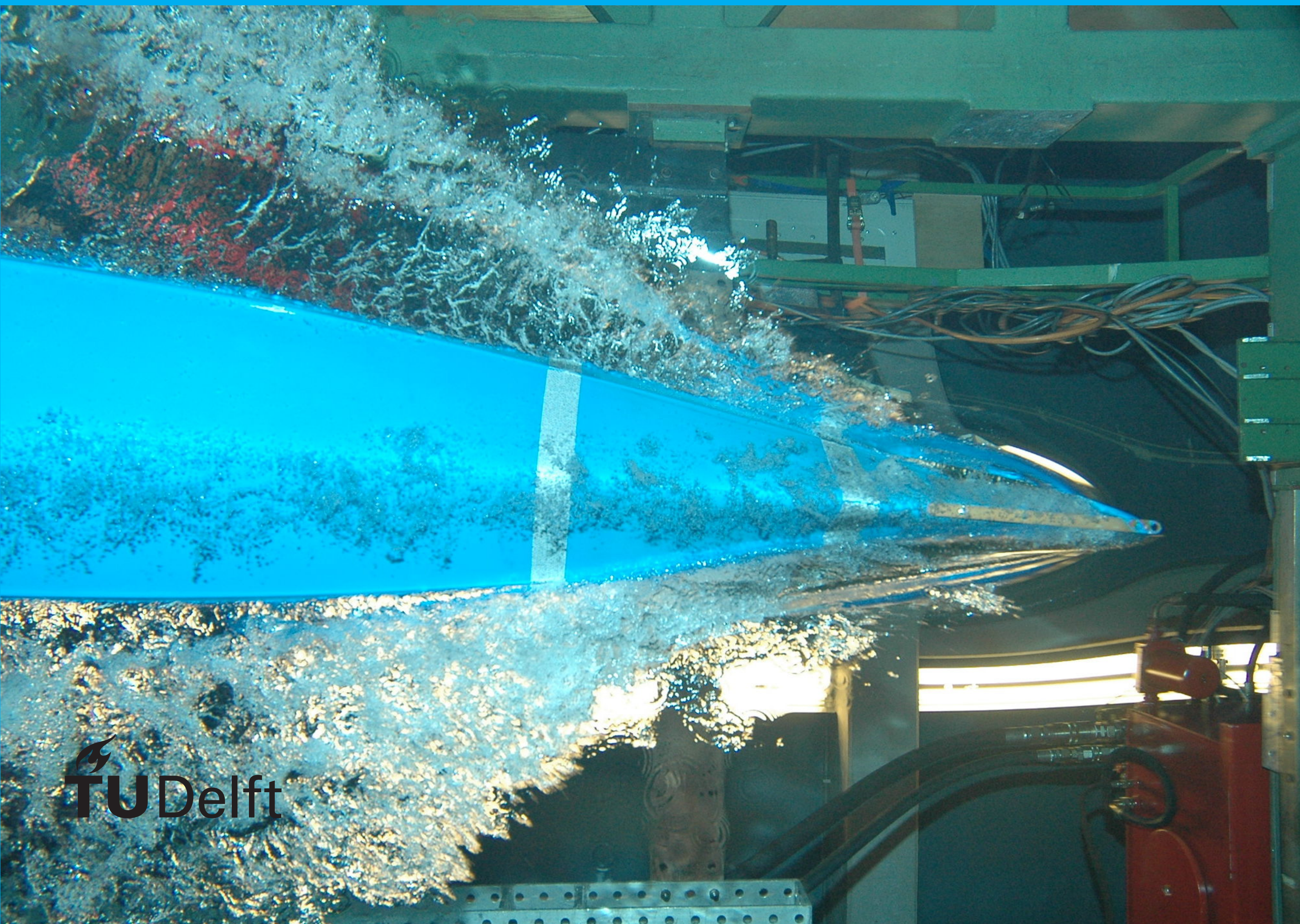
EuroToken

A Central Bank Digital Currency (CBDC) with off-line transfers

R. W. Blokzijl

- Stablecoin
- Blockchain
- Cryptocurrencies
- TrustChain
- CBDC

R.W.Blokzijl@student.tudelft.nl



EuroToken

A Central Bank Digital Currency (CBDC) with off-line transfers

by

R. W. Blokzijl

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on July 7, 2021.

Student number:	4269519	
Project duration:	November 11, 2020 – July 7, 2021	
Thesis committee:	Dr.ir. J.A. Pouwelse,	TU Delft, supervisor
	Dr. C. Lofi,	TU Delft

This thesis is confidential and cannot be made public until TODO.

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Preface

TODO: Add preface

R. W. Blokzijl
Delft, TODO

Contents

1
Introduction

Eccentric visionaries have long been speculating on how the global financial infrastructure could be restructured to better serve the people of the world. When the Bitcoin [54] white paper was published in 2008, it seemed decentralized ledger technologies could be the missing link that would finally enhance the transparency, digital efficiency, and feature set of our payment system. 9 years later, Facebook announced a private currency controlled by a group of corporations [44]. 3 years after that the Chinese government announced that they had reached 92,771 transactions per second in a closed trail of their new Central Bank Digital Currency (CBDC) [46]. And the Eurosystem is set to make a decision on whether to start a digital euro project in mid 2021.

Currently no decentralized currencies are in a position to challenge the upcoming “central coins”. Even the most prominent crypto currencies, including Bitcoin and Ethereum [32], simply lack the scalability and price stability necessary to be a valid medium of exchange and reliable store of value. While there have been attempts to create fully decentralized stablecoins, none have yet been proven to work in practice on a large scale. With high transaction costs and price uncertainty, the most fundamental problems of money are still unsolved by distributed currencies. The future of the financial system might be decided by competition between the governments of the world and opaque proprietary alternatives.

Its starting to become clear that the direction of crypto currencies will not be determined by collections of anonymous individuals imagining a financial system that gives power back to the people. Governments and large corporations have joined the race for the worlds leading digital currency. Motivates by profit, national interests, or the good of humanity, the winner will be left controlling and overseeing a significant chunk of the worlds transactions.

The winner of this race might come to influence the most basic aspects of our daily lives. Where China and Facebook are making rapid progress, the Eurozone is still deliberating. Meanwhile their presence in the race might be vital in incorporating the values of personal freedoms and privacy.

This thesis provides a design for EuroToken, a prototype for a Central Bank Digital Currency. Its primary purpose is to implement, for the first time, a currency that is: digital, universally accessible, central bank issued, and peer-to-peer. Our unique design stems from an analysis of the fundamental challenges distributed technologies face today and exploring how an institution with the reliability, experience and reach of the European Central Bank (ECB) might provide solutions.

1.1. The decline of cash

Most monetary systems of today relies on two main types of money. Private money, managed by private banks, and public money, managed by the European Central Bank (ECB).

Public money is the money we have in our physical wallets. It consists of bank notes and coins and is often referred to as cash. Once upon a time it was possible to exchange this money for gold directly at the central bank of a country and thus it derived its value directly from gold. Today however, the value of this money is guaranteed by the reputation and trustworthiness of the central bank [37]. No physical euros will be created unless by the central bank itself, and no one can seize them unless with physical force. This puts it in opposition to private money.

Private money is the money in our bank accounts. It derives its value from the reliability and reputation of the private bank and is only usable by instructing the bank to transfer it. Without permission from the bank, deposits, transfers and withdrawals are not possible. Effectively, these banks act as a central point at which any individual or group ban be silenced by freezing their assets or withholding service. Additionally, if a bank overexposes itself to market forces and goes bankrupt, the money stored with them might not be payed back in full.

A person in the eurozone can weigh the risks and benefits of these two types of money. The ECB is a large, historically trustworthy, and democratically controlled institution. The persons public money (or cash) would only lose its value in the case of the complete failure of the European economic system and central bank. On the other hand storing value in banks has the benefits of the digital age. Where keeping money in the form of cash means exposure to the risk of having money physically stolen, money in banks is digitally secured. Both impact and risk grow with the amount of money held in cash.

In addition to people storing their money in private banks for security reasons, the digitalisation of society is a powerful motivator. Transacting using private money as opposed to public money allows for transfer of funds all over the world. The ability to use private money in e-commerce, as well as its ease of transfer, has made privately banked money the predominant way people interact with the economy.

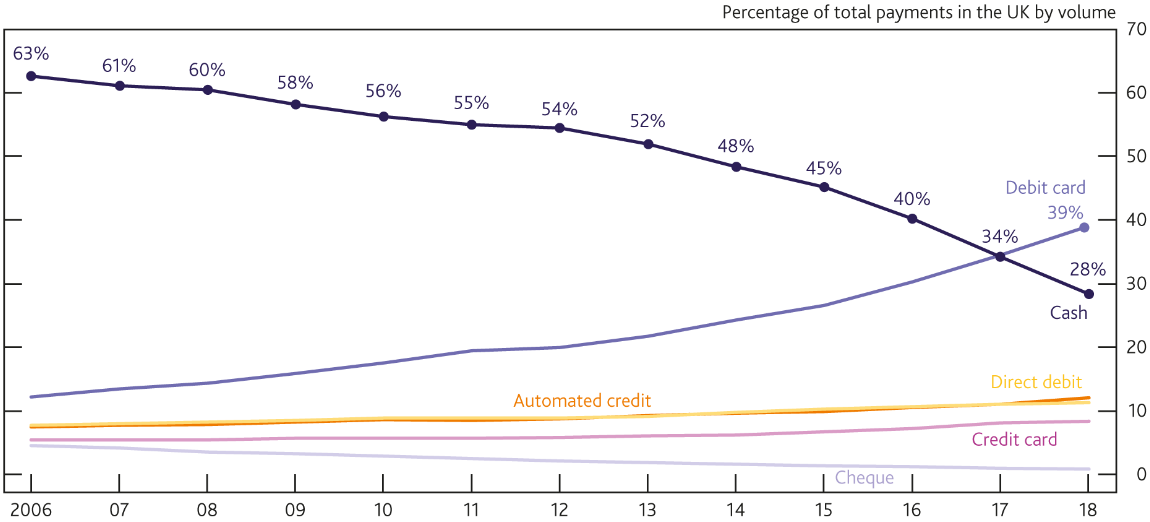


Figure 1.1: UK Decline of cash over 2010-2020 [57]

As a result of digitalisation, the world is moving from cash to cards. In the year 2000, less than 22 percent of transaction in the EU were card transactions. In 2019 this is over 47 percent [68]. This decline of central bank money leads to a number of unfavorable scenarios [45]. The decline of open and off-line money contributes to the financial exclusion of the unbanked and vulnerable in our society. In 2017, 3.6 percent of Europe's household had no registered bank account [52]. As more and more businesses move online or become pin only, these people will see their means of participation in society decrease.

Additionally the increased reliance on private institutions can leave the entire euro system less transparent and more vulnerable to corruption. The 2008 crisis revealed the reliance of the financial world on opaque profit driven institutions with insufficient oversight. While the industry has been scrutinised heavily since then, the broader economy is still not insulated from future failings. The EU does require national funds to insure citizens at least 90% of their bank deposits, up to at least 20.000 euros per person [20]. But for many this is not sufficient to protect their lives savings.

To solve these issues, a digital currency is needed with the reliability of public money and the feature set of private money. An open digital coin, insured by the Central Bank that is easy to use, online capable, but not be reliant on any private institution for its core function of value storage.

1.2. Rise of insufficient challengers to traditional currencies

Decentralized currencies have been working hard to create the ideal currency that is open to everyone, anonymous, and not able to be controlled or destroyed by a single entity. Yet while the work continues, their slowing progress by increasing public attention is creating a market for flawed and inferior payment solutions.

To address the yet unsolved price stability issue, stablecoins have risen in popularity. While attempts at decentralized stablecoins do exist [66], it is so called centralised stablecoins that have gained a reputation as a digital alternatives to the dollar. Tether [50] is the most prominent example of this. With a market cap of 62 billion dollars in June 2021, they are the 3th largest crypto-currency by market cap [22] after Bitcoin and Ethereum. In order to achieve the stability and dependability of their coin, Tether Holdings Limited acts as a centralised middle-man exchanging 1 tether for 1 dollar. Centralised stablecoins are often seen as an intermediary solution that provides a wrapper over the old monetary system in order to extend it with the features of digital currencies. These coins are essentially financial derivatives with the same flaws of their underlying currencies, except for the addition of some digital features.

On June 18, 2019, a new currency conceived by a group of Facebook engineers was announced under the brand name “Libra” [44]. Later renamed to Diem, it would be a new free floating currency managed and governed by a consortium of multi-national companies united under the banner of the Diem association. While Diem presents itself as a solution for the worlds 1.7 billion unbanked, it would essentially be a private world currency, controlled by corporations who will not be accountable to democratic processes.

These current most prominent bidders, while promising to be the future of public money are all but public. Merely by adding a better feature set in some areas, they attempt to become the future of money. Yet because of their specific set of trade-offs, they are falling short of the long term needs of society.

While distributed open-source communities of engineers are trying to create a system free of corruption and private interest groups are trying to extend their reach, governments around the world are beginning to realise the threat to the established order.

In order to not lose their influence of over their respective economies, governments around the world are looking into new digital versions of their currencies. The Federal Reserve has published their “Preconditions for a general-purpose central bank digital currency” [67]. The ECB has published a report specifying a number of Reasons to issue a digital euro, scenarios and implied requirements [45]. The government that has progressed the farthest so far is the Chinese government. With successful public trails [63] they seem to be closest to a working digital currency.

The battle for the future of the eurozone is sill anyones game, and the outcome might depend on the decisions of the European commission. To avoid the euro being usurped by challengers from foreign nations or the private sector a design for a CBDC in-line with the ideals on which Europe is founded is required sooner rather than later.

1.3. The need for a future proof currency

e-invoice, e-receipts, e-identity, and e-signatures

The world is moving online, and commerce is moving with it. E-commerce as a percentage of worldwide GCP has more than tripled in the last decade [53]. With this move to online shopping, commerce also moved from a solely local phenomenon, to incorporating global vendors. Especially trade with China has seen significant growth over the last 10 years.

While the increased globalisation brings wealth like never before, the increased global trade is not without its dangers to the EU. With China well underway in the race to the first digital currency, the digital yuan might find itself in an ideal position to dominate global trade. If China or any other currency can provide a feature set that is more friendly to global commerce than the current euro. The EU might see the control over their own economies fall away.

In addition to the threat of Chinese influence over European markets, opportunity also lies in the provision of a currency to the unbanked population of the world. Where the US dollar currently holds the position of the worlds “default” currency, this position might move to the first CBDC as people from all over the world can be brought into modern commerce. This can be a great opportunity for the EU to spread its values across the world.

In order to stay relevant on the global stage, and to be able to serve its citizens in the modern age, the eurozone needs a currency with a competitive feature set on the global stage.

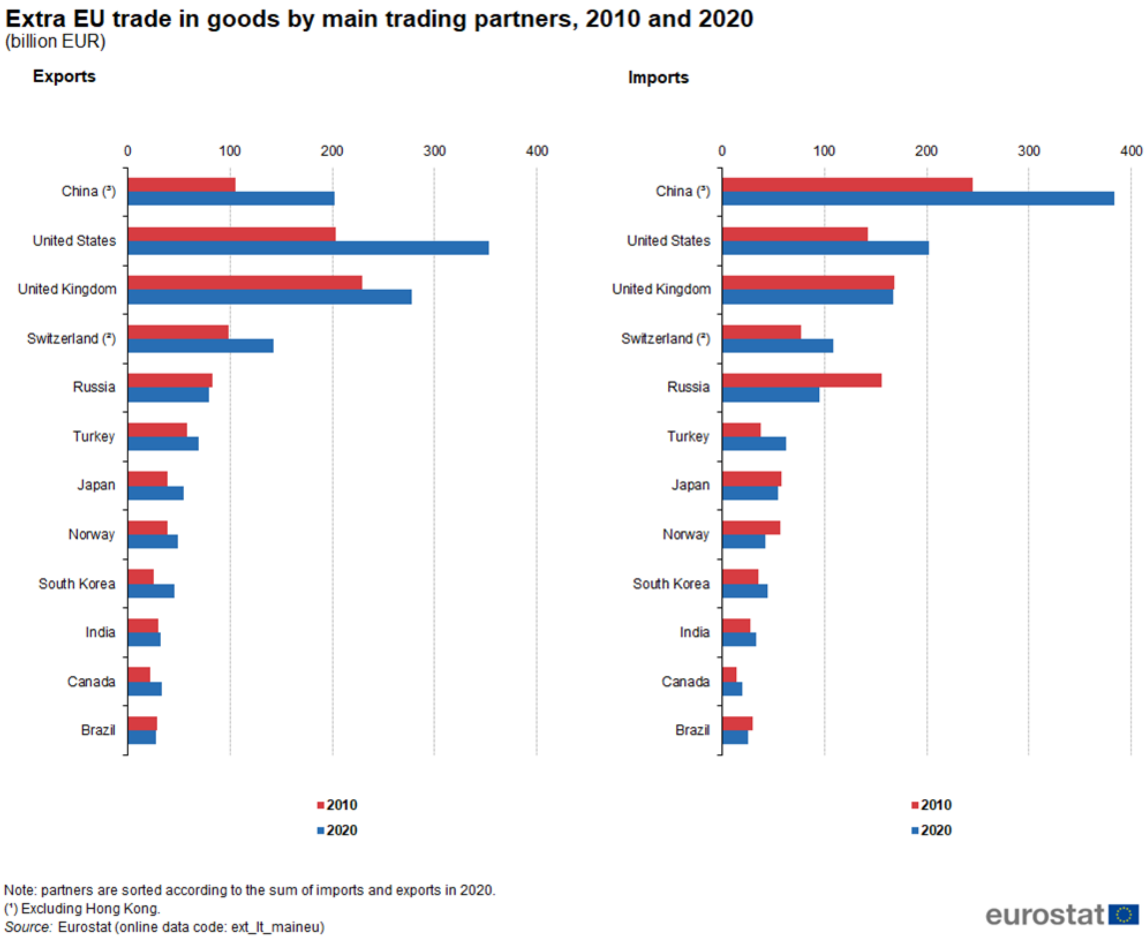


Figure 1.2: E-commerce 2010-2020 [5]

1.4. The technical debt of traditional finance

People have been using various commodities as a unit of account and store of value since 6000 BC [39]. Since then money has taken various forms, at various layers of abstraction, but the function of money has always stayed the same: acting as a medium of exchange [51].

