МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Система электронных платежей

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Абдулина Дмитрия Андреевича

Научный руководитель
доцент _____ И. И. Слеповичев
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

В Интернете есть уже почти все, что может понадобиться для человека. Товары, услуги, общение, возможность самовыражения, игры и так далее. Конечно, за некоторые услуги надо платить и чем быстрее и проще система платежей, тем лучше. Потребность в подобной платежной системе начали ощущать и продавцы, и покупатели [1].

Системы электронных платежей, или сокращенно СЭП, очень распространены в мире, они зачастую используются для оплаты услуг или товаров с помощью кредитных карт, криптовалют или электронных кошельков [2].

Целью работы является рассмотрение СЭП, использующую в качестве оплаты токены, а для этого нужно предварительно ознакомиться с основными понятиями, использующимися в криптовалютных системах. Также необходимо изучить технологию распределенного реестра и его подвид под названием блокчейн.

Технологии на базе распределенного реестра стали весьма распространенными в мире в последнее время. Основным сектором, где технология приобрела наибольшую популярность, является электронная коммерция, так как для проведения всевозможных сделок требуется множество дополнительных бумаг и посредников в виде фирм, предоставляющих юридические услуги для контроля и подтверждения корректности проводимой сделки. Но с появлением и развитием технологии распределенного реестра появилась возможность уменьшить количество посредников и необходимых бумаг с помощью технологии умных контрактов, которые базируются на технологии блокчейна. Во всем мире множество крупных мировых IT-компаний и не только заинтересованы в развитии технологии распределенного реестра, блокчейна, а также непосредственно в платформе «Ethereum».

В 2017 году была основан альянс под названием «Enterprise Ethereum Alliance», на текущий момент в его состав входит более 150 участников. Одними из основных участников альянса являются такие компании как Microsoft, Intel, Accenture. Первым российским участником стал «Сбербанк» [3][4].

Компания Microsoft на база технологии блокчейн совместно с ООН создает систему цифровой идентификации личности под названием «ID2020», которой можно будет воспользоваться в любом месте. Прототип данной системы был создан на блокчейн-протоколе «Enterprise Ethereum Alliance» [5].

В России данной технологией в первую очередь заинтересовались банки.

5 октября 2016 года ЦБ РФ объявил о запуске платформы «Мастерчейн», предназначенной для обмена информацией между участниками финансового рынка. Технология «Мастерчейн» основана на протоколах Ethereum [6].

В данной работе более подробно рассмотрим каждый из аспектов распределенного реестра и одну из популярных технологий под названием «Ethereum», позволяющей создавать сервисы на базе блокчейна.

Основной практической целью является написание приложения, предоставляющего место на жестком диске, с оплатой через токен, и реализация взаимодействия между узлами на базе умных контрактов и Блокчейна. Также задачей является создание своего собственного токена на базе платформы Ethereum.

Дипломная работа состоит из введения, 8 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 57 страниц, из них 42 страницы – основное содержание, включая 20 рисунков и 1 таблицу, список использованных источников из 25 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе описывается система электронных платежей. Приводится классификация систем на дебетовые и кредитные. Описываются основные критерии, предъявляемые к системам электронных платежей. Озвучиваются проблемы, с которыми сталкиваются как пользователи систем, так и их создатели. И рассматриваются три модели представления систем электронных платежей.

Второй раздел описывает что из себя представляет технология распределенного реестра. Приводится несколько видов классификации сетей распределенного реестра. Описываются кем могут быть пользователи сети и приводятся основные преимущества сетей распределенного реестра.

Третий раздел посвящен технологии «Блокчейн», которая является подвидом распределенного реестра. Приводится несколько видов Блокчейна, также описывается внутренняя структура цепочек и блоков. Рассказывается об основных особенностях технологии и приводится схема обмена валют с помощью технологии Блокчейн.

В разделе номер четыре содержится информация об основных криптографических методах, что используются в распределенных реестрах и Блокчейне.

Первый подраздел в четвертом разделе описывает основную технологию, что используется в сетях распределенного реестра и Блокчейне, – это хэширование. Во втором подразделе приводится описание процедуры вычисления хэш-функции ГОСТ Р 34.11-2012 (Стрибог).

Третий и четвертый подраздел описывают электронную цифровую подпись и основные технологии, на которых она строится.

Раздел под номером пять содержит информацию о том, что такое умные контракты, принципы работы и состав умных контрактов, а также основные

функции, которые исполняет умный контракт и особенности данной технологии.

