УДК 004.056.2
DOI: 10.33764/2618-981X-2021-6-219-224

АНАЛИЗ КРИПТОВАЛЮТ И ПРОБЛЕМЫ РАЗВИТИЯ БЛОКЧЕЙНА

Максим Иванович Недобежкин
Сибирский государственный университет телекоммуникаций и информатики, 630009, Россия, г. Новосибирск, ул. Гурьевская, 51, магистрант кафедры прикладной математики и кибернетики, тел. (906)994-66-12, e-mail: firkis@yandex.ru

Андрей Николаевич Фионов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, профессор кафедры информационной безопасности, тел. (383)269-82-16, e-mail: a.fionov@ieee.org

В статье рассматривается история возникновения криптовалют, их преимущества и недостатки, также рассматривается блокчейн, причем особое внимание уделено проблемам развития этой технологии.

Ключевые слова: криптовалюта, блокчейн, история криптовалют, проблемы развития криптовалют

ANALYSIS OF CRYPROCURRENCIES AND PROBLEMS OF BLOCKCHAIN DEVELOPMENT

Maxim I. Nedobezhkin
Siberian State University of Telecommunications and Information Sciences, 51, Gurievskaya St., Novosibirsk, 630009, Russia, Graduate, Department of Applied Mathematics and Cybernetics, phone: (906)994-66-12, e-mail: firkis@yandex.ru

Andrew N. Fionov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Professor, Department of Information Security, phone: (383)269-82-16, e-mail: a.fionov@ieee.org

This article examines the history of the emergence of cryptocurrencies, their advantages and disadvantages, and also considers the blockchains, where special attention is paid to the problem of the development of this technology.

Keywords: cryptocurrency, blockchain, history of cryptocurrency, cryptocurrency development

Введение

Криптовалюта – это виртуальные деньги, которые существуют только в электронном виде. Их использование похоже на использование электронных писем, при их использовании не вовлекаются посредники, например, банк. Это позволяет ускорить выполнение операций и минимизировать комиссию. Хранится такая криптовалюта на специальном аккаунте, который является электронным кошельком. Данные о платежах и транзакциях существуют только как за-

писи в базе данных. Транзакции являются анонимными, так как нет никакой информации о владельце аккаунта. Криптовалюта является одной из многих возможностей использования технологии блокчейн, а биткоин – самая распространенная из криптовалют. Рынок альтернативных криптовалют расширяется ежедневно. По последним данным, их уже несколько сотен и число их постоянно растет. Наиболее популярные криптовалюты – Bitcoin, Ethereum, Ripple, Litecoin, Peercoin, NXT и Namecoin [1]. Любой желающий может не только добывать имеющуюся криптовалюту, но даже создать собственную. Для получения криптовалюты существуют разные способы добычи (майнинга), например, классический, облачный, и т.д. Получить криптовалюту можно только от того, у кого она уже есть, в обмен на разные услуги, реальные деньги, как безвозмездное пожертвование. Зачастую для обмена криптовалютой пользователи используют различные существующие площадки, но это не является обязательным условием. Котировки различных площадок в одно и тоже время могут сильно различаться. В настоящее время ни одна из площадок не имеет соответствующей регистрации и биржевой лицензии. Таким образом, сделки на них, их клиенты не попадают под действие биржевого законодательства стран [2].

Криптовалюта – один из самых популярных способов использования блокчейн технологий.

В 2014 году на сайте Bitcoin Magazine автором Кеном Гриффитом, являющимся соучредителем компании Dinero Limited, которая представляет из себя платформу с богатым инструментарием для обмена цифровыми валютами, размещена статья, где история блокчейна рассматривается начиная с периодов, предшествующих появлению первой криптовалюты, когда идеи лишь отдаленно напоминали то, что мы видим сейчас. Основы криптовалют были разработаны в 1992 году киберпанками — неформальной группой людей, заинтересованных в сохранении анонимности и интересующихся криптографией. В 1993 году американский программист Эрик Хьюз заявил о возможности обеспечения конфиденциальности совершаемых платежных операций путем многоэтапного шифрования [3].

Поскольку блокчейн — это достаточно новая и еще развивающаяся технология, официального и исчерпывающего определения ей нет. Приведем определение данного понятия, с которым согласны ряд деятелей, изучающих данную технологию.

Блокчейн (англ. block chain или blockchain) — это цепочка блоков с информацией. Она является связным непрерывным списком и обеспечивает надежное хранение записей обо всех когда-либо совершенных транзакциях. Объем цепочки блоков растет по мере добавления информации о новых транзакциях. Каждый участник представлен узлом (node), который хранит весь актуальный массив данных и контактирует с другими узлами. Узлы могут добавлять новые записи в конец списка, а также сообщают друг другу об изменениях списка [4]. На своем сайте Андерс Браунворт реализовал демоверсию блокчейна, которую можно проверить и понять, как технология работает [5].

