Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2022, №6, Том 14 / 2022, No 6, Vol 14 https://esj.today/issue-6-2022.html

URL статьи: https://esj.today/PDF/46ECVN622.pdf

Ссылка для цитирования этой статьи:
Самусевич, В. Е. Анализ развития системы биткоин и блокчейн / В. Е. Самусевич // Вестник евразийской науки. — 2022. — Т. 14. — № 6. — URL: https://esj.today/PDF/46ECVN622.pdf

For citation:
Samusevich V.E. Analysis of the development of the bitcoin and blockchain system. *The Eurasian Scientific Journal*. 2022; 14(6): 46ECVN622. Available at: https://esj.today/PDF/46ECVN622.pdf. (In Russ., abstract in Eng.).

УДК 314

Самусевич Владимир Евгеньевич
ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Факультет «Налогов, аудита и бизнес-анализа»
Бакалавр
E-mail: vladimirsamusevich06@gmail.com

Анализ развития системы биткоин и блокчейн

Аннотация. В данной статье автор рассматривает вопрос развития криптовалюты биткоин и blockchain. Автор подчеркивает, что электронные платежные системы и виртуальные валюты представляют собой достаточно новое и быстро захватывающее все страны явление. Биткоин является самой популярной криптовалютой, созданной в 2009 году. Важно отметить, что первое время данная валюта пользовалась совсем небольшим спросом у программистов и заинтересованных пользователей. Также данная валюта была распространена среди торговцев оружием и наркотиков и криптоанархистов, что негативно отражалось на развитии биткоина. Многие страны видели в нем угрозу угрозу монополии национальных валют и запрещали ее. В статье приведены основные особенности системы биткоин. Автор акцентирует внимание на том, что первые попытки создания электронных денег предпринимались ещё в 1998 году, однако они не увенчались успехом и были впоследствии прекращены. Создателем системы биткоин является Сатоши Накамото (организация под псевдонимом или человек). Активный рост курса биткоин валюты начался в 2011 году после того, как появился сервис для обмена — Bitcoin Market. Затем, в 2012 году, была создана биржа MtGox, которая производила обмен и вывод виртуальных денег в реальность. Автор также выделяет 2013 год, который стал одновременно периодом как краха, так и взрывного роста криптовалюты. Относительно стабильное и размеренное развитие биткоина началось с 2016 года. Автор подчеркивает, что многие путают биткоин и цепочку блоков. В связи с этим в статье приведена дефиниция данных понятий, а также их сравнение. В заключительной части статьи автор в результате проведенного исследования приходит к выводу о том, что система биткоин является самозапускающейся, самовоспроизводящейся и самомасштабируемой.

Ключевые слова: биткоин; блокчейн; виртуальные валюты; виртуальные карты; деньги; криптовалюта; международные банковские переводы; международные экономические отношения; национальные валюты; функции денег; экономика; электронные деньги

Введение

До недавних пор Биткоин был известен только узкому кругу экспертов финансовой сферы. Игнорирование криптовалюты официальной властью большинства государств имеет вполне обоснованные причины, но безразличие со стороны научных изданий к альтернативной

виртуальной денежной единице вызывало удивление. В последнее время, наметилась тенденция к улучшению и Биткоин не сходит с передовиц СМИ. Его сущность, становление и роста курса является темой многочисленных дебатов на страницах периодических печатных издании.

Цепочка блоков — это главная инновация, которая была разработана в процессе развития системы биткоин. Каждый отдельный блок цепочки имеет единственный путь к родительскому блоку (genesis block). Однако от родительского блока могут быть и раздвоения (форки). Неограниченное количество майнеров может создавать блоки.

Если это транзакция по передаче биткоинов, то она может быть включена в очередной блок. Транзакции получения вознаграждения за создания отсечённых блоков не дублируются в другой ветке, то есть «лишние» биткоины за отсечённые блоки не получают дальнейших подтверждений и «утрачиваются».

Цель исследования — рассмотреть процесс развития системы биткоин и блокчейн.

Объектом исследования выступает взаимосвязь понятий «биткоин» и «блокчейн».

Предметом исследования является трансформация экономических отношений в процессе развития системы биткоин и блокчейн.

1. Методы и материалы

При написании работы были использованы научные методы, которые основаны на требованиях объективного и всестороннего факторного анализа: монографический, абстрактно-логический, системно-структурный. Кроме того, работу составляют принципы дедукции и индукции в обработке информации, статистические методы обработки массивов информации, методы анализа и синтеза.

