АНАЛИЗ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ ТЕХНОЛОГИИ «БЛОКЧЕЙН» И ЦИФРОВЫХ ВАЛЮТ.

Астраханцев Р.Г[1]., Лось А.Б[2]., Мухамадиева Р.Ш[3].

ANALYSIS OF MODERN TENDENCIES OF DEVELOPMENT OF THE TECHNOLOGY "BLOCKCHAIN" AND DIGITAL CURRENCIES.

Astrakhantsev R.G.[4], Los A.B[5]., Muhamadieva R.Sh[6].

Цель статьи: *исследование направлений развития структуры и работы блокчейн сетей, выявление алгоритмов взаимодействия внутри сети, ускоряющих процесс формирования новых блоков без потери безопасности и устойчивых к масштабированию числа пользователей, изучение тенденций развития криптовалют, прогнозирование их дальнейшего развития, а также исследование мировой практики правового статуса криптоволют.*

The purpose of the article*: to study the direction of development of the structure and operation of blockchain networks, identify interaction algorithms within the network, accelerating the process of forming new blocks without losing security and resistant to scaling the number of users, studying the development trends of cryptocurrencies, predicting their future development, and also as well as a study of the world practice of legal status of cryptocurrency.*

Метод: *анализ литературы и открытых ресурсов по тематике вопроса, определение проблем методов передачи и хранения информации в блокчейн сетях, их моделирование и построение решения, выявление релевантных сетей по быстродействию, изучение законодательства в части мировой практики статуса криптоволют, выявление основных проблем цифровых валют с точки зрения государственных институтов.*

Method: *analysis of literature and open resources on the subject matter, identification of problems of methods for transferring and storing information in blockchain networks, their modeling and creating solutions, identifying relevant networks for speed, studying legislation on the world practice of cryptocurrency status, identifying the main problems of digital currencies from the point view of state institutions.*

Полученный результат: *исследованы направления развития технологии блокчейн, проблемы внедрения современных криптовалют и возможные пути их решения. Проанализированы новые алгоритмы и протоколы, ускоряющие блокчейн и увеличивающие его пропускную способность. Предложен новый вариант алгоритма, предотвращающий двойную трату в нескольких параллельных блоках, имеющих протокол взаимодействия между собой, а также алгоритм, позволяющий согласовывать создание новых блоков без проведения голосования или частичной централизации блокчейна. Проведен анализ текущего правового статуса криптовалюты и высказаны предположения о возможных вариантах развития.*

The result*: the directions of development of the blockchain technology, the problems of introducing modern cryptocurrencies, and possible ways to solve them are investigated. New algorithms and protocols that accelerate the blockchain and increase its throughput are analyzed. A new variant of the algorithm is proposed, which prevents double waste in several parallel blocks that have an interaction protocol with each other, as well as an algorithm that allows to coordinate*

[1] Астраханцев Роман Геннадьевич – ассистент кафедры Компьютерной безопасности МИЭМ НИУ ВШЭ
[2] Лось Алексей Борисович – доцент кафедры Компьютерной безопасности МИЭМ НИУ ВШЭ
[3] Мухамадиева Регина Шамилевна - ассистент кафедры Компьютерной безопасности МИЭМ НИУ ВШЭ
[4] Astrakhantsev Roman Gennadievich - Assistant of the Department of Computer Security, MIEM HSE
[5] Los Alexey Borisovich - Associate Professor, Department of Computer Security, MIEM HSE
[6] Mukhamadieva Regina Shamilevna - Assistant of the department of Computer Security, MIEM HSE

the creation of new blocks without voting or partial centralization of the blockchain. The analysis of the current legal status of cryptocurrency has been carried out and suggestions have been made about possible options for development.

Ключевые слова: модели безопасности, моделирование, технология блокчейн, политика безопасности, цифровые валюты.

Key words: security model, modeling, blockchain technology, security policy, digital currencies.

