Discussion Paper Series

RIEB

Kobe University

DP2020-19

A Proposal for Asia Digital Common Currency

Taiji INUI
Wataru TAKAHASHI
Mamoru ISHIDA

Revised September 29, 2020

Research Institute for Economics and Business Administration
Kobe University
2-1 Rokkodai, Nada, Kobe 657-8501 JAPAN

A Proposal for Asia digital common currency[1][2]

Taiji INUI[3], Wataru TAKAHASHI[4], Mamoru ISHIDA[5],

June 01, 2020

Abstract

This paper proposes to provide Asian common currency in the form of digital currency using technology such as blockchain by an international organization (eg AMRO) in East Asia. In this proposal, we assume that each present currency and the new digital common currency coexist in the respective economies for the time being. With the advent of digital currency, the common currency has become more technically feasible. Our proposal has the following three advantages; (1) merits as a digital currency, (2) merits as a common currency, and (3) a currency that is managed in a multilateral flamework. By the last point, it could prevent dominant control of an international currency by large countries, and political fairness can be secured. This proposal has a perspective to develop into a global digital currency in the future.

JEL Classification: E42, F33, F36
Keywords: Digital Currency, Asia Common Currency, Distributed Ledger Technology, Blockchain, account-based, token-based

---

[1] Authors would like to express their sincere appreciation to Mr. Masayuki Mizuno of American Family Life Assurance Company of Columbus (Aflac), Mr. Yasuo Takamura and Mr. Satoru Yamadera of Asian Development Bank (ADB), Mr. Toshihiro Oritate of JSF Trust and Banking Co. Ltd., Mr. Katsuhiro Endo of Japan Student Services Organization, and so many people who kindly provided insightful advices, impeccable comments, and sincere support. Despite this, all opinions and views in this paper are those of the authors and do not necessary represent any views of the ADB, JICA, the Bank of Japan, Itochu Corporation or any other organizations.

[2] This work is supported by JSPS KAKENHI Grant Number 15H57290

[3] Chief Advisor, JICA CBM TC Project, Central Bank of Myanmar and ADB consultant for Cross-border Settlement Infrastructure Forum (CSIF), E-mail; taiji.inui@home.email.ne.jp

[4] Professor, Osaka University of Economics and Research Fellow, Kobe University (RIEB), 2-2-8, Osumi, Higashiyodogawa-ku. Osaka, 533-8533, Japan. E-mail: wtaka@osaka-ue.ac.jp)

[5] Advisor, Itochu Corporation, Former Professor, Hannan University.

1. Introduction

A digital common currency issued by an international organization (AMRO[6] for example) to be circulated across the countries/economies in ASEAN+3[7] is proposed in this paper. Although the use of RMB is gradually increasing, USD is still mostly used for cross-border payments in ASEAN+3 at present. However, using the currency outside the region may increase the foreign exchange risks as well as possibility of negative impact from the policy of outside country. Furthermore, it is not desirable that the currency of a specific country in the region becomes dominant. We propose to introduce "the digital ASEAN+3 (common) currency" something like ACU[8] in the region. We assume each country/economy keeps issuing current currency for the time being, which means that the digital currency co-exists with the current currency in the region. From this perspective, it is different from that in Europe abolishing the currency in each country unifying to the single currency. Though we don't have any intention to exclude the possibility of single currency in the future, our proposal would have a biggest benefit to provide an infrastructure which enables convenient payment and stable settlement by the common digital currency in the region.

With respect to the Monetary Union, Europe is far ahead of Asia. Around the early 2000s, concept of Asian common currency became very popular and even some methods to calculate Asian common currency unit were proposed. Such an enthusiasm, however, decreased after the European sovereign crisis caused by the global financial crisis. Having said that, we can discuss enhancement of the infrastructures separately from the single currency since the monetary union consists of two features, the currency unification and the integration of financial markets. Financial market integration requires regional-wide payment/settlement infrastructures as well as legal and accounting system. Taking a look at the case in Europe, although currency integration and market integration have progressed almost together, it is also important to note that both policies can be implemented separately, as market integration such as the development of payment systems extends to non-Euro member countries, such as Denmark, Sweden and UK. Regarding the promotion of payment/settlement infrastructures, firstly, high value payment or RTGS[9] systems were connected each other in the region (TARGET Interlinking system), then, by consolidating the RTGS systems into a single shared platform, TARGET2 was established. With respect to the securities settlement, T2S[10] having cash settlement

---

[6] ASEAN+3 Macroeconomic Research Office

[7] ASEAN+3 comprises the Association of Southeast Asian Nations (ASEAN) plus the People's Republic of China, Japan, and the Republic of Korea. Also, ASEAN consists of Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam.

[8] Asian Currency Unit

[9] Real time gross settlement

[10] TARGET2-Securities

inside (which enabled the Auto-collateralization) was developed. Furthermore, an initiative to consolidate the TARGET2 and T2S into a single platform is underway. Such an enhancement of payment and settlement infrastructures may contribute to the further development of financial markets in Europe.

This digital common currency proposed may be a tiny initiative compared to that in Europe, but it may be the first proposal to develop such a financial market infrastructure in the region.

Now, let me explain the merits of the digital common currency briefly. It will not only reduce the foreign exchange risks as already discussed, but also, increase resilience against currency crisis. Considering the Asian Currency Crisis happened from 1997 to 1998, a financial crisis generally starts by an attack to a country/economy which happen to expose vulnerability of its financial system, then contagiously expands its impact to other countries/economies. Common currency would have a capability to reduce such weakness. More importantly, common currency is to be operated based on multi-county/economy cooperation, which means small countries/economies have higher possibility having equivalent voice with big countries/economies. Under current global financial system, US is a hegemony state, and China could be such a country/economy in the future. Multi-country/economy framework of common currency could mitigate such a negative impact by curbing big countries/economies hegemony.

