BANCO CENTRAL
DO BRASIL

WORKING
PAPER

CURRENCY IN THE DIGITAL ERA

ALDÊNIO BURGOS & BRUNO BATAVIA

JULY · 2018

Emails
aldenio.burgos@bcb.gov.br
bruno.batavia@bcb.gov.br

Authorized by: Deputy Governor for Administration
Carolina de Assis Barros

The opinions expressed in this paper are exclusively those of the authors and do not necessarily reflect the views of the Central Bank of Brazil.

Although this article represents preliminary work, source citation is required even when partially reproduced.

Citizen Service Division
Banco Central do Brasil
Deati/Diate
SBS – Quadra 3 – Bloco B – Edifício-Sede – 2º subsolo
70074-900 Brasília – DF
Tel: 0800 9792345
Fax: (61) 3414-2553
Internet: http//www.bcb.gov.br/?FALECONOSCO

Foreword

Remarkable technological advances have routinely impacted our world. The so-called digital transformation is redefining industries, making possible new business models and providing opportunities never imagined before. Its impact, however, is not limited to business; is already changing drastically the way we live, work and relate to each another.

Digitization has the potential to offer immense benefits to society and the environment, presenting a number of opportunities and challenges for companies and policymakers.

According to a study by the World Economic Forum [1], digitization has the potential to unlock near $100 trillion over the next decade for industry and society in general. However, there is no guarantee that society will capture its benefits, as several barriers must be overcome. These include outdated and complex regulatory frameworks, infrastructure gaps, lack of public confidence in innovative technologies and processes, as well as the lack of incentives to generate societal value.

In the spirit of innovation, the study aims to instigate weighing, analyzing reasons and ways to eventually reinvent the most symbolic product of a central bank: its currency.

With regard to physical cash, it is necessary to recognize its benefits and importance in the economy, particularly for the lower income population, for which, at least in Brazil, the money issued by the Central Bank is probably the only means of payment and reserve of value that they can easily access.

Nevertheless, physical money is often targeted by initiatives that seek to reduce its use, due to some well-known repercussions related to its costs and its burdens for society – e.g. with security, as well as its adoption in criminal activities of all kinds, such as corruption, money laundering and tax evasion. In addition, it is estimated that 30% of the coins cease to circulate for reasons such as loss and hoarding.

Thus, in an exploratory approach to the digitization of physical money, this academic essay intends to add value, while seeking solutions, by bringing to the reader's knowledge some of the concepts, architectures, functions and applicable technologies, as well as consolidating part of the international experience in the theme.

Therefore, under the auspices of an organizational environment of healthy stimulus to reflection and innovation, we bring to public knowledge the study "Currency in the Digital Era", in order to humbly contribute with the development and critical mass on the subject.

Rio de Janeiro and Brasilia, July 06, 2018.

Aldênio Burgos and Bruno Batavia

1 Introduction

The current availability and omnipresence of electronic devices and high-speed networks has motivated several central banks and monetary authorities to explore the idea of issuing their sovereign currency in a digital format.

Like cash, this type of digital currency could be: (a) fixed in nominal terms; (b) universally accessible; and (c) valid as legal tender for all public and private transactions. Consequently, an official dematerialized currency is essentially different from virtual currencies created by private entities, such as Bitcoin, whose market prices have fluctuated markedly in recent years.

2 Purpose

We believe that the creation of a system capable of allowing broad access to the national sovereign currency in a digital format should, among other things, improve:

- the efficiency of the monetary function and the underlying payment processes and systems;
- the level of financial inclusion; and
- the general user experience ("ux") - translated into lower "friction" and greater consumer protection.

Under these conditions, we studied forms of digital issuance of a fiduciary currency (5), hoping to minimize uncertainties and risks, as well as to take advantage, to some extent, of existing business models and legacy systems, without, however, abandoning innovative approaches that could bring clear benefits in terms of efficiency and inclusion for the National Financial System.

3 Context

In this section, we will explore some of the motivations that could justify the creation of a new digital support for the Brazilian currency.

As the central theme of the analysis, we believe that only an official digital currency, unreservedly accepted by the public, would have the vitality to disintermediate markets and actually supplement or even replace, in the long run, the physical money.

3.1 Heighten the efficiency of the monetary function

A "tokenized" national currency operated by a distributed payment system, depending on its design, would allow the issuer to access the transactional history, if necessary, in real time. The digital fiat currency (DFC) would thus provide more data to economic and monetary policy makers, including the ability to observe the economy's response to shocks or policy changes almost immediately and more accurately. This is useful for the macroeconomic stability management.

Such a payment solution would allow the final settlement directly between the payee and the payer at the retail level in central bank digital money. The counter-party risk would therefore be avoided, so that any type of guarantee linked to the transaction would not be necessary. Thus, this translates into the release of significant amounts of collateralized capital. To the extent that there is a shortage of good collateral in the financial market, this approach proposes important benefits to the economy.

The model under discussion should disintermediate the digital payments ecosystem and increase transparency, seeking to ensure that its transaction rates reflect more accurately the marginal cost of verification - net of any public subsidy, if provided -, as well as enabling new technologies and solutions on top of it, increasing the offer of digital payment and transfer services and reducing (or even avoiding) user costs.

In this sense, the DFC's architecture needs to be flexible enough to eventually allow the entry of new players, if desired, such as fintechs. Nonetheless, financial institutions could still play a relevant role, validating transactions and/or streamlining the onboarding of new users and services providers, something well aligned with the open banking agenda.

Therefore, as a very low-cost medium of exchange, a digital fiat currency could increase the overall efficiency of the payment system. It would be particularly beneficial to low-income families, who tend to rely heavily on physical money, but also to small businesses that incur in high costs related to cash handling or high transactional rates when making/receiving payments using cards. At the macroeconomic level, productivity gains from the adoption of a DFC would be similar to a substantial reduction in distortionary taxes.

As for the cash cycle in Brazil, a survey carried out in 2015 by "Consultoria Tendências" at the request of MasterCard with 610 merchants from large centers showed that 64% of them believe that cash transactions generate high costs. Among the reasons are (i) the need to have a trustworthy employee whose main job is to deal with money; (ii) the time lost to move values to/from the bank; and (iii) the constant threat of theft. In addition, a quarter of the respondents are insured against robbery and 60% of them know that the cost of insurance would be lower if they depended less on paper money [2].

To combat such crimes, Brazilian banks invest around R$ 9 billion annually. This amount outweighs the banks' own loss to the attacks. "The financial loss is disproportionate to the investment made by the banks", Murilo Portugal, president of the Brazilian Federation of Banks (Febraban), said. "This is one of many causes for our spreads to be bigger".

According to calculations by Diebold, a multinational manufacturer of ATMs, an ATM in Brazil is, on average, 60% to 70% more expensive than in other parts of the world. In large part, the difference is explained by the additional security devices that machines require, which is correlated with the country's violence levels [3].

In this context, the annual cost of the Brazilian cash cycle is approximately R$ 90 billion, considering the issuance, custody, wholesale and retail distribution, as well as the costs of cash handling incurred by the commerce [2].

On the other hand, we understand that credit and debit cards are not a comprehensive solution, since they are out of reach of the unbanked and often impose high transaction fees. Among Brazilians, prepaid cards are gradually gaining momentum and, although they should be able to contribute to the increase in levels of financial inclusion, they are still linked to a heavily intermediated industry, which tends to reduce the offer of more palatable rates.

Deposits - usually via "boletos", which are payment slips - are still one of the primary means by which the unbanked can make payments and engage in the digital economy. In addition, many of the services offered by payment institutions - not necessarily banks - such as electronic money/"digital wallets" (payment accounts), although desired, still lack relevant adoption.

In this sense, even though recent legal and regulatory innovations (Law 12.865/2013, Resolution 4.282/13 and Circular 3.885/18 of the Central Bank of Brazil), as well as the creation of a working group on instantaneous payments (GT-PI), aim to provide a more fertile ground for the flourish of new solutions and payment schemes in the country, there are some remaining technical barriers.

Therefore, we believe that a new payment infrastructure, with focus on interoperability, that allows transactions in a retail version of a central bank digital currency, could be the ideal interface between service providers. Such infrastructure could accelerate the adoption of mobile payment solutions - prevalent in a number of countries, such as China and India, but still timid in Brazil. In this scenario, an official digital currency could serve as a token with a unique potential for increasing the overall liquidity of this new ecosystem.

We assume that the eventual spread of the use of a digital fiat currency, in parallel with the obsolescence of cash, would discourage tax evasion, money laundering and other illegal activities facilitated by the untraceability of physical money - in particular, high-value notes. This benefit is important is even more relevant in developing countries, where a significant fraction of the economic activity is informal and mainly conducted through the use of cash.

Finally, we can highlight some potential environmental benefits brought about by the reduction of the cash supply, in view of the consequent decrease in the consumption of raw materials and fossil fuels, particularly in the stages of production and distribution of national currency. As for the sorting and destruction processes of unfit banknote, we could avoid the generation of hundreds of tons of waste. In this sense, for illustrative purposes, we estimate that, during 2017, 1,189 tons of banknote waste were generated in Brazil.

3.2 Increase financial inclusion

Digital payments serve as a gateway to financial citizenship, since a myriad of services come from this channel. Therefore, we believe that a digital fiat currency could be one of the key drivers of financial inclusion.

In Brazil, according to the Global Findex Report (2017) [4], 70% of adults have a bank account (age: 15+). As for the 30% unbanked: (i) 32% say they do not have accounts because there are no financial institutions close to their homes; and (ii) 57% claim to have no account because of the high costs of financial services. Still, according to the same survey, only 58% of the Brazilian adult population reported having made or received digital payments last year.

Data from the World Bank [5] show that 92% of Brazilian adults (age 15+) have access to mobile phone or residential internet, thus generating an opportunity to integrate around 34% of the population, if a digital fiat currency is successfully deployed.

