УДК 004.03

С. Н. Ткаченко, Д. А. Казакова, С. А. Демин

СПОСОБЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОЙ ОБРАБОТКИ ИНФОРМАЦИИ В ДЕЦЕНТРАЛИЗОВАННЫХ ПРИЛОЖЕНИЯХ

Балтийский федеральный университет им. И. Канта, Калининград, Россия

Поступила в редакцию 22.02.2022 г.
Принята к публикации 13.03.2022 г.

Для цитирования: *Ткаченко С. Н., Казакова Д. А., Демин С. А.* Способы обеспечения надежной обработки информации в децентрализованных приложениях // Вестник Балтийского федерального университета им. И. Канта. Сер. Физико-математические и технические науки. 2022. №1. С. 40—44.

Изложены возможности децентрализованных приложений, проанализировано их функционирование. Рассмотрены способы обеспечения надежности и безопасности использования децентрализованных приложений.

Ключевые слова: блокчейн, банк, информационные технологии, внедрение, эффективность управления

Одной из динамично развивающихся отраслей являются банковское дело и растущие финансовые экосистемы. При работе в подобных сложных информационных агломерациях возникает обязательная потребность в обеспечении безопасности всех операций, прежде всего денежных транзакций. Этим обусловлена актуальность вопросов, связанных с децентрализованными или распределенными системами и обеспечением безопасности работы в сети Интернет.

Децентрализованные приложения представляют собой один из новых типов программного обеспечения и новых видов организации. Такое приложение основано на применении технологии блокчейн. Distributed Ledger — это децентрализованная база данных, которая содержит информацию обо всех осуществленных транзакциях. Уникальная ее особенность заключается в том, что одинаковые копии «распределяются» по нескольким серверам хостинга и хранения, подтверждая транзакции, записанные в «пакете», непрерывным процессом. Непосредственно за осуществлением аутентификации «пакет» блокируется криптографическим «хэшем» и в дальнейшем позволяет хостам аутентифицировать входящие данные с возможным извлечением [1, с. 35]. Технология распределения дает возможность осуществлять сделки анонимно, оперативно и без привлечения посредников. Использование техно-

логии уменьшает вероятность мошенничества, так как предоставляет право на отслеживание истории активов и транзакций в пределах источника достоверных данных.

Распределенные реестры и возможности блокчейна лежат в основе «децентрализованных приложений» [2, с. 13]. Приложение является децентрализованным, если соответствует следующим критериям:

1. Открытый исходный код. Приложение должно быть открытым в полной мере и работать автономно, а также иметь организации, которым принадлежит большая частью его токенов. Приложение может корректировать свой протокол в ответ на предоставленные улучшения, но все последующие изменения необходимо осуществлять с согласия всех пользователей.

2. Децентрализация. Данные и отчеты о производительности необходимо хранить в открытом доступе.

3. Стимуляция. Необходимо применять токены или цифровые активы для поощрения сторонников в сети.

4. Протокол. Генерация токенов должна происходить в соответствии с эталонным криптографическим алгоритмом, работающим как доказательство содержания узлов в распределенном приложении.

Работа децентрализованного приложения основана на следующих методах:

1. Способ получения консенсуса. Возможно использование двух алгоритмов, при применении которых децентрализованные приложения могут генерировать разрешение: proof-of-work и proof of stake. В дополнение к алгоритму proof-of-work решения о модификации децентрализованного приложения основаны на объеме работы, которую каждый участник выполняет при реализации приложения. Такой подход используется, например, в Биткойне и Эфириуме. В случае применения алгоритма proof-of-stack изменения децентрализованного приложения основаны на доле заинтересованных сторон. Поэтому приложение Omni Protocol основано на механизме POS. Оба этих метода также можно использовать параллельно. Это сочетание делает децентрализованные приложения на 51 % более устойчивыми к атакам.

2. Способ распределения токенов. Применяют три известных метода распределения токенов децентрализованными приложениями: майнинг, коллаборация и фандрайзинг. Во время майнинга токены выделяются тем, кто участвует в улучшении функционала децентрализованного приложения. Этот метод используется в Биткойне. При осуществлении фандрайзинга токены также распределяются среди тех, кто изначально финансировал разработку децентрализованных приложений. При коллаборации токены генерируются с использованием предопределенных методов и доступны только для создания децентрализованных приложений.

В зависимости от типа используемого блокчейна различают следующие типы децентрализованных приложений:

1. Децентрализованные приложения, построенные на собственном блокчейне.

2. Децентрализованные приложения, использующие блокчейн первого типа. Это типы протоколов децентрализованных приложений, которые генерируют токены, необходимые для их работы. Omni Protocol — пример второго типа децентрализованных приложений.

3. Децентрализованные приложения, применяющие протокол других типов приложений, такие как сеть SAFE (использует протокол Omni для выпуска криптовалюты Safecoins).

В децентрализованных приложениях применение блокчейн технологий предоставлено в качестве решения проблем безопасности и надежности обработки данных. К примеру, обеспечение безопасности удовлетворяется за счет проверки транзакции, информация о которой хранится в защищенной от злоумышленников памяти. Поскольку историю операций можно восстановить при помощи блокчейна, предположение защищенности не сужает безопасность приложения в целом. Выбранная концепция позволяет вводить ограничения на технологию блокчейн, которые хранят транзакции определенным способом, позволяющим осуществить проверку в короткий срок.

