CER-ETH – Center of Economic Research at ETH Zurich

A Minting Mold for the eFranc: A Policy Paper

H. Gersbach, R. Wattenhofer

Working Paper 20/342
August 2020

Economics Working Paper Series

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

A Minting Mold for the eFranc: A Policy Paper*

Hans Gersbach
CER-ETH – Center of Economic Research at ETH Zurich and CEPR
Zürichbergstrasse 18
8092 Zurich, Switzerland
hgersbach@ethz.ch

Roger Wattenhofer
Distributed Computing Group
ETH Zurich
Gloriastrasse 35
8092 Zurich, Switzerland
wattenhofer@ethz.ch

This Version: August 2020

Abstract

We suggest a blueprint for an **eFranc** as a possible complement for the Swiss monetary system to ensure the long-term stability of its money. An eFranc is a non-interest-bearing digital form of the legal tender available to the public. The public can convert banknotes or part of its bank deposits into eFrancs, subject to the banks' ability to obtain the corresponding amount of eFrancs from the central bank. There is free conversion of eFrancs into bank deposits (and into banknotes). For the technical implementation of the eFranc, we suggest a two-layer system combining a permissioned asynchronous blockchain without consensus which provides a secure environment for validating transactions (base layer) plus a peer-to-peer payment network (top layer).

Keywords: eFranc, Swiss Monetary System, Financial Stability, Swiss National Bank, Proof-of-stake Blockchains

*We would like to thank Florian Böser, David Mangini, Tejaswi Nadahalli, and Harald Nedwed for valuable comments.

1 Introduction

The current monetary system is the result of an evolution extending over several centuries. How it compares to alternative systems is a long-standing question. New technologies that could possibly be used in various parts of the monetary system—validating transactions, transferring money, controlling the supply of money—have fueled the academic and public debate on whether and how our monetary system could and should change.

The current monetary system has three main actors: the central bank, commercial banks, and the public. These are arranged hierarchically, with the following elements (see e.g. Faure and Gersbach [2018]).[1]

(I) The money stock available to the public is composed of deposits at commercial banks (to a large extent) and of banknotes and coins (to a minor extent). Banknotes and coins are physical central bank money (henceforth "cash") and serve as the sole legal tender.

(II) Cash is issued by the central bank to commercial banks, which use it to settle withdrawals of deposits.

(III) Deposits (electronic private bank money) represent claims on cash but are issued by commercial banks when they grant loans or purchase assets or are created when households deposit banknotes with banks .

(IV) Reserves (electronic central bank money) are issued by the central bank to commercial banks, which use them to settle claims arising from interbank deposit flows when the public makes payments. Only commercial banks have access to electronic central bank money.[2]

(V) Commercial banks have to comply with a set of rules such as liquidity and capital requirements. However, they are not (or only to a minor extent) required to hold

[1] For an analysis of the current hierarchical monetary system, see Faure and Gersbach [2018]. Money creation processes are summarized in McLeay et al. [2014] and Bundesbank [2017].

[2] The precise access rules differ across currency areas and may include a varying number of financial intermediaries other than commercial banks.

central bank money as reserves for their deposits.[3]

Three prominent features of the hierarchical monetary system are of particular importance for our considerations here. First, most money is created by commercial banks. Second, the public only has access to cash and bank deposits but not to electronic central bank money. Third, commercial banks interact with the public and the central bank and are thus the crucial bridge between the central bank and the public.

2 Objectives and Alternative Monetary Systems

Before we can talk about alternative monetary systems, we need to outline the objectives a monetary system should fulfill. The most important objectives can be summarized as follows:

(A) Money should play its traditional roles (unit of account, medium of exchange, store of value), which ultimately requires that its value remains stable – or at least approximately stable – across time.

(B) Price stability should always be by far the most important objective in the long run, which requires the presence of an independent central bank.

(C) Disruptions in the monetary system or crises in the wider financial system should be limited to an absolute minimum, and if they do happen, their spillovers to the real economy should be as restricted as possible.

(D) The democratic legitimacy of all governance processes and all policies involved should be well-founded.

