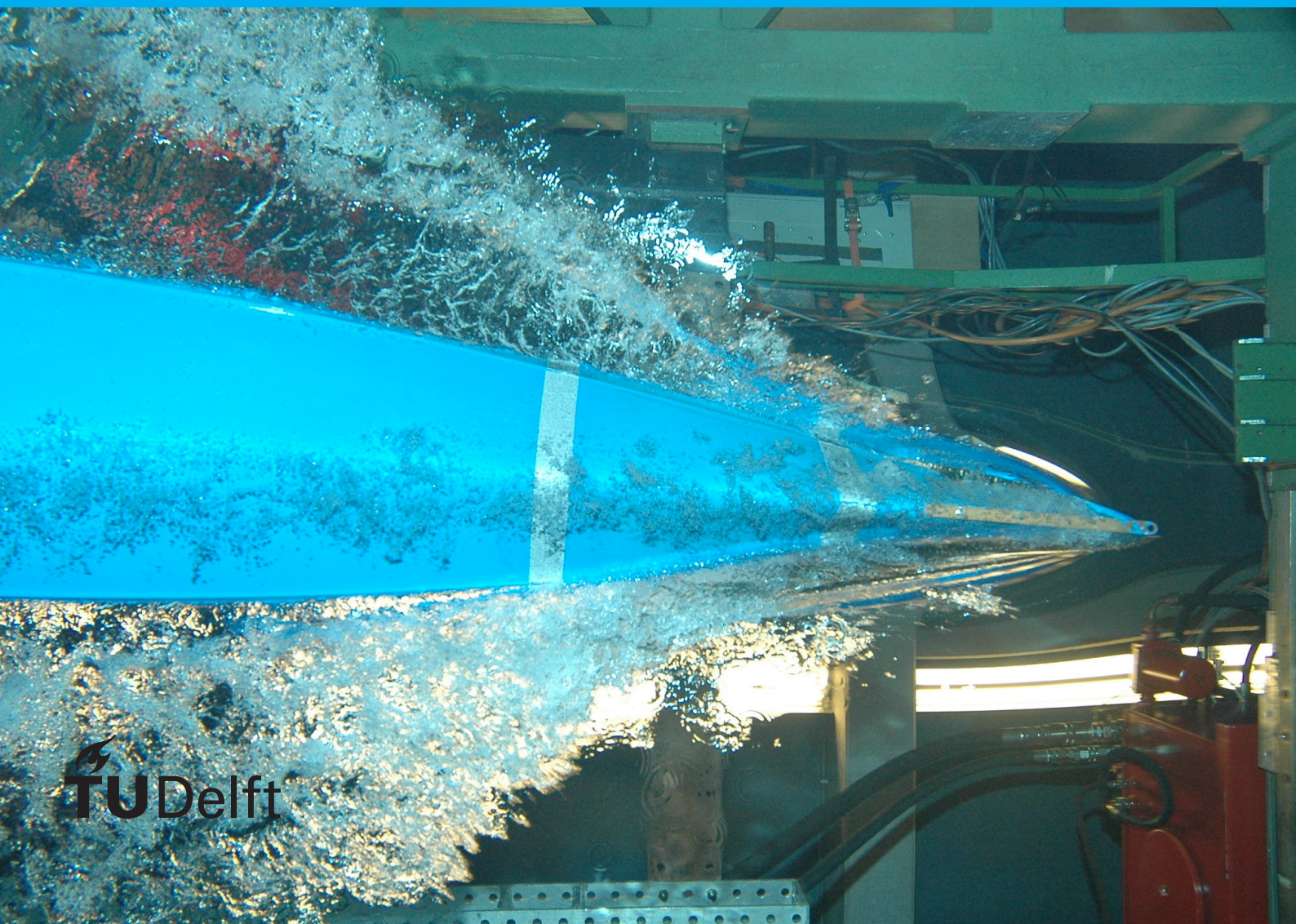
EuroToken
A Stable Digital Euro Based on TrustChain

R. W. Blokzijl

- Stablecoin
- Blockchain
- Cryptocurrencies
- TrustChain
- CBDC

R.W.Blokzijl@student.tudelft.nl



TU Delft

EuroToken

A Stable Digital Euro Based on TrustChain

by

R. W. Blokzijl

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

Student number:	4269519	
Project duration:	November 11, 2020 – TODO	
Thesis committee:	Dr.ir. J.A. Pouwelse,	TU Delft, supervisor
	Member 1,	TU Delft
	Member 2,	TU Delft

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

TU Delft

Preface

TODO: Add preface

R. W. Blokzijl
Delft, TODO

Contents

1 Introduction

Since the Bitcoin [TODO cite] white paper was published in 2008, the world has been speculating on how decentralized ledger technologies could be used to restructure the financial infrastructure of the world to redistribute power towards the masses and away from large opaque organisations. 9 years later, Facebook announced a private currency controlled by a group of corporations [TODO cite]. 3 years after that the Chinese government announced that they had reached 92,771 transactions per second with their new Central Bank Digital Currency (CBDC) [TODO cite]. And the Eurosystem is set to make a decision on whether to start a digital euro project in mid 2021.

