Secure IoT Applications Using Scalable Blockchain Models And PQ Primitives

Sichere IoT Anwendungen unter Nutzung skalierbarer Blockchain Modelle und PQ Primitive

Master-Thesis von Muhammad Rameez
Matriculation No.: 2556345
Tag der Einreichung:

1. Gutachten: Gutachter 1
2. Gutachten: Gutachter 2
Betreuer: Rachid El Bansarkhani

TECHNISCHE
UNIVERSITÄT
DARMSTADT

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Secure IoT Applications Using Scalable Blockchain Models And PQ Primitives
Sichere IoT Anwendungen unter Nutzung skalierbarer Blockchain Modelle und PQ Primitive

Vorgelegte Master-Thesis von Muhammad Rameez
Matriculation No.: 2556345

1. Gutachten: Gutachter 1
2. Gutachten: Gutachter 2
Betreuer: Rachid El Bansarkhani

Tag der Einreichung:

Erklärung zur Master-Thesis

Hiermit versichere ich, die vorliegende Master-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den August 18, 2018

(Muhammad Rameez)

Abstract

Distributed Ledger Technologies like blockchain has emerged as a promising area of research in academia and business. Its tamper resistant nature combined with other properties such as immutability, transparency and byzantine fault tolerance make it particularly useful for applications in Finance, Internet of Things, Supply Chain Management, and Cloud Storage.

In this thesis, I first introduce the basics of blockchain and its related terminologies. Then, I highlight some of challenges faced by this promising new technology along with some potential solutions to those problems. After which, some choice examples of blockchain applications are presented. Next, I focus on the Ethereum blockchain, IPFS and Raiden Network and explore their potential in building powerful new decentralized applications or dApps.

As part of this thesis, a novel decentralized Supply Chain Management System was designed, implemented and tested. The design was realized using the Ethereum blockchain and was evaluated under various scenarios designed to simulate real world application and usage. This design has several key advantages over traditional systems. It is not only secure against distributed denial of service attacks but is also trustless, autonomous, transparent and censorship resistant.

Preface

preface goes here ....

Contents

1 Introduction And Motivation

Blockchain is distributed ledger technology defined as "blah blah"

1.1 Introduction To Blockhain

"Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block contains typically a hash pointer as a link to a previous block, a timestamp and transaction data" [Wik18]. It can serve as a distributed ledger that can record transactions without a central server or trusted third party. The transactions are available to all parties and are easily verifiable. It is inherently resistant to data tampering as altering data in any one block breaks the chain and requires that all subsequent blocks be calculated again using the new data. Technical details of blockchains are discussed in chapter [2], however for a high level overview please refer to Figure 1. Blockchain has the power to revolutionize how business is conducted in digital age. Some are calling it the most important innovation since the development of the internet and the world wide web. The proponents of this technology believe that it will fundamentally transform the web itself. Internet of tomorrow will be powered by decentralized applications or Dapps. The first blockchain was invented by a person or group of persons known only by the pseudonym Satoshi Nakamoto. Bitcoin is a form of peer-to-peer electronic cash designed to transfer value between two parties without involving banks or other financial institutions. It was the first to solve the double spend problem in digital currency. Bitcoin paved the way for exponential growth in crypto currency market which together with other alt coins is worth over 120 billion dollars. The underlying technology which powers Bitcoin, Ethereum and other crypto currencies can be used for much more than just transferring X amount of crypto from Person A to Person B. Researchers are employing blockchain technologies to increase efficiency and reduce costs in industries such as Supply Chain Management, Internet of things, Banking and Finance.

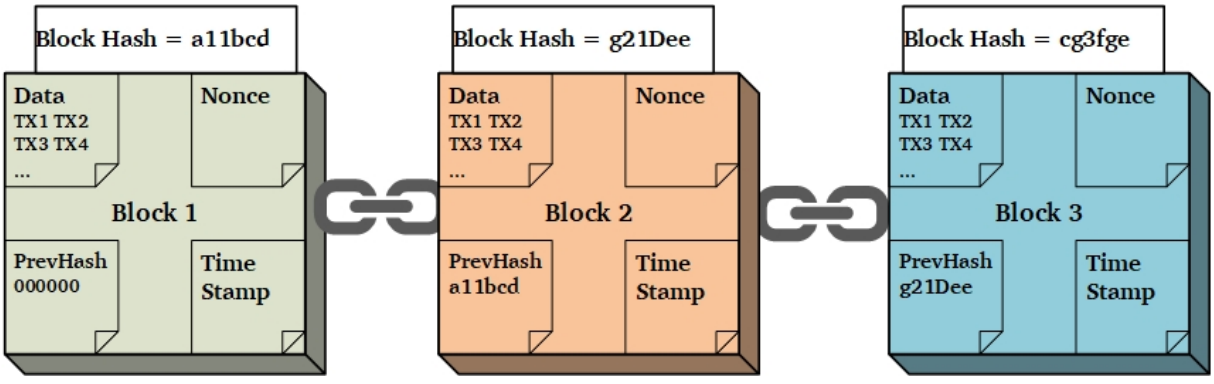

Figure 1: High Level Overview of the Blockchain

1.2 Permissioned Vs Permission less blockchains vs Private blcokchain

i.e. properties of each , reasons for each one to exist https://github.com/ramxis/Thesis/blob/master/Miscellaneou 2020—blockchain-powering-the-internet-of-value—whitepaper.pdf use permissioned and permssione-less table from this paper as a guiding inspiration

1.3 Motivation

Thesis motivation text goes here.... Motivation, relevance, goals, research questions, hypotheses...