There have been various proposals for changing the current monetary system. At the one extreme, there is the so-called "sovereign money proposal" in which money is solely created by the central bank. At the other extreme, the current hierarchical monetary

[3]For Switzerland see https://www.admin.ch/opc/de/classified-compilation/20021117/index.html and https://www.admin.ch/opc/de/classified-compilation/20040259/index.html#a18 for its minimal reserve rules.

system could be supplemented by a variety of privately issued, competing fiat monies, which do not constitute a claim on the legal tender. However, more modest changes lie between these two extremes. For example, the introduction of a publicly available digital form of the national currency, commonly referred to as "Central Bank Digital Currency" (CBDC), could be envisioned. Such a CBDC could take several forms: interest-bearing or not, account-based or token-based, for example.

To design a CBDC, one first has to specify the functions it should be able to fulfill, such as accessibility, privacy, real-time and cross-border payments, resilience, and whether it should be a complement or substitute for cash. Second, one has to determine which technical designs best fulfill these functions. A comprehensive discussion of all options is beyond the scope of this paper (see e.g. Auer and Böhme [2020] and Bank of England [2020]), so we proceed from two observations that guide our proposal.

First, there are important discussions about the pros and cons of CBDCs that are interest-bearing. This literature is discussed in Böser and Gersbach [2020]. While the introduction of interest-bearing CBDCs might have positive effects through increased competition among banks and thus through higher deposit rates, higher refinancing costs may also have a detrimental effect on investment. Importantly, interest-bearing CBDCs might entail a higher liquidity demand on the side of banks, which, in combination with limited liquidity supply by the central bank, may lead to more prudent bank behavior. However, if the CBDC is in widespread use, a limiting liquidity supply by the central bank would endanger the viability of the banking system. (see Böser and Gersbach [2020]). In turn, relaxing liquidity supply will undo any positive effect of interest-bearing CBCDs on the prudent behavior of banks (see Böser and Gersbach [2020] for this line of reasoning). Hence, the first function of a CBDC should be to act as a substitute for cash and not as a bank deposit substitute.

Second, as to the technical design, the basic decision would be between a conventional centrally controlled database and a distributed ledger. While both designs have advantages and disadvantages, we argue that a specific decentralized design promises a net benefit for society.

3 eFranc

We focus on a non-interest-bearing digital form of central bank money for the public. In particular, we focus on the introduction of a crypto form of banknotes with the name **eFranc (eF)**.[4]

This eFranc is simply a digital form of a banknote, i.e. a currency held and traded only on a distributed ledger such as a blockchain, on which transactions are validated decentrally. Everybody should be allowed to hold eFrancs and to make transactions using eFrancs.[5] An eFranc should allow secure, anonymous holdings of cash, subject to legal constraints, in particular anti-money laundering and know-your-customer rules. Ultimately, an eFranc is a close substitute for banknotes and coins but enables combating money laundering at levels that can be as high as bank deposits. Furthermore, an eFranc opens up possibilities for automatizing some of these legal constraints.

Even if the introduction of an eFranc appears to be only a small change, it entails a new monetary architecture. For instance, it needs appropriate rules before suitable technical requirements can be specified. In particular, since the eFranc constitutes an additional form of legal tender, the central bank has to control its creation directly. There are two ways in which this control can be implemented.

First, mirroring the process by which banknotes enter the economy today, the eFranc could be governed by the following rules, henceforth called the *Complement System*:

- Creation of eF through the Swiss National Bank (SNB).
- Borrowing of eF by banks from SNB against eligible collateral.
- The public can transfer part of its bank deposits to eF, subject to the banks' ability to acquire the corresponding amount of eF from the central bank.
- Free conversion of eF into bank deposits (and into banknotes).

[4] While cryptological methods play an essential role in digital transactions, with a crypto form of banknotes we mean that its transactions are validated on a distributed ledger.

[5] An alternative approach for a digital banknote has been developed by Giori Digital (private discussions with Giori Digital SA on the basis of their Retail CBDC solution).

The Complement System simply adds another (digital) legal tender to the existing monetary system. *Ceteris paribus*, it leaves the stock of money (say M_1 as the sum of cash, eF, and sight deposits) unchanged, but the sum of cash and eFrancs may change.

