The Impact of Central Bank Digital Currency: From a Functional Perspective

Soichiro Takagi
(Associate Professor, Center for Global Communications, International University of Japan)
The Impact of Central Bank Digital Currency: From a Functional Perspective

Soichiro Takagi
(Associate Professor, Center for Global Communications, International University of Japan)

Abstract
There is growing attention on “Blockchain” as part of a key technological revolution to change a wide spectrum of the economy and business. Blockchain, also known as a “Distributed Ledger”, was initially created as a platform technology to enable Bitcoin. Bitcoin and similar digital currencies are issued and maintained by anonymous participants around the world. However, as a reaction to digital currency in the private sector such as Bitcoin, there is a growing concern among central banks about their own issuance of digital currency. Central banks in countries such as the United Kingdom, Sweden, Canada, and Cambodia are studying digital currency which is issued by central banks. If certain central banks issue their own digital currencies based on the blockchain technology, this would have a wide impact on national and world economies and their financial systems. The purpose of this paper is to provide a comprehensive set of topics and points to discuss Central Bank Digital Currency (CBDC) by providing the technological and functional features of blockchain technology and its potential impact on the economy and society regarding the implementation of CBDC.

Keyword
Central Bank Digital Currency, Bitcoin, Blockchain, Function, Financial System
1. An Overview of Blockchain Technology

1.1. Development of Blockchain

Blockchain is a new computing platform, initially created to realize the crypto-currency, “Bitcoin”. Bitcoin first appeared in a white paper in 2008 authored by a person or persons using the pseudonym “Satoshi-Nakamoto”, which is still stimulating the discussion on who is the real author. No matter who the author is, and no matter how it initially looked dubious, there is a growing perception that blockchain, the technology behind Bitcoin, was the true innovation, particularly as a fundamental new technology for the economy and society. Blockchain is often discussed in the context of financial innovation and “FinTech”. However, blockchain is a technology which can be adopted for more general purposes, and there is a growing expectation of its uses from general record-keeping to its use in the Internet of Things.

Observing the disruptive nature of blockchain technology, the government of the UK (2015) stated that “Algorithms that enable the creation of distributed ledgers are powerful, disruptive innovations that could transform the delivery of public and private services and enhance productivity through a wide range of applications” (p.5). The paper discusses not only applying such technology in the private sector, but also utilizing the technology in the government sector. If blockchain is used widely, its impact will be enormous. For example, METI (2016) states that blockchain can affect industries worth 67 trillion JPY in total, and suggests blockchain can affect industrial structures.

Whereas the Internet constructed a network to exchange information with other information, blockchain constructs a network to exchange values across entities by decentralized infrastructure. When applied on a point card, for example, blockchain technology can create a network which is capable of managing the flow of values, such as the owner of the value, the amount of the value, and the transfer of the value from one entity to another.

Because blockchain is continuously being developed, there is no clear consensus on the exact definition of blockchain. Some examples of its definition include, “A list of validated blocks, each linking to its predecessor all the way to the genesis block” (Antonopoulos 2014, xix.), and “[…] Blockchain is the public ledger of all Bitcoin transactions that have ever been executed” (Swan 2015, x.). These definitions mostly reflect blockchain as the enabler of Bitcoin. The government of the UK (2015), however, focuses on the general use of blockchain and defines blockchain as follows: “A block chain is a type of database that takes a number of records and puts them in a block (rather like collating them onto a single sheet of paper)” (p.17). Blockchain is still in the initial development stage, but it is expected to be an infrastructural technology which is built on top of the Internet to provide a value-exchange platform for general purposes.

1.2. The Three Attributes of Blockchain Technology

Blockchain is under rapid development and evolution, and has multiple aspects, but three common attributes include the following. The first attribute is its anti-tampering element by connecting data. Blockchain creates a set of data, which is called a “Block” in every certain period of time, by collecting transaction data (for example, transferring a value from A to B) around the world. Blockchain then connects the block to the latest block previously generated. In the course of connecting blocks, an element (hashed data of a previous block header) is included in the next block, which makes it difficult for attackers to tamper with past transactions. Through this structure, blockchain realizes anti-tampering. The overall structure of a blockchain, as an example of Bitcoin, is shown in Figure 1.

