Co-op Money Infrastructure - White Paper

Arne Pfeilsticker

Table of Contents

(Work in progress - Last update: 2018-04-11)

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

1. What is the *Co-op Money Infrastructure*?

The ***Co-op Money Infrastructure*** project aims to develop a global and decentralized infrastructure for payments and other financial services as well as financial instruments. The system is generalized such that any right or obligation can be documented, proven or transferred. As a result, it could also be used as a general trading platform.

The planned infrastructure will be significantly different from the current infrastructure of the financial sector as well as the current cryptocurrencies and will be characterized by the following main features:

- It is developed for classical currencies and converts, for example, euros into crypto central bank euros, also known as digital cash, positive money, secure money or Vollgeld.
- It consists of standards and open source programs that run on users' existing hardware with internet access, such as mobiles or computers.
- It transfers payments or any other rights 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.

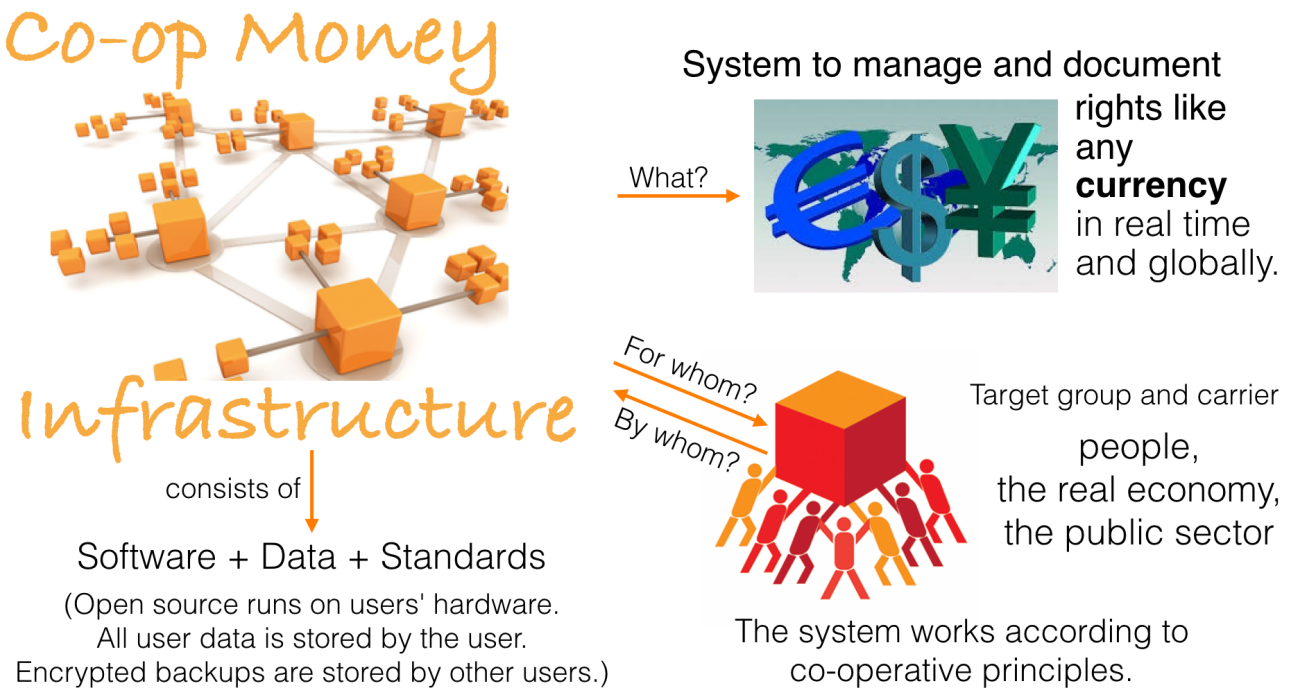

Figure 1. Co-op Money Infrastructure

For the user the *Co-op 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 find that the complexity of banking and financial instruments is significantly reduced and additional features are available.

Through an interface, payments between the *Co-op Money Infrastructure* and commercial banks can be made in the usual way. For a *Co-op Money Infrastructure* account, a regular international bank account number (IBAN) may 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.

2. What is the status quo of today's financial world and the cryptocurrencies?

Today, there is an overwhelming supply of financial services and financial instruments worldwide. Many of them are incomprehensible and not transparent, even to experts. As early as 2006, the global supply was six times greater than the gross domestic product of the entire world.

Despite this glut, the financial sector has left its serving role for the real economy in many areas, with the sole aim of making more money out of money. In terms of value, more than 90% of all payments are made today not with legal tender, but with fiat money made by private commercial banks.

With this self-made money and the income and profits generated in the financial sector, goods and

services of the real economy are bought without the financial sector itself making a substantial contribution.

These '*none performance-related incomes*' are considerable and 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 to the real economy as a whole.

And even the current cryptocurrencies like Bitcoin are not a real alternative, because decoupling money production from any institutional or governmental control only makes the flawed development in the financial sector worse.

Especially with Bitcoin it becomes clear that speculative profits are the goal and not sustainable economic activities.

Not only because of huge price fluctuations and limited transaction capacity, but also because a single transaction with Bitcoin consumes more than 900 kWh of electricity. Bitcoin as a common currency is worse than useless. Global electricity consumption would double if VISA changed its payment system to Bitcoin technology.

Despite this criticism, we do not misjudge the potential of cryptocurrencies. On the contrary, decisive ideas for the money infrastructure come from the field of cryptocurrencies.

3. Why do we want to offer something different?

Because we want:

- To provide financial services for everybody in the world [1: 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.], simple, easy and fair.
- 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, sustainable 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 give central banks a new possibility of their monetary policy independent of the financial sector.
- To leave the field not to the existing crypto currency scene for an uncontrolled private money creation with an irresponsible waste of resources.

4. How do we want to make a difference?

Within the *Co-op Money Infrastructure*, the money becomes central bank money, also known as digital cash, positive money, secure money or Vollgeld. It is thus in contrast to money in a current account at a commercial bank and in contrast to bitcoins, which are still completely unregulated private money and serve a predominantly speculative purpose.

It would be comparable to cash and thus even safer in the case of financial crises than commercial bank money. Compared to cash, it would be better protected against counterfeiting and theft by using cryptographic methods.

