Arne Pfeilsticker

Project Description

New Money Infrastructure

(Status: Jan./4th/2018)

Feedback is welcome to Arne.Pfelsticker@pfeilsticker.de or visit
https://github.com/money-infrastructure

Content

Introduction

WHAT is the *New Money Infrastructure*?

The ***New Money Infrastructure*** project aims to develop a global and decentralized crypto-currency infrastructure for payments and other financial services as well as financial instruments. The planned infrastructure will significantly differ from the current infrastructure of the financial sector as well as from the current crypto-currencies and will have the following main-features:

- It is developed for classical currencies and converts, for example, euros into crypto central bank euros (positive money, Vollgeld).
- It consists of standards and open source programs that run on users' existing hardware (mobiles, computers etc.) with internet access.
- It transmits payments directly between users and prevents them from manipulating their own or others' data.
- It is an instrument for people and the real economy that works independently of the existing financial sector.
- It promotes fair trade and sustainable business practices in a very efficient way.

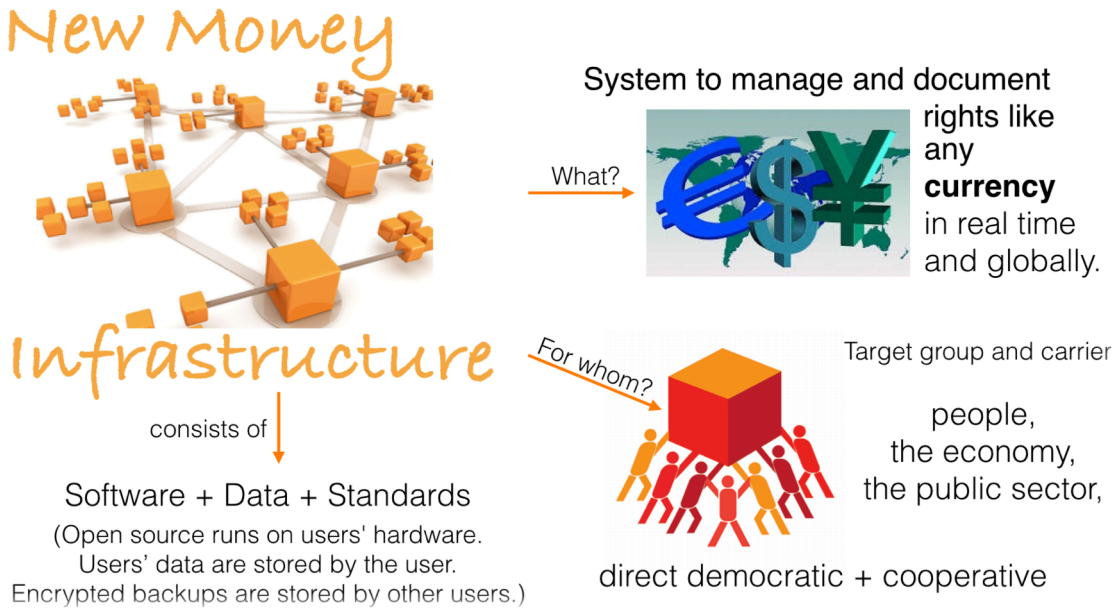


Chart 1: New Money Infrastructure

For the user the *New Money Infrastructure* will appear like a mix of online banking and PayPal with the difference that the users will create and manage their accounts themselves. Users will also experience that the complexity of banking and financial instruments is significantly reduced and additional features are available.

Through an interface, payments between the *New Money Infrastructure* and commercial banks can be made in the usual way. For a *New Money Infrastructure* account, a regular international bank account number (IBAN) can be requested and in that case the account will appear like a regular current account; but would be comparable in terms

of quality with an account at the central bank or cash.

The interface is also a firewall that protects the real economy from turbulences in the financial sector.

Key ideas

Although some key ideas have been adopted from cryptocurrencies, there are significant differences and new ideas.

Crypto-packaging for normal currencies: Banknotes securitize money, current accounts book the money, and the *New Money Infrastructure* proves and provides ownership of money using cryptographic methods. The infrastructure is not meant to create new money, but offers alternative "packaging" for existing money.

Ultimate decentralization: The *New Money Infrastructure* is decentralized in three ways:

1. No central administrative authority.
2. Each user stores only his own data and optionally encrypted backups of other users.
3. Transactions and contracts are only exchanged between the parties directly involved.