1 The introduction of Blockchain is also available in Japanese by the author at Takagi (2016).
The second attribute of blockchain technology is how it connects entity and information assets. The owner of the value is identified by the hashed data of the owner’s public key, and the owner can use the value only if he or she can prove that they have the corresponding private key. When the owners use the value, they make a digital signature on the data which shows where the value comes from, and where it is going. By managing the “source” and “destination” of digital resources together, blockchain prevents the double spending of the asset and manages the transaction of the asset safely. The entity, as the owner of the asset, is usually a natural person or organization, but the definition of an entity can be expanded to devices, in the context of the Internet of Things.

The third attribute is blockchain’s peer-to-peer (P2P) element, which is the management of the data by many and unspecified computers. Instead of storing data in a certain server, distributed and unspecified computers share the data in the blockchain network. There is no need for a massive-scale computer to manage data, and the service can be continuously operated even if one part of the network is broken as long as the other participants’ computer is working. This structure has enabled Bitcoin to work for about 8 years without major downtime.
On the other hand, there is a risk of different versions of data coexisting if the data is stored in unspecified and distributed computers, and the data is updated simultaneously in different places (Figure 2). To avoid this disparity, a consensus mechanism is needed to make sure which is the correct version in this decentralized network. Bitcoin blockchain (the blockchain which is operated for Bitcoin) adopts a “Proof-of-work” algorithm. Simply put, proof-of-work allows the person (or computer) who employs the largest computing resource and becomes the first to create a new block, to add the new block to the latest blockchain. If multiple blocks compete at the same time, the blockchain which becomes the longest is considered the valid chain.

The important point here is that anonymous participants in the network contribute to creating a new block (including checking the transaction data). Their work is rewarded by coins in the network, such as Bitcoin. Through this system, blockchain enables the management of the system without any central control or managers. This attribute of organization is called a Decentralized Autonomous Organization (DAO).

1.3 Digital Currency

Bitcoin is the first and has been the most popular digital currency based on blockchain technology since its creation. Many articles have discussed the fluctuation of the price of the bitcoin, but recently its price has reached a historically high of one bitcoin equals US $1,533 on March 5th, 2017\(^2\). In addition, transactions, representing the remittances, or the ‘buying and selling’ of bitcoins, are also growing (Figure 3).

The supply of bitcoins is designed to have a cap up to 21,000,000 BTC. Every time transactions are composed in a “block” – averaging every ten minutes – a “reward” bitcoin is issued from nothing to miners (people who successfully composed a new block). The reward is halved every four years, and currently 12.5 BTC is issued for every block (every ten minutes). This “fixed” monetary policy of bitcoin is one of the reasons for the fluctuation of the bitcoin price\(^3\).

\(^2\) https://blockchain.info/ja/charts/market-price?timespan=all
\(^3\) Another reason would be massive transactions based on speculation around the world.
However, Bitcoin is not the only digital currency. After the birth of Bitcoin, various similar currencies which have a similar technological architecture with minor revisions have emerged. These are called “Alt-coins”. Additionally, currencies which have more fundamental technological innovation have also been created and are available in the market. As of April 7th, 2017, there were 780 digital currencies with a market cap calculated in USD\(^4\). The recent top 10 digital currencies based on the market cap are shown in Table 1.