Анализ преимуществ и недостатков криптовалют

Перейдем к рассмотрению преимуществ и недостатков криптовалют. Проведенный анализ позволяет выявить ряд достоинств.

1. Высокая скорость транзакций. Скорость транзакции определяется временем, которое требуется для выполнения одной операции перевода. Большая скорость обеспечивает высокое качество обслуживания и большую дальнейшую доступность и работоспособность системы. Многие перешли к данной технологии во многом из-за этого преимущества, которое выгодно отличается от нынешней финансовой скорости транзакций, особенно это касается переводов между странами.

2. Безопасность. В результате создания криптовалюты получается цифровой регистр транзакций, который хакерам взломать довольно трудно. К тому же, для осуществления транзакции иногда требуется двухфакторная аутентификация.

3. Универсальность. Так как криптовалюта не привязана ни к одному государству, она одинаково доступна и для владельца из Санкт-Петербурга, и для владельца из Нью-Йорка.

4. Независимость. Криптоденьги не привязаны ни к одной существующей валюте, ни к цене на нефть, ни к любым другим активам. Ни одна операция и ни одна существующая криптовалюта никем не администрируется. Это гарантирует стопроцентную доставку перевода, так как нет посредника.

5. Отсутствие инфляции. Из-за способа создания криптовалюты количество монет ограничено, так что создать много монет и таким образом обесценить валюту не получится.

6. Открытость и публичность. Открытость подразумевает целый ряд преимуществ. Благодаря открытости с высокой долей вероятности продукт получается качественный. Легко и быстро устраняются ошибки, повышается степень оптимизации, пропадают временные рамки. Хорошее ПО создается совместными усилиями и доступно абсолютно всем желающим.

7. Анонимность. Делая перевод с одного криптокошелька на другой, мы не можем видеть, кто именно стоит за данным кошельком, мы видим только цифровые адреса кошельком и сумму отправления.

8. Возможность зарабатывать. Сегодня на криптовалюте можно зарабатывать разными способами. Для примера можно привести электронные торги, инвестирование, майнинг и много других.

Теперь перечислим выявленные недостатки криптовалют:

1. Отсутствие должного юридического урегулирования и гарантий. Криптовалюта не материальна, на нее нет прав собственности. Не существует способа, с помощью которого можно было бы идентифицировать вора (из-за анонимности и децентрализованности), а также подтвердить свое право на монеты (из-за отсутствия закона о личной собственности), если они были каким-то образом украдены. Тоже самое происходит и в случае, если перевод был выполнен на недоброжелательную личность. Также при инвестировании в обанкротившуюся компанию свои деньги вернуть назад не получится.

2. Недостаточная распространенность. Многие люди ничего не знают о криптовалютах, а пользуются ими еще меньше людей. Из-за этого использовать криптовалюты в повседневной жизни все еще довольно сложно.

3. Нестабильный курс. Одной из причин этого является ограниченность. Это может привести к дефляции, когда стоимость криптовалюты будет снижаться по мере ее вхождения в общее пользование. Еще одной причиной является децентрализованность. Раз отсутствует какой-либо орган управления, то никто не может поддерживать минимальную стоимость криптовалюты, и если большинство инвесторов решит отказаться от криптовалюты и выбросит на рынок много монет, то крайне велик риск, что курс рухнет.

4. Вирусы и киберпреступность. Так как криптовалюта является программой, то она подвержена вирусам. Можно потерять все свои сбережения, если не озаботться способами защиты. Но и они не дают стопроцентной гарантии безопасности. Помимо программ вредоносного характера, атаки киберпреступников также являются проблемой. При столь малом возрасте криптовалюты как технологии и способа ведения бизнеса, уже большое количество бирж подверглось атакам злоумышленников, для которых криптовалюта, из-за своей стоимости, представляет большую ценность.

5. Отсутствие идентификации клиента. Если злоумышленник получит данные для доступа к кошельку, вы никак не сможете отменить перевод или вернуть доступ к своему счету.

6. Сложность добычи. Майнинг требует высоких вычислительных возможностей. Многие вкладывают большие средства в создание так называемых майнинговых ферм, которые представляют из себя компьютеры с самым мощным и дорогим оборудованием. Также растет потребление электроэнергии. Таким образом, для эффективной добычи потребуется вложить много средств и времени.

