A New Peer-to-Peer Double Entry Settlement Network based on Encrypted Asset (1)

Ken ITO, Tomoki YATSUZUKA, Kyôske TOMONARI
Interfaculty Initiative in Information Studies
The University of Tokyo[1]

Abstract

Encrypted assets, based on the Blockchain technology such as Bitcoin, have expanded rapidly. In this paper, we systematically redesign the encrypted asset and propose a theoretical framework using double entry bookkeeping methodology. The Blockchain technology can be viewed as an incomplete application of the ledger system, that is single entry bookkeeping. The ledger is shared by all Bitcoin users in the peer-to-peer network and it enables the system to settle payments. In order to ensure an appropriate accounting practice in the system, the ledger and other accounting information needs to be recorded and organized by using double entry bookkeeping to facilitate a true audit process.

The Blockchain technology was proposed as a peer-to-peer network system without center of trust. However, Bitcoin users have pursued their own profit and changed Bitcoin's quality, from a currency to a speculative investment. In order to overcome this difficulty, Facebook and its cooperative companies proposed a new reserve currency, "Libra" ; a type of stable coin or sovereign coin, which is convertible to legal currencies. However, Libra's management entity, the Libra Association, is composed of commercial enterprises and it is impossible to prevent the association from pursuing profit-motivated activities. Therefore, the association cannot deliver a fair and impartial monetary policy to maintain a stable Libra system.

We propose a peer-to-peer network composed only of central banks, which impartially maintain the stability of the financial system without profit motivations. For such a network, we are developing a new Blockchain system, "NAKASO-IWAI's Post Blockchain systems". In this article, we will outline the fundamentals of this system. Further details will be published in future articles.

Key words: Blockchain, Encrypted Asset, Libra, Key Currency, Central Bank, Not-for-Profit, Double Entry Bookkeeping

1. Global currency, Standard currency and their limitations

In order to stabilize global finance and to facilitate free trade, Davit Ricard and others introduced the Gold Standard in 1816-17, just after the Napoleonic war[1]. The stable

[1] 7-3-1 Hongo, Bunkyo-ku 113-0033 Tokyo JAPAN, mail to: itosec@iii.u-tokyo.ac.jp

but essentially stagnant “Standard System” had facilitated global finance in the 19th century. It collapsed in 1929 due to the Great Depression [2].

John Maynard KEYNES asserted that the Gold Standard should be shifted to a Managed Currency System. However, the IMF system, which contained the conversion system between the US dollar and gold, was accepted in order to rebuild global finance after World War II[3]. The IMF system eventually collapsed due to the Nixon shock and was replaced by the managed currency system in 1971[4]. Since then, the managed global economy has grown rapidly.

The damage of the 2008 Financial Crisis was mitigated by utilizing a dollar swap network, which was established with great effort by Hiroshi NAKASO, at that time the head of the financial market bureau at the Bank of Japan, and representatives of the six major central banks, in order to resolve the US dollar shortage[5]. Just after the crisis, “Satoshi NAKAMOTO” proposed and implemented the Blockchain technology, the Peer-to-Peer network for Bitcoin. It was the first attempt to provide global society with a practical way of payment settlement without a center of trust[6].

However, as pointed out by Katsuhito IWAI, a Japanese economist, cryptocurrencies such as Bitcoin have become speculative investments, and the possibility of its circulation as a currency has been lost[7]. In June 2019, the stable coin Libra was proposed, mainly by Facebook, and it supports the framework of the Blockchain technology[8][9]. Libra is backed by a reserve composed of legal currencies, such as the US dollar and Euro, and has a potential to be the first global and stable digital currency. It may threaten the US dollar as a key currency. Libra is a type of sovereign currency which has an intrinsic risk of stagnancy, similar to the gold standard system which was harshly criticized by J. M. KEYNES.

We propose a new framework that overcomes the two limitations. We first review historical background of encrypted assets, and then outline a basic architecture of NAKASO-IWAI's Post Blockchain system as a possible practical encrypted asset in the 21st century.

2. Public Key Cryptography, Electronic Currency and radial network

The Single-Chip Computers, or LSIs (Large Scale Integrated circuit) appeared in the early1970s[10]. With the progress of information theory, it brought about an innovation in global finance and the money order after the change to the floating exchange rate system[4]. Amongst these technological advancements, the development and implementation of public key cryptography, such as RSA cryptography, played a crucial role[11]. Without the rapid improvement of computer power, the cryptography would

have never been put into practice. The cryptography enabled credit cards and pre-paid cards to be widely adopted and electronic money became popular in the advanced countries from the 1980s[12][13].

Such electronic currency systems always have center of trust. In the case of credit cards, final settlements are executed between the bank accounts of users and their credit companies. Similarly, in the case of pre-paid cards, final settlements are executed in a central server of the pre-paid cards' company. It is shown in the schematic diagram below (Fig. 1). In the left figure, the direction of arrows means the direction of payments.

