УДК 004

В.В. Верусь [1], Р.Ю. Шлаустас [1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ТЕХНОЛОГИЯ BLOCKCHAIN — УЯЗВИМОСТИ, КРИПТОСТОЙКОСТЬ, ПРЕИМУЩЕСТВА, НЕДОСТАТКИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ.

Аннотация: *Рассмотрен принцип работы технологии blockchain, определены и выделены уязвимости, оказывающее сдерживающее воздействие повсеместного распространения данной технологии, оценена криптостойкость, обозначены преимущества, недостатки, а также отмечены возможные перспективы развития.*

Ключевые слова: *биткойн, блокчейн, криптовалюта, хэширования, доказательство работы, майнинг*

V.V.Verus [1], R.Yu.Shlaustas [1]

[1] Irkutsk State Transport University, Irkutsk, Russia

TECHNOLOGY BLOCKCHAIN — VULNERABILITY, STRONG ENCRYPTION, ADVANTAGES, DISADVANTAGES AND DEVELOPMENT PROSPECTS.

Abstract. *Given to the principle of the blockchain technology, identified and highlighted the vulnerability of having a deterrent effect widespread use of this technology, valued strong, identified strengths, weaknesses as well as marked possible future developments.*

Keywords: *bitcoin blockchain, cryptocurrenc, hashing, proof of work, mining*

Технология, которая, по-видимому, окажет огромное влияние на мир в следующие десятилетия, уже существует. И это не социальные сети, как многие думают до сих пор, полагая, что скорость распространения информации может что-то изменить. Это не "big data", не робототехника и даже не искусственный интеллект. Это технология, лежащая в основе криптовалют. Открытие этой технологии сопоставляется по своей значимости с открытием глобальной сети интернет и несет в себе огромное количество решений для общественных, экономических и государственных взаимодействий.

В последние десятилетия мы имели дело с интернетом информации. Передача в нем происходила путем передачи копий оригинала. Тем самым происходил процесс демократизации информации. Когда же дело состоит в передачи ценностей, таких как финансовые активы, деньги, интеллектуальной собственности, музыки, произведений искусства и др. передача посредством передачи копии - плохая идея.

В связи с желанием передавать ценности наше общество обращается к крупным посредникам, таким как: банк, государство, ведущие операторы соцсетей и эмитентов кредитных карт и т.д. Эти посредники занимаются созданием построением и обслуживанием всей рыночной деятельности от определения подлинности до установления личности людей, удаления, создания документов и делопроизводства. В целом данная система довольно успешно справляется со своей ролью. Но нынешняя система обладает рядом проблем. Централизация. Систему посредника можно взломать и это происходит все чаще. Они тормозят весь процесс. Перевод денежных средств может занимать от нескольких дней до нескольких недель. Неприятная комиссия за услуги: от 10-20% за выполнение своих обязательств. Они хранят

наши персональные данные и иногда посредством ошибок посредников наносится ущерб нашему личному пространству.

Что, если бы существовал не только интернет информации, но и интернет ценностей — вроде масштабного, глобального распределенного реестра, работающего с миллионом компьютеров и доступного каждому? Любые ценности от, денег до музыки, могли бы храниться, перемещаться, обмениваться и управляться без могущественных посредников?

В 2008-2009 году в год сильнейшего кризиса Сатоши Накомото [1] создал документ, являющийся протоколом цифровой валюты с использованием базовой криптовалюты — Биткойн. Эта криптовалюта позволила обеспечить надежность и оперировать без посредников; не подконтрольна государству; в данный момент очень волатильный и рисковый актив. Но главное достоинство здесь — это базовая технология Blockchain — построение связанных воедино цепочек хэшей. Впервые во всем мире и впервые за все время существования человечества люди повсеместно могут доверять друг другу и сотрудничать на равных. Доверие не базируется на авторитете могущественных посредников, а на сотрудничестве, криптографии и программном коде [2-8].

Blockchain представляет собой распределенную учетную книгу записей о событиях в цифровом мире. Ключевой составляющей Blockchain является журнал транзакций, а сами транзакции — это единственный способ изменить состояние реестра.