An overview of key features between cash, deposit money, Bitcoin and the co-op money infrastructure is shown in the following table:

	Cash	Deposit Money	Bitcoin	Co-op 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, legal 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.)

Figure 2. An overview of key features between cash, deposit money, Bitcoin and the co-op money infrastructure

The implementation of the *Co-op Money Infrastructure* is planned 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 *Co-op Money Infrastructure* for the design of financial services and financial products and the execution of contracts.

The introduction and operation of the Co-op Money Infrastructure is based deliberately not on the idealism of supporters and users, but on considerable economic benefits for those involved.

Due to the design, only a fraction of the current cost of financial services would be incurred and the gross profit from financial products could be shared by the contracting parties because the business could be done without banks. The gross profit of German banks in 2010 amounted to € 92 billion, of which a substantial part would be up for discussion.

There are additional savings in trading and accounting.

The money infrastructure contributes to the decentralization of the power concentrated in the financial sector, which is given back to the people and the real economy. "Too big to fail" and "too interconnected to fail" would no longer be a problem in the case of financial crises.

5. Project description

5.1. Content of the project

The *Co-op Money Infrastructure* consists of two functional subsystems:

1. A rights and obligations management system to create and fulfil contracts.
2. A rights and obligations documentation system to document, prove 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.

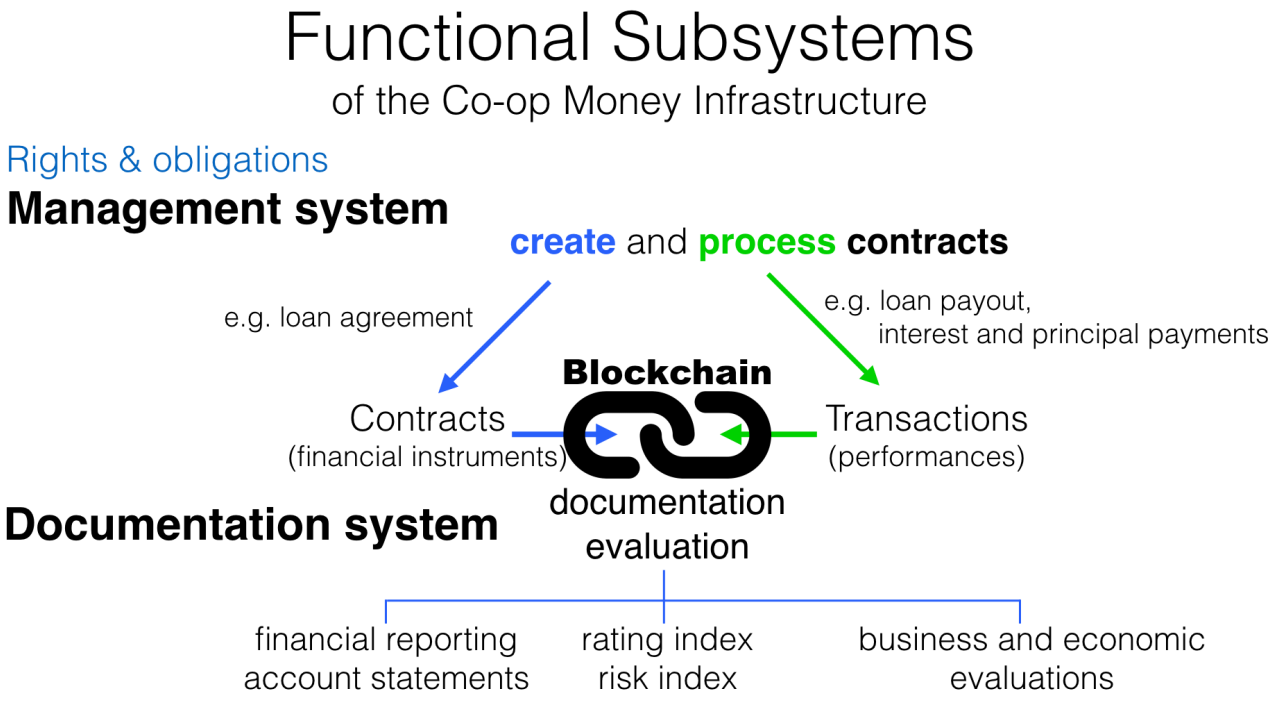

Figure 3. Functional Subsystems of the Co-op Money Infrastructure

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.

Significant simplifications are achieved through extensive 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 focus on legal issues may not seem appropriate at first glance, because we understand trade as a trade in goods and services. But in fact, all trade is a trade in rights and obligations. Control over things is obtained through property rights, not vice versa. If we buy a car, we pay the price for the ownership of the car and because of the acquired ownership we can drive away with this car. The thing car is connected to ownership for free.

All trading begins with a contract and ends with legal action in the performance of the contractual obligations.

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

5.2. Interface with the banking sector

A system-compliant integration could take place analogously to the position "Banknotes in circulation" via a new balance sheet item in the central bank balance sheet: "Crypto-Money in circulation". The underlying accounts would be used to settle payments between the *Co-op Money Infrastructure* and commercial banks.

