Should the central bank issue e-money?

Charles M. Kahn
University of Illinois at Urbana-Champaign,
Bank of Canada,
Federal Reserve Bank of St. Louis

Francisco Rivadeneyra
Bank of Canada

Tsz-Nga Wong
Federal Reserve Bank of Richmond

First version: October 2017.
This version: October 2018.
Check the latest version

Should a central bank take over the provision of e-money, a circulable electronic liability? We discuss how the e-money technology changes the tradeoff between public and private provision, and the tradeoff between e-money and central bank's existing liabilities like banknotes and reserves. The tradeoffs depend on i) the technological setup of the e-money system (as a token or an account; centralized or decentralized); ii) the potential improvement in the implementation and transmission of monetary policy; iii) the risks to safety and privacy from cyber attacks; and iv) the uncertain impact on banks efficiency and financial stability. The most compelling argument for central banks to issue e-money is to address competition problems in the banking sector.

JEL Classification: E42, E51, E58

Keywords: central bank digital currencies, e-money, cryptocurrencies, token- and account-based payment payments

Acknowledgments: We thank David Andolfatto, Ben Fung, Rod Garratt, Ronald Heijmans, John Huntjens, Maarten van Oordt, Warren Weber and participants of the Central Bank Digital Currency working group at the Bank of Canada for comments and suggestions. The opinions here are of the authors and do not necessarily reflect the ones of the Bank of Canada or the Federal Reserve System. All errors remain our own. Contact: Charles M. Kahn: cmkahn@illinois.edu. Francisco Rivadeneyra: riva@bankofcanada.ca. Tsz-Nga Wong: russell.wong@rich.frb.org.

1 Introduction

Wholesale payments systems have typically been operated by central banks.[1] For retail payments, central banks have avoided dealing directly with the general public, relying instead on tiered arrangements in which commercial banks provide direct retail payments activities and services (card-, cheque-, and recently internet-based). These providers in turn rely on centralized backbones to complete the links. The only direct connection between the public and the central bank arises when individuals hold central bank debt in paper form in their wallets.

However, new technological advances like distributed ledger technology (DLT) and mobile computing have made it technologically feasible on the one hand for private parties to develop payments systems which bypass central banks for settlement, and on the other hand for central banks to provide new forms of retail payments media which can bypass the use of intermediaries. Many of these new systems are "token-based" – that is, they rely on identification of the object being transferred as means of payments rather than relying on identification of the individual whose account is being debited.[2]

In this paper we ask if the introduction of the new technologies has fundamentally changed the tradeoffs between public and private provision of payments media? More specifically, does the introduction of these new technologies affect the current role of central banks in the provision of wholesale or retail means of payments? Do these technologies also alter the tradeoff between e-money and the existing central bank liabilities like banknotes and reserves?

Our definition of central bank e-money is an electronic liability of the central bank, which might be held as a token or in an account.[3] Bech and Garratt (2017) have a useful taxonomy of money based on the following attributes: who is the issuer (central bank or other), what is its form (electronic or otherwise), who can access and/or hold it (universal or not) and how is it transferred (centralized or decentralized). Traditionally token-based systems rely on decentralized transactions to effectuate the transfer of the tokens while account-based systems rely on a central party that manages the accounts

[1] Canada is somewhat of an exception. When not operated by central banks they are always closely regulated by them because of their systemic importance and centrality to the workings of the financial system.

[2] For the distinction between token-based and account-based systems see Green (2008b), Kahn and Roberds (2009b), and Kahn (2016).

[3] This definition is broader than the one proposed by the CPMI (2015) which is "value stored electronically in a device such as a chip card or a hard drive in a personal computer."This definition does not mention the distinction between token or accounts but it hardly fits the concept of an account-based system if the credits of participants in the system are all stored in a personal computer.

to record credits and debits between them. In the case of central banks cash is an example of the former and reserves an example of the latter.

To address the questions above we examine several plausible proposals of account- and token-based forms of central bank e-money. For each we discuss the technological setup, how the e-money is issued and how its value is transferred between users. Then we address questions about their efficiency, safety, privacy and potential effects on the banking sector and banking competition. Our analysis suggests that an account-based central bank e-money is unlikely to be the preferred choice of policymakers. The new technologies have not changed the tradeoffs for the universal provision of central bank accounts: this system would be expensive to operate given the central bank's comparative advantages and could put the central bank in a position of directly competing with commercial bank accounts. Indeed this system was feasible even before the advent of the aforementioned technologies.

However our analysis suggests that the new technologies may readjust the policy tradeoffs, shifting the boundaries between central bank and private token-based systems. As it becomes feasible for the central bank to issue electronic tokens, it becomes essential to have a clear understanding of the technological differences between the cash and tokens. Since transferring electronic tokens between two parties necessarily requires third-party involvement, an electronic version of cash cannot be equivalent to physical cash. Therefore, issuing e-money in token form does not follow immediately from the fact that central banks issue cash. The necessity of third-party verification implies, today, high cost and slow speed of transactions compared to cash. With respect to safety, there are still many unanswered questions regarding the risks of cyber attacks and the protection of the privacy of users.

A central bank move into digital tokens will have important effects on financial stability and competition. Today private token-based forms of money, like cryptocurrencies, do not seem to be a major threat to financial stability because their are not widely used as means of payments or store of value. A central bank token would have to be designed appropriately to allay the risk of becoming a source of financial instability.

The issues of competition are even more complex. Although commercial banks have already the technology to issue token-based payments media, banks have chosen not to do so partly because these systems would compete with their deposit-taking business. The new technologies allow broader access to payments services by individuals. Central bank tokens could allow wider access to payments services potentially increasing the contestability of the payments market. However, the effectiveness of competition depends on the regulatory choices of the central bank. Standards for AML and KYC

currently limit the ability of banks to issue token-based payments media. Whether fintech companies succeed in competing with banks depends upon the choices of the regulators to provide interoperability with the new system.