Проблемы развития системы блокчейн

В настоящее время специалисты пришли к выводу о ряде проблемных моментов в развитии системы блокчейн, равно как и том, что данная технология была несколько преждевременно названа универсальной и совершенной.

Итак, блокчейн-технология функционирует с некоторыми ограничениями. Рассмотрим ключевые лимиты, которые характерны для технологии блокчейна, а также сложности, возникающие при использовании технологического решения для целей коммерции.

Приступим к аналитическому обзору лимитов блокчейна как современной электронной технологии:

– система блокчейн не имеет безупречного уровня секретности. По условиям технологии формируется реестр, который позволяет обмениваться трафиком между участниками системы и получать данные по всем выполненным транзакциям. Следовательно, указать на высокую секретность транзакций, проводимых по блокчейн-технологии, невозможно, так как система исходно создана как прозрач-

ная, чтобы эффективно функционировать и осуществлять замысел разработчиков. Но большое число участников системы, способных получить информацию о транзакции, нередко заставляет отказаться от блокчейна, если программный продукт нуждается в повышенной конфиденциальности данных и операций [6];

– сценарий защиты технологии блокчейна предполагает применение асимметричных криптографических решений, позволяющих идентифицировать и аутентифицировать стороны, получающие доступ к системе, равно как и при входе на аккаунт для проведения транзакции. Проведение транзакций осуществляется только при сопровождении распоряжения электронной подписью. Если электронная подпись становится известна посторонним в результате ошибки, случайности, перехвата данных, то аккаунт нельзя рассматривать как защищенный [7];

– система блокчейн характеризуется необоснованно высокими эксплуатационными затратами, так как система имеет категорию ограниченно масштабируемой. Проведение хэш-процедуры, за которой следует одобрение транзакции и уведомление об ее исполнении более чем трудоемко, однако именно этим замыслом руководствовались разработчики, требуя огромных ресурсов для решения этой задачи, а хронологический порядок проведенных транзакций изменить более чем сложно [8];

– систему блокчейн не следует характеризовать как гибкую технологию, так как работа блокчейна достигается в итоге согласования множества архитектурных элементов, принципов и протоколов, совмещенных и адаптированных для выполнения конкретных функций [9];

– система не имеет высокого доверия с точки зрения закона;

– система имеет трудности с регуляцией эволюции технологии блокчейн нормами законодательства [10];

– есть сложность завоевания доверия среди населения.

Заключение

Блокчейн – это технология, у которой есть большая область применения. Потенциально эта технология охватывает все без исключения сферы экономической деятельности. Однако, несмотря на все преимущества, она не является универсальной. Также ее использование в технологии создания криптовалюты имеет ряд ограничений и проблем, которые, в связи с растущим влиянием криптовалют, нужно обязательно учитывать и нельзя игнорировать.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мащенко П.Л., Пилипенко М.О. Технология Блокчейн и ее практическое применение // Наука, техника, образование. – Олимп, 2017. – № 32. – С. 61–64.

2. Хажиахметова Е.Ш. Криптовалюта – деньги XXI века // Новая наука: от идеи к результату. – Агентство международных исследований, 2016. – № 11-2. – С. 177–179.

3. Антонопулос А. Осваиваем биткойн. Программирование блокчейна. – М.: ДМК Пресс, 2018. – 428 с.

4. Интернет-энциклопедия: [Электронный ресурс] – Режим доступа: URL: http://ru.wikipedia.org/wiki/Bitcoin/. (Дата обращения: 15.04.2021).

5. Равал С. Децентрализованные приложения. Технология Blockchain в действии. – СПб.: Питер, 2017. – 240 с.

6. Костень Д. Биткоин – как новая форма товарно–денежных отношений. Блокчейн – как новая форма инфраструктуры. Платформа как новая форма управления проблемы формирования правового социального государства в современной России // Материалы XII всероссийской научно-практической конференции «Проблемы формирования правового социального государства в современной России». – Новосибирский государственный аграрный университет, 2016. – С. 46-51.

7. NIST, “Specifications for a Digital Signature Standard (DSS),” Federal Information Processing Standards Pub. xx (Draft), Aug. 19, 1991, 12 pps.

8. G. J. Simmons, “Subliminal Communication is Easy Using the DSA,”Eurocrypt’93, Lofthus, Norway, May 23–27, 1993, pp. 218-232. In: Advances in Cryptology, Lecture Notes in Computer Science, vol. 765, Springer, 1993.

9. Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах. – М.: ДМК Пресс, 2018. – 312 с.

10. Демченко И.А., Колесникова Н.А. Современные технологии финансового менеджмента в российских компаниях // Экономика управление в XXI веке: тенденции развития. – 2016. – № 29. – С. 125–129.