The direction of crypto currencies is no longer determined by eccentric visionaries imagining a financial system that gave power back to the people and makes money open and programmable by anyone. Governments and large corporations are now competing to create the worlds main digital coin. The winner will be left controlling and overseeing all the worlds transactions, either for profit, or their national interests.

Currently very few decentralized currencies are in a position to challenge the upcoming central coins. The most well known crypto currencies, including Bitcoin and Ethereum, lack the price stability necessary to be a reliable store of value. There have been attempts to create fully decentralized stablecoins, but none have been proven to work in practice on a large scale just yet.

If fully decentralized currencies don't come up with a solution to scalability and stability soon. The future of the financial system might come down to a competition between the large governments of the world and the private sector.

Whether and how these parties succeed will have large implications for the future of financial markets of the world, and might determine the level of freedom of the societies of the future. Where China and Facebook are making rapid progress, the Eurozone is still deliberating while they might have a vital role in including the democratic process in the running of the future financial markets.

This thesis aims to provide a design for a digital euro that utilizes mechanisms used by todays stablecoin in order to create a digital euro analog called EuroToken. EuroToken is a design for a scalable system that allows transfer between parties in a scalable and peer to peer way, while maintaining price stability through maintaining collateral euros in a bank account.

We show how the EuroToken system can be used to create a scalable CBDC as well as serve as a private money alternative to current banks and provide all the benefits of programmable money with the price stability of the euro.

2

Problem description

```
Johan notes:

- specific e-Euro, not broad E-Money, e-Dollar in general
- Discuss the ECB plans in detail to start chapter!
- Retail (use existing banks) versus direct-consumer

Structure:
- ECB plans
    * CBDC
    * Deliberation for 2021
- Stablecoin trends
    * Bitcoin and Ether are unstable
    * Different solutions (include from lit survey)
        + Centralised Collatoralised (tether)
        + Centralised Controlled (Libra)
        + Decentralized Collatoralised (Makerdao)
        + Decentralized Algorithmic (nubits)
- The current day financial system
    * Payments via banks (require connection)
    * International settlemens slow
    * Private money by banks
        + 100.000 FDIC insurance
    * Public money by the Central bank
        + Cash only
- What we want from our financial system
    * Intuduce my solution
    * Requirements
        + Scalable
        + stable
        + Peer to peer
        + intagrateble with current system

Possible flows:
1. ECB CBDC plans --(why?)-> Current finsys bad --(possible solution types)->
   Stablecoin primer --(best solution for digiEuro)-> Requirements
2. Current finsys bad --(solution?)-> ECB plans --(how?)-> Stablecoins
   --(best solution for Euro)-> Requirements
3. Current finsys bad --(possible solutions)-> Stablecoins --(hybrid solution)->
   ECB CBDC plans --(how?)-> Requirements
```

- The current finsys is

  - digitalising and becoming more dependent on banks
  - paying more internatially but dated and slow
- ECB wants to modernise
- Cryptos can have inherent global guarantees
  - Possibly for public money
  - Needs to be properly designed

2.1. The state of the financial system

```
* Payments via banks (require connection)
* International settlemens slow
* Public money by the Central bank
    + Cash only

- Retail is growing toward digital payments
    * safer, faster, cheaper
    * online, bank dependent and controlled
- dependence on banks is dangerous
    * private money in bank failure, only 100 k guaranteed by government
    * bank outages lead to no access to basic necessities
    * compliance enforced by private parties with conflict of interest and
    profit incentive
    * displacement of the unbanked and vulnerable when use of cash declines
- international settlements take multiple days
```

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 [TODO cite]. While digital card payments are often more practical and safer than cash payments, the societal move towards digital money has some unintended side effects.

Digital card payments require an internet connection to succeed. While this is often available, it is not uncommon that a bank IT outage leads to payment capacities being unavailable, for a period of time.

When transfering money to an account with a different bank, especially across borders, the structure of the current system dictates a transfer time of days.

Money stored in a bank account is guaranteed by the bank. If the bank is to fail, the money in the account is usually insured up to 100.000 euro by various local government funds. When banks fail, the uninsured money is gone.

The move towards a bank dependent society will have the greatest impact on the worlds unbanked. In 2017, 3.6 percent of Europe's household had no registered bank account [TODO cite]. As more and more businesses become pin only. These people see their means of payment decrease.

Central bank money, or Cash, has already solved a lot of these issues. It's physical nature makes offline payment trivial. Transfer is instant, and the value of the money is guaranteed by the Central Bank itself, with the note or coin itself being proof of its validity.

However, due to its appeal to robbers and thieves, and its physical limitations, the risks associated with digital money are accepted by many as the cost of doing business. As a result we have two half-solutions to the problem of wealth storage and transfer.