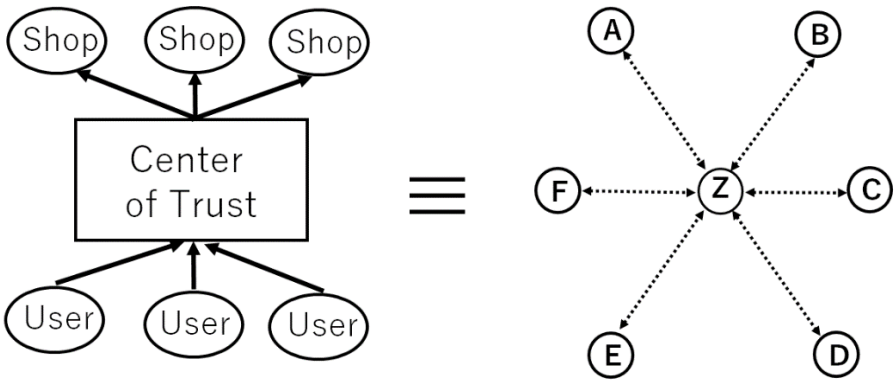

Fig. 1. A schematically radial network of electronic currency based on public key technology.

For a credit card company, consumers purchasing goods and services with the credit card and retail stores selling them are both its customers. In the right graph of Fig. 1, Z denotes a center of trust[2]. Here, suppose that there are three credit card users and three retail stores with the credit card company's membership (see the left graph of Fig. 1). Then, we would gain a radial network structure that connects six customers with Z as the center of the network (see the right graph of Fig. 1). Here, the dotted-lines shown in the right graph indicate the possibility of payment settlements between customers. Z is connected with all customers by the dotted-lines as the center of the network, whereas customers are not directly connected to each other but indirectly connected via Z as it is the only node which can execute payment settlements amongst its customers. Therefore, we can regard Z as a privileged node.

3. The 2008 Financial Crisis and the Dollar swap network

[2] We take the initial letter Z from German word "Zentrum".

In order to deal with the 2008 Global Financial Crisis, triggered by the bankruptcy of Lehman Brothers Holdings Inc. on 15th September 2008, it was crucial to secure a stable and swift supply of US dollars for each country. Representatives of the six major central banks, including H. NAKASO of the Bank of Japan, established the US Dollar swap network which connects the FRB with other central banks to ease the US dollar shortage (Fig. 2)[5]. By utilizing this swap network, these central banks endeavored to restore the stability of the financial system to minimize the damage of the financial crisis[5][7].

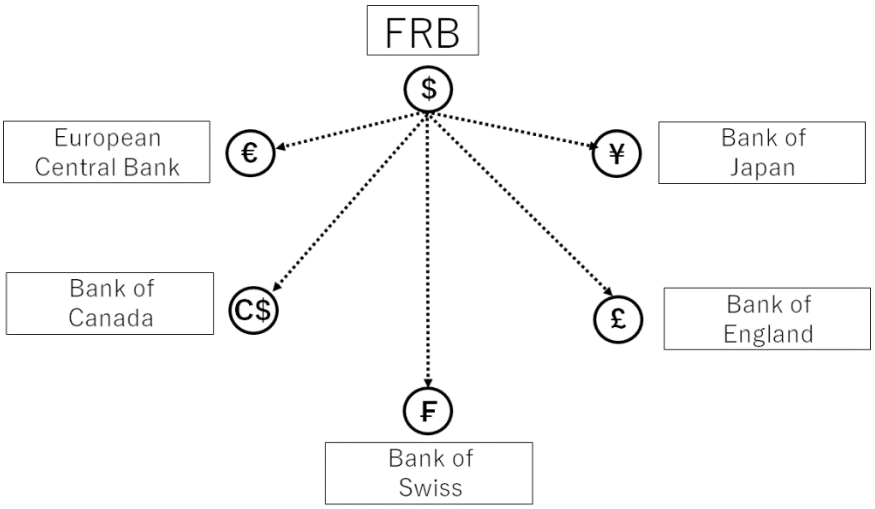

Fig. 2. The Dollar swap network formed amongst central banks to resolve the Global Financial Crisis.

Any central bank, apart from the FRB, cannot issue US dollars even when a serious US dollar shortage occurs. The FRB, on the other hand, can issue as many dollars as it needs, but cannot provide dollars to other central banks facing difficulties due to dollar shortages. Therefore, these central bankers established the swap network in order to enable the FRB to provide dollars to other central banks when necessary. By utilizing the network, these central banks manage to finance dollars into markets where necessary, successfully resolve the crisis based on fairness, and maintain impartial positions[5][7].

The schematic graph in Fig. 2 is a radial network which has the FRB as the center of the “network” since the FRB is the only source of the US dollar supply. Dotted-lines in the Fig. 2 indicate possibilities of suppling the dollar through these routes, rather than actual payments, and show the fact that nodes are connected to each other in the network. Let us call this network "NAKASO's Radial Central Bank network".

