HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

# BACHELOR THESIS

Mr.
**Felix Hildebrandt**

## Tokenization and the Symbiosis between Blockchains

Mittweida, 2020

Faculty of Applied Computer
Sciences & Biosciences

# BACHELOR THESIS

# Tokenization and the Symbiosis between Blockchains

author:
**Mr. Felix Hildebrandt**

course of studies:
**Applied Computer Sciences of Application Development**

seminar group:
**IF17wS-B**

first examiner:
**Prof. Dr. – Ing. Andreas Ittner**

second examiner:
**M. Sc. Steffen Kux (Blockchains LLC)**

submission:
**Mittweida, 24.11.2020**

evaluation:
**Mittweida, 2020**

## Bibliographic Description:

Hildebrandt, Felix:
Tokenization and the Symbiosis between Blockchains. - 2020. – VII, 44, II p.

Mittweida, University of Applied Sciences, Faculty of Applied Computer
Sciences & Biosciences, bachelor thesis, 2020

## Abstract:

Tokenization projects are currently very present when it comes to new blockchain technologies. After explaining the fundamentals of cross-chain interaction, the bachelor thesis will focus on tokenizing technology for Bitcoin on Ethereum. To get a more practical context, implementing the currently most successful decentralized tokenization project is described.

**This bachelor thesis was supervised by Blockchains LLC**

BLOCKCHAINS

# Contents

**List of Figures** .......... **III**

**List of Tables** .......... **IV**

**List of Abbreviations** .......... **V**

**1 Introduction** .......... **1**

**2 Fundamentals** .......... **2**

*2.1 Blockchain Technology* .......... *2*
2.1.1 Bitcoin .......... 3
2.1.2 Ethereum .......... 3

*2.2 Second Layer Technologies* .......... *4*

*2.3 Decentralized Identity* .......... *7*

**3 Token Economy** .......... **9**

*3.1 Technical Specifications* .......... *9*

*3.2 Differentiation of Tokens* .......... *10*

*3.3 Stable Coins in Detail* .......... *11*

**4 Cross-Chain Interaction** .......... **12**

*4.1 Superordinate Cross Chain Solutions* .......... *12*

*4.2 Atomic Swaps* .......... *14*

*4.3 Tokenizing Technology* .......... *16*
4.3.1 Different Lightweight Approaches .......... 17
4.3.2 Aspects of Tokenization .......... 18
4.3.3 Models of Implementation .......... 18

**5 Tokenized Bitcoin on Ethereum** .......... **19**

*5.1 Improvements* .......... *19*

*5.2 Market Analysis* .......... *20*

*5.3 Tokenizing Projects* .......... *21*
5.3.1 Kyber, BitGo: WBTC .......... 21
5.3.2 TokenIon: imBTC .......... 22

5.3.3 Provable: pBTC ........................................................................................23
5.3.4 Synthetix: SBTC & IBTC....................................................................................24
5.3.5 Huobi: HBTC........................................................................................25
5.3.6 Keep Network: TBTC........................................................................................25
5.3.7 Ren Project: renBTC........................................................................................27

*5.4 Comparison of Current Approaches ................................................................29*
5.4.1 Trust Analysis ........................................................................................31
5.4.2 Scalability Analysis ........................................................................................33
5.4.3 Decentralized Tokenization ................................................................................34
5.4.4 Evaluation ........................................................................................36

**6 Demonstration ........................................................................................37**

*6.1 State of Mobile Development........................................................................38*

*6.2 Implementing Ren Project ................................................................................40*

*6.3 Solidity Contract........................................................................................41*

*6.4 React Wallet ........................................................................................41*

*6.5 Future Development ........................................................................................43*

**7 Conclusion ........................................................................................44**

**References........................................................................................45**

**Appendix........................................................................................52**

**Appendix, Part 1........................................................................................I**

**Appendix, Part 2........................................................................................III**

**Declaration of Independence ........................................................................5**

# List of Figures

Figure 1: Growth of locked BTC on Ethereum 2020 .......................................................20

Figure 2: Distribution of locked BTC on Ethereum 2020..................................................21

Figure 3: Mobile Asset Management Application - Layout................................................38

Figure 4: Browser Wallet Extension – Layout ...................................................................40

Figure 5: Wallet Showcase - Regular View.......................................................................41

Figure 6: Wallet Showcase - Advanced View ...................................................................42

# List of Tables

Table 1: Pros and Cons of regular Sidechains ....................................................................5

Table 2: Pros and Cons of regular State Channels .............................................................6

Table 3: Technical Token Specification ..................................................................................9

Table 4: Different Kinds of Tokens.........................................................................................10

Table 5: Categories of Cross-Chain Solutions.......................................................................12

Table 6: Brief Overview of Tokenization Projects ..............................................................30

Table 7: Rating of Tokenization Projects for Software Solutions.......................................30

Table 8: Comparing of Tokenization Projects on Trust......................................................32

Table 9: Comparing of Tokenization Projects on Scalability..............................................33

# List of Abbreviations

| | |
|---|---|
| **AML** | Anti-Money Laundering |
| **API** | Application Programming Interface |
| **DAO** | Decentralized Autonomous Organisation |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **IT** | Information Technology |
| **KYC** | Know Your Customer |
| **PoS** | Proof of Stake Consensus |

# 1 Introduction

Blockchains usually act like isolated ecosystems from each other. Mainly due to their backend infrastructure operating on their networks. But within the last years, many projects published their ideas to build bridges between blockchains. Using secondary structures, which can dock onto a specific blockchain to increase usability or offer new features, cross-chain technologies rose to provide more significant interaction for blockchains themselves. As a result, both concepts can go hand-in-hand to provide applications that take loads from main networks and offer blockchain-wide asset management. This base concept of technologies becomes even more relevant with decentralized identity. Properties of personal data will then need to be linked into subnetworks across blockchains.

Those three trends are mirrored in the Hype Cycle for Blockchain Technology 2020, released by the world’s leading research and advisory company Gartner. Secondary networks or so-called “Layer 2 Solutions”, “Tokenization” as one cross-chain concept, as well as “Decentralized Identity” are at the peak of hype at the time of writing. [1]

The financial world of blockchains is mostly covered by Bitcoin, taking up about 293 billion dollars in market cap at hand. [2] Despite the considerable security and independence the technology offers to the users, it is not easy to adapt to upcoming applications due to the regulated infrastructure. For small-scale transactions, everyday use applications, or access to various crypto technologies and projects, Bitcoin is relatively limited in future development. Most new applications cover currencies from more development-driven blockchains like Ethereum, for instance, which also take the lead in secondary network development. Both ecosystems could profit from each other if the considerable market value could be combined with new emerging use cases for the currently dominating crypto asset.

This thesis will break down blockchain technology fundamentals, token economy, and cross-chain concepts. They lead to the main topic about how current projects can safely use Bitcoin on the Ethereum blockchain. One of such projects will be showcased within a wallet prototype to get a more practical perspective.

# 2 Fundamentals

Within the first chapter, the essential underlying technologies are explained to understand blockchain concepts. It will also be described how such ideas could further revolutionize the internet and expand out of the current most common use case as a digital currency. The bigger picture related to such approaches will lead to second layer technology and decentralized digital identity.

## 2.1 Blockchain Technology

The fundamental groundwork of all described software systems is the blockchain technology itself. Therefore, an introduction is necessary to understand the full meaning of blockchain and why new technologies, which enlarge those mechanisms, are needed.

A blockchain can be viewed as an expanding list of records, which are called blocks. Those are linked and verified using cryptographic hash methods. The linking between blocks is achieved by referring to the previous block's hash while creating the next one. It cannot be altered afterward without changing all following blocks, which requires the consensus of the network majority a blockchain is used in or tremendous computing power. Within blocks, the data stored is accounted for within Merkle Trees to verify them from hashes easily. [3]

Because of those facts, a blockchain is nearly resistant to modification and also denies the possibility of duplicating transactions based on the network's consensus. Therefore, blockchains are often called secure by design and used in software fields in which no intermediary can be trusted.

In more detail, a blockchain is commonly used to record transactions or events between two parties as a distributed ledger. For the use of such a distributed ledger, the blockchain is often managed by a network of servers, so-called nodes, which are following a specific consensus protocol to communicate and validate new blocks. This is done by using a peer-to-peer network concept to prevent central instances and create a resilient environment. Such networks can either be public within the internet or private for use within someone's business. [3, 4.1]

Blockchain solutions are often bound to the economy's financial market. Those are backed by substantial financial resources and the upcoming demand of having full control over their assets while not being tied to trust a central instance or banks. That is why blockchains are often seen as payment rails because most of them are related to their currency. However, it is still quite complicated for dedicated trading and the financial market to exchange assets from multiple blockchains without falling back to central instances. [4.1, 5]

### 2.1.1 Bitcoin

Bitcoin was the first application realized based on blockchain technology in 2009. Its concept was to create an open-source, peer-to-peer technology to transfer digital money between participants. One of the key features is the static cap of the final amount of funds available, which denies stocking up cash afterward. Decentralized servers, so-called nodes, get rewarded by solving cryptographic hash puzzles to generate blocks. Those nodes can also spread and verify other blocks from the network. On the user side, everyone can participate in storing and transferring money to someone else, secured by the nodes. This without any central institution or customer verification. It was the first massive step for crypto assets. However, because of the blockchain's linear scheme and since it is mainly used as a payment system, the significant limitations are scalability and code execution on the chain. This leads to technologies described in chapter 2.2 and 4.3. [4.2, 6]

There are many mechanisms and solutions for such problems, but the main chain will likely stay as introduced. That is not a big issue because Bitcoin is still the leading cryptocurrency based on its current market cap. Instead, it is a massive opportunity for developers to create extensional software around the Bitcoin blockchain.

### 2.1.2 Ethereum

The Bitcoin blockchain is more based around a decentralized financial system. In contrast, the Ethereum blockchain is not a specified chain in a particular field of usage and aims to make blockchain technology available to developers. The blockchain was released in 2015. Like within Bitcoin, servers are used to mine the native cryptocurrency Ether. However, it does not have a static hard cap like Bitcoin, and additionally, everyone can create their token or currency on the Ethereum chain. The chain can also execute transactions with these coins and offers a virtual machine that can run scripts to build decentralized applications. It is valuable for developers and all kinds of problem-solving that require a decentralized and trusted foundation. The current market cap of Ethereum is around 51 billion dollars, making it the second-largest cryptocurrency in terms of market cap. [2, 7, 8]

***Smart Contracts***

The scripts running on the decentralized virtual machine are called smart contracts and act like regular applications. It can be referred to as a decentralized “world computer” where servers, also known as nodes, collectively provide the machine's power. Nodes providing the computing power are paid out in the main currency on the Ethereum blockchain for creating blocks that include those transactions. Decentralized applications are called smart contracts because they are automatically executed by sending specific transactions to them.

For example, smart contracts can provide a crowdfunding service like it was already accomplished from the first decentralized autonomous organization, called TheDAO, in 2016.

Back then, an Ethereum smart contract was set up where people could pool money and further vote for a specific usage, where the money would be used in. This process is utilized with a smart contract, that automatically executes the transactions without a centralized unit or government to hold the money and sign off on the transaction. It can save many transaction fees and organization costs like we currently have in the real world. Developers can also combine smart contracts, like the concept of libraries in common programming languages, or to store information on the blockchain. [9, 10]

## 2.2 Second Layer Technologies

As already mentioned in the introduction, different projects aim to solve specific problems main blockchain ecosystems currently have to deal with. Such projects come with their networks, docking onto the original blockchain, seen as the underlying first layer technology. The systems do not change any functionality on the main blockchain but take the main blockchain's workload to increase scalability, add new functionality, or reduce transaction costs. Within the tokenization technology, even those concepts become relevant. Without the ability to transfer tokens between second layers, there will be a bottleneck on the mainchain or growing silos of tokens. This is not optimal because the user would always split the funds into different solutions without the ability to use them across all platforms.

Especially scalability of blockchains always was and still is a problem when it comes to entirely safe and trusted solutions. The main focus around the blockchain is security and decentralization. Because the security plays such an important role in payments in a blockchain, it can hardly be lowered. However, decentralization can be achieved in multiple ways. At the moment, three main concepts solve the problem of scalability: sidechains, rollups, and state channels. All work to scale up to serve thousands of transactions per second. The idea is moving or locking assets from the main chain to use them for transactions between participants that are done off-the-chain. [11, 12]

***Sidechains***

Sidechains are chains harmonizing with the mainchain. They´re moving much of the logic away from the main chain and loading it onto another blockchain. The chain will then provide another consensus algorithm that includes fewer participants. Crypto-economic incentives or cryptographic proofs ensure that even though the system is more centralized because of the fewer participants, it is nevertheless trustless due to it. Exit strategies are put into place to allow the user to withdraw the deposited money even if the consent participants become malicious. [12, 13]

An example of the implementation of sidechains is Plasma, which uses a unique solution that evolved out of the regular sidechain scheme. By using smart contracts on the main network, funds will be locked and transferred to the Plasma blockchain, where a set of validators are creating new blocks. Only the root hash of the Merkle Tree is stored on the main network within each commitment period. Plasma comes with an elaborate exit scheme to withdraw his funds from the Plasma chain back to the main chain. [14]

**Table 1: Pros and Cons of regular Sidechains**

| Positive | Negative |
|---|---|
| - sidechains are permanent<br>- no transaction on the main chain needed<br>- receiver does not need to be online<br>- no per-party fund lock-up | - can take a lot of initial investment to start off<br>- a federation or trusted party is needed<br>- no guarantee to withdraw additional earnings to the main chain |

### *Rollups*

From the original sidechain solutions, the idea of Rollups was born. There, aggregators put together collateral on the main chain and collect transactions from users off-the-chain. There are two main types of implementation: ZK-Rollups and Optimistic Rollups. Within ZK-Rollups, those transactions are trimmed, and their validity is proven with a unique cryptographic proof algorithm called SNARK. The main chain contract is then keeping two Merkle Trees for users and balances from all the transactions. Each block of transactions is then sent to that contract, which proves the transactions and updates accordingly. In contrast to ZK-rollups, the state within Optimistic Rollups is kept completely off-chain, allowing smart contracts to be created and used. Only each state root is published on the main chain, allowing to bypass heavy proof computation. The main difference between both approaches is data availability. [15]

### *State Channels*

State Channels are another concept of two or more parties agreeing to be bounded by a smart contract or a multi-sig contract. They are locking some portion of blockchain state, called state deposit, into the smart contract, and then use off-chain messaging to exchange and sign valid transactions with each other.