2.2. European Central Bank plans for a Digital Euro

For the reasons stated above combined with the erosion of its control over its currency, the ECB is looking into the creation of a digital euro [TODO cite]. While it is still in

With the looming threat of the Chinese CBDC, the

- lack of a european way of addressing current market concerns opens up europe to foreign currencies to displace current local payment options -> strategic disadvantage

- What is a CBDC
  - a currency that has public money guarantees and stability, while having features and efficiency of digital money
  - Also needs to be available everywhere any time like physical money
  - privacy maintaining like physical money
- What does europe want
  - `satisfy the emerging payment needs of a modern economy by offering, alongside cash, a safe digital asset with advanced functionalities.`
  - Strategic autonomy
  - Protection of citicens (the unbanked and vulnerable) when use of cash declines
    - Requires open access
- What are Europe's requirements?
  - robustness
  - safety
  - efficiency
  - protection of privacy
  - complying with relevant legislation
    - on money laundering
    - on financing of terrorism.

2.3. The state of Distributed Ledger Technologies
2.4. Fitting stablecoin technologies to the Euro

2.5. random text:

Once crypto currencies had been adopted by a significant amount of people and started to be used for real transfers of value, the speculators came.

Cryptocurrencies like Bitcoin were rapidly growing in popularity and therefore price. The interest in a functional distributed currency, combined with the prospect of riding the rise of this new store of value, pulled in enough people to reach a market capitalization of 328 billion USD in late 2017. With the crypto bubble of December 2017 and subsequent crash in early 2018, the significance of these concepts had been demonstrated to the entire world.

The popularity of decentralized crypto currencies is undeniable, yet they have failed to be gain widespread adoption in everyday use. Many crypto currencies are plagued by a lack of scalability, a lack of price stability as well as other issues. While these problems may well be solve in the future, government organisations are looking into CBDCs now.

When the facebook connected Libra was introduced in 2017. Many big payment vendors like Visa and MasterCard were members of the Libra Association.

The Central

This sparked a debate on the shape of the future of money. In order

Completely decentralized crypto currencies like Bitcoin have always been plagued by the same issue.

or at least failed to die,

the future impact of would

impact that this new form of money would h

- Physical money is slow - restricted by the speed of travel
- Digital money is less slow - restricted by the speed of human communication
- New digital money - restricted by the speed of light (and the runtime of cryptographic algorithms)

2.6. problem description

The euro zone is missing an option for a digital currency that mirrors all features of the euro, while providing the benefits of distributed accounting and programmable money.

In the historic paper “On the Origin of Money” (**???**) Karl Menger describes how people settle on a currency as a method of exchange. He describes that the willingness of people to exchange their goods for a commodity depends upon:

1. The ability to trade the currency for goods and services
2. The scarcity of the commodity
3. The uniformity, divisibility, durability and practicality of the commodity.
4. The development of the market, and how others speculate.
5. The limitations imposed politically and socially upon exchange, consumption and transfer from one period of time to another

All these aspects must be managed in any successful currency. In this chapter we will work out these requirements into a concrete set of requirements for the EuroToken system.

2.7. The general requirements for money

Points 1 and 4, the future usefulness of the currency and it’s market demand, are where digital currencies still fall short of traditional currencies. Because of the price volatility there is no way to know whether the coin you have today can still be used to buy the same amount tomorrow.

Anything that aims to replace the euro needs to be as price stable as the euro. Adding guarantees about the price, will make merchants more willing to accept the currency, thus providing the ability to trade the currency for goods.

The EuroToken system needs to satisfy all 5 requirements in order to be a viable currency. However, points 2 and 5 are dependent on the real world implementation, legal guarantees and political backing. And are thus out of scope for this project.

Point 3 is where crypto-currencies add their value, through their digital and distributed natures.

2.8. Requirements for digital assets

The usefulness and viability of a currency is still dependent on its functional aspects. With traditional currencies the issues of uniformity, divisibility, durability and practicality have long been solved. However in digital currencies these aspects bring with them many sub-requirements. In “On the Origin of Money” (**???**) Menger uses the concepts of spacial and “time” limits.

Space limits - The space limits of a currency is how costly a currency is to store, transport, and manage across multiple ‘market places’. Because of the digital nature of crypto currencies, the price of storing any amount of money is the price of storing some data. However, the transport and transfer (practicality) of the currency is dependent on having access to the data and equipment needed to do the transfer. For many digital currencies an internet connection is also required to facilitate a transfer. Additionally any network required for verification needs to have the capacity to transfer the currency for a sufficiently low cost.

Time limits - For digital currencies the time limits of a currency brings with it more complexity than physical money. While A users guarantee that their money is durable and will not be lost becomes a problem of IT systems, backups and cyber-security. As such any protocol and edge implementations need to be secure / securable in order for the currency to be properly durable.

Finally there is one more requirement of money that needs to be maintained in a digital system. That is the uniformity of money, also known as the fungibility of money. This is the concept that any 2 individual units of the currency have to be essentially interchangeable. This means that there cannot be any difference in value or risk based on the source of money. When building on a trust based, by default, the risk attached to any money received is dependent on the trust you have in the sender of the money. As such there needs to be a mechanism that reduces the transaction risk to a negligible level.