After the 2008 Global Financial Crisis was resolved, H. NAKASO and other representatives from the six major central banks extended the swap network to enable all central banks in the network to provide their own currencies to each other(Fig. 3) [5][7]. We can combine these radial networks into the single network shown in Fig. 4. It shows all the possibilities of currency exchange amongst these banks with the six different currencies. Two-dotted-lines indicate network connections for possible swap transactions amongst different currencies[3]. Let us call the network "NAKASO's Central Bank Multilateral Swap Network".

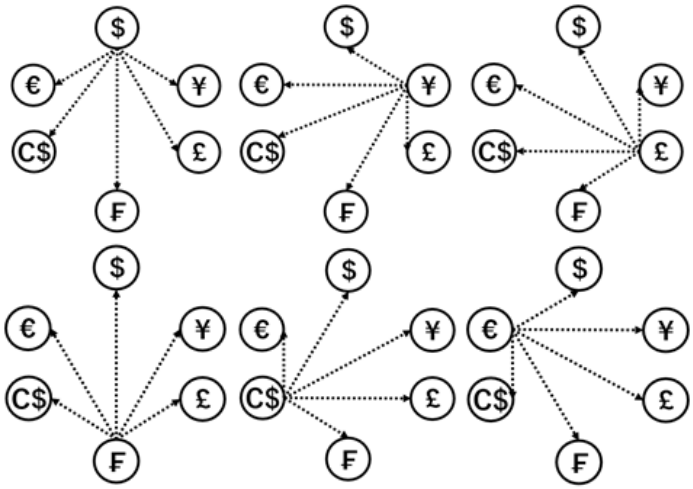

Fig. 3. The mutual expansion of NAKASO's Radial Central Bank network.

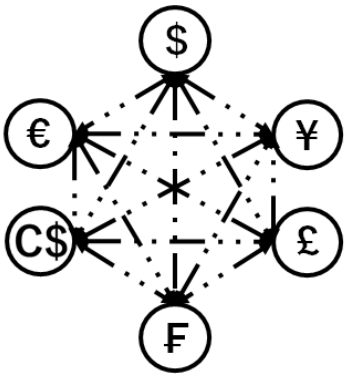

Fig. 4. NAKASO's Multilateral Central Bank Swap Network.

Now, let us examine the graph structure of the NAKASO's Central Bank Multilateral swap network. Firstly, note that all nodes in this network are central banks. There is no user with any profit motivation in this network. In case of a crisis or another situation

[3] Here, we do not discuss actual transactions. The network shows the possibilities of currency exchanges when a crisis occurs.

where the global financial system needs to be maintained, every node cooperatively intervenes just to resolve the issue. Secondly, note that this multilateral network has an unique characteristics as there is no center of trust for the whole system and all nodes transact with each other for the public good. Since there is no privileged center of trust and all nodes are equally connected, this network is a peer-to-peer network. The graph structure of the network is a "complete graph structure" where every vertex is tied to each other.

4. The peer-to-peer network structure of Blockchain

In 2008, “S. NAKAMOTO” proposed the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" just after the Financial Crisis[6]. ”Blockchain”, the core technology of the contemporary encrypted asset system, was introduced and put into practice for Bitcoin in January 2009[14]. As mentioned in the previous sections, all electronic settlement systems before Bitcoin have, without exception, a radial network structure with a center of trust such as a bank. Bitcoin is, to the contrary, conceived as a peer-to-peer network without a center of trust.

The 2008 Financial Crisis was partly caused by dominant and arbitrary information handling by financial institutions[15]. The inventor(s) under the name of “S. NAKAMOTO” criticized such privileged asymmetries in finance[16]. NAKAMOTO proposed a new electronic currency system with a complete graph structured network where all nodes are completely equal and are able to settle payments with each other, and “he” proved that the system actually works. Seemingly Fig. 4 and Fig. 5 are quite similar; they both have complete graph structures. However, between these two, there are some crucial differences.

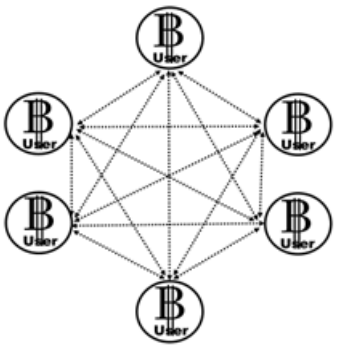

Fig. 5. The P2P network of Bitcoin.

Firstly, multiple currencies are traded in the swap network of Fig. 4 whereas the single bill Bitcoin is traded in the network of Fig. 5. Another difference is the existence of the mining mechanism, even though it is not explicitly shown in the figures[4]. The peer-to-peer network in Fig. 4 consists of central banks which are in impartial positions for the public good, whereas the network in Fig. 5 consists of users who compete against one another for their profit through the mining race. The network in Fig.5 introduces the original Blockchain technology to manage its system but NAKASO's Central Bank Multilateral Swap Network in Fig. 4 does not utilize the Blockchain system.