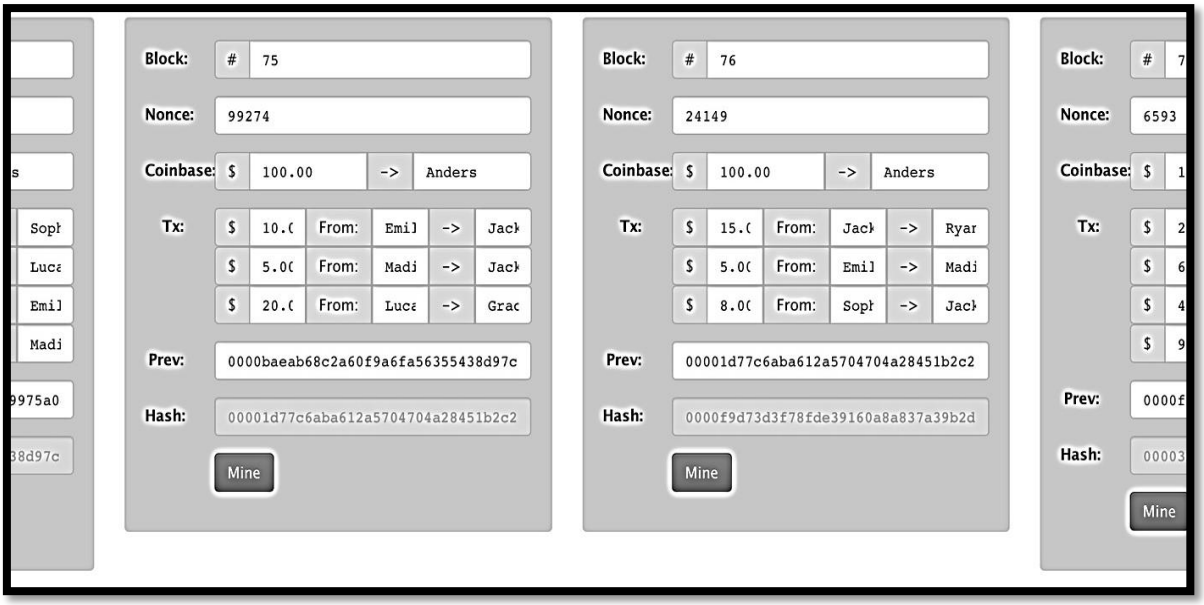


Рис. 1. Упрощенный пример формирования цепочки и содержания блока

На рис. 1 представлено вычисление hash с четырьмя нулями, что соответствовало действительности при появлении технологии и даже обычный персональный компьютер или ноутбук справлялся с вычислением. Однако, с возрастанием вычислительной мощности происходило изменение количества нулей и появление других критериев. На данный момент происходит вычисление хэша с 49 битами нулей вначале и значение следующих 23 бит должно быть меньше 6A93B3 (25.04.18). В последующем, при возрастании мощности сети количество нулей, а начале хеша будет возрастать при примерном сохранении времени построения хеша.

При этом записи в журнал транзакций могут вноситься только с согласия большинства участников сети. Важной особенностью журнала транзакций в blockchain является его неиз-

менность. Хотя blockchain и является распределенной системой, а формировать транзакции может каждый узел, это не означает, что все участники блокчейн-сети равноправны — почти в любой реализации этой технологии введено распределение ролей на валидаторов (участников, пишущих транзакции в журнал), аудиторов и легких клиентов. С глобальной точки зрения, блокчейн представляет собой сеть для обработки транзакций с набором правил («протокол»), следуя которым участники могут прийти к общему видению журнала транзакций и установить состояние сети в определенный момент времени. При этом блокчейн децентрализован: даже если существенная часть узлов выпадет из работы на продолжительное время или будет взломана, система все равно продолжит работать. Стойкость реестра обеспечивается различными криптоалгоритмами, такими как: SHA-256 (вычисление hash значений), ECDSA, Dagger-Hashimoto, Crypto-Night, blake2b, Scrypt, x11 и множество других.