It may be pointed out that the common currency proposed here is complicated because it will coexist with other current currencies in the region. But, considering current situation such as dollarized countries/economies in which two currencies already circulated, and moreover, considering the possibility of private crypt-currencies such as bitcoin and Libra prevail, circulation of publicly authorized common digital currency would be beneficial for the countries/economies as well as for the region. As a matter of fact, electronic money and other payment instruments are already prevailing (coexisting) in some countries/economies in the region.

In ASEAN+3, it is a well-known fact that about 500 years ago, we had a common currency “Yongle coin (永楽通宝)” which is a coin in Ming Dynasty of China prevailing wide area in Asia including Japan. In Japan, we didn’t have our own currency and utilized the Yongle coin as a common currency. This regional common digital currency concept could be a proposal having Yongle coin again but controlled by all the countries/economies in the region. Considering that the Yongle coin is used in Europe, too. The regional common digital currency proposing here may possibly be expanded globally.

2. On digital currency

With respect to the digital currency issued by central banks (CBDC), there are already many papers and some actual initiatives. Among those, the policy and direction of a central bank may be clearly mentioned by the speech "Should the Bank of Japan Issue a Digital Currency?" made by Mr. Masayoshi Amemiya, Deputy Governor of the Bank. More specifically, "Many central banks therefore take the position that they have no plan to issue CBDCs in the near future but will continue research into CBDCs, which is the position of the Bank of Japan also takes" is clearly mentioning the position of central banks. In the speech, CBDC is categorized into two variants "wholesale CBDC" and "general purpose CBDC". Characteristics of each variant are explained as follows:
The "wholesale CBDC" is electronic central bank money, which offers access to a limited group of users such as banks, among whom it is used for funds settlement. The "wholesale CBDC" adopts new information technologies such as distributed ledger technology (DLT) in settlements using central bank deposits, or central bank liabilities which have been digitized. The "general purpose CBDC" is electronic central bank money which is assumed to be widely accessible, including for individuals and firms. The "general purpose CBDC" is also a substitute for cash (banknotes and coins). The "general purpose CBDC" is categorized into two issuing forms, "account-based" and "token-based". In the "account-based" CBDC, individuals and firms open an account at a central bank and use it to make transfers between accounts, which effects payment and settlement. In the "token-based" CBDC, which is also referred as a "value-based" CBDC, users deposit CBDC to their smartphone applications or IC cards and transfer value to other users when making payments. The electronic money prevailing in Japan is categorized as "token-based" digital currency.

By the way, the "wholesale CBDC" scheme can be applied for the issuing fixed income securities, reaching the level of practical implementation. In this paper, a method issuing the digital common currency (AMRO coin) combining the "wholesale" and "token-based" schemes is proposed.

3. An example for implementation of AMRO coin

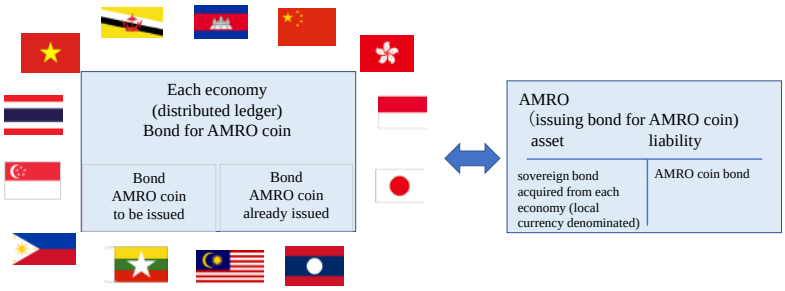
Taking a look at current technological trends, significant numbers of financial businesses and services which fully utilizing DLT are proposed and actually implemented. In this paper, "wholesale" scheme applied for bond issuance using private type DLT[11] and "token-based" scheme applicable for digital currency issued by centralized organization using blockchain technology of narrow definition[12] are

[11] "Project DLT Scripless Bond", 2017 Bank of Thailand for example.
[12] "(WO2009008105) Electronic money intended to be issued as legal currency by central bank or

combined to issue digital common currency issued by an international organization (AMRO).

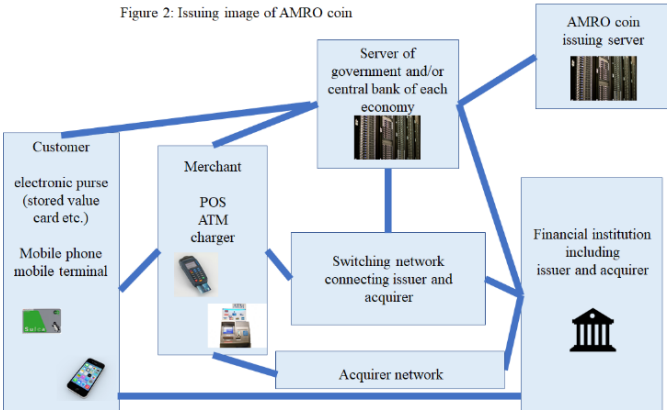
Firstly, the governments and/or central banks in ASEAN+3 provide (invest) their government bonds and/or currencies to an international organization (AMRO). Secondary, AMRO issues "Bond to issue AMRO coin" equivalent with the asset provided. Considering the situation in ASEAN+3, the bond may be "ACU denominated bond". Having said that, from the viewpoint of the "ease of implementation", "USD denominated bond" may also be adopted tentatively as a starting initiative. By doing so, governments and/or central banks in the region can have "Bond for issuing AMRO coin" on their asset side of balance sheet and will be able to issue AMRO coin up the amount. In other words, governments and/or central banks can provide AMRO coin to financial institutions, firms, merchants, and individuals of the countries/economies up to the amount of "Bond for issuing AMRO coin". More specifically, when AMRO coin issued, the exact amount of "Bond for issuing AMRO coin (entitlement)" moves from proprietary account to customer account of "Bond for issuing AMRO coin" (refer to Figure 1).