1. Введение

Интерес в мире к технологии «блокчейн» появился с появлением в 2008 году первой криптовалюты Биткоин [1], показавшей возможность осуществлять операции в условиях полного недоверия к любому участнику сети. Второй революционной идей в блокчейн сетях являлись смарт-контракты, появившиеся вместе с криптовалютой Эфириум в 2015 году [2], идей которых являлась возможность алгоритмизации договорной системы и автоматизации создания третьей стороны в виде программного кода.

В данной статье исследуются основные проблемы применения криптовалют и возможные пути их решения. Предложена идея согласования транзакций в распределённой сети и представлена доказательная база возможности безагентруной реализации шардинга – одной из стратегии масштабирования криптовалют. Изучен мировой опыт в части определения правового статуса криптовалют и подробно рассмотрен вариант цифровой валюты под названием стеблкоин, который рассматривается в нашей стране как предполагаемое законное платежное средство [3].

2. Постановка задачи

Любой распределённый реестр, основанный на технологии «блокчейн» состоит из базы данных вместе с записями всех её изменений, упорядоченных в связный список, и алгоритмом согласования новых записей. Обычно алгоритм представляет из себя решение криптографического уравнения, которое решается только перебором. Представителями таких алгоритмов являются Proof-of-Work и Proof-of-Stake.

Однако процедура обеспечения безопасности этих протоколов требует, как правило, значительных временных затрат на создание новой записи в распределённой базе данных. Так, например в Биткоине создание нового блока осуществляется с помощью Proof-of-Work, а время проведения транзакции пользователя может составлять до 60 минут или больше [4]. Таким образом, первая рассматриваемая проблема это *увеличение скорости создания изменений в блокчейн сети.*

Другим аспектом в технологии «Блокчейн» является процесс взаимодействия пользователя и сети. Следует заметить, что даже если удастся увеличить скорость формирования блоков, то все равно остаются пользователи, не успевающие получать информацию об изменениях блокчейна. Вторая проблема, рассматриваемая в статье это проблема *масштабирования блокчейна*.

Кроме того, в современных схемах поиск блоков является соревнованием между некоторыми участниками сети. Это ведёт к значительным потерям вычислительных мощностей и в целом к затратам на электроэнергию. Таким образом, появляется еще одна проблема – *согласование процесса формирования блоков децентрализованным протоколом.*

Важной проблемой, также рассмотренной в статье, является *юридическая сторона вопроса*. Криптовалюты предоставляют своим пользователям псевдонимность или полную анонимность как, например, Zerocoin [5]. Это дает большой простор для теневого рынка и не может не представлять угрозы для отдельных граждан и всего государства в целом.

Помимо этого, многие экономические аналитики, обеспокоены возможностью организации на основе криптовалют новых финансовых пирамид [6,7].

Далее будет рассмотрена разновидность криптовалют, называемая стейблкоином, имеющая материальное обеспечение и, соответственно, новые проблемы.

3. Технологические улучшения блокчейна и криптовалют

Увеличение скорости транзакций опирается непосредственно на алгоритм формирования новых блоков. Стоит напомнить, что алгоритм Proof-of-Work заключается в получении хеша от нового блока в определённом числовом диапазоне. В схеме Биткоина строковое представление хеша должно начинаться с семи нулей, что гарантирует формирование нового блока в среднем раз в 10 минут.

Алгоритм Proof-of-Stake, используемый в основном в криптовалютах, модифицирует эту идею создания блока и требует, чтобы итоговый хеш от блока был меньше либо равен, чем некая константа, умноженная на произведение числа монет и времени их хранения у нашедшего новый блок. Майнер – пользователь, занимающийся поиском новых блоков – в данном случае должен указать свои монеты в дополнительной информации блока. Для предотвращения полного контроля над сетью, расширяющееся окно множества значений хеша ограничивают сверху некоторым числом. Примером, криптовалюты, использующей Proof-of-Stake является Ripple, скорость проведения транзакции в которой в среднем составляет 4 секунды [8].