The first known true standardised gold coins have attributed to Lydian society back in 640 BC. Slowly over time the gold and silver contents of the coins became less important, and currencies as a proxy for trust, became slowly more dependent trust in the system rather than the real value of the currency. In 806 AD, this culminated in the first use of paper money in China. Since these events, the form of money has varied based on societal conditions. Because of its functional utility, money in the form of bank notes backed by gold has been a popular form of money that has been used in European society since 1440 [37].

By the end of the 1900s Europe had a system of many national currencies. The value of these currency was maintained on a national level, often using the gold standard [37]. Meanwhile private banks act as a trustworthy and secure institution, allowing people to store their money, while they could make a profit lending that money out. For international and cross-currency trade, people would swap different currencies in exchanges when needed, but because of the localised nature of society this was infrequent.

This system worked fine in an era where most exchange was done by cash, and most trade was done within national borders. But as the world became more connected and digital, different solutions had to be built on top of the old system to respond to the changing demands of the population. Private banks, who were once used only for large transactions and money storage, got a more and more central role in day to day transactions. In effect the system as we see it today has accrued a lot of technical debt as the its requirements changed over time. As a result a number of inefficiencies have emerged from this technical debt.

First, international money transfer. Even within the euro-system this can often take up to a week. Second, banks as private institutions are vulnerable to bankruptcy. This makes them a “financial”on their semi-central point of failure, that take a good portion of the financial system with it. Third, transactions are dependent on bank IT systems. This makes them a “technical” semi-central point of failure, potentially leaving people unable to purchase their essentials. Fourth, people are tightly coupled to their banks. While having multiple bank accounts is possible, a lack of standardisation and interoperability makes people easily dependent on their one bank and its features.

2
Problem description

Over last century the world of finance has gone through significant paradigm shifts. Currencies traditionally started as a bottom up distributed system based on some commodity of value. While these currencies seem to need no institution backing them, the fact of their physical nature made physical security an unfortunate necessity. This naturally lead to institutions that act as centralised authority in order to protect the monetary assets.

This age old solution to a physical problem is mirrored in the digitally accounted financial system of today. While the global dependence on digital money for every day transactions is growing, the control over many aspects of the system rests in the hands of large opaque corporations. These private banks, who form the main engine of the financial system, maintain a luxurious position as the creators of money. The Copenhagen Business school estimates that banks in the UK alone have made 182 billion pounds in seigniorage.

With such a luxurious position it is no surprise that innovation in the sector has been slow. Innovation in payments highly depends on the current gatekeepers of the financial world as they hold the money of the users. Any attempt to innovate by other parties is dependent on the interoperability with banks. While traditional physical currencies are still around as an alternative, their usage has declined due to the increasing utility of digital money due to the internet. The increase in the necessity of digital payment solution, combined with the mismanagement of the current system, makes the need for a new open payment system evident.

In order to rectify the offset in the balance of power and to promote productive financial innovation, a new and open medium of exchange is required. Such a currency needs to be digitally efficient, transparent, accountable, and be fit for global transacting in the 21st century. In this chapter we explore the challenges in the creation of such a currency, specify the requirements for such a payment system and describe why a real solution is still lacking.

2.1. The difficulty of modern digital payment solutions

The search for reliable, digital, money can be traced back as far as David Chaum in 1983 when he first released his paper on Blind Signatures for Untraceable Payments [34]. Rather than specifying a full design for a decentralized currency, Chaum describes a mechanism for preserving user privacy against third parties in digital transactions. Since then many implementations have been attempted, including Chaum's own eCash [30] [33]. ECash had the potential to become a standardized digital payment system right from the start. However, the financial institutions of the time had their sights set on another digital payment system. Normally industries come together to define international standards to aid interoperability and strengthen the market as a whole. But rather than standardise digital payments, the banks chose credit cards as their solution. In its competition with Credit Cards, eCash went bankrupt in 1998 [17].

The adoption of credit cards as the predominant method of online payment subsequently lead to a steep rise in credit card fraud. After with theft of social security numbers, theft of credit card numbers is the predominant form of identify theft [28]. While we leave the issue of a digital identity out of scope, the inadequacy of the credit card system at protecting users has been proven again and again.

Over the years, alternative payment systems have been developed in response to the lack of good payment solutions. Direct consumer to merchant payment systems like PayPal [21], Venmo [23] and Skrill [13] have emerged to fill the feature gap left by credit cards. However, while these services do increase innovation in payment solutions, they don't solve the underlying issue.

While the market is generating solutions to adjust for the lack of innovation, without a deeper paradigm shift the growth in the number of payment options will have one of two outcomes. Either the world of payments converges into a few large payment providers, basically reverting us back to an oligopoly. Or the payment systems stay segmented, leading to increasing complexity for users and merchants in supporting these, while creating large overhead in the financial system.

The fundamental paradigm shift that is needed in the industry is one of integration. Payment solutions must be able to integrate with traditional banks in order to allow users to pay from their accounts, or users have to create a separate payment account with the service and transfer money over. This trend is being pushed by European initiatives like PSD2. But because of the lack of standardisation in the industry, integration of payment providers has to be implemented for every bank individually. When this integration is lacking, users are stuck with their financial services segmented among multiple payment providers and bank accounts. An issue that is worsened with cross border payments. It is evident that current payment solutions are inadequate to solve the underlying problem: the tight coupling between a user and their banking/payment provider.

The problem of decoupling users from their banks has been approached from many different angles. Perhaps the most famous solution in recent years is Bitcoin [54]. While criticising a number of issues that lie at the heart of value accounting in our current system, the Bitcoin white paper proposes a digital payment infrastructure with associated currency that completely moves the very core of value accounting to a distributed and open system. While 10 years after the publication of its white paper the crypto-currency is extremely popular as an investment vehicle, any significant payment volumes have yet to be demonstrated. With transaction fees at around 59 US dollars [36] around April 21 2021, Bitcoin is not ready to be a direct consumer facing payment method.

Other solutions to the tight coupling problem have been successful on national levels. In the Netherlands the iDEAL system has succeeded in integrating most dutch banks under a single online payment system. In Norway a similar product called Vipps exists that integrates all Norwegian banks. And similar systems exist in many European countries [3]. These are all payment initiatives that effectively create an abstraction layer over the individual banks, leaving them transparent to the user. While this does create a single payment interface across a whole nation, the lack of international standardisation leads to the failure to support cross border payments. This makes these systems unable to properly support global e-commerce and trade.

The European Union is actively trying to integrate their financial system across borders. With payment-integration initiatives like SEPA, PSD2 and the European Payments Council, the EU is slowly moving towards a better integrated euro zone. Recently the union has started to explore digital currency alternatives to the current euro [45]. A newly designed euro has the potential to act as a single payment interface for both online and off-line transactions.

With this research we provide a design for EuroToken, a Central Bank Digital Currency designed to act as an alternative to the current privately managed digital euro. It implements a blockchain based accounting system that exposes a generalised payment primitive that supports off-line and online digital payments out of the box. It provides a equal footing for financial institutions, and individuals alike as it makes users the gatekeeper of their own fiscal lives.

2.2. Requirements for a digital euro by the ECB

In October 2020 the European Central Bank published a report detailing a number of scenarios where a new digital euro could provide a benefit [45]. Associated with these a number of requirements are provided.

1. **Enhanced digital efficiency**
2. **Cash-like features**
3. **Competitive features**
4. **Monetary policy option**
5. **Disaster back-up system**
6. **International use**

7. Minimise ecological footprint (cost saving and environmentally friendly)
8. **Ability to control the amount of digital euro in circulation.**
9. Cooperation with market participants
10. Compliance with the regulatory framework
11. Safety and efficiency in the fulfilment of the Eurosystem's goals
12. Easy accessibility throughout the euro area
13. Conditional use by non-euro area residents

In this project we aim to conform to these requirements as best we can and we evaluate our solution by these requirements. The technical requirements are emboldened in the list, as they will be guiding in our design. The rest will only be speculated on as they do not pertain to the topic of computer science and fall outside of our area of expertise. Therefore a technical solution to these problems has to conform to the following requirements.

1. Be a secure system of accounting
2. Scale to the size of the European union
3. Preventing unsanctioned money creation
4. Price stability
5. Disaster resilience through off-line transfer ability

We aim to create a payment system that is secure, scalable, off-line transferable, stable, secure and digitally capable.

2.3. Trade-offs around double spending, scalability and decentralisation

When designing a modern digital payment systems with the ability to transfer funds off-line, peer-to-peer systems and distributed ledger technologies are an worthwhile case study. Since Bitcoin in 2009, various crypto-currencies have iterated on the idea of a fully decentralized currency. After 12 years of development a number of trade-offs are becoming visible that show the limitations of the technically.

Ideally a payment system has no central points of control. By keeping a payment system decentralized the failure of one part does not affect the functioning of the ability of the users to make payments. Such a system also has inherent scalability. However, keeping a currency secure from unsanctioned money creation is not a trivial problem in a fully distributed system.

The primary problem of unsanctioned money creation can be split into 2 different problems. First, for any transaction to be valid the payer has to have received the funds in the past. And second, they have not already spent the money.

The first of these is relatively easy to solve. To do this all transactions received in the past can be digitally "signed" by the sender. The signature of the sender on the transaction proves the transfer of funds from one party to another. When receiving funds, the transaction can be trusted by verifying that the sender has received the money in the past from someone else. This way every transaction can be recursively validated back to their creation point.

The second problem is famously called the "double spending problem" and requires some trade-offs to solve. The goal is to construct a way to prove that for any given transaction, the balance of that transaction has not previously been spend by that user. In the first problem a transaction can be rejected if not enough information is available to verify the fund availability. In the second the goal is to prove the non-existence of a transaction.

Solving the double spending problem without a centralised party like a bank that keeps track of all historic transactions is a difficult task. Blockchain based systems have had some success. The most well known distributed ledger technologies are Ethereum [32] and Bitcoin [54]. We will refer to these as single blockchain networks. Both of these networks maintain a single blockchain of transactions which gives transactions a total order.

Blockchain bases DLTs group all transactions into blocks, which are in turn organised in a linked list where every block refers to the block before it. Accounts are identified by a public key. Every transaction is a transfer from one public key to another, and is signed with the associated private key of the sender. Every transaction references previous transactions where the sender received money, thus ensuring the funds are available. Every transaction thus has "input" transactions. In order to allow a user to send less than the output of a previous transaction, a transaction can have multiple "outputs", sending to multiple public keys including the senders. To solve the double spending problem, any "output" of any transaction can only be spent once, and any transaction that spends an already spent output is rejected. If a user has spent that output before, that transaction would exist somewhere in the chain, thus proving the new transaction to be fraudulent.

The problem with single blockchain systems is their inherent lack of scalability. Since the entire chain has to be checked for any conflicting transactions, the entire blockchain, and thus the entire history of the network, has to be kept by everyone that wants to validate a transaction. This means all new blocks have to be distributed to all nodes in the network periodically to redistribute the new transactions made. The speed of the network to propagate transactions, and the limited puts a practical limit on the amount of transactions a single blockchain network can handle since the whole world has to be informed.

To improve the scalability of this system Ethereum 2.0 [6] proposes a network upgrade that adds multiple parallel blockchains called shards. These shards will be responsible for their own fraction of the transactions on the network, only interacting with one another when necessary. While this does increase the capacity of the network, the extent of the scalability gained has yet to prove itself.

Other attempts at a more scalable ledger exist. [9] builds on the concept of the Tangle. Instead of a blockchain, transactions reference each other in a Directed Acyclic Graph model. Users are not required to maintain the entire block-DAG but are required to validate a number of existing transactions before their own transaction is validated. This lowers the change of a double spend significantly, but requires of their users to so quite some work in order to be able to transact. While public nodes are available to validate transactions for you, these are currently run by enthusiasts and altruists. A criticism is that there is no reason the altruistic processing of transactions will continue into the future.

Another example is Nano [11]. Nano employs a block DAG that resembles a lattice structure which assigns a personal blockchain on a per user basis. Transactions happen between users and are incorporated into both chains. Double spending is prevented by having blocks broadcast into the network and representatives nodes validating the transactions. These representative nodes are elected thought a delegated proof of stake mechanism.

The double spending problem has many potential solutions, all with their own set of trade-offs. A payments solution that aims to scale to a global level using distributed technologies must careful balance double-spending, scalability and decentralization.

2.4. The problem of off-line digital payments

The ability to provide off-line payments is an unsolved problem in the world of digital payment solutions. Solving the double spending problem in a Peer-to-Peer network is a challenge on its own. Doing so without a live connection to that network increases the complexity even further.

The problem of double spending and off-line payments is best understood using the CAP theorem. Consider the total set of transactions to be the database, and reads and writes to be updates to the balances of any user. If we decide we want off-line payment, we implicitly choose the value of *partition tolerance*, thus creating a trade-off between *availability* and *consistency*. We can either read a users balance, **or** be sure we know the correct balance of the user.

An "off-line transaction" is thus a transaction done without access to a sufficient a sufficient set of peers to validate consistency. This means that if any user accepts an off-line transaction is **not** possible to know whether a conflicting transaction exists in another part of the network.

Any network wanting to prevent double spending will accept only 1 in a set of conflicting transactions, usually the first to arrive. Anyone accepting an off-line transaction is therefore at risk until they check in with the network.

For this reason a transaction is usually not accepted by the receiving user until we have some guarantee that all conflicting transactions will be dropped by the rest of the network. This is the concept of transaction finality. A transaction is considered *final* is the rest of the world will reject all conflicting transactions.

Most blockchain based systems achieve this guarantee by having a globally distributed blockchain storing all transactions that *finalises* any transaction with some *eventually negligible* probability of conflict.

In all of these systems, the receiving user still chooses when they accept the transaction. While its possible to wait until the network can be reached online before goods are exchanges, any users that know each other can defer the validation. Instead of relying on the network based, the exchange is based on the trust of the receiver in the sender.

Of course the trust between users is hard to quantify, and shouldn't be relied on fully. However, increasing the trust between two transacting users in the period between the transaction and the check-in with the network is the key to implementing dependable off-line transactions.

2.5. The price stability problem

The primary purpose of a currency as a payment solution is to be an "intermediary store of value". This means that anyone that chooses to exchange their assets or services for a currency, can later trade it in for something else of a same, or similar value. If a currency cannot keep its value stable over time it will fail to be a good intermediary store of value. In order to maintain the viability of a currency as a good option for payment, the price thus has to remain stable over time. This concept alone eliminates nearly all of the new crypto currencies as good payment solutions as their price is dependent on daily market fluctuations.

This raises the question: How do we keep a method of payment solutions truly price stable? This is really a question for economists to answer, however, in order to create a digital payment solution, we do need some method of stabilizing the currency.

One problem is the difficulty of measuring stability. Stability means that what you can purchase today is about the same as you can purchase tomorrow. However, tracking this is extremely difficult. The "value" of any item is constantly shifting based on supply and demand, thus getting any measure of the value of anything is very complex. This is why many stablecoins outsource the problem of defining value to an external system, usually an existing fiat currency. The system works by "pegging" the stablecoin against some collateral.

Say a "token" is always directly exchangeable at central exchange A for the US dollar at a 1:1 ratio. The price of the token in the market will tend to follow the price of the dollar. When the price of the token in the market dips *below* 1 dollar, anyone can buy the dollar on the market, and directly sell it at exchange A for 1 dollar, making an instantaneous profit. This decreases the amount of tokens in the market. Because of this reduced supply the price in the market will increase. If the price int he market is *above* 1 dollar instead, any investor can buy the token at exchange A for 1 dollar, and sell it on the market for a profit, thus increasing the supply and decreasing the price.

This principle is behind practically all stablecoins on the market. However, this immediately leads to the next problem: How to run a 1:1 exchange. The simplest solution is also the most successful at the moment. Tether [50], currently the 5th largest crypto-currency by market cap, uses a central exchange to ensure a 1:1 exchange ratio between the US dollar and its crypto-token USDT. The obvious problem with this is the fact that the system has a critical centralised element. Without proper oversight such a system could be secretly severely under-collateralized. Other centralised stablecoins like USDC [16] and the Stasis Euro [14] utilise audits by private auditing firms to increase transparency, however the system remains centralised.