Figure 1: Bond for issuing AMRO coin



As explained the above, information for issuing AMRO coin can be shared transparently among the governments and central banks in ASEAN+3 by applying private DLT. Creating AMRO coin itself will be done by AMRO coin issuing body (AMRO) centrally just like the "ASEAN+3 AMRO coin issuing printing works/mint" in order to secure interoperability of AMRO coin in the region (refer to Figure 2).

Figure 2: Issuing image of AMRO coin



When issuing AMRO coin in each country/economy, AMRO coin should be circulated as value stored in a physical device or hardware such as electronic wallet and/or vault having sufficient tamper

institution having function equivalent to that of central bank and electronic money system" 2007, Taiji Inui for example

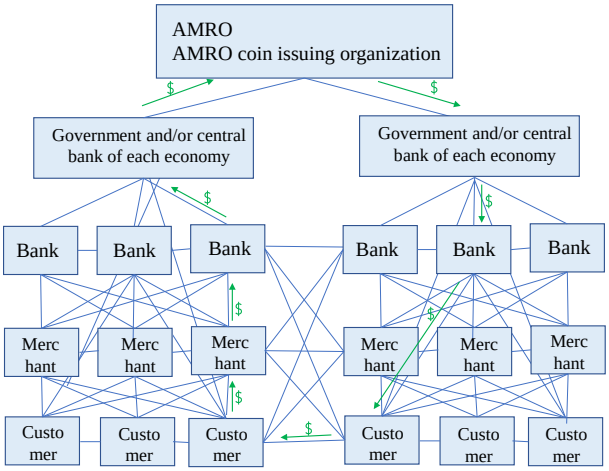
resistance (such as contactless smart card and NFC[13]) protected by strong encryption (value-based digital currency).

When actually implement the AMRO coin, proven technologies such as electronic money systems in Japan and the measures using blockchain technology in narrow meaning such as “Electronic money intended to be issued as legal currency by central bank or institution having function equivalent to that of central bank and electronic money system (WO2009008105)” can be good references to provide safe and efficient AMRO coin. Could you refer to the Attachment as an example of AMRO coin issuing method, showing basic concept, structure, and characteristics of the digital currency, please?

If such an AMRO coin is implemented, cross-border remittance across the countries/economies can be realized (refer to Figure 3).

When AMRO coin issued by other governments/central banks in other countries/economies transferred (returned) to a different country/economy from the issuing one, the coin should be returned to AMRO.

Figure 3: Cross-border usage of AMRO coin



4. Creditworthiness, general acceptability, and finality of AMRO coin

When discussing the functions of CBDC as a currency, creditworthiness, general acceptance, and finality would be the most important issues. Generally, a currency issued by a central bank is a legal tender having mandatory power backed by the creditworthiness of lender of last resort. With respect to the creditworthiness of the AMRO coin without such a legal background, it needs to be guaranteed as a safe asset just as private digital currency. As explained the above, each country/economy provides asset such as bond equivalent with the amount of AMRO coin to be issued by the government and/or central bank in order to secure creditworthiness of the AMRO coin. Also, AMRO has a function and role to conduct surveillance to ASEAN+3 countries/economies and takes proper action when some issues happen after analyzing the situation and financial condition of the country/economy. Furthermore, AMRO has a safety-net named “Chiang Mai Initiative Multi (CMIM)” to support a country/economy, should something such as short-term shortage of liquidity happen in the

[13] Near Field Communication

country/economy, which would be a good evidence for AMRO having sufficient creditworthiness.

With respect to the general acceptability, this would be a most important pre-requisite for AMRO coin to be accepted as a payment instrument widely by the common people in the region. Even though cashless society has been advocated so many years in Japan, cash is still major payment instrument in the country, yet. Also, cheque is still being circulated in some countries/economies. It may be because you don't have to know additional information such as bank account number of payee when you use cash or cheque as a payment instrument. A good evidence of this is QR code payment. By scanning QR code at a merchant when buying something, you (your mobile wallet) can capture all necessary information of payee (the merchant) without entering such information by yourself, which increases user-friendliness and convenience drastically. Considering the case of AMRO coin, AMRO coin can complete payment (transfer of stored value) easily by just touching your mobile wallet (or smart card) to a POS[14] terminal or each other without entering any additional information such as account number because it is "value-based" payment instrument having the value inside the hardware. Also, AMRO coin has the finality by transferring the value from your mobile wallet to others just like cash because it is a "value-based" type payment instrument.

5. Sharing seigniorage

Since the total amount of bonds for issuing AMRO coin will be shown on the liability side of balance sheet of AMRO, equivalent value of safe asset provided by ASEAN+3 governments and/or central banks will be shown on the asset side of the balance sheet of AMRO. The profit obtained from the asset (management) will be distributed to the ASEAN+3 countries/economies as seigniorage[15] after deducting operational cost and savings for future enhancement and maintenance. In other words, profit obtained from the operation (management) of the asset for AMRO coin issuing will be shared with the ASEAN+3 countries/economies based on the period of AMRO coin staying in the country/economy. The period staying in a country/economy for each AMRO coin can be calculated from the history of the coin. As described later, for the dollarized countries/economies it will be a benefit to obtain seigniorage of issuing AMRO coin, though for the countries/economies which issue their own currency may not get much benefit considering the possibility of reducing the amount of their own currency.

6. Benefits of AMRO coin

[14] Point of sale

[15] Seigniorage could be distributed to central banks in the region as a coupon of the bond.