Создание блоков и добавление их в цепочку называется процесс майнинг(mining). Не стоит полагать, что данный процесс прост из-за всеобщего помешательства. Чтобы создать блок нужно проделать огромное количество вычислений для единственно верного варианта хэша. Однако, суть обширной популярности майнинга заключается в награждении майнера за нахождение правильного (соответствующего всем параметрам, описанным в алгоритме) хэша. После того, как правильный хэш найден, записывается в блок и уже новый блок распространяется по всем остальным участникам сети blockchain (рис.2).

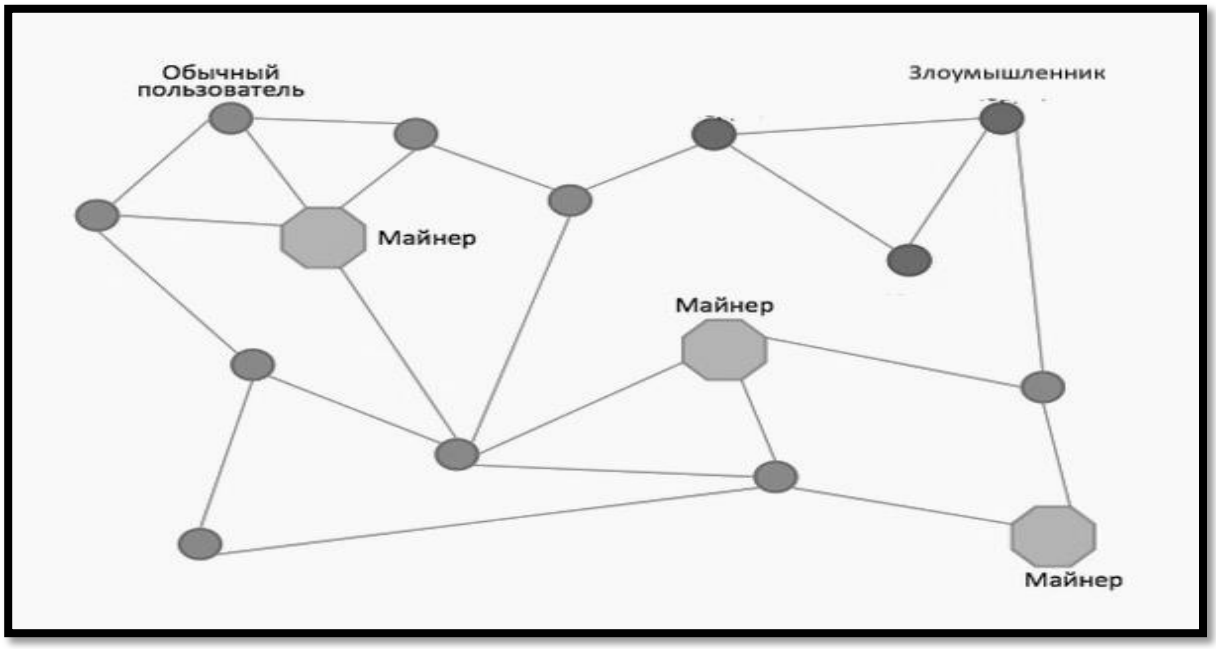


Рис. 2. Схема децентрализованного распределения блоков

На данный момент награждение составляет около 12,5 BTC (около 6,4 млн рублей на 21.04.2018). Чтобы найти правильных хэш нужно обладать огромной вычислительной мощностью (см. рис. 3). Первые майнеры скупали видеокарты, так как они на то время обладали колоссальной вычислительной мощностью, превосходящей мощности процессора (в плане вычисления хэш значений). В последнее время на рынке майнинга довольно плотно обосновались узко специализированные устройства для майнинга называемые, обгоняющие на несколько порядков вычислительные мощности видеокарт. В связи с этим многие основатели криптовалют должны были провести так называемые fork'и (форки) – ответвление от основной криптовалюты, с изменением правил работы. Существует два вида forka – версия soft и

hard. Softfork менее радикальный и заключается в уточнении правил. Hardfork более радикальный и несет в себе большее количество, а так же и радикальные изменения. Применение hardfork является вынуждено-болезненным и при определенных изменениях помогает изменить сложность сети с переходом на другой криптоалгоритм для борьбы с ASIC-устройствами, который в значительной степени может, как и уменьшить так и увеличить сложность вычисления блоков (Monero – переход на CryptoNight).

