Politechnika Warszawska

WYDZIAŁ ELEKTRYCZNY

Instytut Elektrotechniki Teoretycznej
i Systemów Informacyjno-Pomiarowych
Zakład Elektrotechniki Teoretycznej
i Informatyki Stosowanej

Praca dyplomowa inżynierska

na kierunku Informatyka
w specjalności Inżynieria oprogramowania

Zdecentralizowana aplikacja do pożyczek na platformie Ethereum

Adam Kasperowicz
nr albumu 279046

promotor
dr hab. inż. Bartosz Sawicki

WARSZAWA 2018

TYTUŁ PRACY DYPLOMOWEJ

Streszczenie

Praca składa się z krótkiego wstępu jasno i wyczerpująco opisującego oraz uzasadniającego cel pracy, trzech rozdziałów (2-4) zawierających opis istniejących podobnych rozwiązań, komponentów rozpatrywanychjako kandydaci do tworzonego systemu i wreszcie zagadnień wydajności wirtualnych rozwiązań. Piąty rozdział to opis środowiska obejmujący opis konfiguracji środowiska oraz przykładowe ćwiczenia laboratoryjne. Ostatni rozdział pracy to opis możliwości dalszego rozwoju projektu.

Słowa kluczowe: praca dyplomowa, LaTeX, jakość

THESIS TITLE

Abstract

This thesis presents a novel way of using a novel algorithm to solve complex problems of filter design. In the first chapter the fundamentals of filter design are presented. The second chapter describes an original algorithm invented by the authors. Is is based on evolution strategy, but uses an original method of filter description similar to artificial neural network. In the third chapter the implementation of the algorithm in C programming language is presented. The fifth chapter contains results of tests which prove high efficiency and enormous accuracy of the program. Finally some posibilities of further development of the invented algoriths are proposed.

Keywords: thesis, LaTeX, quality

WARSZAWA, 1 lutego 2017

POLITECHNIKA WARSZAWSKA
WYDZIAŁ ELEKTRYCZNY

OŚWIADCZENIE

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa inżynierska pt. Zdecentralizowana aplikacja do pożyczek na platformie Ethereum:

- została napisana przeze mnie samodzielnie,
- nie narusza niczyich praw autorskich,
- nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam, że przedłożona do obrony praca dyplomowa nie była wcześniej podstawą postępowania związanego z uzyskaniem dyplomu lub tytułu zawodowego w uczelni wyższej. Jestem świadom, że praca zawiera również rezultaty stanowiące własności intelektualne Politechniki Warszawskiej, które nie mogą być udostępniane innym osobom i instytucjom bez zgody Władz Wydziału Elektrycznego.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Adam Kasperowicz.....

Contents

Chapter 1

Introduction

The aim of the thesis will be a construction of a decentralized loan system using Ethereum technology. The final product should be a proof of concept of the possibilities of blockchain and smart contracts technologies. Additionally, the thesis should serve as an experiment, in which strengths and flaws of software architectures involving blockchain will be discovered.

1.1 Problem and solution

Loan business is a vital part of the modern financial world. Being one of the oldest financial mechanisms to exist it provides the consumers with required capital. Throughout the whole history it has always been an example of a centralized system. That is one central entity hoarding the money from different sources gets inquired about financing possibilities. Such entity is in power to decide upon who shall receive the funding and with what interest. It is also the burden of the entity to deal with any cases of loan repayment disobedience.

The are a few problems with this concept all of which stem from the design itself. Firstly, if one wants to capitalize on his spare money through this type of scheme he has to create an entire new company with all the legal requirements and an administrative burden. Secondly, all the processes such as storage of money, allocation of loans, interest serving, acceptance of clients etc. have to be taken care of by the workers of the loan company. Thus, costs are generated and sources of human errors and introduced. Lastly, due to the way financial services are diversified around the world it is often very troublesome or even impossible to service loans internationally.

All of the aforementioned disadvantages can be circumnavigated using the fruits of modern computer science. That is blockchain and tightly re-

lated smart contracts. A Decentralized Autonomous Organization(DAO) is introduced which serves as a medium between those who have the capital and those who need the capital. The DAO which acts as a loan system allows anyone with any amount of Ethereum to bid a loan with an arbitrary duration and interest on a public exchange. At the same time a counterparty publishes an ask offer stating how big of a loan is required under specific duration and interest. The whole process closely resembles stock exchange. In result market forces lead to an equilibrium allowing both parties to reach their goal. The exchange itself is based on blockchain and no central server is required.