As a result, data volume and traffic are kept to a minimum while maintaining maximum efficiency, effectiveness and privacy.

The current cryptocurrencies are decentralized in the first sense that there is no *central authority* that manages the system but there is a common ledger, the blockchain, whose data is stored by all full nodes[1].

Early in 2018, the blockchain was about 160 GB in size and there were about 15 million users, but less than 10,000 full nodes that all the other users need to trust in. One of the key objectives of a decentralized system in which no trustees are required is not realized in practice by Bitcoin. - For this, each of the 15 million users would need to store the blockchain, resulting in a data volume of 2,400,000,000 GB, plus an even higher traffic.

In the New Money Infrastructure, the 160 GB would be distributed amongst the 15 million users according to their individual use and without the need of trustees. This result is achieved through a newly developed *inverse consensus mechanism*.

Inverse consensus: For all cryptocurrencies, the consensus mechanism is key to authenticating and validating values or transactions. So far, this problem has been solved purely technically.

Our newly developed *inverse consensus mechanism* will also integrate legal aspects. The signed data will be distributed *inversely* amongst the contracting parties with the result that a user who manipulates his data would destroy his own rights and yet would have to fulfill his obligations under the contract. Rights and data will be inextricably linked, in

[1] The clients in the Bitcoin network are called nodes. A full node is a client who stores the complete block chain. More: https://en.bitcoin.it/wiki/Full_node

the same way as rights and paper is linked in securities. The rights from the data follow the rights at the data. The power of control over the data is ensured by cryptographic methods and possession.

The correctness of the content of the data is also ensured by the inverse interest of the contracting parties: The rights of the creditor are the obligations of the debtor.

For example, a contract signed by the seller certifies the rights of the buyer and the obligations of the seller. This unique data is stored in the buyer's blockchain. As a result, only he can actually and legally dispose this data. The buyer cannot manipulate these data because they were signed by the seller. And without this data, the buyer cannot assert his rights against the seller and the seller is under no obligation to perform.

And vice versa, the contract signed by the buyer certifies the rights of the seller and the obligations of the buyer. This unique data is stored in the seller's blockchain and only he can actually and legally dispose this data.

The inverse consensus mechanism causes users to not manipulate their data, otherwise their own rights would be destroyed. Therefore, the data must be protected only from accidental and third party manipulations, hardware failures and software errors. To prevent such incidents, there are several redundant protection mechanisms installed that can be supplemented by the user himself, if he wishes to do so.

"Proof of Work" is currently the consensus mechanism in the most popular cryptocurrencies, such as Bitcoin. In doing so unimaginable amounts of energy are needed in addition and the scalability of the system is set to very narrow limits.

For our *inverse consensus mechanism*, no energy is needed, scaling is independent from the number of users and transactions can be executed in real time.

Fair trade and sustainable business practices are an extra asset, implemented as an efficient and profitable business model.

Within the *New Money Infrastructure*, business is done with recommended, standardized and balanced contracts (RSB contracts). Contractors should be able to focus on their performance and not have to worry about being tricked by legal intricacies.

RSB contract templates capture and extend the idea of "Smart Contracts". Simply explained an RSB contract is an instrument that allows users to easily and efficiently conduct their business without having to understand the legal side. Users can trust that the different interests are balanced. They are abstract legal structures that, like numbers in mathematics, are described differently in different languages, but have the same meaning in all languages. For RSB contracts there is a localized certified copy in all required languages. The claims and also possible legal consequences in the event of disruptions to performance are clearly indicated in a transparent manner.

What applies to trade in general will apply even more to financial services and financial instruments, which will serve exclusively the people and the real economy.

RSB contracts are well thought out and well coordinated. They implement the idea of international standards in the field of contract law. The motto is as few templates as possible and as much as necessary.

RSB contracts are objects in the sense of object-oriented programming. They have a status, react to events and can communicate with the parties or act legally. For example, payments are not made to the payee but to the contracts, which are then forwarded to the payee upon confirmation of reception of the goods by the payee.

If necessary, RSB contracts generate all the accounting records in various accounting standards that belong to a contract and its related transactions.

RSB contract templates are developed by users, validated by stakeholders and adopted by majority vote.

The RSB contracts go far beyond the points raised, and exploiting their potential will not only be the task of a follow-up project, but will provide business opportunities in many areas.

This includes:

1. Automatic accounting not only for companies but for the public sector as well
2. Business and economic evaluations to an unprecedented extent and quality
3. Risk management and services
4. Default management and services
5. Collateral management and services
6. Rating services

WHAT is the 'status quo' of todays' financial world and the crypto currencies?