2.9. Political requirements for a future of money

The adoption of any new currency system across the euro zone will be dependent on many more factors than just the technical design. Even if the EuroToken system meets all the requirements specified in the last chapters, trust in the system will depend on “The limitations imposed politically and socially upon exchange”.

It is impossible, however tempting, to make any statements about how the system should handle a number of political issues. Instead a some trade-offs will be highlighted and discussed. Any value judgements will be reserved and left out of scope. The political considerations for any real world implementation of the EuroToken system, might include, but are not limited to:

1. the openness of its access vs the prevention of malicious activity
2. the privacy of its users vs the ability of the state to track malicious behaviour
3. the economic tools provided to the central bank vs the natural price development of the market

In the following sections each of these trade-offs will be discussed while specifying some requirements for different positions on the trade-off spectrum.

2.9.1. Openness vs Control

- The openness of its access vs the prevention of malicious activity

Case for openness
Case for control
Requirements:
Openness - No central servers for the core functioning of the network. (transfer without saction)
Control - Central rules that determine the validity of funds based on the source of the transaction. (identity should be verifiable)

2.9.2. Privacy vs Policability

- The privacy of the users vs the ability of the state to track malicious behaviour

Case for privacy
Case for security
Requirements:
Privacy - Future support for encrypting transactions while allowing for ZK-proofs for verifying availability of funds.
Policability - the ability to see information about a transaction regardless of the encryption
Finding a balance in this is not a trivial task.

2.9.3. Central control vs self regulation

- The economic tools provided to the central bank vs the natural price development of the market

Case for central control based on current politics.
Case for free market, new democratic backbone.
Central control - Allow the minting of new coins by the central bank, akin to QE
Self regulation - Build in features that guarantee market invariants, like a set inflation based on trackers. Or minting as a joint decision of many parties, possibly DAO style. Possibly a democratic system in the system, based on identity, separate from nation politics. Possibly deferring voting to financial institutions.

2.10. Summary

Deriving from the fundamental requirements of money the following requirements for the EuroToken system have been determined:
The system must:

- Allow the user to transfer funds to other users
- Allow the user to store funds for a period of time

- Have a mechanism to maintain the value of 1 token at 1 euro
- Maintain the uniformity/fungibility of the token
- Be theoretically scalable to billions of users
- Be completely digital and automated
- Be secure against double-spend attacks

The system should be expandable to allow:

- An integrated identity mechanism that verifies users and makes them accountable
- Mechanisms to hide the details of any transaction
- Mechanisms to bind network properties and rules to a democratic mechanism

System invariants:

- The market equivalence invariant - The amount of euro + EuroToken on the market must never be changed because of a system transaction. (the EuroToken shouldn’t change euro supply)

3

State of the art

Digital currencies

3.1. Money, its requirements and benefits

3.2. problems with money and how digital money solves them

3.3. Problems with digital money and how Bitcoin solved them

- mention ripple and why they aren't widely adopted yet

3.4. Problems with Bitcoin and how TrustChain is an alternative

3.5. Stablecoins

- Intro: Leftover discrepancies between traditional and digital money (stability)
- What is a stablecoin
- What makes a digital currency unstable, real question: what makes a normal currency stable
- What is a peg
- Other stablecoins in the wild
- Vision of the future of the euro zone

3.6. Terms used in this report

- Token
- Gateway
- Wallet
- CBDC - Central Bank Digital Currency

4

Design

4.1. Global Design considerations

```
TODO: Remove

1. general ideas on keeping the currency stable
    a. Solve with Pegging ->
    b. Solve with Collatoral ->
    c. Solve with central bank ->
    d. Move to allowing central bank debt tracking
2. Global system architecture
    a. Money ingress and egress
        i. Trusted Gateway(s) to mint and burn coins.
            - Holding collateral
    b. Money transfer using trustchain
        i. Double spend protections
            - Checkpointing
3. On scalability
    a. Multiple gateways (Central Bank)
    b. A seperate set of trusted transaction validator nodes (Local banks)
4. Trustchain
    a. message types:
        i. Transfer
        ii. Creation
        iii. Destruction
        iv.  Checkpoint
    b. User software
    c. Bank software
5. Scientific novelty
    a. Move the perspective from stablecoin to europe's renewed infrastructure
    b. Other coins that aim to do this: ripple
    c. Our added value (to the current system and other solutions)
        - Users get
            * programmable money
            * Auditability by open source software
        - Banks get
            * One standard for banking ledgers
            * Added benefit of not losing central monetary policy handle.
            * Smooth long term migration to the new system with failsafe

  TODO: Intro
```

4.1.1. Pegging to the euro (Design level 1)

As we have explored in chapter TODO, there are a few ways of stabilising a currency. Since the EuroToken system needs to function as a replacement of the current financial infrastructure and has to be stable with regard to the euro, we have chosen a direct peg to the euro. This requires a mechanism that allows any holder of the euro to exchange it for an equal amount of EuroTokens at all time.