В соответствии с поставленной целью решаются следующие задачи:

1. Рассмотреть историю появления биткоина.
2. Проанализировать состояние биткоина в настоящее время.
3. Изучить технологию блокчейна и ее применение.
4. Проанализировать развитие блокчейна и биткоина.

В процессе проведения данного исследования использовались работы отечественных специалистов в данной области. Наибольшее внимание уделялось работам Коварда В.В. [1], Булгакова И.Т. [2], Баско О.В. [3], Тапскотт Д. [4], Генкина А. [5] и других авторов.

2. Результаты и обсуждения

Развитие электронных платежных систем и виртуальных валют представляет собой новое и быстро захватывающее все страны явление.

Криптовалюта Bitcoin является на сегодняшний день самой популярной среди других виртуальных валют, она была создана в 2009 году, и практически никого на тот момент не интересовала. Использовали ее между собой лишь программисты и заинтересованные пользователи. Со временем биткоин деньги привлекли к себе небывалое количество внимания, начиная от обычных пользователей до высокопоставленных лиц. Котировки данной валюты росли с огромной скоростью, и на данный момент можно точно сказать, что рост стоимости этой валюты составил более 800000 %.

46ECVN622
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Особенности системы (рис. 1):

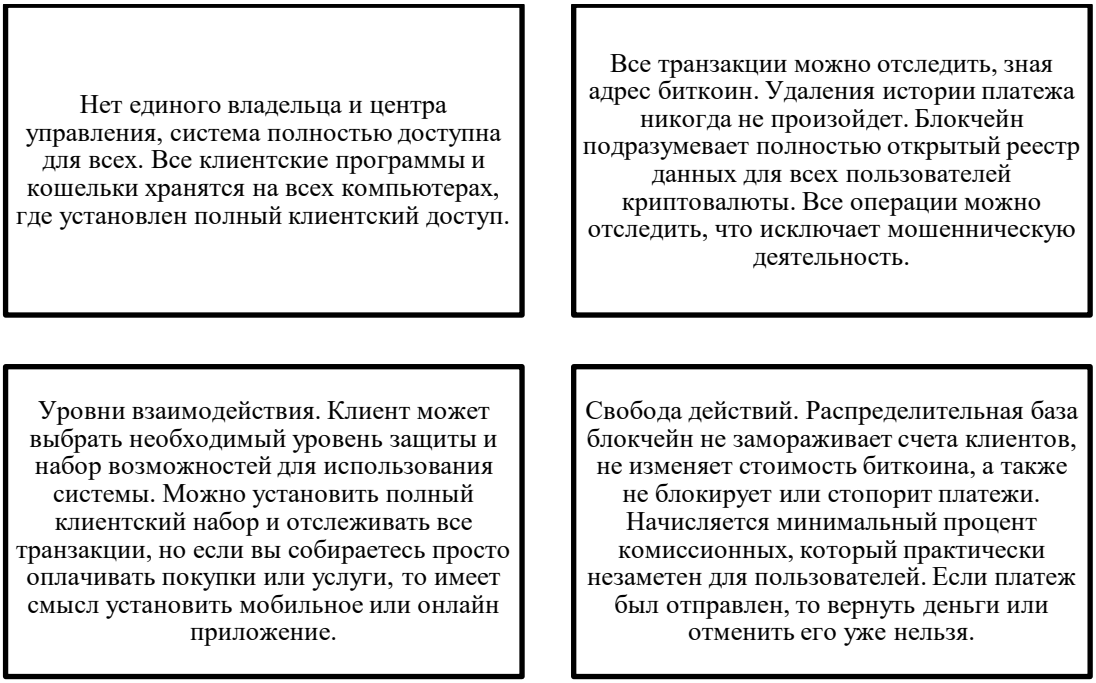

Рисунок 1. *Особенности системы [6]*

По сути, биткоин является огромной вычислительной децентрализованной сетью с надежной защитой от взлома и мощнейшей производительностью.

Предпосылки к созданию электронных денег появились еще в 1998 году, Ник Сзабо создавал надежную системы виртуальных денег битголд вплоть до 2005 года, но потом разработки прекратились. Затем 6 лет назад возникли наработки в этой области от Сатоши Накамото, создателя будущей системы биткоин. Сатоши Накамото (человек или организация под псевдонимом) создали первые пятьдесят bitcoin монет, затем через определенное количество суток осуществили перевод от одного человека к другому. Курс биткоина вычислялся довольно просто: средняя мощность компьютера умножалась на цену за электроуслуги в США, и вся эта сумма делилась на количество, выпущенных биткоин монет [7].