Let us examine briefly the Blockchain System[5]. The inventor(s) of Blockchain under the name of S. NAKAMOTO incorporated two ideas to actualize the electronic currency without a center of trust [6][17]. Firstly, NAKAMOTO redesigned the whole network with sharing settlement information; this information used to be exclusively held by a center of trust in traditional systems. In the new design, ledger information is equally shared by all nodes under a privacy protection policy. Thereby, this new approach ensures the accounting transparency in the whole system. Secondly, NAKAMOTO endeavored to prevent “his” new “coin” from any forgery. Without a relevant prevention mechanism, it would be possible to copy the “coin” without limitations, since a digital currency is merely digital numeric information. In order to resolve this issue, NAKAMOTO implemented electronic signature technology to make it difficult for users to double-spend coins, and the settlement system where a block of approved transactions is validated every 10 minutes (“Proof-Of-Work”). This system is called “Blockchain”. All nodes equally compete with each other to solve a problem, which is appropriately adjusted by its difficulty level for determining the rapidity of validations of a “block”, which is a type of ledger consisting only of correct and fair transactions. Bitcoin is issued as a reward to the node which solves that calculation first. Introducing such a competitive system which stimulates speculative motivation, Bitcoin has grown widely and rapidly.

The total amount of Bitcoin issuance is determined in advance and an issuance amount for each mining is set to decrease over time. Also, Bitcoin was conceived as a pure managed currency without any backing commodities such as gold. Furthermore, the concept of "interest income" is absent in Bitcoin system. It is because Blockchain is designed to deny the present financial system itself, and the Bitcoin system is conceived in a sense for a pure barter economy, similar to primitive communism. Interest income

---

[4] Since the mining is irrelevant to our arguments of this article, we do not examine it in detail (See [17]).

[5] We would like to focus on the points required for our arguments; other points such as the calculation of the Proof-Of-Work to obtain hash values are not examined in this here (See [17]).

is only earned by depositing money in a bank which is a privileged node in the present financial system.

In June 2019, the "Libra" project, which was designed mainly by Facebook, was proposed and was harshly criticized by many countries. Reactions from the US are the most extreme[18]. The US requested a halt to the development of Libra: America regards the digital currency as a threat to the position of the dollar[19].

Before examining the basic structure of Libra below, let us theoretically review the arguments of K. IWAI regarding the requirements for a currency to circulate as money while maintaining an orderly financial system.

5. Katsuhito IWAI's arguments on currency and public interest of central banks

K. IWAI suggested that Bitcoin had become a speculative object and the possibility of its circulation as a currency had been lost[7]. In general, a market price of a speculative object fluctuates violently. Then, a cryptocurrency may potentially circulate as a currency if stable. Facebook's Libra satisfies this condition by adopting a form of "Stable Coin". IWAI also argues that liberalism based on profit motivation should be properly controlled in order to sustain growth of the free market global economy [7].

This point may become clearer if you recall that the 2008 Global Financial Crisis was caused by inappropriate investment and lending. The repeal of the Glass = Steagall act in 1999, which was established in 1933 just after the Great Depression, allowed this to happen[15]. We can also support the argument by pointing out that Bitcoin became a speculative investment due to its high volatility.

A financial crisis or depression might occur when speculative activities disrupt a financial market. IWAI suggests that the existence of an independent organization, such as a central bank, which intervenes in a market without a profit motivation, is crucial requirement for stabilizing the global financial system and preventing a financial crisis. Let us call this requirement "IWAI's Central Bank Neutrality Condition". IWAI calls an organization, which appropriately regulates a market without a profit motivation, as "Big-Brother"[6]. A central bank is a typical example of "IWAI's Big-Brother".

In order to stabilize a payment settlement system based on Blockchain technology in the global financial system, we need the function of IWAI's Big-Brother. IWAI also pointed out that the excessive liberalism, or "Neo-Liberalism", may potentially be harmful for the free trade system and the global financial stability.

We now review Facebook's Libra in light of IWAI's arguments.

---

[6] "Big-Brother" appears in the novel "Nineteen Eighty-Four" written by George Orwell. Also, see [7].

6. The proposal of Facebook's Libra

Facebook, the largest SNS company with about 2.7 billion participants, proposed the architecture of the "electronic currency" Libra in June 2019, in cooperation with 27 companies including credit card giants such as Visa and Mastercard[8]. In the G7 Finance Ministers and Central Bank Governors Meeting in Chantilly, France[20], the central bankers and governments concluded that Libra should be closely monitored. Facebook explains Libra as a digital currency with Blockchain technology[8][9], although Libra differs in various ways from other encrypted assets.

Firstly, Libra will be backed by a reserve composed of real assets including legal currencies to prevent a high price volatility, which Bitcoin failed to control[7]. The Libra association accepts only large investors[8]. Libra has characteristics of a standard currency, which was dominant in the 19th century, rather than a managed currency dominant in the latter half of the 20th century. This classical system is unstable and a bank run can occur in case of credit uncertainty.