Table 1. Top 10 digital currencies in market cap\(^5\)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Currency</th>
<th>Symbol</th>
<th>Market Cap (USD)</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>BTC</td>
<td>$19,011,478,838</td>
<td>$1169.25</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>ETH</td>
<td>$3,936,466,670</td>
<td>$43.51</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>XRP</td>
<td>$1,176,142,960</td>
<td>$0.03</td>
</tr>
<tr>
<td>4</td>
<td>Litecoin</td>
<td>LTC</td>
<td>$525,791,473</td>
<td>$10.41</td>
</tr>
<tr>
<td>5</td>
<td>Dash</td>
<td>DASH</td>
<td>$493,185,766</td>
<td>$68.35</td>
</tr>
<tr>
<td>6</td>
<td>Monero</td>
<td>XMR</td>
<td>$276,084,178</td>
<td>$19.37</td>
</tr>
<tr>
<td>7</td>
<td>Ethereum Classic</td>
<td>ETC</td>
<td>$239,112,149</td>
<td>$2.64</td>
</tr>
<tr>
<td>8</td>
<td>NEM</td>
<td>XEM</td>
<td>$154,800,000</td>
<td>$0.02</td>
</tr>
<tr>
<td>9</td>
<td>Augur</td>
<td>REP</td>
<td>$114,447,300</td>
<td>$10.40</td>
</tr>
<tr>
<td>10</td>
<td>MaidSafeCoin</td>
<td>MAID</td>
<td>$81,494,733</td>
<td>$0.18</td>
</tr>
</tbody>
</table>

Source: https://coinmarketcap.com/all/views/all/

\(^4\) https://coinmarketcap.com/all/views/all/
\(^5\) https://coinmarketcap.com/all/views/all/ (Accessed April 7th, 2017)
Looking at the growing perception and acceptance of private digital currency, central banks have started to examine their own issuance of digital currency. The digital currency which is issued by central banks using blockchain technology is generally referred as Central Bank Digital Currency (CBDC). The interest accumulated by central banks is driven partly by competition between fiat money and private digital currency, but also by the motivation to improve their own currency systems by taking advantage of blockchain technology. For example, the Bank of Canada examined deeply the benefit of issuing CBDC (Fung and Halaburda, 2016). By examining the benefits of using CBDC, they projected such improvements as the efficiency of currency functions, the efficiency and safety of payment systems, and policy responses to the competition against payment innovations in private sector.

In terms of the competition, the market cap of private digital currency is still very small. For example, the market cap of Bitcoin worldwide is only 0.1% of the money stock of JPY (as of July 2016). However, if these digital currencies grow at a rapid pace in terms of quantity and variety, the effectiveness of the current monetary policy of the central banks would be largely undermined.

On the other hand, digital currency has its own unique functional features that could change the concept of money itself. Forward-looking central banks could also gradually examine the impact of employing blockchain technology in their own monetary systems, by taking blockchain's features into consideration.

No central banks have actually issued real digital currency at this time, but several central banks in countries such as the UK, Sweden, Canada6, and Cambodia are reported to be considering their own digital currency. The Bank of England, in particular, has shown an intense interest in this topic in the speech7 of the Deputy Governor of the Bank of England, and in the report on the macroeconomic impact of CBDC8. Bank of Japan carefully suggests the interest in the technology stating “The Bank does not have a specific plan to issue digital currencies at this stage, but will deepen its research and analytical activities so as to understand the impact of technological innovations, FinTech and distributed ledger on financial architectures and FMIs while keeping all options open, including the possibility of the Bank’s utilizing such advanced technologies in its own operations in future.” (Nakaso, 2016).

2. Prior Studies

An increasing number of papers are being published on digital currency and blockchain technology. One example of such a paper is Cheah and Fry (2015), who explores the fundamental value of digital currency. Gandal and Halaburda (2016) discuss the competition among currencies and the network effect of digital currency. Hayes (2016) explores how the value of digital currency is determined, and analyzes three elements of digital currency by regression analysis: “the level of competition in the network of producers, the rate of unit production, and the difficulty of algorithm used to “mine” for the cryptocurrency”(p.1). The legal and political aspects of digital currency are also one of the topics discussed in this paper. Iavorschi (2013) discusses governmental intervention in digital currency, while Kowalski (2015) explores taxation issues.

Several important books have also been written on the general use of blockchain technology. Antonopoulos (2015) provides a detailed description about how Bitcoin and blockchain work. Swan (2015) focuses on the utilization of blockchain, and how it can be used for other digital assets. Tapscott and Tapscott (2016) discuss the general impact of blockchain. Raval (2016) describes a wide range of aspects of decentralized applications and services using blockchain.