Today there is an over-supply of financial services and financial instruments worldwide. A lot of them are incomprehensible and certainly not transparent, even for experts. As far back as 2006, global money and financial instruments' supply had six times more volume than the gross domestic product of the entire world.

However, the financial sector has left its service role in many areas for the real economy, with the sole aim of making more money out of money.

With the income and profits generated, goods and services of the real economy are bought without the financial sector itself making a substantial contribution.

These 'none performance-related incomes' are considered completely normal and perfectly alright by the recipients. It is ignored that in the macroeconomic context, these incomes predominantly go to the disadvantage of the middle and lower classes.

And also the current crypto-currencies, such as Bitcoin do not represent a real alternative, because by decoupling money production from any institutional or governmental control, the failures in the financial sector will only be driven to new and so far unknown levels.

WHY do we want to offer something different?

Because we want:

- To provide financial services for everybody in the world[2], simple, easy and fair.
- To give central banks the possibility of a monetary policy independent of the financial sector.
- To better protect people and the real economy from the negative impact of the financial sector and from financial crises.
- To make banking services much more efficient and user-friendly through innovative ideas.
- To make the entire exchange of goods and services more fair and transparent, not just financial services and instruments.
- To stop banks of buying goods and services from the real economy with self-made money.
- To increase the profit for the community from the central bank money creation.
- To leave the field not to the existing crypto-money scene for an uncontrolled private money creation.

HOW do we want to make a difference?

Within the *New Money Infrastructure*, the money is central bank money (positive money, Vollgeld) in contrast to the money at a current bank account and in contrast to Bitcoins, which is completely unregulated private money and serves predominantly speculative purposes.

It will be comparable to cash and thus even safer as commercial bank money in case of financial crises. It will be more secure against counterfeiting and theft compared to cash since cryptographic methods are used.

Chart 2 shows the key features of cash, deposit money, Bitcoin, and money in the *New Money Infrastructure.*

The technical design of the *New Money Infrastructure* will be implemented in the 'style' of Wikipedia (from bottom to top and supported by many for all).

"As simple as possible, but not simpler" is the guiding principle of the *New Money Infrastructure* for the design of financial services and financial products and the execution of contracts.

The introduction and operation of the *New Money Infrastructure* deliberately does not rely on the idealism of supporters and users but on solid economic benefits for those involved.

---

[2] World Bank documentation shows that 2 billion people in the world do not have any access to bank services, mainly in the developing countries, which does not make their situation any better.

	Cash	Deposit Money	Bitcoin	New Money Infrastructure
Kind of money	central bank money	commercial bank money	private money	central bank money
Kind of rights	claim against central bank	claim against commercial bank	ownership of data	claim against central bank
Proof of ownership	banknotes, coins	current account	common blockchain	individual blockchains
Primary use	medium of exchange	medium of exchange	speculation, medium of exchange	management and documentation of all rights & obligations
Payment is made by	agreement and delivery	digital transmission	digital transmission, (+ agreem. and del.)	digital transmission, (+ agreement and delivery)
Proof of a transaction	none - optional receipt	account entry	transaction entry in blockchain	transaction entry in blockchain
Fraud protection	hard to fake + threat of punishment	account management by bank + statement	blockchain, Proof of Work, cryptography	blockchain-tree, inverse Consensus, cryptography
Holding money	decentralized by owners	centralized at banks	centralized at full nodes	decentralized by owners
Account management by	-	banks, i. at the debtor	miners	users, i. at the creditor + database functions
System carrier	central banks	commercial banks	bitcoin users	users (+ non-profit org.)

Chart 2: Key features of cash, deposit money, Bitcoin, and money in the New Money Infrastructure

Project description

CONTENT of the project

The *New Money Infrastructure* consists of two functional subsystems:

1. A rights and obligations management system to create and fulfill contracts.
2. A rights and obligations documentation system to document and evaluate contracts and transactions.

In the context discussed here only those rights and obligations are considered which can be assigned a value and thus can be bought or sold at a price. The rights and obligations include the assets and liabilities of a balance sheet.

Credit money is considered as a legal relationship between a creditor and a debtor. The one end is a claim and thus a right and the other end a liability and thus an obligation.

The situation is quite different with bitcoins, which are special property rights on data in the blockchain.

