УДК 004.75

Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки

Носиров З. А., Фомичев В. М.

Постановка задачи. *Технология распределённых реестров (блокчейн-технология) обладает важными достоинствами: надёжностью, неизменностью и прозрачностью. Данная технология применяется в различных областях, предоставляющих услуги в финансах, в промышленном Интернете вещей в общественных и социально значимых сервисах. Несмотря на большое количество проведённых исследований, посвящённых применению блокчейна в различных сферах деятельности, все ещё остаются актуальными комплексные исследования с технической и прикладной точки зрения.* ***Цель данной работы*** *– систематизировать знания о блокчейн-технологии, выявить проблемы и недостатки, а также предложить новые направления ее развития.* ***Результаты и их новизна:*** *в работе представлен комплексный обзор блокчейн-технологии (технические особенности). Проведён сравнительный анализ публичных и закрытых блокчейн-сетей, а также 3-х типов протоколов достижения консенсуса. Помимо этого, рассмотрены успешные отечественные блокчейн-проекты и выявлены сферы, в которых данная технология пользуется спросом. Также определены основные проблемы и недостатки данной технологии, а также предложены новые направления для проведения исследовательских работ, связанных с обеспечением безопасности блокчейн-технологии.* ***Практическая значимость:*** *результаты исследования могут быть полезны для начинающих исследователей, выбравших блокчейн-технологию областью своих интересов. Результаты, представленные в статье, также могут быть востребованы государственными учреждениями и крупными корпорациями Российской Федерации, занимающимися разработкой и внедрением блокчейн-решений в информационные системы.*

Ключевые слова: *блокчейн, распределённые реестры, блокчейн-технология, протоколы консенсуса, консенсус, ключевая информация, обзор блокчейна, технологии распределённых реестров.*

Введение

Технология систем распределённых реестров (блокчейн) вызывает интерес у правительств развитых и развивающихся стран, а также данная технология бурно обсуждается в научных кругах. Разработка криптовалюты (биткоин) программистом Сатоши Накамото в 2009 г. положило начало развитию блокчейн-технологии (БТ) [1]. Также появление данной криптовалюты вызвало обеспокоенность у финансовых организаций. Это связано с тем, что биткоин предлагал независимость от какого-либо централизованного воздействия. Данное свойство достигается благодаря БТ, которая легла в основу при разработке криптовалюты.

Библиографическая ссылка на статью:
Носиров З. А., Фомичев В. М. Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки // Системы управления, связи и безопасности. 2021. № 2. С. 37-75. DOI: 10.24412/2410-9916-2021-2-37-75.

Reference for citation:
Nosirov Z. A., Fomichev V. M. Analysis of Blockchain Technology: Architectural Basics, Application Examples, Future Trends, Problems and Disadvantages. *Systems of Control, Communication and Security*, 2021, no. 2, pp. 37-75 (in Russian). DOI: 10.24412/2410-9916-2021-2-37-75.

Во многих работах блокчейн-технологию рассматривают, как часть четвертой промышленной революции [2-5]. Это связано с его основными свойствами такими, как надёжность, неизменность и прозрачность. Благодаря этим свойствам появляются множество потенциальных возможностей использования данной технологии. Наибольшее распространение технология распределённых реестров получила в финансовой сфере [6-9] появились новые виды криптовалют. Также проведены работы, где описаны успешные результаты внедрения БТ в систему образования некоторых европейских стран [10-13]. Помимо этого, БТ активно используется в системах электронного голосования и в технологии Интернета вещей [14-16].

В России блокчейн-технологию на уровне государства стали развивать относительно недавно. Министерством цифрового развития, связи и массовых коммуникаций РФ в 2019 г. была предложена дорожная карта развития «сквозной» цифровой технологии «Системы распределённого реестра» [17]. В данном документе определены приоритеты и перспективы развития БТ в России. Помимо этого, обозначены ожидаемые результаты внедрения БТ и потенциальные зоны международной кооперации. За последние пять лет зарубежными так и отечественными учёными проведено значительное количество инновационных исследований. В обзорных работах [18-22] описаны технические особенности криптовалют; рассмотрены возможности использования БТ в медицине, энергетическом секторе и в промышленном Интернете вещей [23-27]; рассмотрены возможности использования БТ в технологиях, связанных с искусственным интеллектом (ИИ) и анализом больших данных [28-31].

Задача данной работы, определяющая ее отличие от вышеперечисленных работ – систематизировать знания о блокчейн-технологии, выявить проблемы и недостатки, а также определить дальнейшие направления развития БТ. Такой обзор позволяет выделить в дальнейшем наиболее актуальные направления исследований в области БТ.

1. Основы архитектуры блокчейн-технологии

Блокчейн-технология представляет собой выстроенную по определённым правилам непрерывную последовательную цепочку блоков, содержащих информацию [32]. На (рис. 1) приведена структурная схема блоков в блокчейн сети. Каждый блок в блокчейне ссылается на предыдущий блок, данная связь реализована с помощью хеш-значений. Необходимо отметить, что существует так называемый *блок генезиса* (*genesis block*). Это самый первый блок, у которого нет родительского блока в отличие от остальных. Далее подробно рассмотрим типичную структуру блокчейн сети.