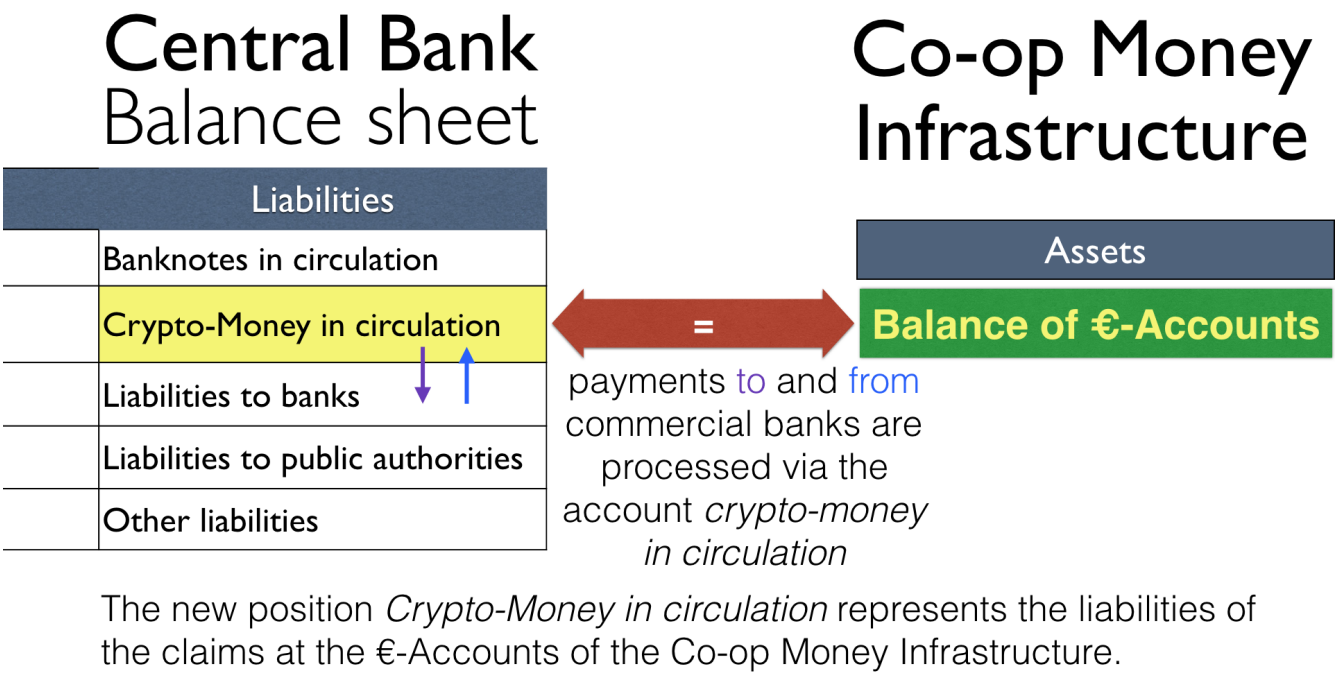

Figure 4. Interface with the Co-op Money Infrastructure through a central bank.

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.

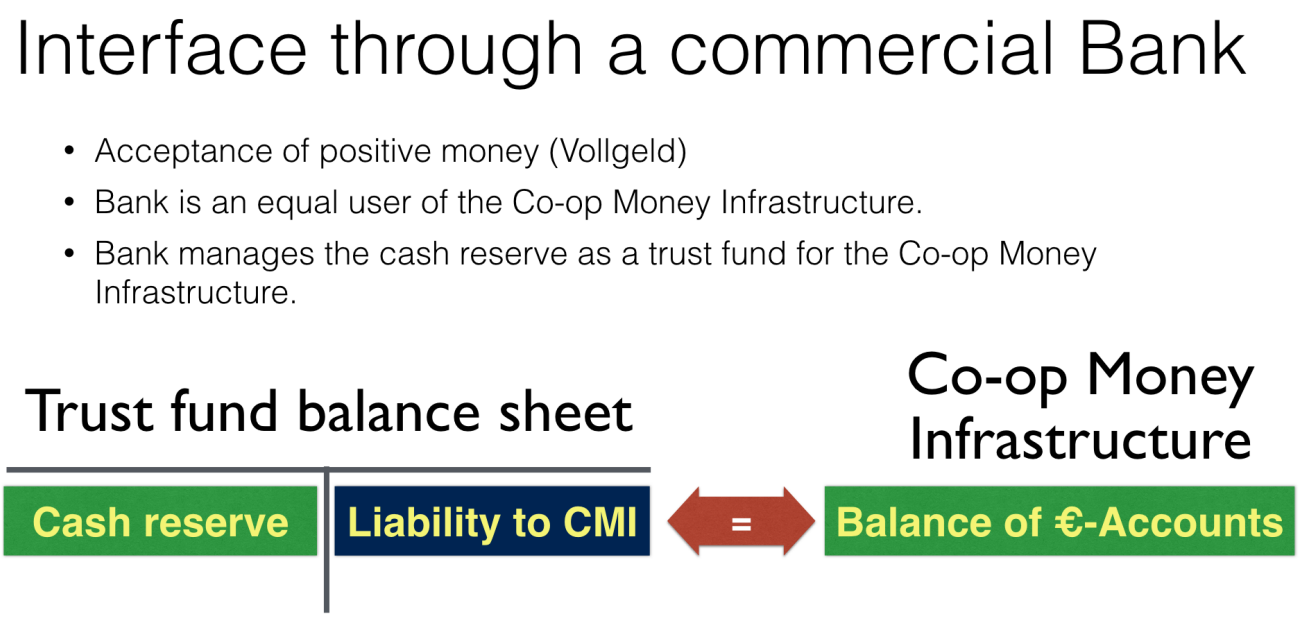

Figure 5. Interface with the Co-op Money Infrastructure through a commercial bank

6. Key ideas

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

6.1. Self-administered crypto accounts

Banknotes securitize money, current accounts book the money, and the *Co-op Money Infrastructure* proves and provides ownership of central bank money on cryptographically protected accounts that are self-administered by the users.

The infrastructure is not meant to create new money, but provides *digital bearer instruments* for existing money. That's a kind of digital cash.

The *Co-op Money Infrastructure* is for any currency. In order to handle several currencies in parallel, the account management is simplified by additionally displaying amounts on an accounts in a currency of your choice. Transfers between accounts of different currencies are automatically converted into the target currency.

The creation of money and monetary policy is seen as the task of the central banks and the profit through money creation should benefit the community.

A national currency used as an international means of payment has serious implications. A neutral global currency or clearing unit of account could be established within the money infrastructure.

6.2. Ultimate decentralization

The *Co-op Money Infrastructure* is decentralized in four ways:

1. No central administrative authority.
2. Each user stores only his own data and optionally encrypted backups of other users.
3. Shared data is stored on distributed server clusters running on users' hardware.
4. Transactions and contracts are only exchanged between the parties directly involved.

As a result, data volume and traffic are cut down to a minimum while maximizing efficiency, effectiveness and privacy. For most, and especially private users, the money infrastructure programs run on their existing hardware and thus cause no additional expenditure.

The current crypto currencies 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 [2: 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].

Early in 2018, bitcoin's 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 Co-op 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 the newly developed *legal consensus mechanism* in combination with the blockchain technology.