The introduction of digital common currency, AMRO coin, would give us various advantages. The main advantages come from (1) being a digital currency, (2) being a cross-border common currency, and (3) being a publicly managed currency rather than a private currency.

(1) Reduction of fee (commission) for international (workers) remittance

As mentioned before, cross-border workers remittance may be able to be securely completed freely with little or no commission (fee). Particularly, when international remittance with mobile phone is implemented, cross-border transferability of AMRO coin will be secure and convenient. Also, it may be used for micro-financing both to conduct finance and get refunded.
Furthermore, with AMRO coins, remittance between companies will be cheaper than before. In the ASEAN + 3 regions, since the supply chain is well developed, the production and sales of companies are already integrated across the border as a region. Institutional development such as FTA (Free Trade Agreement) has promoted intra-regional trade. Meanwhile, financial services were segmented. The development of a regional wide payment system using a digital common currency will provide financial services that respond to the progress of economic integration in production and trade.

(2) Stable monetary policy implementation for developing (particularly dollarized) countries/economies

If AMRO coin is adopted as a legal tender in a country/economy whose monetary policy is not stable, AMRO coin (ACU) may offer a reasonable way to conduct stable monetary operation. As already mentioned, stable seigniorage will be secured for dollarized countries/economies.

(3) Reduction of social cost

By introducing AMRO coin, social cost may be able to be reduced. Generally, digital currency like AMRO coin has high user-friendliness and convenience reducing service time at a merchant such as operation time for POS machine etc., which could reduce workload and time for payment. Also, if AMRO coin is widely accepted, it could be an alternative payment instrument for physical coin, which will also reduce handling cost and workload of physical coin.

(4) Securing safety and security

AMRO coin is much secure that the private virtual coin stored and managed by virtual currency

exchanges, because AMRO coin is protected by not only cryptographic measures (encryption) but also physical hardware with tamper resistance (IC chip such as NFC). AMRO coin will also have measures to address the requirements from Financial Action Task Force (FATF) and Bank Secrecy Act (BSA) without having negative effects for anonymity.

(5) Prevention of direct and physical transmission of infectious diseases

When cash is used as a payment method, it is generally handed over, and there is a risk that viruses and pathogens will be physically and directly transmitted via cash[16]. On the other hand, when using digital currencies such as AMRO coins, (i) contacting a card or mobile device with a built-in NFC (contactless IC chip) with a POS terminal, (ii) mobile device or terminal By reading the QR code with the attached scanner, (iii) electronically transferring between mobile devices, etc., the currency (data) is transmitted without physical intermediaries, and payment is completed. Therefore, by using AMRO coins, direct transmission of viruses and pathogens can be considerably contained.

(6) Providing fair services

Some countries/economies in ASEAN+3 issue a unique card linked with a unique number such as national ID and social security number for all people (nationals) of the countries/economies. If such a national ID and/or social security number can be stored safely in a chip (NFC for example), AMRO coin can also be saved in the chip securely. As such, all people (nationals) in the country/economy will be able to have electronic wallet for AMRO coin. Government payment and expenditure such as social welfare and pension can be transferred to the electronic wallet. The wallet can be used for receiving workers remittance from outside country/economy, too.

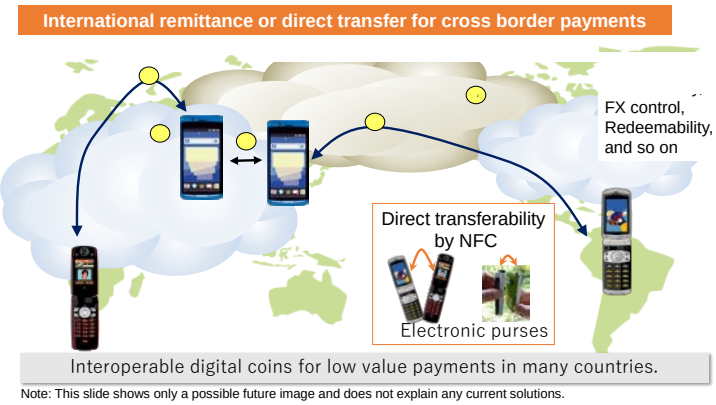
(7) Vitalizing regional activities and enhancing globalization

Through the discussions by the government agencies and central banks particularly AMRO in ASEAN+3, regional activities will be expected. A future topic such as currency unification could be a topic of discussion if environmental conditions become mature in the future. It is especially important to be managed in a multilateral framework. In a multilateral framework, as in the case of the European

[16] However, Auer et al. (2000) points out "Scientific evidence suggests that the probability of transmission via banknotes is low when compared with other frequently-touched objects, such as credit card terminals or PIN pads."

Central Bank, large and small countries have equal voices. International currencies are an global economic infrastructure that can avoid the inadequate situation in which large powers dominate international currencies.

This concept may be applicable for more global range if ASEAN+3, AMRO, and ACU are replaced by G20[17], IMF[18], and SDR[19], respectively (refer to Figure 4).



Note: This slide shows only a possible future image and does not explain any current solutions.

(8) "Common currency" and not "single currency"

In this proposal, it is assumed that AMRO coins and national currencies are simultaneously circulating in each country (economy). In the case of Europe, in 1998 the national currencies were integrated into a single currency, the euro. At the same time, it aimed to make the European financial market a single market. This reflected the strong political will toward economic integration in Europe at that time. The single currency had the great effect of making Europe's financial markets efficient, but it was regarded as a drawback to deprive the member countries of monetary policy freedom. On the other hand, the situation in which a common currency coexists with national currencies is complicated and inferior to a single currency in terms of financial market integration. However, such situation would be more appropriate because it is more flexible system that maintains the degree of freedom in monetary policy to some extent, and that political will is relatively weak in East Asia compared to Europe.