While the discussion about e-money has received significant attention recently,[4] the idea of universal central bank accounts dates back to the "deposited currency" scheme proposed by Tobin (1985). The electronic token idea was discussed during the first wave of the internet in the 1990's. Then policymakers were preoccupied with the risk to the ability of central banks to implement monetary policy, concerns about money laundering, and the reduction of seignorage (see BIS (1996), Friedman (2000), Freedman (2003), among others). Back then the idea of central banks issuing e-money was just a remote possibility. The concern came mostly from the possibility that retail products, like stored value cards, would compete with cash. In fact, stored value cards turned out not to be a significant threat to cash. This time around, central banks have taken a more relaxed perspective in investigating the possible threats from cryptocurrencies. Nonetheless, today central banks are being proactively investigating the possibility of issuing their own form of e-money.[5]

We proceed as follows. Section 2 reviews the literatures on payments systems, counterfeiting and economic history that are relevant for the policy discussions. In section 3 we present the distinguishing features between account- and token-based systems. Then in subsection 4.1 we present the account-based e-money scheme and discuss its tradeoffs, and in subsection 4.2 we do the same for several token-based systems. In section 5 we discuss the public policy objectives relevant to the decision of issuing e-money and propose some ideas on how central banks can approach the evaluation of the tradeoffs. We conclude in section 6 suggesting some open research questions. In the Appendix we discuss some of the alternative proposals by other central banks and academics.

2 Literature

We are related to the literature that discusses the role of central banks in payments systems. There is some consensus on the importance of the role of central banks in maintaining the safety and efficiency of the high value payments systems (CPSS 2003,

[4]See BIS (2015), Berentsen and Schar (2018), Kimball (2013), and citations therein.

[5]See Fung and Halaburda (2016) and Davoodalhosseini and Rivadeneyra (2018) for discussions in the case of Canada. Other prominent examples are Sweden and Uruguay. See Sveriges Riksbank (2017) for a report on the e-Krona project and http://www.epeso.com.uy/ for the pilot project of the Central Bank of Uruguay. More details are provided in the Appendix.

Green and Todd 2001, Green 2008a and Lacker 2008). It is uncontroversial that central banks have a role in providing accounts to financial institutions to allow them to safely settle interbank transactions. Also agreed upon is the role of central banks in providing secured credit to these institutions for that same purpose. There is less agreement if central banks should operate or just oversee the infrastructure in which these systems rely. Either way, central banks generally have a say in the system design and the access and credit policies. For example, during a previous wave of technological change in the 1990's, central banks replaced DNS with RTGS systems, deemed safer in spite of being more expensive in terms of liquidity (CPSS 2005). Access policy is another important lever that central banks have to manage the risk and efficiency of these systems.

Limiting the access of financial institutions to the high value payments system gives rise to tiering, a multilevel structure by which the institutions that do not have access to the system have to rely on the select institutions who do (which frequently is tantamount to having a settlement account at the central bank). Kahn and Roberds (2009a) and Chapman et al. (2013) have discussed the trade-offs of restricting the access to the central bank, specifically between the ability of the operator to monitor the behaviour of participants and the liquidity costs of the system. These tradeoffs are still relevant to our discussion because a decentralized system could allow parties to settle transactions directly.

A new form of central bank money has implications for the competition of means of payments, the transmission of monetary policy and welfare in general. For example, how will central bank e-money compete with other forms of money like cash itself or commercial bank deposits? Would it be welfare improving? There is an active literature debating these questions and the answers usually depend on the model setup. Chiu and Wong (2014, 2015) analyze welfare when there is a form of e-money, not necessarily issued by the central bank. Zhu and Hendry (2017) and Davoodalhosseini (2018) discuss monetary policy under competing currencies or when the central bank issues its own digital currency. The general conclusions of most of these papers is that welfare is likely to improve either because the new means of payments allows additional transactions or because monetary policy has a more powerful instrument.

E-money is no longer the remote possibility it was perceived to be in the 1990s, thanks to new technologies like distributed ledgers that have greatly mitigated the problem of fraud without centralization. Our paper is related to the fields of economic theory and economic history that have investigated counterfeiting of means of payments. These theories are relevant because they highlight aspects of the means of payments that are essential for their design: access, storability and portability, the cost

of counterfeiting, the cost of verification of transactions, recognizability, durability, divisibility, and standardization. Williamson (2002) shows theoretically how counterfeit currency can serve as private money, possibly improving welfare. After all, any fiat money is intrinsically worthless so if a counterfeit is not detected then it can serve as a medium of exchange. Nosal and Wallace (2007) analyse the question when too much counterfeiting will render all genuine tokens worthless.[6]In account-based systems the equivalence to counterfeiting is identity theft studied by Kahn and Roberds (2008).

There are some parallels between today and historical episodes like the free banking era in the US. These episodes reveal lessons about the risks of currency competition and potential policy interventions. Ales et al. (2008) develop a model to explain the discounts that prevailed between different state-chartered banks prior to 1863. This and other papers have documented, not surprisingly, that the discounts between notes varies with distance to the location of the issuing bank and its risk taking behaviour. Weber (2015) analyses the same episode to draw policy lessons for today's cryptocurrencies and private e-money schemes. In Canada between 1817 and 1890 commercial bank notes and provincial notes (later Dominion notes) circulated simultaneously for periods of time. Fung et al. (2017) document the discounts that prevailed between them until the Bank Act of 1890 which established an insurance scheme for the redemption of notes of failed banks. Collectively these papers have important policy implications: regulation and supervision of financial intermediaries is necessary to control the discounting between alternative means of payments, counterfeiting and manage price stability.

Lastly an important concern is that a central bank e-money could directly compete with commercial bank deposits both as means of payments and store of value, potentially diminishing the advantage that depositor institutions have thanks to the access to the central bank payments backbone. In this respect, we are related to the banking and financial stability literatures that examine the implications of new technologies on banking competition. Historically, there are examples of new financial technology and infrastructure having adverse effects on financial stability. For example, Roberds (1995) discusses the financial crises during the national banking era between 1864 and 1912

[6]Other related references are Li and Rocheteau (2011) which shows that the above result doesn't hold under divisible money. Cavalcanti and Nosal (2011) apply the same idea in a mechanism design approach. Li et al. (2012) develop a theory for more complex assets that are vulnerable to fraud, like MBS. Lester et al. (2012) extend this to multiple assets that differ in recognizability. In these studies counterfeit does not happen in the equilibrium because genuine money/asset holders can use signaling. Shao (2014) replaces the signalling game with a competitive search setting under adverse selection. Kang (2017) considers a costly technology that can screen counterfeits. Quercioli and Smith (2015) analyse the rate at which well-intended persons will pass fake notes in equilibrium.

after the introduction of new settlement systems for stocks, markets for commercial paper and foreign exchange.

3 Account- and Token-based Systems

Account- and token-based payment systems are largely distinguished by their identification requirements. For a transaction to be deemed satisfactory in an account-based system the payor has to be identified as the holder of the account from which the payment will be made. In contrast, in a token-based system what needs to be identified is the genuineness of the object being transferred.