State channels are the main kind of payment channels. They share the same idea of a second layer operation, usually performed directly on a blockchain. The order of steps in a state channel is the following:

I. A part of the blockchain currency gets locked via multi-signature or some sort of smart contract. Participants must completely agree with each other to update it.

II. The participants update the state amongst themselves by constructing and signing transactions that could be submitted to the blockchain. They are now held within the state channel. Each new update tops previous steps.

III. Finally, participants submit the current state or currency back to the blockchain after the state channel is closed and simultaneously unlocks the state.

It is a quick and widely spread mechanism for participants to move funds to each other, significantly increasing security risk. It also saves transaction fees because just the first and last transaction must be submitted to the main blockchain. The best use case could be described as long-time trading between a defined set of participants with many exchanges. [14, 16]

When it comes to state channels, Raiden, with its payment channels, is one example. The concept behind it combines bidirectional state channels with pathfinding to get linear scalability. The pathfinding is then used to connect two participants who want to transfer tokens through existing state channels with at least the deposit needed to exchange. No new channels need to be created, and participants profit from small incentives. [17, 18, 19]

**Table 2: Pros and Cons of regular State Channels**

| Positive | Negative |
|---|---|
| - strong privacy within the channel<br>- instant finality<br>- saving transaction costs | - participants always need to be available<br>- channels for a defined set of participants |

***Outlook in Combination with Cross-Chain Technology***

Approaches like the Mimblewimble protocol [20, 21] could be seen realized within a second layer network to gain more anonymity and save bandwidth within an own sidechain. When looked onto the horizon, there is a new trend from developers moving to sidechain approaches or at least being interoperable with multiple chains. The tremendous wave of IoT devices will also lead to much greater usage of secondary solutions to handle the workloads of all those transactions and keep transaction fees low.

Networks that enable cross-chain functionalities can be viewed as second-layer technologies, as discussed in chapter 5. Such a network's primary purpose is to secure the backend from tokens held within the main blockchain network. They do not take away workloads, but they also dock their technology onto the main chain, expanding usability and creating their ecosystem.

As already described, cross-chain technologies may also be combined with scaling solutions or identity to become a strong concept of using assets blockchain wide but also to be stable when it comes to balancing transaction throughput. An example would be combining Mimblewimble with tokenized Bitcoin to create a scalable, totally anonymous trading network where tokenized Bitcoins could be exchanged and converted back to the original Bitcoins.

## 2.3 Decentralized Identity

The topic of using blockchain technology to picture the identities of individuals or machines in a decentralized way is currently on an aspiring branch. The hype also favors the second layer and cross-chain movement because personal wallet solutions representing your identity may become all-in-one solutions holding the user's money for transactions and personal data in the form of tokens within a secure offline database accessed by them. Identity solutions need to ensure the owner can be correctly identified, authenticated, and certified with correct compliance with personal data. This chapter describes why identity matters and how new cross-chain tokenizing technologies support those approaches.

As the internet pushed forward and the initial web appeared, homepages were read-only. The purpose of making information accessible for a wide variety of society was fulfilled quickly, and the urge to interact with computers to exchange data grew. When the interaction between devices evolved, the internet was generally designated as web 2. It was mostly just a frontend revolution, leaving server-centered structures and databases as a backend strategy. IT security and backup mechanisms increased drastically to be able to manage the throughput. On the user side, cookies and API´s developed to track down behavior within sessions, and new use cases like social media, e-commerce, or even knowledge platforms proliferated. A vast market of user data emerged to create intricate user data patterns to optimize monetarization and predict behavior. Data analysis is a considerable immense amount of how digital products gain value nowadays. Taking a closer look at what identity within the web means, it is mostly just tracked down to the device a person uses combined with several accounts created for almost every software product in use. The problem is that the internet was mainly built around machines, not for individuals. There is no real verification nor authentication of identity- rather mechanisms to cover most frauds and giving out copies of user rights. Another negative point: data is stored on servers operated by the company, meaning it technically belongs to the company, even if some distortion needs to be done to be compliant with specific laws. [22.2, 23]

The current state also raised issues with informatics ethical perspective, which lends to the General Data Protection Regulation from the European Union in 2018. As a conclusion from the GDPR, everything that helps identify a person, regardless of whether it refers to a professional, private, or public life of a natural person, counts as personal data. Because identities can be found in every business, may it be healthcare, governments, e-commerce, or future identities in IoT, there is a high relevance in rethinking and changing how data is stored or managed from small companies to big IT giants. The identity infrastructure is not only cost expensive: many companies are still caught up in data ownership lawsuits, data sales, and user behavior prediction. [24, 25]

Web 3 concepts will make it much more efficient to comply with regulations. The term web 3 is already common sense when looking into the future, defining a more decentralized way how the internet works, by using decentralized blockchain networks that act as the processors behind. It develops a bit more gradient than the previous web 2 because the fundamental back-end technology is tackled. But for the first time in history, actual values and not only copies of data can be transmitted in-between instances and used within decentralized applications that will appear on the horizon. Concepts will rely on decentralized peer-to-peer networks, abandoning the centralized server approach for safer user-centric technology. The new backend also creates a massive chance of using IoT devices by leaving single points of failure and introducing more resilient and secure blockchain networks. The governance of software systems will rely on protocol consensus instead of individuals from one entity, also drastically lowering system administration and IT security on such central instances. Future identity solutions will store most data on devices within wallets, pushing self-sovereignty forward. They can then connect to a wide range of such blockchain networks. Actions can be executed by referring to an actual identity, not only commands transmitted by a particular machine without secure verification.

Most importantly, all sensitive data will be kept within the wallet. And that is why tokenization technology matters. To create wallets where every user can interact with many chains but is still using save solutions only modern blockchains offer, the tokens have to be converted. Data that then still needs to be accessed from outside can be encrypted and transferred to decentralized mass storage, like IPFS [26] aims to provide. Within such an approach, multiple software systems can request the verification of one piece of public data, which is only valid if you are granted access with the wallet. Publicly available encrypted files also solve data duplication or storage space wasting. All features described bringing a lot of responsibility back to the user. Therefore, more user-friendly concepts need to develop over time for a seamless transition. [22.1, 22.3]

### *Future Estimation*

Within the Bitcoin community, the adage “not your private key, not your coins” became public. [27] If this would be applied as common sense facing the current web 2, it could be translated into “not your service, not your data.” Even with regulations and the right over data, you can never be sure how the data has been used or utilized until you force deletion. The goal of decentralized identity is to image rights and identifications of identity reliably and give the people back their data's power. This principle is also picked up in chapter 6 regarding building an asset management prototype.

# 3 Token Economy

Within the previous chapter, the fundamental concepts of blockchain technology were described. As a consequence of exchanging actual values and rights, they need to be stored in a blockchain. The demand for digital proofs, rights, and properties, in addition to the already growing payment solutions, will cause a new emerging token economy.

Shermin Voshmgir describes tokens themselves as “the atomic unit of the Web3”, followed by “anything from a store of value to a set of permission in the physical, digital and legal world.“ [22.4] When comparing them to real-life objects, they can act like money or casino coins, bonds, certificates, and so on. Because a token can represent nearly everything, particular terms like “cryptocurrency,” “digital twin,” or also more generalized terms like “crypto-asset” or “proof of right” are used more frequently. Still, tokens are no new topic within informatics. The most common case in web 2 were access tokens bound to a device or login scheme to acquire the right to use some sort of service for a certain amount of time.

## 3.1 Technical Specifications

There are two main types of implementing tokens within a blockchain: protocol tokens and application tokens.

**Table 3: Technical Token Specification**

| | Protocol Token | Application Token |
|---|---|---|
| Layer | functioning on the initial protocol level of a blockchain | operating on application or smart contract level |
| Creation | created from consensus, defined at the release of a blockchain | created by users from smart contracts, instantiated after the initial blockchain release |
| Use Case | network incentive, ordinary currency, or to mandatory favor the purpose of the blockchain | designed for new application possibilities or to represent certain assets held on the blockchain |

While application tokens are not necessary to run a blockchain, they are common sense to build projects on top of a secure decentralized network. As an example, Bitcoin does not offer the ability to create application tokens. The aim was to make a standalone payment system with one main currency, so a second execution layer was not needed. Ethereum, for instance, was built to function as a blockchain for developers and therefore introduced a second layer that uses the virtual machine of the network.

## 3.2 Differentiation of Tokens

Both kinds of tokens can also be clarified by the general use case and comply with rights and laws. The technical layers are not of importance when viewing the purpose of a given token. [28, 29]

**Table 4: Different Kinds of Tokens**

| | Utility Token | Commodity Token | Security Token |
|---|---|---|---|
| Use Case | specific purpose of an application, some right, or the network | payment and exchanges to achieve profits | long time investment bond aimed for profit |
| Representation | context of use case | cash or resources | capital investments |
| Examples | privacy tokens,<br>node tokens | stable tokens,<br>trading tokens,<br>real-world asset tokens | investment tokens,<br>lending tokens, |

It needs to be mentioned that utility token might become commodity tokens when traded within exchanges or seen as a valuable asset overcoming their original purpose.

## 3.3 Stable Coins in Detail

As seen within the examples of commodity tokens, stable coins are categorized for primary trading purposes. Holding a specific stable value with minimal to no fluctuation can always be referred to as a monetary system behind. There are different types of how a stable coin can be collateralized. [22.5]

I. **Asset-Collateralized Token:**
The token refers to goods in the real or digital world, which it is handed out for. This is the case for digital twins or the rights of a particular asset.

II. **Crypto-Collateralized Token:**
The token refers to a token held on another blockchain that is handed out for and secured. Interoperable trading with each other should be given.

III. **Central Bank Stable Token:**
The token refers to a stable token achieved by a governmental approach, executed with an oracle to the outside world

IV. **Algorithmic Stable Token**
The token refers to a stable coin where stability is achieved by algorithmic and mathematical functions mirroring governmental functions fully on their own

For cross-chain technologies, crypto-collateralized tokens are the main focus. Because it is not possible to transfer the initial token across blockchains, workarounds, like described in chapter 4.3, need to be developed.

# 4 Cross-Chain Interaction

Previous knowledge leads to the question of how blockchain interoperability can be achieved. There are three main ways in which cross-chain interaction can be categorized in. They all focus on very different purposes. It might be the case that lightweight concepts also be implemented in more complex cross-chain projects.

**Table 5: Categories of Cross-Chain Solutions**

| | Heavyweight | Lightweight | |
|---|---|---|---|
| Type | Superordinate Cross Chain Solutions | Atomic Swaps | Tokenization |
| Purpose | combining blockchains | exchange tokens | convert tokens |

## 4.1 Superordinate Cross Chain Solutions

Original blockchains can eventually be seen as the backend for the internet. Blockchains, therefore, must be connected to gain standardized communication. If area ranges are overlooked, single blockchains function like a local area network within their use case, servers, and community. Future blockchains may then act like metropolitan or even wide area networks, connecting all the separated blockchain solutions for even more excellent interoperability. That is the reason why superordinate cross-chain solutions are often referred to as a “blockchain of blockchains.”

Additionally, second layer technology could expand functionality or take workloads to scale all the featured blockchains directly. Interconnection and Interoperability are the main goals to achieve a bigger picture for the blockchain and crypto space. Those projects also feature the more lightweight tokenizing technology but integrated within their chains. [30, 31]

### *Wanchain*

The Wanchain project's goal is to become an interoperable decentralized bank with explicit usage of the tokenizing technology. They use proof of work consensus on their chain, providing ring signatures, threshold secret sharing, one-time account creation, and are backed with their networks token. This approach is very appealing when analyzing the decentralized financial market's growth and tokenized coins within it. [33, 34, 35]

### *OAN*

The Open Application Network is working on open-source blockchain software, where user data remains at people and developers. The company tries to support custom blockchain architectures while providing a trustless mechanism for cross-chain interoperable app deployment. The center of this system is a public enterprise blockchain called Aion combined with OpenApps, which are smart contract compatible programs built on top of their blockchain. [34, 36, 37]

Aion is a hybrid chain using Proof of Intelligence, where participants can stake tokens on the network to secure the validators or participate in performing artificial intelligence computation. This training in artificial intelligence could further be used for Open Apps. [38]

### *Cosmos*

Cosmos wants to connect blockchains to run concurrently with one another while retaining interoperability for development. Cosmos tries to solve this with its network running PoS build on Tendermint, a blockchain application platform that provides the equivalent of a decentralized webserver-like database. The first application is called Cosmos Hub and acts as the bridge for all zones, referred to like all the blockchains pegged to the Cosmos ecosystem. [34, 39]

### *ICON*

The Korean project ICON is built around a hub-like blockchain solution based on artificial intelligence. Other than focusing on financial or development sectors, the core aim is to connect organizations in general like banks, schools, hospitals, or healthcare. Therefore, it is more focused on exchanging data and offering their solution directly to the consumer, rather than creating an interface for businesses.

It offers its kind of smart contracts called SCORE. These “Smart Contracts on Reliable Environment” do not need to be executed on a virtual machine. Instead, they run directly in real-time within a container-like environment, separated from the mainchain. Repository-based versioning is one main benefit. [34, 40, 41]

***Polkadot***

The Polkadot project aims to be the standard in cross-chain technology. As the whole blockchain behind, the relay chain is responsible for the network's shared security, consensus, and cross-chain interoperability while running with PoS consensus. It tries to connect any type of data to the blockchain, making it a universal protocol for transmitting on blockchains. Similar to Cosmos zones, Polkadot uses the term Parachains, which refers to parallel blockchains with their sovereign consensus running in parallel. Cross-chain transactions are then resolved using a queuing mechanism based around Merkle Trees and tokenization to ensure correctness.