An alternative approach requires the introduction of an eFranc to leave—*ceteris paribus*—the amount of banknotes and eFrancs outside the central bank unchanged. This system is called the *Substitute System*. It involves the last three rules in the *Complement System*, but the first rule now reads:

- Banks can obtain eF from the SNB by returning the same amount of banknotes to the SNB.

Hence, in the Substitute System, the eFranc can only be created if the same amount of banknotes goes back to the SNB. In turn, this requires that banks have to acquire this amount of banknotes beforehand, either from the central bank or if customers return them. Hence, an eFranc is a substitute for a banknote.

Of course, introducing the requirement that banks have to return physical banknotes to the central bank when they create eFrancs should not add a separate physical process to the system.

Since banks regularly acquire banknotes from the central bank, the amount of eFrancs created by a bank could simply be deducted from these regular flows of banknotes to the banks. One could even envision the central bank only verifying the ability of a bank to acquire the required amount of banknotes to be converted to eFrancs and then decreasing the bank's electronic reserves at the central bank correspondingly. This would be almost equivalent to the Complement System.

We stress that while the SNB controls the creation of eFrancs, the mix between banknotes and eFrancs and between legal tenders and bank deposits is impacted by the public and banks. Moreover, the conversion rules in both systems can be more or less restrictive with regard to the conversion of bank deposits into eFrancs, in order to prevent such switches occurring on a large scale—which would be tantamount to a bank run.[6] At

[6]Moreover, in times of large reserve holdings of banks at the central bank, one might introduce incentives or even restrictions for banks to convert these reserves into eFrancs.

all events, individuals are allowed to switch from eFrancs to bank deposits and, via bank deposits, from eFrancs to banknotes.

Moreover, we envision that banks operating the channels between bank accounts and the blockchain to execute the conversions.[7] Then no further physical and digital infrastructures are needed besides these channels and the blockchain.

Before we address the technical details of the implementation in Section 5, we now focus on the potential economic advantages and disadvantages of an eFranc.

4 Advantages and Disadvantages

An eFranc would have several advantages. First, an eFranc supplements the Swiss monetary system with a digital form of legal tender that is solely controlled by the central bank. The eFranc is a safe nominal asset since holding eFrancs does not involve a counterparty and so there is no default risk. Second, an eFranc acts as a disciplining device on money creation by banks if the use of banknotes declines.[8] Hence, an eFranc can help to stabilize credit and money creation cycles[9] and thus will help the central bank to pursue its main objective—maintaining a stable value for its currency.

Third, the eFranc avoids the costs associated with printing, storing, distributing and protecting physical banknotes. Of course, operating a distributed ledger is not costless, but with an appropriately distributed ledger design as discussed in the next section, these costs are considerably lower than using physical banknotes. Fourth, the use of an eFranc never involves any infection risk, a feature that has suddenly become crucial in the face of the Covid19 pandemic.[10]

Fifth, an eFranc could ensure anonymity for all lawful exchanges and can thus recover

[7] This does not exclude the emergence of further specialized financial institutions operating these channels.

[8] Widespread acceptance and use of banknotes as a medium of exchange is one stability pillar in our monetary system.

[9] The literature has identified several reasons why bank banks allocate too much lending capacity to boom states and too little to bad states (see e.g. Gersbach and Rochet [2017].

[10] Nevertheless, an eFranc does not imply that physical banknotes should be abolished. The unique features of physical banknotes—e.g. complete anonymity, immediate verification of completeness of exchange and protection against negative interest rates—typically outweigh the disadvantages of facilitated tax evasion and criminal activities. Physical banknotes should remain an option for the public (Wissenschaftlicher Beirat beim Bundesministerium für Wirtschaft und Energie [2017]).

properties of physical banknotes. Anonymity is a property that is desired by many citizens as it guarantees freedom to interact with others without the knowledge and potential reaction of third parties. Since an eFranc fulfills anti-money laundering and know-your-customer rules, it does not provide the same level of anonymity as physical banknotes. The state alone is allowed to trace transacting agents back to the distributed ledger, and only in precisely described, exceptional circumstances inscribed in corresponding laws.

