Use Cases and Design of Web Applications in Decentralized Finance

Johannes Hüsers

BACHELORARBEIT

eingereicht am
Fachhochschul-Bachelorstudiengang

Software Engineering

in Hagenberg

im Februar 2021

Advisor:

DI Martin Harrer

Declaration

I hereby declare and confirm that this thesis is entirely the result of my own original work. Where other sources of information have been used, they have been indicated as such and properly acknowledged. I further declare that this or similar work has not been submitted for credit elsewhere. This printed copy is identical to the submitted electronic version.

Hagenberg, February 1, 2021

Johannes Hüsers

Abstract

—0.5 to 1 page—

Kurzfassung

—0.5 to 1 page—

Contents

Chapter 1

Introduction

1.1 Motivation

—1.25 pages—

1.2 Goals

—0.75 pages—

1.3 Structure of the Thesis

—0.5 pages—

Chapter 2

Fundamentals

2.1 Cryptography

— 1.5 pages —-

2.1.1 Public Key Infrastructures

2.1.2 Elliptic Curve Cryptography

2.1.3 Hashing Functions

Blockchain Grundlagen Schritt 11: Hashfunktionen in der Realität, S. 99ff Allgemeine Anwendungen von Hashfunktionen: * Data comparison * Detect data change * Computational complex problems

Blockchain Anwendungen: S 109 * Save transaction data * Digital fingerprint of transaction data * Implement generation costs

2.2 The Ethereum Blockchain

— 2.5 pages —

2.2.1 Blockchain Fundamentals

2.2.2 Clients

2.2.3 Wallets

2.2.4 Transactions

2.3 Smart Contracts

– 1 page —

2.3.1 Solidity

2.4 Decentralized Finance

— 2 pages —

2.4.1 State of the Art

current applications, relevance on the market, technologies, ...

Chapter 3

Use Cases of Decentralized Finance

— 9 pages —

This chapter aims to introduce the five most relevant use cases of Decentralized Finance. Each use case is built on top of the previous one and rises in complexity. For example storing value in digital systems is quite easy nowadays but moving real physical assets such as gold or real estate into a blockchain is still pretty demanding. Note, that each type of financial service is not specific to Decentralized Finance, which means that they are applicable to every financial environment.

3.1 Classification of Financial Services

—0.5 pages—

3.2 Store of Value

No matter of the financial product or service, they all need one essential thing. In fact, our entire economic system depends on it: a currency, or in simpler terms, something to store value. Storing value is a fundamental trait of money alongside with being exchangeable and having a unit of account. The last two characteristics are comparatively easy to accomplish in the online world. Storing value in a digitalized way without having a central trusted authority, however, was a similar challenge as the people had to face in the early days when they started to switch from bartering to a real currency. A common consensus needs to be created where everyone can easily verify that a specific piece of money is authentic and wasn't created illegally. Even further, each person that uses this money needs a proof that it is storing real value. This wasn't possible until Satoshi Nakamoto, an anonymous person or group, published a specification [4] in 2008, on how digital money could be implemented. The first cryptocurrency was founded: Bitcoin.

3.2.1 Proof of Work

Bitcoin uses a mechanism called proof-of-work in order to give each block its value. This utilizes a cost-function which is designed to be easily verifiable but quite expensive to compute [3]. In order to create a new block, a value needs to be found that matches with the correct number of zero bits of the block hash. Once the correct solution has been found, the new block represents real value, because operating this computationally intensive task on a CPU costs a lot of electricity. The integrity of this block is guaranteed as well, because in order to change the history of the blockchain, each changed block needs to be re-computed. The longest chain of blocks on the network is accepted as the “truth”, so if dishonest people want to cheat and change the history of the blockchain, they would need to create the longest chain of blocks which can be only achieved by having more than 50% of the computing power of the whole network. While these so-called 51% attacks are a threat on blockchains with a smaller number of network members, it is very unlikely to happen on a well established network like the Bitcoin blockchain [5]. The concept of proof-of-work in order to achive consensus in a decentralized manner became very popular and can be used in other areas of application too, such as elections, lotteries, asset registries, digital notarization and more [1].