This design solves all of the issues pointed out so far. Anyone in the whole world with a connection to an internet is able to put his money to good use with few mouse clicks while maintaining anonymity. All of the operational activities are also immediately eradicated by market forces backed by smart contracts. Of course the problem of loan repayment still remains but the possible solutions of this specific mischief will be explained in the section describing a loan taker.

1.2 Blockchain

A blockchain is simply a chain of blocks. Where the function of a link is served by a hash. Each block is a record, in it's simplest form containing: cryptographic hash of the previous block, a timestamp, and some arbitrary transaction data. Blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. By design, a blockchain is resistant to modification of any data inside of it. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design.

To put it simply blockchain constitutes of 3 major technologies put together:

1. Peer-to-peer network: In it's simplest form blockchain is stored entirely by every user of the network. Just like torrent users spreading their data to every other user so that perfect replication of every data is accomplished. Usage of this technology allows every user to have the possibility to recreate every series of transactions that have happened on the network.
2. Assymetric cryptography: Users of blockchain communicate between

themselves using their public and private keys. The algorithms used for key generation are often based on RSA or elliptic curves. This type of communication assures us that no malicious manipulation of the data propagation could happen.

3. Proof mechanism: The last element of the jigsaw puzzle is a solution to the double-spending problem. Solution proposed in Bitcoin is inscribed into the method blocks are created. First, a certain number off transactions started are gathered. Then, network participants start looking for 256 characters long hash which contains certain amount of zeros at the beginning. How this amount is determined will be described later. When found, a new block is created which contains the gathered transactions and is signed by the found hash. Only then are the transactions put into life. All of the contradicting transactions are also thrown out of the block. We can see that no malicious information can spread this way. The way this mechanism is implemented is also what differentiates most of the blockchain implementations present nowadays.

What is double-spending? Lets assume there are three participants in the network A, B and C. A sends two different transactions to B and C which can not happen at the same time. But B and C do not know that there are two transactions. At the moment of receiving message from A they only know of the message they received and thus happily follow with it. After some time, when all of the data propagates throughout the network B and C learn that they have been scammed by A but can not do anything about it. A real life example could be A holding 100$ in bank and asking both B and C to buy a product for 100$. B and C will accept the payment because they lack information of the whole network. Hence the name double-spending problem.

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. [1] Is has since sparked an interest of thousands of software developers creating their own cryptocurrencies and developing the whole technology in many ways. Most notably, a new financial microworld has grown around cryptocurrencies bringing fortune to many and financial ruin to even more people. What has happened to bitcoin price througout the last decade is often compared to modern tulipmania and can be clearly seen on the graph 1.1.

But financial prospects are not the aspects this thesis is concerned with. The most groundbreaking features the blockchain posses and which actually put it into the focus of modern computer science are anonymity and trustlessness.

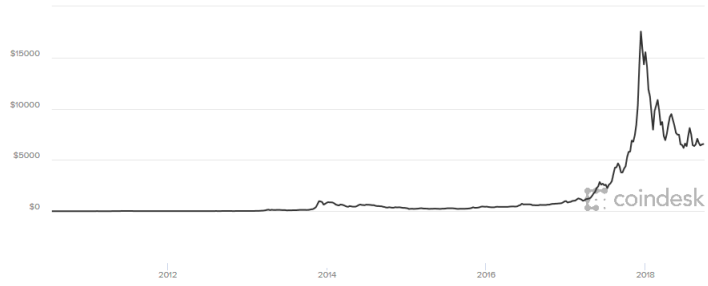

Figure 1.1: Bitcoin price over years

- Anonymity: In the simplest implementations of blockchain such as bitcoin it is not possible to find any information of the user participating in the network. That is a simple consequence of relying purely on assymetric cryptography and no other requirement for allowing to interact with the network other than having a key pair. This simple feature has amazing implications in the real world. Every one in the world with internet connection can actually use blockchain. Coupled with the fact that cryptocurrencies can be used for value storage a way of escaping dangerous national currencies has appeared for every human being. Recent example of that can be seen in Venezuela [2]. There are also people who have found ways to use the anonymity in an illegal way. Silk road, the greatest illegal drug webshop accessible by TOR network has experienced a renaissance every since bitcoin payments have been implemented. [3]
- Trustless: All of the currencies in our world are based on trust. The paper money has only a fraction of the value we assign to it. The numbers in our bank accounts have virtually no value. Currencies are simply are major agreement between all of the people on the world. In this world central parties are required such as banks which hold record of all transactions. We trust banks that when we ask them whether a person willing to buy from us has enough money we will receive a true information. The double spending problem is solved this way. But blockchain has it's own mechanisms for this and thus allows us to omit the central party. We call the blockchain a trustless system because there is no trust required everything is taken care of by the computers, algorithms and protocols. The most grand example is Bitcoin itself which serves as a currency and a bank for all of the participants.