6.3. Legal consensus mechanism

For all cryptocurrencies, the consensus mechanism [3: A good overview of the consensus mechanisms can be found in *Consensus – Immutable agreement for the Internet of value*: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf] is central. It ensures the correctness of payments and prevents manipulation without having to rely on a central authority. So far, this problem has been solved purely technically.

Through the newly developed *legal consensus mechanism* not only money, but all rights and obligations might be turned into *digital bearer instruments* that have been signed by the senders and can only be read and processed by the legitimate recipients.

The signed data, together with the rights and obligations arising from a contract, will be complementarily distributed amongst the contracting parties, with the result that a party who manipulates his data would destroy his own rights and yet would have to fulfil his obligations under the contract. Rights and data are inextricably linked, as are rights and paper in securities. The rights from the data follows the right to the data. The power of control over the data is ensured by cryptographic methods and possession.

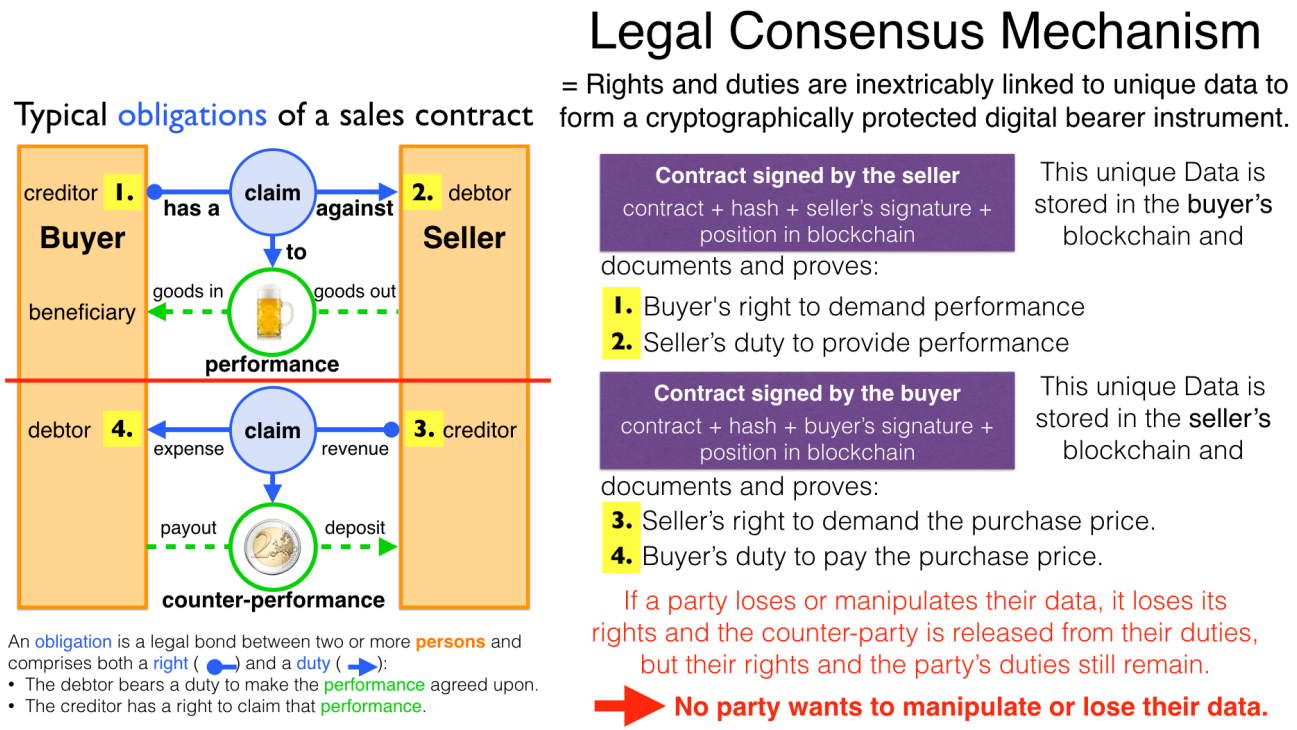

Figure 6. Legal Consesus Mechanism

The correct content of the data is also legally secured through the complementary interests of the parties: The right of the creditor to claim a particular performance refers to the identical performance that the debtor has to provide.

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 of these data. The buyer cannot manipulate these data because the seller signed them. And without these 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 of these data.

The legal 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 crypto currencies, such as Bitcoin. At the beginning of March 2018, Bitcoin's estimated power consumption was 54 TWh per year and will reach 125 TWh per year by the end of 2018. Thus, this power consumption is higher than that of 10 million respectively 25 million four-person households in Germany.

In the money infrastructure, this tremendous energy consumption is not required and is replaced by a single paragraph within the Terms of Use. In addition, this simple solution achieves more than the "Proof of Work" mechanism: the scaling of the system is independent of the number of users and the transactions can be executed in real time.

6.4. Blockchain trees

The legal consensus mechanism leads to the fact that a user does not want to manipulate his data. Any manipulation would destroy the own rights and the obligations of the counterparty.

To efficiently determine the integrity of the payload data, they are embedded in a metadata structure that gives these data additional properties that are essential to the money infrastructure. The data must be authentic, complete and time-related.

The authenticity is necessary so that data can be unambiguously assigned to the creator. The system must ensure that rights, obligations and legal dispositions can be indisputably and legally attributed to the legal entity concerned.

The completeness of the data refers to a specific retention period, which varies due to legal regulations and user needs. For example, completeness has to be ensured for accounting, but outside the compulsory retention periods the data could be deleted by system-internal functions without this being interpreted as an illegal manipulation of the data.

Not storing all the data for all time is a prerequisite for sustainability, efficiency and cost.

The time reference is made by a timestamp. It is a requirement for the retention period and in applications such as the ledger in an accounting system.

The means by which to obtain these additional properties for the data is the blockchain.

6.4.1. Blockchain

The term blockchain is used in two very different ways.

In the proper sense, a blockchain is a continuously growing list of records, called blocks, which are chained together and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and payload data. By design, a blockchain is inherently resistant to modification of the data whose integrity can be checked very efficiently. These features are the reason to use blockchain technology.

The application of this technology to certain cryptocurrencies led to the second meaning: A blockchain is a decentralized, public digital ledger of transactions that can not be manipulated due to cryptographic methods.