В начале 10-ых годов XX века отслеживался быстрый рост курса биткоина. В связи с этим в мире начали открываться первые обменные пункты и биржи.

В 2010 появился сервис для обмена Bitcoin Market, и в том же году пользователь Laszlo сумел приобрести две пиццы за 10 000 биткоинов, что подстегнуло рост курса этой валюты в разы.

В 2012 году произошел прорыв в развитии криптовалюты: была создана биржа MtGox, функции которой заключались в осуществлении обмена и вывода криптовалюты в реальность [8]. Она продолжает действовать и в настоящее время, с помощью нее можно осуществлять различные операции с криптовалютой.

Однако необходимо подчеркнуть, что указанная биржа действовала в совокупности с рынком SilkRoad, который был нелегальным. Несмотря на это криптовалюта получала всю большую популярность по всему миру.

2012 год был не самым простым этапом развития биткоина, поскольку тогда на биржу было совершено несколько хакерских атак. Это привело к некоторым негативным последствиям. В частности, цена одного биткоина была снижена, зашифрованные данные

46ECVN622
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

пользователей были потеряны и украдены. По этим причинам биржа была вынуждена закрыться на неделю, чтобы восстановить защиту данных.

2013 год выдался весьма противоречивым, поскольку, с одной стороны, он был полон громких скандалов и проблем в сфере криптовалюты, с другой — произошел пик роста криптовалюты. Этот факт подтверждается статистическими данными за 2013 год (табл. 1).

Таблица 1

Динамика стоимости одного биткоина [9]

Дата	Стоимость биткоина
Январь 2013	31 доллар
Апрель 2013	100 долларов
Октябрь 2013	300 долларов

Однако 2013 год характеризуется и большим количеством неприятностей. В частности, с помощью криптовалюты осуществлялись денежные операции по покупке оружия и наркотиков на нелегальных сайтах. Это привело к еще большему повышению котировки биткоина до 1200 долларов.

После того, как вскрылась эта информация, контроль за сферой криптовалют был усилен. Стоимость биткоина резко снизилась в два раза.

Стоит отметить, что интерес к криптовалюте растет среди россиян. Например, не так давно, Германом Грефом было объявлено о возможном создании аналога биткоина. Однако необходимо акцентировать внимание и на том, что хакеры тоже повысили свою активность: совершается все больше попыток кражи личных данных пользователей. Очевидным является тот факт, что система безопасности еще не до конца развита, в связи с чем автор считает целесообразным уделить большее внимание данному вопросу.

Можно сказать, что несмотря на недоработки и недостатки системы, она имеет массу плюсов и получает всю большую популярность в силу своего удобства [10].

Мир узнал о криптовалюте Биткойн 21 октября 2008 года из научной статьи некоего Сатоши Накамото «Bitcoin: A Peer-to-Peer Electronic Cash System», в которой описывалась система, известная нам под названием «цепочки блоков». Через 70 дней была запущена первая валюта на ее основе — Биткойн.

Изначально запущенная как закрытая система, Биткойн получил свое развитие как открытая и анонимная система, способная противостоять слежке и цензуре. Криптовалюты по определению не привязаны к государствам или географии.

Еще одна особенность, что легитимность криптовалюты основана на консенсусе, то есть нет центрального органа, который бы разрешал споры или каким-то образом регулировал действие системы.

Первыми, кто стал использовать новую технологию, стали торговцы наркотиками, оружием, криптоанархисты. Многие государства (Россия в том числе) увидели в Биткойне угрозу монополии национальных валют и просто ее запретили.

Но, несмотря на запреты, технология заработала. Относительно недавним доказательством вхождения технологии в мейнстрим стало создание консорциума из 40 банков (R3CEV). Консорциум начал исследования банковского использования цепочки блоков для международных переводов [11].

46ECVN622
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

С момента своего запуска Биткойн уже пережила первый пузырь инвестирования, но это не повлияло на рост капитализации криптовалюты — на момент доклада она оценивалась в 1 млрд долларов США.

К 2016 году появился целый ряд стартапов, работающих на основе технологий цепочки блоков: Coinbase, Blockstream, 21 Inc, Xapo, различного рода кошельки криптовалют.