The element of blockchain technology that needs explanation is the cre-

ation of a new block. As described earlier, in Bitcoin it is achieved by computing hashes of random numbers until a hash with certain amount of zeros at the beginning is reached. The whole process is commonly referred to as mining. This amount of zeros is called *the difficulty*. The purpose of *the difficulty* is to simply hold the rate of blocks being created constant. That is lower the difficulty when there are few miners and the transactions would be processed very slowly or increase the difficulty when everyone starts using supercomputers for mining. Currently, the rate is adjusted every 2016 mined blocks. More exact information about this topic can be found on bitcoin wiki. One important question that is left to be answered is: why do miners should bother with mining? Especially, why do people mine transactions which are not theirs? The answer is *reward* and *fees*. Currently, every mined block grants the miner who has done it some amount of bitcoin itself that is a *reward* for mining. Additionally, people simply putting the transactions can attach fee to their transactions so that miners will be more likely to mine those transactions first and receive the fee.[4]

But looking for specific hashes is only one way of controlling block creation rate. PrimeCoin is especially worth noting as its method of mining is by finding prime numbers. Mining itself has also become a major part of computer hardware world due to computing power is has accumulated. Mining hashes is nowadays done only by GPUs due to parallelism benefits. There has been even created a special hardware called *ASIC* which exist solely for the purpose of mining hashes.

After the subject of mining has been explained we encounter another problem. We know that after a block has been mined it has to be propagated throughout the network as to be actually accepted by the network. What happens when in a large network two blocks are mined at the same time and both are able to propagate only through a part of the network before they collide? Then at least the majority of the miners (that is 51%) has to decide which block to link to the blockchain and which to throw out. It is very important that a solid way of choosing the block by majority is used in a blockchain implementation because otherwise a malicious party could take over the network in some way or another by forcing his blocks with his transactions. It has also occured that the declined block is not thrown away but starts living his own life in a sequence of events that are known as *forks*. What follows is that one blockchain is split into two smaller ones which live from then on their own lives. Most of the time forks happen because a new version of the blockchain implementation is being deployed and not everyone wants this new version. This situation has occured with Bitcoin multiple times and the whole subject is worth thesis on its own.

Possible topics to elaborate:

- Comparing blockchain to sql and nosql? (trustlessness, no scalability)
- What coins are there? (Bitcoin, Ethereum)
- What are forks?
- When to use blockchain? (use cases)
- How to take over the network?

1.3 Ethereum

History? What are the specifications? What is DAO?

1.4 Smart contracts

Is it Turing Complete? What is GAS?

Chapter 2

Current state of the technology

2.1 ETHLend

2.2 Kamboo Finance

2.3 DAI

2.4 Unchained Capital

2.5 SALT Lending

2.6 Othera

2.7 BitBond

2.8 BTCPOP

2.9 Credible Friends

Chapter 3

Software design

3.1 Loans

One loan offer on an exchange will consist of following parameters:

- **Basis**: Size of the loan denominated in Ethereum.
- **Duration**: The time after which the whole loan should be paid back together with interest. Depicted per predefined amount of days.
- **Interest**: Percentage of the loan basis which has to be additionally paid by loan taker. Calculated per predefined amount of days.
- **Collateral**: Information whether the loan is backed by a third party and has a low probability of going default. For example loan taker with no evidence to back his repayment probability will have only access to loans with collateral parameter being equal to None. At the same time loan taker with his loan being backed by a special bank agreement whereas there is a deposit with amount equal to the loan basis and interest incurred which is connected to a smart contract will have access to loans with collateral being equal to Yes.

The process of buying and selling loans will have the same characteristics as the one seen on the stock exchange.

That is loan ask whose size exceeds size of one respective loan bid will automatically cover the second identical loan bid. For example loan taker A asks for a loan of 1 ETH. There are two identical offers by loan provider B and C both equal to 0.5 ETH. The matching will automatically buy for A both loans from B and C.