7. Remaining challenges and possible next steps

When AMRO coin actually being used, there remain some challenges yet. One of the challenges is penetration of mobile wallet with secure IC chip such as NFC in AEAN+3. With respect to the general acceptability, it is expected to provide (distribute) contactless smart card with secure chip such as NFC having national ID inside to entire people (nationals) free by the government in ASEAN+3. Also, distribution of terminal and/or tablet to read such information from the smart card for payment and

[17] Group of twenty
[18] International Monetary Fund
[19] Special Drawing Right

other business purpose. Where AMRO coin operation center and its backup site located could be a serious political challenge. Interface specifications and application interface (API) for the POS terminals and with other devices will also be a challenge. In order to make AMRO coin concept to upgrade to actual implementation initiative, some technical challenges remain. Followings are possible remaining challenges from business practice perspective; (i) the framework for each government and central bank invest to AMRO (legal background, budget, and process), (ii) internal regulation for AMRO to conduct such an operation as a printing works/mint of AMRO coin, (iii) cooperation and competition with other CBDCs and/or virtual currencies, (iv) competition with current banking system in particular with big banks, and (v) possible impact to monetary operations. When issuing AMRO coin as currency in ASEAN+3, a basket currency unit such as ACU may be ideal way. Having said that, considering the enormous workload and time needed for starting euro in Europe, it may be extremely difficult to issue AMRO coin denominated as ACU. Therefore, as the first stage, a regional (AMRO) coin denominated in USD may be possible practical way. Moreover, new currency services such as Libra (basket currency) may be a good reference technologically and operationally to be surveyed and reviewed. As such, in order to implement AMRO coin, it may be suggested that a survey team be established and study this issue for one or two years. Then, the study results may be reported to ASEAN+3 Deputies' meeting and Finance Ministers and Central Bank Governors' meeting through ABMI. Anyway, it may be advised that a organizational framework to discuss this issue be established in ASEAN+3 and AMRO.

8. Conclusions

Issuing digital currency itself has already reached a practical stage of implementation technologically. However, it may need further discussions to issue it as the legal tender of a country/economy. Having said that, considering the characteristics of the digital currency, it may be a possible way if it is used (i) as a measure for small value cross-border remittance and (ii) prepaid "value-based" payment instrument, circulating in ASEAN+3 region. Considering the trend in ASEAN+3 where financial and economic activities across the border have been increasing drastically, the introduction of regional common digital currency such as AMRO coin would be beneficial for the region supporting cross-border transactions providing the convenient way of payment and remittance to the people working in different countries/economies.

Furthermore, if AMRO coin is well accepted by the society and has increased creditworthiness, AMRO may be able to issue AMRO coin exceeding the asset obtained from the ASEAN+3 governments and central banks in the future.

Reference

Auer, Raphael, Giulio Cornell and John Frost "Covid-19, cash, and the future of payments" BIS Bulletin No3, Bank for International Settlement, 2020

Adrian, Tobias and Tommaso Mancini-Griffoli "The Rise of Digital Money", FinTech Notes No. 19/001, International Monetary Fund, 2019

Amemiya, Masayoshi, "Should the Bank of Japan Issue a Digital Currency?", Bank of Japan, 2019,

Bank of Thailand, "Project DLT Scripless Bond", 2018,

Bank of Thailand, "Inthanon Phase2", 2019,

Brunnermeier, Markus K., Harold James, Jean-Pierre Landau, "The Digitalization of Money", Working Paper 26300, National Bureau of Economic Research, 2019

Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, "Security of Electronic Money", Bank for International Settlements, 1996, ,

Inui, Taiji, "Electronic money intended to be issued as legal currency by central bank or institution having function equivalent to that of central bank and electronic money system (in Japanese)" 2007,

Inui, Taiji, "A proposal to start a survey on electronic coins as a common currency issued by an international organization choosing SDR as the currency unit (proposed to BIS)", 2010,

Inui, Taiji, "Common Electronic Coin (Proposed to IMF)", 2014

Ishida, Mamoru, "Exchange Rate Instability: Japan's Micro-Macro Experiences and Implications for China", China and World Economy, Vol.14, No.2, Institute of World Economics and Politics, Chinese academy of Social Sciences, 2006,

Ishida, Mamoru, "Revisiting East-Asian Community -- From Functional Approach to Institutional Approach", International Economic Review, Institute of World Economics and Politics, Chinese Academy of Social Sciences, 2014,

Lagarde, Christine, "Winds of Change: The Case for New Digital Currency", International Monetary Fund, 2018,

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System, 2008,

Nakayama, Yasushi, Hitemitsu Morihana, Masayuki Abe, **and Eiichiro Fujisaki.** "On Measures to Implement Electronic Money (in Japanese)", Bank of Japan, Institute of Monetary and Economic Study, 1997

Nakayama, Yasushi, "Electronic Money Technology and Patent", Institute of Monetary and Economic Studies, Bank of Japan, 1998

Release master, "Hyperledger Fabric Docs", Hyperledger Fabric, 2019

Study Group on the Virtual Currency Exchange Services, "Report from Study Group on Virtual Currency Exchange Services", Financial Services Agency, 2018,

Takahashi Wataru, "Financial Cooperation in East Asia: Potential Future Directions" Chap 2 in "Trade, Investment and Economic Integration of Volume II for Globalization, Development and Security in Asia", World Scientific、2014

Takahashi, Wataru, "Reviving Yongle coin (Eirakusen): The Future of Money and Asian Digital Common Currency (in Japanese)", Financial Forum, Kyoto Bank Economic Rearch Institute, 2020,

Takamura Yasuo, Syunji Ikuta, and Ryotaro Sawada, "Regional Financial Cooperation Related Meetings in Asia", Ministry of Finace, 2018,