Both account and token systems are record-keeping arrangements. Record-keeping arrangements have two essential features: the access permissions to the records and the protocol to update the records. These features determine which party or parties in the system have access to the records and how are the records updated, for example by a single trusted party, bilaterally by the parties in a transaction, by third parties, etc. For our discussion it will be helpful to describe the access and protocol as either being centralized or decentralized. Based on these two features, Table 1 shows the classification of some token- and account-based systems as well as for the e-money proposals of Section 4.

Cash is a typical token system. We can understand cash as a device that summarizes past production, trade and consumption decisions, i.e. bank notes *are* the records (Kocherlakota 1998). As cash changes hands in bilateral (decentralized) transactions, the change in possession of the paper notes amounts to an updating of the records in the system. Note that this system is decentralized because there is no single source of the records and no single party responsible to update the records. Cryptocurrencies like Bitcoin are also token systems in which the records are decentralized as they are distributed in the network. The records in the Bitcoin system, called the blockchain, are updated in a distributed manner via a method called proof of work. Another older example of token systems are prepaid value cards.

In contrast, financial infrastructures like high value payments systems (HVPS) or the central depositories of securities are centralized in the sense that only the operator of the infrastructure has control over the records. These infrastructures are account-based systems where the records are entrusted to and updated by a single party, the operator of the infrastructure. In principle it is possible to have hybrid systems in which the records are distributed but verification is performed by a trusted party among a selected subset of participants, like a clearing house or the RSCoin mechanism proposed

Table 1: Examples of record-keeping systems and proposed schemes. We discuss central bank (CB) accounts in section 4.1, decentralized tokens in section 4.2.1, centralized tokens in section 4.2.2, and delegated tokens in 4.3.

	Access to records	
Updating of records	Decentralized	Centralized
Decentralized	Cash and Bitcoin	
Centralized	CB decentralized tokens RSCoin	HVPS CB reserves CB universal accounts CB centralized tokens CB delegated tokens

by Danezis and Meiklejohn (2015).[7]

Record-keeping systems have tradeoffs in their level of access, privacy and security. For a given cost, there is a trilemma: no system can simultaneously have universal access, perfect security and complete privacy (Figure 1). When access to a system is expanded, it is accompanied by less security (from admitting potentially dishonest participants) or less privacy (relinquished by participants to control the risks).

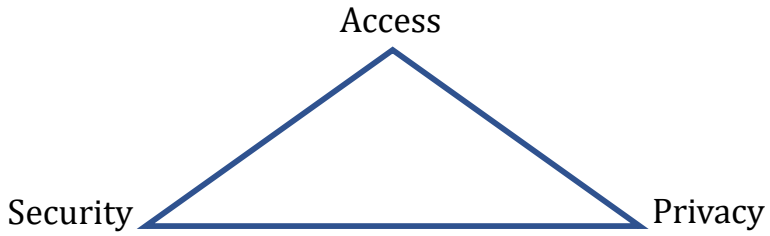
The tradeoff between access and security is determined in part by who bears the liability of fraudulent transactions and of wrong records. In an account system it is the account provider or the party tasked with verifying the message that initiated a payment. This aligns incentives for the account providers or system operators to try to control the risks of fraudulent transactions for example by keeping the security technology up to date and by monitoring the behaviour of the participants in the system. Another way to control risks in the system is to limit the access to certain types of participants.

In a token system the liability of fraudulent transactions lie with the receiver of the token which runs the risk of receiving a counterfeit token or a token already spent before.[8] The counterfeiting risk is determined by the relative cost of verification and the cost of falsification of tokens. In the case of cash, with its easy recognizable security features, verification is cheap and instantaneous –so much so that the physical exchange is automatically a sign of acceptance of authenticity. When those recognizable security features are hard to replicate, the costs of counterfeiting notes are prohibitively high

[7]The case of a system in which the access to records is centralized but the updating is decentralized cannot exist because it would not be incentive compatible.

[8]The latter type of counterfeiting is called the double-spending problem in the case of cryptocurrencies.

Figure 1: Three-way tradeoff between access, privacy and security. For a given cost, a record-keeping system has to balance the extent of access (universal or restricted) with security risks (to the operator and users from admitting potentially risky participants), with privacy (relinquished by users to help control the risks).



for small quantities. Therefore, for transactions of small value bank notes tend to be a very efficient system.

In open systems like Bitcoin, the use of cryptography keeps the cost of verifying the authenticity of tokens low. These systems prevent the counterfeiting of tokens by tracking their provenance by creating a history of tokens. This record is called the blockchain and it is stored in a ledger that is distributed in the computer network. In these systems the cost of falsifying the provenance of a token is the cost of altering the ledger. So for tokens to be valuable, the ledger has to be prohibitively costly to alter. The so-called mining makes the tampering of the records sufficiently expensive to dissuade would-be counterfeiters from doing so.

An important difference between physical and digital tokens is the cost structure of counterfeiting. The variable cost of introducing a counterfeit bank note into circulation is non-negligible (trade goods for the counterfeit note or selling it at a discount to incentivize others to distribute it). Digital tokens, however, can be introduced into circulation in two ways. The typical one is to acquire a real token and attempt to spend it twice. The second way that is only available to digital tokens is due to cyber risks. Cyber risks could allow counterfeit digital tokens to be introduced with close to zero cost if the counterfeiting is done at the source by figuring out unexplored vulnerabilities. Lastly, there is free entry to attempt to counterfeit digital tokens when they are transferred via open networks. Therefore, for digital tokens the speed of the cat-and-mouse game between the issuer and the counterfeiters is likely to be much faster than with bank notes in which new series are introduced decades apart.

Although cyber risk apply also to account-based systems like the Visa or Mastercard payment networks, the operators face serious consequences if they were to be hacked. The difference with account systems is that the liability of the safeguard of the information lies with the account manager and not with the holder of the account. With tokens, the risk of a loss of the tokens is potentially irreversible because the

issuer might not have the ability to distinguish a true from a fake claim of a hack. Furthermore, in contrast to digital tokens, when a security feature of bank notes is compromised a central bank can request the public to exchange those notes, a hassle indeed, but does not create the problem of adjudicating ownership because the flaw in the security does not imply a risk of theft.

The tradeoff between access and privacy is determined in part by the identification requirements. A way to control risks from extending access to a record-keeping system is by demanding users to relinquish privacy, for example at the moment of joining the system or when performing transactions. In a token system the payor need know nothing about the payee's identity and need reveal nothing to the payee beyond the information associated with the specific coin.[9] In an account-based system either the payor knows the payee's account number or the payee knows the payor's account number. However the distinction goes further because of legal requirements in the current environment: even if the transactors need know nothing of each other beyond the account numbers for the transaction, the banks which hold the accounts are required to have information regarding the individuals' identities for a variety of legal reasons including anti-money laundering restrictions (compliance to KYC and to Know Your Third Parties).