In addition, it is important to emphasize that even many of the citizens with access to bank accounts in Brazil can not rely on electronic channels to transfer funds, since financial institutions sometimes charge very high rates in these types of transaction (e.g. "TED" and "DOC", which are two of the most well-known methods countrywide). This situation is aggravated when we consider that low-income citizens generally have reduced ticket sizes and the electronic transfer rates are fixed - not 'ad valorem'.

3.3 Improve user experience ("ux")

In Brazil, a major disadvantage brought by recurring robberies of ATMs, commercial banks and postal banks is the emergence of "cities without money", being small towns in remote regions of the country without any channel for cash withdrawal [6].

When we think about security issues and possible damages to the physical integrity of clients and employees in the Brazilian cash cycle, we conclude that eventual trade-offs related to the exposure of cyber-security risks related to digital payments seem easy to address. We must also consider some great advances in the maturity of digital payment security solutions - such as new industry standards proposed in the last couple of years by the “FIDO Alliance” [7].

It should also be noted that, in general, when dealing with coins in specie, the user experience (ux) is often poor. This is experienced globally. In this sense, the increasing levels of hoarding, taking huge amounts of coins out-of-circulation - about 30%, in the country [8], corroborates this idea. In addition, we highlight the high production and logistical costs of this item when compared to its low face value.

Finally, we point out that the new trends are causing several countries to consider the digitalization of their currency, to engage and facilitate new forms of transactions. Some of them are: (i) “Invisible Finance” (e.g. Uber and Amazon GO), which rely on mobile payments; (ii) the so-called Internet of Things (IoT), which translates into machine-to-machine (M2M) transactions over the Internet; and (iii) “Smart Contracts,” which are encrypted agreements that can automatically move money if specific conditions occur.

4 Taxonomy

According to recent studies of the Committee on Payments and Market Infrastructure (CPMI) of the Bank for International Settlements (BIS) [9], there are ten basic properties that distinguish different types of money. Keeping in mind the Brazilian context, we list them below, as well as propose the addition of a new item to the list, which is related to the function of the cash:

- **Form**: Money can have a physical support, such as paper money; or digital, such as the checking account balances.
- **Issue**: Money can be issued by a central bank or other entities, such as the case of cryptocurrencies that are issued in a decentralized manner by miners.
- **Accessibility**: Money can be broadly accessible to the population such as paper money, or be restricted to a group such as the Brazilian Payments System (SPB) bank reserves.
- **Technology**: There are two basic technologies that pertain to value representation. In this regard, money can be based on accounts, such as bank reserves, or, it can be based on tokens that store value, such as paper money.
- **Availability**: The physical cash has full availability, that is, it can be moved 24 hours a day every day. In its digital form, money may have full or restricted availability, such as bank reserves that are only available during the operating hours of the Reserve Transfer System (STR) in Brazil.
- **Duration**: The duration is the lifetime of the cash, and may be indefinite as in the currency notes, or limited, as for example in a digital money that was created, issued and redeemed daily.
- **Anonymity**: Anonymity refers to the degree of privacy in relation to possession and use. Physical money is completely anonymous. Account-based digital money is not anonymous,

since the depositary institution has full access to its information, and may or may not guarantee the secrecy of balances and transactions with third parties. In digital money based on tokens, in principle it is possible to reach different levels of privacy depending on the architecture adopted.

- **Limits**: This property is related to the existence or not of limits on the monetary amount that can be transferred and stored in digital cash implementations.
- **Transfer Mechanisms**: This option defines how the money transfer operation will take place. The move can be made directly between the parties, called peer-to-peer, or use an intermediary such as a central bank or another participant in the financial system.
- **Interest Incident**: As in bank reserve balances, it is possible to incur interest (including negative) interest on the digitally stored amount. This decision may encourage or discourage the demand for digital money.
- **Function**: Money, in physical or digital format, serves essentially as a means of exchange, reserve of value and unit of account. Recent initiatives such as cryptographic assets issued by governments, when moving away from at least one of these core functions, should not be confused with a digital fiat currency - generally speaking, they are often mechanisms for fund raising and/or speculation.

5 Model

The model studied here proposes a digital form of money issued by the central bank. It would be broadly accessible to the population, based on tokens, with full availability, indefinite duration and subjected to the limits established by the Central Bank of Brazil itself. Its transfer mechanism would be point-to-point, without interest incidence, with the privacy of balance and transactions guaranteed by banking secrecy. Despite following such definitions, the architecture that supports the new digital money is flexible enough to allow for many different configurations.

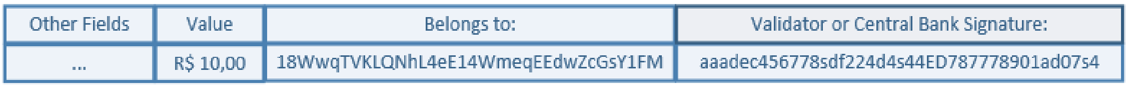
The Brazilian National Financial System already operates with digital representations of monetary values. However, physical money remains one of the main means of payment for retail operations and its life cycle is very onerous. This study devotes its attention to a new central bank digital money, focusing on retail.

5.1 The token

The Digital Fiat Currency would be formed by small digital signed registries called tokens, able to represent the ownership of an arbitrary value by a person or legal entity, see figure 1. Such digital records would circulate through the financial system and society.

The token can be used as a reserve of value while stored in some non-volatile electronic media or as an exchange instrument when transferred between parties through its protocol. This digital record can be understood as a small file.

Any digital currency for its use as a means of payment depends on a minimum infrastructure of electricity and telecommunications. This necessary infrastructure is already in a expansion process driven by the increasing demand generated by new technologies.



Other Fields	Value	Belongs to:	Validator or Central Bank Signature:
...	R$ 10,00	18WwqTVKLQNhL4eE14WmeqEEdwZcGsY1FM	aaadec456778sdf224d4s44ED787778901ad07s4

Figure 1: Simplified token model.

According to data from Brazilian Institute of Geography and Statistics (IBGE), urban areas concentrate 84.35% of Brazilian population [10]. The National Telecommunications Agency (ANATEL) has established the rule that coverage of the mobile service must be at least 80% of the urban area of its municipalities, for all operators. The fulfillment of these obligations by the providers is monitored periodically by the supervision of the Agency [11]. Also according to January 2018 data from Anatel, Brazil currently has 236.2 million mobile lines, of which more than 217 million have access to a sufficient data connection for the operation of the Digital Fiat Currency (DFC) [12].

In the event of an unavailability in the telecommunications infrastructure in a specific area or for a short period of time, the proposed solution can still be used, however, in sub-optimal mode (item A.4.3). Users who do not have smartphones could use the digital currency on their computers, on shared phones, or through digital wallet services provided by third parties.

In extreme circumstances, the user can still use physical money as an alternative. The implementation of this digital currency would not determine the immediate extinction of tangible cash, as it is only a step towards the future. A long transition phase must be carried out until the necessary infrastructure for its full operation is unequivocally served throughout the country.

5.2 Function

The official digital money would function as a large distributed computing system where multiple actors perform different roles to ensure a fluid, correct and timely movement of the dematerialized values. The interaction between the actors takes place through various software, by different types of connections, including the Internet, all according to the rules and protocols defined by the monetary authority.

The figure 2 shows the main roles of the DFC system. The lines between the parties represent communication channels that can be established during the operation of the system.

There is no direct link between the Central Bank and non-financial institutions: any relationship between the Central Bank and society is intermediated by financial institutions, just as with physical cash. The central roles of the monetary authority and the layered organization of the financial system remain preserved.

It is worth highlighting the presence of the validating institutions in the figure 2. This is a crucial new role in this digital currency model, as it is responsible for the reliability and finality of each transaction. The validation role assignment to financial institutions is optional. It is technically possible for the central bank itself to exercise this role exclusively. However, as more validators are participating, and the more distributed they are in different data centers, the greater the resilience and performance of the digital currency as a payment system.

Within the token (figure 1), as it is called the digital cash instrument, the owner of the declared value is defined by a cryptographic identity. This identity could be, for example, the public key of a digital certificate possessed by the token owner. To be considered valid, the token must meet a set of technical rules (which are outside the scope of this document) and must be consumed, only once, by a transaction signed with the private key linked to the cryptographic identity of its owner.

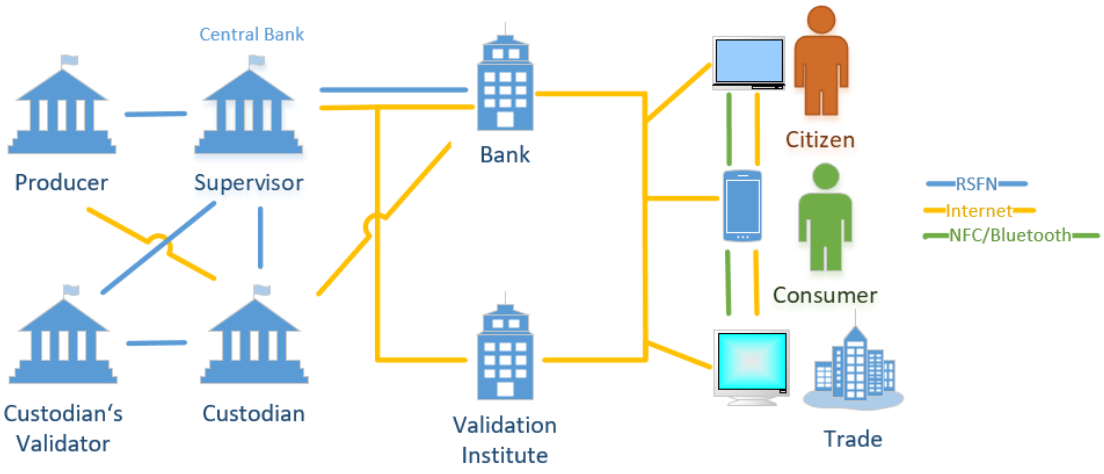


Figure 2: Digital Ecosystem.

The validity of the token is ultimately guaranteed through the digital signature of a validating institution, be it the Central Bank or another institution on its behalf. While operated according to the definitions of the proposed model, such tokens have functions and characteristics very close to those of a physical sovereign currency.