Fully distributed stablecoins like MakerDAO [66] and EOSDT [4] do exist. These are kept at a stable price by providing an exchange of 1 token for 1 dollars worth of "collateral". This collateral is some blockchain accounted token of value. To make sure the system does not get under-collateralized when the price of the collateral drops, the system is over-collateralized at all times. While these systems have seem some success already, they derive their notion of value from the dollar, and are dependent on the value of their collateral.

2.6. Lack of real world implementations of broad featured CBDCs

While many currencies aim to demonstrate and succeed on a specific set of features, the world is stil waiting for a currency that is sufficiently capable to be a CBDC. In Morten Linnemann Bech and Rodney Garratt analyse the set of features a CBDC needs to support. This main feature set is illustrated in figure 2.1.

In recent years, the discussion around central bank digital currencies has been lively among central banks [64] [61] [56] [40] [59] [25] [26] [62] [38] [58] [60]. Central banks around the world are publishing discussion papers and roadmaps, some even dare make some design decisions. Yet, with the exception of China [63], no countries have deployed a real world trail. Meanwhile the currencies that do have real world trails have closed systems and are managed by either corporate conglomerates [44]

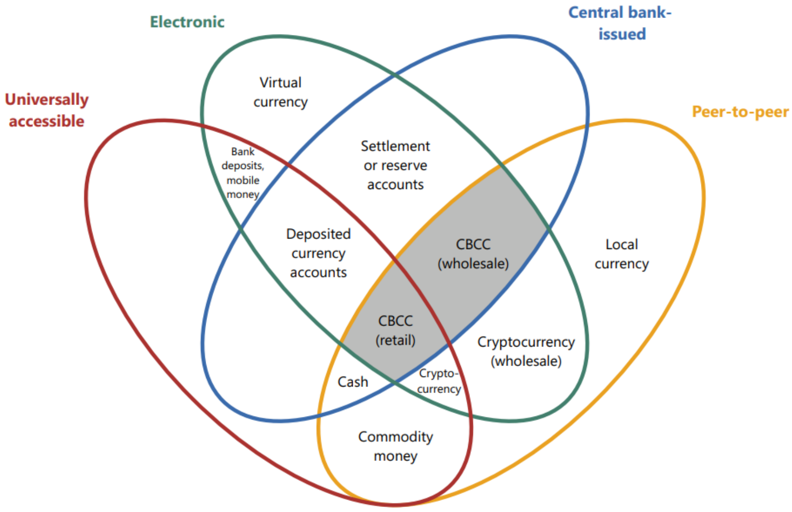


Figure 2.1: The money flower: a taxonomy of money [27].

or totalitarian states.

While stablecoins like Tether have demonstraded the appetite in the world for digital stable currencies, their fundamental flaw is in their centralised nature. The Tether Holdings Limited company holds the power over the entire currency, thus never allowing it to become a widespread payment system.

EuroToken is a prototype for a Central Bank Digital Currency. Its primary purpose is to implement, for the first time, a currency that is: digital, universally accessible, central bank issued, and peer-to-peer.

2.7. Research Focus and Structure

While a complete redesign of Europe's monetary system is obviously out of scope for this thesis, the previously described problems and requirements lead us to the following question:

Can we create a digital payment system that combines the functionality of world-wide online payments, and local off-line payments in a single solution.

This document describes the motivation, design, implementation and evaluation of the EuroToken system. The EuroToken system is a conceptual design that aims to fit the requirements stated in the previous section, as well as a limited proof of concept design testing certain aspects of the design. The structure of this work is as follows, in the next chapter we describe the design of the EuroToken system. The design is approached from the fundamental questions of a currency and answers the fundamental questions first. What is a digital currency? What is the double spending problem? And how to design a system that is scalable while not compromising the principle of double-spend prevention? The design aims to provide the following features:

1. Be a fully functional system of accounting
2. Preventing unsanctioned money creation
3. Scale to the size of the European union
4. Be off-line transferable

In order to not be limited in the same way as Bitcoin and similar currencies, we choose to sacrifice the following feature: Decentralization. This give us the required leeway to create a scalable and off-line capable system. However, we do attempt to provide the necessary tools to overcome the downsides of the centralisation.

3 EuroToken Design

Any payment system that aims to replace public money while being able to operate at the scale of the euro system needs to conform to a number of requirements. Such a system needs to be scalable, privacy aware, allow peer to peer transactions off-line. In needs to be price stable, exchangeable for euros, and most importantly, it needs to be secure and cheating resistant. In this chapter we first describe how a distributed block-lattice provides a good basis for a scalable, private, and off-line friendly transaction system. We then explain how we position the system in relation to the euro, how the price can remain stable, and how a system can mimic the properties of cash. We then go in to the details of how the system is secured, and how we prevent double spending while still remaining scalable and allowing off-line transactions. Finally, we explain how the system could be expanded upon by legal frameworks that can provide varying risk vs privacy trade-offs and how certain guarantees could be enforced in the system.

3.1. Distributed accounting and networking

The possibilities and limitations of any virtual currency are dependent on its system of accounting. In order to conform to the off-line, scalability and transparency requirements, a system of distributed accounting is chosen. As the fundamental building block for the EuroToken system we use a Hyper-Sharded block-lattice that keeps track of every users transaction history on their own edge device. By storing all information required for transacting at the physical end points of transactions, we create the possibility of direct off-line transaction between users, without any link to the outside world.

While the EuroToken system design is independent of the underlying communication technology, the off-line requirement leads to there being some limitations on the way users interact. Since off-line users cannot connect to servers we choose to work with a Peer-to-Peer system that allows users to find each-other based on personal identifiers.

We build on Peer-to-Peer networking, that provides a mechanism to discover the network location of users based on the same public key that is used to identify their wallet. This allows us to almost completely abstract away from locating users using IP addresses and ports. As a result we only have to worry about maintaining a users public key to identify and communicate with them across time. Our peer to peer network does not only abstract away from IP addresses, bus also from the IP network completely. Namely, it provides communication over Bluetooth without the need for any internet connection. This becomes very useful for demonstrating the off-line capabilities of the EuroToken system.

3.2. Block-lattice accounting

As mentioned for our distributed accounting system we choose to build on a block-lattice structure. As illustrated in figure 3.1 every user has a personal blockchain structured as a chronological, one-dimensional string of “blocks”. Every block will include a cryptographically secure hash identifying what block preceded it. Because of the trapdoor effect of the hash, any block will uniquely identify all blocks that come before it. This allows anyone to verify the validity of entire history of another user, given the last block in this history. Every block will contain a single transaction that specifies the transfer of funds from one user to another, as well as a reference to a corresponding block in the chain of the transaction counterparty. This effectively creates a system of double accounting.

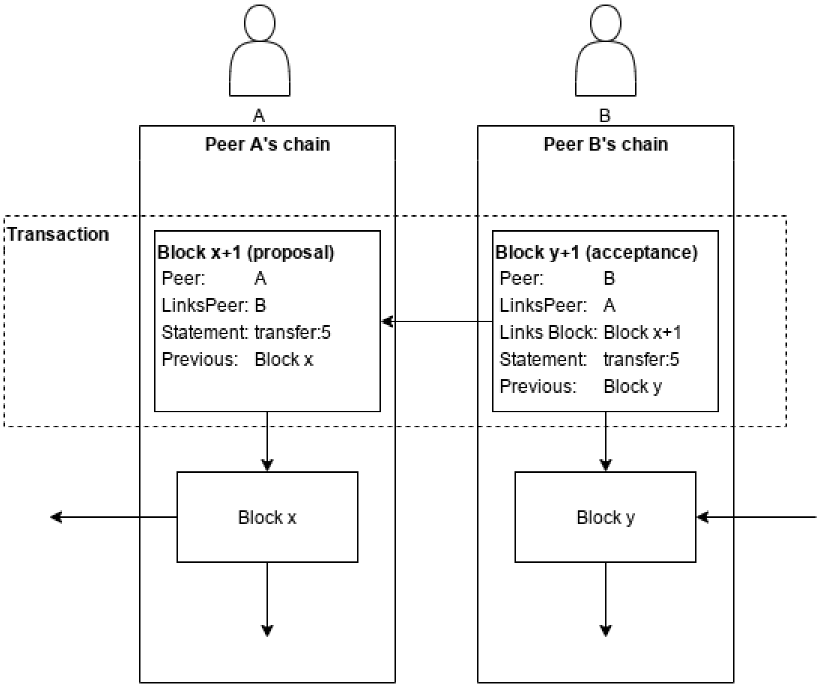


Figure 3.1: Block-lattice structure

Every block can contains a “declaration” by the user, or a reference to the declaration of another party. These declarations are digitally signed by the declaring party and form the base of any transaction. To do a transaction the sending user (Alice) will create a new (half)block with a declaration stating “I transfer 1 EuroToken to Bob”.

When Bob receives this block from Alice, he can accept it by creating a block in his own chain and returning it Alice. Before Bob accepts the block, he first validates the history of Alice by requesting enough of her chain make sure that Alice doesn’t validate any of the network rules that would invalidate Bob’s receiving of the money. Once Bob is satisfied with the correctness of Alice’s transaction history he incorporates a new block declaring the acceptance of Alice’s transaction. This block includes the hash of Alice’s block, thus entangling the chains of Alice and Bob together. Bob now has a signed proof by Alice that the transaction happened. He can use this to prove the transaction happened at any point in the future.

3.3. Gateways: Euro to EuroToken exchange

The viability of any currency as a store of value over a given time frame is dependent on the stability of its price over that time frame. This is an issue that has plagued decentralised crypto currencies from the very beginning. The hope is that the currency will stabilise itself when it reaches a critical adoption level. However even currencies like the euro and US dollar don’t remain stable without periodic interventions of their respective central banks.

The euro has long served as the core of the financial infrastructure of the European economy. It has essentially done this using two consumer facing versions of money: the euro as a publicly accepted, physical item of value (the public euro), and the euro as a digital, privately managed, unit of account (the private euro). These public, and private types of money serve citizens in different ways. The public euro is the most stable store of value since its guaranteed by the central bank, it also has the advantaged of requiring no internet connection to use. While the private euro has digital advantages in usability and security, but derive their value from the “reliability” of private banks, and are typically only insured by governments up to 100.000 euros [20]. With the declining usage of public money in favor of digital money, the need for a new type of euro to fill the gap of public money is getting stronger.

For these reasons we present the EuroToken system as a 3rd type of money. Instead of reinventing

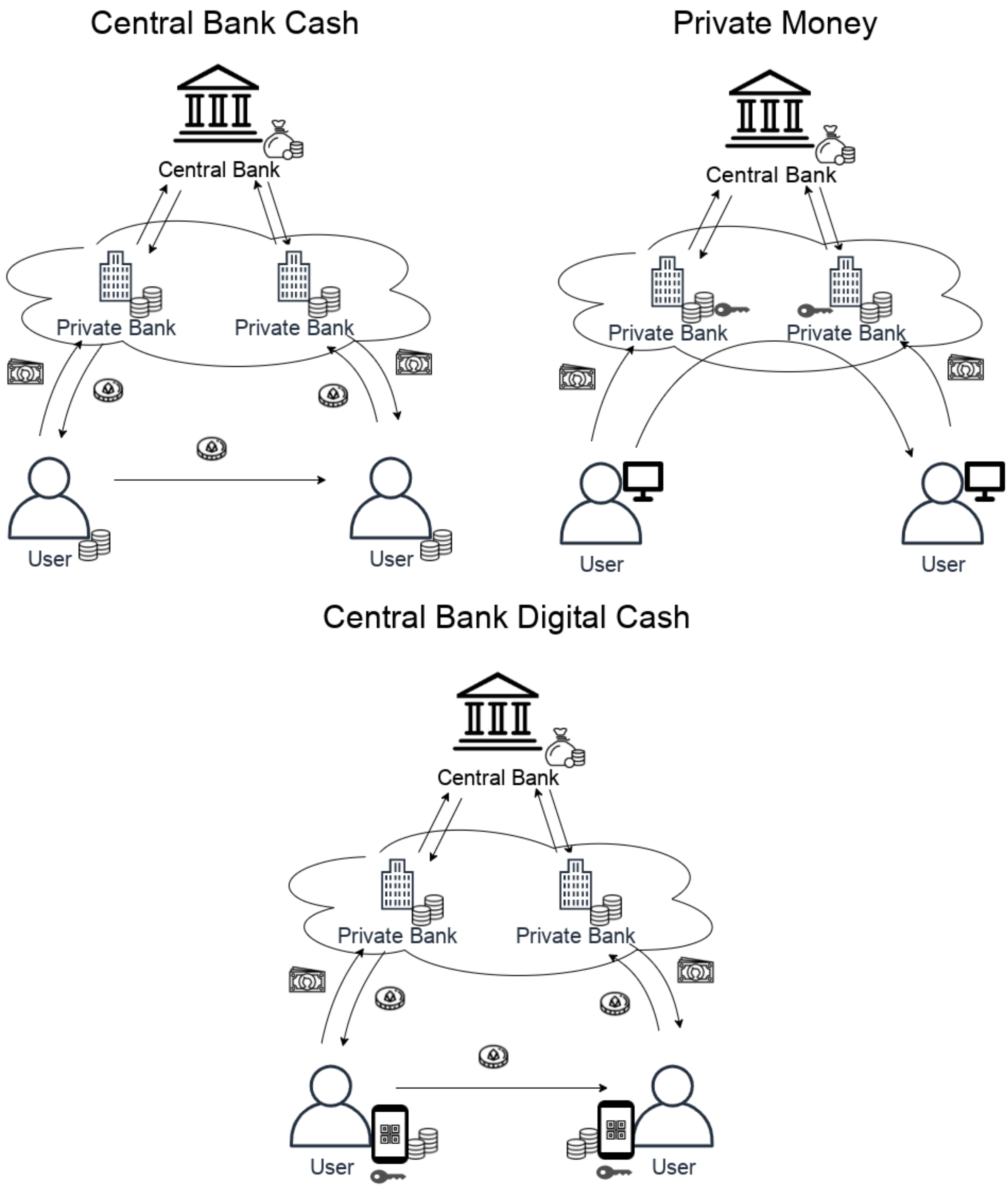


Figure 3.2: Usage flow of cash, private money, and EuroToken.

the wheel of “stability” we connect the EuroToken system directly to the euro system, while providing extra features on top of the current euro system.

In order to properly connect EuroTokens to the euro system, an easy and value-transparent method of exchange is required. Just like private and public euros are exchangeable though local banks, a mechanism is needed to exchange between euros and EuroTokens at a 1:1 ratio. To do this, we implement a “gateway” between the private euro system and the digital euro. This gateway implements the EuroToken protocol on the one hand, and interfaces with banks on the other.

In our current design, the gateways are designed to be run by public parties associated with the central bank. Any detailed speculation on the best way to connect such a system to the established euro is best left to economists. However, we envision a possible future where multiple gateways are run by existing private money institutions who perform the heavy lifting of day to day exchange. In such a system private banks would act as an accounting system for the EuroToken exchange without being allowed to leverage their EuroToken position. The Central bank would allow these private institutions to conform to reserve requirements in the form of EuroToken holdings rather than only cash. By not allowing private banks to mint new EuroTokens, but only exchange them, the central bank can control the amount of EuroToken in circulation in a similar way to current public money. This would insulate the EuroToken from the impact of a failing euro or bank, in the same way as physical public money is currently insulated from such failing.

This way of connecting to the euro could allow for a smooth transition to a digital form of public money, while the established and regulated financial institutions are still positioned properly in a place where financial services can be provided.

3.4. Transaction finality and Double-spending

In order to remain a viable store of value, a currency needs to provide protection against any non-sanctioned creation of that currency. If a network allows its users to “create” new money in any significant way, the value of the coin will drop as the supply increases, thus undermining one of the most fundamental function of the currency. The structure of the blockchain provides an immutable and signed history of any transactions, thus enabling users to prove that the funds they are attempting to send actually exist. However the blockchain does not inherently allow users to prove that they have not spent, and will not spend, the same balance again.

In this section we explain how the network prevents unsanctioned creation of currency.

3.4.1. The double spending problem

In order to spend their money twice, a user has to create 2 blocks that are positioned in the same place in their blockchain. This is what is called a “double-spend attack”. This attack is only detectable if both of the conflicting blocks are found. Since we have opted for a distributed blockchain this detection becomes a non-trivial problem to solve. The transactions of 2 conflicting blocks might be re-spent many times by the time anyone sees the 2 conflicting blocks and notices that a double spend happened.

Bitcoin and similar currencies solve this problem using a global blockchain that everyone has access to. This allows users to check whether a given balance has already been spent by inspecting the global database of transactions. However, the global knowledge of the Bitcoin chain is inherently unscalable. Additionally, the details of the Proof of Work method of block generation leaves a certain measure of uncertainty with regards to the “finality” of any transaction in the newest blocks. This often requires users to wait up to an hour to be sufficiently confident their transaction really happened.