7 http://www.bankofengland.co.uk/publications/Pages/speeches/2016/886.aspx
8 http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf
Prior studies on CBDC, however, are relatively limited. Broadbent (2016) provides an overarching insight on the impact of CBDC on financial systems. As the Deputy Governor of the Bank of England, he argues that the introduction of CBDC would allow all money holders and firms to access the balance sheet of central banks and as a result, all money holders would have their own accounts in the central banks. He warns this change could undermine the function of intermediary finance such as loans and deposits by commercial banks.

Barrdear and Kumhof (2016), in a Staff Working Paper of the Bank of England, present a detailed macroeconomic analysis of CBDC using monetary-financial DSGE analysis. They conducted the analysis from a monetary policy perspective and its impact through factors such as interest rates and liquidity, and found that CBDC issuance of 30% of GDP would increase the GDP by 3%.

From the more technological side, Danezis and Meiklejohn (2009) proposed the concept of the RSCoin⁹. The RSCoin is designed to enable a scalable capability to process massive scale transactions and to allow central banks to hold control of monetary policy. Another report specifically mentions the involvement of the Bank of England on the RSCoin¹⁰.

Generally, prior studies on CBDC are limited, and only a few focused points have been examined, such as monetary policy and scalability. However, blockchain technology offers a wide range of technological features and possibilities, rather than just a new form of currency. Therefore, the purpose of this paper is to provide a comprehensive set of topics and discussion points introducing CBDC and also introductory analyses on each point. This paper also reviews the technological and functional features of blockchain technology and its impact on the economy and society regarding the implementation of CBDC in the hopes of promoting future studies on this topic.

3. Technical Features of Blockchain-based Digital Currency

This section discusses the technological features that should be considered with the introduction of CBDC.

3.1 Transparency of Transactions

One of the most important features of blockchain is its comprehensive record of transactions which require transparency. For example, the ledgers, which contain transactions, are shared among participating nodes (computers). Therefore, all participants are capable of looking into transactions which show what amount of money was sent to which addresses. Even though the link between the identity of users and their addresses is not disclosed and one user can change addresses frequently, anyone can find what kind of transaction was made in the blockchain system if they are familiar with the technology.

Another aspect of blockchain's transparency is in the history of trading an asset. In blockchain, which employs UTXO architecture such as with the bitcoin, any new transaction is created by referring to a previous transaction. This feature completely changes the concept of traditional money, because it enables anyone to track where this money came from and where it is spent.

It is worth noting that there are two types of blockchain: open (Non-Permissioned) and closed (Permissioned). The original blockchain employs open architecture, which allows any computer to join the network and carry out the work to maintain the blockchain. The most innovative feature of blockchain is its ability to secure the consensus of the distributed ledger even among anonymous participants, including malicious ones. Through this feature, bitcoin has
enabled a currency service without central control or authority. Using this transparency, an analytics service, such as “BlockSeer” can exist on bitcoin. However, with various factors such as privacy, data security, and scalability becoming more and more important, a “closed” blockchain, in which only approved computers can participate in maintaining the blockchain or are allowed to view the contents of blockchain is also gaining popularity for enterprise use. However, whether open or closed, a comprehensive record is the most common feature of blockchain.

3.2 Direct Linkage between Ledgers and Users

Blockchain builds direct and logical connections between assets and the end-user by public and private keys. In the traditional financial system, money proliferates from the central bank through commercial banks, to individuals. However, if central banks issue CBDC based on blockchain, the ledgers in the central banks and the end-users are logically connected directly (Figure 4). From the central bank’s perspective, all money holders’ transactions can be seen. In Bitcoin, personal identity and public-and-private keys to control the asset are not linked unless additional legal instructions are implemented. It is also possible to change the keys frequently. From privacy’s perspective, it is one of the issues whether the keys are linked to personal identities and how the keys are managed. This direct linkage between Ledgers of central banks and users raise another concern on the role of commercial banks. Broadbent (2016) suggests the introduction of CBDC may allow all money holders, including individuals, to access the balance sheets of central banks, and this enables that the all money holders have bank accounts in central banks, rather than commercial banks.