In addition to the main consensus, their network security is pooled together from connected chains, composing and applying combined consensus to all participants. This feature can help smaller blockchain projects. With a small overhead in traffic, the network offers a bigger security pool and extra validators, so small Parachains are less likely to get overrun by attacks. [34, 42, 43]

***Evaluation***

Future technologies will likely be more directed to developers to gain more interfaces and a more significant community around them. Out of this fundament, applications and userbase will return in the long run. A few of them want to become some sort of protocol standard for cross-chain technology but have to deliver their ideas and mechanisms described in whitepapers in actual software first. An approach to use the server power for smart contracts, hash puzzles, and training artificial intelligence are mostly rough ideas at the current point. Both ICON and the OAN do not have a specific publicly released answer on this topic. Nowadays, most AI is trained by hand, and the future technology in this field has to show how to connect such behavior onto autonomous and decentralized server-concepts.

## 4.2 Atomic Swaps

An atomic swap can be described as a technology that safely introduces a token exchange or trade without using centralized intermediaries. They can happen directly between blockchains of different cryptocurrencies, or they can be executed off-chain while always bypassing the problematic counterparty risk. It is often used within smart contracts, which will also be discussed later. [44, 45]

Assuming Alice and Bob want to exchange coins. The atomic swap can be arranged in three sequences to comply with the security: The first sequence acts as a preparation of the transactions without any on-chain event. None of the parties needs to get refunds because they still own everything. [46]

I. Alice pics a secret random number x
II. Alice creates a transaction “alice_tx,” which
   - sends her tokens from her address to Bob´s address
   - can only be spent if x is given
   - is signed by Alice
III. Alice creates a second transaction, “alice_refund,” which
   - sends her token from Bob´s address back to her address
   - is signed by Alice
   - is locked 48h in the future
   - need to be signed by Bob
IV. Bob creates a transaction “bob_tx,” which
   - sends his token from his address to Alice´s address
   - can only be spent if x is given
   - is signed by Bob
V. Bob creates a second transaction, “bob_refund,” which
   - sends his token back from Alice´s address to his address
   - is signed by Bob
   - is locked 24h in the future
   - need to be signed by Alice
VI. Alice sends the transaction “alice_refund” to Bob
VII. Bob signs the transaction “alice_refund” and returns it to Alice
VIII. Bob sends the transaction “bob_refund” to Alice
IX. Alice signs transaction “bob_refund” and returns it to Bob

In the next sequence, both will transmit their transactions on-chain. To get the coins back from fraud, they can both publish the refund transaction signed by each other before. Bob, in this case, can do this after 24, Alice after 48 hours.

I. Alice submits the transaction “alice_tx” to the network.
II. Bob submits transaction “bob_tx” to the network

The last sequence can be called the spending-phase. Both parties need to make sure they finally transmit their coins to their addresses- otherwise, the counterparty can claim their refund transaction after the certain amount of time is over.

I. Alice now spends the transaction “bob_tx,” which was released to the network before. She cannot do this without revealing the secret number
II. Bob can now spend his transaction “alice_tx” using the secret number from Alice that was shown before

Because this process needs some technological understanding when creating transactions offline and exchanging them, Hash Time-Lock Contracts have been developed. HTLC´s are time-bound smart contracts between parties that automate the process of atomic swaps for blockchains that support smart contract functionality. [44, 46]

Commonly, the process for exchanging cryptocurrencies is very time consuming if it is done without a middleman regarding waiting times. But even with HTLC´s or exchanges, there are several other inconveniences. For instance, not all cryptocurrency exchanges support all coins. A trader has to assign multiple accounts or trade another crypto asset in between to maintain the same value on another chain.

## 4.3 Tokenizing Technology

Where atomic swaps can solve currency exchanges to use them on other blockchains, tokenization aims to convert assets, so the initial value can be used on other chains. This makes exchanging tokens just to maintain values obsolete.

Only by the wording, anything that can be represented as a token. However, when tokenizing technology is viewed from the crypto space, the converted token is used in a specific concept. The tokenization technology can then be described as an initial token becoming an equal asset with more functionality on another blockchain while maintaining the original value. This asset then becomes a crypto-collateralized stable coin, as described in chapter 3. Commonly, this also implies that a protocol token is becoming a secure application token. Still, in the future, “application-to-application-token”-conversion could evolve within second layer technology as well. For instance, by wanting to make a digital twin available on another chain. At the moment, there is no such network for custom tokens or even concepts. There is also a big question mark on how such ideas could safely expand for systems only handling non-fungible tokens. With totally different values, asset management and security backing can easily become unpredictable.

Tokenization itself does not guarantee the ability to get back the initial asset. For instance, Liquid's tokenizing solution, which operates outside of the Ethereum ecosystem, only ensures to trade back the tokens if the user is actively participating within their network. For the majority of projects, full backward compatibility is essential when keeping tokens stable. It is also crucial for software products to send and receive the initial asset autonomously while using smart contract technology on another blockchain.

The main problem of tokenizing technology is that there either needs to be a verified and trustworthy middleman for centralized solutions or a technology within decentralized approaches, which ensures that the initial currency or asset is backed with the same amount, making it 1:1 in scale. There are many different implementations on the market covering both types- even when a fully decentralized version is always the most secure at the cost of more complexity and scalability.

***Regular Order of Conversion***

To ensure that the currency is handed out for the tokens and no fraud has happened, the initial assets will be securely locked on the first chain. After a verification time, new tokens for the locked assets are created. To give an example: If the currency from a financially based blockchain like Bitcoin is locked, it can be used afterward to make it's token accessible on a development-driven chain like Ethereum. Tokenization of the original Bitcoins is initiated, original tokens locked and equal once handed out. Now they can be used in smart contracts. After using the application, the tokens can then mostly be traded in for the initial Bitcoins. Within this process, the tokens are burnt to prohibit double-spending, and the original currency remains. [47, 48]

### 4.3.1 Different Lightweight Approaches

As a result of explaining both techniques, it would be great to compare them with each other. Atomic Swaps require price discovery by whoever starts the trading. Further, existing wallets and decentralized exchanges need to accept the atomic swap mechanisms. Tokens, on the other side, have the luxury to be mostly available in any ERC20 supported wallet, which is a common standard nowadays. Price discovery also does not need to be done for us because the asset's value remains the same.

Compared in timing, Atomic Swaps are slow. Even if there is a KYC process involved during tokenization, it will still complete way faster. Further, when doing an atomic swap on a common decentralized exchange platform, it may require a separate deposit plus an atomic swap fee. This is another inconvenience of multiple exchanges.

The real benefit of atomic swaps is maintaining the main currency and that nothing has to be locked up during the process. It is also quite handy for any person who does not want to get anyone else involved other than the two persons exchanging the tokens. It is just not for frequent use and will also not give access back to the initial asset, which tokenizing is known for. The use cases could not be much more apart. [45, 48, 49]

### 4.3.2 Aspects of Tokenization

Tokenization is bringing liquidity and application support. When tokenizing Bitcoins, the liquidity on decentralized exchanges will grow through smart contracts and impact the huge decentralized financial market of Ethereum.

Also, tokens backed by fiat currencies offer a safe way for traders to keep their money within the crypto world. Because they are pegged to the real-world, price fluctuations in between would not happen. The stability offers a way to exchange fiat currency values in decentralized exchange applications where no direct fiat currency can be used. Conversion rates or taxes can be saved, opening the world for digital currencies without dispense common money.

Finally, there are a lot of different projects on approaching exchanges on a decentralized fundament. Tokenizing technologies would make it easy to represent any other cryptocurrency across those projects and enhance it with new technology that offers token-support. Institutions that accept cryptocurrencies could focus on the development on one chain, rather than needing to interact with multiple blockchains simultaneously. [50]

### 4.3.3 Models of Implementation

There are two main types of implementing tokenizing technology: either algorithmic or centralized. Within the algorithmic approach, demand and supply are controlled by smart contracts or formulas, for example, Dai or Basis. If it is centralized, assets are stored and handed out by an organization that publishes proof of reserves. Projects like Tether [51], True USD [52], USDC [53], or future governmental bonds can all be seen as such.

As for now, most tokenizing technologies are leaning on the centralized model, but instead of relying entirely on one institution, they rely on a consortium of institutions performing different roles in the network. Some approaches are even outsourcing the fee-calculation to central models. Those can be viewed as a hybrid version with chosen governance on specific aspects of the technology. [50]

# 5 Tokenized Bitcoin on Ethereum

Given the great potential of decentralized applications from Ethereum using tokenizing technologies, the use cases for Bitcoin and other blockchains could expand dramatically. It could resolve in much more user-friendly applications to interact with cryptocurrency. The fundamental need comes from smart contracts, wanting to use the current number one digital currency. This chapter will cover how tokenizing technologies implement Bitcoin on Ethereum.

## 5.1 Improvements

I. Ethereum increases transaction speed. Blocks are roughly created every 15 seconds, and it is considered to have the confidence of a transaction in less than 24 future blocks. On Bitcoin, blockchain blocks are approximately created every 10 minutes with confidence within six blocks.

II. Better Usability. Tokens can be used within all second layer networks and smart contracts, enabling Bitcoin to be used in privacy-solutions, micro-payment solutions, decentralized financial markets, etc.

III. The ERC20 standard has been adopted by many institutions and provides users with various exchanges and wallets that may come with more user-friendly backup schemes.

IV. Ethereum achieves greater liquidity for Bitcoin in general. Ethereum currently handles up to 15 transactions per second, Bitcoin approximately 5. The throughput on Ethereum will further increase within the future due to Ethereum 2.0 and by splitting up the network to provide scaling.

V. It can offer greater exchangeability to other coins and tokens, which also features the trading against custom application tokens created on Ethereum. The exchangeability also safely enables custom token trades within smart contracts using the most common cryptocurrency.

VI. It can offer more privacy by using second-layer technologies like sidechains, rollups, and state channel solutions.

VII. Increased transaction bandwidth referred to the transactions per second. Ethereum has an average block size of 25 kilobytes [54], meaning little under 5.9 megabytes per hour. Bitcoin is currently onto an average block size of 1.3 megabytes [55], which sums up to about 7.8 megabytes per hour while offering three times less throughput.

## 5.2 Market Analysis

Within this year, there was a massive increase in tokenized Bitcoin on Ethereum. Mainly in June and July, where some of the first fully decentralized attempts were released on the main network of Ethereum. The growth was fired up by the decentralized financial market of Ethereum, which was to be noticed in substantial transaction fees. Individuals but also a lot of trading bots used tokenization to participate in a decentralized stock exchange.

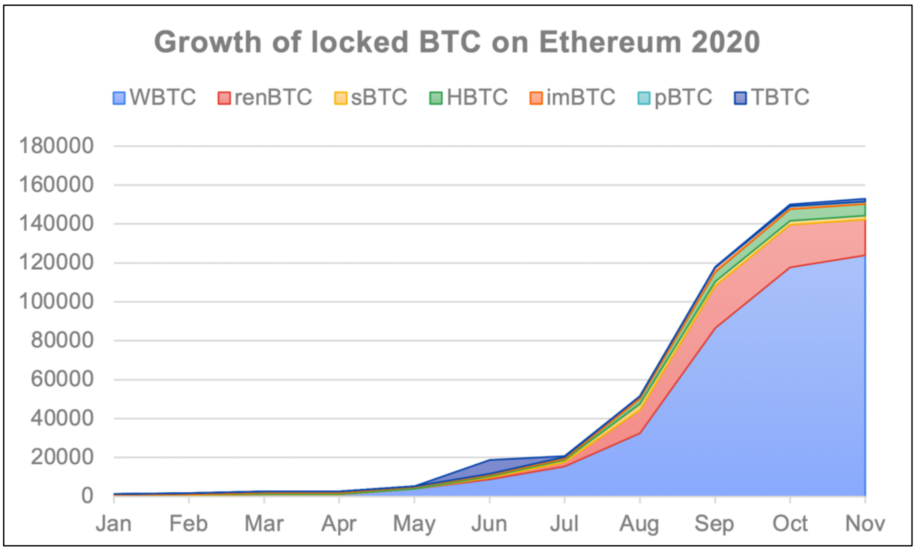


**Figure 1: Growth of locked BTC on Ethereum 2020**

As for now, there are about 152,000 Bitcoins locked- worth about 2.8 billion USD. The amount equals 0.8 percent of all minted Bitcoins already being transferred over. From rising nearly exponentially in the period from March to September, tokenization is now growing more leisurely. [56] As estimated on the analysis of lost Bitcoins published from Chainalysis in 2018, those numbers could resolve in realistically more than 1 percent of total minted Bitcoins. [32]

When looking at the distribution of different projects, there was a massive spike in June. Two of the main decentralized projects about tokenizing went onto the main network of Ethereum. Afterward, it settled a bit, and about 80 percent of the tokens are currently locked and maintained by one of the first tokenizing projects released, minting WBTC. Seeing fully decentralized backed tokens like renBTC, which grew to 12 percent of market capacity, there is a lot of room to think about how the market could change soon.

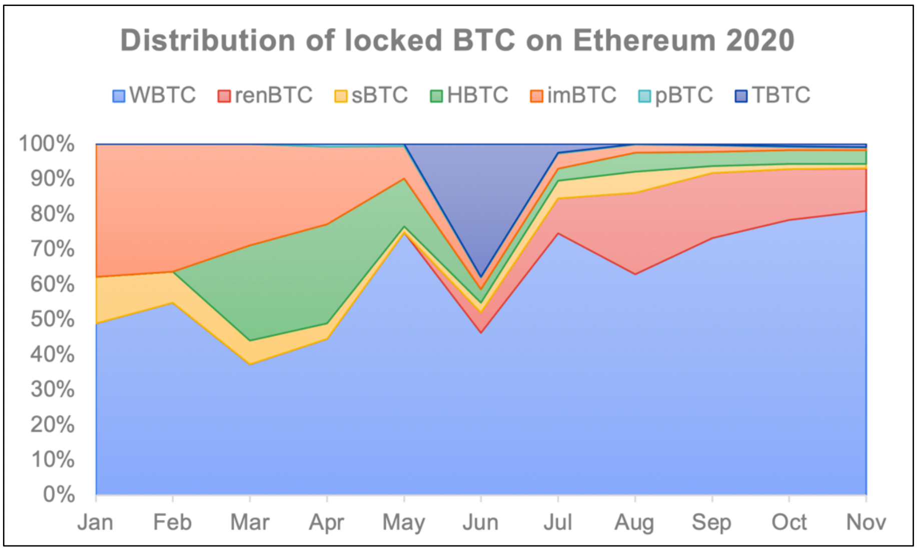


**Figure 2: Distribution of locked BTC on Ethereum 2020**

## 5.3 Tokenizing Projects

In the following sections, Bitcoin tokenization on Ethereum is viewed. This snapshot of solutions currently involves seven projects. They use different approaches of tokenization, which were discussed within chapters 4.3.2 and 4.3.3. They can all easily be used within smart contracts without any porting- or hub- mechanism like it may be the case for projects outside of Ethereum. Integration-wise, relying on the most successful developer-driven blockchain also is a decent benefit. Those properties make them the best-in-case scenario to integrate them in applications like the asset management solutions currently in development by Blockchains LLC, which operate on top of the Ethereum blockchain.