A solution to this problem in a network with a distributed block-lattice, starts with the realisation that the issue of detecting double-spending can be reduced to the issue of detecting “chain forking” in our network. The usage of the blockchain allows us to make sure that all transactions are ordered and consistent, this means that double-spend needs to be in 2 separate versions of that history. Thus requiring 2 blocks that refer back to the same historic block. This is a fork in the chain. We cannot “prevent” a user from creating 2 conflicting blocks in their chain as their chain is stored on their own device. But we can make sure that the rest of the network only accepts one of the 2 blocks, thus only accepting 1 “spending” of the balance. This choice between 2 conflicting blocks needs to be consistent so anyone in the network is working with the “same history”. Additionally, forks need to be detected and resolved before the balance is spent again by any of the 2 receiving parties. This way a double-spend will not propagate into the network and is limited to the users involved in the 2 transactions. To resolve the conflict between blocks we define the concept of “transaction finality”. For a transaction to be final, it needs to be “validated” and “stored” in the network, while any conflicting transaction will be rejected by the network. Transaction finality the guarantee that a merchant needs before they can send their goods to a paying customer.

The transaction finality problem in our network has several possible solutions. In [31] Brouwer presents a method of distributing blocks to a randomly and fairly selected list of witnesses that would probabilistically detect any conflicting block before the receiver would accept them. In [47] Guerraoui Et. Al present a more theoretical method of block broadcast. These might be good candidates for future research. However since these solutions are inherently probabilistic, there is no hard guarantee that any double-spend will be detected in time.

3.4.2. Balance vs spendable balance

Currently lacking a good exact and distributed solution, we choose to utilize a decentralized network of trusted validators. These validators maintain the last transaction of users that register with them. Any user who receives money, can verify the non-existence of a conflicting block with the associated validator of the sender.

In the rest of this section, we define the concepts of “spendable balance” and specify the information requirements for marking a transaction as finalised.

In order for Alice verify if Bob is able to send her the money he is sending, she needs to know that Bob has sufficient funds. For this reason a rolling a balance across all transactions could be maintained across all blocks. Where the balance B for a given block with sequence i (B_i) is:

$$B_i = B_{i-1} + C_i$$

.

Where C_i is the change in balance for the block with sequence number i. This is negative when sending money. However the balance of a user does not take into account the concept of transaction finality. So instead we maintain the total “spendable balance” instead.

3.4.3. Finality statements

Before Alice can add the output of a block she received from Bob to her “spendable balance”, the transaction from Bob first has to be finalised. To achieve this a validation is performed with Bob’s associated validator. This is done by sending the validator a finality proposal.

3.3 The finality proposal block includes notes a list of hashes that point to transactions from Bob. Together with this block for the validator to sign, Alice will send all of Bobs blocks from the last transaction to validate to the last block the validator knows about. The way for Alice to determine what information this is, is explained in the section on checkpointing later in this chapter. In addition to Bob’s blocks, she will also send her “accepting blocks” that include the transaction in her chain. This is to make sure she can only claim a transaction from Bob once. Bob’s validator will then verify:

1. That there are no other transactions that conflict with the one to Alice.
2. That there are no other “accepting blocks” already linked to this transaction.
3. That Bob’s chain is valid up to the last transaction to verify.

If this is the case it will sign the proposal. If a later transaction from Bob is received that marks a fork in his chain, the fork from Alice becomes the only accepted fork, and the other one is rejected. Using this finality statements as proof of this, Alice is now allowed to spend the output of the transaction.

In the case that a different fork from Bob has arrived at the validator first, the fork where Alice receives money is rejected. Since Alice has already accepted the transaction in her chain and may have built other transactions after it (though not spent the output), she could be requested to submit a new finality proposal without this block. Since Alice is not permitted to spend the funds from Bob until it has been finalised this is the point where double spending is handled.

Note that the specific handling of this event might not involve the forfeiture of a transaction. We discuss this further in the section on off-line payments and conflict resolution.

3.4.4. Verification

For a block to be considered valid:

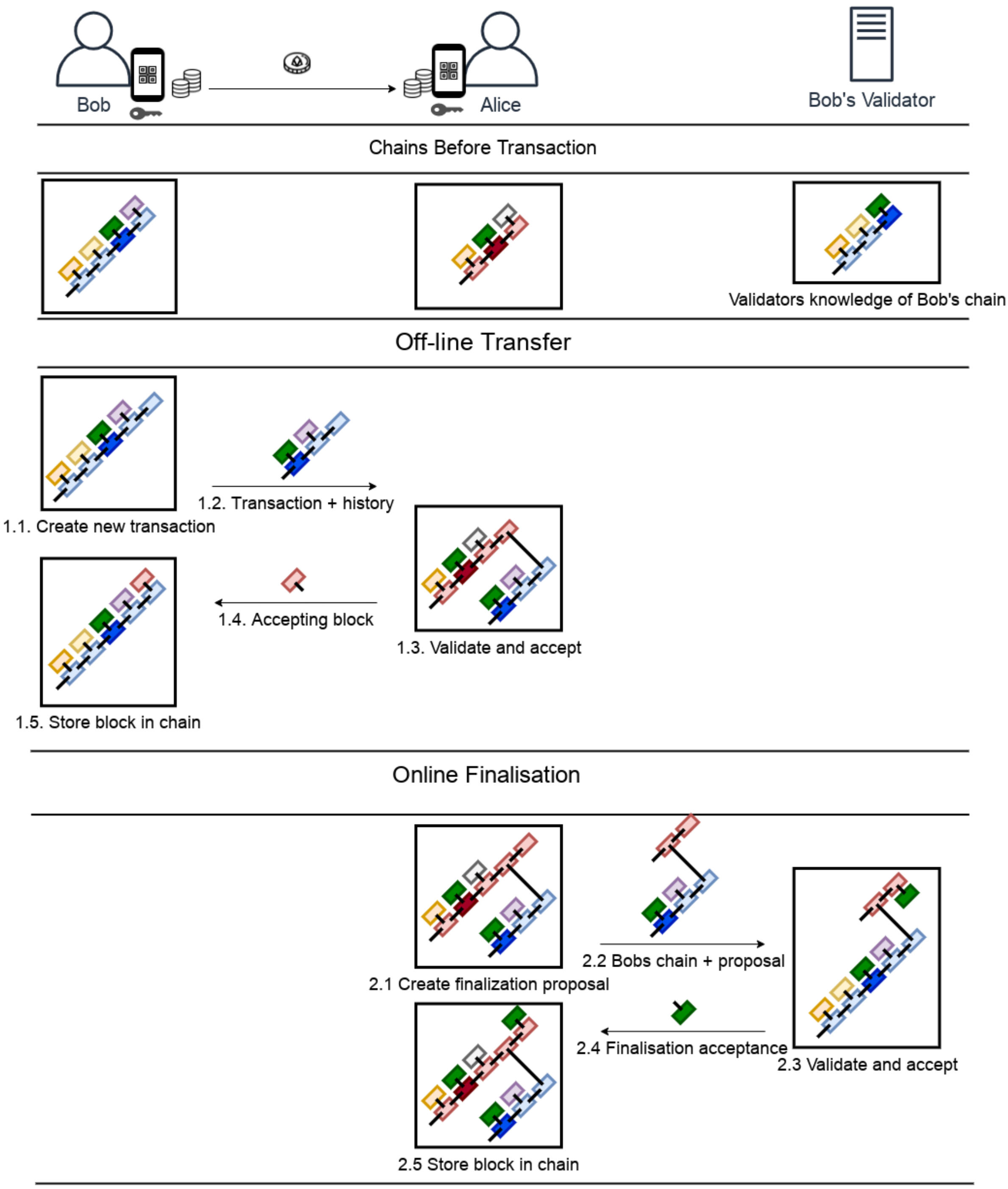


Figure 3.3: Off-line transfer and finalisation

1. All standard block-lattice invariants are maintained.
2. All blocks preceding it are verified to be valid
3. The total spent amount is to be less than the spendable balance.

For a transaction of a receiving block to be considered final:

1. A checkpoint from from the validator of the sender has to be exist in the chain of the user AFTER the transaction.

By introducing checkpoints, the required information at the point of transactions is reduced. When Alice and Bob set transact between them, Alice can determine the validity of Bob's transaction by inspecting only Bob's chain, down do his last checkpoint. However, Alice must also request all Bob's information down to the last Full checkpoint, in order to

3.4.5. Spendable balance

Once a transaction if finalised, "spendable balance" of Alice can be calculated. The spendable balance changes at two events, the finalisation of an earlier receiving transaction and when Alice spends her money. As such the spendable balance SB_i for a given block with sequence number i is:

$$SB_i = SB_{i-1} + F_i - S_i$$

Where S_i is the total amount spent in the block with sequence number i, F_i is the total amount finalised in the block with sequence number i.

3.4.6. Conclusion

In the future we envision the system to take one of three routes regarding transaction finality. First, system could be built on a future breakthrough in distributed transaction finality. Second the system could be built on a probabilistic but bounded transaction finality, where the rare double-spend is eventually detected and settled through the legal system. Or third, like in our solution, the system is build on trusted nodes that verify transactions for user. Like the gateways, these validators could be run by regulated financial institutions. Such a system would most resemble the current financial system, with the added benefits of off-line transactions, programmable money, a standardised system of accounting, instantaneous international transactions, etc.

3.5. Checkpointing

Because of transaction finality, when Alice receives the transaction from Bob, she can rely on the finality statements, rather than having to validate the chain of everyone he received money from. This reduces the validation load to only Bob's chain. However this still has some issues. First, Bob's chain will grow larger over time, thus slowly increasing the validation load. Second, all this information needs to be stored by Alice until it can be delivered to Bob's validator.

The way this problem has been solved in traditional blockchain systems is through the global blockchain and limited transactions per second. By having only miners or stakers being required to maintain the whole blockchain, only a few machines have to be able to know the entire chain and store all that data. But this is still inherently unscalable.

A second issue is one of privacy, when Bob has to send Alice all of his chain for verification, Alice can derive much from this information. Though we would like to see methods of privatization added to perhaps conceal transfered amounts, we still need a way to minimize the information leakage to 3rd parties.

To solve this issue of validation scalability, we define a form of checkpointing. We periodically create a checkpoint block in a users chain that , that includes a summary of the entire chain before it. This information is:

1. The total "spendable balance" at that point in the chain

2. The public key of the validator who is responsible for this wallet.

3. A statement that the validator has received all blocks before this point

Alice now knows the blocks that are already stored by the validator. When Alice is receiving money from Bob, she only requires Bob's blocks down to the his last checkpoint.

3.6. Off-line transactions and online validation

The EuroToken system has the intentional distinction between transactions and their finalisation. Because of this, the first step of transactions only require a direct connection between users. In theory, this allows to transact off-line, if they're willing to risk that a conflicting block already exists in the validator. Of course, in this case, the transfer of funds depends on the trustworthiness of the sending party.

In this section we discuss a few ways of interacting with the system that allows for different risk exposure to the parties.

3.6.1. Online transactions

When users are connected to the internet, a real life interaction can easily combine the finalisation step with the transaction, only transferring goods or services once the transaction is finalised. We envision this as the default way for users to interact, especially for large transactions, and transactions with strangers, since this reduces the risk to either party to zero.

3.6.2. Off-line transactions

Since money only becomes spendable after finalisation, the receiving user is the one that will lose funds when a double spend happens. To lower the risk and damage of this, certain systems might be put in place. For this, we build on the fact that transactions are always signed by both parties. This makes sure that a proof of double-spending always exists, and is obtained no later than the finalisation attempt.

A way to ensure a user that they will receive the funds is by allowing senders to register their identity with their validator. The validator would sign a statement that the identity of the sender is known and that they will take legal action in the event of a double spend. This then optionally allows the validator to accept the risk of double spending. In the case of a double spend the validator would sign a special statement with the receiver, that invalidates the double-spent transaction, but transfers and finalises the funds from the validator instead. The validator will then pursue legal action against the sender for fraud.

In the meantime the validator could block the sender to perform online transactions and checkpoints until they first settle the double spent funds. The details of what is both technically and legally possible here is a good subject for future research.

3.7. Regulation of validators

One could argue that system hasn't solved the issues of transaction finality and double-spending, and that we only defer the problem to a different point. It is entirely conceivable that trusted validators could cheat by allowing certain wallets to double-spend. To add to this, using the checkpoint functionality a validator can specify a higher spendable balance than is actually logged in the chain.

However, when comparing our system to the current way private institutions are regulated, the blockchain structure of transaction can provide a powerful method of maintaining the integrity of the institutions. While we cannot prevent fraud at the institutional level, we do provide an option for detection to allow for regulation.

In order for a regulator to check that a validator has done their job with integrity, they need to be sure of 2 things:

1. That all "statements" have been made consistently with the rules of the network.
2. That no other "statements" have been hidden from the regulator.

"Statements" in this context, describe anything that the rest of the network puts their trust in. These are:

1. Finality statements
2. Checkpoints

Both of these statements are created in the form of "accepting blocks" and are stored by users and their validators with an associated hash. We now propose a two round system for validating all transactions within a given time period. In round one, we validate that all statements have been made correctly and publicly store the hashes. In the second round, once we have the hashes of all statements available, we validate that all statements from other validators exist.

In the first round all information in the database of the validator is processed for consistency. Since all statements by the validator are made in the form of blocks in their personal blockchain, they have an explicit order. The blocks of the validator, together with the blocks of all the users the validator is responsible for, are processed in the same way as the validator was responsible for processing them. This step in the process ensures that all statements are made correctly.

In the second round, we ensure that there is no statement withheld by the validator. This is done by publicly publishing a signed list of the hashes of all statements made by the validator. This allows regulators to cross-check that all inter-validator statements have been reviewed by a validator. To make this step more efficient, we propose that when checking a validators consistency, regulators generate a list of statements for each distinct validator to increase the efficiency of distributing these hashes to relevant parties.

A possibility also exists to allow the public access to these records to ensure the integrity of their institutions.

4

EuroToken Implementation

In this section we describe the implementation of the EuroToken protocol, as well as the prototype we built to test and showcase the capabilities of the EuroToken system. The protocol is implanted on top of IPv8. In includes an android/kotlin implementation as well as a python implementation. We then built a Euro to EuroToken exchange and transaction validator on top of the python implementation. On top of the kotlin implementation we built a wallet app that is fully capable of securely transferring EuroTokens between wallets, as well as exchange them with the EuroToken exchange.

4.1. Architecture

The architecture of the EuroToken system has two main components. The gateway and the wallet. The gateway is managed by a central trusted party and fulfills two main functions from the design. These are to asynchronously validate transactions made by users, as well as handling the exchange between EuroToken and Euros. As such it maintains a bank account as well as its own wallet. The wallets are operated by each user, and they are fully capable of transferring funds between each-other without having to interact with anyone in the euro system.

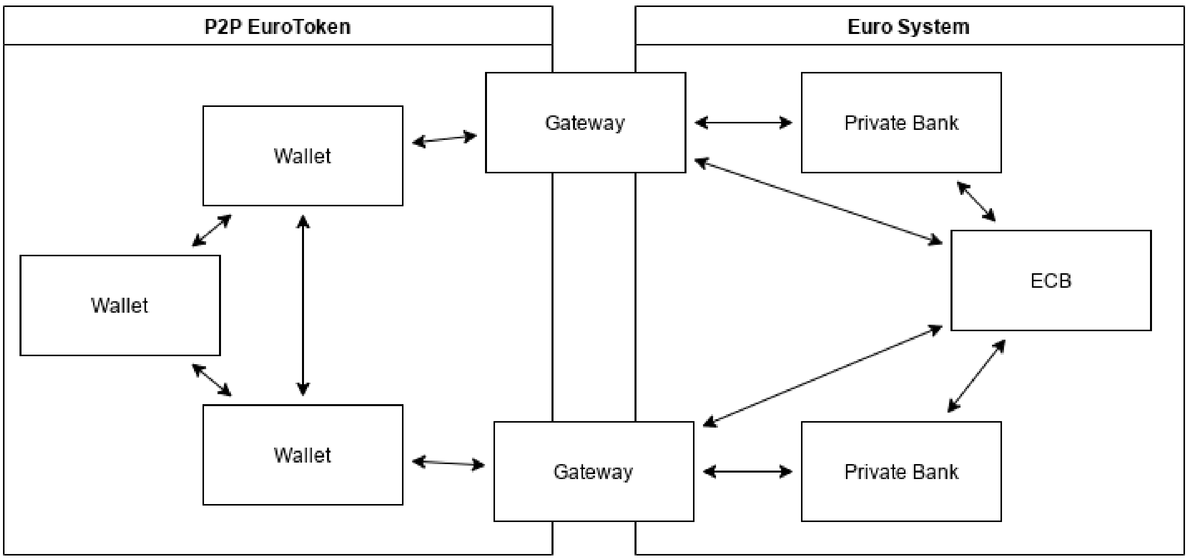


Figure 4.1: EuroToken architecture

In figure 4.1 we model the main communication channels. Within the P2P EuroToken system we have all wallet to wallet, and wallet to gateway communication. This communication happens directly between the communicating nodes using Peer-to-Peer technology.

In the Euro System, we make use of bank APIs for gateway to bank communication. The communication with the ECB symbolises monetary policy enacted by the ECB on bank EuroToken reserve requirements or possible direct exchange of euro for EuroToken.

Rather than implementing both an exchange as well as a validator we chose to implement and test these as a single entity. However, since the gateways roles might be split in the future the technical implementation of the gateway keeps the validator roles separate from the exchange roles. This results in a single EuroToken exchange software product, that is able to perform either or both of the functions.