Sixth, an eFranc would further limit the possibilities of imposing negative nominal interest rates on market participants. In particular, one consequence of the eFranc is that interest rates on bank deposits will no longer become negative once the monetary system with the eFranc is fully developed. Arguably, this is a desirable property, since it fosters trust in the currency and ultimately helps to stabilize its value.

Seventh, it is envisioned that transactions with eFrancs can be executed in a technical infrastructure that is independent of the existing payment system involving bank deposits and the associated clearing system. The technical infrastructure on which eFranc transactions take place should be tailor-made, such that it can even become a central part of future payment and clearing systems. In particular, the interface between bank-based payment systems and the new blockchain-based payment system could be designed in such a way that a failure of the first would not spill over to the other and vice-versa, thus enhancing resilience against cyber risks, for instance. An eFranc could also help if parts of the whole current electronic payment system, the Swiss Interbank Clearing System (SIC), incurred disruptions.

Eighth, the blockchain with eFrancs allows for new kinds of advanced financial interaction via so-called "smart contracts", which are mutual agreements embedded in an executable computer code. Thus, the contractual clauses would be executed and enforced automatically, without the need of a third party. While smart contracts and the opportunity of borrowing and operating collateralized lending would create a rich financial system on the blockchain, the technical resilience of the infrastructure must be given first priority.

Could an eFranc also have disadvantages? One issue is the conduct of monetary

policy. While any new form of money has an impact on the transmission channels of monetary policy, banknotes in cryptocurrency form would have the least disruptive effects on monetary policy, as long as bank runs are avoided. This takes us to the second issue, since if the interest on bank deposits moves towards zero or when insolvency concerns of banks are present, the eFranc could lead to financial instabilities. At least initially, this requires sufficient restrictions on the conversion of bank deposits to eFrancs. Moreover, a well-capitalized banking sector is not only essential for times without an eFranc, it is even more important when the eFranc has been introduced.

Third, an eFranc needs a functioning blockchain infrastructure—which is not guaranteed at the moment. Since existing proof-of-work blockchains, with their high energy consumption, are not suitable, a new type of blockchain protocol is required, which we will outline in Section 5.

These concerns mean that it is advisable to plan three phases, which we illustrate here for the Substitute System:

- **Launch:** In this phase, creation, access, and amounts of eFranc holdings on the distributed ledger are limited.
- **Experimentation:** Access is granted to the public, while the amounts of eFranc holdings remain limited.
- **Full integration:** All three conversion rules apply:
  - free exchange of physical banknotes into eF,
  - free exchange of eF into bank deposits (and banknotes),
  - exchange of bank deposits into eF subject to the banks' ability to acquire the corresponding amount of banknotes from the central bank.

Ultimately, everybody should have the right to make transactions freely on the blockchain by using the eFranc as a means of payment, and to store the eFranc on the blockchain.

While the above process demonstrates the need for a careful, step-by-step introduction in launching the eFranc, two additional considerations are important. First, the full

integration phase should not take place when the interest rate on sight deposits is zero or below. Otherwise, we might have conversions of such large amounts of deposits that the stability of the banking system would be threatened. Second, at least for some time, banks should keep logs of all the conversions to eFrancs that customers have ordered.

5 Technical Implementation

The technical architecture must satisfy the principles of security, throughput, accessibility, low-cost, and programmability (for a differing classification, see Norges Bank [2018]). A modern architecture will comprise two layers, a base layer that validates basic transactions and a payment network that allows for payments between banks or between a bank and its customers.

5.1 Base Layer

The base layer provides the security of the system. We propose the use of a permissioned asynchronous blockchain without consensus. The basic idea of this base layer was presented in the Asynchronous Blockchain without Consensus (ABC) protocol by Sliwinski and Wattenhofer [2019]. Note that ABC is more highly developed than is necessary for an eFranc design, as it is permissionless. Recently, Facebook's Libra cryptocurrency has advocated for an ABC-like architecture Baudet et al. [2020].

