Безопасность электронных платежей при использовании блокчейн технологий

Афошина Арина Дмитриевна, студентка 3-ого курса финансового факультета РЭУ им. Г.В. Плеханова, г. Москва, Российская Федерация

E-mail: Arishka.afoshka@mail.ru

Норова Анастасия Юрьевна, студентка 3-ого курса финансового факультета РЭУ им. Г.В. Плеханова, г. Москва, Российская Федерация

E-mail: nastyanorova18@gmail.com

Научный руководитель: Жданова Ольга Александровна, к.э.н., доцент кафедры «Финансовый менеджмент», РЭУ им. Г.В. Плеханова, г. Москва, Российская Федерация

E-mail: Zhdanova.OA@rea.ru

Аннотация

Блокчейн технологии стали новой вехой развития современных финансовых рынков. В статье рассматриваются основные аспекты безопасности электронных платежей, которые основаны на технологии блокчейн. Приведены аргументы в поддержку блокчейн технологий как наиболее безопасных систем, а также рассмотрены риски, сопутствующие развитию и повсеместному применению данной технологии.

Ключевые слова: блокчейн, криптовалюты, безопасность, электронная наличность, децентрализованная система, биткойн**.**

Security of electronic payments using blockchain technologies

Afoshina Arina Dmitrievna, student, Plekhanov Russian University of Economics, Moscow, Russian Federation

E-mail: Arishka.afoshka@mail.ru

Norova Anastasiya Yurevna, student, Plekhanov Russian University of Economics, Moscow, Russian Federation

E-mail: nastyanorova18@gmail.com

Scientific Advisor: Zhdanova Olga Aleksandrovna, PhD, Associate Professor, Plekhanov Russian University of Economics, Moscow, Russian Federation

E-mail: Zhdanova.OA@rea.ru

Annotation

Blockchain technology has become a new milestone in the development of modern financial markets. The article deals with the main aspects of security of electronic payments, which are based on blockchain technology. The arguments in support of blockchain technologies as the most secure systems are given, as well as the risks associated with the development and widespread use of this technology are considered.

Keywords: blockchain, cryptocurrencies, security, electronic cash, decentralized system, bitcoin.

Сегодня каждый человек слышал о том, что не так давно денежные отношения получили новый виток своего развития. В сфере финансовых рынков произошла своего рода эволюция: образовалась новая ступень существования денег, которая стала инновационной формой оплаты и накопления денежных средств. Этот уровень сначала именовался как «электронная наличность», а впоследствии получил термин «криптовалюты». По своей сути это особый механизм электронного обмена цифровых активов, эмиссия которых, чаще всего, не является централизованной. Другими словами, новый уровень развития денег уже не подразумевает наличие главного органа управления, который является неким гарантом безопасности (как, например, Центральный Банк РФ для рубля, ФРС для доллара, ЕЦБ для евро). Сегодня эту безопасность обеспечивают компьютеры, имеющие в своем арсенале тысячи гигабайт информации о всех транзакциях внутри системы.

Стандартной базой для обращения электронной наличности является построенная по определенным правилам последовательная и непрерывная цепочка блоков информации, называемая определением «блокчейн». Впервые данная технология была использована именно при реализации пиринговой платежной системы Биткойн, однако впоследствии технология взаимосвязанных цепочек блоков стала распространяться и на другие сферы жизни. Сегодня основные инструменты этой технологии используются во многих секторах существования общества: в финансах, в банковской деятельности, при государственном управлении и т.д. [2]

Безусловно, главным и приоритетным местом применения блокчейна по сей день остается сфера криптовалют и электронных платежей. Более того, прослеживается четкая настающая тенденция развития этого сектора экономики, во многом из-за понимания все большим количеством людей преимуществ данной технологии. Так называемые криптоанархисты уверяют, что инновационная технология не только перевернет мир сильнее, чем в свое время Интернет, она станет отправной точкой в построении нового

общества, которое не будет иметь политических границ и зависимости от мегарегуляторов валютного рынка, чаще всего действующим исходя из собственных интересов в ущерб интересам остальных участников рынка. Принцип работы «электронной наличности», основанной на технологии блокчейн, можно увидеть на рисунке 1.

Рис. 1. Схема работы системы блокчейн [4]

В настоящий момент ведется множество дискуссий о безопасности этой технологии в мире огромного количества взломщиков, а также специалистов по копированию и «угону» конфиденциальной информации, денежных средств и других данных пользователя. Для того, чтобы разобраться в этой проблеме, следует рассмотреть основные аспекты и особенности защиты системы блокчейн.