![Figure 4. Direct Access to Ledgers](image)

3.3 Smart Contracts and Programmable Money

11 [https://www.blockseer.com/](https://www.blockseer.com/)
12 Management of keys includes the issues such as who should create the keys, how often the keys can be changed, and when the keys are revoked.
One of the most important features of blockchain is its “Smart Contract”. A Smart Contract is a computer program located and executed on the blockchain. It enables an automatic execution to change the status of digital assets on the blockchain that interact with other codes and even with systems outside of the blockchain.

Swan (2015) argues that Smart Contract eliminates the need for trust with other parties on the agreement to act or not act, because “[...] Smart Contract is both defined by the code and executed (or enforced) by the code, automatically without discretion”. If contract terms are “codified” perfectly in a computer program and hosted in a blockchain, the codified contract autonomously interacts with other programs and executes what should be done based on the contract.

Blockchain’s innovation is in the network of trust, and is therefore an automation that eliminates human intervention. As Swan (2015) writes: “Minimal trust often makes things more convenient by taking human judgement out of the equation, thus allowing complete automation”. Aiming at an expansion of the versatility of codification, new blockchain platforms other than Bitcoin, such as Ethereum and Hyperledger have been developed and introduced. By utilizing Smart Contract architecture, decentralized entities can conduct jobs even without human intervention. For example, a proof of concept of peer-to-peer electricity exchange was conducted in New York City. People who have solar panels sell, and those who need electricity buy electricity using Smart Contracts and blockchain technology.

By using Smart Contracts, code can be used to define the conditions on a certain payment, and the code can then be executed once the conditions are met. The employment of this technology in the CBDC means that the management of the contract also resides in the blockchain of central banks.

4. Implementation Challenges

This section discusses topics which should be covered when introducing CBDC in practice.

4.1 How to introduce and what to replace

Several issues should be pointed in the introduction of CBDC in practice. The first is what to replace: cash or bank deposit such as seen in Broadbent (2016). However, Digitizing cash is already commonly seen in the modern payment. In Japan, electronic money that is stored in smart cards is commonly used. In 2016, about 5,144 billion JPY was transacted by these electronic money. Replacing the form of these electronic moneys to blockchain-based digital currency would not make a major difference in terms of monetary systems. Regarding the replacement of bank deposit by digital currency, the most of bank deposit are also managed in digital forms. Therefore, simply converting bank deposit to digital currency would also make little impact.

On the other hand, there is other important issue on the introduction, such as partial introduction or full introduction. If CBDC replaces only a part of money stock of the economy, conventional money and CBDC coexist. If CDBC replaces all of a certain fiat money, there would be an issue of digital divide. The issues related to the partial-or-full replacement is discussed in the section 4.3.

4.2 Credit Creation

Considering the direct linkage between the ledger of CBDC and end users, there is a concern on the credit creation through commercial banking. For example, Broadbent (2016) suggests that switch from bank deposit to CBDC, which particularly could happen during financial crisis, would undermine credit creation through banks and eventually lead to narrow banking.

Even without the presence of a financial crisis, credit creation through commercial banks might be undermined by the introduction of CBDC. Particularly in low-interest economies such as in Japan, the primary reason to deposit money in the banks is to securely store its value and to be able to make transactions to others. This advantage on security is only viable when comparing bank deposit with physical cash. In other words, if all money is digitized and securely transacted through the CBDC system, there would be less reason for people to deposit money in commercial banks.

Alternatively, there would be an opportunity to create and provide a new set of financial services based on the blockchain - based digital currency. An example is peer-to-peer lending using digital currency as seen in Bitbond. Bitbond intermediates the peer-to-peer lending between individual investors and small business borrowers, using Bitcoin with interest rates. Recently, Coincheck, a Japanese cryptocurrency exchange, announced to start the deposit of Bitcoin with interest rate. It is certain that there is a need for utilizing unused money and also for the demand for supplementing the shortage of fund. Therefore, there would be a continuous service of financial services such as lending, but it might not be through the traditional banking system.

