УДК 004.04 Вестник УрФО № 3(29) / 2018, с. 23–28

Гончаренко Ю. Ю., Паво Ф. Н.

DOI: 10.14529/SECUR180304

РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННОГО ПРИЛОЖЕНИЯ ДЛЯ РЕАЛИЗАЦИИ ЦИФРОВОЙ ИДЕНТИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

В данной работе были проанализированы виды архитектур систем, выявлены их преимущества и недостатки. Приведены аргументы в пользу децентрализованных систем и способы достижения децентрализации. Одним из выявленных эффективных методов децентрализации является цепочка блоков – блокчейн. В работе был произведен анализ свойств и структуры блокчейна, исследованы методы обеспечения безопасности и достижения консенсуса между участниками сети. Рассмотрены преимущества децентрализованных приложений в сравнении с традиционными централизованными. Проанализированы популярные платформы для разработки децентрализованных приложений и выявлена наиболее оптимальная платформа для реализации приложения. Рассмотрены основные функции умного контракта Ethereum и методы взаимодействия с блокчейн-сетью средствами программного кода. Были исследованы популярные приложения на технологии блокчейн и направления их применения. В отличии от подобных статей с исследованием технологии блокчейн, в данной работе был представлен вариант реализации собственного приложения с использованием блокчейн платформы Ethereum. Разработанное приложение позволяет производить регистрацию и авторизацию пользователя. В данной работе были описаны основные функции и интерфейс приложения. Также его можно использовать как модуль для более сложных систем. Например, в системах голосования, контрольно-пропускных пунктов и других, где требуется идентификация пользователя и надежное хранилище учетных данных.

Ключевые слова: *блокчейн, децентрализации, Ethereum, идентификация, авторизация, умный контракт, приложений, цифровая подпись, QR-код.*

DEVELOPMENT OF A DECENTRALIZED APPLICATION FOR THE IMPLEMENTATION OF DIGITAL IDENTITY USING BLOCKCHAIN TECHNOLOGY

In this paper, the types of system architectures were analyzed, their advantages and disadvantages were revealed. The arguments in favor of decentralized systems and ways to achieve decentralization are presented. One of the effective methods of decentralization identified is the chain of blocks - block. In this work, the analysis of the properties and structure of the block was carried out, methods of ensuring security and achieving consensus between the participants of the network were explored. The advantages of decentralized applications are compared with traditional centralized ones. Analyzed popular platforms for the development of decentralized applications and identified the most optimal platform for implementing the application. The main functions of the smart contract Ethereum and the methods of interaction with the blockchain network by means of program code are considered. Popular applications on the technology of blockades and the direction of their application were investigated. Unlike similar articles with research on blockchain technology, in this paper we presented an implementation version of our own application using the Ethereum platform block. The developed application allows you to register and authorize the user. In this paper, the main functions and interface of the application were described. It can also be used as a module for more complex systems. For example, in voting systems, checkpoints and others, where you need to identify the user and a reliable store of credentials.

Keywords: *blocking, decentralization, Ethereum, identification, authorization, smart contract, applications, digital signature, QR code.*

В наше время, с ростом вычислительных мощностей открываются новые возможности и способы построения приложений. Растет и количество ценной информации, обрабатываемой приложениями. Появляется необходимость использовать новые, более защищенные системы для обработки и сохранения целостности данных.

Еще недавно, такая технология как Интернет в корне изменила подход к созданию программного обеспечения, заменив полностью клиентские приложения клиент-серверными. Теперь же, клиент-серверные приложения постепенно вытесняются децентрализованными. Централизованная архитектура имеет свои недостатки и проблемы безопасности. Децентрализованные приложения на основе технологии Блокчейн позволяют избавиться от посредников, обеспечить отказоустойчивость и предотвратить потерю или порчу данных.

Таким образом, выделяют три основных архитектуры систем: централизованная, распределенная децентрализованная [4]. В наше время наибольшей популярностью пользуются централизованные приложения. С появлением сети Интернет практически все приложения используют централизованную архитектуру.

Централизованные системы предполагают единый центр обработки и хранения данных – сервер. На стороне сервера, как правило, обрабатываются пользовательские данные и критически важные операции. Например, авторизация пользователя, хранение и

обработка его персональных данных, или различные финансовые транзакции.