Because of the system invariant to not change the total supply of euro + EuroToken, every addition of a EuroToken to the system should result in the removal of a euro, and vice versa. Since we cannot create and destroy euros at will, a collateral system will be used to ensure absolute availability of euros and EuroTokens at any time to facilitate both directions of exchange.

The collateral system will work as follows: A holder of euro will trade their euro for a EuroToken with a central bank certified gateway. The gateway will store the euro in a bank account, effectively removing it from the market. These gateways have the sole power of EuroToken minting and the only situation where EuroTokens will be minted is when a euro is provided as collateral.

Firstly, this maintains the market equivalence invariant as EuroTokens only enter the market when a euro is removed. And secondly the collateral equivalence invariant, that the amount of euro held in collateral is always equal to the amount of EuroToken on the market.

Because of this guarantee, the other direction of trade is always possible as well. When a EuroToken holder wants to exchange their token for a euro, it can always do so with a gateway. The gateway will remove the EuroToken from circulation while adding a euro back to the market. Thus again maintaining the market equivalence invariant as well as the collateral equivalence invariant.

4.1.2. The blockchain

The EuroToken system can be build with any ledger technology, but the choice of this technology is fundamental to the well functioning of the system as a whole. For the EuroToken system, the following requirements for the systems should be considered.

First, any EuroToken ledger technology **must** scale to the size of the Euro zone, it must allow for rapid micro-transactions to take place, while maintaining a negligible transaction cost. Any centrally managed database would practically be a centralised rebuild of the current banking system, which beside being incredibly expensive, would introduce a centralised point of failure towards which malicious behaviour like denials of service attacks and fraud would be directed. This is where a distributed ledger technology has its added value. By having standard day to day transactions happen between users directly, the cost of any transaction between any parties is the cost of the communication between these parties. For this project we therefore choose to user a distributed ledger technology. The issue of the security of funds in the ledger is now the responsibility of the owner of these funds, while only leaving the security of the nodes responsible for the minting and burning of EuroToken to the parties that manage the system.

Second, transactions **must** be final, therefore users **must** have a indisputable, dependable and therefore immutable record of their income and transactions. When storing data in a distributed way, the task of keeping data immutable is partly solved by using a blockchain data structure that guarantees the immutability of all transactions before any given block in the chain.

Even with a blockchain however, finality is still dependent on the availability of any users last transaction. Some currencies use a single distributed blockchain that is maintained by all participants in the network to store this information. However, using a solution that requires constantly updating global state makes maintaining a sufficiently high transaction throughput a significant challenge[TODO, onderbouw en citeer]. Though there are efforts to increase the throughput of global data networks [TODO, cite eth 2.0], in this project we will use a blockchain that scales first and attempt to solve transaction finality is alternative, less general, but viable ways.

4.1.3. TrustChain

For the reasons stated above, we choose to use TrustChain as the backend blockchain for the EuroToken project. TrustChain is a hyper sharded blockchain where every peer maintains their own blockchain. All blocks that involve a counterparty have a link to that chain. This mechanism entangles the chain of any user with the chains of everyone they interact with.

[Explanation of TrustChain with pictures].

- Transfer using any application

- Transfer scales infinitely
- Transfers Require verification by trusted node

4.1.4. Double spending prevention, accountability and identity

TrustChain gives us the scalability needed for a eurozone wide currency. However, because of the lack of a global component a double spending attack would be possible.

The blockchain guarantees us that given a signed block with a hash, all blocks before it are immutable without invalidating the chain of hashes. This allows any user to inspect and verify the full history of any other user. However it does require the inspecting user to have the last block of the counterparty.

A malicious user can simply withhold information about their last transactions to make it seems like funds that have recently been spent are still available. As illustrated in Figure [TODO], this means the attacker creates a fork in their chain, and shows a different history to different users.

[Picture of double spend fork].

While there have been promising developments in TrustChain to prevent forks [TODO CITE bami], these are relatively recent and are not ready in time for this project.

If we look at the implications of the double spend attack, we see a mechanism that is very similar to “double-entry bookkeeping” the current banking world. However with additional benefit of having indisputable signatures of both parties on any transaction. This means that any fork can be detected by anyone simply having both blocks in the fork, that are both signed by the attacker.

If an identity system is integrated into the EuroToken system, where any user is identifiable and thus accountable, double spend could be considered fraud under the legal system, and be prosecuted by the authorities or victimised parties. In this case, simply having both blocks of a fork would be sufficient proof.

However we would like to **prevent** double spending. While we cannot prevent any users from making a fork in their chain, we can have a mechanism that decides what fork is considered valid, and what forks should be discarded. In addition to this, a mechanism is needed to allow any user to discover whether a fork already exists for the block they just received.

As with detection, a decision can only be made in a place where both sides of any for would show up. This requires all blocks of a user to end up in the same place eventually. While bami aims to do this dynamically by connecting all interested parties for every peer [TODO cite bami]. Another way is to have specially selected trusted parties to gather and verify all blocks for a user.