4 E-money Proposals

4.1 An account-based scheme

The first proposal we consider is a central bank e-money based on accounts. The idea that the general public could have direct access to accounts at the central bank seems appealing but the reality is that the comparative advantage of the central bank is not, at least at the moment, in the verification of identities of a large number of individuals and the associated account management that would be required. It is true that many government agencies are in the business of identifying individuals for the purpose of issuing official documents such as a passport or a drivers license. Likewise, central banks could choose to establish a large number of branches or points of contact with the public to identify individuals before opening accounts on their name.

There are differences however. The burden of record keeping and management

[9]There is another difference between digital and physical tokens that further constrains privacy. Digital tokens need to be verified by a third party as opposed to cash transactions that typically are verified by the parties involved in the transaction. Although users could agree to receive digital tokens without verifying them this would not be an sustainable. If users accept tokens without verification then too many counterfeiters would attempt to defraud the receiving party.

become immensely greater once the accounts are used for frequent transactions. The central bank would then have to operate systems to allow individuals to access their balances and to verify the authenticity of proposed transactions, as well as a system to settle transactions in its balance sheet.[10]

The new technologies have not changed the tradeoffs between the public and private provision of these systems. Moreover, past examples of government-provided accounts show that central banks have had the ability to provide accounts to the general public but have chosen not to. An account-based system is inherently centralized because the liability of identifying the individuals (when opening an account or when attempting to access funds to make a transfer) lies with the account operator. Although DLT, blockchain and mobile computing technologies could allow the central bank to set up a system of accounts where the storage of records and their updating is distributed, these technologies do not address the problems of identification; the liability would still lie on the cental bank.

In addition to the comparative disadvantage in managing a large number of accounts, the central bank would have to determine its stance towards customers and competitors. When dealing with the public, government bodies tend to be relatively less costumer-focused than private companies. This might lead to low customer satisfaction. Further, central banks could be at risk of political pressures if they were to deal with the wider public. With respect to competitors, for example, the central bank would have to decide if its accounts would be subsidized or priced above commercial competitors. This choice would have direct crowding-out effects on the commercial provision of deposit accounts.

Since the new technologies have not changed the trade-offs presented in the provision of central bank accounts, we conclude that is unlikely that central banks will offer this type of system.

4.2 Token-based schemes

4.2.1 Decentralized token scheme

Consider a fully decentralized token system. For this scheme the central bank could use the infrastructure of an existing cryptocurrency or some other open distributed ledger while committing to stabilize the value of the tokens. Fedcoin is an example of

[10]There are examples of widely-available government-backed accounts that can be used for infrequent transactions. The UK Post Office Money operates a large number of points of contact with the public but its accounts are somewhat limited, for example to receive government benefits. Japan Post Bank, privatized in 2007, still operates mainly as a savings bank.

a proposal for a system using an existing cryptocurrency (Koning 2016 and Andolfatto 2015). RSCoin is an example where the central bank sets up a new decentralized verification infrastructure (Danezis and Meiklejohn 2015).[11]

Central banks have recognized that using DLT or blockchain schemes will not be a cost effective substitute for the core infrastructure of national payments systems (Chapman et al. 2017). The reason lies in the tradeoff between the openness of the system and the cost of verification: distributing the updating of the ledger makes it more costly to control counterfeiting. Chiu and Koeppl (2017) calculate that the lower bound of transactions costs in some cryptocurrencies are an order of magnitude larger than current wholesale payments systems *even* if they are designed optimally.[12] For retail systems an additional cost would be the delay in verification of transactions which currently is longer than current arrangements.

4.2.2 Centralized token scheme

The next scheme we consider is a centralized token system. In this scheme the transfer of each token is verified by a centralized system, which could be run by the central bank system or a regulated private company. The central bank would determine the technical standards for verification and guarantee the safety of the system.

There are two variants to the centralized scheme. In one, sometimes called "digital cash", the central bank issues the tokens and maintains the list of outstanding tokens. When a transactions occurs, the central banks authenticates the tokens against its list destroying the old token and crating a new one for the recipient.

In the second variant, tokens are issued and tracked in a ledger maintained by the central bank or operator of the system. This variant would require establishing policies to manage the use and access to the records. Still users might have doubts about the privacy of their transactions. The large amount of data in the ledger available to the central bank could be used for good purposes like reversals of fraudulent transactions. However, as with the account-based system, this scheme would face similar issues of record-keeping and privacy and would require the central bank to deal with individuals frequently.

Both variants require third party verification. A way to circumvent it would be for the central bank to develop, as part of the system, a technological feature that allows devices like mobile phone to perform the verification on the spot.[13] This is equivalent

[11] The details of these proposals are explained in the Appendix.

[12] Economists and computer scientists are exploring alternative methods of verification which could reduce these costs, see for example Saleh (2018) and Chiu and Koeppl (2018).

[13] These are called off-line transactions. Mondex and DigiCash are examples of the mid-1990s of

to today's easily recognizable security features of bank notes or verification tools like ink testers.

4.3 Delegated schemes: custodians and intermediaries

All the schemes discussed above have central banks dealing directly with the public. Now we explore schemes in which individuals access the central bank token indirectly. This would lead to tiering arrangements much like we have today with national payments systems. In the first tier the central bank issues a token to a special set of regulated institutions like custodians and intermediaries. These institutions can be thought as narrow banks or "deposited currency"schemes (Tobin 1985). In the second tier, individuals acquire the individual tokens or a claim on some tokens from custodians or intermediaries possibly in exchange of cash or bank deposits. Individuals would receive an identified digital object like a code.

The distinction between custodians and intermediaries lies in how these objects are managed on behalf of the clients. Custodians would not be allowed to exchange one token for another even if they are of the same denomination. Custodians would in effect offer safekeeping services much like today's online wallet providers that manage electronic keys of cryptocurrencies. Intermediaries would have additional flexibility because they would not be required to deliver the exact same token as the one deposited by the client. Their tokens would have to be fully backed by central bank tokens therefore would have to be regulated to hold 100% reserves. The freedom allowed to intermediaries would allow them to offer incentives to clients like remunerating their balances, additional security features or customized interfaces.