Moreover, if loan taker asks for a loan of interest higher than the lowest present on the market he will be sold the loan with the lowest interest. For

example loan taker asks for a loan of interest 2%. There are loans on the market being bid with both interest of 2% and 1%. The loan of 1% will be sold to the loan taker.

In terms of repayments the loan will function as an amortized loans. That is, the repayments will be constant with principal amount being paid back increasing and the interest amount decreasing. The formula for computing the installments looks as follows:

$$C = \frac{rP}{1 - \frac{1}{(1+r)^n}}$$

Where C is monthly installment, r is interest rate per month, P is principal amount/basis and n is a duration of a loan in periods equal to predefined amount of days.

3.2 Types of users

The project provides for three types of possible actors. They are as follows:

- **Loan providers**: Any user with spare Ethereum and access to the application. Such person bids his loan offer and once the loan is sold automatic processes backed by smart contracts care for repayments.
- **Loan takers**: User who has fulfilled required information inquires and can be assured of that at least one of the methods of repayment can be exercised on him. The methods are:
  1. Regular individual refilling of his repayment account.
  2. Usage of a collateral deposit from a third party.
  3. Following legal procedures by bailiff of a country where the loan taker is located.
- **Authorities**: Third parties which for example serve the role of a collateral deposit or bailiff chasing the loan taker. This user has the possibility to refill the account of the loan takers repayment account.

3.3 Processes

3.4 Requirements

The complete system should provide following functions:

1. Loan providers and loan takers should be able to:
    - check and transfer funds to and from their accounts using external wallet based on Ethereum network.
    - specify the following parameters in their loan bids and asks: Basis, Duration, Interest, whether it has collateral.
    - check their open bids and asks as well as the whole public exchange.
    - cancel all of their open bids and asks.
2. Loan takers should be able to:
    - specify legal informations which could be used by bailiff if repayment did not happen. At the same time the information should remain confidential so long there is no need to use them.
    - bind his account with an account of a third party. The additional account will always hold a sum required to repay the whole loan when needed.
    - repay the loan earlier.
3. Every user should be able to:
    - access the application having only internet connection.
    - maintain his anonymity while using the system.

3.5 Architecture

3.6 Visuals

Chapter 4

Software implementation

4.1 Ethereum network

4.2 Solidity

4.3 Java

Bibliography

[1] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf

[2] „How Venezuela Came to Be One of the Biggest Markets for Crypto in the World", https://cointelegraph.com/news/how-venezuela-came-to-be-one-of-the-biggest-markets-for-crypto-in-the-world

[3] „The Effect Of Silk Road On Bitcoin And Tor", https://silkroaddrugs.org/the-effect-of-silk-road-on-bitcoin-and-tor/

[4] https://en.bitcoin.it/wiki/Difficulty

Opinia

o pracy dyplomowej magisterskiej wykonanej przez dyplomanta
Zdolnego Studenta i Pracowitego Kolegę
Wydział Elektryczny, kierunek Informatyka, Politechnika Warszawska
Temat pracy
TYTUŁ PRACY DYPLOMOWEJ

Promotor: **dr inż. Miły Opiekun**
Ocena pracy dyplomowej: **bardzo dobry**

Treść opinii

Celem pracy dyplomowej panów dolnego Studenta i Pracowitego Kolegi było opracowanie systemu pozwalającego symulować i opartego o oprogramowanie o otwartych źródłach (ang. Open Source). Jak piszą Dyplomanci, starali się opracować system, który łatwo będzie dostosować do zmieniających się dynamicznie wymagań, będzie miał niewielkie wymagania sprzętowe i umożliwiał dalszą łatwą rozbudowę oraz dostosowanie go do potrzeb. Przedstawiona do recenzji praca składa się z krótkiego wstępu jasno i wyczerpująco opisującego oraz uzasadniającego cel pracy, trzech rozdziałów (2-4) zawierających opis istniejących podobnych rozwiązań, komponentów rozpatrywanychjako kandydaci do tworzonego systemu i wreszcie zagadnień wydajności wirtualnych rozwiązań. Piąty rozdział to opis przygotowanego przez Dyplomantów środowiska obejmujący opis konfiguracji środowiska oraz przykładowe ćwiczenia laboratoryjne. Ostatni rozdział pracy to opis możliwości dalszego rozwoju projektu. W ramach przygotowania pracy Dyplomanci zebrali i przedstawili w bardzo przejrzysty sposób duży zasób informacji, co świadczy o dobrej orientacji w nowoczesnej i ciągle intensywnie rozwijanej tematyce stanowiącej zakres pracy i o umiejętności przejrzystego przedstawienia tych wyników. Praca zawiera dwa dodatki, z których pierwszy obejmuje wyniki eksperymentów i badań nad wydajnością, a drugi to źródła skryptów budujących środowisko.