5.2.1 Issuance

The control of the digital cash issuance is exclusive to the monetary authority. According to its policies, the Central Bank could determine in what quantities and amounts the Digital Fiat Currency (DFC) should be produced.

The choice of the responsible institution that would produce new amounts of digital cash (through the specific software) is mainly a policy decision. It is technically possible for the Central Bank of Brazil itself to play this role. The producer, however, must keep the digital certificate and new tokens securely.

This step has its parallel in the production of the physical currency.

5.2.2 Custody

Digital values are born linked to a cryptographic identity. Such identity must belong to the institution chosen to act as custodian of the new cash form. Again, the choice of such an institution is a policy decision, and it is technically feasible for the Central Bank itself to accumulate this role.

The custodian receives the newly produced digital currency from the Central Bank, or directly from the chosen producer, then validates it and ensures its safety. The security of the digital cash data and the custodian certificate are its responsibility.

The tokens in custody are stored by specific software until a withdrawal is requested by a bank and authorized by the monetary authority. We can see a direct relationship of this stage with the logistics of the physical money, as shown in figure 3.

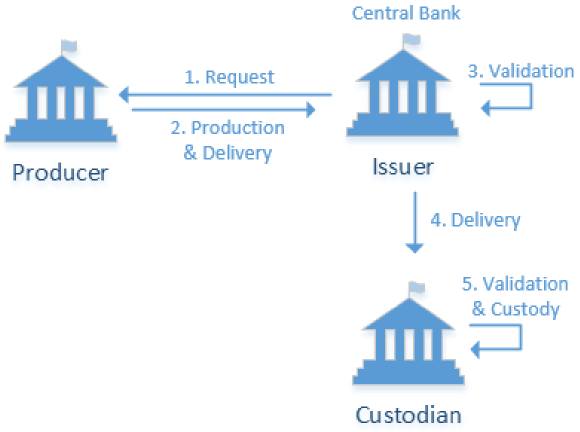


Figure 3: Simplified emission scheme.

5.2.3 Bank account opening

Financial institutions should register the public keys that will represent the cryptographic identities of their digital cash stocks in a Central Bank system for digital currency accounts management. Once registered and authorized by the Central Bank, banks will be able to operate, receive and keep linked to these accounts the values needed to serve their customers.

The amounts stored in the bank's DFC stock accounts would follow rules and controls similar to those applied to the physical custody of cash by Banks.

5.2.4 Withdrawal from bank reserves

To request a digital cash withdrawal, financial institutions (FI) should send a specific message of the Brazilian Payment System (SPB) to the Central Bank of Brazil, informing, among other things, its digital fiat cash account (section 5.2.3) of destination. The tokens referring to the amount withdrawn from the bank's reserves can be transferred also via a specific SPB message. These messages have not been implemented yet, their definitions should be part of an in-depth study phase.

When triggered by such institution, the central bank should debit the banks's reserves account and trigger the custodian, requesting the transfer of the digital value demanded. The custodian should create a withdrawal transaction using the tokens in its custody, in accordance to the instructions in the section 5.2.11. Such transaction, in addition to the custodian's own digital signature, would be recognized by the institution occupying the role of Custodian's Validator, as instructed in the 5.2.12 section.

Assigning the role Custodian's Validator is again, a policy choice, however, this role should be performed preferably by the Central Bank of Brazil. All validators of the system must ensure the security of the digital certificate that grants them such power.

The digital value transferred to the FI would be in its possession, linked to its DFC account (section 5.2.3) and stored by a digital wallet software, similar to the physical money in its custody, until a new transaction takes place.

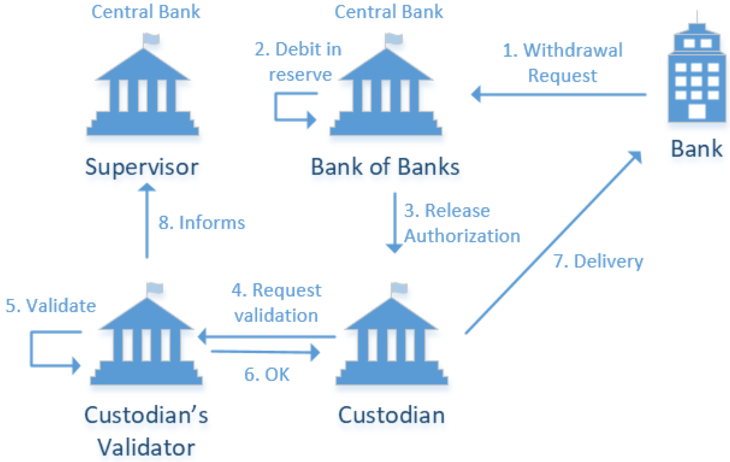


Figure 4: Simplified scheme. Withdrawal from bank reserves.

5.2.5 Personal or business account opening

All digital currency accounts (DCA) are public keys of their owners digital certificates. Personal and business DCA are opened by registering them in the DFC support system so that they are authorized to operate. Such registrations are done by financial institutes.

In the 5.3.10 item we discussed in some depth privacy and anonymity issues. The procedure described below was the one that presented the best cost-benefit ratio among the trade-offs already analyzed.

The registration of digital currency banking accounts are carried out directly by the central bank, while the other account types registrations are done by authorized financial institutions. These operations will be linked to the *"Know Your Customer"* procedure, but the actual identity of the owner of each registered DCA will be maintained by the banks and will be protected by bank secrecy.

5.2.6 Withdrawal from checking account

The withdrawal in digital currency can be carried out in person at the bank teller just as it happens with the physical money. However, it is also possible to make withdrawals remotely, through a mobile banking application, not depending on the physical presence of the client in a bank branch or ATM. To do this, it would be enough to have an internet connection and the mobile banking application interacting with the personal digital wallet application, or simply receiving the necessary information to execute the service.

When a withdrawal is requested, the bank should create a transaction, transferring ownership of the requested value to the customer. This transaction will be constructed according to the instructions in the 5.2.11 item. It will then be ratified by the validating institution, according to the instructions of the item 5.2.12. Once validated, the transaction is transferred by the bank to the customer's device, where it will be checked and later stored by her or his personal digital wallet application.

5.2.7 Physical/digital conversion

Conversions between the cash supports will depend on the physical presence of the client next to a bank teller or ATM, it can't be done remotely due to the tangibility of cash.

The digital to physical conversion may be performed automatically by ATMs regardless of whether or not there is a relationship between the customer and the ATM bank owner.

The customer should approach the self-service point of his choice, select the desired conversion options. The ATM would present a QRCode with its cryptographic identity, the requested value, and the the transaction address. The customer's digital wallet application would prepare the transaction correctly, sending it to the address given by the terminal.

The bank, in turn, would send the transaction for ratification by the validator, according to the instructions of the item 5.2.12. Once the transaction has been validated, the bank can make available the agreed amount in paper money to the customer. This procedure should not take more than a few seconds.

The exchange of physical money for digital could have a similar flow, in the opposite direction, but it depends on the confirmation of the cash delivered veracity, a function usually performed by humans or sensors (ATMs).

5.2.8 Transfer

With digital money stored in a digital wallet app, the DFC user can make payments, transfers and deposits. The transfer of digital cash between users does not depend on the geographical location of those involved. Several data communication channels can be used to transfer tokens to the payee, for example, e-mail, instant messaging systems like WhatsApp, or even another direct connection protocol between personal digital wallet applications.

To start a transfer, a QRCode would be offered by the payee (even through internet) containing one of their digital currency accounts. The same QRCode could also inform the value to be transferred, its validator of preference and an electronic address for delivery. With these information, the customer's digital wallet would produce new tokens from the tokens it possesses, as described in 5.2.6. So the customer transfers the transaction to the payee, which must submit it to the validating institution.

If the credited wallet cannot connect with the validator for any reason, he can ask the client to ratify with the validating institution before delivering the new tokens. However, nothing prevents the two from requesting the validation of the same transaction to the validator: the second-arriving request will consume few resources and will be instantly confirmed. In the figure 5 we can see a schematic of these alternative paths.

The transfer of values between two users of the digital cash system occurs in a distributed and peer-to-peer manner between the parties involved. However, at least one participant needs to connect to the validator defined in the token to request invalidation of the tokens consumed and validation of the new tokens.

In order to improve the system performance and credibility, the cryptographic identities of the official validators should be widely disseminated by the Central Bank of Brazil. Those public keys should also be stored along with their electronic addresses in each digital wallet application before it can operate with such validators. The credited digital wallet application may consider the

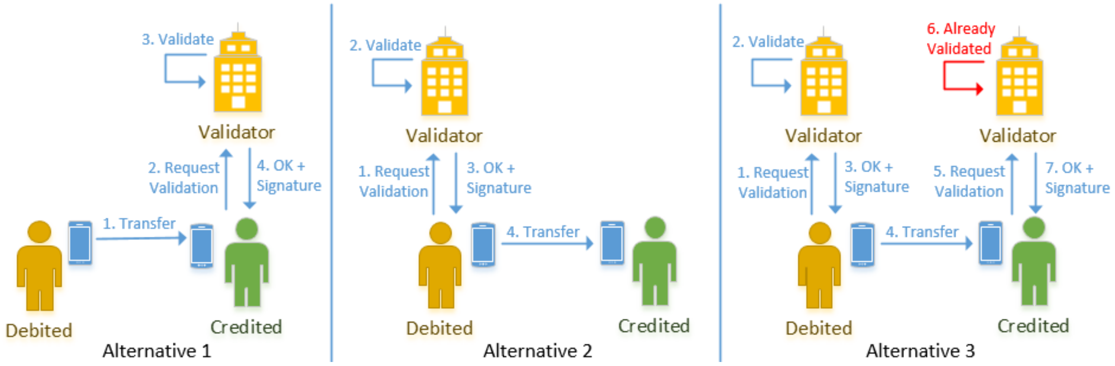


Figure 5: Alternative validation paths.

transaction finalized, when it confirms the signature of the official validator defined in the token itself. The list of validators and their addresses should be updated periodically by the digital wallets using an official service created for this purpose.

