University of Konstanz

Department of Computer and Information Science

Master Thesis

Secure Smart Contracts & Scalable Decentralized Applications (dApps)

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	**First Assessor** :: *Prof. Dr. M. Waldvogel*
Focus :: *Applied Computer Science*	**Second Assessor** ::
Topic :: *Distributed Systems*	**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 Background

2.1 Blockchain

The current Internet Protocol stack consists of four layers: the *Link Layer* puts data onto a wire; the *Internet Layer* routes the data; the *Transport Layer* persists the data; and the *Application Layer* provides data abstraction and delivers it to the end user in the form of applications. All four layers work seamlessly for exchanging of data, but not value. Bitcoin[1] and other cryptocurrencies help define the fifth Internet Protocol layer which enables the exchange of value as fast and efficiently as data[2].

Exchanging value across the Internet presents two challenges. First, every participant in the network must agree upon a shared state and Second, the asset being exchanged should have a clearly defined owner. These challenges are commonly referred as the *Byzantine General's* problem[3] and *Double-spending* problem[4] respectively. Blockchain, the technology underlying Bitcoin and most cryptocurrencies solved the above problems by means of decentralized consensus[1].

At a higher level, blockchains are append-only, totally-ordered, replicated logs of transactions[5]. A transaction is a signed statement that transfers the ownership of an asset from one cryptographic keypair to another. Peers[2] in the network, append new transactions by packaging them into a block and then executing a leader election protocol which determines who gets to append the next block[6]. This election protocol is determined by the underlying consensus algorithm of the blockchain. Each block contains the cryptographic hash of the previous block along with some transactional data.

[1] https://en.wikipedia.org/wiki/Consensus_(computer_science)

[2] A Node having the full copy of the blockchain.

3 Decentralized Applications

3.1 Introduction

3.2 History

3.3 Enabling Technologies and Concepts

4 Smart Contracts

4.1 Introduction

4.2 Smart Contract Platforms

4.3 Smart Contract Vulnerabilities

4.4 Secure Smart Contracts

5 Scalable Decentralized Applications

6 Discussion

7 Conclusion

A Acknowledgements

References

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

[2] S. Raval, *Decentralized applications: harnessing Bitcoin’s blockchain technology.* ” O’Reilly Media, Inc.”, 2016.

[3] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[4] U. W. Chohan, “The double spending problem and cryptocurrencies,” *Available at SSRN 3090174*, 2017.

[5] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Research perspectives and challenges for bitcoin and cryptocurrencies (extended version),” *Cryptology ePrint Archive, Report 2015/452*, 2015.

[6] J. Nelson, M. Ali, R. Shea, and M. J. Freedman, “Extending existing blockchains with virtualchain,” in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.