Yanagawa, Noriyuki, and Hiromi Yamaoka "Digital Innovation, Data Revolution and Central Bank Digital Currency", The Bank of Japan Working Paper Series No. 19-E2, the Bank of Japan, 2019

Attachment

Electronic money and the electronic money system intended to be issued as legal tender by a central bank or an institution having function equivalent with the central bank (Preliminary draft)

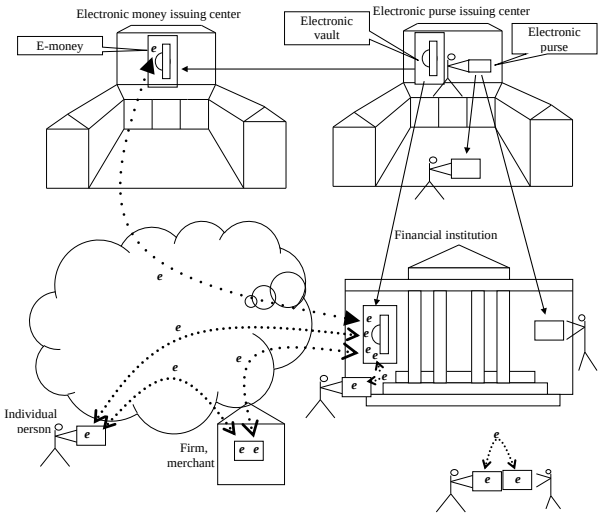
Technologies to be used for the electronic money to be used as a legal tender and/or common currency issued by central banks and/or international organizations having equivalent functions and/or roles are described here. More specifically, (i) electronic money issuing technology including PKI (public key infrastructure), (ii) electronic money storing technology safely and securely including electronic purse and electronic vault, (iii) electronic money transferring technology between electronic purses safely and securely using encryption, and (iv) counterfeit electronic money detection technology utilizing history of transfer (block chain using PKI) are discussed hereinafter.

Note: This attachment describes salient points of the concept applied for the patent in 2007. Since there was no terminology “digital currency” at that time, “electronic money” is used instead of “digital currency” as a similar meaning. Also, technological elements explained here are stable at that time and can be used as proven technologies currently, too. Having said that, if this concept can be further studied, it is suggested that further study be conducted to utilize more relevant technologies and products to provide better (more secure, safe, and user-friendly) services.

1. Overview of Concept

Electronic money system which consists of “Electronic money issuing center” and “Device providing (Electronic purse issuing) center” as main components of the system (refer to Figure A1). Electronic money is authenticated by the “Electronic money issuing center” as the certificate authority (CA) using PKI. The “Device providing center” provides tamper resistance hardware such as electronic purses and electronic vaults authenticating those devices as the CA. In this electronic money system, all encryption keys not only private (secret) keys but also public keys are kept in a secure and safe environment without being disclosed to the outside of the system. If electronic money is counterfeit, the counterfeit money should be detected and reported to predetermined organization in predefined way to handle such an incident timely. “Electronic money issuing center” should be operated by central banks or an international

【figure A1】 Overall concept and structure



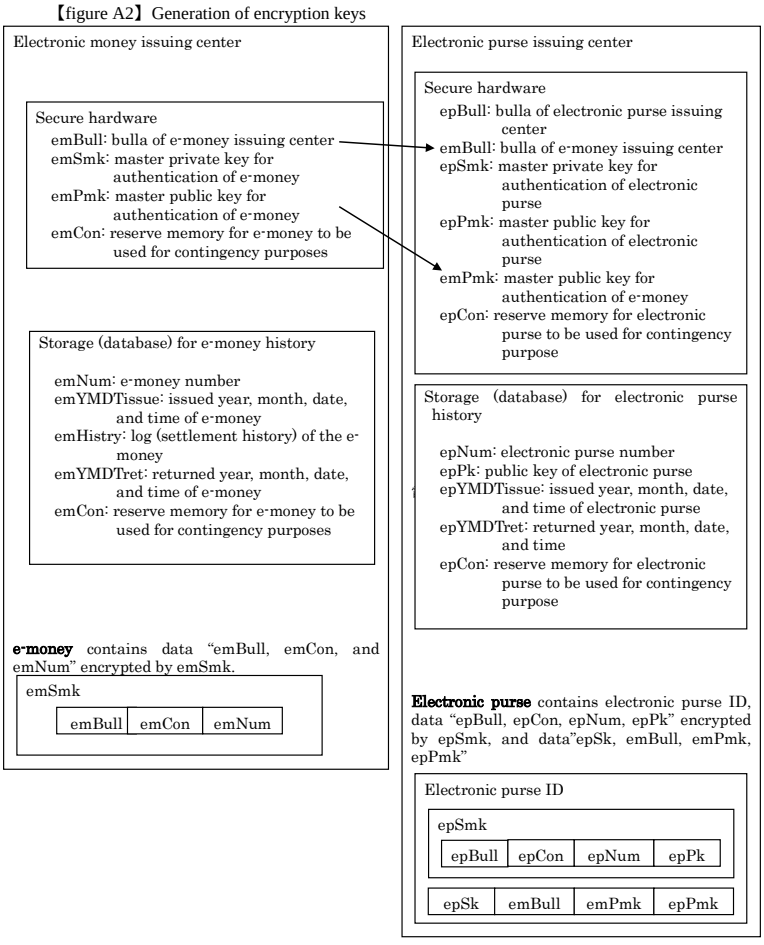
organization. “Device providing center” is operated by government or an international organization.

2. Issuing electronic money and electronic purse

A pair of keys, “Master private (secret) key for authentication of electronic money (emSmk)” and “Master public key for authentication of electronic money (emPmk)” are generated at the “Electronic money issuing center”. The Master keys are stored in a secure place both physical and information technology perspective (refer to Figure A2). “Electronic money number (emNum)” having sufficient digits is increased sequentially when issuing electronic money. The “Electronic money number (emNum)”, “Bulla of electronic money issuing center (emBull)”, and “Reserve memory for electronic money to be used for contingency purposes (emCon)” are put together and encrypted by the “Master private (secret) key (emSmk)” as one unit (lowest denomination) of electronic money, which means that an unit of electronic money is issued.