Возникающая проблема может быть решена при использовании криптографии с открытым ключом. Всем непосредственным пользователям приложения должна быть выделена пара закрытых и открытых ключей. Открытый ключ возможно выпустить в открытый доступ для прямой идентификации цифровой личности пользователя. Эксплуатация цифровых подписей предоставляет возможность решения проблем прав, а также значимых проблем с изменчивостью транзакций. В том случае, когда цифровая подпись работает для всех транзакций в блокчейне, злоумышленники, разрешившие внутренний доступ к приложению, не смогут модифицировать эти транзакции.

Применение блокчейна обеспечивает надежность и безопасность информационных технологий, а так же предотвращает все возможные атаки, в частности нападения Man-in-the-Middle (MITM), которые включают зашифрованные соединения (такие, как HTTPS и TLS) для безопасных каналов и основываются на инфраструктуре аутентификации с открытым ключом (PKI) и центрах сертификации (CA). Каждая сеть имеет открытый и закрытый ключ. Когда пользователь хочет осуществить установку безопасного соединения, он производит запрос исходного открытого ключа из центра аутентификации и осуществляет шифровку данных, перед тем как их отправить. Сайт использует собственный ключ для расшифровки данных. Степень защиты системы зависит от безопасности центра сертификации. При осуществлении MITM-атаки происходит распространение поддельных открытых ключей, среди которых у хакера есть соответствующий закрытый ключ, и при их применении передаваемые данные расшифровываются. Но поскольку в системе на основе блокчейн MITM исключается, при публикации пользователем открытого ключа для блокчейна об этом «узнают» все узлы. Данная информация записана в блок, а шифрование на основе блокчейна защищает целостность реестра. Например, Pomcore

предлагает проект на основе блокчейна для хранения хэшей выпущенных и отозванных сертификатов. Этот метод позволяет пользователям проверять сертификаты, оптимизируя доступ к сети.

Следующий тип атаки — манипулирование данными — может произойти с различной информацией, находящейся в сети. Тем не менее в блокчейн-системе сетевой партнер имеет возможность опубликовать различные хэши, которые имеют непосредственную связь с конкретным файлом и другими данными, требующими надежной защиты. Если случится сбой или намеренный взлом системы и хакеры получат информацию и откорректируют ее или подменят, у них не будет возможности зафиксировать количество хэшей в блокчейне. Стартап GuardTime рекомендует применять платформу подписи без ключа, включающую в себя хэши данных и файлов, и осуществляет тщательную проверку копии с использованием алгоритмов хэширования. Предложенный подход предоставляет возможность осуществить модификацию процесса аутентификации с использованием ключей.

В итоге отметим, что блокчейн позволяет обеспечить совершенно иной подход для высоконадежной обработки информации, в том числе к защите критической инфраструктуры, пользовательских данных, каналов связи и бизнес-процессов организаций. Но необходимо обозначить, что существуют и некоторые технические проблемы, например плохая масштабируемость, тенденция к централизации, проблема доверия к данным.

Тем не менее используемые технические решения на базе технологии блокчейн находят все большее применение в самых разных отраслях современной инфраструктуры, от медицины до банковских услуг. Получаемая надежность информационных систем при использовании блокчейн-решений, как правило, перевешивает необходимые затраты на их внедрение и дальнейшую поддержку.

Список литературы

1. *Равал С.* Децентрализованные приложения. Технология Blockchain в действии. СПб., 2017.

2. *Генкин А.С., Михеев А.А.* Блокчейн: Как это работает и что ждет нас завтра. М., 2018.

Об авторах

Сергей Николаевич Ткаченко — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград, Россия.

E-mail: tkasergey@yandex.ru

Дарья Александровна Казакова — магистрант, Балтийский федеральный университет им. И. Канта, Калининград, Россия.

E-mail: darya.kazakova.99@list.ru

Сергей Александрович Демин — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград, Россия.

E-mail: SDemin@kantiana.ru

S.N. Tkachenko, D.A. Kazakova, S.A. Demin

WAYS TO ENSURE RELIABLE INFORMATION PROCESSING IN DECENTRALIZED APPLICATIONS

Immanuel Kant Baltic Federal University, Kaliningrad, Russia
Received 22 February 2022
Accepted 13 March 2022

To cite this article: Tkachenko S.N., Kazakova D.A., Demin S.A. 2022, Ways to ensure reliable information processing in decentralized applications, *Vestnik of Immanuel Kant Baltic Federal University. Series: Physical-mathematical and technical sciences*, №1. P. 40–44.

The article outlines the possibilities of decentralized applications and analyzes their functioning. The ways of ensuring the reliability and security of the use of decentralized applications are considered.

Keywords: blockchain, bank, information technology, implementation, management efficiency

The authors

Dr Sergey N. Tkachenko, Associate Professor, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.
E-mail: tkasergey@yandex.ru

Daria A. Kazakova, Master's Student, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.
E-mail: darya.kazakova.99@list.ru

Sergey A. Demin, Assistant Professor, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.
E-mail: SDemin@kantiana.ru