Базисом данной технологии является децентрализованный реестр записей всех финансовых транзакций. Это означает, что одиночный компьютер или система не сможет получить доступ к общей базе данных, поскольку вся информация хранится не в одном общеизвестном месте, а разбита на тысячи разных частей на разных устройствах. Если блок-цепь хранится на крупной широко распределенной сети, защищенной от внешних и внутренних атак, то взломщику требуется собрать в одно целое большой объем информации для получения доступа к зашифрованным данным [3].

Из этого можно сделать однозначный вывод о том, что получить несанкционированный контроль над всеми данными одновременно либо невозможно, либо крайне сложно для реализации. Автору хакерской атаки для взлома данных будет необходимо знать не только весь перечень устройств, на которых хранятся данные, но и

получить скоординированный доступ ко всем ним в один и тот же момент. На практике возможность осуществления такого сценария крайне мала.

Другой отличительной особенностью исключительной безопасности этой технологии является тот факт, что блокчейн строится не по принципу единственной транзакции, а состоит из большой цепи последовательных блоков транзакций. Иными словами, основной реестр записей представлен длинной цепью последовательных данных. Общая структура состоит из нескольких сотен блоков цепочки, начало которой идет от самой первой операции, произошедшей в данной системе. Следовательно, чтобы изменить информацию какой-либо транзакции, сначала необходимо изменить все записи, которые ведут к этой транзакции. Вот почему даже гипотетическое вмешательство в систему является труднейшим способом получения или изменения данных в системе блокчейн.

По своей сути блокчейн дает возможность людям, не доверяющим друг другу, делиться информацией высокой важности защищенным и безопасным способом. В цепочке блоков хранятся данные, состоящие из крайне сложных инновационных алгоритмов и математических правил, которые чрезвычайно трудно преодолеть путем взлома или хакерской атаки для последующего использования информации в корыстных целях.

Эту технологию делают теоретически защищенной от незаконного доступа два аспекта: уникальный для каждого блока криптографический ключ и так называемый «консенсусный протокол» (под ним понимается процесс, посредством которого узлы в сети согласуются со всей историей транзакций).

Генерация (т.е. формирование) уникального кода, именуемого «хешем», требует большого количества энергии и времени. Он является доказательством того факта, что для создания блока в цепочке был проделан некоторый объем вычислительной работы. По итогу проделанного труда создатель блока (майнер) получает определенное вознаграждение за расход своей вычислительной мощности. Именно поэтому алгоритм большинства криптовалют, основанных на технологии блокчейн, в том числе алгоритм создания новых блоков Биткоина, называется «доказательством выполненной работы». Более того, наличие хеша в системе служит своего рода монолитной печатью, а это значит, что для изменения когда-либо созданного блока потребуется генерация нового уникального кода.

Система блокчейн осуществляет проверку соответствия хеша определённому блоку, и как только этот процесс завершается, обновляются все соответствующие копии блочной цепи после присоединения нового блока. Такой алгоритм имеет название «консенсусный протокол» [1].

Кроме вышеназванных пунктов, существуют и другие элементы, которые обеспечивают защиту технологий блокчейна. Во-первых, обеспечение и подтверждение безопасности проводимых транзакций подтверждают более двух пользователей. У большинства современных пиринговых систем проверка обеспечивается только несколькими уровнями верификации (особыми подтверждениями) – со стороны продавца, со стороны покупателя и со стороны третьих лиц (банков или кредитных агентств). Однако в технологии блокчейна присутствует комплекс из нескольких сотен (а иногда и тысяч) разного рода узлов, на которых хранится копия реестра абсолютно каждой записи. Вот почему любой из этих узлов может быть использован при проверке транзакции: если транзакция не пройдет проверку хотя бы одним из узлов, то ее реализация будет отменена. Данная функциональная возможность снижает риски создания мошеннической или ложной транзакции до минимальных значений.

Во-вторых, одним из важнейших аспектов современной кибербезопасности являются криптографические ключи, которые повсеместно используются в работе технологии блокчейн. Каждый такой ключ в зашифрованном виде представляет из себя сложнейшую, длинную и практически неподдающуюся для расшифровки последовательность данных. Следует также отметить, что для подтверждения транзакции требуется не один, а целых два криптографических ключа одновременно, что делает эту систему сложной для взлома как человеком, так и искусственным интеллектом. По мнению многих экономистов и финансистов, которые называют себя приверженцами технологии блокчейн, в настоящий момент в мире нет компьютера, способного одновременно подбирать по несколько криптографических ключей для каждого блока огромной цепи системы блокчейн. Считается, что описываемая технология обладает уникальной по своим свойствам системой безопасности, поскольку при всей надежности от взлома и подмены данных удается сохранить практически максимальную прозрачность, которой славится вся система блокчейн и связанная с ней сфера криптовалют [5].