4.1.5. Validators

`maybe move this to somewhere else`

While having trusted parties is one of the things many popular crypto currencies are trying to avoid, the benefit of having a system of validator nodes can be a great benefit to the overall system.

The current eurozone banking system has been using a similar system for a long time. Where banks are responsible for the day to day running of money transfers, while they’re regulated and overseen by government entities such as the ECB.

Beside having these institutions prevent forks, they can also serve other roles like large transaction validation, tax accounting, prevention and detection of fund transfers for criminal and terrorism purposes. If they are a bank in the current system they could even be allowed to hold and exchange between euros and EuroTokens, or leveraged lending to customers.

In a system like this, EuroToken would allow a slow transition to a standardised accounting standard by allowing the current euro system to coexist while building a new monetary system for the whole eurozone. Banks will be incentivized to participate because it allows them to provide faster, cheaper and better service to their customers.

4.1.6. Ledger checkpointing

We can prevent most double spending by simply gathering the blocks of any user in a simple location. When a transaction is accepted by a validator, the transaction can be considered “verified”. We call this “checkpointing”. If another transaction then arrives to the validator, it will be rejected and never verified. This means that forks will be selected on a first come first serve basis.

Since a transaction can only be considered verified, every user that receives money is incentivized to send the transaction to the validator that is responsible for that user.

4.1.7. Determining validators

A peer has to know where to checkpoint messages transactions for a transaction with a given user, in fact all peers that interact with that user need to be able to find the validator responsible at any time.

To achieve this, a user maintains their current validator as a block on their chain. When the user wants to change validators, they will register another block, that specifies the next validator. This block will be signed by the new validator and be sent to the old validator as well. Anyone interacting with the user at this point will see the change in the chain an contact the new validator instead. If the block is not provided with the next peer, the old validator will be contacted, who will not accept the transaction as it is would be a fork [TODO image].

4.1.8. Validators in a CBDC

A system of private validators makes the money that is managed private. This means that the money a user has validated by them derives its value from the reputation of the validator [TODO, cite public vs private]. Because of this, a system that requires private validators is unfit to be a CBDC. Any central bank money, should derive its value from the reputation of the central bank, and no private entity should be involed. However, this is a feature of the backend of the system. If the Central Bank is the only entity able to mint new EuroTokens, and double spending is prevented by a decentralized mechanism, the stablecoin mechanism can still be used to introduce a CBDC that matches its value to the euro. This would still allow private parties to exchange the currency, just not guarantee its value.

A viable backend for a CBDC could be TrustChain with its new Bami extension [TODO cite].

4.1.9. Global design summary and conclusion

[TODO].

4.2. Protocol design

[TODO intro].

```
Structure:

1. Needed events and how they create a working system
    a. Creation
        i. Created ET
        ii. Stores Euro
        iii. has to be validated by gateway
        iv.  Peer to gateway interaction
    b. Destruction
        i. Destruction of ET
        ii. Sends euro to payee
        iii. Is performed only by gateway
        iv.  Peer to gateway interaction
    c. Checkpoint
        i. Validates transactions
        ii. Perfomed by the gateway
        iii. Temporary solution to solve double spending and transaction finality
        iv.  Peer to gateway interaction
    d. Transfer
        i. Basic command to send money
        ii. Peer to peer interaction
        iii. Balance not yet validated
2. Creation Step by step
3. Destruction
4. Checkpoint
```

```
5. Transfer
6. Demo specific choices (maybe this should go in implementation)
    a. TrustChain without bami
    b. A single gateway
    c. that acts as validator also
```

4.2.1. System events
In order to realise the

4.2.2. Demo specific choices
What will this thesis implement

1. Single central bank
2. Central bank is also validator
3. Expansion on preexisting TrustChain super app to add EuroToken user capacities.

4.2.3. The gateway - enabling the peg
In order to

- acts as a link between 2 assets
  - Could be expanded
- Is central bank certified
- Scalability might require backend communication
- Management of euros on backend is up to the central bank.
  - Individual banks might not have enough collateral for all trades.
  - What happens on bank failure
    - Exit scamming

4.2.4. TrustChain message and interaction types
1. Transfer
2. Creation
3. Destruction
4. Checkpoint

4.3. Extra System considerations
4.3.1. Security
4.3.2. Scalability
4.3.3. Usability
4.3.4. Auditability
4.4. Scientific novelty

5 Implementation

The implementation of the stablecoin system consists of 2 main elements: the wallet Android app, and the gateway REST API. A web front end for the rest API has also been created.

The wallet demonstrates the ability of TrustChain to handle the transfer of the EuroTokens peer to peer without a central entity.

The Gateway demonstrates how a bridge can be created between the traditional euro system and a blockchain based analog.

5.1. Gateway (Central Bank API)

The only way tokens are created is when a central bank creates them. In our implementation this only happens when a user has transfered an equal amount of euro into the central bank account.