Dyplomanci dość dobrze zrealizowali postawione przed nimi zadanie, wykazali się więc umiejętnością zastosowania w praktyce wiedzy przedstawionej w rozdziałach 2-4. Uważam, że cele postawione w założeniach pracy zostały pomyślnie zrealizowane. Proponuję ocenę bardzo dobrą (5).

(data, podpis)

Recenzja

pracy dyplomowej magisterskiej wykonanej przez dyplomanta
Zdolnego Studenta i Pracowitego Kolegę
Wydział Elektryczny, kierunek Informatyka, Politechnika Warszawska
Temat pracy
TYTUŁ PRACY DYPLOMOWEJ

Recenzent: **prof. nzw. dr hab. inż. Jan Surowy**
Ocena pracy dyplomowej: **bardzo dobry**

Treść recenzji

Celem pracy dyplomowej panów dolnego Studenta i Pracowitego Kolegi było opracowanie systemu pozwalającego symulować i opartego o oprogramowanie o otwartych źródłach (ang. Open Source). Jak piszą Dyplomanci, starali się opracować system, który łatwo będzie dostosować do zmieniających się dynamicznie wymagań, będzie miał niewielkie wymagania sprzętowe i umożliwiał dalszą łatwą rozbudowę oraz dostosowanie go do potrzeb. Przedstawiona do recenzji praca składa się z krótkiego wstępu jasno i wyczerpująco opisującego oraz uzasadniającego cel pracy, trzech rozdziałów (2-4) zawierających bardzo solidny i przejrzysty opis: istniejących podobnych rozwiązań (rozdz. 2), komponentów rozpatrywanychjako kandydaci do tworzonego systemu (rozdz. 3) i wreszcie zagadnień wydajności wirtualnych rozwiązań, zwłaszcza w kontekście współpracy kilku elementów sieci (rozdział 4). Piąty rozdział to opis przygotowanego przez Dyplomantów środowiska obejmujący opis konfiguracji środowiska oraz przykładowe ćwiczenia laboratoryjne (5 ćwiczeń). Ostatni, szósty rozdział pracy to krótkie zakończenie, które wylicza także możliwości dalszego rozwoju projektu. W ramach przygotowania pracy Dyplomanci zebrali i przedstawili w bardzo przejrzysty sposób duży zasób informacji o narzędziach, Rozdziały 2, 3 i 4 świadczą o dobrej orientacji w nowoczesnej i ciągle intensywnie rozwijanej tematyce stanowiącej zakres pracy i o umiejętności syntetycznego, przejrzystego przedstawienia tych wyników. Drobne mankamenty tej części pracy to zbyt skrótowe omawianie niektórych zagadnień technicznych, zakładające dużą początkową wiedzę czytelnika i dość niestaranne podejście do powołań na źródła. Utrudnia to w pewnym stopniu czytanie pracy i zmniejsza jej wartość dydaktyczną (a ta zdaje się być jednym z celów Autorów), ale jest zrekompensowane zawartością merytoryczną. Praca zawiera dwa dodatki, z których pierwszy obejmuje wyniki eksperymentów i badań nad wydajnością, a drugi to źródła skryptów budujących środowisko. Praca zawiera niestety dość dużą liczbę drobnych błędów redakcyjnych, ale nie wpływają one w sposób istotny na na jej czytelność i wartość. W całej pracy przewijają się samodzielne, zdecydowane wnioski Autorów, które są wynikiem własnych i oryginalnych badań.

Rozdział 5 i dodatki pracy przekonują mnie, że Dyplomanci dość dobrze zrealizowali postawione przed nimi zadanie. Pozwala to stwierdzić, że wykazali się więc także umiejętnością zastosowania w praktyce wiedzy przedstawionej w rozdziałach 2-4. Kończący pracę rozdział szósty świadczy o dużym (ale moim zdaniem uzasadnionym) poczuciu własnej wartości i jest świadectwem własnego, oryginalnego spojrzenia na tematykę przedstawioną w pracy dyplomowej. Uważam, że cele postawione w założeniach pracy zostały pomyślnie zrealizowane. Proponuję ocenę bardzo dobrą (5).

(data, podpis)