The Libra system has three tiers, namely, investors who provide reserves and various assets, the Libra association which runs the system, and users who use the “currency” for payment settlements. These tiers are shown in Fig. 6 as a schematic chart. At a glance, we can point out that the structure is different from Fig. 4 and Fig. 5. However, there is a privileged node as a center of trust in the Libra network (See Fig. 6). This is one of the major and essential differences from the Bitcoin network. The privileged node is denoted as “f” in Fig. 6. The “f” plays a role similar to a conversion bank in the gold standard system. Note that for an investor, the node “f” is the one which earns profits by investing the funds. Therefore, the “f” functions like an investment bank, which issues the Libra “currency”, as well as like a hedge fund. The Libra system may potentially have a serious risk in terms of the separation of a bank and investment fund. We distinguished the arrows between “users” from the arrows between the “f” and “users” in Fig. 6, since “users” transact the common currency “Libra” but also can exchange Libra for legal currencies, such as the US dollar and Euro with the “f” as a conversion bank.

Secondly, this digital “currency” itself does not generate any interest income. This condition is totally against the economic growth of the of the “users’ Libra” network = society. Therefore, the capital of the Libra users does not increase by any interest income. Let us assume the same situation which occurs in one country; the country’s capital will not grow. The investors gain an investment return from the Libra reserve. The Libra Reserve plays the role of an investment bank to pursue profit income and is totally different from a central bank which operates to maintain the financial system.

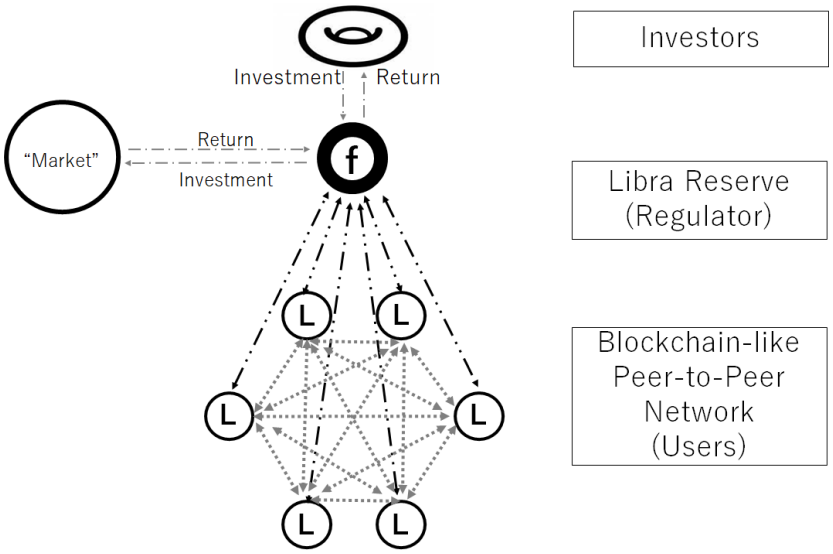

Fig. 6. The schematic graph of Libra network.

Finally, although Facebook explains that the Libra association headquartered in Switzerland will operate as an impartial and independent "third party", this "third party" only means that the association treats all the investors equally, but does not satisfy an impartiality requirement for a currency issuer [8]. Rather, the association will make a business decisions with a clear profit motivation as a part of the private sector. Because of this, the proposed Libra association cannot operate any true neutral financial policy to maintain the financial system. Therefore, it will be difficult to expect Libra to function as a stable global currency for a long term. According to the present Libra proposal, the "investor" can manipulate the system to earn profit from the "users" network society.

7. Conditions required for a possible global encrypted asset

Then, what kind of encrypted assets or global digital currencies should be considered? As mentioned in the previous sections, it is essentially difficult for private companies such as Facebook, to become the core of global finance for the public good. As K. IWAI pointed out, a financial system is vulnerable without fair and impartial moderator. There would be no way to avoid a financial crisis, if a moderator without a profit motivation does not operate appropriate monetary policies, such as a quantitative easing, to restore stability in the financial system.

Regarding this issue, J. M. KEYNES pointed out the fact that "God's invisible hand" failed to avoid the Great Depression in 1929, and he advocated fiscal and financial policies, such as public investments and central bank's monetary controls, with a fair and neutral stance[21].

Now, let us consider a network which is composed only of central banks, similarly to NAKASO's Central Bank Multilateral Swap Network(Fig. 7). In this network, there is no private company which would pursue its own profit. We would design an original global settlement system in this network by operating the peer-to-peer network system similar to Bitcoin. This network has a similar structure to KEYNES's proposal in the Breton Woods conference in 1944, for the rebuilding of the world economy after the World War II [3].

KEYNES proposed a “managed currency system” to replace the pre-era gold standard system. He proposed a system named "BANKOR" which is a type of peer-to-peer network. This idea was not conceived by himself, but he modified the proposal of Ernst Fritz SCHUMACHER (1911-77) who was born as a German citizen and immigrated to the UK after the Nazi era [22]. KEYNES proposed a new key currency named "BANKOR" but it has never been materialized. The Breton Woods conference accepted the IMF proposal that nominated the US dollar as the key currency, the only convertible currency to gold, and partly maintained the gold standard [3]. Even after Richard NIXON, the president of US, abolished the conversion system in 1971, presented the managed currency system is still based on the US dollar as virtual key currency [4]. Libra may potentially challenge this US-dollar-centered system.