### 5.3.1 Kyber, BitGo: WBTC

Wrapped Bitcoin was initiated by a community formed out of more than 30 institutions, e.g., Kyber and BitGo. It was one of the first ERC20 tokens backed 1:1 with Bitcoin in 2019. WBTC posts their proof of reserves on the Bitcoin chain from a consortium out of validated custodians. WBTC is semi-permissioned, meaning there are AML and KYC processes involved, but approved merchants are incentivized to quickly initiate the minting of more tokens to users. The pyramid-like scheme is similar to how Tether´s USDT has massively scaled with a permissioned minting and burning mechanism. The custodianship is secured by multi-sig contracts that require multiple parties from a DAO to sign transactions. [57, 58, 59]

***Structure and Minting/Burning***

Within the project, there are three main roles. The Custodian, represented by BitGo, holds the keys to mint tokens. Merchants, represented by Kyber, then initiate minting and burning events related to wrapped tokens from the Custodian. Users can acquire wrapped tokens or burn them by only talking to such merchants involving a KYC process and AML laws. As the last role, there are DAO members, pushing contract changes and adding or removing custodians and merchants. A multi-signature contract controls the consortium. Holders of the keys to the multi-sig contract act like DAO members. This solution is very scalable because only members talk to the custodian, and members are splitting up tokens to all users. [59]

***Current Status***

WBTC is currently the most significant player in the decentralized financial space with listings on Compound, Nuo, and Fulcrum. At the moment, there are about 124,000 Bitcoins tokenized with WBTC, taking up about 80 percent of Bitcoin tokens on Ethereum. [56] Due to the AML and KYC, it cannot be used in automated processes.

### 5.3.2 TokenIon: imBTC

The project imToken from TokenIon lets you manage multiple crypto assets in one wallet, including imBTC as a 1:1 backed tokenized Bitcoin stable coin. Bitcoin from TokenIon can be generated by locking up Bitcoin using the imToken wallet from the company. Locking up Bitcoin sends BTC to a multi-signature account and simultaneously mints an equal amount of imBTC tokens. These tokens can then be used on Ethereum apps and later reimbursed again for Bitcoins. While not trustless, the locking and unlocking process is fully automatic and quick. An exciting feature of imBTC is that it bears interest by merely holding it. This interest comes from fees incurred by other users transforming Bitcoin. The wallet awards you about 1% annually. [57, 60]

***Structure and Minting/Burning***

The locked Bitcoins are stored on a cold wallet. Users can acquire and redeem their BTC anytime within the wallet. In both cases, the customer transmits his bitcoin directly to TokenIon´s smart contract. This smart contract mints and burns the tokens and locks or hands out Bitcoins. [57, 60]

***Current Status***

The wallet itself can be used for trading a lot of other currency due to TokenIon being an exchange platform. Currently, more than 1,100 Bitcoin are tokenized with the imToken wallet. [56] However, due to the fully centralized approach, it is only used by people who already use their wallet or those who own Bitcoins and want to gain more annual profits.

### 5.3.3 Provable: pBTC

The project from Provable, called pTokens, aims to solve liquidity and interoperability between blockchains. The project is currently implementing EOS and BTC tokens on the main network of Ethereum but also got a network for testing purposes to experiment as a developer. The way pTokens peg to the original asset is by running each involved blockchain simultaneously in a Trusted Execution Enclave. The TEE is a physical piece of high-security hardware. Both full nodes from the blockchains of the two tokens need to be involved. In the future, it is planned that secure enclaves running inside the TEEs cooperate within a network concept to jointly generate and manage private keys for the peg-in/out process. The Enclave has access to both sets of keys and can execute transactions on both blockchains, effectively linking the two assets together. It is to mention that this concept fully relies on the security of the hardware. [57, 61, 62, 63]

#### *Structure and Minting/Burning*

The enclave represents the secure sandbox container in which private keys for both corresponding blockchains can be generated and stored. These are then used for the transaction-signing that both mines and burns pTokens and validate incoming blocks and their transactions. The principle ensures that only valid transactions from both blockchains are verified from the enclave. Decentralization will be achieved later by spreading the operation to a federation of operators with multiple TEEs each.

The user can deposit the original asset using the pTokens deposit smart contract, providing their desired destination token address in the transaction. The block in which the initial transaction takes place gets sent to the enclave and all of its transactions. The enclave then validates the block header along with all the transactions. If the transaction is validated, the enclaves locate the pTokens transaction sent to the smart contract and parse the amount and the destination address. With this data, the enclaves prepare a transaction to mint the equal number of tokens on the token-side smart contract. Enclaves now perform a multi-party computation to sign the transaction and the derived private key to address where the initial asset is held. Enclaves emit the transaction, which is broadcasted to the destination blockchain. If the transaction is confirmed, minted tokens will now be held by the user's destination address. The functionality of gaining access back to the original asset is the same in reverse. The only difference is the call of the burn function in the smart contract. [61, 62, 63]

#### *Current Status*

At the moment, there are about 170 Bitcoins locked into the system. [56] That is mostly due to an early centralized version on the main network only using one validator TEE. In the future, this will be replaced by DAO-like governance and a decentralized network consisting of TEE´s. The end will prove if such an attempt is safe and can be turned into reality with multiple TEE´s within a system. In the past, many vulnerabilities have recently been discovered that subvert such high-security assumptions. If large amounts of Bitcoins are locked, the incentive to exploit these vulnerabilities will grow tremendously. [63, 64]

### 5.3.4 Synthetix: SBTC & IBTC

Synthetix Bitcoins and Synthetix Inverse Bitcoins are synthetic assets, so-called synths, built on the Synthetix platform on top of Ethereum. Synths are considered more trustless because they do not require the underlying asset to be held when using Bitcoins values on Ethereum. However, this makes Synthetix the only approach without real Bitcoin tokenization, where the initial currency is locked up. Having no locked Bitcoin also means that the underlying asset is not redeemable for the synthetic itself. This solution does not fit asset management solutions where the user wants to use the initial asset on another blockchain. [57, 65, 66]

***Structure and Minting/Burning***

Synthetics are a form of interoperability that aims to give users exposure to an underlying asset's price. The user is required to deposit 800% of collateral to mint a smaller number of synthetic Bitcoins. If the collateral value drops too much concerning the synthetic value, then the collateral is liquidated. Within the liquidating process, tokens are taken from the user and used to burn the old and mint the new synthetic asset with the current ratio. [78]

They are implemented as ERC-20 tokens and pegged against any crypto, real-world asset, or other value. Synths are backed by the Synthetix Network Token, short SNX, which is staked at a ratio of 800%, thus providing enough collateral to absorb large price shocks. Assets on Synthetix are assigned to an exchange rate through price feeds supplied by an oracle.

There are trading pairs for BTC against other synths such as ETH, USD, EUR and even precious metal pegged tokens such as XAU (gold) and XAG (silver). Synthetix also allows the creation of synths that are inversely correlated to the asset they are tracking. IBTC, for example, follows the inverse Bitcoin price and can be used to take a short position in Bitcoin by merely buying into it. [65, 66]

***Current Status***

It only appears as a trading platform for betting on assets, rather than holding them and using an owned initial asset on another chain. Currently, there are about 1,900 Bitcoins locked in the Synthetix ecosystem. [56] Exchanges can also be done on the Synthetix Exchange App, where this scheme bears interest. [59, 65]

### 5.3.5 Huobi: HBTC

Huobi is one of the world's leading crypto exchanges, more common in Asian regions. With HBTC, they try to implement tokenized Bitcoin to the Ethereum decentralized financial system.

#### Structure and Minting/Burning

It can be viewed as a 3-step-scheme, where Huobi acts as a centralized custodian on top. From there, chosen acceptors can deposit Bitcoin and mint HBTC in return. Users can then trade Bitcoins to the acceptors to get HBTC tokens. The scheme is very similar to the Wrapped Bitcoin approach. Like WBTC, this mechanism offers the ability to scale well because users only contact the acceptors. [67, 68]

#### *Current Status*

Currently, there are about 6,000 Bitcoins locked on Huobi. [56] Users need to trust Huobi as a centralized institution. The interest here comes from advertised decentralized finance applications. [2, 67, 68, 69]

### 5.3.6 Keep Network: TBTC

The goal of TBTC from Keep Network is creating an ERC-20 token that maintains the most important property of Bitcoin- it's status as hard money on a decentralized network foundation. While other projects offer to mint any number of Bitcoins, within TBTC, only fixed lots, e.g., 0.01, 0.1, 0.2, 0.5, and 1 BTC can be converted. But even with lot-sizes, the significant advantage of the system is that anyone can convert currency without going through a KYC process neither central instances. It´s essential to automated processes without human interaction. [56, 70]

#### *Structure*

The backing Keep Network already implements a token and a random beacon for signer selection, a distributed key generation protocol, and an efficient multi-party threshold protocol. The only link between the Bitcoin blockchain and the host chain is the TBTC system itself, which runs as smart contracts on the host chain.

Due to the mechanism being decentralized, there are a lot of security approaches. Each signer in the keep network has to deposit an amount of currency from the host chain to prevent the network's signers from stealing deposited Bitcoins. Deposits are calculated based on the number of signers per group used to hold the original Bitcoin and mint new Bitcoins on Ethereum via ECDSA cryptography. The technology could handle up to 80 signers per group in future versions. In the first version of the TBTC Network, the signer groups will consist of three signers. Because of the low number, they will need 3 out of 3 to guarantee transactions. In the beginning, the collateral will therefore be 150% from the current

Bitcoin price in Ether. If one of the participants cheated, the other two could recreate the 1:1 backed stable coin. Ether is used to buy back Bitcoins, and the signers will be automatically removed from the keep network. The signer groups will also change every six months.

While maintaining the backing of equal Bitcoins, Ether holds it´s security. If the collateral is significantly lower or higher than Bitcoin, a liquidation process can and needs to be initiated. Within this process, signers close their deposit and pull out their Ether to create new collateral with the current ratio. If the network is undercollateralized, signers need to put in more Ether to maintain security. Otherwise, nodes have spare Ether to create another signing group after liquidation.

There is also a hard abort trigger for the developers to freeze the system for ten days. After this option is pulled once, they cannot freeze it another time. The developers also have the right to change lot sizes, collateral threshold, or delay fee rates.

At the start, Keep will choose 60 secure signers. Afterward, there will be six months where anyone can apply as a signer and participate. Signers will be paid for their deposits. For every Bitcoin they deposited in Ether, they will receive 0.009375 TBTC. As each stake has a fixed term of six months, that implies a total signing revenue of 1.875% each year. Fees are managed by MakerDAO, which is an external consortium of MKR token holders. This system can be viewed as an oracle because the network itself does not calculate the fees. Developers do have a key to correct fees if they bring damage to the system.

Signers also have to choose if they only want to participate in signing groups or even in the network's random beacon. The beacon is used to select and recreate signer groups randomly. Suppose they want to participate in both, Ether and KEEP tokens are needed. KEEP tokens will be distributed to the best participants that stake ETH for signing groups. They can also be earned within their staking test network before launch or by contributing to the stake drops that will happen monthly in the range of two years after the regular launch. The KEEP token will also work within future applications realized with the network. The distribution graph can be found within Appendix, Part 1. [70, 71, 72, 73]

***Minting/Burning***

To acquire tokenized Bitcoin with TBTC, the user requests the creation via the Ethereum smart contract requiring a small amount of Ether. The TBTC network is then creating a signing group within the network. Afterward, multiple signers are chosen by a requested random seed from their beacon. Then, group keys and a public key are created from elliptic curves through distributed key generation. The signing group's public key is published to the host blockchain and corresponds to its Bitcoin wallet. When the user requests the Bitcoin wallet address from the signing group, the wallet address is created by converting the public key. In the end, the user will deposit Bitcoins into the address, the signing group will prove the transaction block of the deposit through SPV and is assigning the user a non-fungible token. With this token, the user sends the non-fungible deposit-token to the Keep Network to guarantee the deposit of Bitcoin was made by him, which now mints and assigns the TBTC to the Ethereum address. [71, 72, 73]

***Current Status***

Due to a bug found quickly after the initial release date, the project shut down only two days later. The issue was related to the redemption flow of deposit contracts, which put signer bonds at risk. Currently, they have managed the second release and are growing steadily on Ethereum´s main network. There are currently about 200 signers and more than 1300 addresses in the hold of their Bitcoin on Ethereum. [73, 74, 75]

### 5.3.7 Ren Project: renBTC

Ren is a platform to make tokens of all blockchains interoperable, allowing decentralized exchanges and decentralized financial apps to leverage the liquidity available on them, using fully decentralized tokenizing. The Ren tokenizing process is very similar to the principle of the Keep Network. However, it has some minor changes when it comes to secure backing. [57, 78]

***Structure***

While TBTC uses Ether to guarantee collateral of signers, Ren Project uses their network token, called REN, to back up the system. That means that the system is regulated by itself, regarding demand and fees. The network consists of independent servers connected, called Darknodes. Those Darknodes run a virtual machine called RenVM to create signer groups, so-called Shards, holding the original Bitcoins and minting fresh Bitcoin tokens on Ethereum. The whole signer group will need to put down three times more collateral in REN than the Bitcoin deposit held for security purposes. As within the Keep Network, signer groups use ECDSA cryptography to secure the token. Fees within the network are bound to algorithmically defined formulas that dynamically adjust based on the current workloads at minting and burning.