The verification technology in these schemes could be centralized or decentralized. A centralized verification would require the intermediaries to connect to the central bank (or a utility set up for that purpose). On the other hand, a decentralized verification would allow intermediaries to underwrite the settlement risk and verify transactions with the central bank or other intermediaries. A variation of the scheme with intermediaries would allow them to issue a digital token of their own in exchange of a central bank token. This would allow them to use their own verification technology which could be faster.[14]

systems that permitted these transactions by using cards with embedded chips. See Chaum (1983) and Chaum et al. (1990) for the description of cryptographic blind signatures and their application to prevent double spending in off-line transactions.

[14]The settlement speed that custodians could offer would likely be slower due to the requirement to deliver a specific token in a transaction. On the other hand, intermediaries would face liquidity management risks from the use of a float of tokens to facilitate faster settlement. In addition, fraud risk would be present in custodians and intermediaries as in any other financial institution.

Given the current legal environment (AML, KYC and liability rules), accounts would most likely emerge because custodians and intermediaries would need to link the identity of the client with the property of the tokens. Thanks to the ability to identify clients, custodians and intermediaries could provide safety and convenience to customers fearing the risk of personally holding a large amount of tokens.[15] By linking the tokens and identities, these institutions would be able to offer guarantees to clients, for example alternative ways of identifying themselves in case they loose their private keys.

There are also some competition and regulatory challenges to implementing these schemes. Will custodians and intermediaries have the incentive to distribute the central bank tokens? In the case of bank deposits, fractional reserves provide an incentive to distribute cash. No bank has chosen to become a narrow bank. This suggests that there is no demand by customers for a payments medium superior in safety to existing insured deposits accounts or no desire by banks to supply them without a heavy subsidy. Non-traditional financial institutions might be more willing to offer the central bank tokens as they would not endanger a deposit-taking business. However, competing with established financial institutions can be challenging given the network effects in payments.

Regulation could be one way to direct traditional intermediaries to offer the central bank tokens.[16] Economic history suggest that unless there is a competitive threat or an underlying demand from the public, banks will not have incentives to distribute the tokens. In 1865 the U.S. taxed state bank notes driving them out of circulation which eventually generated the customer demand for federal reserve notes distributed by national banks. This suggests that fintechs should have access to the tokens early on to explore the use cases of digital tokens and to generate competitive pressures for banks.

An important question that policy makers will have to ask is what would be the effect on the aggregate amount of bank deposits. With traditional and non-traditional financial institutions offering access to the central bank token, some amount of deposits will migrate to the central bank token system. However it is hard to predict the total effect on aggregate lending by banks (Chiu et al. 2018). In the long run there may be differences in monetary policy if the terms of settlement, netting and the properties of float in the token system differ from the ones in the deposit system.

[15] Kahn et al. (2018) explore the tradeoff between convenience and security of tokens and accounts.

[16] The Canada Savings Bond is an example of a government product distributed by banks which competes with the products offered by them. The program was discontinued in 2017.

At the outset, fintechs would likely be required to hold tokens one for one, but nothing in our discussion prevents the central bank to allow some institutions to become fractional intermediaries. In this case, we would quickly revert to a similar system as the one we are running today, albeit initially inferior because tokens are less flexible than central bank reserves.[17] This could be remedied once the links that allow settlement of different tokens are established. Further, compared to the current system with deposits, a token system might allow simpler resolution of a troubled payment provider by allowing easier identification of ownership, streamlining deposit insurance.

5 Policy Discussion

The technologies that now allow the central bank to issue e-money are also driving the development of new private means of payments including alternatives to cash. Simultaneously, in many countries the use of cash is declining. It is possible that in the absence of government intervention the adoption of these alternatives could lead to coordination problems. In this section we discuss the policy objectives that could motivate issuing e-money as well as other simpler interventions for those objectives (Table 2).

5.1 Monetary and financial policy objectives

The literature surveyed in section 2 suggests that the conduct of monetary policy could improve because e-money, if appropriately designed, would be a more powerful tool. This has to be revisited with more complete models that can address questions about the transmission mechanisms of monetary policy specially if the make up of the financial system were to change. Specifically, would a central bank e-money enhance or hinder financial stability, increase or reduce bank deposits and bank lending?

Some central banks might be motivated to issue e-money as a reaction to the reduction in seignorage that comes with the fall in cash of usage. It is possible that if funding is received from the fiscal authority, the independence of the central bank could be at risk.

The exclusive provision of cash is one of the current central bank mandates. For two reasons, this does not translate into a mandate to provide the digital alternative to cash. First, cash and digital tokens cannot be equivalent because cash and digital tokens have different tradeoffs of security and privacy. Second, central banks do not

[17] Tokens would be less fungible that reserves if for example each commercial banks has it's own token and they do not share the same verification technology or ledger.

need to have a monopoly of e-money to achieve uniformity (i.e. trading at par).[18] When there are multiple private issuers of money, monetary uniformity can be achieved through regulation of the issuing entities and a deposit insurance scheme (Fung et al. 2017).

The broadening of the access to the wholesale payments could be a motivation to issue e-money. The argument is that some forms of e-money would be simultaneously a settlement asset and a settlement system that could serve as a basis for innovation. This however can already be achieved today with a risk-based widening of access to current national payments systems. This has been the approach taken by the Bank of England (2018). On the retail side, a motivation could be to improve the efficiency of retail payments. For example if e-money was cheaper to use, easier to access and more divisible than cash it could enable micropayments.[19]

5.2 Other policy objectives

Broadening financial inclusion is frequently mentioned as an important objective that could be advanced with the issuance of some form of e-money.[20] It is however not clear why the public version would be technologically superior to the one provided by the private sector for this purpose. Moreover, regulation could direct banks to extend access of basic services.

The possibility of reducing criminal and underground activities have been advocated by Rogoff (2015, 2016) as worthwhile reasons to eliminate cash (or at least large denomination notes). Since the elimination of cash would likely require alternatives, a central bank e-money would be a clear candidate. There would be costs of phasing out cash however. One would be the cost to the well-intended users of cash who lack access to electronic devices (Camera, 2017). Also, if e-money were to substitute cash, criminal organizations would likely respond to find new means of payments and store of value, possibly with worse outcomes (McAndrews, 2017).

It has been discussed if anonymity and privacy should be part of public policy considerations. There is a natural and lawful demand for anonymity and to some

[18] Scotland and Hong Kong are two examples of countries where commercial banks can issue their own notes at par to the notes of the Bank of England and Hong Kong Monetary Authority. These are largely historical legacies and their commercial banks issue in small amounts but point to the fact that printing and distribution of notes are not activities that a central bank has to perform to achieve uniformity of the different means of payments.