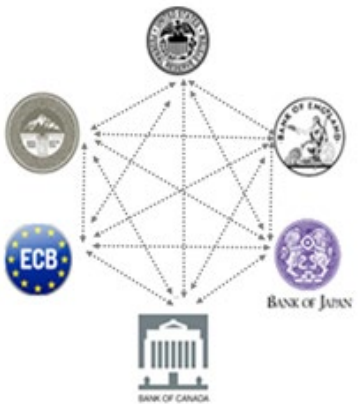

Fig. 7. An example of P2P network amongst central banks.

Examining the “Clearing Union” from the KEYNES’ and SCHUMACHER’s perspective, S. NAKAMOTO's Blockchain has an essential shortcoming. Namely, the lack of a double entry bookkeeping structure.

In general, NAKAMOTO's Blockchain is regarded as a digital “currency”, but its entity is an incomplete and unique type of single bookkeeping “ledger”. Minimum security is provided by applying technologies such as electronic signatures. However, both debit and

credit information, which are crucial for accounting to maintain fair financial systems, are lost by executing the Proof-Of-Work. Thus, we do no propose to discuss the cryptographic security for now. It would be enough to apply cryptographies to the system during the implementation phase. In addition, the central bank's peer-to-peer network does not require mining competitions based on profit motivation. Therefore, we would omit all relevant details of cryptography. Assume that there is a peer-to-peer network consisted of six central banks such as the one shown in Fig. 7, we may express these transactions in the form of the 6×6 matrix（Fig. 8）. We call matrix X the "primary-transaction matrix".

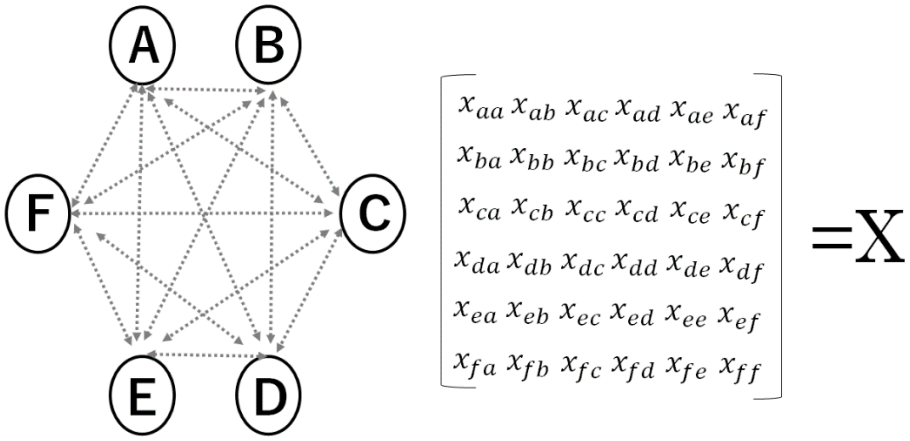

Fig.8 Transaction Matrix.

Diagonal elements and non-diagonal elements in this primary transaction matrix have different meanings. The non-diagonal elements indicate transactions amongst central banks whereas the diagonal elements indicate the amount of assets held in each central bank. Here, we separate the matrix into two parts (Fig. 9).

We can organize all the transactions into the primary-transaction matrix by adequately defining it and adding information to the matrix. We call a matrix composed of only the diagonal elements of a primary matrix as a "primary stock matrix", and a matrix composed of only the non-diagonal elements as a "primary flow matrix", respectively. In the current Blockchain system, we cannot check the debit and credit of each transaction. However, in the case of a network where all nodes are composed of central banks, cryptographies for system security protection are not necessary.

In practice, the matrix would not be in such a simple form as the example above. However, by expressing stocks and flows in a matrix form, we can adequately summarize all transactions into a form which facilitates a true audit. Furthermore, we would

transform the transaction matrices into a matrix-form database where one can easily grasp all the transactions as a whole. We call such a system “Post-Blockchain”. We can regard a matrix of a financial statement of every fiscal year as a stock matrix. In addition, we can gain a stock matrix of the next fiscal year by acting the flow matrix of the next year to the stock matrix of the previous year.

$$X = \begin{bmatrix} x_{aa} & 0 & 0 & 0 & 0 & 0 \\ 0 & x_{bb} & 0 & 0 & 0 & 0 \\ 0 & 0 & x_{cc} & 0 & 0 & 0 \\ 0 & 0 & 0 & x_{dd} & 0 & 0 \\ 0 & 0 & 0 & 0 & x_{ee} & 0 \\ 0 & 0 & 0 & 0 & 0 & x_{ff} \end{bmatrix} + \begin{bmatrix} 0 & x_{ab} & x_{ac} & x_{ad} & x_{ae} & x_{af} \\ x_{ba} & 0 & x_{bc} & x_{bd} & x_{be} & x_{bf} \\ x_{ca} & x_{cb} & 0 & x_{cd} & x_{ce} & x_{cf} \\ x_{da} & x_{db} & x_{dc} & 0 & x_{de} & x_{df} \\ x_{ea} & x_{eb} & x_{ec} & x_{ed} & 0 & x_{ef} \\ x_{fa} & x_{fb} & x_{fc} & x_{fd} & x_{fe} & 0 \end{bmatrix}$$

$$= \quad S \quad + \quad F$$

Fig. 9. Primary Stock Matrix and Primary Flow Matrix.