Ещё большим потенциалом обладает алгоритм Delegated Proof-of-Stake, в котором периодически происходит голосование за выбор майнеров. Количество голосов у пользователя – это количество его монет. Майнеры поочерёдно ищут новые блоки и меняются друг с другом случайным образом, чтобы в среднем у каждого из них было одинаковое количество блоков. Если одного майнера заметили в мошенничестве и совершении двойной траты, то другие имеют право отклонить созданные блоки и отменить транзакции. Криптовалюта EOS – типичный пример блокчейна, использующего Delegated Proof-of-Stake. Создание блока в этом алгоритме занимает в среднем 0.5-1.5 секунды [8,9], а число транзакций достигает 1200 в секунду [10], что довольно близко к 1700 транзакциям в секунду у платежной системы Visa [11,12].

Такое решение не только решает проблему согласования транзакций, но и делает ненужным соревнование в вычислительных мощностях, что приводит к ускорению транзакций. Правда, появляется необходимость в соревновании за повышение репутации. Кроме того, сосредоточение большого числа монет у узкого круга лиц может привезти к полному контролю за процессом голосования, а значит и за всей работой сети, то есть, к централизации.

С решением проблемы масштабируемости может помочь шардинг – сегментация распределённой базы данных на небольшие кусочки. По своей сути, введение шардинга в блокчейн сети является распараллеливанием одного блокчейна на шарды – множество небольших блокчейнов, в которых пользователи совершают транзакции в удобной им скорости. Именно эту технологию планирует ввести Эфириум в 2020 году, как часть нового блокчейна Эфириум 2.0 [13].

Поскольку параллельно будет реализовываться несколько шардов, то необходим процесс их взаимодействия друг с другом. Аналогично тому, как в современном мире можно переводить деньги между банками разных стран, между разными блокчейнами можно совершать транзакции. Алгоритм заключается в последовательном добавлении транзакции сначала в один блокчейн, а затем в другой [14].

Однако проблема появляется в ситуации, когда один шард полностью захвачен злоумышленниками. Поскольку внутри своего блокчейна злоумышленники никак не получают деньги, то им нужно взаимодействие с остальными пользователями. Внутри своего шарда злоумышленники могут создавать развилки в блокчейне, так как они хотят

навязать свои правила консенсуса. В данном случае, проблема заключается в том, что вышеописанный протокол взаимодействия двух шард не может проверить наличие или отсутствие развилки. В то же время, с помощью указанного разветвления злоумышленники могут совершить двойную трату, используя протокол взаимодействия с разными шарадами (рис.1). Всё, что им нужно сделать – это из каждого ответвления сделать по транзакции между двумя разными блокчейнами.

