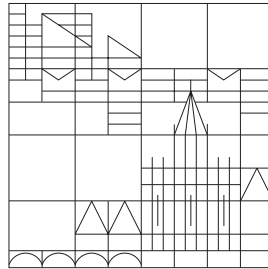


University of Konstanz
Department of Computer and Information Science



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
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. Humans have evolved over thousands of years building systems which deals with land ownership and property rights. With the advent of Internet our lives has become more and more digital, but we have no experience in managing data ownership. It's clear that data is becoming the new currency in today's digital economy. Big tech companies understood this a long time ago and therefore offered their services free of charge in exchange of our data which they then used to generate profits, control our perception about how we see the world and also tamper with public affairs like the election. There's clearly a need to define data ownership and build systems which enable users to own their data.

With data ownership comes the question of digital identity. How can we identify ourselves over the internet? With username and passwords we can uniquely identify ourselves when using a service, but then we have to create an identity for each service we want to use. It has another drawback, i.e. our passwords are stored on a central server which is prone to hacking. There exists systems like *Google Sign-in* or *Facebook Connect* which allows us to carry our identity across multiple services but then again this identity is not owned by the user but by Google or Facebook. Therefore, there is a need for a self-sovereign identity which is owned by the user and can be verified independently by anyone.

Blockchain along with Public key cryptography allows us to build a Decentralized Public Key Infrastructure (DPKI) thereby empowering users to create self-sovereign identity. Combining self-sovereign identity with encrypted storage enable us to build systems where users own their identity as well as their data.

Blockchain also enables Smart Contracts, which are self executing code and which run when some conditions are met without requiring any intervention by any third party.

Blockchain along with smart contracts and decentralized identity allows us to build interesting applications which are more aligned with the ethos of how the Web was intended in the first place.

This thesis explores technologies like smart contracts and decentralized identity and identifies the properties of a secure decentralized applications.

Table of Contents

Abstract.	i
List of Figures	iii
List of Tables	iv
1 Introduction	1
1.1 Problem Context	1
1.2 Thesis Statement	1
2 Background	3
2.1 Blockchain	3
3 Decentralized Applications	5
3.1 Introduction	5
3.2 History	5
3.3 Enabling Technologies and Concepts	5
4 Smart Contracts	7
4.1 Introduction	7
4.2 Smart Contract Platforms	7
4.3 Smart Contract Vulnerabilities	7
4.4 Secure Smart Contracts	7
5 Scalable Decentralized Applications	9
6 Discussion	11
7 Conclusion	13
A Acknowledgements	15
References	16

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 consensus¹.

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. Peers² 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_\(computer_science\)](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.