Ren Project can use up to 90 or even 200 singers per group, which then uses Shamir´s Secret Sharing to centralize the full key and offers a frequent swap of shuffling Shards once a day, meaning new signer groups will be instantiated. The fundamental aspect of the Ren Project is the virtual machine. When Bitcoin is transferred to the address, RenVM with its signer groups takes custody of the coins and mints a representation of it on the host blockchain. The network fully remains on itself and is open for anyone to create a Darknode, without any stake drops. The only requirement being 100,000 REN. With a total supply of one billion REN, this makes up for a maximum node capacity of 10,000. There is no abort trigger or extra rights for the developers. [78, 79, 80, 82]

### *Minting/Burning*

To acquire tokenized Bitcoin with Ren Project, the user requests the creation via the Ethereum smart contract requiring a small amount of Ether. RenVM within the network is then creating a signing group. After multiple signers are chosen, group keys and a public key are created from elliptic curves through distributed key generation. The signing group's public key is published to the host blockchain and corresponds to its Bitcoin wallet. When the user requests the Bitcoin wallet address from the signing group, the wallet address is created by converting the public key. In the end, the user will deposit Bitcoins into the address, the signing group will prove the transaction block of the deposit through SPV and instantly mints the Bitcoin on Ethereum and sends the token to the user's Ethereum address [78, 81]

### *Current Status*

At the moment, Ren has an application called Roundabout [83] to get tokenized Bitcoin quickly to Ethereum. Ren is the most successful solution that is fully decentralized. Only three months after release, they already got about 1,200 nodes running, which further increased to almost 1,500 at the moment. There are 17,200 Bitcoins locked within the network. [56, 84]

## 5.4 Comparison of Current Approaches

When looking at comparing the solutions, the most important is evaluating the current snapshot of projects containing all basics. This evaluation will be done within a table where answers can be normalized for rating purposes. The rating relies on using such tokenizing technology within autonomous software solutions for asset management.

I. **What is its relative market size of their Bitcoins on Ethereum?**
- relative market size on three decimals

II. **What is the current type of implementation?**
- concept: 0
- prototype: 0.5
- main release: 1

III. **What is the type of permission?**
- permissioned: 0
- semi-permissioned: 0.5
- permission-less: 1

IV. **What is the Bitcoin backed with, to achieve stable value?**
- Custom Token: 0
- BTC: 1

V. **What is the current type of distribution?**
- centralized: 0.25
- semi-centralized (e.g.: consortium): 0.50
- semi-decentralized (e.g.: assigned nodes): 0.75
- fully decentralized: 1.00

VI. **Are external relations needed and if so, which kind?**
- multiple: 0.25
- one: 0.5
- none: 1.00

***Question Weights***

| | | | |
|---|---|---|---|
| I. | 0.10 | minor: | userbase grows from integration of technology |
| II. | 0.20 | essential: | software in production must have audited release |
| III. | 0.25 | main point: | only usable when permission-less |
| IV. | 0.20 | essential: | needs to be convertible to Bitcoins |
| V. | 0.15 | important: | decentralized solutions are more trustworthy |
| VI. | 0.10 | minor: | one adaptive ecosystem is favored |

***Agenda***

░ perfect to good ▒ ok to moderate ▓ poor to unpleasant

**Table 6: Brief Overview of Tokenization Projects**

| | renBTC | tBTC | sBTC | pBTC | imBTC | HBTC | WBTC |
|---|---|---|---|---|---|---|---|
| Relative Market Size | 0.113 | 0.009 | 0.013 | 0.001 | 0.008 | 0.039 | 0.817 |
| Type of Release | main release | second main release v.1 | main release | prototype | main release | main release | main release |
| Type of Permission | permissionless | permissionless | permissionless | permissionless | permissionless within wallet | permissionless within wallet | semi permissionless |
| Pegged to | BTC | BTC | SNX | BTC | BTC | BTC | BTC |
| Current Type of Distribution | fully decentralized | fully decentralized | fully decentralized | centralized | centralized | centralized | semi-centralized consortium |
| External Relations | none | MakerDAO fees and ETH to BTC ratio | synthetic network token ratio | none | none | none | none |

**Table 7: Rating of Tokenization Projects for Software Solutions**

| | renBTC | tBTC | sBTC | pBTC | imBTC | HBTC | WBTC |
|---|---|---|---|---|---|---|---|
| 0.100 | 0.113 | 0.009 | 0.013 | 0.001 | 0.008 | 0.039 | 0.817 |
| 0.200 | 1.000 | 1.000 | 1.000 | 0.500 | 1.000 | 1.000 | 1.000 |
| 0.250 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 0.500 |
| 0.200 | 1.000 | 1.000 | 0.000 | 1.000 | 1.000 | 1.000 | 1.000 |
| 0.150 | 1.000 | 1.000 | 1.000 | 0.250 | 0.250 | 0.250 | 0.500 |
| 0.100 | 1.000 | 0.250 | 0.500 | 1.000 | 1.000 | 1.000 | 1.000 |
| Score | 0.911 | 0.826 | 0.651 | 0.688 | 0.788 | 0.791 | 0.782 |

***Conclusion***

The projects always need to be permission-less so that they can be used within autonomous software. Secondly, they must peg to Bitcoin. The main release that went through audits is also essential to use such software in production. Other specifications are less relevant but also neat to look at if multiple solutions accomplish equal scores.

Ren Project and Keep Network both take leading positions. That is the reason why they will be compared separately from others within chapter 5.4.3.

### 5.4.1 Trust Analysis

Trust is the most important key point when looking at stable coin approaches in general. When looking at trustworthiness, there are simple factors that give a rating:

*I. Custody*

*II. Consensus*

*III. Backing Mechanism*

*IV. Backing Type*

*V. Governance*

*VI. Price Feed*

**Table 8: Comparing of Tokenization Projects on Trust**

| | renBTC | tBTC | pBTC | sBTC | imBTC | HBTC | WBTC |
|---|---|---|---|---|---|---|---|
| Custody | non-custodial smart contracts without admin right | non-custodial smart contracts with admin key to pause the network for ten days, delay fee rate settings, or change lot sizes and collateral threshold | non-custodial smart contracts with admin key to upgrade, the goal is a shared key within a DAO that manages updates, trust relies on TEE producer | non-custodial smart contracts with admin key to the SNX network, which is fully upgradable on its own | startup TookenIon with low to moderate risk maintaining custody and proofs reserve | tremendous Asian crypto exchange service maintaining custody and proofs reserve | digital asset custodian BitGo who has more than one billion USD under custody and proofs reserve |
| Consensus | validators enter with 100,000 REN collateral to sign transactions via multi-party ECDSA threshold and Shamir´s Secret Sharing | validators enter with 150% of BTC value collateralized in ETH to sign transactions via multi-party ECDSA threshold | validators run trusted execution environments and coordinating transactions via threshold signature schemes | participants use the synthetic asset issuance protocol, tokenizing is done by smart contracts using over-collateralized tokens | one custodian controls bond to blockchains, smart contracts realize peg-in and peg-out | one custodian controls bond to blockchains, smart contracts realize peg-in and peg-out | BitGo controls bond to blockchain, peg-in and peg-out is initiated from registered merchants with KYC and AML |
| Backing Mechanism | fully collateralized by BTC | fully collateralized by BTC | fully collateralized by BTC | over-collateralized by 800% SNX | fully collateralized by BTC | fully collateralized by BTC | fully collateralized by BTC |
| Backing Type | IOU | IOU | IOU | synthetic | IOU | IOU | IOU |
| Governance | decentralized network of validators | migrating from a semi-decentralized system of validators moving to decentralized | migrating from centralized validator to DAO-based network | migrating from centralized to SNX-holders-based | trusted central custodian | trusted central custodian | trusted federation |
| Price Feed | calculated from a formula which dynamically adjusts by minting and burning fees | semi-centralized price feed from external MakerDAO members | no price feed because bond and slashing amounts are not proportional to BTC | managed by a centralized closed source oracle system | no price feed, because centrally controlled bridge in between | no price feed, because centrally controlled bridge in between | no price feed, because centrally controlled bridge in between |

Fully decentralized approaches have a considerable advantage in trust, giving Ren Project and Keep Network a vast leap forward. Also, WBTC is a consortium of big tech giants within the crypto space- giving good trust by involving KYC and AML. Trusted Environments like pBTC may take the lead when it comes to fees but currently still rely on one validator.

### 5.4.2 Scalability Analysis

Scalability is another essential point when looking at the throughputs of such solutions if specific economic fields like the financial market plan to integrate them. The reason being, that second layer technology on Ethereum can only be used after tokenization. Those solutions still need to maintain full mint-, burn- and security functionality. There are simple factors that give a rating:

*I. Type of Permission*

*II. Scalability Mechanism*

*III. Peg-in and Peg-out Speed*

*IV. Peg-in and Peg-out Costs*

*V. Liquidity*

**Table 9: Comparing of Tokenization Projects on Scalability**

| | renBTC | tBTC | pBTC | sBTC | imBTC | HBTC | WBTC |
|---|---|---|---|---|---|---|---|
| Type of Permission | permission-less | permission-less | permission-less | permission-less | permission-less within wallet | permission-less within wallet | semi-permissioned |
| Scalability Mechanism | scales ok, but the network is always bound to participants that are willing to bond REN, maximum nodes: 10,000 | scales good, but the system is always attached to participants that are willing to bond ETH, maximum nodes: until ETH shortage | scales fine because it is permission-less and not bound to some value | scales ok, constrained by the synthetic supply within the network and the value of SNX tokens | scales fine because it is permission-less and not bound to some value | scales fine because it is permission-less and not tied to some value | Scales well because merchants can initiate minting and hand tokens to users with a pyramid-like concept |
| Peg-in and Peg-out Speed | instantly after the transaction is complete | relatively fast, slowed by additional non-fungible token | Instantly after the transaction is complete | relatively quickly, due to Synthetix´s protocol | instantly after the transaction is complete | instantly after the transaction is complete | up to 48h with manual approval, but shorter once a customer is known |
| Peg-in and Peg-out Costs | very low | relatively high gas prices | very low | relatively high gas prices | medium | medium | very low |
| Liquidity | high due to low costs and instant speed | medium due to gas-costs | high if decentral and low costs, currently only medium due central validator | low because of the parallel synthetic market | medium due to costs and central instance | medium due to costs and central instance | low due to speed |

There are scalability issues for Ren Project, Keep Network, and Synthetix because of their decentralization. However, Ren Project can convince with liquidity, speed, and costs. Trusted enclaves surpass all others in terms of the combination of scale and fees. However, there is no decentralized solution for it. Where signing-group approaches have their risk on cryptography, TEE´s have the risk related to hardware exploits.

### 5.4.3 Decentralized Tokenization

Comparing the two main decentral networks that are out there, taking the leading positions within the tokenization technology, there are many more properties to look at.

As known, the backing mechanism is the spine of such networks. Keep Network can scale much more initially because operators of nodes have a lot of ETH to bond. They need to bond 150% of the initial Bitcoin value, due to signer groups only consisting of 3 people.

$$bind\ ratio = \frac{\left[\frac{current\ market\ cap\ of\ ETH\ in\ USD}{collateral\ in\ percent * 0.01}\right]}{current\ market\ cap\ of\ BTC\ in\ USD}$$

$$bind\ ratio = \frac{\left[\frac{66325718857}{1.5}\right]}{344836056447} = 0.1282\ldots$$

With signing groups of 3, Keep Network could theoretically bind more than 12% of all Bitcoins. All tokenizing projects on Ethereum together currently only scratch the mark of 0.8% locked. There are two options to overcome not being able to maintain security for all Bitcoins: speculating that the market cap will increase or lowering the collateral needed in percent. Following the simple formula by which collateral is calculated:

$$collateral\ in\ percent = \left[\frac{signers\ per\ group}{signers - 1}\right] * 100$$

If Keep Network is going on the maximum capacity of 80 signers per group, the collateral being needed if someone steals the Bitcoin could reduce to roughly 101.27%, which sums up to about nearly 19% of all Bitcoins.

$$collateral\ in\ percent = \left[\frac{80}{79}\right] * 100 = 101.2658\ldots$$

$$bind\ ratio = \frac{\left[\frac{66325718857}{1.012658}\right]}{344836056447} = 0.1899\ldots$$

Both solutions use a much more complicated formula for nodes, including statistics of frauds to decrease the ratio. Within the podcast “Unchained - Ep. 169”, Matt Luongo, founder of the Keep Network, talks about future versions that could reduce the binding ratio to only 30%. [85] Recalculated, that means 64% of all Bitcoin could be locked without a further redo. While the rate is always related to Bitcoin's full supply, analysis done by Chainalysis suggests that there are lost Bitcoins in the range from 2 to 3.7 million. The shortage would resolve in higher percentages of assets that can be tokenized. [32]

Ren Project provides an even higher number of signers that can be managed per group. At the moment of writing, the price of the REN token is about 0.35 USD. To operate a Darknode, 100,000 REN are needed, which resolves in about 35,000 USD. With 1,463 nodes running, the network is currently utilized by 14%, with about 17,000 BTC. Scaling linearly, it settles in a maximum of 122 thousand Bitcoins if there would not be dynamically adaptions to REN's value. If the network cannot maintain the value that it locked in Bitcoin, nodes will be incentivized to steal. [84]

While Keep Network can scale up a lot faster instantly, just by creating nodes, the downside is that it's locking up valuable Ether, lowering liquidity on Ethereum. The Ethereum blockchain would be staking up huge collateral in Ether just to maintain security. When there are many massive price fluctuations from the Bitcoin to the Ethereum blockchain, Keep Network will also have stability issues from nodes not being available. Due to the security approach being copied from a synthetic-like system, most nodes would have to move into the liquidation process to prevent under-collateralization from price drops. Still, then it lowers the number of nodes available for signer groups. If a certain number of nodes is stuck, putting up more collateral to operate secure again, the network may not handle the workloads.

On the other hand, Ren Project has issues at the start, raising enough value to the REN token, securing the network, and acting slower than Keep Network. The value will rise with transactions and secured assets because of its bond to the virtual machine. Where Ren Project is significantly faster than Keep Network is on the peg-in and peg-out speeds. While Keep uses a non-fungible token to assign the user right of the deposit to the user group, this process is obsolete within Ren because the network combines both deposit steps into one, creating only two instead of three transactions. Ren Project can also calculate fees directly within the system because it is bound to REN's value, where Keep Network involves external sources to estimate costs for them. Ren is currently maintaining low fees of 0.2% mint and 0.1% burn (meaning there is more input than output, presently). In perspective, you can tokenize 5 euros worth of BTC for only 1 cent, excluding mainchain transaction costs.