3.2.2 Proof of Stake

A different approach to storing digital value is proof-of-stake. Instead of making the participants of the network solve computational expensive problems, the consensus is created by proving that someone owns specific funds. A blockchain that uses a proof-of-stake algorithm to achieve consensus has a set of validators. These validators are running a master node which gives them the opportunity to vote. In order to do so, the validators need to prove that they own a specific amount of funds. This is done by sending a special transaction, which locks away their currencies for a specific time. If the validators are honest and their vote corresponds to the result of the majority, they will get their funds back and an additional reward proportional to their deposited stake. If their vote gets rejected, the dishonest validator risks loosing his money [2].

3.2.3 Switching the Consensus Algorithm

At the time of writing this in October 2020, the Ethereum blockchain uses a similar proof-of-work algorithm like Bitcoin, called *Ethash*. However, Ethereum plans to switch to a proof-of-stake algorithm called *Casper* in the near future [9]. Algorithms that are based on proof-of-stake have the big advantage of less energy consumption because they are not focused on computational intensive tasks. The Bitcoin network, for example, has an annual electrical energy consumption of approximately 72.18 terawatt hours which is comparable to the consumption of Austria [8]. But proof-of-stake comes also with a caveat. Implementing incentives on a voting system which are based on the amount each validator is willing to stake means that the rich validators get richer and the poor validators stay poor.

The process of changing a consensus algorithm of a blockchain is not easy to accomplish. Because the network is decentralized, there is no single entity which can force all members to change the algorithm from proof-of-work to proof-of-stake. Just letting the people choose what they prefer to use is also not a good idea, because it is very unlikely that all agree on one type of algorithm. That would probably trigger a hard fork of the blockchain resulting in two separate networks, similar to what happened to Bitcoin in August 2017.

Bitcoin’s network is by design very slow in verifying transactions. A block which is mined approximately every 10 minutes has a size of about 1 MB. Due to the small block size, Bitcoin is only capable of processing 7 transactions per second. Some people wished for a Bitcoin network which is more suitable for day to day payments. That's why Bitcoin Cash was created, emerged out of a hard fork of the Bitcoin network [7]. In order to prevent a hard fork on Ethereum due to the transition from proof-of-work to proof-of-stake, the Ethereum protocol [6] has a built in mechanism called *difficulty bomb* which makes it more difficult over time to be profitable with mining[1] by increasing the size of the problem to solve. This ensures a smooth transition of all members to switch to proof-of-stake.

For a simple user of the blockchain who is neither a miner nor a validator it doesn't matter which consensus algorithm is being used. In fact, it isn't even important when developing decentralized applications based on smart contracts like it's done in chapter 4. What's important is, that the blockchain is able to store real value on the network by reaching consensus by its members.

3.3 Payments

—1.5 pages—

3.3.1 Bitcoin

3.3.2 Stable Coins

3.3.3 Dynamic Supply Protocols

3.3.4 Stability Protocols

3.4 Lending & Borrowing

—1.5 pages—

3.5 Exchanging

—1.5 pages—

3.5.1 Characteristics of Decentralized Exchanges

With the arise of many new fintech enterprises in the last few years, online exchanges started to grew in importance on the market too. While they all were very centralized in the first place, Decentralized Finance made it possible to establish new ways of exchanging money. Although each online exchange may behave very different, they can be all categorized into three big types when it comes to their structure: Centralized, decentralized and non-custodial exchanges. Centralized exchanges (CEXes) are the traditional approach where all the power is centralized to one specific organization. Decentralized exchanges (DEXes), however, are the complete opposite where there is no single entity in

[1] used synonymously to proof-of-work

control and decisions are made completely based on Smart Contracts. Non-custodial exchanges are somewhere inbetween but are often confused with decentralized exchanges. It is important to note, that none of the types are superior in comparison to the others. Each type of exchange has its own benefits and risks. In order to assess whether an exchange is suitable for a specific use case, it is crucial to know how to classify it.

Probably the most apparent indicator is the ownership of the private keys. On centralized exchanges the assets are coffered for the user. If someone buys Bitcoin on a centralized exchange, private keys are never an issue. On non-custodial and decentralized exchanges you have to manage your private keys by yourself. While this is usually a good thing, because you don't have to trust someone else[2], it comes also with the risk of losing all your assets if you forget your private key, since nobody can restore it for you.