The considerable simplifications result from this abstraction and generalization. This makes it possible that not only money but all rights and obligations can be mapped, managed and processed internally in the same way.

The planned project will be an open source project being managed in GitHub: https://github.com/money-infrastructure

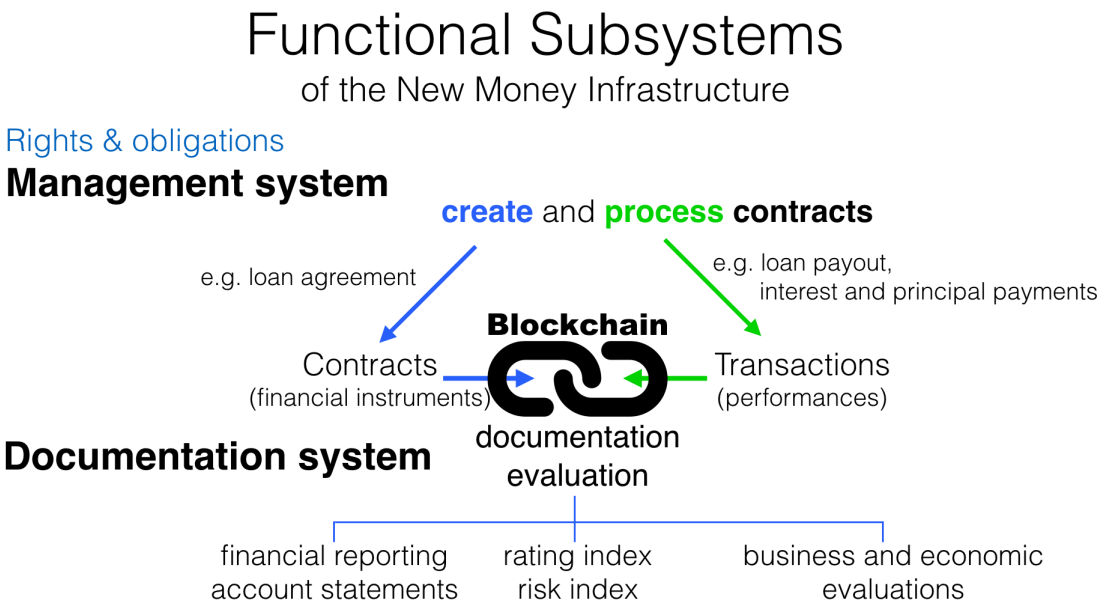


Chart 3: Functional Subsystems of the New Money Infrastructure

WHAT are the planned deliverables of the project?

The planned deliverables consist of:

1. Research into and gathering the latest developments of the current crypto-money scene and evaluate/analyze the results for this project.
2. Specifying features of the New Money Infrastructure in detail, serving as guide-lines for the software development.
3. Defining the architecture that will make up the New Monetary Infrastructure.
4. Develop, program and build an app that allows users to manage and handle their accounts and contracts.
5. Develop and build an Identity Server Cluster (ISC) prototype, where users can register to participate in the New Monetary Infrastructure.
6. Development and production of examples of recommended, standardized and well-balanced contract templates (RSB-Contracts) by which financial services can be used and financial instruments realized.
7. Technical documentation, handbook and video-tutorials for the New Money In-frastructure.

HOW MANY people will work on the project?

Like any open source project, this project will appreciate any form of support.

However, besides the 4 acting NGOs, Monetative e.V., FairShare e.V., Schweizer Vollgeld-initive and the Dutch organisation OnsGeld, a professional base of paid staff is needed as it will involve a great deal of IT, banking, payments and legal expertise, and work in a coordinated and result-focused way.

Therefore, a research, development and expert team of approx. 15 people is planned.

HOW long will the project take?

The project is planned for about 18 months.

HOW will the software be developed?