4.2. EuroToken transfer protocol

The method for accounting and transferring of EuroTokens lies at the heart of this project. Because of this the choices regarding the implementation of the networking stack and blockchain technology will have a direct effect on the feature set and scalability of the whole EuroToken network. We need a network stack that allows communication both off-line directly between devices, as well as online across the world. Finding and connecting to any wallet without relying on central servers is a main requirement. In addition, the off-line transfer ability of the system is best demonstrated by creating an android client. Another requirement is therefore that an implementation is available for android as well.

One option is to implement a full blockchain protocol and associated network stack from the ground up to adhere to our exact requirements. This would give us a lot of say in the exact feature set of the network. However, since the science of distributed networking algorithms has mostly settled, most peer to peer communication technologies have already been implemented somewhere.

The second option is then to build upon some existing peer to peer networking library, while implementing the blockchain protocol ourselves. This option has some benefits as the usage of a block-lattice is not yet very common, and thus is not implemented as a stand alone package anywhere. For the P2P library we have several options. We considered LibTorrent [19], Libp2p [18] and IPv8[PyIPv8]. LibTorrent has a number of interesting peer to peer features like peer discovery and data transfer but sadly fell short when it comes discovery of peers based on public keys. It can be classified more as a file location protocol than a peer location protocol. This would mean we would have to implement a peer location system ourselves. Libp2p is a modular peer to peer networking stack that provides a large suite of P2P tools. Libp2p uses a Distributed Hash Table (DHT) to allow peer discovery based on a peer-id [49]. There is an JVM/android implementation available, which also makes it possible to create an android client. Finally we looked at IPv8. IPv8 offers direct peer discovery based on public key and provides a framework for interaction called Overlay networks. Overlays provide a context for peers to interact within with particular message types. Crucially, IPv8 has an implementation in kotlin [43].

Rather than implementing the blockchain mechanism ourselves, there is a third option. IPv8 includes a module called TrustChain. TrustChain is in essence a block-lattice type distrusted ledger technology[41]. The technology does not fully solve double spending they way we originally designed it, so some work is required to adapt TrustChain to the EuroToken system, but it would provide a good basis for our implementation.

We choose to build on IPv8/TrustChain for this project as it allows us to build on their kotlin implementation for the wallet as well as the python implementation for the gateway.

4.2.1. TrustChain structure

Every user runs a *Peer* which consists of a public/private key pair as well as a collection of their *transaction* history in the form of their *blockchain*. The Peer can be uniquely identified by their public key. Every statement made by the peer is signed using their private key, and the validity of any signature can be verified using the public key of the Peer.

Every peer has a list of their own history of transactions in the form of a collection of *blocks*. Every block is created and signed by a Peer, and includes the details of the transaction as well as a cryptographically secure hash of the previous block signed by the user. Importantly, the hash of a block uniquely identifies the block, as the trapdoor effect of cryptographically secure hashes ensures the infeasibility of finding another block with a given hash. The block thus uniquely references the previous transaction of the Peer. Since every transaction uniquely references the block before itself, the hash of any one block, recursively identifies *every* transaction made before by the Peer. This is as long as the Peer honestly references to their previous block. This referencing mechanism effectively links all blocks together in a gradually growing chain, thus making is a *blockchain*.

Every Peer in within TrustChain has their own chain, yet most transactions are *between* users. For this reason all transactions are made to happen in the chains of both users involved. In TrustChain, this is achieved by having one of the two parties create a proposal block. In addition to the public key of the Peer, their previous hash, and the contents of the statement, the proposal also includes the public key of the counterparty. When the counterparty receives the proposal and agrees to the terms in the statement, they create an acceptance block. This acceptance block functions includes the public key of the counterparty, as well as the hash of their previous block, thus placing it in their blockchain. In addition the acceptance includes a reference to the proposal, thus linking them together. Both the proposal and acceptance blocks are then stored by both users, so they can both prove the transaction fully happened.

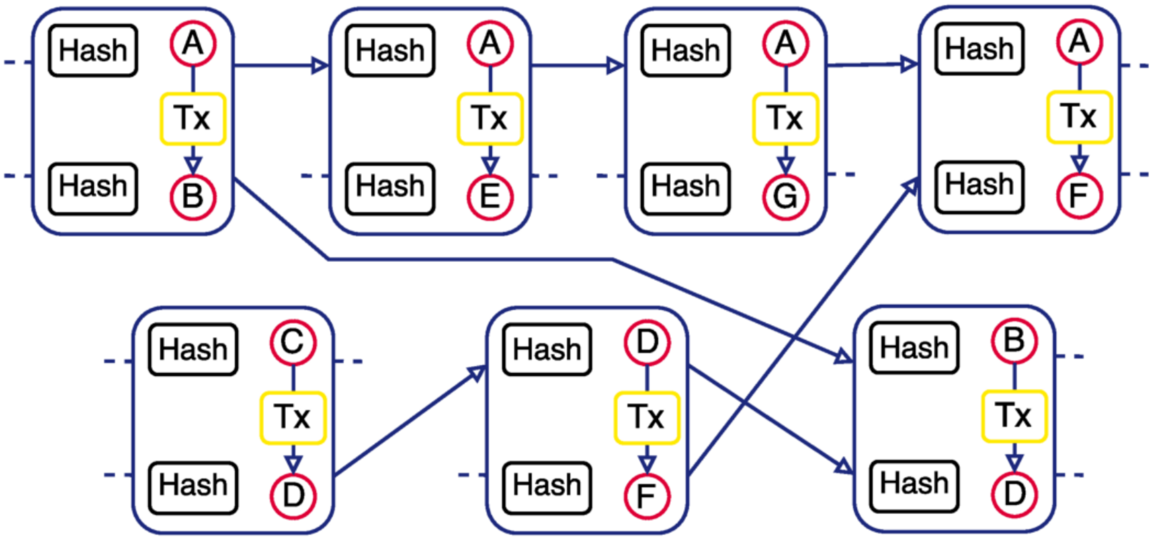


Figure 4.2: TrustChain block-lattice, interconnected personal blockchains [41].

4.2.2. EuroToken extension

The structure inherited from TrustChain serves us quite well as it conforms quite well to the block-lattice design we require. However, neither the python, nor the kotlin implementation includes any logic for running a currency. Before TrustChain can be used for EuroToken, it needs to be expanded to allow for value tracking and transfer.

TrustChain is quite open for expansion. It allows users to define their own block-types as well as validation logic for these blocks. TrustChain will make sure blocks are valid as a chain, by enforcing typical block invariants like hash correctness and signature validity. TrustChain makes use of IPv8 for its communication and exposes an API to create and sign blocks to other peers. TrustChain will then handle the process of sending the blocks over the IPv8 network.

In order to create the EuroToken logic we defined a number of TrustChain block types to achieve our goals. In order to conform to the scalability requirements all EuroToken proposal blocks by a user will include the balance of that user. This is part of the rolling-checkpoint mechanic that allows us to scale each users personal blockchain indefinitely without sacrificing scalability. The EuroToken block subtypes are as follows:

Transfer block

The transfer block is the core of how users interact. The proposal is created by the sender of a transaction and the acceptance by the receiving party. The block includes the amount to be sent as well as the balance of the sender at that point. The receiver will verify that the balances of the sender are valid before creating the acceptance. The receiver will then calculate the spendable balance all the way back to the last “full” checkpoint block in order to validate whether the balance of the sender is even spendable.

Checkpoint block

In order to be able to spend the balance a user has received they need to proof that a validator has taken notice of the blocks of the senders. The checkpoint block serves as this proof of validator. The proposal is created by the user and the acceptance is created by the validator. A checkpoint block is only considered “full” if the both the proposal and acceptance exist. If the acceptance does not exist, the block is meaningless and any validation will keep recursing the chain until a full checkpoint is found.

Creation block

The creation is a special type of transfer that is done by a trusted exchange. This block is the only way in which new EuroToken are allowed to enter the system and will only be considered valid if it is made by a trusted party. The proposal is made by the exchange and the acceptance is made by a user.

Destruction block

The destruction is the opposite of a creation. The proposal is made by a user and acts as a transfer to an exchange. The exchange then also creates an acceptance block. The creation and destruction blocks are used to convert between Euro and EuroTokens.

4.3. Wallet

The core of the EuroToken network is the wallet. The wallet allows users to transfer funds to any other wallet anywhere on earth over the internet, or directly from device to device over Bluetooth. The wallet also has the capacity to exchange Euro for EuroToken and vice versa.

Instead of building a wallet from scratch we build on top of the TrustChain superapp [15] [65]. This app was developed to showcase the capabilities of the kotlin implementation of IPv8 [43]. The superapp in implemented as a collection of different subapps that use the same underlying IPv8 implementation. The app includes multiple other projects which we can integrate with the EuroToken system.

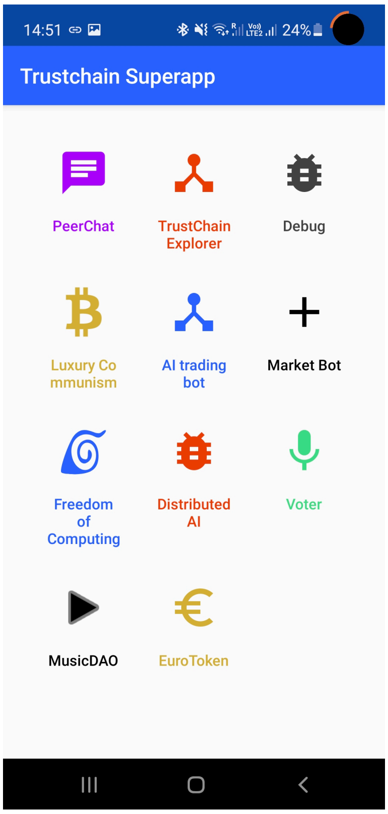


Figure 4.3: TrustChain Superapp [15]

4.3.1. Peer-to-Peer transfer

The main feature to showcase is the ability to transfer the EuroTokens. Before a user can send money to another user, they first need to know their public key. While sending money directly to a user is possible as part of the app, the share and transfer of public keys is not very practical. For this reason we implemented 2 ways of handling this. The first way is by generating a money request with QR code. This works best when the users are in the same room, or can share the QR code through some other means.

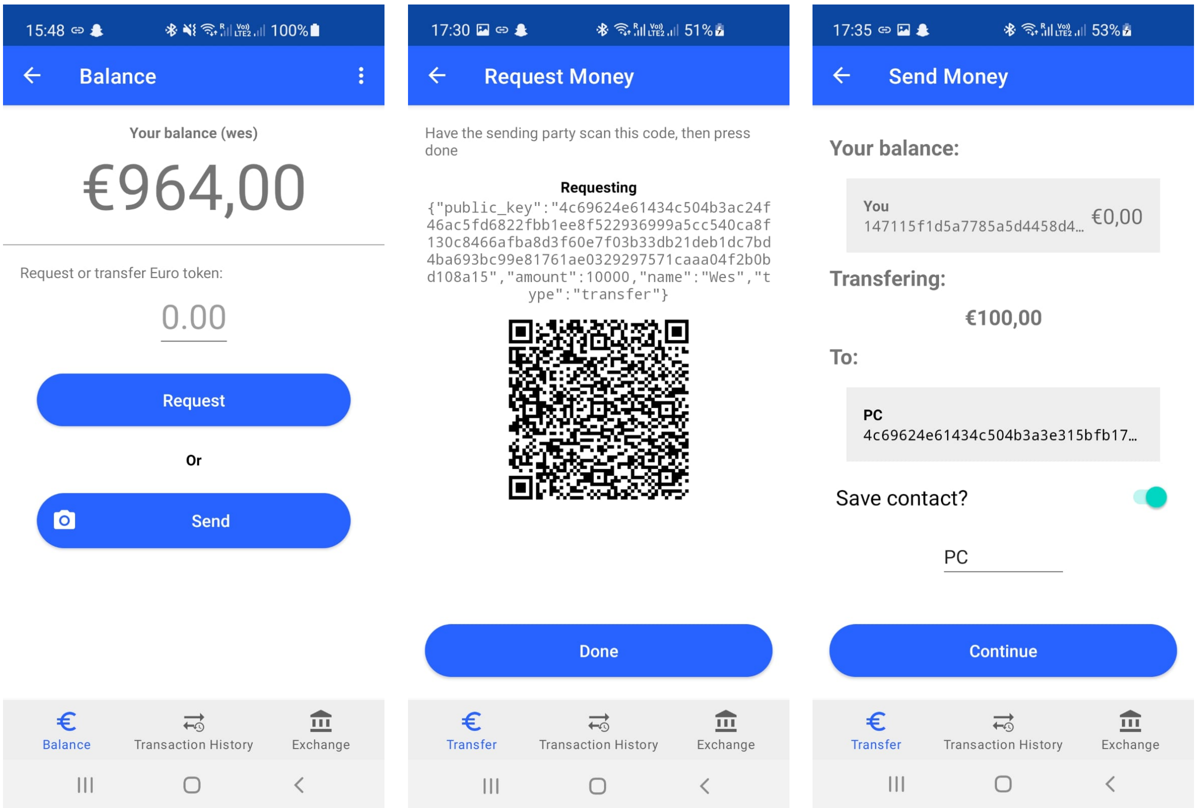


Figure 4.4: Wallet transfer by QR

A second and more user-friendly away to send money is through the already existing chat app PeerChat. PeerChat allows users to add each other as contacts and then uses IPv8 to send public key addressed messages. Instead of reinventing the wheel we added EuroToken payments to PeerChat. This mirrors payment apps like the Chinese WeChat Pay and the Norwegian Vipps. We believe this method of payment in the most natural for users.

Regardless of how users send money, their entire transaction history is available within the EuroToken sub app. Here all the different transaction types can be seen. The transaction screen also shows debug information like all checkpoints that have been performed with a validator. It also shows information about whether an acceptance block has been received from the counterparty. On this screen money can be payed back as well, and blocks van be resent in case of network failure.

4.4. Exchange

For the EuroToken to be part of the Euro system a mechanism of exchange is required. The exchange forms the bridge between the digital EuroToken and the rest of the Euro systems. The exchange mechanism must support the two main flows of value.

The first we call the creation flow. This flow handles the exchange of Euro for EuroToken, thus creating EuroToken. This involves the handling of payment into a bank account, verifying this, and paying out and equivalent amount of EuroToken to the users wallet. The second flow is the destruction flow. This flow does handles the opposite conversion. It handles a payment of EuroToken and pays out the equivalent amount to a IBAN bank account.

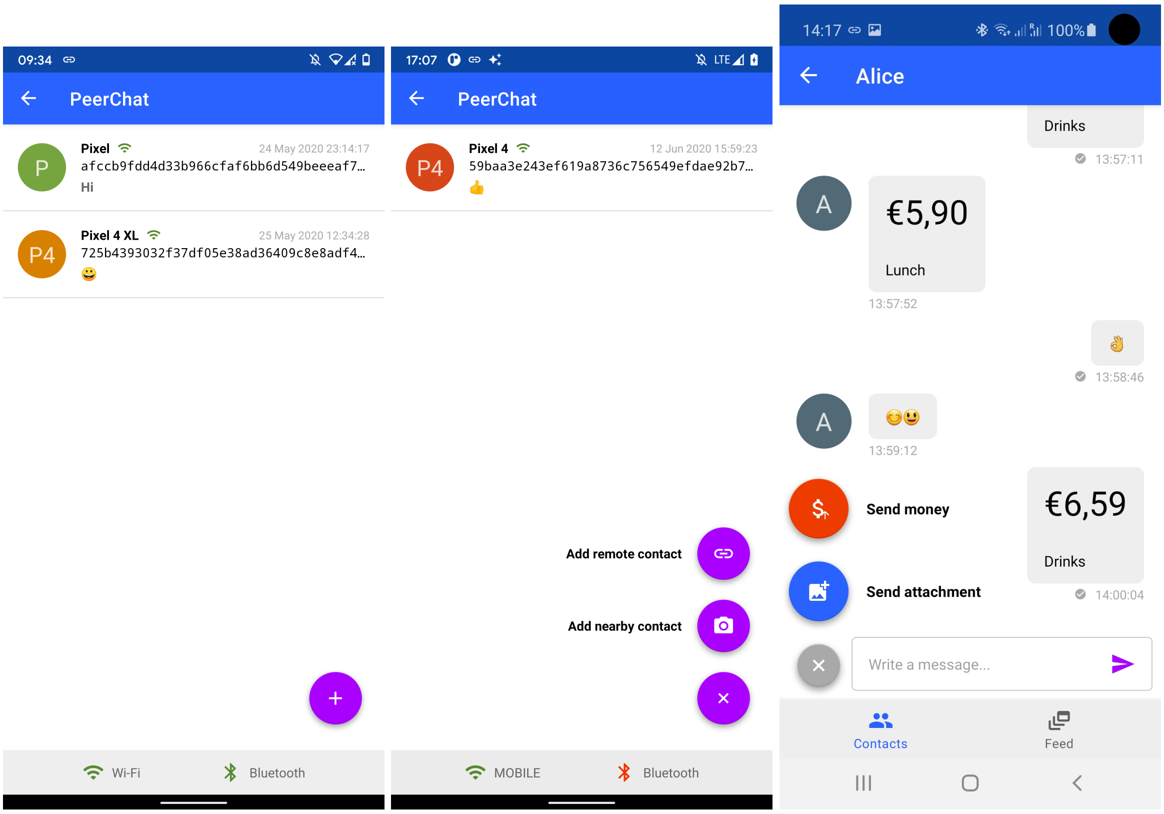


Figure 4.5: PeerChat, contacts [65] and pay via PeerChat

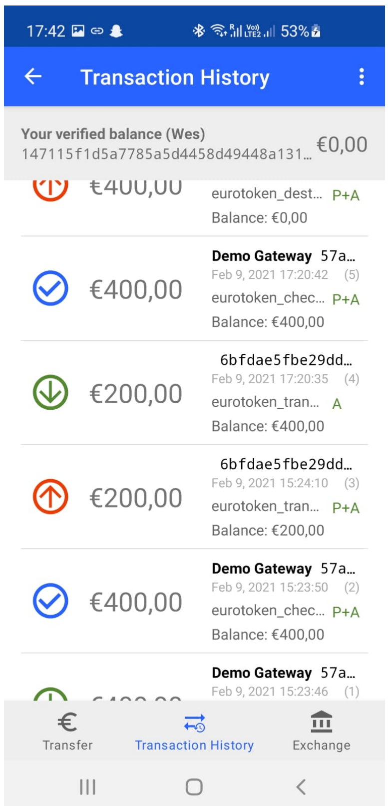


Figure 4.6: Wallet transactions

To handle this flow we build the exchange node. This node exposes a web frontend that allows the user to exchange their money in either direction. The exchange is implemented in python, and is based on the python implementation of IPv8 [12].