We assume the cryptographic functionality is provided by asymmetric encryption and hashing. Apart from these cryptographic necessities, the base layer does not employ randomization and is completely deterministic. A deterministic protocol is usually simple, which allows for a swift and precise implementation. Moreover, deterministic protocols are easier to understand for laypersons, which might foster acceptance of the eFranc by the public.

ABC is asynchronous, without making any assumptions about network latency: No matter how slowly messages are transmitted, the protocol is guaranteed correct. As such, ABC is fully resilient to all network-related threats, such as delaying messages from

some party or denial-of-service attacks. By disabling communication, an adversary could stop the system from creating and approving new transactions, but the adversary cannot invalidate previously approved transactions or approve illegal transactions. In comparison with orthodox blockchains such as Bitcoin, this improves the security of the eFranc.

Unlike proof-of-work systems, the security of the eFranc system does not depend on the amount of resources devoted, such as energy, computational power, or memory.

In Table 1, we show a summary of the properties of the base layer of the eFranc and the properties of other well-known blockchain approaches.

Table 1: Comparison of ABC to selected other blockchain protocols, adapted from Sliwinski and Wattenhofer [2019]

	Bitcoin Ether.	PBFT	Ouro -boros	Algo -rand	Honey -Badger	eF (ABC)
Permissionless[1]	✓		✓	✓		
Energy-efficient[2]		✓	✓	✓	✓	✓
Finality[3]		✓		✓	✓	✓
Asynchronous[4]					✓	✓
Deterministic[5]		✓				✓
High throughput[6]						✓
Smart contracts[7]	✓	✓	✓	✓	✓	(✓)

[1] The infrastructure of the protocol is provided by the general public.
[2] The total power consumption of the whole system is in the order of 1 kilowatt.
[3] As soon as a transaction is approved, the transaction is final and cannot be reverted.
[4] There are no timing assumptions; the protocol is correct even if the underlying internet is suffering from severe problems.
[5] To keep the protocol simple, randomization is only used in cryptographic primitives.
[6] The system can handle a load as high as millions of transactions per second.
[7] The system allows for smart contracts that can be called by arbitrary participants.

The participants of the eFranc in the base layer form a *Committee* that should be made up of trusted entities of the Swiss financial system, such as the Swiss National Bank SNB, the Swiss Financial Market Supervisory Authority FINMA, the Swiss payment service provider SIX, and possibly some of the core banks in Switzerland such as UBS and Credit Suisse. Since these entities perform quite different functions in the Swiss financial market system, one could also envision the base Committee consisting only of larger banks,

possibly complemented by large insurance companies.

Each of these participates with a computer authenticated with a known public key. We call the set of participants on the base layer the *Committee*. The eFranc requires that strictly more than two thirds of the Committee members obey the protocol. In other words, if the Committee consists of 4 members, at least 3 should be honest.

In the following, we always require the Committee to have 4 members, at least 3 of them being "honest", i.e., complying with the protocol. Alternative designs require 5 honest members out of 7, or 7 out of 10.

The main operation is a transaction transferring eFrancs from one or more input accounts to one or more output accounts. Transactions can be initiated by anyone, including banks that are not part of the Committee.

Every transaction refers to at least one previous transaction, such that all transactions form a directed acyclic graph (DAG). The initial transaction of the DAG represents the initial stake in the system, i.e., no eFranc is assigned to anybody. The eFranc is created with a transaction as well. The input of such a creation transaction is simply signed by the central bank, the outputs are accounts of the commercial banks that have provided cash to the SNB in exchange for the newly created eFranc.

An adversary issuing conflicting transactions is a primary threat to blockchain systems. Traditionally, it has been assumed that blockchains need to feature a technical primitive known as "consensus" to validate *exactly* one of the transactions issued by a misbehaving party. The eFranc does not need such a costly consensus routine. If an adversary is issuing conflicting transactions, the eFranc only guarantees that *at most one* transaction is valid.