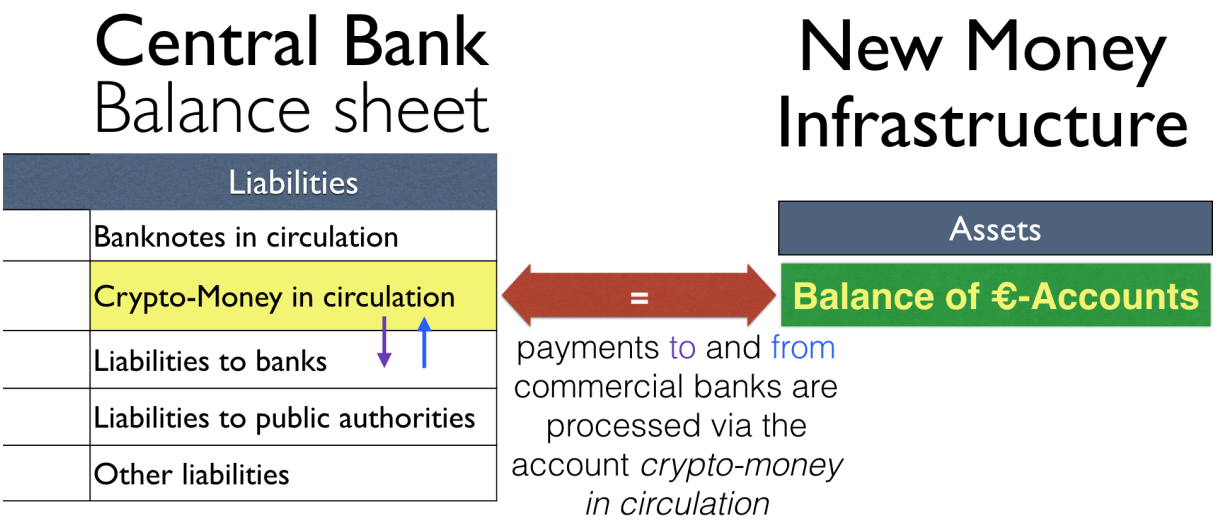
The software will be developed by mixing Scrum and Extreme Programming ideas. This method also involves continuous testing throughout the development.

Parallel to the development environment, a test infrastructure will be set up that allows testing of all aspects under real conditions. In this test environment, anyone who wants to get to know and test the system can participate but participants will also be selected and invited by profile and randomly. The "money" used in the test environment will be test-money.

On the provider side it would be particularly helpful if one or more central banks would be involved in this project.

A system-compliant integration could be carried out analogously to the position "Banknotes in circulation" via a new balance sheet item: 'Crypto-Money in circulation'.

The underlying accounts would be used to settle payments between the *New Money Infrastructure* and commercial banks.



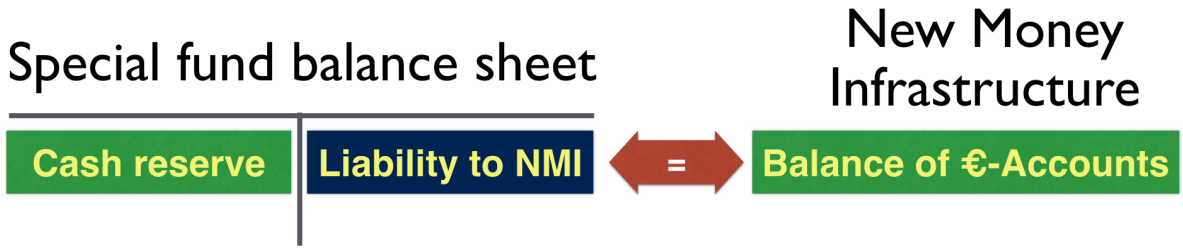
The new position *Crypto-Money in circulation* represents the liabilities of the claims at the €-Accounts of the New Money Infrastructure.

The cooperation with a central bank is not mandatory. If no central bank agrees to cooperate, the interface to the central bank could also be established through an ethical bank.

This bank would manage the cash reserves of the money infrastructure, legally owned by the respective crypto-money holders.

Integration of Banks

- Acceptance of positive money (Vollgeld)
- Banks are equal users of the New Money Infrastructure.



Risks and chances

Risks arise in the areas in which completely new territories are entered and the concepts must be proven in practice.

The project itself could be seen as competition to existing banking services and therefore be opposed by commercial banks.

But since many banks have already announced their interest in crypto currency systems they might very well also be open to this concept and want to join in rather than fighting the new challenges.

The opportunities are incomparably greater than the risks.

Once the *New Money Infrastructure* will be implemented it will be recognized as a real alternative and supplement to existing banking- and payment systems.

Users in all categories of income and transaction volumes will be treated equally in the system, giving access to financial services even to such users who are today uninteresting customers for commercial banks.

A mobile phone, tablet or computer with internet access is all the users will need to participate and the users will quickly understand all the advantages the *New Money Infrastructure* is providing for them.

In case of financial crisis the decision makers in politics could react and act much more relaxed since banks would no longer be systemically important and could be liquidated in the event of bankruptcy.