4.3 The Co-existence of Normal Currency and CBDC

One of the problems of the introduction of CBDC is the digital divide and financial inclusion. Not all people can use CBDC by using smartphones and PCs. Some countries such as Sweden have a cash-less policy, which means that retailers are not required to accept cash. If these countries can eliminate cash, CBDC and cash will not co-exist and CBDC dominates as the means of transaction. However, in most of the other countries may not be able to eliminate cash.

Conventional money and CBDC have wide differences functionally and through actual use, as we have seen. Therefore, the demand for two types of money is naturally different. In other words, a dynamic exchange rate between the two forms of money would be necessary. This situation would bring the burden of complication on the economy such as in accounting, banking, financial policy, and monetary policy.

4.4 Transparency and Privacy

As seen in section 3.1, blockchain offers a transparent record of all transactions. Even if the central bank adopts CBDC with a closed (permissioned) ledger, central banks can monitor all the transactions of money. Even in a setting where the identity of the user and the address of the money are strictly divided, there is the possibility of an authority monitoring economic activity. This would cause concerns of privacy.

From a technical perspective, even if the ledgers are stored in a private and closed network, most of the transactions can still flow on the Internet because it is almost impossible to build a private and secure network which covers all economic transaction using the CBDC. An alternative solution is to encrypt all transactions such as is seen in Zcash. Nonetheless, this solution must also be considered carefully and verified thoroughly before its adoption.

---

15 https://www.bitbond.com/
16 https://www.bitbond.com/
18 https://z.cash/
4.5 Extensibility of Functions

The positive side of the transparency of the ledgers is the extensibility of the platform. If all monetary transactions are recorded and available, there is the possibility for many entities to analyze the records and create value. For example, a government authority might be able to monitor transactions to see the purposes to which the benefit payments are used. In the case of benefit payment, a government can make sure that the money is paid for daily essentials, not for gambles. In other case, banks can find money which has not been used for a long time and offer the money owners an investment opportunity. Additionally, third-party vendors can create tax forms for their clients automatically from transactions.

If the blockchain of CBDC uses a Smart Contract, central banks may play even a larger role. For example, payment can be executed and authorized only when pre-designed conditions are met, such as the completion of certain work, the signature of multi-parties, and the transfer of other assets. Central banks may also be able to set a kind of interest rate for individual coins, rather than for a collective amount of money. This extensibility of function can change the concept of money.

4.6 International Use of CBDC

If central bank money is fully digitized as CBDC, it would be much easier for people who live outside of the jurisdiction of a country to access the CBDC than to access physical cash. In practice, the only barrier to buying CBDC is access to the Internet with devices and the ability to open an account to exchange money from other currencies to CBDC. Opening an account for the “digital” exchange of CBDC and exchanging digital money are much easier than physical cash, because in the latter case, one needs to go to the physical banks carrying physical cash, and there is a physical limit of amount on the exchanged money. The international use of CBDC could have a beneficial impact for countries whose currency is unstable and unreliable. In those countries, people may prefer to use digital GBP or digital JPY instead of the local currency as a medium for economic activity. From the central bank’s perspective, they can use CBDC to construct an economic sphere across borders with low friction on the international trade. On the other hand, it might become difficult to deal with the unexpected demands of the currency.

5. Conclusions and Future Research

This paper reviewed the technological and functional features of blockchain technology and provided a comprehensive set of topics and discussion points to introduce CBDC as well as introductory analyses on each point. This paper also discussed the technological and functional features of blockchain technology in terms of its impact on the economy and society regarding the implementation of CBDC.

Blockchain technology provides a currency system with important technological possibilities such as transparent records, direct linkage between ledgers and users, and the functional extensibility as seen in a Smart Contract. However, there are many challenges to be solved before implementing CBDC in the real economy. A comprehensive and in-depth discussion is essential to uncover CBDC’s potential benefits and risks. In this regard, research from multiple disciplines and methodologies on the introduction of CBDC is required, and a trial in an experimental setting is also desirable.
References


http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf


METI (2016) Survey on blockchain technologies and related services