The gateway is responsible for the exchange of euro for tokens and vice versa. This involves taking payments in both tokens and euros, and payments in both currencies. This means the gateway needs to interface with the bank to allow a user to make payments in euro when creating EuroTokens, as well as a mechanism for paying out euro to the user when they trade in EuroTokens. On the other side of the gate the system needs to be able to create/send, and destroy/receive tokens on TrustChain.

The gateway aims to automate and link all of this interaction, so EuroTokens can be bought and sold at any time by anyone.

5.1.1. EuroToken Creation

When a user wants to convert a euro to a EuroToken, a creation event is initiated with the gateway API. The user sends their TrustChain wallet address and amount to convert with the request.

The API will then create a payment request with the associated bank for the specified amount, and store the information in its database. The payment link is returned to the user.

When the user has paid the request, a transaction for the EuroTokens will be created using TrustChain. The gateway will create a proposal half-block which will be sent to the user, who will create an accepting half-block registering the transaction on both chains.

The user is now free to send the EuroTokens to anyone they like, requiring only a TrustChain transaction.

5.1.2. EuroToken Destruction

When a user wants to trade in a EuroToken for a euro the process happens in reverse. For the demo the user does a request to the API with the desired amount, their TrustChain address and an IBAN.

The system creates a TrustChain transaction for negative the amount. This transaction is sent for the user to accept.

When the user has then signed the accepting half-block. The system will pay out the amount to the specified IBAN.

5.1.3. Frontend

To aid everyday users in the purchase and sale of EuroTokens a web frontend is created where the user can interact with the API. It demonstrates the ease of use of the system.

[Screenshots]

5.1.4. Implementation considerations

The design specified a general architecture for the EuroToken system. However in order to make an implementation possible within the constraints of the project some implementation trade-offs have been made.

Bank support

The EuroToken is designed to work with any bank account for euro collateral. However in this implementation we only implemented the API for ABN AMRO. Adding other banks is a simple as implementing the `Bank` class.

Euro Payment Initiation

The design specifies a requirement of automatic euro payout on EuroToken destruction. In order to automate this, most banks (including ABN) requires registration and use of the PSD2 payment initiation API. This API requires a Payment Initiation Service Provider (PISP) licence, which in turn requires a banking licence. Since both of these licences require you to be a fully functioning bank, the payment initiation part of the ABN API has not been implemented and is done manually in the field trial.

TrustChain

Since the main implementation if the TrustChain software (Tribler, n.d.) is build on python so is the gateway API. The server is provided as a single docker container that also provides the frontend.

5.2. Android Wallet

In order to use the EuroToken system on a daily basis, users need a way to send and receive the token. Because the added value of the system is its distributed nature, a way to send and receive the asset in a convenient and peer to peer way is needed. The TrustChain team has recently come out with an Android super-app[TODO, cite] that showcases some of the IPv8 (Tribler, n.d.) and TrustChain[TODO CITE] capabilities. This app provides the perfect platform to showcase the EuroToken capabilities.

5.2.1. PeerChat Extension

The super-app already includes a number of applications, including PeerChat. A chat application that uses IPv8s peer to peer capabilities to communicate. In order to show that the EuroToken can be used in a modern context, the PeerChat app has been expanded to include the capacity to send money attached to a message.

To send money, the user simply selects the option to send money, and is taken to a screen where a transaction can be created. The message is then sent to the receiver who within a few moments sees the transaction appear as a message in their shared chat. The transaction amount is also added to their balance.

The capacity to send transactions as shown in Figure 5.1 is not tied to PeerChat messaging. When money is sent, a transaction is created and transferred to the receiver using the TrustChain main community. The transaction hash is then sent as part of the PeerChat message. The receiver then fetches the transaction it received earlier via TrustChain.

- [TODO diagram of TrustChain and PeerChat interaction]

This implementation demonstrates the simple way in which EuroToken allows monetary transactions to be seamlessly and programmatically inserted into any application.

5.2.2. EuroToken app

The PeerChat app is one specific use case. In reality different applications would simultaneously use the EuroToken system. This would leave the user with a splintered record of their financial life.