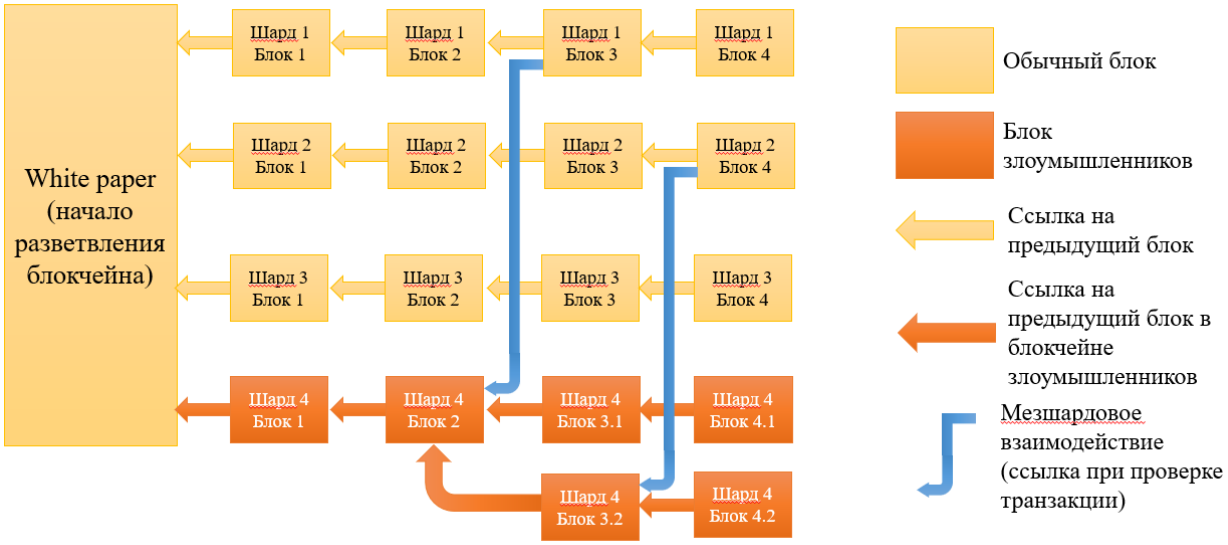

Рис. 1. Пример двойной траты, совершаемой злоумышленниками. Проверка осуществляется проверкой предыдущих блоков, то есть движением по направлению стрелок.

Таким образом, обычного алгоритма взаимодействия между двумя шардами недостаточно. Однако, если между блокченами, с которыми взаимодействовали злоумышленники, произойдёт транзакция, то у одного и того же адреса (адреса, с которого была проведена двойная трата), будет существовать два разных маршрута, имеющих общую часть. Предложением авторов является создание валидирующей транзакции, которая не будет участвовать в передаче денежных средств, и которая будет посылаться на все шарды для создания именного такой ситуации (рис. 2).

Такая схема позволит проверять наличие оговорённых выше маршрутов и возникновение двойных трат. Данный алгоритм не является оптимальным, а лишь говорит о возможности решения проблемы двойного расходования средств.

Стоит заметить, что вопрос согласования процесса формирования новых блоков также относится к проблемам внедрения технологии шардинга. Как уже было отмечено выше, алгоритм Delegated Proof-of-Stake позволяет её решить, хотя в его реализации имеется опасность в централизации сети.

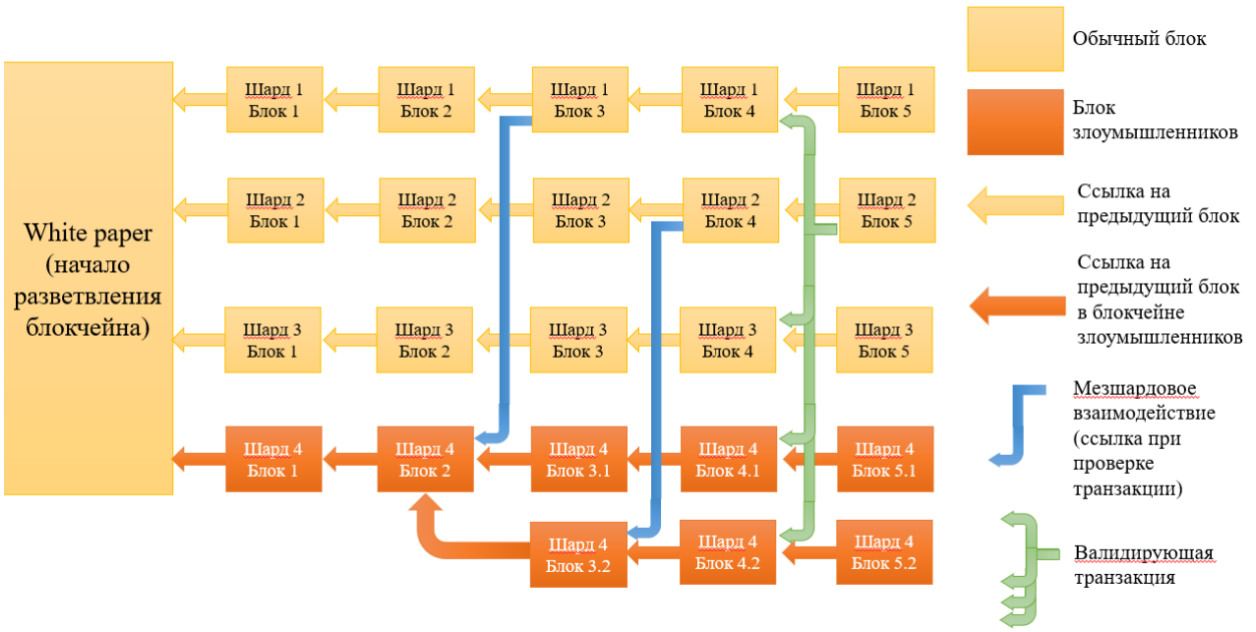

Рис. 2. Пример валидационной транзакции, которая создаёт связь между всеми шардами и позволяет найти блокчейн злоумышленников.

