Use Cases and Design of Decentralized Financial Web Applications

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

TODO: 0.5 - 1 page

Kurzfassung

TODO: 0,5 bis 1 Seite

Contents

Chapter 1

Introduction 2.5

1.1 Motivation

1.2 Goals

1.3 Structure of the Thesis

Chapter 2

Fundamentals 10

* definition of technical terms (e.g. DeFi, Blockchain, Smart Contracts, Security Tokens, ...) * explanation of fundamental concepts (e.g. Decentralization, Ethereum Network, Gas Price, Proof of Stake, Proof of Work...)

2.1 Cryptography

2.2 The Ethereum Blockchain

2.3 Smart Contracts

2.4 Decentralized Finance

2.5 State of the Art

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

Chapter 3

Use Cases of Decentralized Finance 10

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 pretty easy nowadays but moving real physical assets such as gold or real estate is still pretty demanding. Note that each type of financial service is not DeFi specific, which means that they are applicable to every financial environment.

3.1 Classification of Financial Services

* classify financial services

* extending financial seervices * classifiying types of financial institutions (traditional, fintech, .. * tabelle

3.2 Store of Value 1.5 - 3.5

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 one of the three traits besides being exchangeable and having a unit of account each type of money needs to have. 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 to the one 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.

Bitcoin uses a mechanism called proof-of-work in order to give each block that is being added to the blockchain a real 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 the bitcoin blockchain [5]. The concept of proof-of-stake 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].

A different approach to store digital value is proof-of-stake. [2]

3.3 Payments 1.5 - 3.5

3.4 Lending 1.5 - 3.5

3.5 Exchanging 1.5 - 3.5

3.6 Investing 1.5 - 3.5

Chapter 4

Design and Architecture 25

Chapter 5

Closing Remarks 2.5

5.1 Criticism

5.2 Risks

5.3 Prospective Impact

References

Literature

[1] Andreas Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. 2nd ed. Sebastopol: O'Reilly Media, Inc., 2017 (cit. on p. 4).

[2] Andreas Antonopoulos and Gavin Wood. *Mastering Ethereum: Building Smart Contracts and Dapps*. Sebastopol: O'Reilly Media, Inc., 2018 (cit. on p. 4).

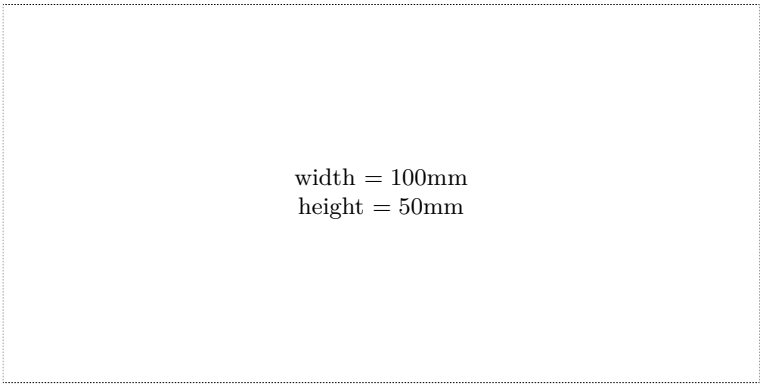
[3] Adam Back. *Hashcash - A Denial of Service Counter-Measure*. Aug. 2002. URL: http://www.hashcash.org/papers/hashcash.pdf (cit. on p. 3).

[4] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Oct. 2008. URL: https://bitcoin.org/bitcoin.pdf (cit. on p. 3).

[5] Melanie Swan. *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly and Associates, 2015 (cit. on p. 4).

Check Final Print Size

— Check final print size! —



— Remove this page after printing! —