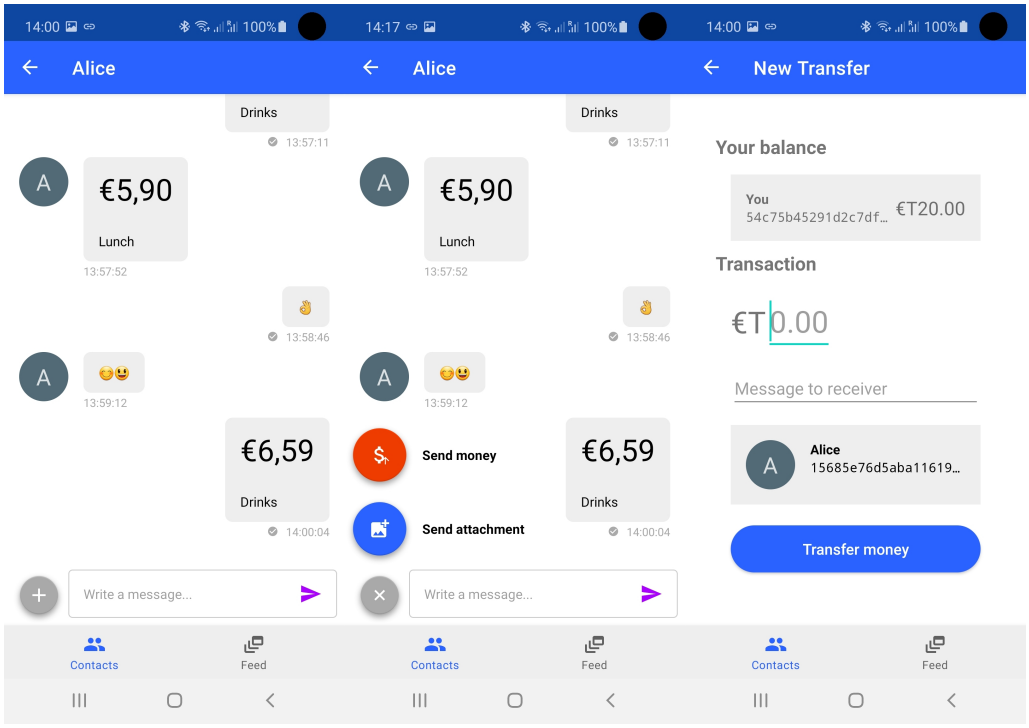


Figure 5.1: Attach money in PeerChat

In order to solve this, a EuroToken accounting app has been added to the super-app. The purpose of this is to show that the systems data can be reorganized in whatever way. The EuroToken app shows a history of all transactions, and provides another interface to the gateway.

5.2.3. EuroToken transactions in depth

- Validation (TODO)
  - Creation/destruction:
    - Trust Central Bank only
  - Transactions (prevent double spend)
    - Trusted users (based on identity later)
    - Validated by bank
    - Bami double-spend protection

5.2.4. EuroToken Settings

In addition to providing convenient services to the user, the EuroToken app has some configuration options to give the user control over their role in the EuroToken network.

Trusted Minters - Since the network has a central component that regulates the creation and destruction of the tokens, a demo requires a running server. Since there is no party to maintain such a server indefinitely right now, an option is added to allow the user to specify public keys of trusted "central banks". If this option is enabled, the wallet in the super-app does only accepts blocks signed by the configured public keys.

- [TODO: image of minter config]

Trusted validators - Validation of transactions and prevention of double spending is unsolved in TrustChain but is an important part of any currency. Solving this problem in general is being worked on [TODO CITE bami] and is out of scope for this project. However the issue of transaction finality being important to a EuroToken system, a way to prevent double spending has been added. A transaction is not considered final until a trusted entity has signed a block in the senders chain that comes after

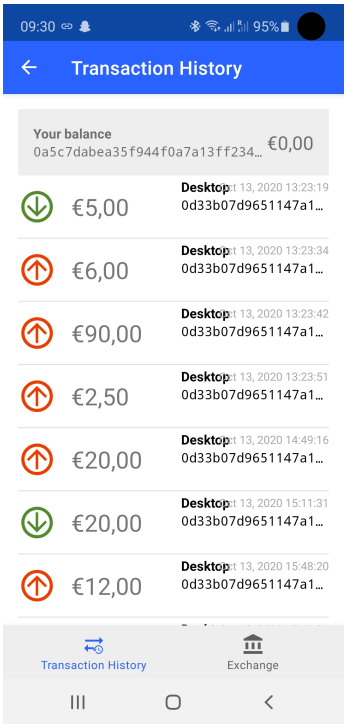


Figure 5.2: EuroToken Transaction History

the send block. This means that the trusted entity is responsible for the validation of the block and its dependencies. These validators can be configured in the app in order to make de demo repeatable.

- [TODO: image of validator config]

6

Field trial

7 Discussion

7.1. System dangers

7.1.1. Under-collateralization

Causes:

- By central bank printing without collateral
- Licenced gateway banks going bust, taking collateral with them

Effects:

Future bank runs could leave some token holders without their collateral, this makes token holders less confident in tokens. This would lower their value, but the direct exchange peg maintains the price. This hides the problem while undermining trust in the value of the tokens.

Solution:

- Don’t print without collateral.
- Short term:
  - Keep collateral liquid at all times (also stops inflation)
- long term:
  - see system future

7.2. System future

- euros are deleted by banks on euro2token exchange, and created on token2euro exchange.
- Banks don’t manange the collateral, only the CBDC exchange.
- Banks get a place in trust instead of investment.

8

Conclusion

Related Work

Tribler. n.d. “Tribler/Py-Ipv8: Python Implementation of the Ipv8 Layer.” Accessed: June 13, 2020. https://github.com/Tribler/py-ipv8.

Bibliography

[1] Tribler. Tribler/py-ipv8: Python implementation of the ipv8 layer. Accessed: June 13, 2020. URL https://github.com/Tribler/py-ipv8.