Взлом цепочки связанных хэшей в настоящее время невозможен. Так, при длине хэша в 256 битов нужно перебрать

$$2^{256} \approx 10^{77}$$

вариантов на один хэш в цепочке, а таковых может оказаться несколько сотен тысяч.

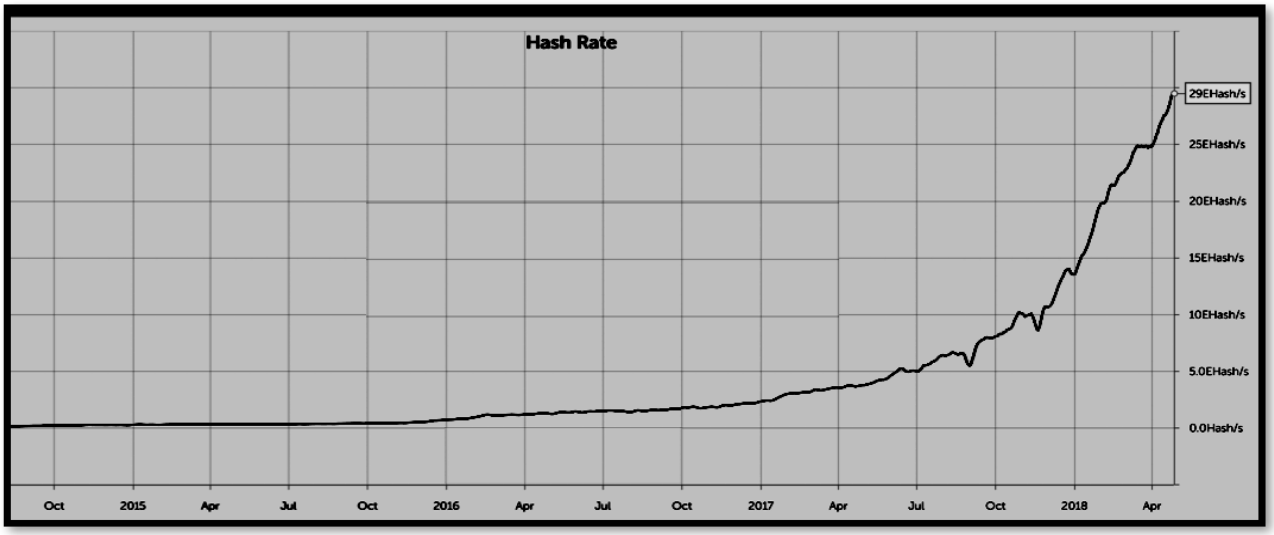


Рис. 3. Кривая роста вычислительной мощности (hashrate) bitcoin сети. (EHash/s – 10^{18} хэшей в секунду)

Вычислительных мощностей всего мира явно недостаточно, чтобы решить подобную задачу.

Уязвимости и криптостойкость blockchain'a в последнее время активно обсуждаются, так как многие из стран начинают разрабатывать свои приватные blockchain'ы. На данный момент специалисты в области компьютерной и кибербезопасности выделяют следующие векторы атак:

— Алгоритмы для вычисления хэш-функции стандартов SHA-256 и ECDSA (алгоритм цифровой подписи с эллиптическими кривыми) считаются весьма стойкими при существующих вычислительных мощностях. Однако, появление высокопроизводительных квантовых компьютеров увеличит риск взлома этих криптографических функций, что, по мнению экспертов, в следующие 10 лет маловероятно;