Данный подход является наиболее распространенный и экономически выгодный в наше время. Существует, как правило, одна точка отказа которую несложно поддерживать и масштабировать. Но централизованные системы требуют от пользователя полного доверия, так как работают по принципу «черного ящика» и только владельцу сервиса известно, как именно обрабатываются пользовательские данные и не передаются ли они третьим лицам. Также подобные системы имеют множество уязвимостей и злоумышленник, получивший доступ к единому центру, получает контроль над всеми данными пользователей.

Децентрализованная архитектура подразумевает исключение центрального узла и равномерное распределение полномочий между всеми участниками сети. Подобные сети также называют одноранговыми или пиринговыми, где каждый узел выполняет роль сервера и клиента и функционирует независимо от других узлов. Данная структура позволяет сети продолжать работу даже при отключении или выходе из строя одного из узлов и обеспечивает масштабируемость сети в целом. Одной из важнейших характеристик децентрализованной архитектуры является полная открытость и прозрачность ее работы, что предотвращает различные скрытые действия на стороне сервера.

Можно выделить три основные преимущества децентрализации:

– отказоустойчивость – децентрализованные системы менее подвержены случайным ошибкам, так как они полагаются на множество отдельных компонентов, ошибка в которых менее вероятна;

– устойчивость к атакам – децентрализованные системы более массивные дорогостоящие, чтобы их атаковать, так как в них исключены центральные точки воздействия, которые можно атаковать с гораздо меньшими затратами, чем экономические размеры всей инфраструктуры;

– стойкость к сговору – участникам децентрализованных систем гораздо труднее вступать в сговор, чтобы получить выгоду от менее скоординированных участников.

Технология одноранговых сетей и их применение исследуется многими разработчиками. Но уже сейчас есть множество вариантов реализации технологии децентрализованных сетей.

Одна из областей применения децентрализованных сетей – это обмен файлами. В подобных торрент-сетях узел размещает файл, другие узлы получают возможность загрузить его. При этом загрузка может происходить сразу с нескольких источников. Наибольшую популярностью имеют цифровые валюты: Bitcoin, Ethereum, Litecoin и также реализации децентрализованного облачного хранилища – такие проекты как: Storj, Sia, MaidSafe, Decent, LBRY Credits, FileCoin и другие [3].

Большинство подобных проектов использует специальную технологию хранения данных и транзакций – цепочку блоков. Данная технология нашла свое применение в децентрализованных системах благодаря своим уникальным свойствам и характеристикам, что позволяет эффективно распределять информацию по всем узлам и обеспечивать ее целостность и подлинность.

Реализовать децентрализацию наиболее эффективно позволяет распределенный реестр – блокчейн.

Несмотря на новизну технологии, существует множество решений и блокчейн-платформ для реализации полноценных децентрализованных приложений. Количество приложений и их аудитория стремительно возрастает, все больше сфер услуг охватывают приложения с использованием данных платформ, которые постоянно совершенствуются с учетом недостатков своих предшественников Большинство из них решают многие проблемы централизованных приложений и предоставляют удобные интерфейсы для разработки. Чем больше узлов в сети, тем она безопаснее, в следствии большей децентрализации. Следовательно, для реализации децентрализованного приложения нет необходимости разрабатывать собственную блокчейн-сеть, достаточно использовать проверенные и более безопасные платформы.

Наиболее развитой структурой и сообществом обладают блокчейн-сети Ethereum и Bitcoin. В январе 2018 года группой ученых Корнеллского университета были опубликованы результаты исследования степени децентрализации перечисленных платформ [1]. Было выявлено, что сеть Bitcoin имеет большую пропускную способность, в отличии от Ethereum, но узлы первой более сконцентрированные и, вероятно, содержатся в датацентрах, что нарушает принципы децентрализации. По данным исследования около 56 процентов узлов Bitcoin сконцентрированы в

дата-центрах, в то время как у Ethereum 28 процентов.

Следовательно, для реализации децентрализованного приложения предпочтительней использовать наиболее распространенные платформы. Среди которых можно выделить блокчейн Ethereum.