Owning your private keys is a good indicator but by far not the only trait a decentralized exchange needs to have. When looking at the technical infrastructure of the exchange, many things could be structured in a centralized manner. While the code of a centralized exchange is usually proprietary, a DEX needs to have code that is licensed exclusively with an open-source licence, making it possible for anyone to fork the project in case the service is no longer available. That is also highly related to emergencies. How does an exchange react to bad or unexpected events such as hacking attacks? CEXes have the option to put their service temporary offline until the issue is resolved, in order to save the funds of the users. On decentralized exchanges, there is no such thing and assets may be lost forever.

Another crucial topic to consider is censorship and geo blocking. Is the service not available in the whole world, it is probably not a DEX. Centralized exchanges always decide which coins are listed on the exchange, which is usually a pay to play model. Decentralized exchanges don't have such regulation. Anyone can add a new pair of coins to swap on a DEX, which often leads to a tremendously high amount of unknown and irrelevant listed coins.

The last key indicator on how to categorize an online exchange is the way how the order matching and the settlement works. Centralized exchanges use the same algorithm as stock exchanges, which utilizes an order book. Buy and sell orders are listed in a centralized ledger and the settlement happens when two orders match. Non-custodial exchanges usually use price oracles which try to get price information through Smart Contracts. Truly decentralized exchanges even go a step further and solve this problem without a third party price oracle. A DEX uses a concept that relies on Liquidity Pools, which will be discussed in detail in the next section.

[2] often referred to as "not your keys, not your coins"

3.5.2 Liquidity Pools

3.5.3 Risks

3.6 Investing

3.6.1 Tokens

3.6.2 Derivatives

—1.5 pages—

Chapter 4

Design and Architecture

— 9 pages —

4.1 Architecture of Decentralized Web Applications

4.1.1 Technologies

React Truffle Ganache Web3 Solidity Mocha / Chai

4.2 Lending and Borrowing Application

4.3 Token Exchange

4.4 Asset Management Platform

Chapter 5

Closing Remarks

5.1 Criticism

—0.5 pages—

5.2 Risks

—0.5 pages—

5.3 Prospective Impact

—2 pages—

Appendix A

Technical Details

Appendix B

Supplementary Materials

List of supplementary data submitted to the degree-granting institution for archival storage (in ZIP format).

B.1 PDF Files

Path: /

thesis.pdf . . . . Master/Bachelor thesis (complete document)

B.2 Code-Files

Path: /media

. . . .

B.3 Reference Files

Path: /online-sources

. . . .

References

Literature

[1] Andreas Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain.* 2nd ed. Sebastopol: O'Reilly Media, Inc., 2017 (cit. on p. 5).

[2] Andreas Antonopoulos and Gavin Wood. *Mastering Ethereum: Building Smart Contracts and Dapps.* Sebastopol: O'Reilly Media, Inc., 2018 (cit. on p. 5).

[3] Adam Back. *Hashcash - A Denial of Service Counter-Measure.* Aug. 2002. URL: http://www.hashcash.org/papers/hashcash.pdf (cit. on p. 4).

[4] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Oct. 2008. URL: https://bitcoin.org/bitcoin.pdf (cit. on p. 4).

[5] Melanie Swan. *Blockchain: Blueprint for a New Economy.* Sebastopol: O'Reilly and Associates, 2015 (cit. on p. 5).

[6] Gavin Wood. *Ethereum: A Secure Decentralised Generalised Transaction Ledger.* Version 3e2c089. Sept. 2020. URL: https://ethereum.github.io/yellowpaper/paper.pdf (cit. on p. 6).

Online sources

[7] *Bitcoin Cash.* Nov. 2020. URL: https://www.bitcoincash.org/ (visited on 11/13/2020) (cit. on p. 6).

[8] *Bitcoin Energy Consumption Index.* Oct. 2020. URL: https://digiconomist.net/bitcoin-energy-consumption (visited on 10/12/2020) (cit. on p. 5).

[9] *Ethereum Casper.* Sept. 2018. URL: https://twitter.com/i/events/1036281460704112645 (visited on 11/13/2020) (cit. on p. 5).

Check Final Print Size

— Check final print size! —

width = 100mm
height = 50mm

— Remove this page after printing! —