5.2.9 Payment

The payment transaction is very similar to the transfer transaction, described in the item 5.2.8, with the following differences:

- The credited digital cash account may be of the commercial type (item 5.3.13).
- New fields can be added to reference, for example, the customer's number, in case of ticket payment.
- Fees or taxes collection can be automated.
- Specific limits can be assigned.

5.2.10 Deposits

The digital fiat currency deposit in checking accounts can be performed in person, at a bank teller or ATM, or remotely, via integration between the personal digital wallet and the mobile banking applications.

The operation of deposits does not differ from that of a transfer(item 5.2.8). Here the debited DFC account belongs to the depositing client and the credited DFC account belongs to the chosen bank. The deposit transaction, as well as the payment transaction (item 5.2.9), allows the inclusion of auxiliary fields that, in the case of a deposit, identify the savings or checking account that should receive the value.

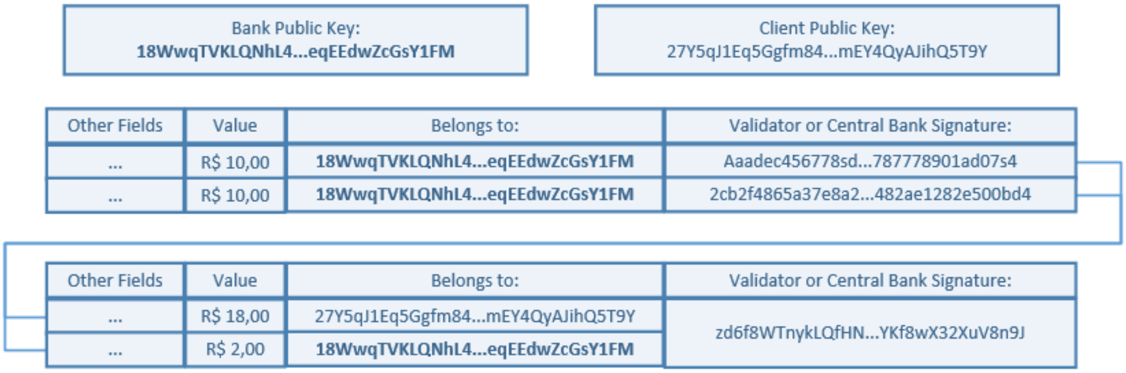
A bank, in turn, may find itself over-stocked with digital cash. To make the transfer of the extra value to its bank reserve, it must follow similar procedure, except that it will send the validated transaction to the Central Bank through specific message of the SPB, for safety reasons.

5.2.11 Token union and unbundle

Every transaction in digital currency involves the transfer of values between two accounts, the source account and the target account. Transaction type defines validation rules, optional fields and which types of accounts can be present at these two ends.

Each new transaction generated, regardless of its type, will consume one or more tokens from the source account. These are the input tokens of the transaction, which will be summed and, from the result, one or two new tokens will be generated. These are called output tokens. One of the output tokens will always display the value be credited to the target account. The other, if present, will have the remaining balance of the sum of the input tokens, and will be linked to the originating account.

The sum of the generated tokens must be equal to the sum of the consumed tokens. The creation or destruction of digital money through its use is forbidden. Although other combinations are possible, in this model we propose to limit the maximum number of input tokens to 255 and outgoing tokens by up to two for each transaction.



Bank Public Key:
18WwqTVKLQNhL4...eqEEdwZcGsY1FM

Client Public Key:
27Y5qJ1Eq5Ggfm84...mEY4QyAJihQ5T9Y

Other Fields	Value	Belongs to:	Validator or Central Bank Signature:
...	R$ 10,00	**18WwqTVKLQNhL4...eqEEdwZcGsY1FM**	Aaadec456778sd...787778901ad07s4
...	R$ 10,00	**18WwqTVKLQNhL4...eqEEdwZcGsY1FM**	2cb2f4865a37e8a2...482ae1282e500bd4

Other Fields	Value	Belongs to:	Validator or Central Bank Signature:
...	R$ 18,00	27Y5qJ1Eq5Ggfm84...mEY4QyAJihQ5T9Y	zd6f8WTnykLQfHN...YKf8wX32XuV8n9J
...	R$ 2,00	**18WwqTVKLQNhL4...eqEEdwZcGsY1FM**	

Figure 6: Simplified union model and token breakup.

5.2.12 Transaction validation

In order to promote confidence in the system, the transactions are signed by both its originator and its validator. Validators perform the role of a neutral third party, who will sign the transaction ensuring it is valid. When the transaction is considered correct by the validator, the original tokens will be consumed, becoming unfit for reuse. If it is rejected, the transaction is considered to have no effect for all purposes. Validators are responsible for the system's resistance to counterfeiting. Before signing the transaction recognizing it as effective, the validator performs the following checks, among others:

- Am I the validator of this transaction?
- Do input tokens belong to the proponent of the transaction?
- Is the sum of the generated tokens equal to the sum of the tokens consumed?
- Are input tokens being used for the first time?
- Are the values within the limits determined by the monetary authority for this type of transaction?

- Are the accounts involved allowed to perform this type of transaction?
- Are the accounts involved in the transaction all valid, active, and unblocked?
- Is the digital signature from the proponent of the transaction valid?

When receiving the token withdrawn, the recipient's digital wallet performs some simple validations, before storing the received values:

- Is the token linked to one of my DFC accounts?
- Does this token value match the expected value? (e.g. request user confirmation)
- Is the transference validator on my list of trusted validators?
- Is the validator digital signature correct?

5.2.13 Validator migration

The migration of tokens between the validators allows for a better distribution of responsibility and load within the validation process. It is technically possible to migrate active tokens to other validator by creating a specific transaction for that, or simply allowing any new token to freely specify its validator, regardless of the transaction type.

If a specific transaction is created, the validator migration would always have one or more input tokens and a single output token whose value would be equal to the sum of its inputs. All tokens, both incoming and outgoing, would belong to the same DFC account, but the outgoing token would have a different validator than that from the incoming tokens.

If validator migration is allowed in all transactions, each token of the digital currency would have within itself the cryptographic identity of its validator. Because tokens are digitally signed from their source, there is no way to change the identity of the validator without invalidating the digital signature and the token itself. However, with each new transaction there will always be tokens consumed and new tokens created. Each of these new tokens can be linked to a different validator, regardless of the validator of the source tokens.

5.2.14 System supervision

The central bank, in the role of supervisor, would receive from all validators a copy of each confirmed transaction. Thus the Central Bank would have access to the Directed Acyclic Graph (DAG) of all tokens, consumed and actives.

This transmission should be done in such a way that, if the Central Bank gets disconnected, the validators would not cease their work and the DFC system would not have a hiccup. They should be able to send the validated transactions to the central bank as soon as the it is online again with delivery guarantee.

With such a mechanism of communication between the validators and the Central Bank of Brazil, the later would have instruments to:

- Monitor the economy in near-real time.
- Supervise and monitor the behavior of validators.
- Replace a validator in case of systemic failure or catastrophe related to the validator's data center.

- To recover a validator's database from a disaster.
- Calculate some kind of remuneration for services provided by validators.
- Provide banks with a funds recovery service for their customers.
- Provide banks with a personal account recovery service for the customers that loose the private key of their DFC accounts.
- Combat financial illicits, such as money laundering and terrorism financing.

It is important to mention that, even possessing the DAG, the Central Bank of Brazil would not have access to the real identity of any user. It would only have access to the identity of the bank that the user registered and activated the DFC account.

The privacy of the user and their financial transactions will be protected by the same instruments that we have today for the guarantee of banking secrecy. However, with a judicial ruling, a bank secrecy breach would be possible, as any other digital payment system today.

5.3 Characteristics of the studied model

The official digital currency would have the following characteristics:

5.3.1 Availability

The use of digital cash issued by the central bank would be guaranteed 24/7/365 - independent of the direct involvement of the Central Bank. Transaction validation, which is the only kind of transaction that really needs to run uninterruptedly, could be performed by the Central Bank of Brazil or delegated to one or more institutions. In the later scenario, the Central Bank occupies the roles of issuer and supervisor, without its momentary downtime having an impact on the performance of the DFC. The transaction between banks and the Central Bank of Brazil, in turn, would continue to occur within the normal hours of the Brazilian Payment System (SPB).

5.3.2 Duration

The DFC token, because of its digital nature, has indefinite duration.

Should there be a need to replace or update the DFC version, as in the case of changing the national currency (e.g. Cruzeiro Real to Real in 1994), the proposed model would allow it to be done at low cost through automatic procedures, which would facilitate the whole process.

5.3.3 Format and transfer Mechanism

The DFC would have an immutable but consumable digital token format. The transactions would be done in a distributed architecture - point-to-point - in two steps that have no definite order (e.g. validation after transfer or transfer after validation).

5.3.4 Settlement

The settlement in the DFC would be instantaneous, irrevocable and irrefutable, being carried out in the act of validation. That is, after validation, the new token already belongs to the beneficiary, even if it is not yet delivered to him. In the case of transmission problems, after this point, it is possible to request the recovery of tokens, as described in item A.3.3. In case of value errors, a new transaction should be performed to correct the payment or transfer.

5.3.5 Monitoring

All transactions related to this DFC would be available in near-real time within the Central Bank's systems for any kind of economic monitoring. All validators should report transactions validated to the Central Bank of Brazil on a timely basis for monitoring and oversight purposes, except, case the Central Bank is out of service. This communication must be asynchronous, with delivery guarantee, where the Central Bank would have a passive role, not becoming a point of failure, or retention if it is out of service.

5.3.6 Target audience

The DFC would focus on retail operations. However, its architecture is flexible enough to serve the interbank market or even both simultaneously, if necessary.

5.3.7 Issuance

The issuance of digital cash would be exclusive to the Central Bank of Brazil. However, its production could be carried out in a manner similar to the production of today's currency.

5.3.8 Non-interest bearing

The DFC would not provide any type of interest.