[19] One way to evaluate the potential benefit is the resource cost of handling cash. Kosse et al. (2017) estimate that the resource cost of cash usage at the point of sale (POS) in Canada in 2014 was 0.45% of GDP.

[20] Financial inclusion has been cited as an important development factor. See Levine (2005) and GPFI (2016).

Table 2: Public policy objectives and central bank mandates. List of reasons for issuing central bank e-money categorized in three groups: monetary policy, financial system policy or other public policy objectives. We indicate if these objectives are currently central bank mandates and if those objectives could be achieved with tools other than e-money.

Objective and tools	Central bank mandate	Alternative tools
Monetary policy		
Direct monetary policy implementation	Yes	No
Seignorage (which provides independence)	Yes	Equity, tax transfers
Break below the effective lower bound	Yes	Yes (cash/reserve wedges, etc.)
Financial system policies		
Payments systems safety and efficiency	Yes	Regulation
Financial stability/lender of last resort	Yes	Regulation
Other objectives		
Reserve currency status	No	No
Reduce crime and tax evasion	No	Yes (needs elimination of cash)
Broaden financial inclusion	No	Regulation
Provide or protect anonymity/privacy	Incidentally (cash)	Yes (private suppliers)

analysts this is one key attraction of private digital currencies. This comes of course with drawbacks because anonymity might facilitate nefarious activities. It is important to notice that the anonymity that cash provides is incidental to its form and not a feature that was factored in as its design evolved over the years. Still, a central bank e-money could be designed to balance the legal demand for anonymity and privacy with its risks, possibly offering more *or less* anonymity than cash (Kahn 2017 and Kahn et al. 2005).

An objective that has not received enough attention is the desire of a government to create the first digital version of an international reserve currency. Of course this requires more than technological advances. The feasibility a digital form of cash would be a necessary but not sufficient condition for a digital reserve currency status. For countries that have the other necessary conditions for their national currencies to acquire reserve status, the prospect of large seignorage revenues or of denominating international trade transactions in their digital currency has an obvious appeal.

Although the efficiency of payments could be improved, an e-money system would be exposed to catastrophic cyber risk. These risks could be managed but they will require new skills that central banks do not currently have. In addition to managing new types of risks, central banks would have to decide how the new e-money system would be developed. The central bank could acquire the leading technology, partner with private companies, or develop some new technology internally. Given that national payments systems perform critical functions in the economy, central banks have a higher bar than private companies when testing new means of payments.

6 Concluding Remarks

Cash and the wholesale payments systems, traditionally supplied by central banks, perform socially useful record-keeping services. These have coexisted with many private forms of payments media and clearing and settlement systems. In this paper we addressed one positive and one normative question. First, have the new technological developments fundamentally changed the tradeoffs between centralized and decentralized payments systems? Second, has the role of central banks in the provision of means of payments changed? We looked into several e-money proposals with special focus on the technological details and their implications for efficiency of payments systems and competition of financial intermediaries. We contrasted these proposals to a wide set of public policy objectives.

Our main conclusion is that the new technologies like DLT and mobile computing have not significantly changed the tradeoffs for the specific case of providing central bank accounts to the public. In contrast, these same technologies might have changed the tradeoffs in the provision of token-based systems by central banks. Surprisingly this change will not come through the changes in the efficiency or risk of token systems. Instead, the fundamental change will be that the new technologies might allow central banks or regulators to increase the competition in the market for payments services at the wholesale and retail levels. By offering a token-based system to a wider set of participants, which could include individuals but most likely new financial firms, central banks could increase competition and spur innovation. Although this could have been done even before by opening the high value payments systems to non-traditional financial institutions, the new technologies make the entrance of the central bank a real possibility.

Many questions were left unanswered. The most important ones relate to the effects on the industrial organization of payments services providers, in particular banks. Plenty of work remains to be done to examine the quantitative implications of a new type of token-based system offered by the central bank to bank deposits and bank lending. Also we discussed the evaluation of the tradeoffs from the point of view of the decision to issue e-money by the central bank. However, should the decision be not to issue, or not immediately, the alternative could imply needing to regulate the issuance of private e-money. To be able to make the decision to issue or regulate, central banks will have to evaluate the tradeoffs quantitatively. This justifies further theoretical and empirical work.

References

Ales, L., F. Carapella, P. Maziero, and W. E. Weber (2008). A model of banknote discounts. *Journal of Economic Theory 142*(1), 5 – 27.

Andolfatto, D. (2015). Fedcoin: On the desirability of a government cryptocurrency. http://andolfatto.blogspot.com/2015/02/fedcoin-on-desirability-of-government.html.

Bank of England (2018). https://www.bankofengland.co.uk/news/2017/july/boe-extends-direct-access-to-rtgs-accounts-to-non-bank-payment-service-providers.

Bech, M. and R. Garratt (2017). Central bank cryptocurrencies. *BIS Quarterly Revieew September*, 55–70.

Berentsen, A. and F. Schar (2018). The case for central bank electronic money and the non-case for central bank cryptocurrencies. *Federal Reserve Bank of St. Louis Review 100*(2), 97–106.

Bergara, M. and J. Ponce (2018). Central bank digital currency: the uruguayan e-peso case. *Banco Central del Uruguay*.

BIS (1996). Implications for central banks of the development of electronic money. Technical report, Bank for International Settlements.

BIS (2015). Digital currencies. Technical report, Bank for International Settlements.

Camera, G. (2017). A perspective on electronic alternatives to traditional currencies. *Sveriges Riksbank Economic Review* (1), 126–148.

Cavalcanti, R. and E. Nosal (2011). Counterfeiting as private money in mechanism design. *Journal of Money, Credit and Banking 43*(s2), 625–636.

Chapman, J., J. Chiu, and M. Molico (2013). A model of tiered settlement networks. *Journal of Money, Credit and Banking 45*(2-3), 327–347.

Chapman, J., R. Garratt, S. Hendry, A. McCormack, and W. McMahon (2017). Project jasper: Are distributed wholesale payment systems feasible yet? *Bank of Canada Financial System Review*, 59.

Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology*, pp. 199–203. Springer.

Chaum, D., A. Fiat, and M. Naor (1990). Untraceable electronic cash. In S. Goldwasser (Ed.), *Advances in Cryptology — CRYPTO' 88*, New York, NY, pp. 319–327. Springer New York.

Chiu, J., M. Davoodalhosseini, J. Hua, and Y. Zhu (2018). Central bank digital currency and banking. *Bank of Canada mimeo*.

Chiu, J. and T. Koeppl (2017). The economics of cryptocurrencies - bitcoin and beyond. Technical report.