Ren can also calculate all network fees on a dynamic, fully algorithmic level to maintain the network's REN value, while Keep relies on external sources. Third-party suppliers could become a problem. If there are transaction fluctuations, Keep would need to intervene manually with their development rights. It is also to mention that Ren project is the only fully decentralized solution at the moment.

### 5.4.4 Evaluation

Looking at the backing type, all solutions excluding Synthetix rely on IOU, meaning that real Bitcoins are locked to gain usability of personally owned Bitcoins on Ethereum. Viewing the governance of the remaining approaches, only Ren is fully decentralized from the beginning. Keep and pTokens plan to move from federated- to decentralized in the future, but all others probably remain a trusted federation or centralized. Even though centralized institutions seem like safe custody and have no price feeds, the type contradicts blockchain principles in general.

Within three months after their release, Ren Project has caught up to more than a third of WBTC holdings and may overtake them as the first fully decentralized project running tokenized Bitcoins on Ethereum. Keep Networks had a rough start but are now live again, acting as an opponent to Ren. Comparing it to Ren Project, it is still the more complicated solution facing fees and liquidation but offering much more scalability to tokenize huge chunks of Bitcoins. Both can grow within the developer space using it in autonomous software and get a lot of application support in the long run. The imTokens and HBTC projects will probably remain as long as they are used in their big exchange wallets with less potential to grow for the mass. Leaving Synthetix for crypto stock exchange traders as a user group and WBTC as the first tokenizing project and current leader on Ethereum, where individuals can lock and redeem with good conscience involved KYC and AML processes.

# 6 Demonstration

This bachelor thesis was supervised by Blockchains LLC, a company aiming to revolutionize safe asset management, including identity. Bringing back power to the users with the help of blockchain technology is one of their guiding principles. But creating a secure entry to Web 3 for everyone by developing digital asset custody and digital identity is not a simple task. To fulfill its goal, the company acquired Slock.it GmbH in May 2019.

When trying to build blockchain-infrastructures, it is almost essential to make the product connect with every device. This demand is mostly coming from the emerging IoT economy and self-sovereign infrastructures. [86] Slock.it´s vision was to make blockchain technology accessible for such small IoT devices. Enabling anyone to rent, sell or share their properties without an intermediary when their software called IN3 can be embedded on microcontrollers connected to cars, homes, or other shared goods is a massive step for the ecosystem. The client itself can do all verifications. [87] Blockchains IN3 will serve as a safe connection to read blockchain-related data from smartphones within future software solutions. Those could then create a whole ecosystem for IoT, self-sovereign asset management, payment, and secure wallet backups. [6]

When developing applications, where the focus needs to be set for outstanding usability, tokenization can be beneficial. The user experience needs to be catchy, intuitive, and plausible to be used by the majority. Tokenization offers the possibility to have assets across chains within a single wallet sitting on one blockchain to be used in smart contract applications. This chapter focuses on the implementation concepts featuring a standalone prototype wallet add-on, interacting with MetaMask.

## 6.1 State of Mobile Development

The asset management solution of Blockchains is currently in the process of development. The structure of the application, which combines asset management, IN3 verifications, key backups, and tokenization with the main wallet, can be seen as the following:

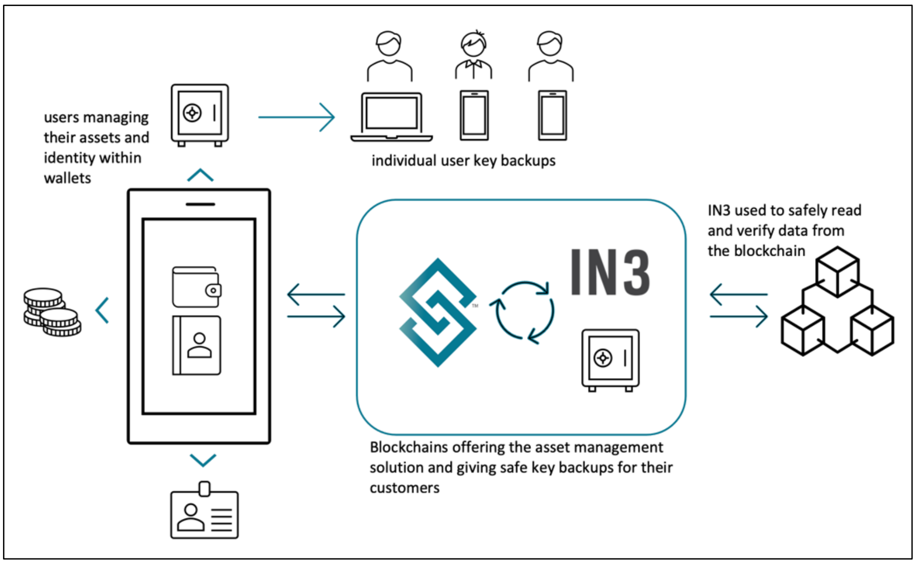

users managing their assets and identity within wallets
individual user key backups
IN3 used to safely read and verify data from the blockchain
IN3
Blockchains offering the asset management solution and giving safe key backups for their customers

**Figure 3: Mobile Asset Management Application - Layout**

As described in chapter 5, Ren Project was chosen for being the currently most successful solution. However, there is no direct support for custom wallets like the one in development. At the moment, they only feature support for MetaMask, which is a wallet solution used in the browser. It can be connected easily on mobile, but then, the user would need to install both apps and always switch to make transactions. The other relevant player, Keep Networks, only offers native support for existing wallets like MetaMask, Ledger Legacy, Ledger Live, and Trezor. It is not a coincidence that all wallets are working with the browser. Both JavaScript libraries are currently only available to be compiled and run within the browser and native smartphone applications.

Within their developer channels, it has been discussed that there are plans to work on mobile-device compatibility after they reached a more stable state. Both projects went live this summer, so there is much more on their tables to focus on. In the case of RenProject, they are releasing more support for other blockchains where their network can dock onto. Within the project “Multichain,” developers will soon connect to any blockchain using their interface. Keep Network is still working on its node system. But the initial interoperability problem doesn’t come from them specifically. The issue is related to web 3 libraries for JavaScript. Both and almost every other blockchain project running on JavaScript is using them. It can be challenging to port the library, adding support for mobile, or create workarounds. This leaves three main problems:

I. No guidance or support for custom wallets other than MetaMask
II. No support for mobile builds due to JavaScript libraries
III. No support for test networks other than Kovan

The first problem could be solved by reverse engineering how the MetaMask wallet is communicating with RenProject. This would be relatively easily because MetaMask is fully open source but would not help due to the second dilemma. Until libraries are not natively working with mobile devices, they would need to be rebuilt on a machine for the browser environment and inserted into the smartphone's mobile build. Within Blockchains LLC, such prebuild attempts are common in the current state because there is a lack of compatibility but emerging demand to create new software.

The decision here is to create meaningful software with the best technologies that deliver good support, rather than delaying development until excellent support is patched. With this approach, the lead over other projects can be extended.

The last problem arose from the fact that not everything is entirely open-source within guidance. While the code of Ren Project´s Registry is available in public, it cannot just be ported to any other blockchain due to some relations to other smart contracts. By the end of this year, their code will be completely open-source with full documentation. It correlated with their project named “Multichain,” which will be the next big release that will give developers full functionality on their tokenizing libraries. But at the current state, that would´ve included swapping the existing developing test networks from Goerli to Kovan, including the change of all bindings to the different chain.

All issues were faced at an early stage. Due to the fact, that library incompatibilities could not be resolved with prebuilds, and the prototype could not be implemented directly into the asset management wallet without going into in-depth development, the decision was made to program the prototype within the browser to showcase the functionalities outside the mobile application.

## 6.2 Implementing Ren Project

The implementation of the wallet extension described within the next chapters can be found on GitHub, a service known for hosting software development based on source code management and version control. [91]

When it comes to the implementation, Ren offers two different libraries for the programming language JavaScript. Both target other user groups.

I. GatewayJS
II. RenJS

While GatewayJS is the easy but heavy weighted way of tokenizing, RenJS focuses on developers who want specific customization and efficiency. GatewayJS offers already implemented local storage, an excellent user interface, animations, and parallel tokenizing transactions, which can be directly imported to your web application. Because RenProject may run in future Blockchains software with its corporate design and custom storage solutions for more security, the light weighted version RenJS was chosen.

To generate the JavaScript application, the user-interface software environment React comes in handy. React and React Native can be seen as common standards while working with browser- or native mobile applications. It offers excellent functionality to combine functions with essential user interface elements. It comes with terminal commands and listener functionality, which enables programming while the application is running to directly see changes. The architecture of the app can be seen in the next figure.

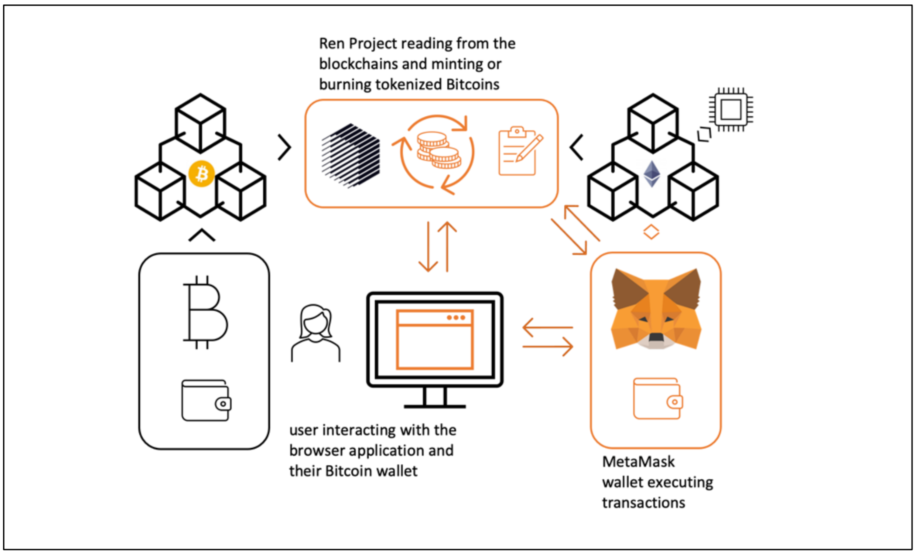

Ren Project reading from the blockchains and minting or burning tokenized Bitcoins
user interacting with the browser application and their Bitcoin wallet
MetaMask wallet executing transactions

**Figure 4: Browser Wallet Extension – Layout**

## 6.3 Solidity Contract

The main solidity contract is deployed to the Ethereum Kovan Testnet. It´s the bridge from the app to the Ren Network. The contract needs to feature three functions to enable the most basic transactions within the wallet. This contract can be expanded with functions to fulfill the developer's approaches to save bandwidth when interacting with the blockchain. The code of the contract can be found in the Appendix, Part 2.

I. deposit (sending BTC to custom address, minting renBTC for it)
II. withdraw (burning renBTC, receiving BTC on custom address for it)
III. balance (receiving the current balance of renBTC on Ethereum)

## 6.4 React Wallet

The wallet itself is working within the browser and can be implemented in any web service. The application is running as a local server and can be accessed by localhost.

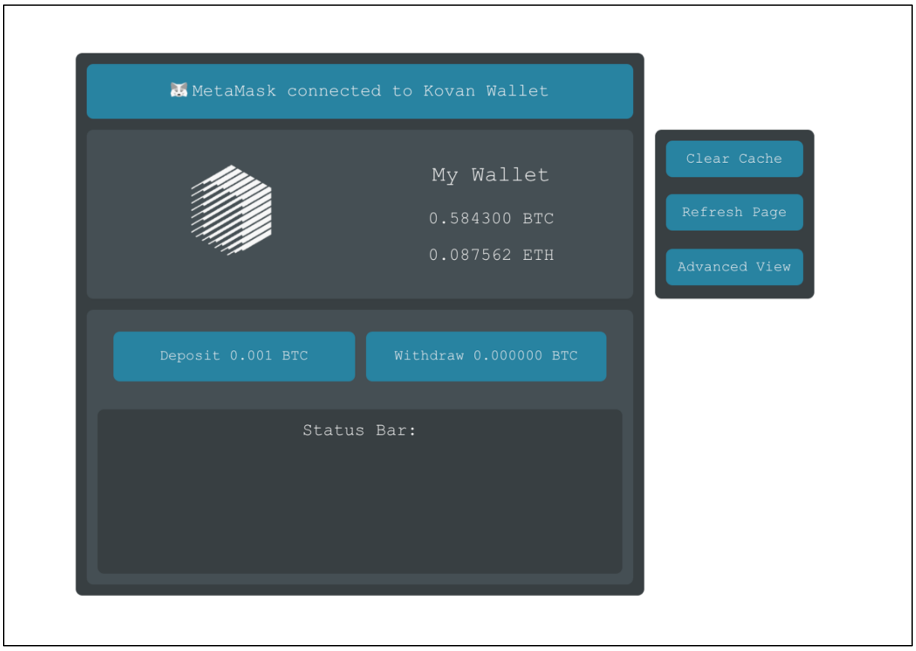


**Figure 5: Wallet Showcase - Regular View**

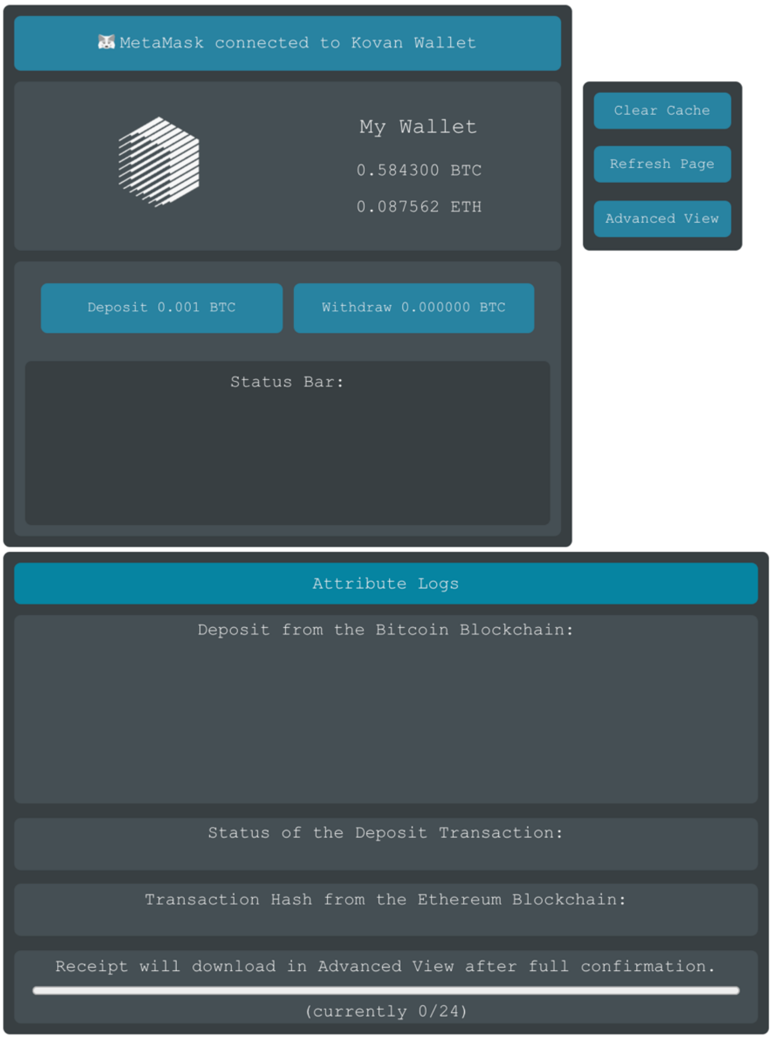
The application's front end contains the main wallet extension for MetaMask and a docked settings window on the right side where the user can refresh the page, clear the current transaction, or get into the advanced view. The primary wallet extension is split up into two parts:

### *Wallet Status*

The wallet status features the current balances of Bitcoin and Ether hold by the user within the Ethereum blockchain. The status bar on the top indicates the connection to MetaMask and serves as communication for the user.