Ещё одним интересным предложением является алгоритм согласования транзакций внутри децентрализованной сети. Его идея состоит в том, чтобы возможность поиска нового блока была у лишь у тех адресов, чей хеш находится недалеко от хеша блока, отстоящего на несколько единиц от текущего. Понятие «недалеко» означает, что эти хеши отстоят на какую-то константу, определённую в правилах блокчейна. Однако, чтобы блокчейн не остановился после нахождения какого-нибудь нового блока, который находится далеко от всех участников, можно сделать так, чтобы допустимое окно расширялось со временем.

Для понимания этой идеи рассмотрим небольшой пример. Пусть каждое расстояние между связанными в данной схеме блоками будет пять единиц. Предположим, что в блокчейне уже на какой-то момент времени есть сформировавшаяся достоверная цепочка. Тогда, например, десятый блок будет говорить, кто имеет право находить пятнадцатый блок, одиннадцатый блок говорит о шестнадцатом и так далее (рис. 3).

Такая схема позволяется заранее знать, кто и когда сможет создать новый блок, то есть можно будет заранее отправлять транзакции майнерам на обработку.

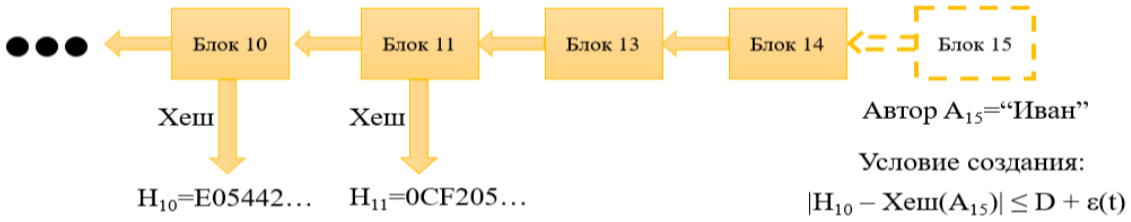

Рис. 3. Пример согласования транзакции.

4. Правовой статус криптовалют

С точки зрения закона правовой статус криптовалют очень спорен и меняется от страны к стране. Так, например, в США, начиная с 25 марта 2014 года, Служба внутренних

доходов постановила, что «Биткоин» не валюта, а собственность для налогообложения. В начале того же года Народный банк Китая запретил операции с «Биткоином» всем китайским финансовым учреждениям. Европейский суд 22 октября 2015 года постановил, что обмен «Биткоина» на фиатные деньги не облагается НДС и отнес все операции с «Биткоином» к валютно-денежным, всем членам Евросоюза было рекомендовано отменить налогообложение со всех операций с криптовалютами. В 2016 году Япония приняла ряд законопроектов, которые признали криптовалюту законным платежным средством. На территории России считается незаконным покупать товары на любую валюту, кроме рублей. Однако не существует контролирующего этот процесс органа.

Государственная Дума Российской Федерации приняла ряд законопроектов касающихся криптовалют в первом чтении: о цифровых правах [15], о финансовых активах [16] и о краудфандинге [17]. Данные законопроекты официально вводят определения таких понятия как майнинг, криптовалюта, смарт-контракты. Кроме того, данные законопроекты позволяют на законных основаниях менять рубли на криптовалюту и обратно. Однако они фактически приравнивают майнинг к предпринимательству, которое влечет за собой соответствующее налогообложение и оформление соответствующей документации, а создание новой криптовалюты приравнивается к инвестициям. Помимо этого, вводится обязательная идентификация личности для формирования электронного кошелька, что полностью дискредитирует идею самой криптоволюты. Однако, стремление государства контролировать рынок криптовалют вполне объяснимо: это попытка не допустить незаконный товарооборот, потерю налогов на добавленную стоимость и многое другое.