Шестой раздел посвящен описанию криптовалюты и токена, в чем их основные отличия и основные сферы применения.

Седьмой подраздел посвящен платформе Эфириум, как представлена технология Блокчейн, транзакции и умные контракты в нем. Также содержит описание основных инструментов для работы в среде Эфириум, а именно язык программирования, что используется для создания умных контрактов в Эфириум.

В восьмом разделе содержится описание интерфейса программы «Хранилище данных». Приводится пример работы приложения, его основные выходные данные.

Показано окно входа в систему, где пользователь вводит свои данные для входа, а именно логин и пароль. После перед пользователем предстает интерфейс приложения позволяющий пользоваться следующим функционалом:

Функционал «Добавление файлов в хранилище» позволяет выбрать необходимый файл для дальнейшей отправки его в хранилище.

Функционал «Открыть хранилище» позволяет просмотреть хранилище и скачать файл на локальный компьютер.

Функционал «Расширить хранилище» позволяет увеличить доступное дисковое пространство хранилища.

Показана реализация функционала расширения хранилища данных, а именно выбор нужного количества места для расширения. Далее создается файл, с необходимыми данными, который необходим для формирования умного контракта и подтверждения получения оплаты.

ЗАКЛЮЧЕНИЕ

В наши дни все больше внимание уделяется скорости и надежности проведения сделок, так что необходимо иметь надежный инструмент для их совершения, обладающий высокой скоростью и наибольшей безопасностью.

Технология распределенного реестра и подвид Блокчейн – это один из тех инструментов, что развивается в данном направлении и заинтересовал большой пласт компаний не только работающих в коммерции, но и множество IT-компаний, для которых данная технология открывает большие горизонты развития.

В ходе работы была изучена система электронных платежей, ее основные определения, а так же технология распределенного реестра и что она из себя представляет. Ознакомились более подробно с Блокчейн, который является подвидом распределенного реестра. Были изучены и разработаны умные контракты для совершения сделок в системе под названием «Ethereum». Был создан токен на базе платформы «Ethereum» и написано приложение, предоставляющее место на жестком диске с оплатой через токен.

Таким образом, все поставленные задачи выполнены в полной мере.

Данные из работы могут быть использованы для создания любого сервиса, использующего токены в качестве оплаты. А сами сервисы могут быть любого назначения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Вихарева, Д. С. Электронные деньги. Современная схема компактных электронных денег на билинейных группах [Электронный ресурс]. Загл. с экрана. Яз. рус.

2 Научная работа по теме: «Электронные деньги» [Электронный ресурс] // StudentBank [Электронный ресурс]. URL : http://studentbank.ru/view.php?id=50750 (дата обращения: 04.11.2018) Загл. с экрана. Яз. рус.

3 Enterprise Ethereum Alliance [Электронный ресурс] // EntethAlliance [Электронный ресурс]. URL : https://entethalliance.org (дата обращения 04.11.18). Загл. с экрана. Яз. англ.

4 «Сбербанк» стал первым российским банком в составе Enterprise Ethereum Alliance [Электронный ресурс] // CoinMarket.News [Электронный ресурс] : интернет-журнал о криптовалютах, блокчейне и технологиях. URL : https://coinmarket.news/2017/10/18/sberbank-stal-pervym-rossijskim-bankom-v-sostave-enterprise-ethereum-alliance/ (дата обращения: 04.11.2018). Загл. с экрана. Яз. рус.

5 ООН, Microsoft и другие компании работают над системой цифровой идентификации на основе блокчейн для лиц, лишённых документов [Электронный ресурс] // ITC.UA [Электронный ресурс] : ведущий украинский информационный ресурс об IT. URL : https://itc.ua/news/oon-microsoft-i-drugie-kompanii-rabotayut-nad-sistemoy-tsifrovoy-identifikatsii-na-osnove-blokcheyn-dlya-lits-lishyonnyih-dokumentov/ (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

6 Мастерчейн ЦБ РФ: есть ли что-то принципиально новое в государственном блокчейне? [Электронный ресурс] // Crypto fox [Электронный ресурс] : статьи обзоры по криптовалютам и блокчейну. URL : https://crypto-

fox.ru/article/masterchain-rf/ (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

7 Развитие технологии распределенных реестров [Электронный ресурс] // Центральный банк Российской Федерации [Электронный ресурс]. URL : http://www.cbr.ru/Content/Document/File/36007/reestr_survey.pdf (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

8 Что такое распределенный реестр? [Электронный ресурс] // BlockChainDesk.ru [Электронный ресурс] : Блокчейн и криптовалюта. URL : https://blockchaindesk.ru/blockchain/chto-takoe-raspredelennyj-reestr (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

9 Генкин, А. С. Блокчейн. Как это работает и что ждет нас завтра [Электронный ресурс] : учеб. пособие / А. С. Генкин, А. В. Михеев. Альпина Паблишер, 2018. 592 с. Загл. с экрана. Яз. рус.