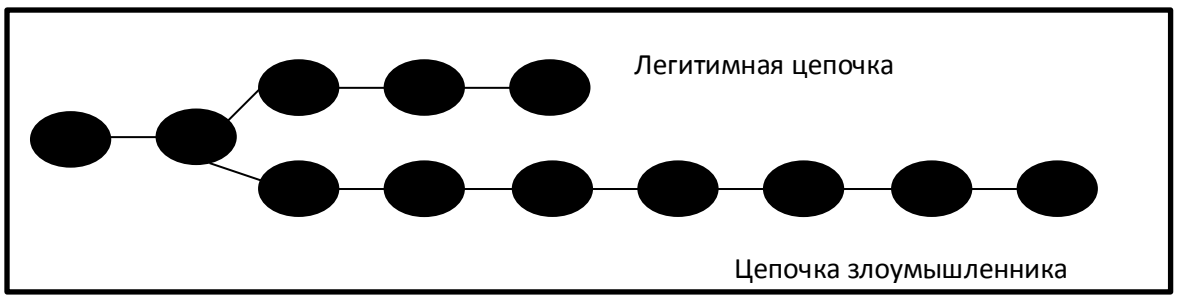


Рис. 4. Иллюстрация реализации атаки 51%. Легитимная цепочка в результате становится не основной - дописывание новых блоков производится в цепочку злоумышленника, в которой происходят как отмена предыдущих транзакций, так и появление новых не достоверных транзакций

— Появление коллизий — количество вычисляемых hash-значений огромно, однако существует вероятность того, что в определенный момент вычисленный hash будет подходить по всем условиям к ранее вычисленному абсолютно другому hash-значению или к еще не вычисленному верному, что приведет к потенциальной возможности создании блока с неверными данными;

— Атака 51% (Рис.4). Суть атаки в том, что злоумышленник, контролируя более пятидесяти процентов подтверждающих ресурсов блокчейн-сети, может напечатать свою цепочку блоков, или же дополнить существующие ответвление, которая обгонит основную цепочку блокчейна и в результате станет основной. При этом он легко и беспрепятственно отменит часть транзакций, сделанных в отброшенных им блоках. Например, транзакции о денежных переводах. Таким образом, теоретически можно отменить транзакцию задним числом. Если более детально анализировать данный вектор атаки, то для того, чтобы это сделать, злоумышленнику следует обладать вычислительной мощностью, превосходящей 15 миллиардов GH/s(15*10^18 hash в секунду), что на данный момент технически невозможно(для сравнения NVIDIA GTX 1080 TI–35*10^6 H/s , узкоспециализированное направление для майнинга ASIC Antminer S9 13,5*10^12 H/s) стоимость данного оборудования крайне велика и даже покупка и майнинг с помощью данных устройств в числе перекрывающей своей вычислительной мощностью хотя бы 15 EH/s не дает гарантии замены предыдущих блоков и запись измененных блоков;

— DDoS —отправка большого количества "мусорных" данных на узел, обрабатывающий транзакции, может усложнить его работу;

— Атака Сибиллы. Хакер может попытаться наполнить сеть подконтрольными ему узлами, и остальные пользователи смогут подключиться только к блокам, созданным для мошенничества. К примеру, Атакующий блокирует транзакции от других пользователей, отсоединив вас от общей сети. После этого атакующий подсоединяет вас только к блокам, которые создает он, в отдельной сети. В результате этого будут появляться транзакции, которые будут пересылать деньги повторно (double-spending);

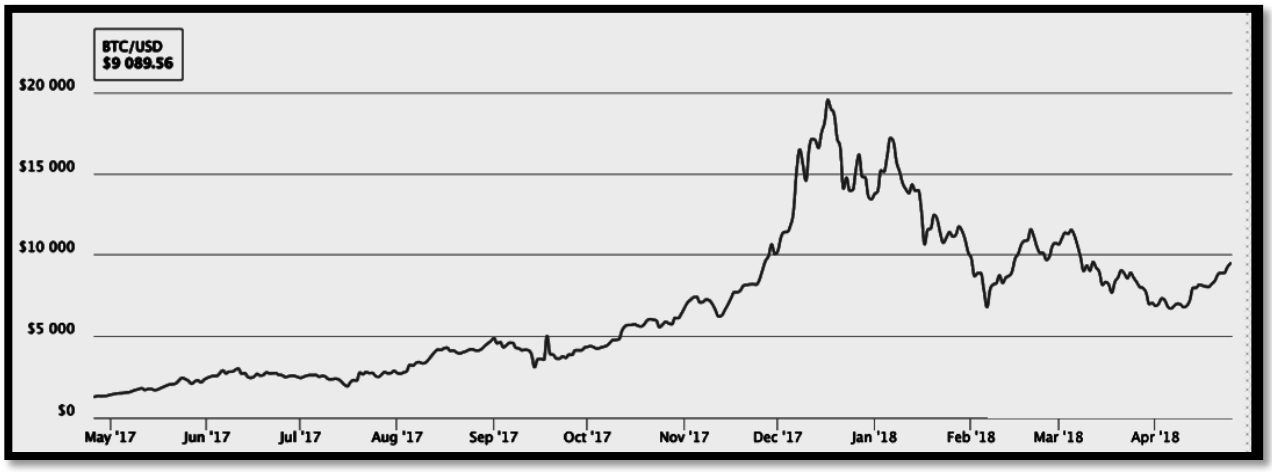
— Ошибки кода — баги могут привести к нестабильности в защите системы. Например, в узле информация должна обновляться за короткий отрезок времени. Если из-за бага это не произошло, в цепочке не появилась нужная информация, неправильные данные начали распространяться по сети и т.д. Все это может стать причиной остановки работы сети на несколько часов.