В России вопросы разработки собственной цифровой валюты и встраивания ее в хозяйственную деятельность активно изучается. Однако глава Центробанка Эльвира Набиуллина подчеркивает, что Центробанк рассматривает в качестве отечественной цифровой валюты исключительно стейблкоины в привязке к золоту и только для расчётов с другими странами. Стейблкоин это вид криптовалют, имеющий материальное обеспечение, чаще всего он имеют привязку к какой-то не цифровой валюте, например, к доллару или рублю.

Если обратиться к истории одной из самых успешных стейблкоинов Tether [17] , то можно увидеть то, что наибольшей проблемой в данном случае является вопрос обеспеченности ее материальными ресурсами. Если выпуск валюты децентрализован и нет какого-то эмиссионного центра, то вопросы контроля за ее обеспеченностью становятся сложной задачей. В связи с этим, в отношении компании создателя данной криптовалюты было инициировано разбирательство в связи с подозрениями в том, что на самом деле данная криптовалюта не обеспечена долларом из капитала в отношении один к одному. Анализ данной ситуации позволяет предположить, что выпуск стейблкоинов возможен только под контролем государственных органов, что с одной стороны, обеспечит надежность данного типа валют, а с другой повлечет потерю децентрализованности выпуска токенов.

5. Выводы

Современные протоколы взаимодействия внутри «блокчейн» сети позволяют достигать близкой к банковской системе скорости обработки транзакций. Появляются стратегии масштабирования сетей, однако для их реализации нужно согласовать одновременно работу нескольких блокчейнов. Авторами статьи продолжен конкретный алгоритм, показывающий возможность такого согласования без потери безопасности сети. Кроме того, предложен вариант алгоритма согласования транзакций внутри блокчейн сети, который позволяет реализовать шардинг блокчейна.

При исследовании вопроса о дальнейшем развитии криптовалют стоит учитывать множество факторов, рассмотренных выше. Анализ современных тенденций позволяет сделать вывод о том, что стремительное развитие криптовалюты, с точки зрения

технологий, делает ее реальной альтернативой современным деньгам. Однако при этом, возникают проблемы анонимности и отсутствия возможности контроля ситуации. По мнению авторов, в скором времени данная технология займет место среди других валют, а проблема контроля будет решена. Способ решения, данной проблемы представленный в отечественных законопроектах, при некоторой доработке, позволит обеспечить необходимый уровень контроля и сделает возможным использование цифровой валюты в качестве платежного средства.