10 Что такое Blockchain (блокчейн)? Технология распределенного реестра [Электронный ресурс] // Майнинг Криптовалюты [Электронный ресурс] : информационно-аналитический портал. URL : https://mining-cryptocurrency.ru/blockchain/ (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

11 Что такое блокчейн и для чего он нужен [Электронный ресурс] // BestInvestpro [Электронный ресурс]. URL : http://bestinvestpro.com/blokchejn-chto-eto-ponyatnym-yazykom/ (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

12 Хэширование [Электронный ресурс] // No.1 ВС [Электронный ресурс] : сайт о шифровании. URL : http://backup.autolifeinfo.com/ru/support/articles/datahashing/ (дата обращения: 02.12.2018). Загл. с экрана. Яз. рус.

13 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. [Электронный ресурс] : учеб. пособие / Б. Шнайер. Триумф, 2002. 816 с. Загл. с экрана. Яз. рус.

14 ГОСТ Р 34.11—2012 Информационная технология. Криптографическая защита информации. Функция хэширования.

15 ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

16 Смарт-контракт [Электронный ресурс] // wikipedia.org [Электронный ресурс] : свободная энциклопедия. URL : https://ru.wikipedia.org/wiki/Смарт-контракт (дата обращения 2.12.2018). Загл. с экрана. Яз. рус.

17 Что такое «умный» контракт [Электронный ресурс] // VisINVEST [Электронный ресурс] : Инвестиционный путеводитель. URL : https://visinvest.net/chto-takoe-smart-kontrakty.html (дата обращения: 02.12.2018). Загл. с экрана. Яз. рус.

18 Токен [Электронный ресурс] // wikipedia.org [Электронный ресурс] : свободная энциклопедия. URL : https://ru.wikipedia.org/wiki/Токен (дата обращения 2.12.2018). Загл. с экрана. Яз. рус.

19 Чем токены отличаются от криптовалюты [Электронный ресурс] // ECRYPTO [Электронный ресурс]. URL : https://ecrypto.ru/kriptovalyuta/chem-tokeny-otlichayutsya-ot-kriptovalyuty-i-kak-na-nih-zarabatyvat.html (дата обращения: 02.12.2018). Загл. с экрана. Яз. рус.

20 Ethereum [Электронный ресурс] // Ethereum BLOCKCHAIN APP PLATFORM [Электронный ресурс]. URL : https://www.ethereum.org (дата обращения: 02.12.2018). Загл. с экрана. Яз. англ.

21 Ethereum [Электронный ресурс] // wikipedia.org [Электронный ресурс] : свободная энциклопедия. URL : https://ru.wikipedia.org/wiki/Ethereum (дата обращения 2.12.2018). Загл. с экрана. Яз. рус.

22 Что такое Эфириум (Ethereum) простыми словами [Электронный ресурс] // Prosto Coin [Электронный ресурс] : проводник в мире криптовалют. URL : https://prostocoin.com/blog/what-is-ethereum (дата обращения: 02.12.2018). Загл. с экрана. Яз. рус.

23 Как работает Эфириум (Ethereum)? [Электронный ресурс] // habr [Электронный ресурс] : крупнейший в Европе ресурс для IT-специалистов. URL : https://habr.com/post/407583/ (дата обращения: 02.12.2018). Загл. с экрана. Яз. рус.

24 Solidity [Электронный ресурс] // wikipedia.org [Электронный ресурс] : свободная энциклопедия. URL : https://ru.wikipedia.org/wiki/Solidity (дата обращения 2.12.2018). Загл. с экрана. Яз. рус.

25 Solidity [Электронный ресурс] // solidity.readthedocs.io [Электронный ресурс]. URL : https://solidity.readthedocs.io/en/v0.4.21/ (дата обращения: 02.12.2018). Загл. с экрана. Яз. англ.