5.3.9 System costs

The DFC would translate into a computational system with a low cost of production and operation, when compared to others payment systems and cash itself. However, the system would consume some resources from the parties involved, with a cost of support that may be subjected to reimbursement.

This reimbursement could be done in some ways, for example:

- **Charging a fee**: charging a token operating fee to be paid by the end user. However, this approach distances itself from the user's experience of physical money;
- **Subsidy**: it would also be possible to pay for the whole operation of this new system with the public cost reductions related to an eventual decrease in physical cash usage;
- **By a partnership**: a new arrangement agreed upon in an eventual Public-Private Partnership;
- **By validators**: the costs would be borne entirely by the validators themselves, if there were clear indirect benefits derived from this service provision - such as the opening of new channels of relationship and the provision of services to their user base.

5.3.10 Privacy and anonymity

It is possible to allow anonymous cryptographic identities to operate with the DFC. The degree of privacy in this case would be even greater than that of Bitcoin, since the database that stores the DFC full transaction history would be private to the Central Bank of Brazil, and not of public knowledge like the case of the mentioned crypto-currency. On the other hand, it is also possible to ensure that only DFC accounts duly identified by the Central Bank could use digital money.

In the first situation, the Central Bank of Brazil, although still having the traceability, would not have the capacity to identify the owners of the digital currency amounts. Actions to combat money laundering and terrorist financing would be hampered. There would be no practical means of preventing foreigners from using the national currency and would make it impossible to apply limits on the use of currency.

In the situation where the Central Bank of Brazil would have all the data about the citizens using the digital currency, the risks presented above would be mitigated by rules and system validations. However, the concentration of such information in a single government institution could jeopardize the privacy of the citizens. The coexistence of anonymous accounts and identified accounts is possible, but it would bring the same problems of anonymous accounts alone.

The approach of this study aims at finding a balance between anonymity and total lack of privacy in the use of DFC. To do so, the user should identify himself with the chosen financial institution to have an active digital money account. However, the identity will remain protected by bank secrecy.

5.3.11 Security

For the use of a token it is necessary to have it, and the private key of the DFC account that the token declares as owner of the amount described therein. Without one of these elements it is impossible to use or steal the digitized cash. In addition to this criterion, by common sense, the simple fact that tokens are traceable already discourages the practice of related crimes, although it could discourage its usage as a true substitute of the physical currency.

5.3.12 Central Bank of Brazil: defined limits

With different types of accounts and transactions, it would be possible to define several specific limits, such as limits on withdrawals, deposits or transfers, with different values for each type of account. You could also place limits on the number of any kind of transaction per period, with different values for each type of account.

Placing a limit on the total DFC account balance is possible, but there are few specific situations where, despite the best efforts, given the current system architecture, an account may exceed a set limit. For example, if there are simultaneous transfers to the same account, through different validators that are not in sync, whose value added exceeds the defined limit. Although it seems to be an infrequent situation, it is possible. However, it is worth considering whether the very existence of a limit on the DFC balance would be desirable for the system, since other limits and controls could lead to similar results.

Limits on the number of DFC accounts per banking customer are also possible. The financial institutions would be responsible for the registration of new DFC accounts and the identity of their user would not be shared with the Central Bank, nor with the other banks. If implemented in this way, the limit's compliance would have to be assessed outside the DFC system.

5.3.13 Different types of digital fiat currency accounts

Some types of digital money account can be created, three types considered important for the operation of the DFC are:

- **Digital currency bank account**: It should be treated as the digital equivalent to the balance of physical currency available in the banks, even being part of the calculation of compulsory deposits. The Central Bank of Brazil would only send digital currency to this type of account. The Central Bank of Brazil would only receive digital currency from this type of account. It should not carry out transfer operations or payments only withdrawals and deposits. If the bank wants to operate with the DFC, it will have to create a commercial wallet and use it to make transfers and payments.

- **Digital currency commercial account**: It should be the digital equivalent of physical cash in the drawer of the cash registers. Its main purpose is to enable the digital payment of changes to physical cash payments at points of sale. It will mainly receive payments and make transfers of small values.

- **Digital currency personal account**: It should be treated as the digital equivalent of the physical money held by the user. Its main purpose will be to allow the custody of digital cash and its use as a means of payment. It will make withdrawals, deposits, transfers and payments within the limits determined by the central authority.

5.3.14 Combating money laundering and terrorist financing

Should the suspect's bank secrecy be broken by court order, it would be possible to track his financial movement in digital money. If necessary, also by court order, the DFC account can be blocked by preventing the use of its electronic money as a means of payment. Other investigative tools may be used to combat illicit activities such as the addition of a special marker to the DFC account which will indicate to the validators to collect and dispatch extra information about the location and activities of the criminal.

5.3.15 Account recovery

According to the characteristics of the studied model, it would be possible to provide services to the population such as tokens recovery and DFC accounts. These services would be carried out by the financial institutions through a system made available by the Central Bank. Recovery procedure is described in the A.3.3, A.3.4 and A.3.5 items.

5.3.16 All service is provided in layers

All the services provided by the Central Bank would be consumed by society through the banking system. The Central Bank of Brazil would not need to increase its staff in order to meet population needs with the DFC.

5.4 Advantages

- Reduces costs of the national financial system.

- Allows near real-time monitoring.
- Increase the efficiency and resiliency of the payment system.
- Increases traceability and enables greater effectiveness in combating corruption.
- Decentralize payment systems.
- Responds to the advance of the crypto-coins.
- Potential increase in digital inclusion and financial citizenship.
- Does not use immature technologies.
- Does not cause bank disintermediation.
- Does not significantly impact bank runs.
- Does not compete for remunerated securities or repurchase agreements.
- Does not imply an increase in the central bank's balance sheet.
- Does not imply an increase in the demand for the provision by the Central Bank of personal assistance to the population.
- Does not change the central bank's key roles.

5.5 System risks

- **Counterfeit and double spend**:

  All token-based money depends on the ability of the payee to verify the validity of the paying instrument. With physical cash, the concern is in the counterfeit of the physical currency, in the digital world the concern is to verify if the token is genuine or not (electronic forgery) and if it has not yet been spent in a previous transaction (double spend).

  Double Spending is a potential problem for digital tokens, since there is a risk that the payer will use the same token (or a copy) in different transactions. In order to avoid this problem, it was necessary to have a validation software participating in each movement, to guarantee to the beneficiary that it is actually receiving the value digitally presented and not an invalid copy of the value. Such a validation system could be operated by the CB or authorized financial institutions and th so called validator in this document.

  There are other solutions that mitigate the risk of double spending (fakes) of digital values without the participation of a third party on each transaction. Rechargeable smart card systems, such as those used in Brazil for public transportation ticketing, are examples of this. These systems, however, are not feasible for the application of a sovereign digital currency for several factors:

  - Its nationwide rollout would require large investments similar to those already made by the credit and debit card industry, as it uses specific hardware built solely for this purpose.
  - The physical security breach of smart card is possible, despite the high cost.

  - The late discovery of a security flaw in the hardware could require the replacement of all equipment already deployed.

  In systems such as public transport ticketing, where the average balance of smart cards is low, the breach of their physical security is discouraged. The combination of smart card systems and the proposed model would require a specific approach, which might be studied later.

- **Cyber attack - theft**:

  As the Central Bank would assume the role of network supervisor and the system would have great importance in the National Financial System, it would become even more attractive to cyber attacks. However, the Brazilian Central Bank's ability to act in the security of its systems has been publicly known and it has not suffered any kind of invasion despite being a constant target of numerous cyber attacks.

  However, in case of a successful cyber invasion, with the digital theft of DFC tokens stored in the Central Bank of Brazil, the hacker would not benefit because it is still necessary to have the correct private keys to use such tokens as a means of payment. The private key of each token belongs to its owner, and would not be known by the Central Bank of Brazil or any other financial institution.

- **Cyber attack - Denial of Service**:

  Denial of Service (DoS) attacks, interrupt the system's availability to the citizen. A DoS attack targeting the Central Bank of Brazil could not cause any harm to the operation of the DFC. However, addressed to an unprotected validator, it could impact the provision of the validation service for the tokens associated with this validator. Nevertheless, there are several techniques already employed today by banks in their internet banking and mobile banking services, which could be successfully applied to mitigate this type of attack.

  In addition to the mechanisms already used in the fight against DoS, it is possible to implement composite validators, that is, the union of more than one institution in the same role as validator. This option would increase the system's overall attack resilience and resistance, but would add marginal latency to the validation processing.

  Another solution to a successful DoS attack (and other kinds of disasters), would be the Central Bank temporarily replace the disabled validator, as a contingency agent, following disaster recovery procedure to be defined in an eventual implementation phase.

- **Future protocol failure**:

  The proposed approach is supported by widely used public domain encryption protocols. Eventually new cryptanalysis techniques are discovered that may weaken its safety. If any algorithm used by the system has been compromised, its replacement by a more secure version will be performed in a timely manner by the Central Bank. The same will apply to all payment and banking systems supported by the same technologies.

5.6 Other risks

There are factors that can interfere with the citizen's demand for digital money. Among them, we highlight the following items:

- **Low Demand - Competition**: Big technology companies like Google and Facebook are investing in instant electronic transfer systems. In India, for example, Google Tez's operation, started in September 2017, contributed to the increase in the number of instant transactions using the Unified Payment Interface (UNI). The number of transactions using this protocol went from approximately 17 million/month to almost 145 million/month from August to December 2017 [13]. Until the date of the writing of this study, at least one initiative to build a similar system was announced by Brazilian banks.

  The global movement of private players in the direction of creating payment systems and solutions with characteristics quite similar to a digital fiat currency (e.g. stable cryptocurrency) is an indicative of popular demand. The presence of a government solution in this market, through the provision of a new infrastructure, as well as the adoption of a legal tender in a digital format, as a transactional token, would avoid the concentration of means of payment in the hands of a few private institutions and would stimulate the maintenance of operating fees in competitive values, in addition to allowing, in real time, the deep monitoring of digital payments made in retail - even by the informal/shadow economy.