4.4.1. Buy and sell instantly

The frontend of the exchange is kept as simple as possible for demonstration purposes. Users do not need to login, and can buy or sell their EuroTokens directly on the front page.

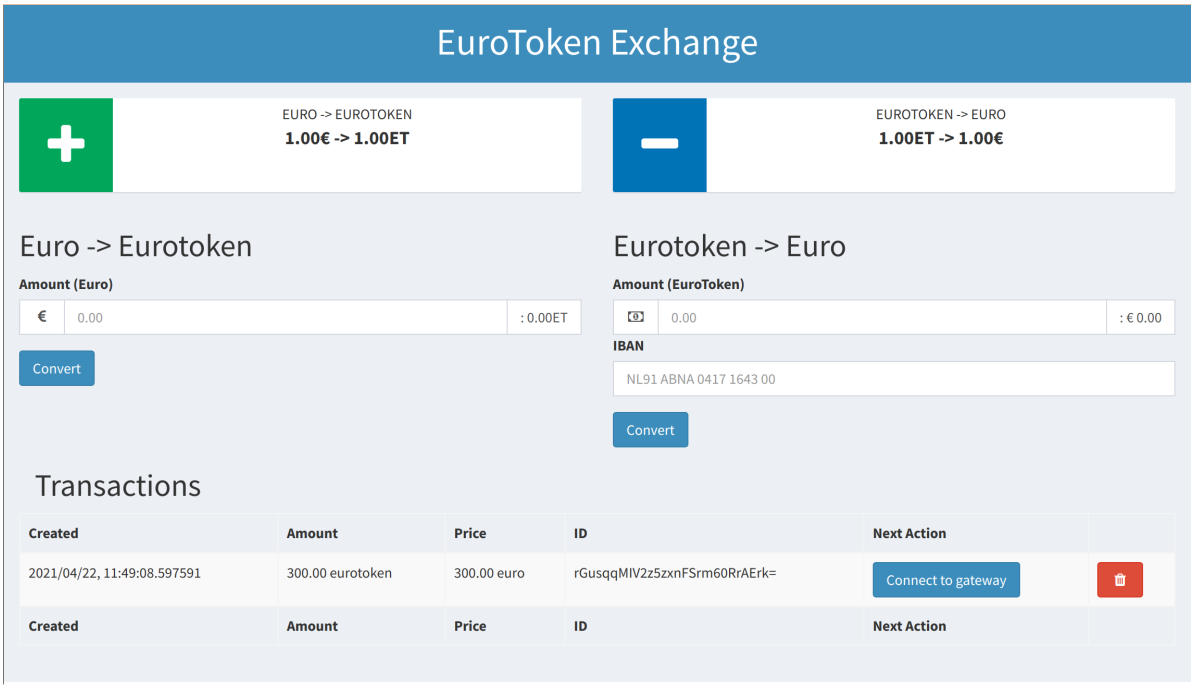


Figure 4.7: EuroToken Exchange Frontend

4.4.2. Exchange flow

The flow of exchange is different in each direction and require different steps from the user.

Creation

In our prototype we use the payement system API of a popular bank to enable users to pay us Euros. The creation flow can be seen in figure 4.8. The creation step is the most complex. This is because the sending of money to a user requires the exchange to know the public key of the user. In order to obtain EuroTokens the user accesses the web interface of the exchange, which will lead it through the following steps:

1. The user specifies the amount of EuroToken to buy. This creates a new transaction. The user then scans a QR code generated by the exchange using the wallet. The QR code contains the public key of the exchange, as well as a payment id. The wallet will then send a special connect message to the exchange over IPv8 with the payment id. When the exchange receives the message, the public key of the sender of the message is stored in association with the payment. This will be the public key to which the EuroToken will be transfered once the transaction is complete.
2. The exchange creates a new payment request with the bank for the specified amount, which the user is then redirected to.
3. The exchange is alerted by the bank once the payment is complete.
4. The exchange will now send the money over IPv8.

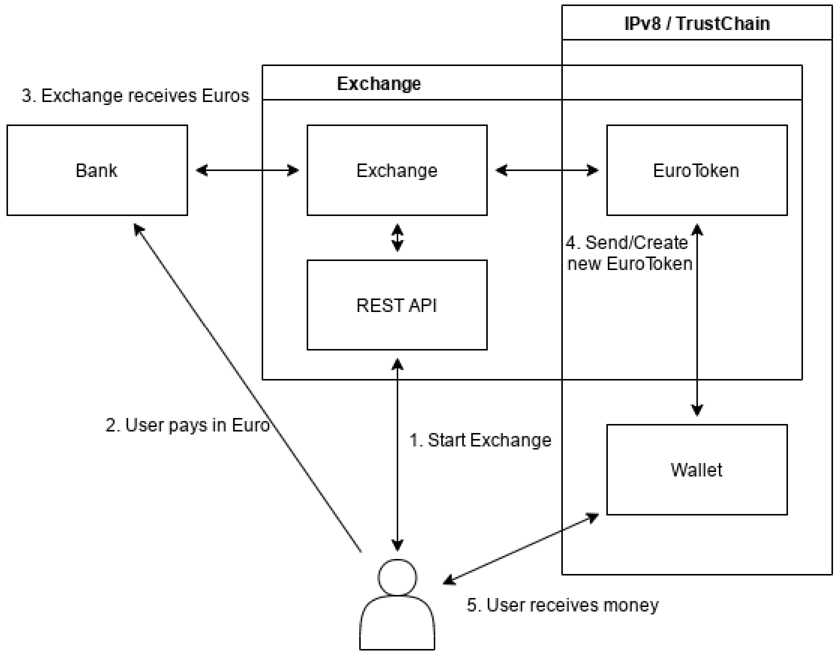


Figure 4.8: EuroToken Creation Flow

Destruction
The destruction flow is a simpler process. If the user knows the public key of the exchange it can be performed completely in the wallet app. The user would simply send a destruction transaction to the exchange which includes the IBAN the user would like the money to be payed out to as part of the block.

However if a user does not know the public key of the exchange, the interaction has to happen through the UI. This would involve the following flow:

1. The user specifies the amount to exchange along with their IBAN.
2. The exchange generates a QR code which includes their public key, as well as the amount.
3. The user scans the QR code and confirms the transaction in the app.

Within the app the exchange flows are handled using the pages shown in figure 4.9.

4.5. Validator

Together with the exchange, the validator is one of the special nodes that allow the EuroToken system to function. As can be seen in 4.6, a validation checkpoint is automatically requested after a transaction has been received by a user. The checkpoint makes the entire balance if the user “spendable”. The main task of the validator is to maintain the last blocks of all users in the network. This makes it impossible to double spend a transaction since any conflicting block has already been accepted by the validator. This makes the first block to arrive to the validator the one and only block at that position in a users chain.

Since the output of a transaction is only spendable when a full checkpoint comes after it, the wallet automatically performs a checkpoint after every transaction. This keeps the amount of blocks that have to be validated during every transaction as low as possible. This leads to every transaction involving only 4 half-blocks from the perspective of the sender. A sender only needs to share the transaction proposal itself, the block before (which is a checkpoint proposal), and the associated checkpoint acceptance. The receiver then only needs to verify the correctness of these 3 blocks and send back the acceptance to the sender. This preserves the transaction privacy of the both the sender and the receiver, revealing only the relevant transaction.

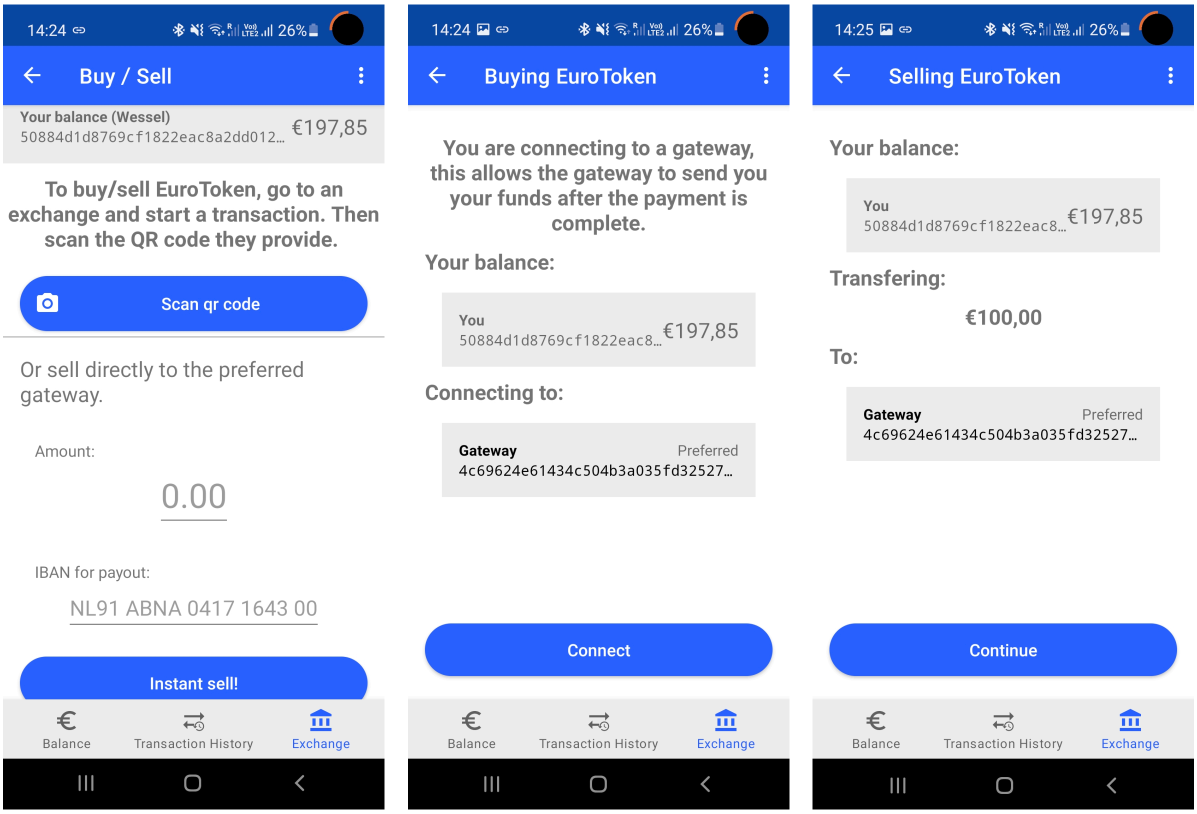


Figure 4.9: Wallet exchange

5 Evaluation

In this chapter we will evaluate our solution to the problems as explored in the problem description. We first describe two field trails that showed the proof-of-concept in action. This demonstrates how EuroToken is able to perform the basic functions of money and allows for off-line spending. We then describe some structured experiments that measure the scalability of the network and evaluate whether the promise of a double-spend proof but still scalable network has been met.

5.1. Field trial

The purpose of the implementation in the super app was to demonstrate the features of the EuroToken system. In order to test the implementation and the viability of the protocol in the real world, a field trail was conducted. We tested the EuroToken system during the morning hours, at café Doerak in Delft. As showcased in figure 5.1, the owner of the café generated a payment request for the amount of a single coffee and displayed it in the restaurant. Customers could then scan the code to transfer the money, and the owner who immediately see the money appear in their account.

Figure 5.1: Field trial

This trail showcases the simplicity of taking digital payments without having to go through the process of registering with a traditional payment provider. Using the EuroToken system all the owner of Doerak needed was a smartphone in order to participate in the modern economy.

5.2. Off-line trial

By building the EuroToken app on the TrustChain super app we could build on the Bluetooth transfer features to implement the off-line transfer of funds. In order to test this implementation and showcase the off-line transfer capabilities of the EuroToken system, we conducted another trail away from civilisation. As showcased in Figure 5.2, in the mountains of norway, away from all network connectivity, we conducted a transfer of funds using the bluetooth connect feature of the superapp.

Figure 5.2: EuroToken off-line trial

There is room for improvement in the practicality of off-line transfer of data between two devices. We found the process of creating a Peer-to-Peer bluetooth connection between two mobile devices somewhat cumbersome. And the system would greatly benefit in usability from proximity based data transfer via NFC.

Regardless of the possibilities for improvement, the trail successfully showed the viability of off-line transfer. It shows the potential of the EuroToken system to act as a disaster proof payment system that remains functional at any distance from civilisation and during any disaster that would wipe out global communication infrastructure.

The user trades the risk of deferring transaction validation until they connect to the network again for off-line transfers which allow for an instantaneous transfer of funds, without requiring a connection to anyone in the rest of the network in order to perform the initial transfer.

Exploring the possibilities of reducing the transaction risk between initial transfer and transaction finalisation is an interesting topic for future research. Using reputation systems or digital identity solutions combinded with judicial accountability, the risk could potentially be reduced to near 0. - TODO work this out in more detail

In order to prevent double spending, the current implementation of the protocol disallows the re-spending of transactions that have not first been finalised. In order to provide a full disaster mode, re-spending funds without full transaction validation by the network is a must. This could be achieved by expanding the protocol to enable the settling of multi-hop transfers. Like the original off-line transfer system, this would require the 2nd receiver to accept the risk, that both of the peers that their transation depends on have double spent. When performing the initial off-line transaction, they would receive all the blocks neccesary to finalise all transactions before it with the gateways of the 2 peers before them. - TODO work this out in more detail

5.3. Scalability in network size

In order for the EuroToken system to be able to function at the scale of the eurozone, the ability to scale is crucial. In order to evaluate how the system performs as the number of users grows, we performed the following experiments.

We adapted the python implementation to simulate the network as it grows. We configured a set number of nodes to continuously transact with one another and performed check-ins with their gateway whenever they had received a set number of transactions. The nodes chose random transaction partners for each transaction and check pointed with their gateway after every 4 transactions. In order to asses the scalability of the network, we ran several experiments where we varied the number of transaction nodes in the network. For each transaction we measured the time taken for each node to validate the transaction and how many transactions have been validated in order to calculate the transactions per second of the gateway. We also recorded the number of blocks the gateway validated for each transaction they validated.

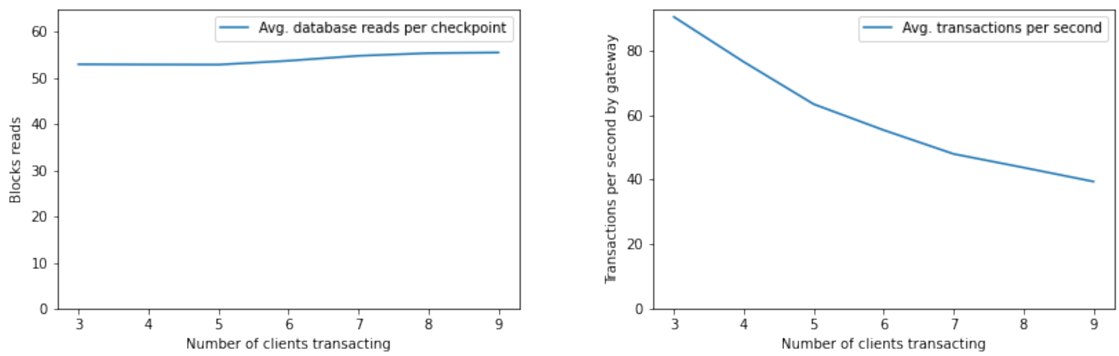


Figure 5.3: Effect of network size on scalability

The results of our experiments are illustrated in figure 5.3. While there initially seems to be a drop in transactions per second as an effect of the number of users in the network, this effect cannot be seen when looking at the number of blocks validated. This discrepancy can be explained by the circumstances of our test environment. Since all nodes are run on the same machine there is some competition over resources like disk access. When looking at the number of blocks required to validate a single transaction, the increase in nodes in the network, even when users have a complex transaction history, has no effect on the complexity of validating a single transaction for the gateway.