Глядя на данные векторы атак и уязвимости, можно сказать лишь одно: на данном этапе развития компьютерных технологий и тех вычислительных мощностей, что есть у нас в распоряжении, маловероятно, что в видимом будущем существует реальная угроза, способная внести хоть каплю недоверия к данной технологии, и тем более к информации и ценностям, распространяемым по данной технологии.

Неоспоримыми достоинствами данной технологии являются децентрализация, способствующая колоссальной надежности и правдивости системы; прозрачность и анонимность; основания для доверия каждого к каждому; мобильность и масштабируемость технологии

под различные цели и задачи – и это только малая часть того, за что многие уже сейчас стараются перейти на данную технологию в своем деле. Однако у вас может сложиться ложное представление о том, что эта технология без изъянов. Основными недостатками данной технологии эксперты выделяют: для того, чтобы в системе существовали доверительные отношения и различные транзакции не подвергались сомнению, система должна состоять из огромного числа пользователей; существует проблема аутентификации; огромный вес реестра и огромное количество времени уделяется проверке достоверности, что усложняет работу как майнеров, так и увеличивает время отправки ценностей от одного пользователя к другому; неопределенный нормативный статус. Кроме этого, следует отметить значительную волатильность курсов валют — рис 5-6.

Все эти недостатки негативно сказываются на распространении революционной технологии. Если же мы посмотрим на позицию государств в вопросе о внедрении в целом как криптовалют, так и blockchain технологии, то столкнемся с той ситуацией, при которой достоинства сразу становятся недостатками, а именно: если же происходит оплата каких-либо услуг, то государство должно иметь с этого налог, а так как система анонимна, то и обязать не получится; с помощью криптовалют и технологии Blockchain возможно осуществлять финансирование террористических групп на территории разных стран; возможность отмывания денег и т.д. Решением данных проблем является создание как нормативно-правовой базы в государстве, так и создание своей внутригосударственной криптовалюты и своего реестра



Blockchain.

Рис. 5. График курса 1 bitcoin к Американскому доллару (25.04.18г.). В пике (декабрь 2017 г.) стоимость в некоторые промежутки времени превышала 20000$

Рис. 6. График курса 1 bitcoin к Рублю (25.04.18г.).

Так же стоит отметить в целом положительное воздействие криптоиндустрии на общество. В свете разработки и реализации разнообразных проектов на базе криптовалют и блокчейн технологии все больше и больше людей начинает осознавать, что технологии уже перестают быть средством, способным только помочь в работе или в другом узко специализированном деле, а вступают в новый виток развития, становясь той самой движимой силой, которая может изменить всю систему целиком. Именно те самые люди, кто сейчас загорелся и вдохновился этой идеей, кто сейчас начинает осваивать технологии использования или создания своего собственного продукта на основе элементов блокчейн и криптовалют, кто погружается в технические подробности и пытается собственными руками создать свою «цепочку», они и будут менять наше будущее и привносить в настоящее преимущества технологий. Уже сейчас многие фирмы перешли или готовы к тому, чтобы перейти на технологию блокчейн. Многие трейдеры и брокеры сколотили себе состояние на стоимости криптовалют. Только представьте, какие бы у вас могли бы сейчас быть миллионы, если бы в далеком 2010 году вы бы вложили все свои деньги в bitcoin.