### *Ren Interaction*

This section features to deposit Bitcoin from the Bitcoin blockchain or withdraw Bitcoin from the Ethereum blockchain. If there is a pending transaction, the Logo in the application is starting to pulse. In both cases, the transaction is saved within the local storage of the browser. The status bar will update the user with information on the current action. It can show the current state of the pending transaction or if errors occurred.



MetaMask connected to Kovan Wallet

My Wallet

0.584300 BTC

0.087562 ETH

Status Bar:

Attribute Logs

Deposit from the Bitcoin Blockchain:

Status of the Deposit Transaction:

Transaction Hash from the Ethereum Blockchain:

Receipt will download in Advanced View after full confirmation.

(currently 0/24)

**Figure 6: Wallet Showcase - Advanced View**

Within the advanced view, the user can gather all the metadata that will be transferred and download the final Ethereum transaction recipe. The recipe includes information on the deposit transaction and the Ethereum transaction for minting the new Bitcoin.

## 6.5 Future Development

As already teased at the start of the implementation, tokenizing technologies are just at the starting point of decentralization and become used within applications on every device type. As soon as the current issues can be bypassed, Ren Project will be implemented in a wide variety of mobile applications.

When this state of development is reached, it would be great to integrate it into the asset management wallet from Blockchains LLC. The application will help people to transition into the self-sovereign blockchain space by offering a user-friendly asset service and providing top usability for all their different currencies, rights, and identity- securely backed up. Storing the pending transaction needs to be reworked within this step to gain more security. Any persistent storage could be used, including a standard database.

# 7 Conclusion

Cross-chain tokenizing technologies, in general, are currently in tremendous growth, and there are different solutions for covering various use cases- either directly to be used by enthusiasts or implemented within wallets as backend software. The approaches on Ethereum are either used to increase interest for wallets or stock exchanges but can also be used within decentralized financial markets. Within the future, it will need decentralized tokenization to be viable with smart contract trading or any other application requiring tokenized Bitcoin as input for autonomous software. Such decentralized projects are just in their starting area, defining new concepts on bypassing central custodians, lowering fees, or making them scale well.

The research and comparisons lead to the result that Ren Project is currently the best practice solution for autonomous software development. Others either lack decentralization, real Bitcoin backing, permission-less interaction or network stability on price fluctuations. This mirrors the market growth of Ren Project. At the moment, all projects try to gain trust from the first wave of users- and therefore use a lot of collateral. Within the future, there will be new fraud-proof schemes to reduce the security collateral of such decentralized versions, requiring only a glimpse of what they currently need. More supported chains and usable devices for programmers will also evolve after a solid userbase grew, and bigger networks are reached. Such wide-range concepts are already in the making: Ren Project leaps forward again by not only providing compatibility to big chains like Bitcoin, Bitcoin Cash, Zcash, or Ethereum but also allowing developers to build their bridges based on their open-source software development kits.

It is also a tremendous goal to connect current blockchains and intergrade those tokenizing technology into superordinate chains, second layer solution, and identity applications to ignite the real potential and show actual applications outside from the decentralized financial space. Therefore, it is essential to keep researching tokenizing projects while building asset management solutions like Blockchains LLC. Using prototypes like the one provided within this bachelor thesis is always an excellent way to compare technical differences and find fitting solutions. This strategy also creates a modularity mindset, utilizing itself in code, making programs more efficient and comfortable, while always relying on the best-in-case software.

# References

[1] Hype Cycle for Blockchain Technologies, 2020. (n.d.). Gartner. Retrieved November 24, 2020, from *https://www.gartner.com/en/documents/3987450/hype-cycle-for-blockchain-technologies-2020*

[2] CoinMarketCap. (n. d.). Cryptocurrency Market Capitalizations. Retrieved November 24, 2020, from *https://coinmarketcap.com*

[3] Blockchain: Everything You Need to Know. (n. d.). Retrieved November 24, 2020, from *https://www.investopedia.com/terms/b/blockchain.asp*

[4] Antonopoulos, A. M., & Klicman, P. (2018). Bitcoin - Grundlagen und Programmierung. Weinheim, Germany: Beltz Verlag. Pages [1] 15 ff., 197 ff. [2] 1, 4, 15 ff., 173 ff., 215 ff., 290

[5] BLOCKCHAIN AND FINANCIAL MARKET INNOVATION. (n. d.). Retrieved November 24, 2020, from *http://www.jpmcc-gcard.com/wp-content/uploads/2019/03/GCARD-Summer-2019-Chicago-Fed.pdf*

[6] A Peer-to-Peer Electronic Cash System. (n. d.). Retrieved November 24, 2020, from https://bitcoin.org/bitcoin.pdf

[7] Antonopoulos, A. M., Wood, G., & Klicman, P. (2019). Ethereum - Grundlagen und Programmierung. Weinheim, Germany: Beltz Verlag. Pages 6, 9, 127 ff., 221 f.

[8] Ethereum whitepaper - whitepaper.io. (n. d.). Retrieved November 24, 2020, from *https://whitepaper.io/document/5/ethereum-whitepaper*

[9] Ethereum Book. (n. d.). ethereumbook/ethereumbook. Retrieved November 24, 2020, from *https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc*

[10] Hoffman, C. (2018, May 8). What is Ethereum, and What Are Smart Contracts? Retrieved November 24, 2020, from *https://www.howtogeek.com/350322/*

[11] The Blockchain Trilemma. (2019, October 4). The Blockchain Trilemma: Decentralized, Scalable, and Secure? Retrieved November 24, 2020, from *https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3*

[12] What are Sidechains? | Hacker Noon. (n.d.). Retrieved November 24, 2020, from *https://hackernoon.com/what-are-sidechains-1c45ea2daf3*

[13] State Channels. (n. d.). Retrieved November 24, 2020, from *https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/state-channels/*

[14] Plasma: Scalable Autonomous Smart Contracts. (n. d.) Retrieved November 24, 220, from *https://plasma.io/plasma.pdf*

[15] Optimistic vs. ZK Rollup: Deep Dive - Matter Labs. (n.d.). Medium. Retrieved November 24, 2020, from *https://medium.com/matter-labs/optimistic-vs-zk-rollup-deep-dive-ea141e71e075*

[16] Understanding Payment Channels. (n.d.). Retrieved November 24, 2020, from *https://blog.chainside.net/understanding-payment-channels-4ab018be79d4*

[17] Raiden Network. (n. d.). Retrieved November 24, 2020, from *https://raiden.network*

[18] Raiden 101. (n. d.) Retrieved November 24, 2020, from *https://raiden.network/101.html*

[19] Raiden Network Nightly Documentation. (n. d.). Retrieved November 24, 2020, from https://raiden-network.readthedocs.io/en/stable/

[20] mimblewimble/docs. (n.d.). GitHub. Retrieved November 24, 2020, from *https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin*

[21] mimblewimble/grin. (n.d.). GitHub. Retrieved November 24, 2020, from *https://github.com/mimblewimble/grin*

[22] Voshmgir, S. (2020). Token Economy: How the Web3 reinvents the Internet (Second Aufl.). Shermin Voshmgir, BlockchainHub Berlin. [1] 27 ff., 32 ff. [2] 84 ff. [3] 95 ff. [4] 152 ff. [5] 190 ff.

[23] The Evolution of the Internet, Identity, Privacy and Tracking – How Cookies and Tracking Exploded, and Why We Need New Standards for Consumer Privacy – IAB Tech Lab. (n.d.). IABTechLab. Retrieved November 24, 2020, from *https://iabtech-lab.com/blog/evolution-of-internet-identity-privacy-tracking/*

[24] General Data Protection Regulation (GDPR) Compliance Guidelines. (n.d.). GDPR.Eu. Retrieved November 24, 2020, from *https://gdpr.eu/*

[25] Bernet, D. (Director). (2015). Democracy [Documentary]. INDI FILM.

[26] Interplanetary File System. (n. d.) Retrieved November 24, 2020, from *https://ipfs.io*

[27] Not Your Keys, Not Your Coins: Why It Matters. (n.d.). Ledger. Retrieved November 24, 2020, from *https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters*

[28] The Various types of Crypto Tokens - Medipedia. (n.d.). Medium. Retrieved November 21, 2020, from *https://medium.com/@medipedia/the-various-types-of-crypto-tokens-26bab8f6622c*

[29] Three types of cryptocurrency tokens explained as quickly as possible. (n.d.). Hard Fork | The Next Web. Retrieved November 21, 2020, *from https://thenextweb.com/hard-fork/2018/11/19/cryptocurrency-tokens-explained/*

[30] Internet of Blockchains Explained. (n. d.). Retrieved November 24, 2020, from *https://perfectial.com/blog/internet-of-blockchains/*

[31] Types of Computer Network - javatpoint. (n.d.). Retrieved November 24, 2020, from *https://www.javatpoint.com/types-of-computer-network*

[32] The Importance of Cross-Chain Solutions in the DeFi Economy | Hacker Noon. (n.d.). Hackernoon. Retrieved November 23, 2020, from *https://hackernoon.com/the-importance-of-cross-chain-solutions-in-the-defi-economy-5en3w9a*

[32] Bitcoin’s $30 billion sell-off. (n.d.). Lost Bitcoin Analysis from Chainalysis. Retrieved November 24, 2020, from *https://blog.chainalysis.com/reports/money-supply*

[33] J. (2020, February 28). Wanchain - Decentralized Finance Interoperability. Retrieved November 24, 2020, from https://www.wanchain.org

[34] S. (2019, June 18). 5 Top Internets For Blockchains- The Capital. Retrieved November 24, 2020, from *https://medium.com/the-capital/aion-cosmos-icon-polkadot-wanchain-connecting-blockchains-55a2e80dbd27*

[35] Wanchain Whitepaper EN Version. (n. d.). Retrieved November 24, 2020, from *https://wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf*

[36] The Open Application Network. (n. d.). Retrieved November 24, 2020, from *https://theoan.com*

[37] Spoke, M. (2019, November 4). The Unintended Consequences of Platform Economies - The OAN. Retrieved November 24, 2020, from *https://medium.com/theoan/the-unintended-consequences-of-platform-economies-b40f36f97db1*

[38] Aion whitepaper - whitepaper.io. (n.d.). Retrieved November 24, 2020, from *https://whitepaper.io/document/31/aion-whitepaper*

[39] Cosmos Network - Internet of Blockchains. (n.d.-b). Retrieved November 24, 2020, from *https://cosmos.network/resources/whitepaper*

[40] ICON. (n.d.). Retrieved November 24, 2020, from *https://icon.foundation/?lang=en*

[41] ICON Whitepaper. (n. d.). Retrieved November 24, 2020, from *https://icon.foundation/resources/whitepaper/ICON_Whitepaper_EN.pdf*

[42] Polkadot: Decentralized Web 3.0 Blockchain Interoperability. (n. d.). Retrieved November 24, 2020, from https://polkadot.network

[43] Wiki Index · Polkadot Wiki. (n.d.). Retrieved November 24, 2020, from *https://wiki.polkadot.network/docs/en/*

[44] What Are Atomic Swaps? (n.d.). Retrieved November 24, 2020, from *https://www.investopedia.com/terms/a/atomic-swaps.asp*

[45] Atomic swap - Bitcoin Wiki. (n.d.). Retrieved November 24, 2020, from *https://en.bitcoin.it/wiki/Atomic_swap*

[46] Ks, K. (2018, November 12). Atomic Swaps – Trade Between Two – BitcoinWiki. Retrieved November 24, 2020, from *https://en.bitcoinwiki.org/wiki/Atomic_Swap*

[47] C. (2019, June 13). What is Tokenization? Everything You Should Know – CoreLedger. Retrieved November 24, 2020, from *https://medium.com/coreledger/what-is-tokenization-everything-you-should-know-1b2403a50f0e*

[48] O'Neal, S. (2019, June 2). Tokenization, Explained. Retrieved November 24, 2020, from *https://cointelegraph.com/explained/tokenization-explained*

[49] Token Swaps and Atomic Swaps Explained. (2018, July 25). Retrieved November 24, 2020, from *https://blockwolf.com/token-swaps-and-atomic-swaps-explained/*

[50] Wrapped Tokens Whitepaper. (n. d.). Retrieved November 24, 2020, from *https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf*

[51] Tether Whitepaper. (n. d.). Retrieved November 24, 2020, from *https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf*

