

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра веб-технологий и компьютерного моделирования**

ЛЮБИМОВ
Александр Андреевич

**РАЗРАБОТКА СИСТЕМЫ РАСПРЕДЕЛЕННОГО И ЗАЩИЩЕННОГО
РЕГИСТРА НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН**

Аннотация к дипломной работе

Научный руководитель:
Доцент кафедры веб-технологий
и компьютерного моделирования,
кандидат физ.-мат. наук
С.В. Суздаль

Минск, 2018

Дипломная работа содержит

- 48 страниц,
- 21 иллюстрацию (рисунок),
- 1 таблицу,
- 7 использованных источников.

Ключевые слова: БЛОКЧЕЙН, СМАРТ-КОНТРАКТ, ETHEREUM, РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ, SOLIDITY, РЕЕСТР.

Целью дипломной работы является разработка приложения с распределенным и безопасным реестром на основе технологии блокчейн.

Дипломная работа состоит из введения, двух взаимосвязанных глав, заключения и списка литературы.

В первой главе рассмотрены математические и технические основы технологии блокчейн. Автором дано описание хэш-функции и ее применения в блокчейн, цифровой подписи, основанной на асимметрической системе шифрования, одноранговой сети, алгоритмов консенсуса, лежащих в основе процедуры синхронизации.

Во второй главе приводится описание децентрализованной платформы Ethereum, которая позволяет создавать и запускать смарт-контракты, а также инструментов, предназначенных для их разработки. Во второй главе также описывается задача создания регистра на основе блокчейн на примере веб-приложения для букмекерской конторы. В работе описывается разработанная автором архитектура приложения, а также функции, доступные пользователям приложения.

В ходе выполнения работы:

- Изучены математические и технические основы технологии блокчейн;
- Изучены технологии для создания смарт-контрактов;
- Разработана архитектура веб-приложения, использующего смарт-контракты;
- Создано веб-приложение, основанное на технологии блокчейн, для ведения регистра ставок, сделанных на результаты исхода футбольных матчей.

Работа представляет интерес с практической точки зрения. Веб-приложение, созданное в рамках данной дипломной работы, может быть использовано в практической деятельности букмекерских контор. Расчет экономической эффективности не производился.

Дипломная работа выполнена автором самостоятельно.

Дыпломная работа змяшчае

- 48 старонак,
- 21 ілюстрацыю (малюнак),
- 1 табліцу,
- 7 выкарыстаных крыніц.

Ключавыя словы: БЛОКЧЭЙН, СМАРТ-КАНТРАКТ, ETHEREUM, РАЗМЕРКАВАНЫЯ СІСТЭМЫ, SOLIDITY, РЭЕСТР

Мэтай дыпломнай працы з'яўляецца распрацоўка прыкладання з размеркаваным і бяспечным рэестрам на аснове тэхналогіі блокчэйн.

Дыпломная праца складаецца з ўвядзення, двух узаемазвязаных частак, заключэння і спісу літаратуры.

У першай частке разгледжаны матэматычныя і тэхнічныя асновы тэхналогіі блокчэйн. Дадзена апісанне хэш-функцыі і яе прымянення ў блокчэйн, лічбавай подпісы, заснаванай на асіметрычнай сістэме шыфравання, аднарангавай сеткі, алгарытмаў кансэнсусу, якія ляжаць у аснове працэдуры сінхранізацыі.

У другой частке прыводзіцца апісанне дэцэнтралізаванай платформы Ethereum, якая дазваляе ствараць і запускарць смарт-кантракты, а таксама інструментаў, прызначаных для іх распрацоўкі. У другой частке таксама апісваецца задача стварэння рэгістра на аснове блокчэйн на прыкладзе вэб-прыкладання для букмекерскай канторы. У працы апісваецца распрацаваная аўтарам архітэктара прыкладання, а таксама функцыі, даступныя карыстальнікам прыкладання.

Падчас выканання працы:

- Вывучаны матэматычныя і тэхнічныя асновы тэхналогіі блокчэйн;
- Вывучаны тэхналогіі для стварэння смарт-кантрактаў;
- Распрацавана архітэктара вэб-прыкладання, які выкарыстоўвае смарт-кантракты;
- Створаны вэб-дадатак, заснаваны на тэхналогіі блокчэйн, для вядзення рэгістра ставак, зробленых на вынікі зыходу футбольных матчаў.

Праца ўяўляе цікавасць з практычнай пункту гледжання. Вэб-прыкладанне, створанае ў рамках дадзенай дыпломнай працы, можа быць выкарыстана ў практычнай дзейнасці букмекерскіх кантор. Разлік эканамічнай эфектыўнасці не вырабляўся.

Дыпломная праца выканана аўтарам самастойна.

The diploma work contains

- 48 pages,
- 21 illustrations (figures),
- 1 table,
- 7 sources used.

Keywords: BLOCKCHAIN, SMART-CONTRACT, ETHEREUM, DISTRIBUTED SYSTEMS, SOLIDITY, REGISTER.

The purpose of the thesis is to develop an application with a distributed and secure registry based on blockchain technology.

The thesis consists of an introduction, two interrelated chapters, conclusion and references.

The first Chapter describes the mathematical and technical basis of blockchain technology. The author describes the hash function and its application in the blockchain, digital signature based on the asymmetric encryption system, peer-to-peer network, consensus algorithms underlying the synchronization procedure.

The second Chapter provides a description of The Ethereum decentralized platform, which allows to create and run smart contracts, as well as tools designed for their development. The second Chapter also describes the task of creating a register based on the blockchain on the example of a web application for a bookmaker. The paper describes the application architecture developed by the author, as well as the functions available to users of the application.

In the course of the work:

- Mathematical and technical bases of blockchain technology were studied;
- Technologies for smart-contracts development were studied;
- Architecture of web applications, that is using smart-contracts, was created;
- Web application based on blockchain technology to maintain a bets register made on the results of the outcome of football matches was created.

The work is of interest from a practical point of view. Web application created within the framework of this thesis can be used by the bookmakers. The calculation of economic efficiency has not been made.

The thesis was made by the author himself.