A transaction, denoted by t, is confirmed by the system if enough (3 out of 4) Committee members (directly or indirectly) acknowledge t. If a transaction receives 3 (out of 4) support (digital signatures) by the Committee, no other transaction conflicting with t can be confirmed. In particular, if the owner attempts to execute the transaction t' that is trying to spend (some of) the same input(s) as t, the eFranc system (the honest Committee members) will reject t'. If an owner issues two conflicting transactions t

and t' at roughly the same time, it is possible that (a) either t or t' is confirmed (but not both), or (b) neither t nor t' are ever confirmed. Case (b) happens if some system Committee members see and try to confirm t, while others see and try to confirm t'. The system might remain in this state forever, with the Committee being split between t and t', without any clear majority. Crucially, such a situation can only arise if the issuer of t and t' intentionally misbehaves – and has not done so by accident. In such cases, it is reasonable to punish the issuer.

What if an honest participant suggests a transaction t, but only 2 out of 4 Committee members sign this transaction t? In this case, the issuer of the transaction must simply wait. The issuer can remind the two trailing Committee members to sign the transaction t, but no signature can be enforced. Honest Committee members will sign all transactions that are correct. They cannot abstain from signing a correct transaction. The only excuse for not signing a correct transaction t is that a Committee member has not yet received transaction t, e.g. because of a damaged internet. As soon as the underlying internet is fixed, transaction t will be signed.

The bottleneck in this system is that every Committee member needs to verify validity before digitally signing any transaction. We can mitigate this problem in two ways. First, verifying validity and digital signing can take place in parallel. If a Committee member is overwhelmed by the number of transactions, it can set up k computers, each being responsible for a different set of transactions. For instance, depending on the last b bits of the input(s) of a transaction, the transaction will be sent directly to the right machine out of $k = 2^b$ machines in total. This machine will independently verify and digitally sign the transaction on behalf of the Committee member owning the machine. This way, the base layer can achieve a k times higher throughput than blockchains that rely on consensus, for an arbitrarily large k.

However, an even more efficient remedy would be the introduction of a payment network as a higher layer. This we discuss next.

5.2 Payment Network

On this layer, participants do not have to be Committee members. Payment channels or payment networks are peer-to-peer agreements between any set of participants. They permit implementation flexibility, and as such, they will not be discussed in detail in this paper. More detailed information on payment networks can be found in the literature, including the original papers: Decker and Wattenhofer [2015], Poon and Dryja [2016].

Payment networks can make use of financial institutions acting as eFranc financial intermediaries or simply as middlemen. A middleman can be a commercial bank, another existing financial institution, or an institution specifically created for operating eFranc transactions.

Small payments can be exchanged back and forth directly between two or more participants or middlemen. Transactions may use sequence numbers, so that the latest state of the channel is always clear. Each transaction will be signed by the issuer of the transaction.

More concretely, let us have two financial middlemen A, B who establish a payment channel. Originally, the two middlemen assign some funds to the channel by transferring some amount of eFrancs to that channel. This eFranc might stem either from their own assets, or could be partially borrowed from the central bank against collateral.

Now the middlemen could send each other transactions. If middleman A wants to make a payment to middleman B, A simply signs a transaction and sends the signed transaction to B. At some point, middlemen A and B might disagree on the total amount of eFrancs they have exchanged so far, i.e., on how much money is owed to whom.

In the event of such a dispute, either A or B can call on the underlying base layer. The eFranc base layer will then ask A and B to present their evidence on the current state of the channel. This evidence takes the form of the last signed transactions, reflecting the current state of the payment channel. Based on this evidence presented by A and B, the Committee will then close the channel and the funds will be distributed to A and B accordingly. Note that the base layer Committee will judge the situation entirely mechanically, without human intervention.

In contrast to the operations on the base layer, this is a synchronous operation because the Committee needs to wait to hear from *all* involved channel parties (both A and B in our previous example) before making a decision. One might implement some form of timeout if one of the involved channel parties does not answer within a given time frame. Note, however, that such channel disputes should be rare, as one of the involved channel parties must act maliciously, for such situations to occur. Since the other channel parties have hard evidence of malicious behavior in the form of signed transactions, such punishable behavior should be even rarer.

Alternatively, one might involve some watchtower for each channel, which will also provide evidence if the base layer Committee asks for evidence and one of the participants does not provide it. This variant of a payment network has recently been described by Avarikioti et al. [2019].