- **Low demand - Adoption barriers** It is common knowledge that part of the population has difficulties to adopt new technologies. The difficulty in handling mobile phones may be a barrier to the adoption of the solution proposed by this study.

  Possible actions for mitigation:

  - Make broad disclosure about what digital money is and how it works;
  - Include the digital fiat currency in financial education programs;
  - Conduct a usability and user interface study on the handling of mobile applications by the general public;
  - Create contests, or Hackathons [14], to encourage the development of secure and intuitive personal digital wallet applications.

- **Low demand - Lack of confidence**: Although supposedly reduced, a share of the demand for physical money comes the from distrust in the government and the national financial system, especially in the group of people who have suffered the actions of confiscation of resources in economic plans (e.g. Collor plan - 1990). It is reasonable to assume that in this group of users the same distrust would occur with a digital fiat currency, since the system would allow the locking of amounts without the consent of the citizen and would not guarantee absolute anonymity such as physical money. In the same sense, the solution would not be appealing to criminals, who have a preference for the use of physical cash and even anarchic virtual coins.

5.7 Topics for discussion

Throughout the research, a number of issues were raised (not exhaustive), which could still be further assessed during an in-depth phase of studies:

- What are all the opportunities for monetary policy? What are the risks?
- Is there a need to adapt the legal framework? What adaptations should be made?

- What are the impacts on economic efficiency and GDP?
- How to reconcile a possible digital money competition with other means of payment?
- Will we have limitations in the cellular infrastructure? How to overcome?
- How to promote the use and dissemination of knowledge?
- What is the best way to deploy?
- To what extent would the digitization of money increase the susceptibility of the financial system to cybercrime?
- How to combat new cybercrimes?
- How to deal with badly behaved validators?
- How to deal with loss/leakage of validators' private keys?
- How to avoid creating fake accounts?
- Is there a risk of digital money competing with treasury bonds as low risk assets?
- In a scenario of instability in the financial system, is the risk of bank run mitigated?
- What would be the best approaches to facilitate access and increase the levels of digital financial inclusion?

6 Conclusion

Decisions on the design level of a digital fiat currency may bring about a number of changes in the way financial systems currently work - changing incentive, players, processes, economic and monetary policy instruments, as well as stability mechanisms. In this sense, the studied model adopts a pragmatic approach, minimizing obstacles and mitigating uncertainties, while avoiding bank disintermediation and preserving the essential roles of the Central Bank of Brazil.

Nonetheless, we believe that this model could be capable of promoting a series of innovations and benefits, which might translate into notable increase in levels of efficiency and financial inclusion within our national financial system.

Finally, we emphasize that this document is merely an exploratory study that aims to consolidate and deepen the understanding on the subject.

Annex A: Frequently Asked Questions

A.1 Private keys

A.1.1 Where will people store their private keys?

We understand that it should be common to keep the private key of the DFC account encrypted and stored on the mobile device. This would be the daily use copy and should be cryptographically protected by a local password. As an additional layer of security, it is advisable that digital wallet applications request the user to set a password to unlock the stored data.

A.1.2 Would private key backups be possible?

It would be possible to keep a backup of the private key on another storage device, a pen-drive, for example. In the cloud, if it is in the user's interest. It could also be possible to even make a paper backup of the key, by keeping a record of twelve randomly drawn words.

A.2 Digital fiat currency accounts

A.2.1 How to temporarily block a DFC account?

It is up to the user to contact their bank and request the temporary blocking of a DFC account. Other alternatives might be offered. For instance, the user may directly ask a validator to do the same, as long as he possess its private key.

A.2.2 How to unblock a DFC account?

If the user wants to unlock a DFC account, he must identify himself to bank where the account was originally opened and request its unblocking.

A.2.3 How to permanently cancel a DFC account?

The cancellation of a DFC account, blocked or not, would be carried out exclusively by the bank responsible for its opening, after the request of the identified account owner. The bank may request the creation of a new surrogate account and the transfer of funds from the canceled account to the newly created account.

A.3 About solution security

A.3.1 What to do if someone copies the user's tokens?

As long as the private key is safely stored, there is no risk. It is impossible to use the system without the private key of the token's DFC account. Additionally, once the user makes a transaction, the copied tokens will be consumed and no longer useful to the hacker.

A.3.2 What to do if someone copies the citizen's private key?

The private key is not sufficient to transact with the DFC. To do so, one must also possess valid tokens. However, the private key is the main security tool of the system. As soon as possible, the user should follow the temporary DFC account lockout procedure (item A.2.1). After blocking the account, the user can choose at some point to follow the unlocking procedure (item A.2.2) or even cancel the account (item A.2.3).

A.3.3 What to do if the user loses the tokens?

In control of the private key, the user could request to the bank that opened the DFC account to reload her tokens in her digital wallet application. To do so, the bank should access the central bank token retrieval service.

A.3.4 What to do if the user loses the private key?

The user should follow the temporary DFC account lockout procedure (item A.2.1). After blocking the account, the user can choose at some point to follow the unlock procedure (item A.2.2) or simply cancel the account (item A.2.3).

A.3.5 What if the user loses the cell phone with all her tokens and the private key?

The user should follow the procedure to temporary block the DFC account (item A.2.1). After its blocking, the user can opt to follow the unlock procedure (item A.2.2) or cancel the account (item A.2.3).

A.3.6 What to do if the user has the device that runs the digital wallet application stolen?

The thief will likely have access to an encrypted copy of the user's valid private key and tokens. In this case, the procedure is similar to the case of debit / credit card theft, as described in ref lostCellular. It is important to mention that decrypting the user's private key would be as complex and time-consuming as the strength of the user's password. In this sense, with a strong password, the user would have enough time to lock the DFC account, making the theft unsuccessful.

In addition, some mobile phone manufacturers have already considered the possibility of deploying a remote "self-destruction" function of the device along with their data. This function can be useful in the discussed case. Also, manufactures are already starting to offer hardware solutions for the storage of private keys embedded in mobile phones as an additional security mechanism.

A.3.7 What if the criminal transfers the user's digital money before the temporary DFC account lockout?

Unlike credit cards, where banks reimburse the customers and charge merchants ("charge back"). Unlike the physical money, which is hardly recovered. The digital fiat currency, is traceable and the user could follow the procedure of the item A.3.8.

A.3.8 What to do if the user is coerced to withdraw DFC by a criminal?

The user should request the police authority to initiate a criminal investigation. This procedure, after a judicial ruling, may lead to the tracking and the breach of confidentiality of other digital accounts possibly involved with the crime.

A.3.9 Which is safer: physical money or its digital version?

The security of physical money depends on its possession. Once lost, as it is non traceable, it is very difficult to be recovered. The theft of digital fiat money requires the subtraction of the active tokens and the private key of a DFC account. In addition, the thief must also transfer the stolen value to another digital wallet, or use it in the purchase of a product, before the account is blocked. As digital money is traceable, at the request of the individual, the bank secrecy of the account may be broken, providing the necessary information for a police investigation.

Mobile banking applications, which are responsible for the largest portion of banking transactions today, are good examples of secure applications. Similar security mechanisms would be used in the development of personal digital wallets.

Current mobile operating systems do not allow an application to access data from another application, so it is not possible for a malicious application to purge data from the digital wallet without express authorization from the user. Even if this authorization occurs, the digital wallet data stored on the mobile phone should be protected by a password.

A.4 Devices and the connection

A.4.1 What are the minimum requirements for a mobile phone to operate digital money?

To illustrate, the personal digital wallet application will probably require fewer resources than popular messaging application, such as WhatsApp, which in May 2017 already had more than 120 million active users in Brazil [15]. Based on these data and in view of the exponential speed of technological advances, it is easy to conclude that the Brazilian digital currency would not find in the capacity of mobile devices a barrier to its adoption at the time of its implementation.

A.4.2 Who should develop and distribute the personal digital wallet application?

This application could be developed exclusively by the Central Bank. However, we believe that the private sector should fill this gap. Nevertheless, to ensure the safety of DFC users, the Central Bank could homologate commercial applications, informing society which ones are secure enough, possibly by listing them on a specific page in its own site.

A.4.3 What to do if there is no internet connection?

If at least one of the parties involved has some kind of internet connection, even if it is a “dial-up” connection, it could be able to validate the transaction. If neither party has any type of internet connection, the payment still can be made normally. The party that received the DFC would be responsible for performing the validation at a later time, when an internet connection is available. At this point, if the transaction is rejected for any reason, the injured party may proceed the same way it does with bad checks nowadays. In any case, the physical money may alternatively be used, since it will coexist with the proposed solution.

A.5 About bits and bytes

A.5.1 What is the size of the tokens?

A token has 72 bytes, but what is transferred among system parts are the transactions actually.

A.5.2 What is the size of the transactions?

The size of transactions varies by several factors: the number of tokens consumed (from 1 to 255 tokens), the number of tokens generated (1 or 2), the transaction type (withdrawal, deposit, payment and etc.), the auxiliary fields if necessary (e.g. customer number for the payment of bank tickets).

To illustrate, a simple transfer between two individuals, when finalized, can have between 211 bytes and 8,837 bytes (8.5 kilobytes). Although, the full transaction will only be transferred between the digital wallet applications. Between the wallets and the validators, the payload transferred is different.

A.5.3 Finally, how many bytes do the network uses?

The payload transferred depends on the size of the transaction (item A.5.2) and the process. Considering the transaction exemplified in the item A.5.2, we will have the following scenarios:

- User to validator: from 171 bytes to 8697 bytes (8.5 kilobytes).
- Validator to user, on success: 48 bytes.
- Validator to user, on error: 8 bytes.
- Debited to Credited: from 211 bytes to 8737 bytes (8.5 kilobytes).

A.5.4 Where these digital fiat currency tokens stay?

Each transaction consumes and creates new tokens. The active tokens stay inside the transaction itself. Only the involved parties, the validating institution and the system supervisor have access to the transaction data (there is no broadcast). Transactions should only be stored by the owners of its active tokens and the supervisor (Central Bank of Brazil).