As shown above, we can now consider combining stock matrices and flow matrices into a set of series where these matrices are related to each other in a chain. At this stage, it would be possible to assure a security for the system by applying adequate cryptographies. We name this encrypted asset system “Flog-Chain”, because the system includes two series of matrices interacting with each other and we have got ideas from the “Leapfrog integration” algorithm[23]. Even if all nodes in a network are central banks and the network itself acts impartially for its constituents, each node may take an action to benefit its own nation. We could think of a "central bank of central banks", such as the Bank for International Settlements (BIS), in this configuration (Fig. 10). Note that the network in Fig. 10 differs from the structures of a peer-to-peer network (Fig. 5 and Fig. 7). This structure is similar to certain of the structure of Libra shown in Fig. 6. Here, "Z" denotes the central bank for a group of central banks.

There are several differences between Fig. 6 and Fig. 10. Firstly, note that all arrows in the network in Fig. 10 are the same type. An encrypted asset in this system would not be backed by either gold or any reserve of legal currencies. This network would operate under a complete managed currency system, similar to the “Multilateral Clearing Union” proposed by SCHUMACHER and KEYNES [24]. Furthermore, in Fig. 10, there are no investors with a profit motivation. This network is gained by developing the NAKASO-

IWAI's Central Bank Multilateral Swap Network under the principle of IWAI's Central Bank Neutrality. Therefore, we would call this structure "NAKASO-IWAI's Post-Blockchain Network".

The implementation of this network can be applied for several purposes. In future papers, we would introduce PUBLOR-MODELs (PUBLIC + OR) as an example of the NAKASO-IWAI's Post-Blockchain Network.

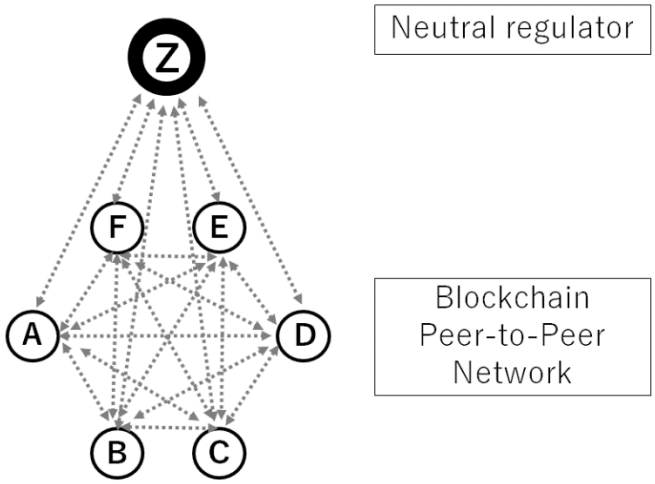

Fig. 10. The schematic graph of NAKASO-IWAI's Post-Blockchain Network.

8. Concluding remarks

In concluding, we would revisit this article as a whole while examining the 2030 United Nations agenda[25].

The 2030 agenda is also known as the SDGs; Sustainable Development Goals, which consist of 17 field goals to achieve sustainable developments in the world economy. Amongst them poverty eradication, or the reduction of disparities, has been repeatedly emphasized in the G20 and G7 meetings [20].

Currently, numerous people are suffering in poverty while only a few monopolize a majority of wealth in the world.

K. IWAI mentioned the research of Anthony ATKINSON and Thomas PIKETTY on the economic and social gap, and expressed a concern that private companies tend to pursue innovation only for their shareholders' benefit, not for the public good, even though these companies play an important role in innovation[7]. PIKETTY argued that an increase in disparities is caused by when the rate of capital return is greater than the economic growth[26]. Considering PIKETTY's argument, IWAI criticized capitalism for investors[7]. A financial system without a fair and impartial moderator cannot remain

stable in the long term. We will now examine Facebook's Libra from the SDGs agenda perspective.

Firstly, in terms of sustainability, Libra is unlikely to be sustainable because it lacks a fair and impartial moderator so that it cannot operate a relevant financial policy in order to maintain the stable Libra system.

Secondly, in terms of development, Libra is unlikely to facilitate economic growth in areas where Libra is used. Libra would just be used as a medium of exchange by users. There would be no economic growth as it lacks the ability to earn interest income. Facebook stated that Libra would provide financial opportunities to the 1.7 billion people in the world, who remain outside of the current financial system[8]. By connecting these people and others, Libra might potentially bring growth of real economies. However, the schematic graph of the structure of Libra (Fig. 6) clearly shows that profit and growth from Libra would be distributed mostly to investors, not to people in the developing countries.