1.4 Thesis Objective

objective.....

2 Blockchain Echo System

In this chapter I will explain some fundamentle concepts related to blockchain and some of the technical termanologies surrounding it.

2.1 Decentralized Ledger Technology

https://hackernoon.com/the-ultimate-guide-to-understanding-blockchain-and-cryptocurrencies-f37cf4c0043

2.1.1 Asymmetric Cryptography

2.1.2 Hashing and Digital Signatures

https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/

2.1.3 Merkle Trees

https://medium.com/byzantine-studio/blockchain-fundamentals-what-is-a-merkle-tree-d44c529391d7

2.2 Consensus Mechanisms - Mining

explain the role of miners and minning in the echo system https://blockgeeks.com/guides/blockchain-consensus/

2.2.1 Proof of work

2.2.2 Proof of Stake

if need to fill pages put other eight mechanisms from the following list https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits

2.3 Transaction Finality

mention how finality can impact confirmation times and how it might impact any potential supply chain management app. https://medium.com/coinmonks/blockchain-finality-pow-and-pos-35915a37c682

2.4 Blockchain Scaling

There are three main solutions proposed and explored sharding and offchain solutions

3 Blockchain Applications

use case examples....

3.1 Crypto Currencies

3.2 Internet of Things

3.2.1 Adept

3.2.2 Filament

3.3 Supply Chain Management

3.3.1 Skuchain

3.3.2 Provenance

3.4 Filesharing

3.4.1 FileCoin

4 Fundamentals

4.1 Ethereum

created by vitalik beutarin, a platform for smart contracts

4.1.1 Ethereum virtual machine

4.1.2 Smart Contracts

Use a figure to exaplain how smart contracts are, i.e. draw a figure/ flowchart like showing signed transaction comming in, smart contract executing it, and triggering events or results or altering state of blockchain. etc use the figure of smart contract given on the following papers as starting point https://github.com/ramxis/Thesis/blob/master/Miscellaneous/Recommended/bank-2020—blockchain-powering-the-internet-of-value—whitepaper.pdf

https://blockgeeks.com/guides/different-smart-contract-platforms/

4.1.3 Advantages of smart Contracts

https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a ———————————————————————— describe what smart contracts are and what they can do write about eVM, solidity, and how to communicate with smart contracts from dapps i.e. web3 py3 etc create a graphical figure showing interaction between smart contract and web3 dapp

4.1.4 Block limits and Gas

https://hudsonjameson.com/2017-06-27-accounts-transactions-gas-ethereum/ text goes here....

4.2 Raiden

4.2.1 Netting Channel Smart contract

4.2.2 Channel Life cycle

4.2.3 Raiden Transfers

4.2.4 Network Protocol

4.2.5 Raiden API

4.3 InterPlanetary File System (IPFS)

4.3.1 Cost of Storage on BlockChain

4.3.2 Curious Case of Crypto Kitties

due to sky rocketting transaction costs largely in part of one dapp called crypto kitties the network became congested https://medium.com/@mycoralhealth/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0

4.4 Quantum Threat to Blockchain

https://medium.com/wolverineblockchain/the-quantum-threat-to-blockchain-2adc429fd88b

5 Decentralized Supply Chain Management System

5.1 System Architecture

5.1.1 Supply Chain LifeCycle

5.1.2 System Work Flow

say that a shipper key will be transferred when a new shipper scans the package

5.2 System Components

5.2.1 Decentralized Monitoring Application - Master Node

Include figure of monitoring app

5.2.2 IoT Powered Smart Packages - Sensor Nodes

include figure of pi with sensors

6 Implementation Details

give the algorithm that professor told you

6.1 Hardware Setup

Master Node PI Node

6.2 Software Architecture

6.2.1 Master Node

give class diagrams and some details about monitoring dapp

6.2.2 Sensor Nodes

give class diagrams and some details about sensor nodes

6.2.3 Integrated Payment Solution

6.3 Securing the System Against Post Quantum Adversaries

7 Testing and Results

7.1 Testing Environment

ropsten, pi, ganachi,IPFS

7.2 Results

7.2.1 Unit Testing

7.2.2 Scenario - I

7.2.3 Scenario - II

7.2.4 Scenario - III

7.3 Evaluation

7.3.1 Gas Consumption

deployement,each tx cost, word about gas price etc

7.3.2 Transaction Verification Time

dependent on gas price, network congestion etc

8 Conclusion and Future Work

To conclude...

List of Figures

List of Tables

Bibliography

[Wik18] Wikipedia contributors. Blockchain — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=855030838, 2018. [Online; accessed 17-August-2018].

A Appendix Stuff

the Appendix

B Acronyms

Dapps Decentralized Applications