Here I use the term blockchain in the first sense and call the second meaning a *blockchain application*. The term *blockchain tree* used in the following is also a blockchain application, which however differs substantially from the previous use in cryptocurrencies.

A blockchain tree consists of independent blockchains linked by a rooted tree structure. The root and leave nodes of the tree contain blockchains. The first block in a leave blockchain contains as the first entry the hash of the first block of the root blockchain and the path.

6.4.2. Identity blockchain tree

Identity services are important whenever people become interactive. They are particularly

important in situations where people no longer meet in person and legal relationships are involved. If the identity of a business partner is unknown, significant disadvantages can arise if rights are claimed and the debtor does not want to fulfill his obligations. If in such situations the identity of the debtor is unknown, a claim can not be asserted in court.

Identity services are the bridge between the computer-generated virtual world and real people. Technically speaking, an identity in the sense used here is an object in the sense of object-oriented programming. That means an identity has attributes and a behavior that is governed by the represented real person.

Storing and managing identities is the job of the distributed identity server cluster. The data of the identities are stored in a graph database management system that implements a blockchain tree. The Identity Server Cluster is a common component of the money infrastructure and runs on particularly suitable user hardware. The motivation for users to provide resources for an Identity Server is the ability to earn money and to process their own transactions faster.

Since the rights, duties and legal dispositions of a natural or legal person are documented and inextricable linked to data in the money infrastructure, a one-to-one connection to the person concerned is indispensable. A person is represented in the system by a virtual identity and can act through that identity in the system. All rights, duties and legal acts that are assigned to an identity are directly attributed to the person concerned.

In the legal sense, there are two types of persons. *Natural persons* refer to humans. *Legal persons* refer to all other legal subjects, e.g. companies or institutions.

A *legal* person acts through the identity of another identity that occupies one or more roles within that legal entity. In this way, as in reality, chains of representations can emerge, at the ends of which a natural person stands.

A role gives an identity certain rights, obligations and powers on behalf and by authority of the represented legal subject.

Informational self-determination is a basic principle of the money infrastructure. Therefore, a person decides which data they want to make accessible to whom. In turn, this decision determines a person’s rights and possibilities in the system.

An identity and its data may be confirmed to varying degrees: fake, unconfirmed, confirmed by other IDs, certified, etc. If an identity is recognized as fake, then it is banned from the system.

For example, a person in a developed country could only conclude a loan agreement within the money infrastructure if it has an officially confirmed identity whose data is made available to the contracting party. This restriction makes the money infrastructure compliant with legal requirements and prevents a person from evading their duties.

However, in regions where government structures are poorly developed, it should be possible to obtain loans based on identities verified by counterparties or by personal inspection.

For both cases, mechanisms are available that promote and, if necessary, enforce sanctity of contracts. One mechanism is called the *compliance index* and the other is implemented through so-called recommended, standardized and balanced contracts.

The profile of an identity and the changes are stored in its own blockchain. The first block contains all the necessary data to identify a person and a video in which the person expressly commits to comply with the rules of the money infrastructure. This declaration of commitment is a specific sentence that must be repeated.

When setting requirements, recommendations from international standards, such as ISO / IEC 24760, should be considered.

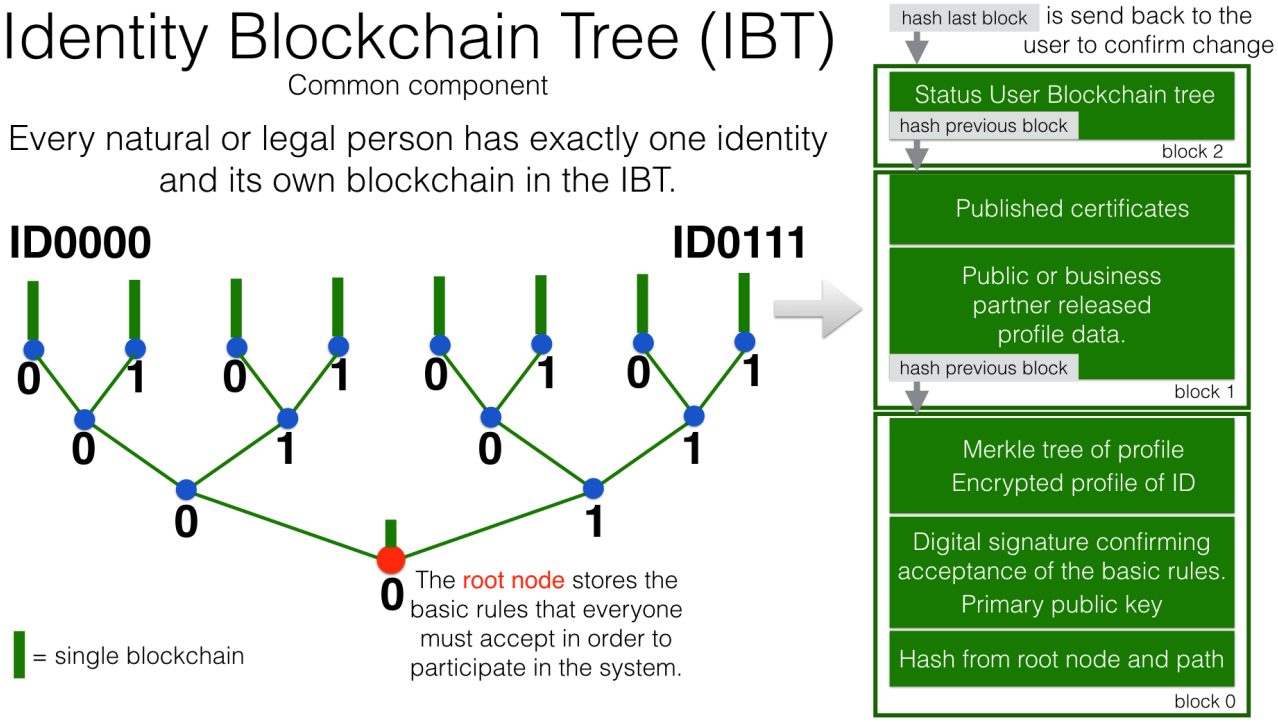

Figure 7. Blockchain tree for identities

The first block contains encrypted all necessary data for the identification of a person and a video in which the person expressly commits himself to comply with the rules of the money infrastructure. This commitment is a specific sentence.