A.5.5 Does this system use Blockchain technology?

The architecture is inspired by the concept of a Directed Acyclic Graph (DAG), through distributed validation. However, unlike traditional Blockchain technology, there are no blocks, no block strings, no consensus algorithms, no proof of work and no broadcasts. The Digital Fiat System would only use mature, battle-proven technologies already used by financial systems around the world for many years, such as digital signatures and certificates.

A.5.6 As for the performance of this system, how many transactions per second can it handle?

The exact number of transactions per second that a validator can process is not known to date, since the system has not been fully prototyped yet. However, due to its distributed validation characteristic, an increase in the number of transactions per second of the system would be directly proportional to the number of validators installed (horizontal scalability). Each validating institution can and should operate several validating programs simultaneously. Because there are no limits to the number of validating programs that can operate in parallel, there are no limits to the number of transactions per second that the system can achieve. In addition, due to the minimalist and parallel characteristics of validation services, we estimate (based on theoretical premises) a high transaction throughput with low cost of investment in hardware, which seems suitable for a digital payment solution designed to the retail.

A.6 Use by foreigners

A.6.1 Would it be possible to exchange other national currencies for the local digital fiat currency?

Yes. The foreign exchange company would have to open a DFC account for this specific purpose with an authorized financial institution. From that moment, it will be able to receive and deliver the Reais in both physical currency and digital format.

A.6.2 Would it be possible for non-Brazilian citizens to use the digital fiat money?

The procedure for opening digital money accounts suggested in this paper would be through financial institutions. The regulation for opening accounts is going to define whether it will be possible for a foreigner to have digital fiat cash or not. A second control can be done by the validators through the geographic region bound to the IP address of the user who is requesting the validation.

A.7 About system governance

A.7.1 The deployment of this system would imply the end of physical money?

No. Although the main objective is the gradual reduction of the demand for cash, coexistence of the two types of cash is expected over several years. In the long term, the central bank could decide on a possible discontinuation of the physical cash supply if it considers that the solution in the digital format, and its necessary infrastructure, have reached a sufficient degree of maturity so that such a decision does not entail losses to society.

A.7.2 How would updates would work in the digital fiat currency system?

Once in circulation, digital money would be present in countless mobile phones and personal computers. However, digital cash has a version, or family, embedded in the header of all tokens in circulation. This header would be used to enable automatic updating of the cash during its normal operation.

With respect to cash stored in a non-volatile media for use as a reserve of value, a procedure similar to the one adopted on the substitution of the national sovereign currency would be used.

A.7.3 What is the relationship between wholesale digital money and retail digital money?

Since the model has been idealized to handle retail transactions from the beginning, which is a more complex use case, the system could theoretically be adapted at some point to handle wholesale transactions - the main differences would be the types of transaction, its players and the transaction limits allowed. However, it might not be the case in Brazil, since the country already counts with a well functional RTGS system.

A.7.4 Why are there multiple transaction types and accounts if they all work the same?

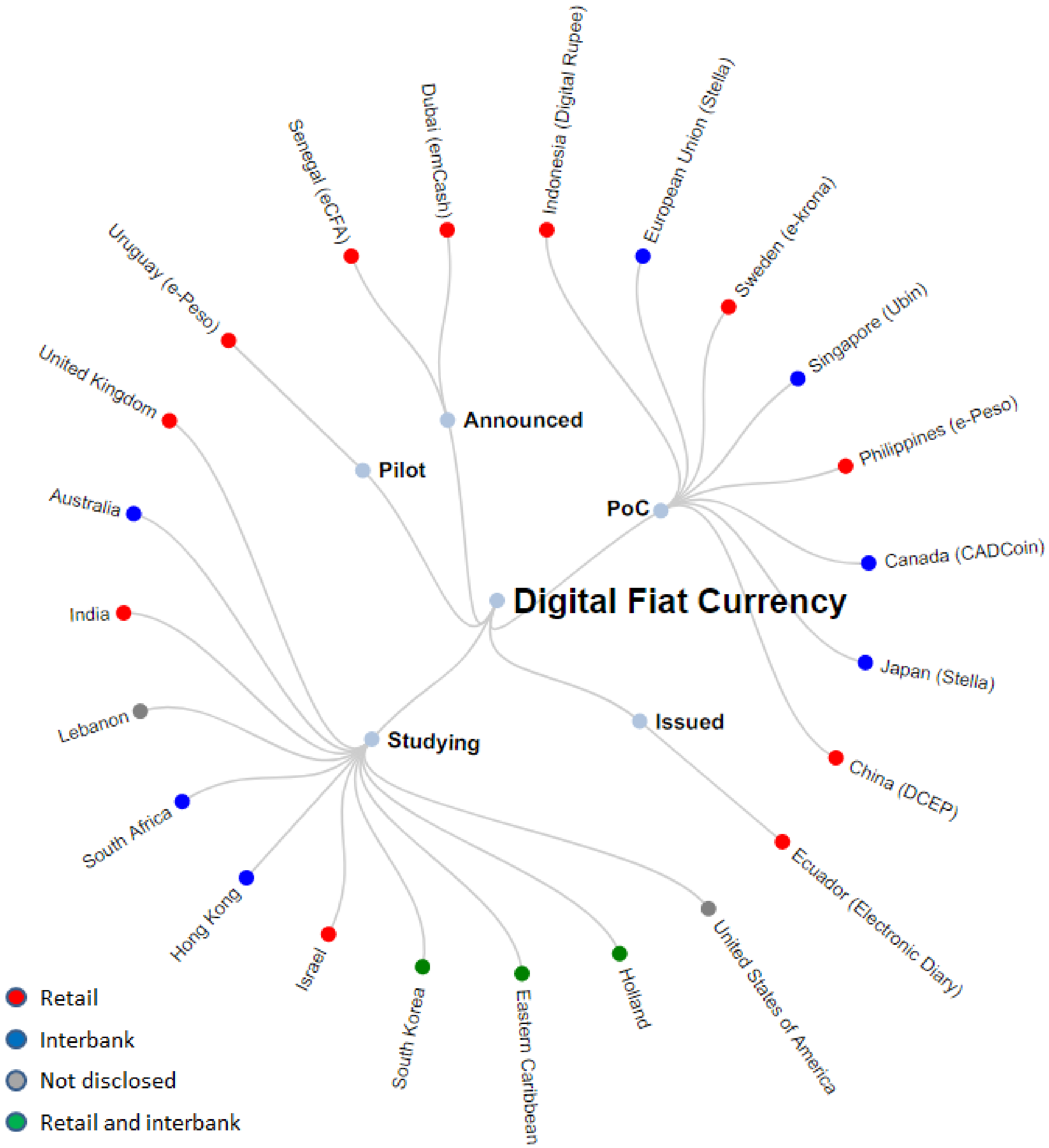
The different types of transactions and accounts, listed below, are designed to allow greater control over the operation of the digital fiat money. This list is not final and we understand that its update is natural, as the system definitions to be deployed are deepened.

- Transaction types:
  - Withdraw from bank reserve,
  - Withdraw from checking account,
  - Transfer,
  - Interbank transfer,
  - Payment in cash,
  - Ticket payment,
  - Checking account deposit,
  - Reserve account deposit.
- Account Types:
  - Custodian account,
  - Bank account,
  - Business account,
  - Personal account.

Annex B: Government Digital Coins - Survey

B.1 Digital Fiat Currency

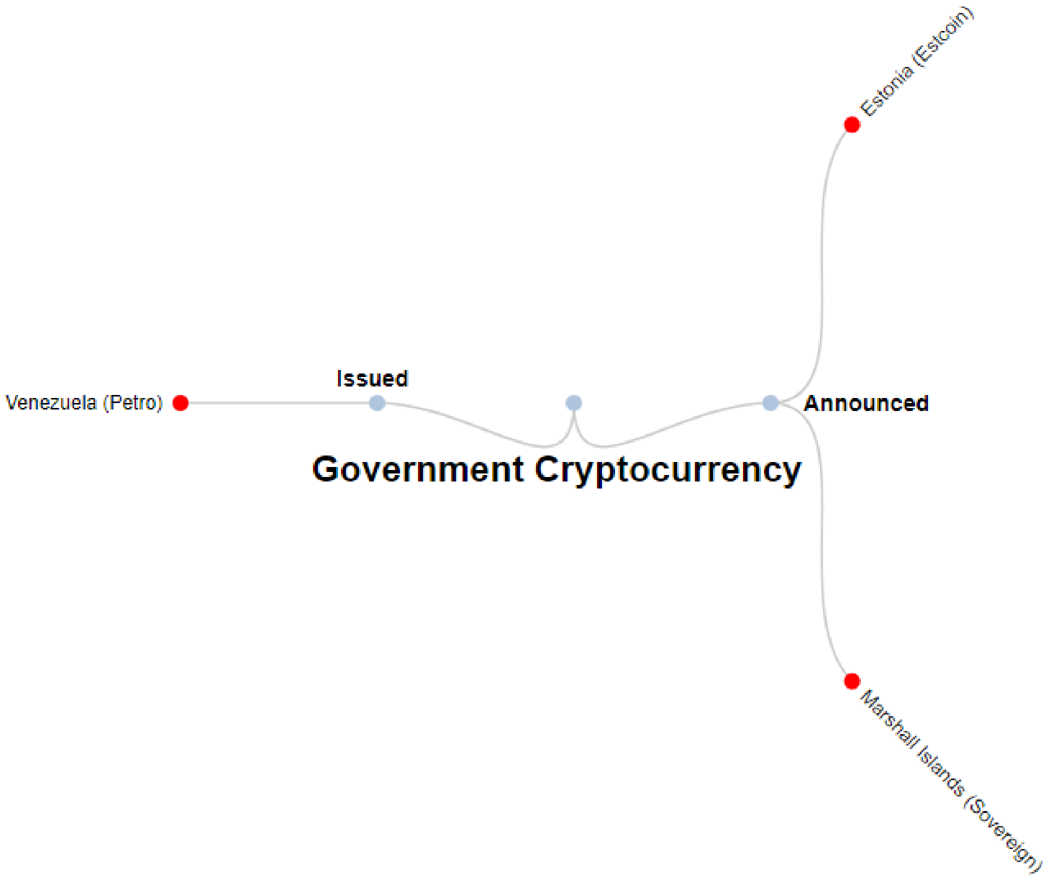
Several countries are evaluating or seeking options for the dematerialization of their national currencies. In some cases, the focus is limited to the creation or update of their interbank payment system - a problem solved by the Brazilian Payment System (SPB) about 16 years ago -, in others, studies and tests turn their attention to its retail side, aiming to supplement or even replace their physical currencies. The chart below seeks to summarize and classify these experiences, based on publicly available information.