Для взаимодействия с блокчейном Ethereum существует множество программных решений. Среди них различные библиотеки для интеграции блокчейна Ethereum в приложения. В разработке децентрализованного приложения была использована библиотека web3 и расширение браузера Metamask для доступа к учетным записям Ethereum и взаимодействия с умным контрактом.

Умный контракт состоит из хранилища учетных записей и функций для регистрации и извлечения данных учетных записей. В хранилище записываются такие данные как: имя, фамилия, пол, дата регистрации и публичный адрес в сети Ethereum с которого производилась регистрация.

Было разработано веб-приложение использующее расширение Metamask и функции умного контракта.

Интерфейс приложения представляет собой панель навигации и основные разделы:

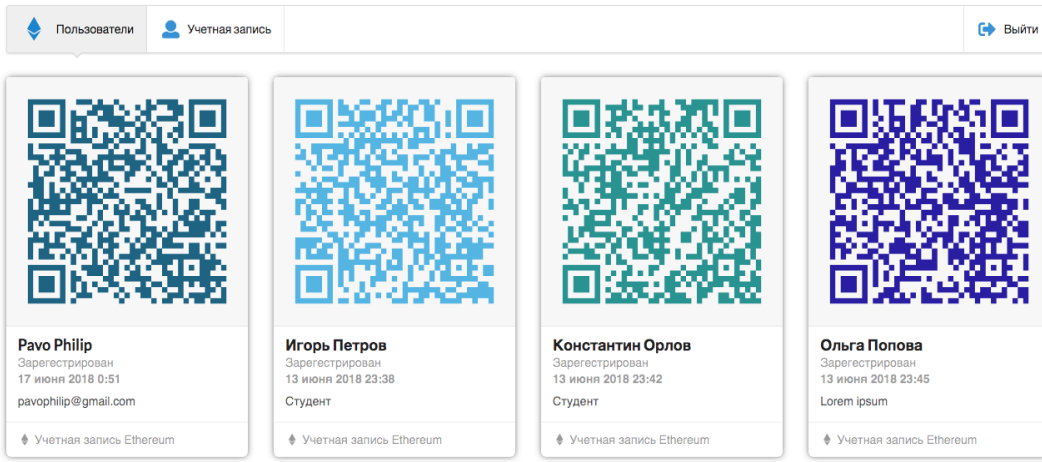

Рис. 1. Раздел с учетными записями пользователей

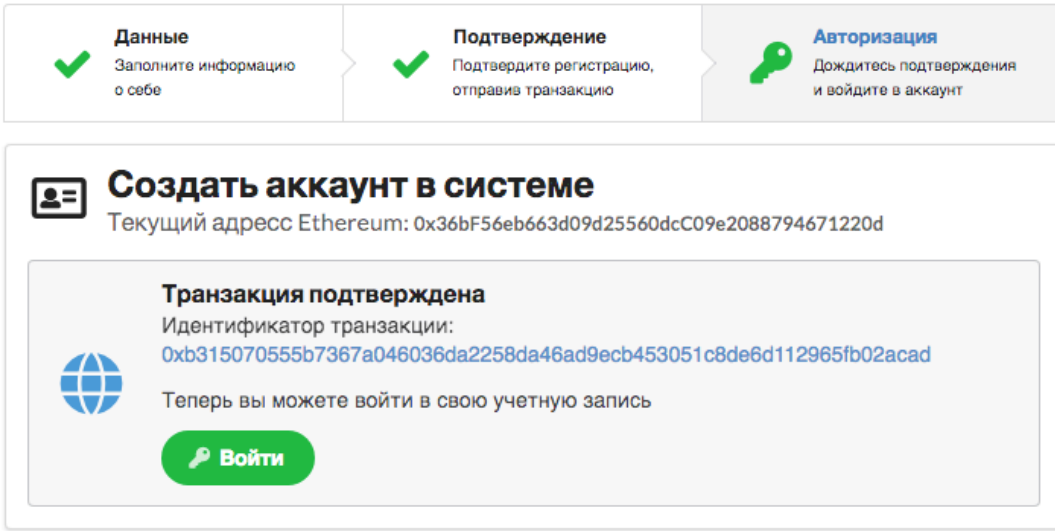

Рис. 2. Создание учетной записи.

– список зарегистрированных пользователей;

– форма создания учетной записи;

– форма авторизации;

– карточка пользователя.