Безусловно, при всех положительных аспектах системы блокчейн, существуют определенные риски,сопутствующие развитию и повсеместному применению данной технологии. Любому пользователю технологии необходимо знать и учитывать слабые места и потенциально уязвимые стороны, чтобы снизить риски потерь информации, ценных данных и денежных средств. В таблице 1 представлены основные особенности блокчейна, которые иллюстрируют самые незащищенные места системы.

Исходя из названных рисков, можно сделать определенный вывод о том, что система блокчейн хоть и очень безопасна, она все равно имеет некоторые слабые стороны.

Безусловно, технический прогресс не стоит на месте, а значит, вместе с ним будут развиваться и технологии взаимосвязанных цепочек блоков, пиринговых систем, электронной наличности. Однако в настоящий момент, блокчейн и криптовалюты, созданные на его основе, следует использовать предельно аккуратно и правильно с учетом всех рисков и возможностей. Также необходимо понимать, что безопасность этой технологии во многом зависит не от ошибок в компьютерном коде или неправильной работы алгоритмов системы, а из-за пресловутого человеческого фактора, который является корнем большинства слабых мест блокчейн технологий.

Таблица 1

Самые незащищенные места системы blockchain[1]

Наименование	**Расшифровка**
Сложность системы	Среднестатистический пользователь «электронной наличности» может не до конца осознавать и взвешивать риски, связанные с использованием системы. Более того, даже человек имеющий современное финансовое образование может не знать о всех системах безопасности и доступном функционале, который имеет массу инструментов защиты данных. В связи с этим мошенники могут с легкостью завладеть информацией, которую в последующем используют для взлома кошелька или «угона» данных.
Размеры, скорость и эффективность сети	Как было описано выше, блокчейн функционирует на основе огромного количества взаимосвязанно работающих узлов. Именно по этой причине система является уязвимой к атакам хакеров на начальных этапах своего развития. Например, если один компьютер сможет получить контроль более, чем над 51 процентов узлов системы, основанной на блокчейн технологии, то он будет иметь возможность контроля всей системы в целом. А в тот момент, когда система получает слишком широкое распространение, есть вероятность появления проблем с хранением данных и скоростью проведения транзакций.
Политика использования	В начале статьи было отмечено, что система блокчейна является децентрализованной и распространенной по всему миру (т.е. международной). При распространении и использовании криптовалют повсеместно, по сути, будет происходить обесценивание национальных валют ведущих государств, которые начнут терять влияние на денежные средства, обращающиеся в стране. Уже сейчас правительства развитых стран пытаются взять под контроль использование блокчейн технологий, понимая тот факт, что однажды «электронная наличность» может стать серьезным конкурентом национальной валюте. Чаще всего этот контроль осуществляется через систему законодательных актов, которые, в свою очередь, препятствуют развитию и замедляют распространение технологии блокчейн.

[1] Составлено автором

На сегодняшний день можно смело утверждать, что блокчейн имеет такой уровень безопасности, который во многом превосходит большинство других систем обмена данными (в том числе платежных), а это значит, что технология в настоящий момент более, чем актуальна и потому она имеет все предпосылки к тому, чтобы стать главным изобретением XXI века в сфере финансов и IT-технологий.

Список использованных источников

1. Федеральный закон от 02.12.1990 № 395-1 (ред. от 03.07.2016) «О банках и банковской деятельности» (с изм. и доп., вступ. в силу с 01.01.2017).
2. Laurie B., Clayton R. (2004) Proof-of-Work Proves Not to Work, 42 p.
3. Morabito V. (2017) Big data and analytics. Springer International Publishing, 188 p.
4. Scoping SIG, Tokenization Taskforce PCI Security Standards Council (2011) Info Supplement: PCI DSS Tokenization Guidelines, 23 p.
5. The future of financial infrastructure [электронный ресурс] – Режим доступа. – URL: https://bravenewcoin.com/assets/Industry-Reports-2016/WEF-The-future-of-financial-infrastructure.pdf (дата обращения: 16.09.2018).

References

1. Federal'nyi zakon ot 02.12.1990 № 395-1 (red. ot 03.07.2016) «O bankakh i bankovskoi deyatel'nosti» (s izm. i dop., vstup. v silu s 01.01.2017).
2. Laurie B., Clayton R. (2004) Proof-of-Work Proves Not to Work, 42 p.
3. Morabito V. (2017) Big data and analytics. Springer International Publishing, 188 p.
4. Scoping SIG, Tokenization Taskforce PCI Security Standards Council (2011) Info Supplement: PCI DSS Tokenization Guidelines, 23 p.
5. The future of financial infrastructure https://bravenewcoin.com/assets/Industry-Reports-2016/WEF-The-future-of-financial-infrastructure.pdf