At the “Electronic money issuing center”, "storage (database) for electronic money history” is established to store the information of the electronic money including “issued year, month, date, and time of e-money”, “log (settlement history) of the e-money”, “returned year, month, date, and time of e-money”, and “reserve memory for e-money to be used for contingency purposes” and the “Electronic money number (emNum)” as the key of the database (refer to Figure A2)

【figure A2】Generation of encryption keys



A pair of keys, “Master private (secret) key for authentication of electronic purse (epSmk)” and “Master public key for authentication of electronic purse (epPmk)” are generated at the “Device providing center”. Also, the Master keys are stored in a secure place both physical and information technology perspective. IC chip (or a hardware having equivalent or higher level of physical security, processing functions, and data storage functions with IC chip) is provided as electronic purse at the

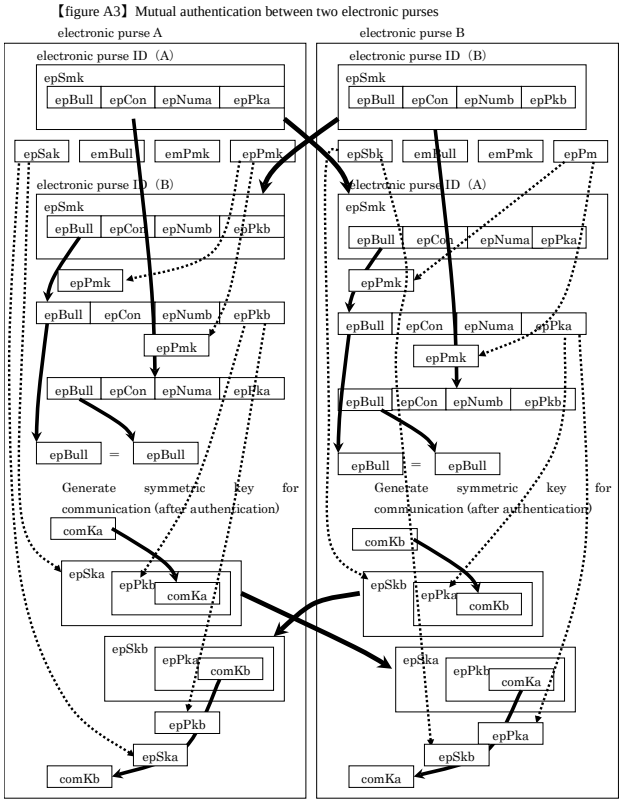
“Device providing (electronic purse issuing) center”. “Electronic purses” are issued (initially set) only at the “Device providing center”. Unique “Electronic purse number (epNum)” is allocated and stored in each “Electronic purse”.

A unique pair of keys, “Private (secret) key of electronic purse (epSk)” and “Public key of electronic purse (epPk)” are generated at the “Device providing center”. The “Public key of electronic purse (epPk)”, “Electronic purse number (epNum)”, “Reserve memory for electronic purse to be used for contingency purpose (epCon)”, and “Device providing center (epBull)” are put together and encrypted by the “Master private (secret) key for authentication of electronic purse (epSmk)”, which forms electronic purse ID.

At “Device providing center”, a unique “Electronic purse ID” is stored in each “Electronic purse”. Also, at the “Device providing center”, “Master public key for authentication of electronic purse (epPmk)”, “Master public key for authentication of electronic money (emPmk)”, “Bulla of Device providing center (epBull”), and “Private (secret) key of the electronic purse (epSk)” are stored in the “Electronic purse”. As mentioned before, “Electronic purse” should have sufficient level of security to secure the data stored. In particular, the “Private (secret) key of electronic purse (epSk)” will never go out of the “Electronic purse” once it stored.

At Device providing center, “Electronic purse number (epNum)”, “Public key of electronic purse (epPk)”, “Issued year, month, date, and time of electronic purse (epYMDTissue)”, “Returned year, month, date, and time (epYMDTret)”, “Reserved memory for electronic purse to be used for contingency purpose (epCon)” are stored in “Storage (database) for electronic purse history”.

【figure A3】Mutual authentication between two electronic purses



3. Mutual authentication of electronic purses

Electronic purses are authenticated each other as shown in Figure A3. Firstly, an electronic purse (electronic purse B) send “Electronic purse ID (B)” to the other electronic purse (electronic purse A). Then, at the electronic purse A, “Bulla of Device providing center (epBull)” is extracted by decrypting the “Electronic purse ID (B)” sent from electronic purse B

by using “Master public key for authentication of electronic purse (epPmk)”. Next, by comparing the extracted “Bulla of Device providing center (epBull)” with that (epBull) stored in the electronic purse A, authenticity of electronic purse B is confirmed by electronic purse A.

Electronic purse A is also authenticated by electronic purse B with the same procedure.