Литература

1. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto – портал Bitcoin.org , 2008 – Режим доступа: https://bitcoin.org/bitcoin.pdf (Дата обращения: 15.06.2019)
2. Статья «Эфириум: долгожданный запуск состоялся» – портал BitNovosti, 2015, – Режим доступа: https://bitnovosti.com/2015/07/31/ether-annonce-start-date/ (Дата обращения: 15.06.2019)
3. Статья «ЦБ выразил готовность обсудить выпуск криптовалют с привязкой к золоту» – портал Интерфакс, 23.05.2019) – Режим доступа: https://www.interfax.ru/business/662191 (Дата обращения: 14.06.2019)
4. Статья «Сколько идет биткоин-транзакция и как сократить это время?» – портал Crypto Fox, 2018, – Режим доступа: https://crypto-fox.ru/faq/skolko-idet-tranzaktsiya-bitkoin/ (Дата обращения: 15.06.2019)
5. Статья «'Zerocoin' Add-on For Bitcoin Could Be Anonymous And Untraceable» – портал Forbes, 2013, – Режим доступа: https://www.forbes.com/sites/andygreenberg/2013/04/12/zerocoin-add-on-for-bitcoin-could-make-it-truly-anonymous-and-untraceable/#3adf688e65b2 (Дата обращения: 14.06.2016)
6. Статья «In Search of a Stable Electronic Currency» – The New York Times, 2014 – Режим досступа: https://www.nytimes.com/2014/03/02/business/in-search-of-a-stable-electronic-currency.html?_r=0 (Дата обращения: 03.05.2019)
7. Статья «The Bitcoin Bubble and a Bad Hypothesis» – портал «The National Interest» – https://nationalinterest.org/commentary/the-bitcoin-bubble-bad-hypothesis-8353 (Дата обращения: 03.05.2019)
8. Статья «Скорость транзакций: какой криптовалютой переводить быстрее» – портал The Blockchain Journal, 2018, – Режим доступа: https://thebcj.ru/2018/06/10/skorost-tranzakcij-kakoj-kriptovalyutoj-perevodit-bystree/ (Дата обращения: 15.06.2019)
9. Статья «EOS и EOSIO: обзор криптовалюты, курс и майнинг токенов» – портал Crypto Fox, 2018, – Режим доступа: https://crypto-fox.ru/currency/eos/ (Дата обращения: 15.06.2019)
10. Статья «Скорость транзакций EOS дошла до 1200 в секунду. В эфириуме затор. Совпадение?» – портал The Blockchain Journal, 2018, – Режим доступа: https://thebcj.ru/2018/07/16/v-akcii-chas-zemli-v-rossii-primut-uchastie-majnery-16/ (Дата обращения: 15.06.2019)
11. Статья «24 000 транзакций в секунду от Visa продолжают оставаться эталоном» – портал Rucoin, 2018, – Режим доступа: https://rucoin.net/24-000-tranzaktsiy-v-sekundu-ot-visa-prodolzhayut-ostavatsya-etalonom/ (Дата обращения: 15.06.2019)
12. Статья «Сможет ли блокчейн заменить Visa и MasterCard» – портал Let Know, 2018, – Режим доступа: https://letknow.news/publications/smozhet-li-blokcheyn-zamenit-visa-i-mastercard-7457.html (Дата обращения: 15.06.2019)
13. Статья «Будущее Эфириума: «газовый кризис» и шардинг в 2020 году» – портал Bits.media, 2018, – Режим доступа: https://bits.media/budushchee-efiriuma-gazovyy-krizis-i-sharding-v-2020-godu/ (Дата обращения: 15.06.2019)
14. Статья «Шардинг в Ethereum: полный FAQ от команды проекта» – портал Crypto Fox, 2018, – Режим доступа: https://crypto-fox.ru/faq/sharding-ethereum/ (Дата обращения: 15.06.2019)
15. Статья «Законопроект о «цифровых правах» прошел первое чтение» – официальная страница Государственной думы, 2018 – Режим доступа: http://duma.gov.ru/news/27029/ (Дата обращения: 15.06.2019)
16. Статья «В первом чтении принят законопроект о цифровых финансовых активах» – официальная страница Государственной думы, 2018 – Режим доступа: h http://duma.gov.ru/news/27027/ (Дата обращения: 15.06.2019)

17. Статья «Депутаты поддержали в первом чтении законопроект о краудфандинге» – официальная страница Государственной думы, 2018 – Режим доступа: http://duma.gov.ru/news/27031/ (Дата обращения: 15.06.2019)
18. Статья «This U.S. Dollar-Backed Token Issued On Bitcoin And Ethereum Is A Ticking Time Bomb» – портал Forbes, 2017 – Режим доступа: https://www.forbes.com/sites/ktorpey/2017/09/30/this-u-s-dollar-backed-token-issued-on-bitcoin-and-ethereum-is-a-ticking-time-bomb/#18487b356a16 (Дата обращения: 15.06.2019)
19. Статья «Деньги из воздуха. Создатели криптовалютного «доллара» подозревают в афере» – портал Forbes, 2017 – Режим доступа: https://www.forbes.ru/tehnologii/356785-dengi-iz-vozduha-sozdateley-kriptovalyutnogo-dollara-podozrevayut-v-afere (Дата обращения 16.06.2019)