References: Ecuador [16] [17], Uruguay [18] [19], Dubai [20] [21], Senegal [22] [23], USA [24] [25], China [26] [27] [28] [29]. Japan [30] [31], European Union [32], France [33], Canada [34], United Kingdom [35], Australia [36]. South Africa [37], Singapore [38], Hong Kong [39], Sweden [40], Philippines [41], Indonesia [42] [43], India [44]. Lebanon [45], Eastern Caribbean [46], South Korea [47], Israel [48], Netherlands [49].

B.2 Government issued cryptocurrency

The initiatives listed in this section differ markedly from a digital fiat currency. This type of cryptoasset is often a state funding mechanism, similar to the so called Initial Coin Offer (ICO), which is commonly adopted by private cryptoassets. In this sense, they are not considered as a digital representation of a fiat currency, but only an independent class of "crypto", with a speculative focus and/or restricted functionalities, when in existence, linked to a particular ecosystem.



References: Venezuela [50] [51] [52], Estonia [53] [54], Marshall Islands [55] [56]

References

[1] World Economic Forum. Unlocking digital value to society: A new framework for growth. http://www.ciab.org.br/download/researches/research-2017_en.pdf. [Online; accessed 3-june-2018].

[2] http://www.abecs.org.br/revista/22/Revista_Abecs_22. [Online; accessed 23-april-2018].

[3] http://www.cnf.org.br/noticia/-/blogs/bancos-investem-ate-r-9-bi-para-proteger-caixas-e-agencias. [Online; accessed 23-april-2018].

[4] WBG. Global findex report 2017. https://globalfindex.worldbank.org. [Online; accessed 3-june-2018].

[5] http://datatopics.worldbank.org/financialinclusion. [Online; accessed 23-april-2018].

[6] http://g1.globo.com/fantastico/edicoes/2017/03/12.html!v/5719023. [Online; accessed 23-april-2018].

[7] https://fidoalliance.org/participate/members-bringing-together-ecosystem. [Online; accessed 23-april-2018].

[8] Banco Central do Brasil. https://bit.ly/2L7OkMg. [Online; accessed 23-march-2018].

[9] Klaus Löber and Aerdt Houben. Committee on payments and market infrastructures markets committee. [Online; accessed 3-june-2018].

[10] IBGE. http://www.brasil.gov.br/governo/2011/02/demografia. [Online; accessed 23-march-2018].

[11] Agência Nacional de Telecomunicaçoes. http://www.anatel.gov.br/consumidor/telefonia-celular/direitos/cobertura-e-zona-de-sombra. [Online; accessed 23-march-2018].

[12] Agência Nacional de Telecomunicaçoes. http://www.anatel.gov.br/dados/destaque-1/283-brasil-tem-236-2-milhoes-de-linhas-moveis-em-janeiro-de-2018. [Online; accessed 23-march-2018].

[13] https://qz.com/1216715/googles-tez-not-modis-bhim-is-winning-the-upi-payments-race/. [Online; accessed 29-march-2018].

[14] Wikipedia. https://pt.wikipedia.org/wiki/Hackathon. [Online; accessed 29-march-2018].

[15] Estadão. http://link.estadao.com.br/noticias/empresas,whatsapp-chega-a-120-milhoes-de-usuarios-no-brasil,70001817647. [Online; accessed 23-march-2018].

[16] https://www.bis.org/publ/qtrpdf/r_qt1709f.htm. [Online; accessed 23-april-2018].

[17] https://seekingalpha.com/article/4159982-worlds-first-central-bank-electronic-money-come-gone-ecuador-2014minus-2018. [Online; accessed 23-april-2018].

[18] http://www.bcu.gub.uy/Comunicaciones/Conferencias/20171103_BCU_Billete_Digital.pdf. [Online; accessed 23-april-2018].

[19] https://negocios.elpais.com.uy/noticias/funcionan-billetes-digitales-hoy-lanzaron-plan-piloto.html. [Online; accessed 23-april-2018].

[20] http://www.dubaided.ae/English/MediaCenter/Pages/PressReleasesDetails.aspx?ItemId=233. [Online; accessed 23-april-2018].

[21] https://www.khaleejtimes.com/news/government/uae-strategy-to-cash-in-on-blockchain-. [Online; accessed 23-april-2018].

[22] https://qz.com/872876/fintech-senegal-is-launched-the-ecfa-digital-currency. [Online; accessed 23-april-2018].

[23] https://www.ecurrency.net/static/news/201611/press_release_BRM_translated.pdf. [Online; accessed 23-april-2018].

[24] https://www.wsj.com/articles/dudley-says-fed-has-started-thinking-about-official-digital-currency-1511968465. [Online; accessed 23-april-2018].

[25] https://cointelegraph.com/news/us-federal-reserve-has-no-plans-to-introduce-digital-currencies-says-san-francisco-fed-president. [Online; accessed 23-april-2018].

[26] https://www.coindesk.com/chinas-central-bank-opens-new-digital-currency-research-institute/. [Online; accessed 23-april-2018].

[27] https://www.technologyreview.com/s/608088/chinas-central-bank-has-begun-cautiously-testing-a-digital-currency. [Online; accessed 23-april-2018].

[28] https://www.ethnews.com/pboc-governor-digital-currency-could-replace-cash-in-china. [Online; accessed 23-april-2018].

[29] http://news.ifeng.com/a/20180309/56592674_0.shtml. [Online; accessed 23-april-2018].

[30] https://www.bloomberg.com/news/articles/2018-04-04/banks-rush-to-turn-japan-cashless-ahead-of-looming-tech-rivals. [Online; accessed 23-april-2018].

[31] https://www.bloomberg.com/news/articles/2018-01-28/japanese-don-t-need-digital-currency-as-they-love-cash-boj-says. [Online; accessed 23-april-2018].

[32] https://www.boj.or.jp/en/announcements/release_2017/data/rel170906a1.pdf. [Online; accessed 23-april-2018].

[33] Morten L Bech and Rodney Garratt. Central bank cryptocurrencies. 2017.

[34] Carolyn Wilkins. Canada explores digital currency.

[35] https://www.bankofengland.co.uk/research/digital-currencies. [Online; accessed 23-april-2018].

[36] http://www.rba.gov.au/speeches/2017/pdf/sp-gov-2017-12-13.pdf. [Online; accessed 23-april-2018].

[37] https://www.coindesk.com/south-africas-central-bank-eyes-jpmorgan-blockchain-tech/. [Online; accessed 23-april-2018].

[38] Monetary Authority of Singapore. Project ubin. http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx. [Online; accessed 3-june-2018].

[39] http://www.legco.gov.hk/yr16-17/english/panels/fa/papers/fa20170418cb1-777-3-e.pdf. [Online; accessed 23-april-2018].

[40] http://www.riksbank.se/en/Financial-stability/Payments/Does-Sweden-need-the-e-krona/Reports. [Online; accessed 23-april-2018].

[41] http://congress.gov.ph/press/details.php?pressid=8212. [Online; accessed 23-april-2018].

[42] https://www.businesswire.com/news/home/20171018006021/en/Indonesia-Takes-Steps-Digital-Fiat-Currency-Solution. [Online; accessed 23-april-2018].

[43] http://www.thejakartapost.com/news/2018/01/29/bank-indonesia-considers-issuing-digital-rupiah.html. [Online; accessed 23-april-2018].

[44] https://www.coindesk.com/indian-central-bank-studies-fiat-cryptocurrency-for-digital-rupee/. [Online; accessed 23-april-2018].

[45] https://themerkle.com/lebanon-to-issue-its-own-digital-currency/. [Online; accessed 23-april-2018].

[46] https://www.coindesk.com/eastern-caribbean-central-bank-pilot-bitt-blockchain-tech/. [Online; accessed 23-april-2018].

[47] https://www.coindesk.com/koreas-central-bank-forms-task-force-to-study-cryptocurrency-impact/. [Online; accessed 23-april-2018].

[48] https://www.reuters.com/article/us-israel-cenbank-currency/israel-central-bank-mulls-issuing-digital-currency-for-faster-payments-idUSKBN1EI0D5. [Online; accessed 23-april-2018].

[49] Ron Berndsen. If blockchain is the answer, what is the question? In *Speech delivered at the Dutch Blockchain Conference, De Nederlandsche Bank*, volume 20, 2016.

[50] http://www.elpetro.gob.ve/index-en.htmlabout. [Online; accessed 26-april-2018].

[51] https://www.bloomberg.com/news/articles/2018-04-12/venezuela-says-government-bodies-must-soon-accept-cryptocurrency. [Online; accessed 26-april-2018].

[52] https://oilprice.com/Latest-Energy-News/World-News/Venezuelan-Parliament-Finally-Approves-Oil-Backed-Cryptocurrency.html. [Online; accessed 26-april-2018].

[53] https://qz.com/1072740/mario-draghi-of-the-ecb-dashes-estonias-plan-for-an-estcoin-cryptocurrency-backed-by-the-government. [Online; accessed 26-april-2018].

[54] https://e-estonia.com/were-planning-launch-estcoin-only-start. [Online; accessed 26-april-2018].

[55] https://www.sov.global. [Online; accessed 26-april-2018].

[56] https://www.reuters.com/article/us-crypto-currencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD. [Online; accessed 26-april-2018].