The individual data and the video are used to calculate hash values, which are summarized in a Merkle tree.

The second block contains public or business partner released profile data and published certificates. The Merkle tree over the profile data is used to check whether the published profile data matches the encrypted profile data.

The other blocks contain additions and changes to the profile data.

Due to their general importance, the identity service of the money infrastructure should also be available to other applications. In this case, one could consider whether the sponsor organisation of the money infrastructure becomes an official certification authority and controls the identity server cluster.

The identity blockchain of a person is the root of an user data blockchain tree.

6.4.3. User data blockchain tree

A user data blockchain tree might be viewed as a general tamper-proof database and might be used wherever appropriate. The structure of the payload data within a blockchain can be chosen as required.

All rights and obligations and all contracts of a person might be stored in a user's data blockchain tree. This data is encrypted by the owner of the tree so that only he has access to the data.

At least three copies of this encrypted data are stored as backups by other users. A user can make requirements on the quality of the backup resources, but on which server the backups are ultimately stored will be decided by the system at random and quality requirements. Backup storage providers do not know who they are backing up and can not do anything with the data because they are encrypted.

If a backup server does not meet the promised characteristics, then the data is automatically saved to another server if the requested quality is not reached. This ensures that at least the required odd number of backups are available when needed.

The blockchains are used as accounts or as storage for contracts or other data. A blockchain evolves from the transactions in the case of an account or from the performances provided under a contract.

An account can either store a right as a *digital bearer instrument* or the right will only be documented. In the second case, the owner may need to prove his ownership by additional other means.

By default, rights are stored as *digital bearer instruments*. This means that the right is inextricably linked to unique signed data and only the **owner and possessor** of that data can in fact and legally transfer or assert such right. This applies, for example to the money accounts provided by the co-op money infrastructure.

However, this close connection between rights and data is not mandatory and in many cases not possible or desired. This applies, for example, to otherwise securitized rights or if land is registered in an official Land Register. This also applies to all accounts that are managed by banks and for which the customer receives a bank statement.

An account can store a single or multiple similar rights:

1. A single right, such as a certain real estate right.
2. A quantity of similar rights that can be individually identified. For example, ownership of notebooks identified by a serial number.
3. An amount of fungible rights that are treated alike, such as money, claims to money or the ownership of a fungible commodity.

The identity blockchain tree together with the user data blockchain trees can be considered as one large tree spanning across the internet in which each right has a globally unique address. The first part of the path uniquely identifies the legal owner of a right and the second part leads to the right itself.

In that sense, the money infrastructure creates an **Internet of Rights** and, indirectly, an **Internet of Things** because things depend on the right, not the other way around.

In the profile of an account, additional metadata can be stored, such as: Cost centers so that the organizational structure of a company can be mapped.

To prevent bookkeeping in a company from being done twice, all posting-relevant business transactions can be documented in the company's blockchain tree. In this way, the blockchain tree can be used as a particularly tamper-proof database for accounting.

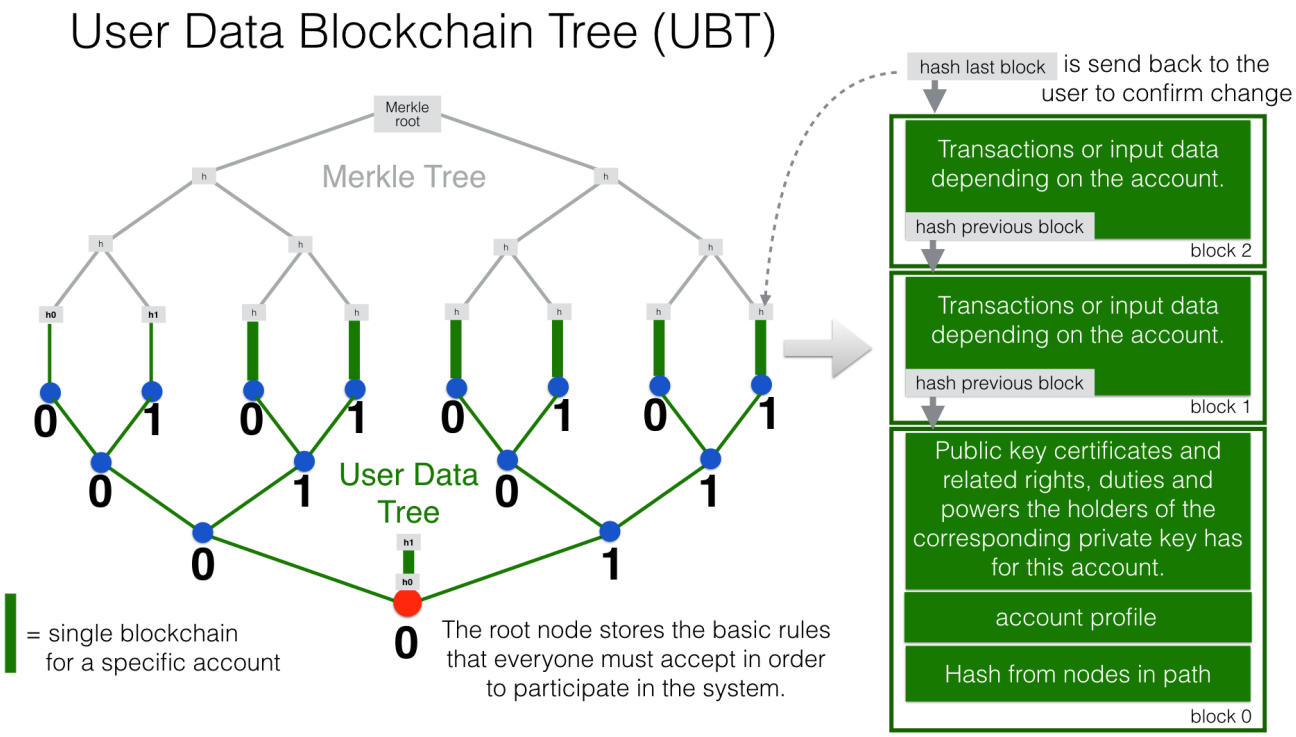

Figure 8. Blockchain tree for user data

Each blockchain ends with the hash of the last block. These hash values are summarized in a Merkle tree. The first two hash values come from the first and last block of the root blockchain.