Smart contracts can be supported by these payment channels. Indeed, the eFranc will probably have various forms of payment networks, with some channels supporting smart contracts and others not.

5.3 Accounts

As a consequence of our two-layered system, various forms of eFranc accounts may exist. Banks (and other financial institutions) will have one or more base layer accounts. These accounts will, for instance, be used to establish new eFranc accounts for consumers.

In addition, banks, as part of the set of eFranc middlemen, will also hold accounts on the payment layer. Some of these accounts will engineer payments among customers and between customers and service providers. These payment layer accounts may form channels with other eFranc middlemen, and, as such, a payment layer account might be directly funded with eFrancs.

Also on the public side, different accounts may exist. For instance, a person may wish to (a) own a base layer account. The advantage is that such an account is relatively anonymous, as only the bank that originally established the account knows the identity

of the account holder.[11] The account is independent of the bank that established the account, as the account holder can issue (signed) transactions completely autonomously without interacting with third parties. Such an account is relatively close to cash and shares a major downside risk incurred by cash: If the account holds a large amount of eFrancs, the account holder must protect its digital signature (private key) carefully, since anybody who knows the digital signature can immediately transfer money to another eFranc account. On the other hand, a person may independently store large amounts of eFrancs in a tiny security box.

For eFranc accounts storing large amounts of money, it may be beneficial to create (b) a multi-signature account. In this case, every transaction must be co-signed by both the account owner and his/her bank (or some other third-party trustee). This type of eFranc account is similar to a bank safe deposit box.

Finally, a person may also have (c) a payment layer account. This account may be used for daily payments of small sums. There might be a payment network between the consumers and a coalition of merchants. A consumer simply sends a signed payment layer transaction to a merchant, for example by holding the consumer's near-field communication (NFC) mode enabled phone against a merchant tag. This type of account is similar to cash and debit cards.

5.4 Offline Payments

One of the fundamental advantages of cash is its availability in disaster situations, e.g., earthquakes, revolutions. A situation without internet would pose a challenge to the banking infrastructure, while cash also works offline—without electricity, internet, or computer. Following the example of Sweden, we may become a cashless society at some point in time. Then any lengthy interruption in the electricity supply or of the internet infrastructure would be problematic! It is of paramount importance for the eFranc to offer some form of emergency offline payments. Such payments are possible with both (a) base layer accounts and (c) payment layer accounts.

[11] One might envisage law enforcement being entitled to learn the identity of the account holder, in the event of the account displaying connections with illegal activities.

We envision the eFranc being able at least to withstand a situation where neither consumers nor merchants have access to the internet. Both consumers and merchants have, however, a battery-powered device such as a smart phone. These devices can communicate via some short-range means of communication such as NFC or Bluetooth. In an emergency situation, the merchant may decide to accept a transaction from the consumer although it cannot be validated by (a) the base layer Committee or (c) the payment channel mechanism. After accepting the payment, the merchant will present the transaction to (a) the base layer Committee or (c) the payment channel at a later stage, when online services are working again.

There are two risks associated with offline payments. First, a fraudulent consumer may have manipulated their phone and present a transaction for which the input is a non-existent (imaginary) account. The merchant can fend off such an attack by only accepting offline payments from accounts already known to the merchant. For instance, the merchant knows the account because the consumer has shopped at the store before; or the consumer may have registered an account in a public list of accounts (known to merchants), so that the consumer can continue to make transactions if only offline payments are possible.

Second, a fraudulent consumer may have little or no money in their account but nevertheless wants to buy goods and services. Again, for this to happen, the consumer's phone must have been manipulated. Otherwise, the consumer's phone (knowing the account balance) will not sign the transaction. During the payment process, such an attack is not detectable by the merchant. However, since the merchant receives a signed transaction from the consumer, the merchant has proof in the form of the signed payment. The fraud will be detected when the internet connection is reestablished, as the transaction cannot be validated by (a) the base layer Committee or (c) the payment channel. We assume that such cases of fraud will be rare, as the consumer's name can be identified by law enforcement. Changing the software to commit fraud is a severe breach of the law, and a dishonest consumer will incur prosecution.