[52] TrueToken Whitepaper. (n. d.). Retrieved November 24, 2020, from *https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/true-usd-whitepaper.pdf*

[53] USDC Whitepaper. (n. d.). Retrieved November 24, 2020, from *https://crypto-actu.com/wp-content/uploads/2018/12/WhitePaper.pdf*

[54] What's the Maximum Ethereum Block Size? (n.d.). ETH Gas Station. Retrieved November 24, 2020, from *https://ethgasstation.info/blog/ethereum-block-size/*

[55] avg-block-size. (n.d.). Blockchain.Com. Retrieved November 24, 2020, from *https://www.blockchain.com/de/charts/avg-block-size*

[56] BTC on Ethereum. (n.d.). Retrieved November 24, 2020, from *https://btconethereum.com*

[57] Russo, C. (2020, April 20). It Was Almost Impossible to Keep Up With all the Bitcoin-on-Ethereum Efforts —Until Now. Retrieved November 24, 2020, from *https://thedefiant.substack.com/p/it-was-almost-impossible-to-keep-26b*

[58] WBTC Wrapped Bitcoin an ERC20 token backed 1:1 with Bitcoin. (n.d.). Retrieved November 24, 2020, from *https://wbtc.network/*

[59] Wrapped Tokens. (n. d.). Retrieved November 24, 2020, from *https://www.wbtc.network/assets/wrapped-tokens-whitepaper.pdf*

[60] Tokenlon - An easy-to-use cryptocurrency DEX. (n.d.). Retrieved November 24, 2020, from *https://tokenlon.im/*

[61] Things, P. (2020, April 23). pTokens launch on mainnet! - Provable. Retrieved November 24, 2020, from *https://medium.com/provable/ptokens-launch-on-mainnet-8c0a0cffa24f*

[62] pTokens DApp. (n.d.). Retrieved November 24, 2020, from *https://dapp.ptokens.io/*

[63] Provable pTokens. (n. d.). Retrieved November 24, 2020, *from https://ptokens.io/ptokens-rev5b.pdf*

[64] AsyncShock: Exploiting Synchronisation Bugs in Intel SGX Enclaves. (n. d.). Retrieved November 24, 2020, from *https://www.ibr.cs.tu-bs.de/users/weichbr/papers/esorics2016.pdf*

[65] Synthetix | Decentralised synthetic assets. (n.d.). Retrieved November 24, 2020, from *https://www.synthetix.io/litepaper/*

[66] Synthetix. (n.d.). Retrieved November 24, 2020, from *https://www.synthetix.io*

[67] HBTC (n. d.). Huobi Bitcoin. Retrieved November 24, 2020, from *https://www.hbtc.finance/static/pdf/whitepaper-en.pdf*

[68] Official Launch Of Huobi BTC (HBTC) On Ethereum Network. (n.d.). Retrieved November 24, 2020, from *https://huobiglobal.zendesk.com/hc/en-us/articles/900000196603-Official-Launch-Of-Huobi-BTC-HBTC-On-Ethereum-Network*

[69] Huobi Center. (n.d.). Retrieved November 24, 2020, from *https://www.huobi.fm/*

[70] Bitcoin on Ethereum. (n.d.). Retrieved November 24, 2020, from *https://tbtc.network*

[71] tBTC: A Decentralized Redeemable BTC-backed ERC-20 Tokens. (n. d.). Retrieved November 24, 2020, from *https://docs.keep.network/tbtc/index.pdf*

[72] KEEP Network Stakedrop - Chandru. (n.d.). Medium. Retrieved November 24, 2020, from *https://chdru.medium.com/keep-network-stakedrop-3e63355a18ec*

[73] keep.community - Welcome! (n.d.). Keep.Community. Retrieved November 24, 2020, from *https://keep.community*

[74] An Update on tBTC's Launch. (n.d.). TBTC. Retrieved November 24, 2020, from *https://tbtc.network/news/2020-05-22-an-update-on-tbtc%E2%80%99s-launch/*

[75] tBTC Is Live. (n.d.). TBTC. Retrieved November 24, 2020, *from https://tbtc.network/news/2020-09-22-tbtc-is-live/*

[76] tBTC Explorer. (n.d.). Keep Network. Retrieved November 24, 2020, from *https://tbtcexplorer.com*

[78] renproject/ren. (n.d.). GitHub. Retrieved November 24, 2020, from *https://github.com/renproject/ren/wiki#introduction*

[79] L. (2019, December 5). Welcome to the RenVM Developer Center - Ren Project. Retrieved November 24, 2020, from *https://medium.com/renproject/welcome-to-the-renvm-developer-center-c1ade842fe07*

[80] L. (2020, January 17). December Development Update - Ren Project. Retrieved November 24, 2020, from *https://medium.com/renproject/december-development-update-e910df747d38*

[81] Ren Litepaper. (n. d.). Retrieved November 24, 2020, from *https://renproject.io/litepaper.pdf*

[82] Ren. (n. d.). Retrieved November 24, 2020, from *https://renproject.io*

[83] Roundabout Exchange. (n. d.). Retrieved November 24, 2020, from https://roundabout.exchange

[84] Ren Explorer (n. d.). Retrieved November 24, 2020, from *https://mainnet.renproject.io/darknodes*

[85] tBTC: What Happens When the Most Liquid Crypto Asset Hits DeFi? - Ep.169. (n.d.). YouTube. Retrieved November 24, 2020, from *https://www.youtube.com/watch?v=A17BdRDGbHc&ab_channel=UnchainedPodcast*

[86] Pauw, C. (2018, December 4). How Significant Is Blockchain in Internet of Things? Retrieved November 24, 2020, from *https://cointelegraph.com/news/how-significant-is-blockchain-in-internet-of-things*

[87] IN3 Client (n. d.). Retrieved November 24, 2020, from https://www.blockchains.com/our-products/incubed/

[88] blockchainsllc/in3-c. (n.d.). GitHub. Retrieved November 24, 2020, from *https://github.com/blockchainsllc/in3-c*

[89] Blockchains LLC. (n. d.). Retrieved November 24, 2020, from *https://www.blockchains.com*

[90] Welcome. (n.d.). Developers. Retrieved November 24, 2020, from *https://docs.renproject.io/developers/*

***Published Code:***

[91] Ren Wallet Prototype (24.11.2020). GitHub. Retrieved November 24, 2020, from *https://github.com/felixhildebrandt/renwallet*

***Also written within this context:***

[92] Hildebrandt, Felix. Symbiosis in between Blockchains. Internship Report. University of Applied Sciences Mittweida. June 2020. Mittweida.

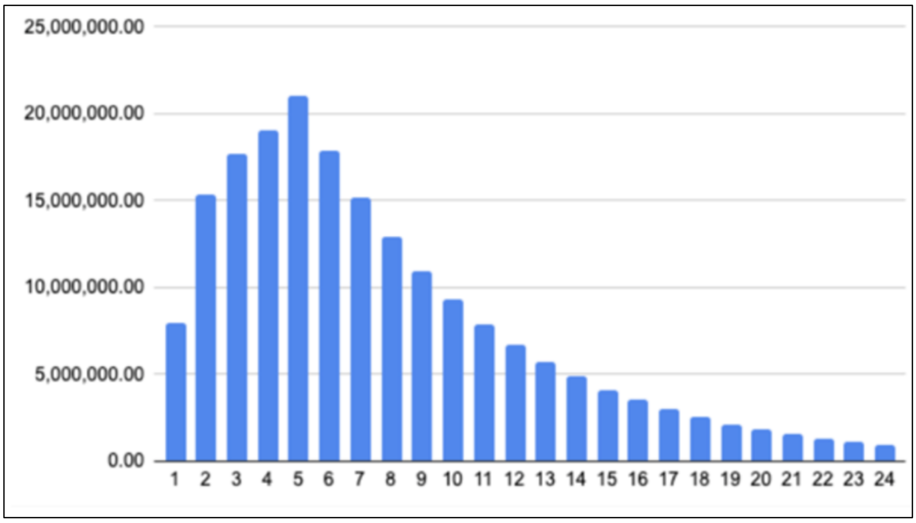
[93] Hildebrandt, Felix. Tokenization and the Symbiosis between Blockchains.
Conference proceedings of the Scientific Track of the BAS 2020.
University of Applied Sciences Mittweida. October 2020. Mittweida.

# Appendix

Part 1 .......................................................................................... A-I

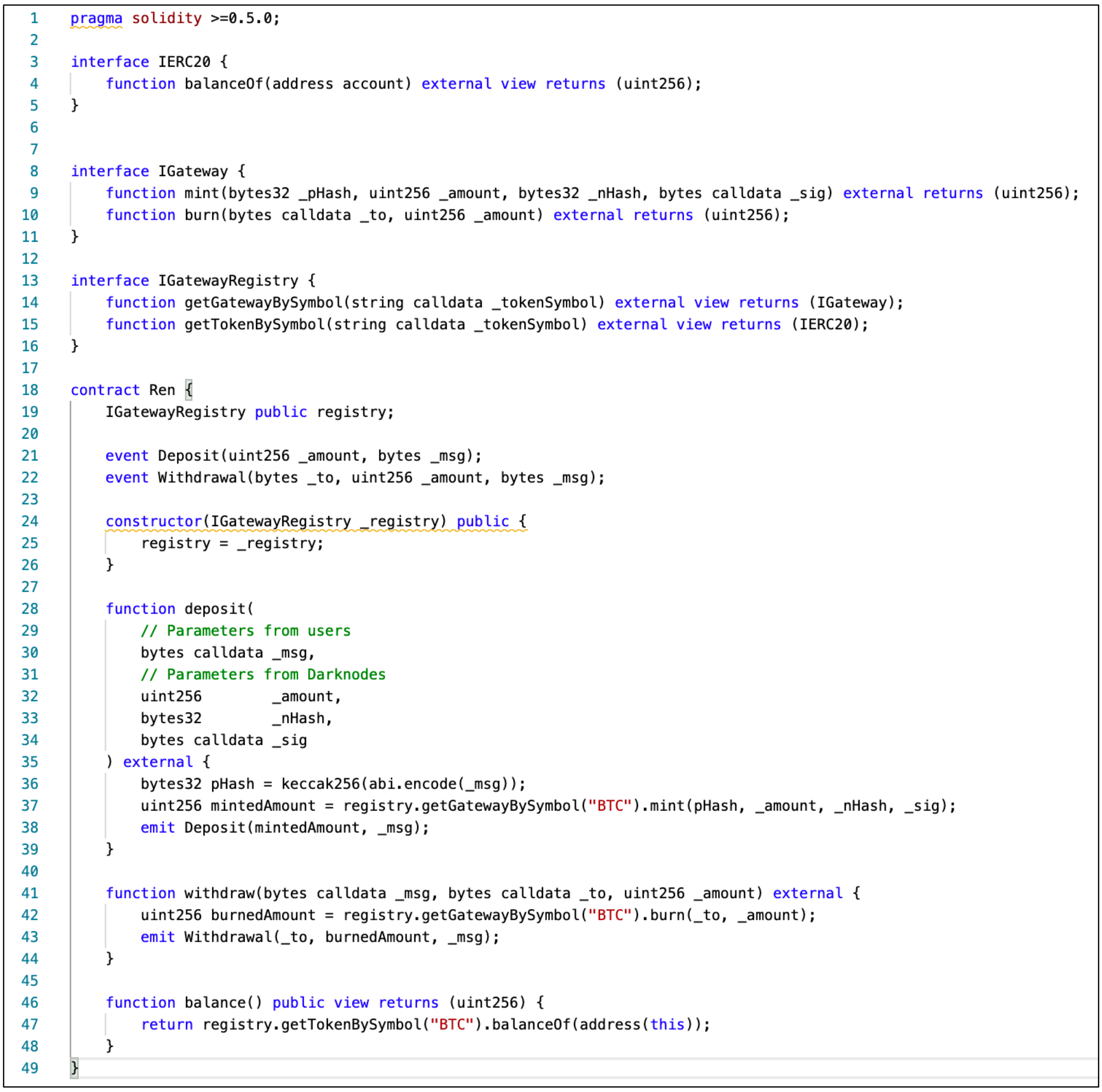
Part 2 .......................................................................................... A-III

# Appendix, Part 1



Distribution Graph of the Keep Network Token as Security for Signer Selection [72]

# Appendix, Part 2



```
pragma solidity >=0.5.0;

interface IERC20 {
    function balanceOf(address account) external view returns (uint256);
}


interface IGateway {
    function mint(bytes32 _pHash, uint256 _amount, bytes32 _nHash, bytes calldata _sig) external returns (uint256);
    function burn(bytes calldata _to, uint256 _amount) external returns (uint256);
}

interface IGatewayRegistry {
    function getGatewayBySymbol(string calldata _tokenSymbol) external view returns (IGateway);
    function getTokenBySymbol(string calldata _tokenSymbol) external view returns (IERC20);
}

contract Ren {
    IGatewayRegistry public registry;

    event Deposit(uint256 _amount, bytes _msg);
    event Withdrawal(bytes _to, uint256 _amount, bytes _msg);

    constructor(IGatewayRegistry _registry) public {
        registry = _registry;
    }

    function deposit(
        // Parameters from users
        bytes calldata _msg,
        // Parameters from Darknodes
        uint256        _amount,
        bytes32        _nHash,
        bytes calldata _sig
    ) external {
        bytes32 pHash = keccak256(abi.encode(_msg));
        uint256 mintedAmount = registry.getGatewayBySymbol("BTC").mint(pHash, _amount, _nHash, _sig);
        emit Deposit(mintedAmount, _msg);
    }

    function withdraw(bytes calldata _msg, bytes calldata _to, uint256 _amount) external {
        uint256 burnedAmount = registry.getGatewayBySymbol("BTC").burn(_to, _amount);
        emit Withdrawal(_to, burnedAmount, _msg);
    }

    function balance() public view returns (uint256) {
        return registry.getTokenBySymbol("BTC").balanceOf(address(this));
    }
}
```

Solidity Contract for Ren Project Browser Wallet Extension [90]

# Declaration of Independence

I declare that I have prepared the present work independently and only using the literature and aids indicated. Parts that have been taken literally or analogously from sources are marked as such. This paper has not yet been submitted in the same or similar form to any other examination office.

Mittweida, 24.11.2020

F. Hildebrandt

Felix Hildebrandt