The Merkle root is used to prove the integrity of all data in the blockchain tree.

When a user starts a money infrastructure application, it checks in the background whether the Merkle root of the local blockchain tree matches the backed up Merkle root on the identity server and on a backup. If there are deviations, then the local blockchain tree is restored based on the majority of the backups. Normally, all backups are the same.

The data from the backups and the identity blockchains tree are leading in determining the integrity of the data. In this way, the user data blockchain tree is replaced if it has been accidentally or intentionally corrupted.

To successfully manipulate a user data blockchain tree, the following barriers would have to be overcome.

1. The identity server cluster would have to be hacked to find the cluster server containing the backup information for a particular blockchain tree.

2. This specific identity server would need to be hacked to find out on which backup servers the backups of a particular blockchain tree are stored. That alone should be very difficult with a redundant server cluster with a distributed database in which the servers control each other.
3. One of the backup server must be hacked to steal the backup.
4. The correct private key must be stolen from the attacked user to decrypt the backup.
5. The data backup must be manipulated in the desired way and the affected hash values recalculated. This manipulation is extremely difficult, because the database transaction log is backed up and not the individual tables.
6. Since most of the relevant data was signed by a third party, the signature would also need to be rebuilt using the private key of the signer. These private keys would have to be stolen beforehand.
7. Then the majority of backup servers must be hacked and the backups replaced.
8. So that when comparing the Merkle roots the manipulation is not noticeable, all changes would have to be made on the server of the attacked user too. The manipulation would be completely different, because not the log files, but the tables would have to be manipulated.
9. If digital bearer instruments are transferred such as payments, points 1. - 8. would have to be made for each transfer along the entire chain. For payments, there would also arise a difference between the total amount of the cash accounts in the system and the external escrow account. At the latest here, the manipulation would be noticed and could be traced back to the origin.
10. All break-ins and manipulations would have to be done in a very tight time frame, because the normal use of the system could permanently change the blockchain involved. While an attacker manipulated a particular blockchain backup, the original blockchain could be updated and the backups moved to completely different backup servers.

Even if some barriers can be taken, it is very unlikely to overcome all obstacles as required. On the one hand, the security concept is based on cryptographic methods, and on the other hand, the effort to manipulate is set to an extreme disproportion to the potential yield. In addition, every user can choose to protect their data according to their own needs and options. Shared data is hosted only on servers that provide high security.

The attacker would also have to pass unnoticed at the permanent internal security checks.

However, the Achilles heel is the protection of private keys. Anyone who has access to a user's private keys and hardware could make dispositions attributed to the owner of the private keys. This vulnerability can only be reduced by additional security measures, such as the integration of biometric procedures. Additional safety precautions can be determined by the user according to their own needs.

To protect the integrity of the entire system, traffic is encrypted among the servers and applications and each transaction is embedded in a three-phase commit protocol.

6.5. Recommended, standardized and balanced contracts

The more voluminous and complex a legal system becomes, the less it is generally understood. Too many laws are the rule of law's death.

Already today it is objectively impossible even for lawyers to completely understand a single area of law. And even if everyone could recite all the laws and regulations by heart, there are so many different opinions that the outcome would probably not be much better.

In order to smash this Gordian knot, legal standards and self-enforcing rights are introduced.

Within the *Co-op 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.

The sense and purpose of a contract is to document and prove the agreed rights and obligations and that the resulting performances are provided.

Normal contracts are *imperative*, i. the contracting parties must

1. know what they want and
2. how it is contractually implemented and therefore understand the legal details and
3. hope that the desired result will be achieved.

RSB-Contracts are *declarative*, i. the contracting parties need only

1. know what they want and
2. can trust that the interests of the parties will be balanced and fairly taken into account and contractual details have been carefully considered and worked out.

The difference is similar to solving a complex calculation manually or with the help of a calculator. Here, too, you have to know what you want, but the rest is incomparably easier and faster in a declarative approach. The idea for declarative contracts is inspired by the declarative programming style.

The most important features are listed in the following table and compared with today's contracts.

Characteristics	Today's Contracts	RSB-Contracts
Proof of agreed rights and obligations	yes	yes
User interface	imperative	declarative
Legal knowledge required?	yes	no
Contractual design	Freedom of contract, this means free up to immorality	Only with approved RSB templates
Right Patterns	no	yes
Localization	no	yes
Saves status	no	yes
Responds to events	no	yes
Self-enforcing rights	no	yes
Effort to enforce rights	high and tedious	automatic to low for self-enforcing rights
Predictability of litigation	uncertain	deterministic
Behavior	passive	active
Handling	manually, partially automated	largely automated
Security during settlement	low or high for notarial settlement	high through three-phase commit protocol and trust settlement

Figure 9. Main characteristics of RSB-Contracts

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 details. 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 many as necessary.

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

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

Today's economic system works according to the motto: freedom and the power of the strongest. RSB contracts realize the idea: freedom and responsibility. No participant should be able to impose his contract conditions on the other. While the price / performance ratio could still be unbalanced, the general terms of the contract should be fair and balanced.

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

6.6. Self-enforcing rights

Self-enforcing rights is a concept in which legal claims can be enforced without courts and bailiffs or vigilantism.

Ordinary jurisdiction is not meant to be replaced, but relieved from cases that can be decided on the basis of indisputable and sufficient facts. If one of the contracting parties does not agree with the measures carried out, ordinary legal remedies remain open. However, the chance of getting a different verdict is unlikely, especially since the contracting parties agreed with the procedure and also know exactly what to expect.

The most important features of self-enforcing rights are listed in the following table and compared with classic rights.

Characteristics	Classic Rights	Self-enforcing Rights
Intended application area	Everything: things, data, rights, immaterial things	data, rights
Exclusion of third parties	penal threat, state authority	cryptographic keys
Verification	documents, witnesses, etc.	digital documents
Protection against counterfeiting or modifications	signature, printing technique, digital signature	digital signature, blockchain
Determine rights	courts	data in blockchain
Enforce rights	bailiffs	programs
Legal knowledge required?	yes	no

Figure 10. Main characteristics of self-enforcing rights

In the implementation of self-enforcing rights RSB contracts play a crucial role. Through RSB contracts, the system is not only aware of the agreed claims and their due dates, but also the performances provided. For example, if a borrower does not pay his installments, the lender may initiate his contract to send a dunning notice to the Identity Server. On the next contact between the debtor and the identity server, the notice is transmitted to the contract in question. If the claim is justified, then a prioritized compulsory payment is inserted in the outgoing payments of the debtor.