5.5 Governance and Challenges

Although transactions on a blockchain rely on decentralized validations of transactions, the maintenance and development of the infrastructure requires additional governance and funding. In particular, improvements to the technology, introducing technical upgrades, and changes of parameters and in communication have to be taken care of. While some of the these tasks can also be decentralized over time, they should be entrusted to a new public entity operating the eFranc infrastructure. It might be conceived in a similar way to SIX, which operates the infrastructure for the Swiss financial system.

Moreover, a number of technical challenges still need to be addressed, as our paper can only be a first draft of these new processes and structures. In particular, the eFranc might explicitly support offline money.[12]

Moreover, if the internet is down, no transactions can be verified by the Committee. Hence, no new channels and payment systems can be established until the internet resumes its functions. As discussed above, the payment layer can continue to operate for some time if the internet is down.

6 Conclusion

We suggest introducing the eFranc in an experimental phase in the Swiss monetary system. The eFranc would not revolutionize or disrupt the monetary system, but would enable the system to evolve in a controlled manner. Such caution is desirable, as each step towards new technologies has to be adapted and analyzed carefully to maintain the systems in their functions at all times.

[12]The current e-krona project of the Sveriges Riksbank intends to develop a "value-based" system that would enable the public to hold electronic central bank money either on a prepaid card or on a mobile phone (https://www.riksbank.se/en-gb/payments–cash/e-krona/, accessed on 04/11/2019). For an analysis of the differences and similarities between a value-based and an account-based system, we refer the reader to Kahn et al. [2018].

References

Raphael Auer and Rainer Böhme. The technology of retail central bank digital currency. *BIS Quarterly Review*, March 2020.

Georgia Avarikioti, Eleftherios Kokoris Kogias, and Roger Wattenhofer. Brick: Asynchronous State Channels, 2019.

Bank of England. Central bank digital currency: Opportunities, challenges and design. *Bank of England Discussion Paper*, March 2020.

Mathieu Baudet, George Danezis, and Alberto Sonnino. Fastpay: High-performance byzantine fault tolerant settlement, 2020.

Florian Böser and Hans Gersbach. Monetary policy with a central bank digital currency: The short and the long term. *mimeo*, 2020.

Bundesbank. The role of banks, non-banks and the central bank in the money creation process. *Deutsche Bundesbank Monthly Report*, 2017.

Christian Decker and Roger Wattenhofer. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In *17th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), Edmonton, Canada*, August 2015.

Salomon Faure and Hans Gersbach. On the money creation approach to banking. *CEPR Discussion Paper*, Nr. 11368, 2018.

Hans Gersbach and Jean-Charles Rochet. Capital regulation and credit fluctuations. *Journal of Monetary Economics*, 90:113–124, 2017.

Charles Kahn, Francisco Rivadeneyra, and Tsz-Nga Wong. Should the central bank issue e-money? *Bank of Canada Staff Working Paper*, 2018.

Michael McLeay, Amar Radia, and Ryland Thomas. Money creation in the modern economy. *Bank of England Quarterly Bulletin*, 2014.

Norges Bank. Central bank digital currencies, 2018. URL https://www.norges-bank.no/en/news-events/news-publications/Reports/Norges-Bank-Papers/2018/norges-bank-papers-12018/.

Joseph Poon and Thaddeus Dryja. *The Bitcoin Lightning Network*. 2016. URL https://lightning.network/lightning-network-paper.pdf.

Jakub Sliwinski and Roger Wattenhofer. ABC: Asynchronous Blockchain without Consensus, 2019.

Wissenschaftlicher Beirat beim Bundesministerium für Wirtschaft und Energie. Zur Diskussion um Bargeld und die Null-Zins-Politik der Zentralbank, 2017. URL https://www.bmwi.de/Redaktion/DE/Publikationen/Ministerium/Veroeffentlichung-Wissenschaftlicher-Beirat/gutachten-wissenschaftlicher-beirat-gutachten-diskussion-um-bargeld.pdf. Accessed: 17. December 2019.