14 марта 2016 года Лиза Эллис (Lisa Ellis) и Винсент Спизири (Vincent Spiziri), специалисты инвестиционного фонда Бернстайн (портфель управляемых фондом активов оценивается в 474 миллиарда долларов), представили посетителям SXSW 2016 взгляд крупных инвесторов на нарождающиеся технологии цепочки блоков (blockchain) и самой популярной ее производной — криптовалюты Bitcoin. Эти технологии, считают докладчики, уже сейчас совершают революцию в банковском деле за счет безопасности, эффективности, прозрачности децентрализованных транзакций.

Лиза Эллис начала с собственной истории покупки дома. В США неотъемлемой частью покупки недвижимости является страхование на случай того, что продаваемая недвижимость не принадлежит продавцу [12].

Отсутствие единого реестра транзакций с недвижимостью во многих странах создает дополнительные риски как для продающих, так и для покупающих. Система, основанная на децентрализованной системе единого реестра транзакций с недвижимостью, могла бы решить подобный вопрос не только на национальном, но и на международном уровне.

Можно привести еще один пример. В случае, если необходимо отправить деньги за рубеж, на проведение данной операции требуется около 4–5 дней. Это обусловлено не тем, что банки медленные, а потому, что международная банковская система так устроена. Неэффективность многих процессов прежде всего проблема для самих банков. Биткойн и цепочка блоков могут сильно улучшить ситуацию.

Важно отметить, что многие путают Биткойн и цепочку блоков. Биткойн — это существующая единая интегрированная платежная система. Блокчейн (цепочка блоков) — это технология, описывающая различные варианты технологий распределенного реестра (distributed ledger technologies) [13].

Биткойн представляет собой уже функционирующую систему, безопасность и принцип работы которой доказаны, а вокруг существует целая экосистема разработчиков и кода. В это же время блокчейн — это скорее принцип ведения реестра, который может быть применен для любых других целей.

При этом если в Биткойне сделан упор на безопасность транзакций (из-за платежной специфики), следовательно, Биткойн крайне требователен к вычислительным мощностям участвующих в системе компьютеров, то в блокчейне нет такого упора на безопасность, в связи с чем и требования к ресурсам ниже.

Если Биткойн уже вытеснил конкурентные криптовалюты, то в случае со стандартом технологии цепочки блоков ситуация не столь однозначна — до сих пор происходит острая конкуренция реализации этой технологии.

В теории, квантовые компьютеры достаточной разрядности позволят быстро вычислять дискретные логарифмы, а это означает, что сломаются распространённые сейчас криптосистемы электронной подписи, в том числе, ECDSA. Стоит подчеркнуть, что в настоящее время функционирование криптовалюты основывается именно на ней, поскольку ее функции заключаются в удостоверении транзакции, для чего необходим секретный ключ из пары, связанный с биткоин-адресом.

46ECVN622
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Рассмотрим данный механизм в виде схемы (рис. 2).