Finally, in terms of inequality and poverty eradication, the current Libra plan, which is cooperatively developed by large companies in order to pursue their own profit, is a typical system of capitalism for investors, just as ATKINSON and IWAI severely criticized. The implementation and expansion of the current Libra plan may not be sustainable and may in fact worsen socio-economic disparity and poverty problems.

In short, the current Libra proposal may hamper development of regional economies and worsen disparity and poverty as the system is not sustainable or stable. We can consider the "NAKASO-IWAI's Post-Blockchain System" as a set of conditions for an encrypted asset, to overcome those problems. Note that we do not deny the potential of Facebook's Libra completely[7]. The current Libra proposal has too many serious defects, and the implementation of the system may cause a financial crisis. However, if an adequate digital currency is widely adopted, the system could have the potential to solve the serious problems in the SDGs agenda. The current Libra proposal is clearly insufficient, but possibilities would be opened up if Libra overcomes the major defects we identify in this paper. We would discuss these possibilities in following papers.

We would like to send our sincere thanks to Lang WILLETT, Kerryn POOK and Michelle YATSUZUKA for their fruitful discussion.

[7] We will propose alternative models in the following papers.

References

[1] Hayek, Friedrich, “The Restriction Period, 1797-1821, and the Bullion Debate”, 1991, The Trend of Economic Thinking., ISBN 978-0865977462.

[2] John K. Galbraith, “The Great Crash 1929”, 2009, MARINER BOOKS.

[3] Steil, Benn, “The Battle of Bretton Woods: John Maynard KEYNES, Harry Dexter White, and the Making of a New World Order”, 2013, Princeton University Press. ISBN 978-0-691-14909-7.

[4] Lewis, Paul, “Nixon’s Economic Policies Return to Haunt the G. O. P.”, August 15, 1979, The New York Times.

[5] H. NAKASO, "Evolving Monetary Policy: The Bank of Japan's Experience - Speech at the Central Banking Seminar Hosted by the Federal Reserve Bank of New York -", 2017, Bank of Japan, https://www.boj.or.jp/en/announcements/press/koen_2017/ko171019a.htm/

[6] Satoshi NAKAMOTO,“Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, www.bitcoin.org.

[7] K. ITO ed. “Encrypted Asset and the Capitalism”, 2019, to be published by The Tokyo University Press.

[8] The Libra Association Members, “An Introduction to Libra”, 2019, https://libra.org/enUS/white-paper/

[9] Zachary Amsden, Ramnik Arora, Shehar Bano, et. al., “The Libra Blockchain”, 2019, https://developers.libra.org/docs/the-libra-blockchain-paper

[10] Mead, Carver A. and Conway, Lynn, “Introduction to VLSI systems.”, 1980, Boston: Addison-Wesley. ISBN 0-201-04358-0.

[11] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, 1978, dl.acm.org.

[12] Davit S. Evans, Richard Schmakensee, “Paying with Plastic: The Digital Revolution in Buying and Borrowing”, 2004, The MIT Press.

[13] Finn Brunton, “Digital Cash; The Unknown History of the Anarchists, Utopians, and Technologies Who Created Cryptocurrency”, 2019, Princeton University Press.

[14] "Block 0 – Bitcoin Block Explorer". Archived from the original on 15 October 2013.

[15] Jacob Soll,“ THE RECKONING: FINANCIAL ACCOUNTABILITY and the RISE and FALL of NATIONS ”, 2014, Basic Books.

[16] "Satoshi's posts to Cryptography mailing list". Mail-archive.com. Retrieved 26 March 2013.

[17] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, 2016, Princeton University Press.

[18] See https://www.theverge.com/2019/6/18/18684268/facebook-libra-cryptocurrency-stop-congress-house-democrat-maxine-waters-regulation

[19] See https://medium.com/hackernoon/the-shocking-reason-why-the-united-states-wants-to-stop-libra-5ee97d68647e

[20] See https://www.japantimes.co.jp/news/2019/06/29/national/full-text-g20-osaka-leaders-declaration/#.XX07bSj7SUl

[21] J. M. KEYNES, “The General Theory of Employment, Interest and Money ”, 1936, Palgrave Macmillan.

[22] Barbara Wood,“ E. F. Schumacher, his life and thought”, 1984, Harper & Row1st U. S. ed.

[23] Radford M. Neal, “MCMC using Hamiltonian dynamics”, 2012, arXiv:1206.1901v1[stat.CO] 9 Jun 2012.

[24] E. F. SCHUMACHER, “Multilateral Clearing”, 1943, Economica-New-Series-Vol.-10-No.-38-May-1943-pp.-150165.

[25] See https://www.un.org/sustainabledevelopment/

[26] T. PIKETTY, "Capital in the Twenty-First Century", 2014, The Belknap Press of Harard University Press.