In addition to varying the number of transaction nodes we also wanted to test the effect of increasing the number of gateways. Based on our implementation we expect a linear relationship between the number of gateway compute power in the network and the transactions per second that can be validated. This is because there is no communication between the gateways that makes their validation dependent on one another. We ran 4 transacting nodes split among with 1, 2 and 4 gateways. We then again measured the TPS of the gateways.

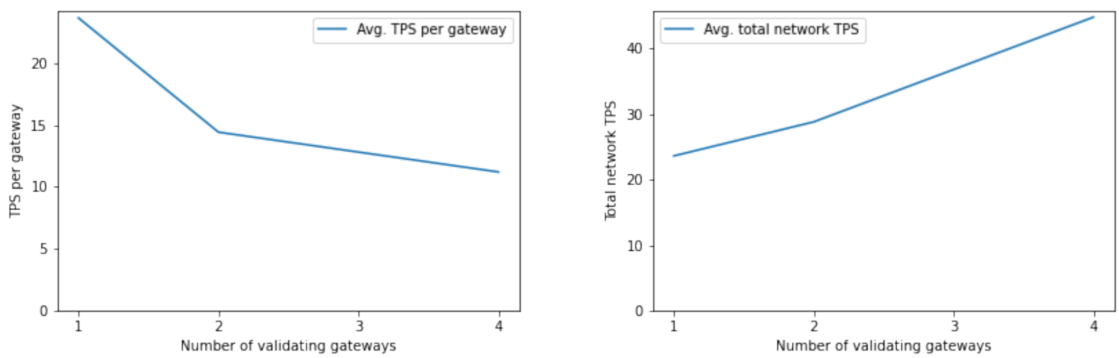


Figure 5.4: Scalability in gateways

As illustrated in figure 5.4, the number of gateways seems to have an effect on the per gateway transactions per second. However the number of blocks validated around 16 for each gateway count, we believe this to be the effect of the shared resources between the nodes. When we then look at the total transactions per second of the network, we do see an increase in total TPS with a growing gateway count. We still expect this to grow linearly in the real world.

5.4. Scalability in history size

Another way in which EuroToken achieves scalability is by mitigation of the effect of a growing chain size using checkpointing. We claim that this allows the network to scale indefinitely as the personal chains of the users grow. In

In order to validate this effect we set up a simulation where multiple users transacted up to 1000 transactions. All users started with an empty chain and transact together at the same rate. This means that all of the chains have the same length throughout the testing process. We measured both the time taken to validate a transaction, as well as the number of blocks validated.

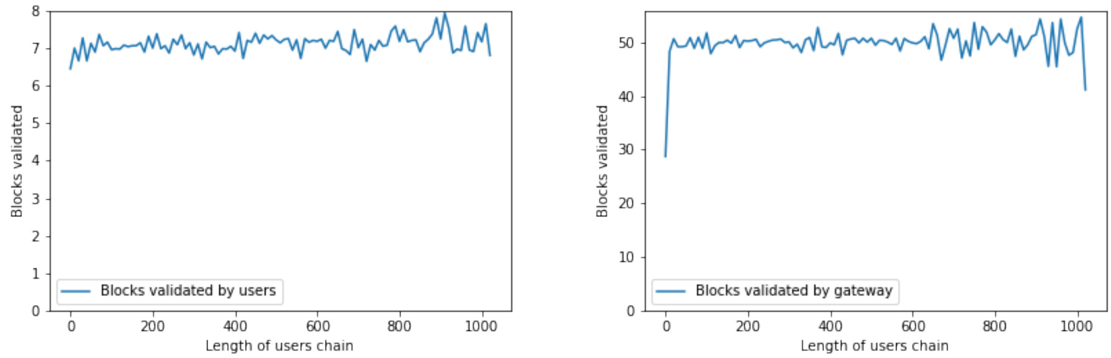


Figure 5.5: Effect of chain length on number of blocks validated

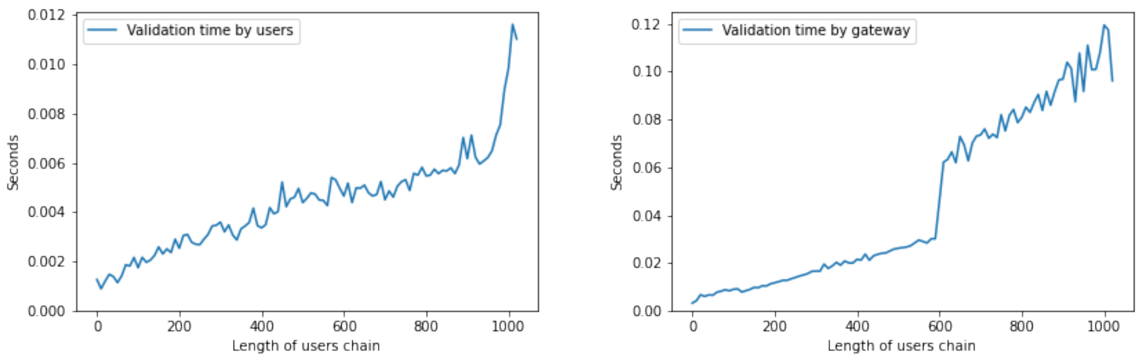


Figure 5.6: Effect of chain length on validation time

The results are illustrated in figure 5.5. Here we plotted the number of blocks that are required to validate as a function of the number of transactions the user has transacted before this. This shows that the number of blocks a user or gateway has to validate does not change as the chains grow.

In figure 5.6 we show the time to validate the transaction as a function of the number of blocks transacted. Here we do see a gradual rise in the processing time as the chains grow. However, since the number of blocks validated seems to stay constant over time this rise in validation time is best explained by the rising cost of database lookups of the blocks, which takes longer as the size of the database grows over time. Since all blocks before the last checkpoint has been evaluated and are no longer required for validation in the future, these can be written to a longer term storage as to not unnecessarily increase the validation times.

Most importantly, the number of block accesses stays the same over time. This is a direct result of checkpointing, as users only need to validate blocks down to the last checkpoint. This separates EuroToken from currencies like Bitcoin where the database of blocks is constantly growing leading to higher validation costs and validation times during startup.

5.5. Trade-offs in user and gateway validation times

The EuroToken gets its scalability and off-line transaction ability from the concept of checkpointing. The collapsing of all transactions before a given point into a single checkpoint block allows any counterparty to simplify the entire history of a user to the balance in the checkpoint block. This prevents the exponential growth of required validation, which allows the system to scale to any size. In this section we explore the effect of various checkpointing frequencies and demonstrate some trade-offs.

We simulated a network of randomly transacting users. Every run of the experiment we varied the number of transactions the users would do without checkpointing. Each users performed over 1000 transactions each run. We then measured the total number of blocks their counter parties had to verify in order to validate their transaction. The entire network varied their checkpointing frequencies together.

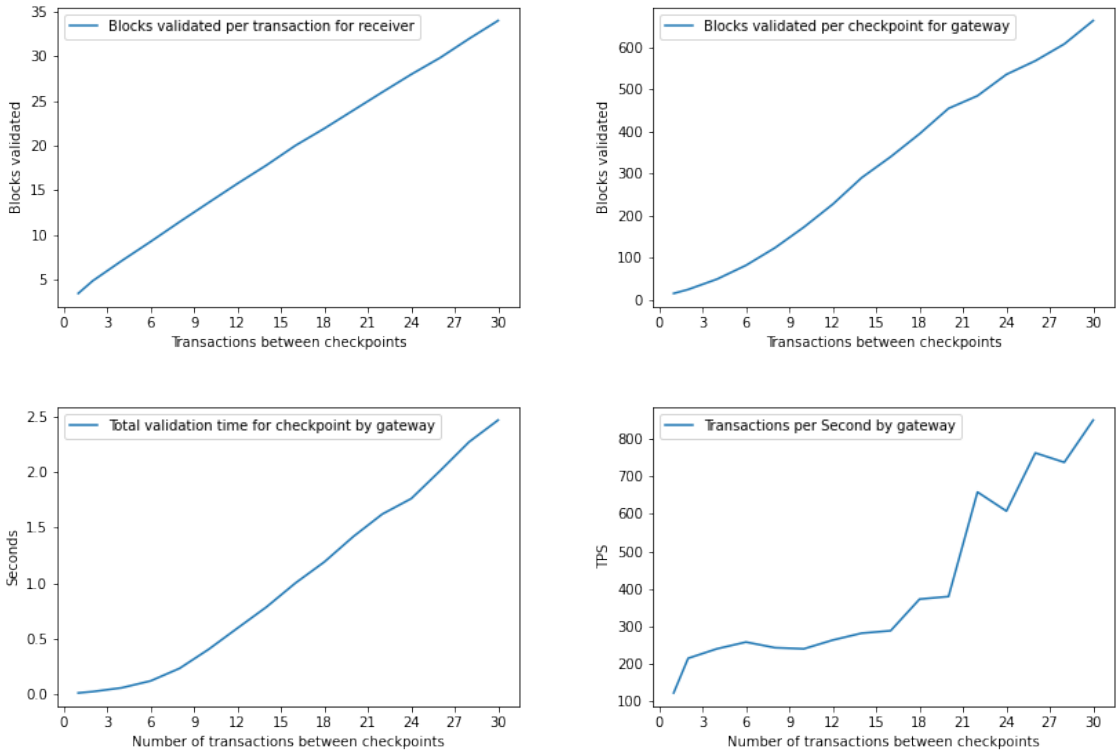


Figure 5.7: Effect of checkpointing on validation

As illustrated in figure 5.7 the effect of the checkpointing frequency is present. As the time we wait between checkpoints increases the effort for each transaction increases for the clients.

When looking at the effect on the gateway the image different. While the number of blocks the gateway has to validate does grow as well as the time taken to validate the transaction, the gateway has to do this much less frequently. This removes some overhead from the validations, allowing the gateway to validate more total transactions as the frequency of validation decreases.

In any implementation of EuroToken in the real world some attention should be dedicated to this phenomenon, as users are incentivized to checkpoint as frequently as possible, while this might not be optimal for the network.

5.6. ECB requirements

In the problem description of this document we described the requirements of a digital euro as specified by the ECB. In this section we review the extent to which the EuroToken system conforms to the requirements. The requirements are summerised as follows:

- 1 **Enhanced digital efficiency**
- 2 **Cash-like features**
- 3 **Competitive features**
- 4 **Monetary policy option**
- 5 **Disaster back-up system**
- 6 **International use**

- 7 Minimise ecological footprint (cost saving and environmentally friendly)
- 8 **Ability to control the amount of digital euro in circulation.**
- 9 Cooperation with market participants
- 10 Compliance with the regulatory framework
- 11 Safety and efficiency in the fulfilment of the Eurosystem's goals
- 12 Easy accessibility throughout the euro area
- 13 Conditional use by non-euro area residents

We achieve **enhanced digital efficiency** and a **competitive feature set** by designing EuroToken as a digital, peer-to-peer, programmable payment system. We achieve **cash-like features** with direct and off-line transferability without the need for intermediary parties. EuroToken provides the ECB with a new set of **monetary policy options** by having the Central Bank controlling the creation and destruction of EuroTokens. The off-line transaction capacity could be extended to make EuroToken a **disaster proof** payment system. With backing during deployment of the ECB, EuroToken could become the standardised digital currency of Europe allowing **international** with ease. The rest of the requirements are legal questions and are left out of scope.

6 Discussion and future work

The process of designing a digital currency is not something that can be done in one master thesis. There are many challenges left to solve before we have a distributed currency that has the features necessary to serve the payment needs of the entire eurozone.

In this section we go over the three main contributions EuroToken makes, their limitations and their possibilities for improvement. We then more generally discuss the ability of EuroToken to conform to the requirements set forward by the ECB and what issues are still left to address.

6.1. Trade-offs between anonymity and off-line transactions

EuroToken achieves off-line transactions by making every transaction a signed statement by the sender that transfers their funds to the receiver. Regardless of any action by the sender, this statement is cryptographically linked to their wallet and can be used by the receiver at any time to prove that the transaction happened. This can then be used to keep the sender accountable to their statement. While we provide the mechanism for the receiver to ensure that the sender has the funds available, we do not provide a mechanism to prevent the sender from off-line spending a second time.

The main limitation of our method of off-line transfers, and perhaps all methods of off-line payments, is that double spending is only prevented and addressed when interacting with online with the network. This does keeps the currency from inflating, but still leaves some risk with the receiver.

Here we address some solutions to prevent, disincentivize, and limit the recurrence of off-line double spending fraud. We see potential solutions to this problem in 2 areas. The first is at the point of transaction, and the second at the point of double-spend detection at the gateways.

At the point of detection the gateway learns that one of their associated wallets has cheated. If the identity of the sender is know to the gateway, they can block the sender from doing any online transactions until the double-spend has been resolved. The gateway can refuse the signal of any checkpoints after the detection.

The gateway could also include a reputation for the sender in every checkpoint, so this becomes visible to future receivers at the point of transaction. The checkpoint could also include a statement as to what degree the identity of the sender has been verified by the gateway.

Then at the point of transaction the receiver can verify some details about the sender. The receiver could choose not to interact with wallets that have been created very recently, have a poor reputation, hasn't checked in with the gateway for a long time, or doesn't have their identity registered with the gateway.

Of course these solutions rely on the identity of the sender being known to the gateway, something that may have negative implications on privacy. For this reason the identity itself could be registered with an identity provider that maintains all the personal information of the sender and only uses this in the event of overt cheating. The design of such a system and its integration with EuroToken has been left to future research.

6.2. Scalability without centralisation

In order to allow for the features of scalability, price stability and off-line transfer, the main trade-off has been in decentralization. The original promise of a decentralized currency that also has the three aforementioned feature, while promising, might never come to fruition.

Our design currently relies on trusted central gateways to solve the main issues of digital currencies. In decentralized system this role is usually performed by a blockchain or similar store, combined with some consensus algorithm to determine what gets written. Our solution has a different concept of consensus by allowing anyone to make any transaction on their own chain. By storing at least the last few transactions of a user, anyone can ask the gateway if a double spend has happened. Consensus is thus delegated completely to the gateway.

One possible criticism of this solution is that by its reliance on central gateways the problem of network-level double spending prevention only moves to the level of the gateways.

In the context of decentralized finance (DeFi) this would disqualify the system entirely, but in the context of a trans European payment system, some level of centralisation can be tolerated if not desirable. Institutions have been the daily runners of our monetary system for a very long time, and while not without its issues, the system has been overall successful.

The issue of the auditing of the gateways can then also be solved in the same method at it has been so far. Only this time, the bookkeeping is not only done by both the sending and receiving banks, but also the customers themselves. Additionally, the digitally standardised nature of the system, would make this process much easier, and be nearly automatic.

While the risks that are associated with centralisation are no worse than those of the current economic system, a system that does not rely on this should always be preferred. While not quite ready to be global payment systems, the decentralized currencies of the world have made significant progress over the last decade, especially in the efficiency of consensus protocols. The possibility still exists that a scalable solution to the global storage problem can be found. When this happens, the EuroToken system can start to rely on other methods of consensus.

One of the challenges that remains in that area is the decentralized method of double-spending settlement. This would involve the global storage of a persons double-spend history for a period of time, limiting their future spending capabilities. This still requires identity solutions, something that will likely always require some real world verification by some party.

While the promise of decentralized finance has some merit to it. The main problem is the correction of mistakes. Stolen Bitcoin can never be retrieved, judgements to pay damages cannot be enforced, assets cannot be frozen, collection agencies cannot lay claim on digital assets, etc. While some of these practices are considered by many to be cruel and outdated, they do stem from the general option of society on how the world and economy should be run. The mechanisms by which government sanctioned parties can intervene in our financial lives have been serving some human driven purpose. Any system that removes the ability to intervene needs to also solve these issues.

Ideally these rules have been set by society through the democratic process. Any system that is completely disconnected from this mechanism is likely grow out of sync with the needs of the people. The utility of having some centralised, but highly scrutinised parties should not be underestimated.

6.3. Price stability, deflation and remuneration

The price stability of EuroToken is derived directly from the euro. By having the central bank guarantee the exchange between EuroToken and Euro both ways, the system is able to keep the price stable.

This is not the whole story however. EuroToken can derive its value from the euro if and only if the euro remains stable. EuroToken will effectively become an extension of the current euro, rather than a currency itself. While the euro is unlikely to negatively influence EuroToken, the other way around also needs to be addressed. This is also why double-spending prevention is so important. If some method of unsanctioned money creation is possible the hyper inflation that would take EuroToken down would take the entire euro with it.

While preventing double spending is a technical and policy problem, economic problems with the EuroToken system can also threaten the euro system as a whole. On example of this is the concept of deflationary currencies. While Bitcoin intentionally built in deflation in its currency and sells it as a feature, the ECB of intentionally maintain a steady inflation of the euro. This is done for the express purpose of discouraging people from storing their funds as euros, thereby encouraging money to be invested in relevant ventures. Any form of deflation would make the euro an investment. This would lead people to passively store the currency, thus decreasing supply, driving up the price, making it an even better investment. This positive feedback loop continues until the economy grinds to a halt. Anyone with loads is forced to default, investment dries up, prices and wages drop, and the currency seizes to be a good denomination of value.