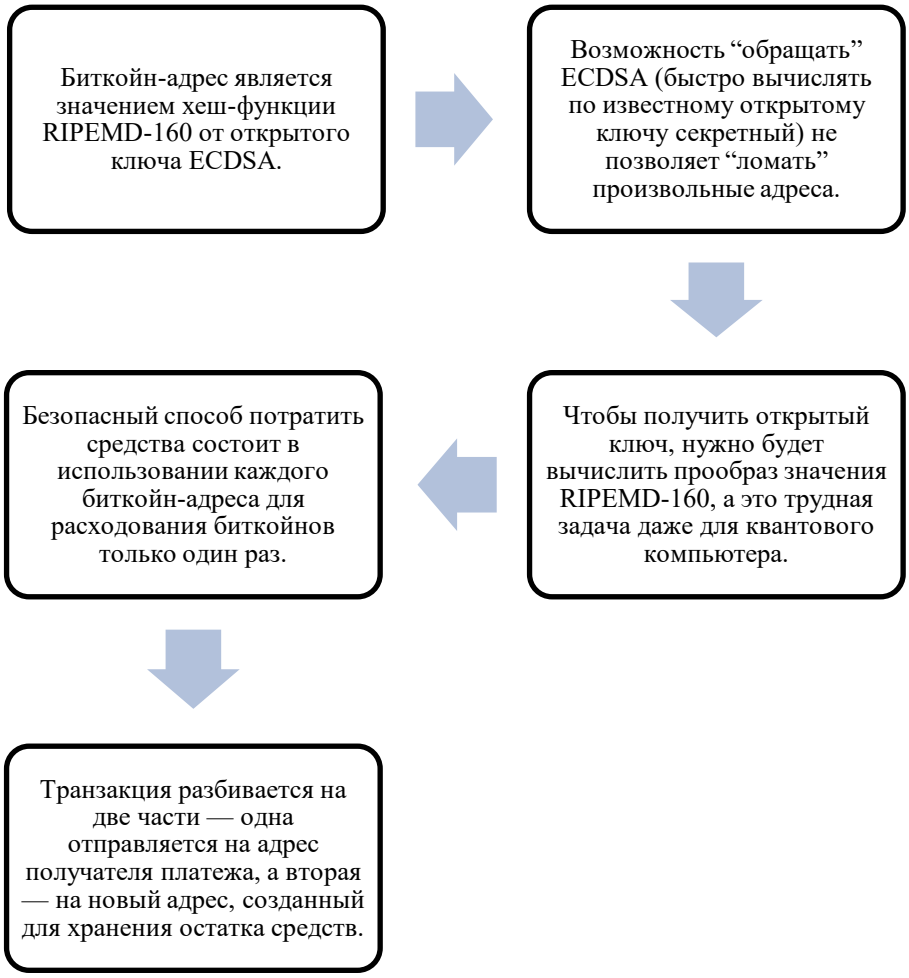

Рисунок 2. *Осуществление расходования биткоинов [13]*

Открытый ключ должен быть указан в явном виде, чтобы осуществить операцию по расходованию денег. Он выступает в качестве индикатора валидности операции. Однако это приводит к тому, что при проведении каждой последующей операции может возникнуть проблема: транзакция может быть в любой момент перехвачена хакером. Квантовый компьютер позволяет ему вычислить секретный ключ и осуществить подменную транзакцию. Чтобы избежать этого, необходимо перехватить новую транзакцию. Рекомендуется делать это быстро и практически сразу, то есть еще до того, как она достигнет глубины в один блок. Осуществить указанные действия вовсе несложно, поскольку передача транзакций осуществляется в открытом виде в P2P-сети.

После получения секретного ключа хакером возможны два варианта развития событий (рис. 3).

Стоит понимать, что получить ключ достаточно непросто. Во многом это обусловлено отсутствием подходящих квантовых компьютеров и долгой работы в онлайн-режиме. Несмотря на это такие случаи иногда происходят, что не только вызывает полное недовольство пользователей, но и приводит к утрате смысла биткоинов. На данный момент специалисты еще не смогли найти решение данной проблемы: подошла бы та или иная квантовостойкая схема электронной подписи на замену ECDSA, однако её выбор и внедрение в протокол представляют собой весьма и весьма непростую задачу [13].

Рисунок 3. *Возможные варианты при получении атакующим секретного ключа*

Важная особенность технологии в том, что она самозапускающаяся и самовоспроизводящаяся. Безопасность транзакций в системе обеспечивается ресурсоемким шифрованием, которое распределяется между подключенными к системе компьютерами. В этом случае человек, выделяющий ресурсы своего компьютера для работы в сети, становится «майнером» (miner дословно — добытчик, шахтер). Майнеры вознаграждаются за использование своих ресурсов получением небольших объемов криптовалюты. Чем больше майнеров, тем больше масштаб системы. Таким образом, система самомасштабируется.

Выводы

Таким образом, можно сформулировать вывод о том, что биткоин в современном мире выступает в качестве наиболее популярной цифровой валюты. Применяется он при осуществлении оплаты или денежных переводов. На сегодняшний день этой валютой пользуются практически во всех странах мира. Привлекает биткоин простотой и удобством своего сервиса: например, создание счета не займет много времени. Азия, Африка, Европа и США уже давно сотрудничают с биткоин, в некоторых городах есть банки, которые принимают и производят вывод биткоин валюты.

Сеть узлов-майнеров обеспечивает поддержание работоспособности биткоина на необходимом уровне, поскольку именно она отвечает за вычисление заголовков блоков. Если посмотреть на статистику по текущему распределению (предполагаемому) мощности сети на сайте blockchain.info, то нетрудно подсчитать, что около 60 % этой мощности контролируют китайские пулы (AntPool, F2Pool и BTCC Pool). (Пулы — это объединения майнеров, действующих согласованно, и делящих полученную от майнинга биткоин-прибыль).