Chiu, J. and T. Koeppl (2018). Incentive compatibility on the blockchain. *Bank of Canada Working Paper* (2018-34).

Chiu, J. and T.-N. Wong (2014). E-money: efficiency, stability and optimal policy. Technical Report 2014-16, Bank of Canada Working Paper.

Chiu, J. and T.-N. Wong (2015). On the essentiality of e-money. *Bank of Canada Staff Working Papers* (2015-43).

CPMI (2015, November). Digital currencies. Technical report.

CPSS (2003). The role of central bank money in payment systems. Technical report, Bank for International Settlements.

CPSS (2005). New developments in large-value payment systems. Technical report, Bank for International Settlements.

Danezis, G. and S. Meiklejohn (2015). Centrally banked cryptocurrencies. *arXiv preprint arXiv:1505.06895*.

Davoodalhosseini, M. (2018). Central bank digital currency and monetary policy. *Bank of Canada Working Papers* (2018-36).

Davoodalhosseini, M. and F. Rivadeneyra (2018). A policy framework for e-money: A report on bank of canada research. *Bank of Canada Working Paper* (2018-5).

Freedman, C. (2003). Reflections on three decades at the Bank of Canada. Technical report, Bank of Canada.

Friedman, B. M. (2000). Decoupling at the margin: the threat to monetary policy from the electronic revolution in banking. *International Finance 3*(2), 261–272.

Fung, B., S. Hendry, W. E. Weber, et al. (2017). Canadian bank notes and dominion notes: Lessons for digital currencies. Technical Report 2017-5, Bank of Canada.

Fung, B. S. and H. Halaburda (2016). Central bank digital currencies: A framework for assessing why and how. *Bank of Canada Staff Discussion Paper 2016-22*.

Garratt, R. (2016). Cad-coin versus fedcoin. *Mimeo*.

GPFI (2016). G20 high level principles for digital financial inclusion. Technical report, GPFI Global Partnership for Financial Inclusion.

Green, E. J. (2008a). The role of the central bank in payment systems. In S. Millard, A. Haldane, and V. Saporta (Eds.), *The Future of Payment Systems*, pp. 45–56. Routledge.

Green, E. J. (2008b). Some challewnges for research in payments. In S. Millard, A. Haldane, and V. Saporta (Eds.), *The Future of Payment Systems*, pp. 57–67. Routledge.

Green, E. J. and R. M. Todd (2001). Thoughts on the fed's role in the payments system. *Federal Reserve Bank of Minneapolis. Quarterly Review-Federal Reserve Bank of Minneapolis 25*(1), 12.

Kahn, C. M. (2016). How are payment accounts special? *Payments Innovation SymposiumFederal Reserve Bank of Chicago*.

Kahn, C. M. (2017). Privacy. In M. Manning, F. Rivadeneyra, J. Cruz-Lopez, R. Heijmans, E. Benos, D. Muphy, and J. Braithwaite (Eds.), *Proceedings of the Financal Markets Infrastructure Conference II: New Thinking in a New Era*, pp. 1–10. Journal of Financial Markets Infrastructure.

Kahn, C. M., J. McAndrews, and W. Roberds (2005). Money is privacy. *International Economic Review 46*(2), 377–399.

Kahn, C. M., F. Rivadeneyra, and T.-N. Wong (2018). Eggs in one basket: Choosing the number of accounts. *Bank of Canada mimeo*.

Kahn, C. M. and W. Roberds (2008). Credit and identity theft. *Journal of Monetary Economics 55*(2), 251–264.

Kahn, C. M. and W. Roberds (2009a). Payments settlement: tiering in private and public systems. *Journal of Money, Credit and Banking 41*(5), 855–884.

Kahn, C. M. and W. Roberds (2009b). Why pay? an introduction to payments economics. *Journal of Financial Intermediation 18*(1), 1–23.

Kang, K. Y. (2017). Counterfeiting, screening and government policy. Technical report, Washington University in St. Louis.

Kimball, M. (2013). A minimalist implementation of electronic money. *https://blog.supplysideliberal.com/post/50888412664/a-minimalist-implementation-of-electronic-money*.

Kocherlakota, N. R. (1998). Money is memory. *Journal of Economic Theory 81*(2), 232–251.

Koning, J. (2016). Fedcoin: A central bank-issued cryptocurrency. *R3 Report*.

Kosse, A., H. Chen, M.-H. Felt, V. D. Jiongo, K. Nield, A. Welte, et al. (2017). The costs of point-of-sale payments in canada. *Bank of Canada Staff Discussion Paper* (2017-4).

Lacker, J. (2008). Payment economics and the role of central banks. In S. Millard, A. Haldane, and V. Saporta (Eds.), *The Future of Payment Systems*, pp. 68–72. Routledge.

Lester, B., A. Postlewaite, and R. Wright (2012). Information, liquidity, asset prices, and monetary policy. *The Review of Economic Studies 79*(3), 1209–1238.

Levine, R. (2005). Chapter 12 finance and growth: Theory and evidence. Volume 1 of *Handbook of Economic Growth*, pp. 865 – 934. Elsevier.

Li, Y. and G. Rocheteau (2011). On the threat of counterfeiting. *Macroeconomic Dynamics 15*(S1), 10–41.

Li, Y., G. Rocheteau, and P.-O. Weill (2012). Liquidity and the threat of fraudulent assets. *Journal of Political Economy 120*(5), 815–846.

McAndrews, J. J. (2017). The case for cash. *Asian Development Bank Institute Working Paper Series* (679).

Nosal, E. and N. Wallace (2007). A model of (the threat of) counterfeiting. *Journal of Monetary Economics 54*(4), 994–1001.

Quercioli, E. and L. Smith (2015). The economics of counterfeiting. *Econometrica 83*(3), 1211–1236.

Roberds, W. (1995). Financial crises and the payments system: lessons from the national banking era. *Economic Review* (Sep), 15–31.

Rogoff, K. (2015). Costs and benefits to phasing out paper currency. *NBER Macroeconomics Annual 29*(1), 445–456.

Rogoff, K. S. (2016). *The curse of cash*. Princeton University Press.

Saleh, F. (2018). Blockchain without waste: Proof-of-stake. *NYU mimeo*.

Shao, E. (2014). The threat of counterfeiting in competitive search equilibrium. *Journal of Economic Dynamics and Control 47*, 168–185.

Skingsley, C. (2016, November). Should the riksbank issue e-krona? Speech. Speech by Sveriges Riksbank Deputy Governor Cecilia Skingsley at the FinTech Stockholm Conference 2016.

