MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef de departament: conf. univ., dr. Viorica SUDACEVSCHI

„09" 01 2019

SISTEM VIRTUAL PENTRU MONITORIZAREA TRANZACȚIILOR ÎN CRIPTOVALUTĂ

Teză de master în

Calculatoare și Rețele Informaționale

(programul de masterat)

Masterand:

Student. Popițac Ion (Popițac)

Conducător:

Lect. sup. Cârlușa Viorel (Cârlușa)

Chișinău 2019

ADNOTARE

La teza de master: „Sistem virtual pentru monitorizarea tranzacțiilor de criptovalută”,

elaborat de Popriţac Ion, Chișinău, 2019.

Cuvinte cheie: Ruby, Ruby on Rails, Blockchain, Mining, P2P, SHA-256 și prime-256v1(algoritmul curbei eliptice), Docker, produs soft, tranzacție electronică de criptomonedă.

În lucrarea de față este stabilit scopul proiectării și implementării unui sistem virtual bazat pe tehnologia Blockchain, ce va permite monitorizarea din interior a tranzacțiilor de criptovalută. La baza acestui sistem este protocolul rețelei P2P ce va fi decentralizat ce va garanta anonimitate participanților. Sistemul urmează funcționalul creării și generării un bloc de date ce va conține istoricul tranzacțiilor, iar pentru a declara dreptul de proprietate a blocului, fiecare participant va avea grupul propriu de chei publice-private pentru identificare.

Teza urmărește crearea și dezvoltarea unei aplicații actuale, ce urmărește principiul de funcționare a tehnologie Blockchain, iar termenul de ”minare” utilizat pe parcurs, prevede o remunerare pentru crearea și validarea blocurilor cu datele tranzacțiilor. Automatizarea procesului de inițiere și asamblare este efectuată cu ajutorul softului Docker, ce va permite rularea sistemului în câteva secunde.

Tehnologiile utilizate sunt: Limbajul de programare Ruby, pentru dezvoltarea nucleului aplicației, framework-ul Ruby on Rails, softul de automatizare Docker, librăria Dry pentru structurarea și implementarea codului cât mai simplificat și corespunzător standartelor de stil și baza de date SQLite3 cu scopul de stocare a datelor. Protocolul de rețea P2P permite participanților cât de a crea blocuri, atât și valida tranzacțiile acestuia, deci funcționează ca client sau server totodată. Baza de date va stoca toată informația ce o conține blocul și la afișarea listei de blockchain vor putea fi văzute datele necesare. Pentru securizarea datelor identității participanților, este folosit algoritmul curbei eliptice ce nu va permită orice dezvăluire a acestora.

Memoriul explicativ conţine: Introducere, 3 capitole, concluzii, bibliografie cu 18 titluri, dintre care 40 pagini text de bază, 47 figuri și 2 tabele.

Capitolul 1 definește cadrul elaborării lucrării, cunoștințele necesare pentru crearea sistemului și tehnologiile deja existente pentru lărgirea spectrului de idei pe parcursul elaborării.

Capitolul 2 definește analiza conceptului sistemului, softul și tehnologiile ce vor fi utilizate pe parcurs, automatizarea procesului și analiza vulnerabilităților ce ar putea apărea.

Capitolul 3 descrie structura generală a sistemului ce conține însuși arhitectura și procesul implementării acestuia, iar pentru demonstrarea funcționalității, va fi descris procesul de testare.

ANNOTATION

On the Master thesis “Virtual system for monitoring of cryptocurrency transactions”

elaborated by Popritac Ion. Chișinău, 2019

Keywords: Ruby, Ruby on Rails, Blockchain, Mining, P2P, SHA-256 and prime-256v1 (elliptical curve algorithm), Docker, software product, electronic cryptocurrency transaction..

The purpose of this document is to design and implement a virtual system based on Blockchain technology, which will allow internal monitoring of encrypted transactions. The base of this system is the P2P network protocol that will be decentralized, which will guarantee anonymity to the participants. The system follows the functionality of creating and generating a data block that will contain transaction history, and in order to declare ownership of the block, each participant will have its own public-private key group for identification.

The thesis aims to create and develop current application, which follows the principle of Blockchain technology, and the term "mining" used along the way, provides remuneration for the creation and validation of blocks with transaction data. The automation of the initialization and building process is done with the Docker software, which will allow the system to run in seconds.

The technologies used are: Ruby programming language for application’s core development, Ruby on Rails framework, Docker automation software, “Dry” library for structuring and implementing the code as simple as possible and corresponding style standard and SQLite3 database for storage purposes of data. The P2P network protocol allows participants to create blocks and validate its transaction, so it works as a client or server at the same time. The database will store all the information contained in the block and the necessary data will be displayed when the blockchain is displayed. In order to secure the participant's identity data, the elliptical curve algorithm is used which will not allow any disclosure of them.

The report contains Introduction, 3 chapters, conclusions, bibliography with 18 titles, 40 basic text pages, 47 figures and 2 tables.

Chapter 1: Defines the knowledge required to create the system and the technologies that already are in place, to expand the spectrum of ideas during development.

Chapter 2: Defines the analysis of the system concept, the software and the technologies to be used along the way, the process automation and the analysis of the vulnerabilities that might arise.

Chapter 3: Describes the general structure of the system that contains the architecture itself and its implementation process, and to demonstrate its functionality, the test process will be described.

CUPRINS