46ECVN622
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Блокчейн — уникальная система хранения данных о выданных кредитах, правах на собственность, бракосочетаниях и т. д. На основе системы цепочки блоков (блокчейн) создаются и другие криптовалюты, а также системы финансовых операций, ведь данная схема очень удобна, за счет распределительного хранения информации.

ЛИТЕРАТУРА

1. Коварда В.В., Лаптев Р.А., Рогов Р.А. Основные направления развития системы прослеживаемости товаров в качестве фактора обеспечения безопасности России в условиях расширения процесса глобализации // Вестник Евразийской науки. — 2020 № 1. — URL: https://esj.today/PDF/15ECVN120.pdf.
2. Булгаков И.Т. Правовые вопросы использования технологии блокчейн // Закон. — 2016. — № 12. — С. 80–89.
3. Баско О.В. Инновационные продукты и технологии российских коммерческих банков в условиях формирования цифровой экономики // Вестник Евразийской науки. — 2019 № 5. — URL: https://esj.today/PDF/66ECVN519.pdf.
4. Грылева И.В. Смарт-контракты и технология блокчейн // Экономика и бизнес: теория и практика. — 2019. — № 4-2. — С. 63–66.
5. Спешилов А.В., Калинин Н.В. Исследование интереса пользователей к технологии блокчейн в россии //современное состояние рынка инвестиций в АПК России. — 2022. — С. 199.
6. Бондарев М.С. Регулирование криптовалютного рынка: проблемы, мировая практика // Вестник Евразийской науки. — 2020 № 2. — URL: https://esj.today/PDF/11ECVN220.pdf.
7. Чернышева М.А., Гребеник В.В. Криптовалюта, как платежный инструмент денежно-кредитной сферы // Вестник Евразийской науки. — 2022 № 3. — URL: https://esj.today/PDF/45ECVN322.pdf.
8. Кочетков А.В. Становление и развитие рынка цифровых финансовых активов в 2009–2019 гг. // Вестник Евразийской науки. — 2019 № 4. — URL: https://esj.today/PDF/28ECVN419.pdf.
9. Пряников М.М., Чугунов А.В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International journal of open information technologies. — 2017. — Т. 5. — № 6. — С. 49–55.
10. Руденко Е.А. Понятие системы блокчейн // Проблемы современных интеграционных процессов и пути их решения. — 2016. — С. 163–164.
11. Арефьева А.С., Гогохия Г.Г. Перспективы внедрения технологии блокчейн // Молодой ученый. — 2017. — № 15. — С. 326–330.
12. Соколова Т.Н., Волошин И.П., Петрунин И.А. Преимущества и недостатки технологии блокчейн // Экономическая безопасность и качество. — 2019. — № 1(34). — С. 49–52.
13. Федотова В.В., Емельянов Б.Г., Типнер Л.М. Понятие блокчейн и возможности его использования // European science. — 2018. — № 1(33). — С. 40–48.

Samusevich Vladimir Evgenievich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: vladimirsamusevich06@gmail.com

Analysis of the development of the bitcoin and blockchain system

Abstract. In this article, the author considers the development of bitcoin and blockchain cryptocurrencies. The author emphasizes that electronic payment systems and virtual currencies are a fairly new phenomenon that is rapidly capturing all countries. Bitcoin is the most popular cryptocurrency created in 2009. It is important to note that at first this currency was in very little demand among programmers and interested users. Also, this currency was common among arms and drug dealers and crypto anarchists, which negatively affected the development of bitcoin. Many countries saw it as a threat to the monopoly of national currencies and banned it. The article presents the main features of the bitcoin system. The author focuses on the fact that the first attempts to create electronic money were made back in 1998, but they were unsuccessful and were subsequently discontinued. The creator of the Bitcoin system is Satoshi Nakamoto (an organization under a pseudonym or a person). The active growth of the bitcoin exchange rate began in 2011 after the exchange service appeared — Bitcoin Market. Then, in 2012, the MtGox exchange was created, which made the exchange and withdrawal of virtual money into reality. The author also highlights 2013, which was both a period of collapse and explosive growth of the cryptocurrency. The relatively stable and measured development of bitcoin began in 2016. The author emphasizes that many people confuse bitcoin and the block chain. In this regard, the article provides a definition of these concepts, as well as their comparison. In the final part of the article, the author, as a result of the study, comes to the conclusion that the Bitcoin system is self-starting, self-reproducing and self-scaling.

Keywords: bitcoin; blockchain; virtual currencies; virtual cards; money; cryptocurrency; international bank transfers; international economic relations; national currencies; money functions; economy; electronic money