4. Generation of common encryption keys for communication between electronic purses

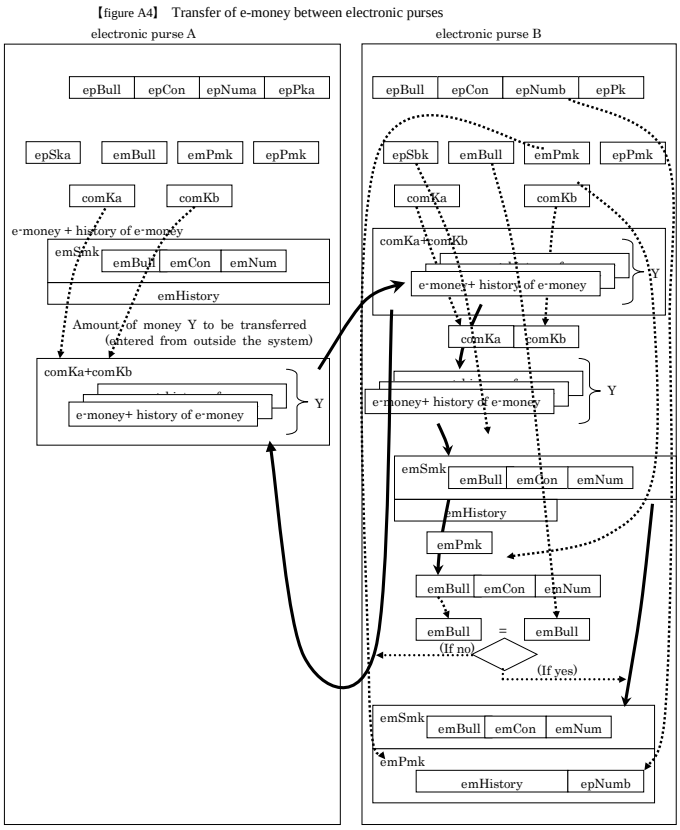
Common encryption keys for communication between the electronic purses are generated as shown in Figure A3. Firstly, after confirming the authenticity of electronic purses, electronic purse A generates a “Common encryption key (comKa)” for communication with electronic purse B and encrypt it with “Public key of electronic purse B (epPkb)” and “Pprivate (secret) key of electronic purse A (epSka)”, then sends it to electronic purse B. Secondly, after conducting same processes at electronic purse B to authenticate electronic purse A, “Common encryption key for communication (comKb)” is sent after encrypted by “Public key of electronic purse A (epPka)” and “Private (secret) key of electronic purse B (epSkb)”. Then, at electronic purse A, the “Common key for communication (comKb)” sent from electronic purse B is extracted by decrypting “Public key of electronic purse B (epPkb)” and “Private (secret) key of electronic purse A (epSka)”. By combining the common keys generated by electronic purse A and B, common key for communication between the electronic purses is generated. Common key to send data from electronic purse A to electronic purse B is to be comKa+comKb and vice versa.

5. Process of transferring electronic money between electronic purses

After establishing Mutual authentication of electronic purses and generating the common key for “Communication (comKa+comKb)”, electronic money is transferred between electronic purses as shown in Figure A4. Firstly, when sending electronic money from electronic purse A to B, same number of electronic money with specified amount are collected and bundled together. Each electronic money carries its history of transfer. Secondly, bundled set of electronic money is encrypted by the common key for “Communication (comKa+comKb)”. The encrypted set of electronic money is sent to electronic purse B. At the electronic purse B, the set of electronic money is decrypted using the common key for communication (comKa+comKb). Then, each electronic money is decrypted by “Master public key for authentication of electronic money (emPmk)” to identify the “Bulla of electronic money issuing center (emBull)”. The extracted “Bulla of electronic money issuing center

(emBull)" of each electronic money is compared with that (emBull) stored in the electronic purse B. Then, authenticity of electronic money is confirmed when the both of the emBull are same. Also, the number of electronic money is counted and confirmed that the number is equal to the specified amount (refer to Figure A4).

【figure A4】 Transfer of e-money between electronic purses



After confirming the amount received, the result is sent back to electronic purse A. If received electronic money is regarded as counterfeit money, it is sent back to the electronic purse A. With respect to the electronic money received, "Electronic purse number (epNum)" of electronic purse B is added to the previous history of transfer as new history of transfer. Then, the entire history is encrypted by "Master public key for authentication of electronic money issuing center (emPmk)" as new history of transfer.

6. Detection measures of counterfeit electronic money and electronic purse

The process to identify counterfeit electronic money at the "Electronic money issuing center" is shown in Figure A5. When returning to the "Electronic money issuing center", firstly, the electronic money is decrypted by "Master public key for authentication of electronic money (emPmk)" to extract the "Bulla of electronic money issuing center (emBull)". Secondary, the extracted "Bulla of electronic money issuing center (emBull)" is compared with the emBull stored in the Electronic money issuing center. Next, by decrypting the history of transfer of electronic money by "Master private (secret) key for authentication of electronic money issuing center (emSm)" sequentially, all the electronic purse numbers through which the electronic money has been transferred after generated are extracted and stored to the storage (database) for returned electronic money history. Then, the stored data are checked their consistency by comparing the data stored in the storage to detect counterfeit electronic money. If there is any discrepancy of the history of electronic money transfer, such information should be reported to the authorities pre-defined.

If counterfeit electronic money is found, the information such as suspicious electronic purse number related to the counterfeit electronic money is to be distributed to the devices with detection functions such as electronic vaults. Also, when such suspicious electronic money is detected based on the information, it should be informed back to “Electronic money issuing center” and “Device providing center”.

Returned electronic purses are checked at the “Device providing center”. Firstly, electronic purse ID is decrypted by “Master public key for authentication of electronic purse (epPmk)”. Then, “Bulla of Device providing center (epBull)” is extracted and compared with the epBull stored in the Device providing center to authenticate the returned electronic purse to be genuine. Also, “Electronic purse number (epNum)” is extracted and compared with all stored epNum in the “storage (database) for returned electronic purse history” to check whether the electronic purse is not duplicated. Electronic purses are recovered regularly to check the counterfeit electronic purse at the “Device providing center” comparing with the records stored in the “Storage (database) for electronic purse history”. If there is discrepancy among the records stored in the database, the incident should be reported to a pre-defined relevant authority to address the incident.

The process to identify counterfeit electronic purse at the Device providing center is shown in Figure A5.

【figure A5】Detection of counterfeit e-money