Even then, a set inflation can be acceptable to some people. If this happens on any significant scale, the managed inflation of the ECB will be counteracted. In times of economic turmoil, the euro will be the safest option leading to drops in investment right when they are needed most. Currently, both our private and public money are fundamentally bad at storing large amounts. Holding a lot of cash is impractical and dangerous, meanwhile storing large amounts in the bank leads to exposure to the risk of bank failure, something that is extra likely in hasher economic times. The failing of the euro to be a good store of value is an important aspect. The ECB has been speculating on some solutions to this problem. One way is to simply limit the amount of money they can hold in digital form, or to charge interest above a limit [1].

This is only one example where the ECB needs direct control over its currency. The ECB is directly responsible for maintaining the price stability of the euro, and any digital euro variant will have to be a part of that [45]. Because of this the centralised nature of the EuroToken gateways can act as the point of control for the ECB to enforce monetary policy, to stabilise the currency and provide direction for our economy.

6.4. Interoperability

The ECB has not yet decided on the reach they want their CBDC to have. One option is to open the system to the world. This has the benefit of increasing the reach of the euro and the success of the European economy. However, there is some risk associated with such tight coupling to other economies as the effect of monetary policy at home is reduced.

Using the gateway as an intermediary, EuroToken provides the option to integrate with other CBDCs in seceral ways. The first is by allowing transfers between the currencies without a counterparty. A gateway could run both EuroToken and DollarToken and transfer between them at an exchange rate that can be set by agreements between the two central banks. Effectively this allows for the coupling of currencies with an opt out at any time.

6.5. Universal asset storage and granular monetary policy

The digital and peer-to-peer nature of EuroToken provides the possibility of anonymous users, while the gateway centered design allows for integration of digital identity solutions. This allows for a hybrid system where different rules can apply to anonymous accounts. This would allow the ECB to encourage the adoption of the currency domestically, while discouraging usage abroad.

Additionally, the ECB can greatly increase the granularity of its monetary policy using differing types of EuroToken accounts. Each account can have different rules and regulations which are applied automatically. These become particularly interesting when considering that the current banking system can eventually be integrated.

Currently, banks store and reinvent the money of their customers with the promise that their money will return with some interest. This investment is an important mechanism that keeps the price of the currency stable. Even if economic instability encourages people to save their wealth, the amount of money in circulation remains mostly the same as all the money in the banks is re-invested into the economy on the other end.

As an alternative to the direct limitation on static EuroToken holdings with the ECB, the banking mechanism can be recreated in EuroToken. By creating different accounts at different levels of risk, users can store their money with similar security and features to the current banking system. On the other end, the user can specify other parties that are allowed to invest their money. These accounts can be limited in their spending to a certain frequency for less volatile banking.

One benefit is that the current system does not allow users to choose what their money is invested in. Within EuroToken, identity verification can be decoupled from banking and investing operations thus creating a system where users can quickly move their capital between banks.

Additionally to currency accounts, other assets like stocks, bonds and other assets can also be tracked on the blockchain. As time progresses financial players can provide banking or investment services directly to the customer using the same system as their banking.

This effectively unites the whole financial world into one accounting system. Especially when combinded with e-identity, e-signatures, e-invoices, e-receipts, and smart-contracts this could usher in a whole new wave of innovation.

7 Conclusion

Baring a natural disaster that wipes out the human race, the future of money will be digital. With commerce and banking moving online, a new modern payment system is required with features that fit the digital age.

The future of money will be digital because the features are needed, the question is: who gets to decide how these currencies are designed?

While there are many bidders to becomer the worlds next digital currency, the difficulty lies in creating a currency that is (1) scalable, (2) off-line transferable, and (3) stable.

These problems are difficult if not impossible to solve without some form of centralisation. Private parties like Tether and Diem are attempting to become this trusted third party. But if we don't want opaque corporations controlling our money supply we might have to centralise somewhere else. The European Central Bank is ideally positioned to provide the centralised control that is required to achieve the goals of money.

In order to create a currency that is scalable we use a block dag structure where every user has their own personal blockchain. This system is inherently distributed in its data storage and control. We then centralise the validation of transactions in gateways. These gateways validate the validity of the transactions and attest to their correctness and compliance with the rules of the network as well as regulations.

Another benefit is gained by maintaining the transaction history of each user on their own personal blockchain. By decoupling the transaction at the point of trade from the validation of the transaction we allow the transaction to happen off-line. This mechanism can then be expanded to a disaster proof currency that allows users to trade using digital money even without internet connectivity.

Price stability is ensured the same way as the psychical euro. By allowing the currency to be exchanged for traditionally banked euros, we effectively peg the price of the euro to that of EuroToken. This exchange can be fully regulated and controlled by the central bank, and the money that is exchanged belongs fully to the user, without any intermediary. Even the organisation that runs the gateway is only responsible for validating correctness and exchanging according to ECB rules. This effectively creates a new digital form of public money that is held by the individual and backed by the European Central Bank itself.

We implemented a proof of concept on top of the TrustChain blockchain. We created an mobile wallet that allows people to transfer the currency. We also created a gateway application that handles the transaction validation and exchange of the EuroToken.

We tested our system in two field trails to make show the viability of the system. Users were able to scan a QR code to send money using only their phone. We also tested the off-line transfer capacity of the PoC in the real world.

By running a simulation of multiple EuroToken wallets and gateways, we measured the way the network scales over time and see a linear increase in network capacity as the number of gateways increase. Additionally, we found our method of checkpointing allowed the transacting between users in constant time as the both the size of the network, and the size of the blockchain grows.

EuroToken is a CBDC design that is scalable, price stable and off-line transferable. It has to potential to become the technology that becomes the foundation of the financial infrastructure of Europe unifying the scattered payment and banking system of today.

Bibliography

[1] Interview with der spiegel. https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210209~af9c628e30.en.html. (Accessed on 06/13/2021).

[2] Delft café premieres with eemcs blockchain euro. https://www.delta.tudelft.nl/article/delft-cafe-premieres-eemcs-blockchain-euro. (Accessed on 04/19/2021).

[3] Empsa - european mobile payment systems association. https://empsa.org/. (Accessed on 04/28/2021).

[4] Stablecoin on eos blockchain | eosdt. https://eosdt.com/en. (Accessed on 04/30/2021).

[5] E-commerce statistics for individuals. https://ec.europa.eu/eurostat/statistics-explained/pdfscache/46776.pdf. (Accessed on 04/12/2021).

[6] Ethereum 2.0 (eth2) vision | ethereum.org. https://ethereum.org/en/eth2/vision/. (Accessed on 04/28/2021).

[7] Statistics | eurostat. https://ec.europa.eu/eurostat/databrowser/view/ext_lt_maineu/default/table?lang=en, . (Accessed on 04/12/2021).

[8] International trade in goods. https://ec.europa.eu/eurostat/statistics-explained/index.php/International_trade_in_goods#Strong_increase_in_trade_in_goods_with_China_in_2010-2020, . (Accessed on 04/12/2021).

[9] Tangle_white_paper_v1.4.2.pdf. https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf. (Accessed on 04/12/2021).

[10] The maker protocol white paper | feb 2020. https://makerdao.com/en/whitepaper/. (Accessed on 04/30/2021).

[11] Nano_whitepaper_en.pdf. https://content.nano.org/whitepaper/Nano_Whitepaper_en.pdf. (Accessed on 04/12/2021).

[12] Tribler/py-ipv8: Python implementation of the ipv8 layer. https://github.com/Tribler/py-ipv8/. (Accessed on 03/23/2021).

[13] Online wallet for money transfers & online payments | skrill. https://www.skrill.com/en/. (Accessed on 04/28/2021).

[14] Stasis: Digital assets for intelligent investors. https://stasis.net/. (Accessed on 04/30/2021).

[15] Tribler/trustchain-superapp: Kotlin implementation of trustchain and ipv8 with rich networking: multihoming of local bluetooth+4g, decentral social networking, udp hole punching, etc. https://github.com/Tribler/trustchain-superapp. (Accessed on 03/23/2021).

[16] Introducing usd coin. https://www.circle.com/blog/introducing-usd-coin. (Accessed on 04/30/2021).

[17] Requiem for a bright idea. https://www.forbes.com/forbes/1999/1101/6411390a.html?sh=4e0608c6715f. (Accessed on 04/12/2021).

[18] libp2p. https://libp2p.io/, . (Accessed on 04/26/2021).

[19] libtorrent. https://www.libtorrent.org/, . (Accessed on 04/26/2021).

[20] Directive 94/19/ec of the european parliament and of the council of 30 may 1994 on deposit-guarantee schemes. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31994L0019, May 1994. (Accessed on 06/07/2021).

[21] *Introduction to PayPal*, pages 1–12. Apress, Berkeley, CA, 2007. ISBN 978-1-4302-0353-7. doi: 10.1007/978-1-4302-0353-7_1. URL https://doi.org/10.1007/978-1-4302-0353-7_1.

[22] Tethers market cap. https://forkast.news/tether-usdt-reserves-stablecoin-bitfinex/, June 2021. (Accessed on 06/14/2021).

[23] Amelia Acker and Dhiraj Murthy. Venmo: Understanding mobile payments as social media. In *Proceedings of the 9th international conference on social media and society*, pages 5–12, 2018.

[24] ABN AMRO. Tikkie - bedrijven. https://www.tikkie.me/bedrijven. (Accessed on 04/27/2021).

[25] De Nederlandse Bank. Digital currency issued by central banks can protect public interests in payment systems. https://www.dnb.nl/en/actueel/dnb/dnbulletin-2020/digital-currency-issued-by-central-banks-can-protect-public-interests-in-payment-systems/, . (Accessed on 06/02/2021).

[26] Norges Bank. Central bank digital currencies. https://www.norges-bank.no/contentassets/166efadb3d73419c8c50f9471be26402/nbpapers-1-2018-centralbankdigitalcurrencies.pdf?v=05/18/2018121950&ft=.pdf&v=05/18/2018121950&ft=.pdf, . (Accessed on 06/02/2021).

[27] Morten Linnemann Bech and Rodney Garratt. Central bank cryptocurrencies. https://www.bis.org/publ/qtrpdf/r_qt1709f.htm. (Accessed on 06/02/2021).

[28] Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, and J. Christopher Westland. Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3): 602–613, 2011. ISSN 0167-9236. doi: 10.1016/j.dss.2010.08.008. URL https://www.sciencedirect.com/science/article/pii/S0167923610001326.

[29] R.W. Blokzijl. rwblokzijl/stablecoin-exchange. https://github.com/rwblokzijl/stablecoin-exchange. (Accessed on 03/23/2021).

[30] Stefan A Brands. An efficient off-line electronic cash system based on the representation problem, 1993.

[31] Jetse Brouwer. Consensus-less security, 2020. URL http://resolver.tudelft.nl/uuid:d3d56dd8-60ee-47f7-b23a-cdc6c2650e14.

[32] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2013.

[33] D. Chaum. David chaum on electronic commerce how much do you trust big brother? *IEEE Internet Computing*, 1(6):8–16, 1997. doi: 10.1109/MIC.1997.643931.

[34] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[35] David Chaum, Christian Grothoff, and Thomas Moser. How to issue a central bank digital currency, 2021.

[36] CoinDesk. Bitcoin transactions are more expensive than ever - coindesk. https://www.coindesk.com/bitcoin-transaction-fees-more-expensive-than-ever. (Accessed on 04/28/2021).

[37] Richard N. Cooper, Rudiger Dornbusch, and Robert E. Hall. The gold standard: Historical facts and future prospects. *Brookings Papers on Economic Activity*, 1982(1):1–56, 1982. ISSN 00072303, 15334465. URL http://www.jstor.org/stable/2534316.

[38] Swiss Federal Council. Central bank digital currency. https://www.newsd.admin.ch/newsd/message/attachments/59639.pdf. (Accessed on 06/02/2021).

[39] Glyn Davies. *A history of money: from ancient times to the present day*. Cardiff: University of Wales Press, London, 2002.

[40] Banque de France. Experiment on the use of central bank digital currency (cbdc). https://www.banque-france.fr/en/communique-de-presse/experiment-use-central-bank-digital-currency-cbdc. (Accessed on 06/02/2021).

[41] Martijn de Vos and Johan Pouwelse. Real-time money routing by trusting strangers with your funds. https://repository.tudelft.nl/islandora/object/uuid:c51ac99d-3013-44b3-8ddd-fbd951a2454a, 2018.

[42] Martijn de Vos, Can Umut Ileri, and Johan Pouwelse. Xchange: A blockchain-based mechanism for generic asset trading in resource-constrained environments, 2020.

[43] TU Delft. Tribler/kotlin-ipv8: P2p communication library for android. https://github.com/Tribler/kotlin-ipv8. (Accessed on 04/26/2021).

[44] Diem. White paper | diem association. https://www.diem.com/en-us/white-paper/, 04 2020. (Accessed on 03/19/2021).

[45] ECB European Central Bank. Report on a digital euro. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf, 10 2020. (Accessed on 03/19/2021).

[46] Forbes. Alibaba, tencent, five others to receive first chinese government cryptocurrency. https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/?sh=33d423fb1a51, 08 2019. (Accessed on 03/22/2021).

[47] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Dragos-Adrian Seredinschi, and Yann Vonlanthen. Scalable byzantine reliable broadcast (extended version). 2019. doi: 10.4230/LIPIcs.DISC.2019.22.

[48] Charles M. Kahn and William Roberds. Credit and identity theft. *Journal of Monetary Economics*, 55(2):251–264, 2008. ISSN 0304-3932. doi: 10.1016/j.jmoneco.2007.08.001. URL https://www.sciencedirect.com/science/article/pii/S0304393207001250.

[49] LibP2P. Peer identity :: libp2p documentation. https://docs.libp2p.io/concepts/peer-id/. (Accessed on 04/26/2021).

[50] Tether International Limited. Tether whitepaper. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf, 06 2016. (Accessed on 03/19/2021).

[51] Karl Menger. On the Origin of Money. *The Economic Journal*, 2(6):239–255, 06 1892. ISSN 0013-0133. doi: 10.2307/2956146. URL https://doi.org/10.2307/2956146.

[52] Michael Ehrmann Miguel Ampudia. Financial inclusion: what's it worth? https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1990.en.pdf, 01 2017. (Accessed on 03/23/2021).

[53] Simona Moagar-Poladian, George-Cornel Dumitrescu, and Ion Alexandru Tanase. Retail e-commerce (e-tail)-evolution, characteristics and perspectives in china, the usa and europe. *Global Economic Observer*, 5(1):167, 2017.

[54] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. URL http://www.bitcoin.org/bitcoin.pdf.

[55] Danmarks Nationalbank. Central bank digital currency in denmark? https://www.nationalbanken.dk/en/publications/Pages/2017/12/Central-bank-digital-currency-in-Denmark.aspx. (Accessed on 06/02/2021).

[56] Reserve Bank of Australia. Retail central bank digital currency: Design considerations, rationales and implications | bulletin – september quarter 2020 | rba. https://www.rba.gov.au/publications/bulletin/2020/sep/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.html. (Accessed on 06/02/2021).

[57] Bank of England. Central bank digital currency: opportunities, challenges and design | bank of england. https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper, . (Accessed on 06/02/2021).

[58] Bank of England. Discussion paper - central bank digital currency: Opportunities, challenges and design. https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593, . (Accessed on 06/02/2021).

[59] Central Bank of Iceland. Rafkróna? - central bank digital currency. https://www.cb.is/library/Skraarsafn---EN/Reports/Special_Publication_12.pdf, September 2018. (Accessed on 06/02/2021).

[60] Bank of Israel. Report of the team to examine the issue of central bank digital currencies. https://www.boi.org.il/en/NewsAndPublications/PressReleases/Documents/Digital%20currency.pdf. (Accessed on 06/02/2021).

[61] □□□□ Bank of Japan. Central bank digital currency. https://www.boj.or.jp/en/paym/digital/index.htm/. (Accessed on 06/02/2021).

[62] Bank of Russia. A digital ruble | bank of russia. http://cbr.ru/eng/analytics/d_ok/dig_ruble/. (Accessed on 06/02/2021).

[63] Reuters. China's $1.5 million digital currency giveaway impressed analysts. shoppers, not so much | reuters. https://www.reuters.com/article/china-currency-digital/chinas-1-5-mln-digital-currency-giveaway-impressed-analysts-shoppers-not-so-much-idUSL4N2H71NR?rpc=401&, 10 2020. (Accessed on 03/19/2021).

[64] Sveriges Riksbank. E-krona pilot phase 1. https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf, April 2021. (Accessed on 06/02/2021).

[65] Matouš Skála. Technology stack for decentralized mobile services | tu delft repositories. http://resolver.tudelft.nl/uuid:bd3a5fbd-430b-4af6-bc33-eab436f4f7db, 08 2020. (Accessed on 03/23/2021).

[66] The Maker Team. The maker protocol white paper | feb 2020. https://makerdao.com/en/whitepaper/, 02 2020. (Accessed on 03/19/2021).

[67] Fed The Federal Reserve. Preconditions for a general-purpose central bank digital currency. https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm, 02 2021. (Accessed on 03/19/2021).

[68] ECB Statistical Data Warehouse. Share of card payments in number of total payment transactions. https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.U2.F000.I1A.Z00Z.NP.X0.20.Z0Z.Z. (Accessed on 03/23/2021).