Sveriges Riksbank (2017). The riksbank's e-krona projet, report 1. Technical report, Sveriges Riksbank.

Tobin, J. (1985). Financial innovation and deregulation in perspective. *Bank of Japan Monetary and Economic Studies 3*(2), 19–29.

Weber, W. E. (2015). Government and private e-money-like systems: Federal reserve notes and national bank notes. *Bank of Canada Working Paper*.

Williamson, S. D. (2002). Private money and counterfeiting. *FRB Richmond Economic Quarterly 88*(3), 37–58.

Zhu, Y. and S. Hendry (2017). A framework for analyzing monetary policy in an economy with e-money. *Bank of Canada Working Papers*.

A Other Proposals

In recent years there have been several proposals by central banks and academics ranging from a central bank digital currency to wholesale tokens. Here we describe some of the most notable ones focusing on their design features and discuss some of their potential implications.

CADcoin

The Bank of Canada has experimented with distributed ledger technology in their project Jasper.[21] This experiment is a private and permissioned (restricted) ledger which uses the protocols of Ethereum. The members of this ledger first exchange central bank reserves for an asset called CADcoin. Technically this is done by exchanging settlement balances held at the central bank using the Canadian wholesale payments system called LVTS. In effect CADcoin is a deposit receipt for settlement balances. After acquiring CADcoin, members of the ledger can exchange CADcoin as in most DLT systems: transfers of tokens are subject to the verification of the Ethereum protocol. Within the ledger there is little anonymity of the transactions, something that was deemed as undesirable. See Garratt (2016) for details.

CADcoin is not a widely-available central bank liability, therefore does not fully fit the schemes we consider in this paper. However CADcoin could be the first layer in the delegated schemes we described in section 4.3.

Fedcoin

Fedcoin is another proposal that has received some attention although it has not being official endorsed by the Fed. The theoretical proposal is to have the Fed agree to the creation of Fedcoins by being readily available to convert paper money or bank deposits into Fedcoin. The original proposal was largely based on trying to separate the store of value from the medium of exchange functions in Bitcoin. By having the Fed committed to two-way convertibility between reserves and Fedcoins the value of the token system would be fixed at par. However this proposal did not address the fundamental problem with the costs of exchange of token systems (Chiu and Koeppl 2017).

This proposal is in fact in broader and not necessarily linked to the Fed itself. The general concept is a "stable coin", a token whose supply is managed to maintain its purchasing power either by a peg, a flexible supply by a central bank, or a self-stabilizing supply rule (Koning 2016). The Fedcoin proposal fits the decentralized token scheme described in section 4.2.1.

E-krona

The Swedish central bank is exploring issuing a digital alternative to cash called e-krona. Ths has been motivated in part because the amount of cash in circulation as a percentage of GDP has been falling rapidly and is already below the levels of

[21] https://www.payments.ca/industry-info/our-research/project-jasper

most developed economies at less than 2% of GDP. In a 2016 speech the Sveriges Riskbank deputy governor Cecilia Skingsley launched a project to determine the features of the e-krona specially if it should be account- or token-based and if it should pay interest (Skingsley 2016). The Sveriges Riskbank has committed to an ambitious plan to possibly issue a pilot e-krona by 2019. The first project report (Sveriges Riksbank 2017) outlines the proposals that the Riskbank is considering: register-based and value-based e-krona systems. These largely map to our account- (described in section 4.1) and token-based systems (in section 4.2). Like us, the report examines the payment efficiency, competition and financial stability implications of these two types of systems. In addition the report examines questions about monetary policy.

Central Bank of Uruguay e-Peso Project

The e-Peso was a pilot of the Central Bank of Uruguay intended to test the technology and the adoption by individuals and firms (Bergara and Ponce 2018 and `http://www.epeso.com.uy/`). This pilot fits the delegated token scheme with custodians we described in section 4.3. The e-Peso digital token was issued between November 2017 and April 2018 by the Central Bank of Uruguay. The issuance was 20 million Uruguayan Pesos and the number of users was limited to 10,000 individual mobile phone users and some retail businesses. The maximum balance in e-Pesos wallets was set to 30,000 Uruguayan Pesos (approximately 1,000 US Dollars) for final individual users and to 200,000 for retail business. To acquire e-Pesos, individuals had to exchange bank notes at branches of a specialized retailer called RedPagos. The pilot did not allow exchanging commercial bank deposits for e-Pesos.

In the first layer, the central bank cryptographically issued the e-Peso aided by a technology company which provided the storage, security and verification of transactions. In a second layer, anonymous digital wallets were provided by one fintech company (InSwitch Solutions). The wallets were linked to the mobile phone number of the user therefore potentially providing a way to identify the users. In other words, the e-Peso transactions were pseudonymous. This feature could be useful if for example a judge or the tax authority requires access. Users would initiate transactions through their digital wallets which were verified by the central bank. To prevent double spending each e-Peso token had a cryptographic signature and specific denomination. This is similar to the UTXO model of Bitcoin.[22]

[22] `https://www.smithandcrown.com/definition/unspent-transaction-outputs-utxo/`

RSCoin

The RSCoin proposal by Danezis and Meiklejohn (2015) intends to mitigate the problems of high energy consumption and poor scalability of Bitcoin. In this scheme the central bank is responsible for money creation (the monetary policy) and recording transactions, and delegates the tasks of transaction collection and verification to "mintettes" (similar to miners in Bitcoin). Unlike Bitcoin which maintains one complete blockchain consisting of all nodes, the blockchain of RSCoin consists of two parts: the decentralized lower-level blockchains of all transactions maintained by mintettes and the central bank's main blockchain aggregating all lower-level blockchains. RSCoin has a two-phase commit method to verify a transaction. In the first phase, every mintette in the shard validates the transaction independently. If the RSCoins in the transaction have not appeared before (i.e., double spent), then the mintette returns its signature. If the transaction obtains signatures from more than half of the shard, then the transaction deems "legal" and moves to the second phase. In the second phase the RSCoin user learns another shard which he should send his signatures and transaction to verify the verification. Every mintette in the shard validates all the signatures independently. If the valid signatures are more than half, the mintette records the transaction in its own lower-level blockchain with its own signature. The central bank eventually signs the public key of mintettes (authorization) and incorporates all lower-level blockchains (and its money policy, if any) in the main blockchain. Participants of RSCoin need only keep track of the main blockchain. In the RSCoin system, the set of transactions in lower-level blockchains are decentralized to different shards. RSCoin eliminates the proof of work and reduces the confirmation delay. RSCoin fits the description of decentralized tokens we discuss in section 4.2.1.