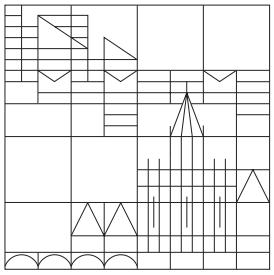
University of Konstanz

Department of Computer and Information Science



Master Thesis

Secure and Scalable data exchange using Public Blockchain

in fulfillment of the requirements to achieve the degree of

Master of Science (M.Sc.)

Harsh Kedia

Matriculation Number :: 01/752437

E-Mail :: ⟨harsh⟩.⟨kedia⟩@uni-konstanz.de

Field of Study :: Information Engineering
Focus :: *Applied Computer Science*
Topic :: *Distributed Systems*

First Assessor :: *Prof. Dr. M. Waldvogel*
Second Assessor ::
Advisor :: *Prof. Dr. M. Waldvogel*

Any dedications or other fancy stuff???

Abstract. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur non velit eget urna dictum bibendum. Vivamus lacinia nunc non felis. Suspendisse neque. Cras non nulla. In et lorem in nunc aliquet gravida. Morbi venenatis aliquam enim. Aenean ac justo. Mauris pretium varius mi. Proin sagittis gravida lectus. Ut non ante. Praesent tincidunt rutrum augue. Ut dolor. Maecenas est. Integer semper metus et dolor. Sed vitae orci ac risus ultrices vehicula. Duis dolor turpis, pharetra sed, blandit eget, consectetur sit amet, eros. Etiam ultrices velit eu quam. Curabitur laoreet nibh sit amet turpis posuere sagittis. Quisque tellus turpis, ornare vel, mollis sed, tristique eu, orci. Vestibulum sodales nisl vitae diam.
Fusce vitae diam. Aliquam porttitor. Sed neque urna, lobortis sed, pellentesque ac, facilisis id, nibh. Suspendisse mi. Suspendisse diam velit, venenatis a, malesuada sed, faucibus eget, magna. Praesent semper venenatis nisl. In hac habitasse platea dictumst. Suspendisse potenti. Pellentesque interdum, orci eu tristique venenatis, elit neque interdum quam, sit amet semper nisl mi a velit. Praesent a quam nec lacus interdum malesuada. Integer diam. Cras ante nulla, ultrices et, vestibulum id, pulvinar auctor, nisl. Sed ornare aliquet est. Donec interdum tortor at ante. Phasellus tristique viverra lorem. In rutrum viverra velit.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Problem Context

Blockchain technology emerged in 2008 with the creation of Bitcoin, a decentralized protocol for exchanging value among peers on the internet. With the Bitcoin network, it became possible to send value across the internet without any 3rd party.

Soon later, in 2014, Ethereum was invented. It allowed us to create complex applications by writing programs in a Turing complete language. These programs called smart contracts run as they are written and once they are deployed on the blockchain, they become immutable.

Blockchain, the technology which enabled Bitcoin and Ethereum, also enabled the emergence of decentralized applications. But currently, it's not clear, what a decentralized app or dApp is? As of this writing, the most popular platform for building dApps is Ethereum. It uses solidity as it's smart contracting language. Applications built on Ethereum uses a combination of smart contracts along with a traditional web architecture. The front end of the application talks to the smart contract for interacting with the blockchain and uses traditional storage for handling large data sets.

But, do dApps need a smart contract? Is it possible to create dApps without smart contracts? Also, on what specific use cases are smart contracts required?

To explore these questions we created a decentralized file sharing dApp both on Ethereum, a 1 layered protocol and Blockstack, a 2 layered protocol.

1.2 Thesis Statement

In this thesis, we want to explore what constitutes a decentralized application and how it differs from a traditional web application. We will also explore smart contracts, their security aspects, and certain use cases where they are required as part of a decentralized application.

Based on the below metrics, we will analyze our dApp build on Ethereum and Blockstack.

- User Experience
- Scalability
- Security

Above analysis will allow us to explore questions related to smart contract security and application scalability. Results from this analysis can help us determine what constitutes a secure smart contract platform?

At the end of this thesis, we will have a clear understanding of decentralized applications, when using smart contracts makes sense and how to make secure scalable dApps.

2 Related Work

3 Decentralized Applications

3.1 Introduction

3.2 Architecture

3.3 How Security is Guaranteed?

4 Smart Contracts

4.1 What is a Smart Contract?

4.2 What makes a Secure Smart Contract Platform?

5 Discussion

6 Conclusion

A Acknowledgements

References

[1] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.