Перспективы развития технологии безграничны: начиная, от перевода денег до передачи музыки, от согласования крупных государственных проектов до инноваций в регулировании земельных участков, от прозрачного наблюдения за тратой государственных средств до регулирования поступления заработной платы чиновников и депутатов. Применение данной технологии многогранны и труднее будет сказать, где человечество не найдет применение данной технологии.

БИБЛИОГРАФИЧЕСКИЕ СПИСОК

1. [Электронный ресурс] Документ Сатоши Накамото. URL: https://bitcoin.org/bitcoin.pdf (дата обращения 25.04.2018)

2. Тапскотт А., Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня. М.: Эксмо, 2017. 560 с.

3. МихеевФ.,Генкин А. Блокчейн: как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. 650 с.

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

5. [Электронный ресурс] Все о bitcoin и blockchain. URL: https://ru.bitcoinwiki.org/wiki/Заглавная_страница– (дата обращения 25.04.2018)

6. [Электронный ресурс] SecurityLab о blockchain. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/343072.php– (дата обращения 25.04.2018)

7. [Электронный ресурс] Иллюстрация работы blockchain. URL: https://anders.com/blockchain/coinbase.html (дата обращения 25.04.2018)

8. [Электронный ресурс] Перечень важных электронных ссылок о blockchain с кратким описанием. URL: https://habrahabr.ru/company/bitfury/blog/332438/– (дата обращения 25.04.2018)

REFERENCES

1. [Electronic resource] Document Satoshi Nakamoto. URL : https://bitcoin.org/bitcoin.pdf to (date of circulation 25.04.2018).

2. Tapscott, d. Tapscott blokchein Technology: what moves the financial Revolution today: Eksmo, 2017. 560 pages.

3. MiheevF., Genkin a. Blokchein: how it works and what awaits us tomorrow: Alpina Publisher, 2018. 650.

4. Raval with. decentralized application. Technology Blockchain. Spb.: Piter, 2017.240 c.

5. [Electronic resource] is all about bitcoin and blockchain. URL : https://ru.bitcoinwiki.org/wiki/Заглавная_страница to (date of circulation 25.04.2018).

6. [Electronic resource] SecurityLab about blockchain . URL : https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/343072.php to (date of circulation 25.04.2018).

7. [Electronic resource] illustration work blockchain . URL : https://anders.com/blockchain/coinbase.html (date of circulation 25.04.2018).

8. [Electronic resource] electronic list of important links about blockchain with a brief description. URL : https://habrahabr.ru/company/bitfury/blog/332438/ to (date of circulation 25.04.2018).

Информация об авторах

Владислав Вячеславович Верусь— бакалавр., кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: jukovtv@icloud.com

Ромас Юргевич Шлаустас— к. ф.-м. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: shlaustas@gmail.com

Authors

Vladislav Vyacheslavovich Verus— Bachelor, “Information Systems and Information Protection”, Irkutsk State Transport University, Irkutsk, e-mail: jukovtv@icloud.com

Romas Yurgevitch Shlaustas — Ph.D., in phisics and mathematics, Assistant Professor of “Information Systems and Information Protection”, Irkutsk State Transport University, Irkutsk, e-mail: shlaustas@gmail.com

Для цитирования

Шлаустас Р.Ю. Технология blockchain — уязвимости, криптостойкость, преимущества, недостатки и перспективы развития / Шлаустас Р.Ю., Верусь В.В. // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2018. – №1. – С. 64-71 – Режим доступа: http://ismm-irgups.ru/toma/11-2018, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.10.2018)

For citation

Shlaustas R. Yu., Verus V.V. Tekhnologiya blockchain — uyazvimosti, kriptostojkost', preimushchestva, nedostatki i perspektivy razvitiya [Blockchain technology — vulnerabilities, cryptofirmness, advantages, shortcomings and the prospects of development] // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the man-agement of complex systems: electronic scientific journal], 2018. No. 1. P. 64-71. [Accessed 01/10/18]