На главной странице расположен список

зарегистрированных пользователей. Карточка учетной записи состоит из QR-кода (Quick Response Code) с уникальной ссылкой на учетную запись, имени пользователи, даты и времени регистрации, дополнительной информации, которая была указана при регистрации. Также присутствует ссылка на информацию о кошельке Ethereum с которого производилась регистрация (рис. 1) и ссылка на кошелек в etherscan.io [2].

После чего будет создана запись в хранилище умного контракта. Для каждого зарегистрированного пользователя генерируется QR со ссылкой на его учетную запись.

Для авторизации и идентификации пользователя необходимо выполнить цифровую подпись с использованием своего приватного ключа (рис. 3). Это делается также с помощью расширения Metamask.

Данное приложение позволяет создавать учетные записи и идентифицировать пользователя без использования сервера. Все данные хранятся децентрализовано в сети Ethereum.

В контракте можно реализовать хранение дополнительных данных, а также данных в зашифрованном виде либо файлов, что позволит пользователю надежно хранить важную информацию децентрализовано. Умный контракт может наследовать другие контракты, следовательно, данное приложение может быть использовано как модуль для других систем, таких как голосование, что обеспечит точный подсчет и невозможность подделки голосов или систему для проверки прав на владение цифровыми ресурсами и произведениями.

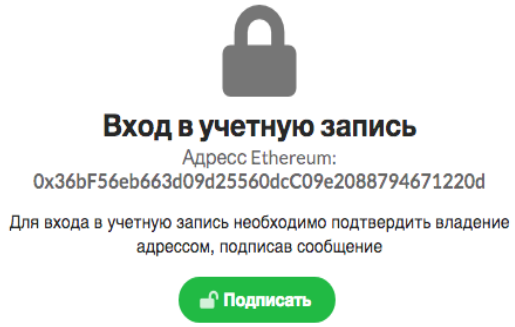

Рис. 3. Сообщение об успешной проверке подписи.

Литература

1. Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer. Decentralization in Bitcoin and Ethereum Networks [Электронный ресурс] / Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer // Financial Cryptography and Data Security 2018. – Режим доступа: URL: https://arxiv.org/abs/1801.03998v2. – (дата обращения: 03.04.2018).

2. Etherscan [Электронный ресурс] - URL: https://ethersan.io

3. Jay J.Wylie, Michael W., Bigrigg, John D. Strunk Survivable Information Storage Systems // Computer. 2000. Volume 33, Issue 8, p. 61-68

4. The Meaning of Decentralization [Электронный ресурс] - URL: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

References

1. Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer. Detsentralizatsiya v setyakh Bitcoin i Ethereum [Elektronnyy resurs] / Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer // Finansovaya kriptografiya i bezopasnost' dannykh 2018. - Rezhim dostupa: URL: https://arxiv.org /abs/1801.03998v2. - (data obrashcheniya: 03.04.2018).

2. Etherscan [Elektronnyy resurs] - URL: https://ethersan.io

3. Jay J.Wylie, Michael W., Bigrigg, John D. Strunk Survivable Information Storage Systems // Komp'yuter. 2000. Tom 33, vypusk 8, str. 61-68

4. Znacheniye detsentralizatsii [Elektronnyy resurs] - URL: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

ГОНЧАРЕНКО Юлия Юрьевна, доктор технических наук, доцент, про-фессор кафедры «Информационная безопасность» ФГАОУ ВО «Севасто-польский государственный университет». Россия, 299053, г. Севастополь, ул. Университетская 33. E-mail: luliay1985@mail.ru.

ПАВО Филипп Николаевич, студент 1 курса магистратуры кафедры «Информационная безопасность» ФГАОУ ВО «Севастопольский государственный университет». Россия, 299053, г. Севастополь, ул. Университетская 33. E-mail: pavophilip@gmail.com.

GONCHARENKO Julia, doctor of technical Sciences, associate Professor, Professor of "Information security" FSAEI HE "Sevastopol state University". Kurchatov street 7, Sevastopol, Russian, 299015. E-mail: Iuliay1985@mail.ru.

PAVO Philip, student of the 1st year of the master's degree of the "Information security" FSAEI HE "Sevastopol state University". Kurchatov street 7, Sevastopol, Russian, 299015. E-mail: pavophilip@gmail.com.