The consequence is that the debtor can not make any other payments until he has cleared the compulsory payment.

The consequences of a breach of contract are already specified in detail in the RSB contract template and can be displayed by the contracting parties at any time.

Consequences can, but do not have to be asserted. In any case, breaches of contract will worsen the compliance index.

6.7. Compliance Index

Trust in a mass society is a difficult task. The *Compliance Index* is a weighted measure of sanctity of contracts and compliance with fair and sustainable business practices.

A Compliance Index of 100 means that the person has fulfilled his contractual obligations in full and in good time. The index is weighted with the value of the transaction and the time. A current failure to comply with rules and obligations is weighted more heavily than if it is older.

The index can reach over 100 points if the person is particularly fair and responsible. These include e.g. fair wages, responsible use of the environment and social commitment.

An index over 100 points is referred to as *prime compliance* and not only a visible sign to others, but

also associated with privileges in the system.

Instead of bank status, prime compliance could be the criterion for obtaining low-interest loans from the central bank as part of their monetary policy.

It would also be conceivable that companies with prime compliance would be preferred in public procurement according to their status.

Companies that pay fair wages and protect the environment have a cost disadvantage to companies that exploit their workers and the environment, which could be compensated in this way.

Moral appeals are well-intentioned, but badly done, because in the end they weaken responsible companies. As long as the external costs caused by companies do not redound upon these companies, measures will remain ineffective. Cost is the language that is well understood and responded by companies.

Prime compliance should also be a prerequisite when a person offers asset management services.

6.8. Risk index

Through the RSB contracts, the system knows the type of business and the sanctity of contracts of the parties involved. Before concluding a contract, a statistically calculated risk index is displayed for the participants, which also indicates where potential problems might arise.

6.9. Financial reporting and account statements

From an accounting point of view, the user data blockchain tree is a generalized basis for any form of accounting. The blockchains store rights, duties and legal dispositions. That and a set of accounting principles is all you need, if this information is complete.

The business transactions are stored in their original form and can then be mapped as required into a specific accounting standard. Thus, different standards can be mapped in parallel from a common database.

By customizing the mapping procedures, financial reports are automatically generated.

How a business transaction is booked is decided on the basis of the RSB template, the purchased goods or services and possible additional information.

6.10. Business and economic evaluations

Timely business and economic evaluations are of utmost importance for economic and political decisions. Reliable information and transparency are also of enormous importance to society as a whole. Therefore, a user of the money infrastructure must accept statistical evaluations of his data.

The procedures for the evaluations as well as the reported data are always available to the user in full. Statistical evaluations are available to all users. Personal data protection is guaranteed.

The evaluation procedures automatically run in the background with low priority so that they do

not interfere with a user's work.

A user has the right and the ability to stop the evaluations at any time, but then in return he can no longer use the system.

Which statistics are collected with which programs is decided by the majority of stakeholders.

6.11. Trading platform

It is typical for markets that suppliers make offers and potential buyers compare and accept these offers. Legally, a contract is concluded by offer and acceptance.

Each user and in particular companies can use the RSB contract templates to enter general offers in their blockchain tree. These offers are then automatically visible to all users and can be accepted as on trading platforms.

If a supplier provides for a product all information relevant to the user and guarantees this information, then this product appears in a price-performance-oriented list of competing products. All other product appear in an unordered list because these products can not really be compared.

Which information is relevant for a product and how the features are weighted in terms of warranty will be decided by the buyers. For easier handling, quality grades and quality seals can be determined, which summarize and evaluate several properties according to use classes.

Suppliers who provide insufficient information about their products or do not take responsibility for the information provided are assumed that the product is of medium quality, unless the deficiencies are specifically mentioned.

The consequences for poor performance or false information are already set in the RSB templates.

In today's complex and diverse world of products, every buyer is mostly a layman and can easily be deceived. Therefore, relevant information is so important and therefore deceptions should be sanctioned accordingly hard. The relevant information also includes production conditions so that buyers can decide whether they really want to buy textiles that have been produced under exploitative conditions and therefore can be offered much cheaper.

The trading platform of the money infrastructure is deliberately designed to foster sustainable production and fair trade.

7. Basic principles

7.1. Privacy for people

Privacy for people, but transparency for the rest of the world - that's the tenor.

If we do not want to be trapped into a new slavery, people need to know what their governments, corporations, and all those many other organizations are doing, tolerating, and not doing.

The new chains are not made of steel, but insurmountable because they are invisible. It's the fake

news and worse the mix of facts, half-truths and lies we're constantly showered with. They shape our beliefs and our actions and even make us fanatical against our own interests and the good of the community.

The tenor describes the two extremes, but of course also governments, companies and organizations have sensitive information, which should also be protected. But if, over time or circumstances, the reasons to protect fall away, there are no good reasons why the truth should not be brought to light.

These demands are easier to set up than implemented because neither the world nor the information about the world is simply black and white.

The approach to implementation is a close connection between freedom and responsibility.

7.2. Informational self-determination

Informational self-determination is considered a central right of freedom. It is an architectural principle of the money infrastructure in that user data are not only the property of the users, but also in their possession and cryptographically protected.

7.3. Freedom and responsibility

One of the fundamental design principles in our economy and society today is freedom of contract and the power of money.

Freedom of contract is not simply used for the exchange of goods and services, but at the same time more or less the economically weaker has to accept the conditions up to immorality.

Money gives power, which is exercised in the semblance of law, enforced by governments and paid for by the taxpayer.

RSB contracts not only make trading much more efficient, but also more balanced. Contractors should not have to worry about being tricked by legal intricacies and false or insufficient information.

A particularly important task of RSB contracts is to combine freedom with responsibility in order to strengthen sustainable business practices and fair trade.

7.4. No advertising

The money infrastructure is not financed by advertising. Much of today's advertising is deception. It is the continuous force that leads to more and more consumption, regardless of the actual needs of people, society and environment.

Within the money infrastructure, companies can draw attention to their goods and services by providing good value for money, relevant information and taking responsibility for the information provided. These criteria determine whether and where products are listed on the sales platform.