issued by a private entity was sustainable when the issuer had the power to arbitrarily control the supply volume.

As for distributed digital currencies, there may be difficulty to maintain the pretext that no issuer exists, if the network becomes more concentrated and centralized.

Bitcoin has an upper issuance limit and is designed to be difficult to arbitrarily control the issuance supply. Such issuance limit is one of the sources for people to believe that Bitcoin has value. On the other hand, such limit makes it difficult to maintain a stable value against fluctuations in demand and speculative behavior, and thus to use as a unit of account. Ultimately, only a centralized authority, such as a central bank, could appropriately issue currency by flexibly changing the supply amount in light of overall price movements. Indeed, if the central bank itself cannot be trusted, there could be cases where a currency issued by a private company might become more reliable.

In case of central bank issued digital currencies, one issue that may need to be considered is how to secure universal access to central bank money during the transition from cash to the digital currency. For example, to what extent should measures be taken to distribute devices to hold digital currencies as banks withdraw from providing cash supply services in rural areas? Examples in Scandinavian countries where the cashless society is progressing may be useful in considering such practical issues.

6. "Distributed" and "centralized" network from the perspective of security

It is inappropriate to conclude that a system is secure merely because it uses a distributed network. In a distributed system, each node is individually responsible to take security measures. If most of the nodes use the same software as in the case of Bitcoin, a malfunctioning of the software can have a significant impact.

Some people argue that distributed systems are less costly than centralized systems, but a cost comparison should be conducted between systems with similar security levels. It is unclear whether a distributed system is less costly to achieve the same security level. Further, when evaluating costs, it is necessary to take into consideration the cost of recovery when a risk materializes, in addition to the cost for system development and maintenance.

Use of open source software has become popular in order to reduce system development costs. However, there is concern as to whether necessary maintenance could be accomplished. In open source software, engineers or academics are not paid remuneration for the systems’ appropriate development and maintenance. Users have to accept the possibility that the system will not be adequately and continuously maintained, and take into account such risks and costs.

In terms of security, since hackers have a stronger incentive to attack a system as the number of users increases, it is necessary to strengthen the system's security as it expands. However, users may not have sufficient knowledge of the security concerns, and thus may be reluctant to pay the cost to heighten the security level.

Provision of financial services through FinTech involves the handling of abundant personal information such as user identity and purchase history. Not only leakage of personal information but also the issue of the collecting and managing of personal information by specific powerful companies, need to be discussed from a privacy perspective. Further, the security requirement differs between a blockchain as infrastructure and the application level functioning on a blockchain such as a cryptocurrency. Thus, the issue of privacy needs to be considered separately for each layer.