Каждый блок в блокчейн сети состоит из двух главных частей – *заголовка* (*head*) и *тела* (*payload*). Head содержит информацию, которая отвечает за стабильность, а также иммутабельность сети. Payload – содержит список всех транзакций, которые должны быть сохранены в данном блоке и попасть в блокчейн-сеть (БС). На (рис. 2) приведена структура блоков БС.

В классическом блокчейн сети Head содержит следующие поля:

– номер версии блока (*ver_block*);

№2. 2021
ISSN 2410-9916

– хеш предыдущего блока (*prev_block*);
– хеш всех транзакций в текущем блоке (*mrkl_root*);
– временную метку, когда был создан блок (*timestamp*);
– «*bits*» и «*nonce*» параметры используемые при майнинге.

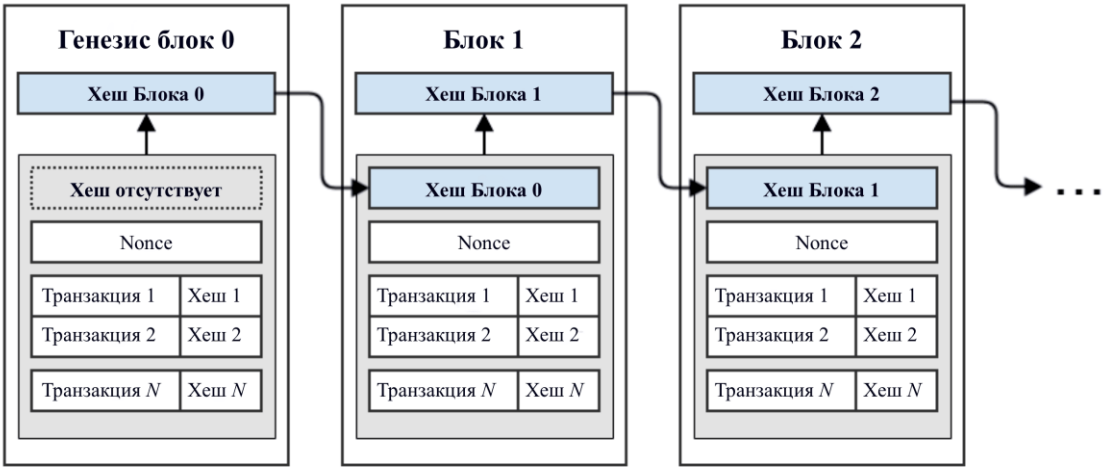

Рис. 1. Последовательность блоков в блокчейн сети

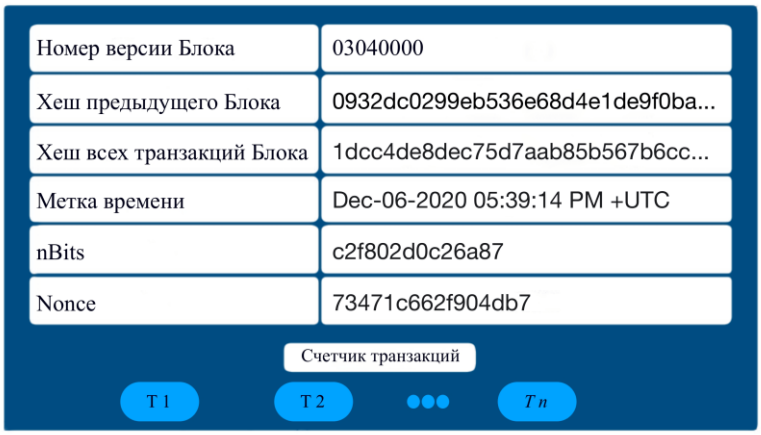

Рис. 2. Структура блока

Как ранее упоминалось payload состоит из счётчика транзакций и списка всех транзакций входящих в текущий блок. Также существует максимальное количество транзакций, которое может содержать блок. Данное значение зависит от размера транзакции. Для того чтобы проверить подлинность транзакции используется механизм ассиметричной криптографии.

Цифровая подпись – это криптографический алгоритм, применяемый пользователем к документу (сообщению), который используется для проверки подлинности и целостности документа (сообщения), а также для удостоверения авторства по отношению к документу (сообщению) [33]. Криптография с открытыми ключами (*public-key cryptography*) и хеш-функции предоставляют математические средства, позволяющие эффективно использовать цифровую подпись. Отметим, что использование хеширования и цифровых подписей является необходимым для БТ. Хеширование даёт возможность каждому из участников

DOI: 10.24412/2410-9916-2021-2-37-75
URL: http://sccs.intelgr.com/archive/2021-02/03-Nosirov.pdf

сети определить текущее состояние блокчейна. А подписи обеспечивают доказательство того, что все транзакции были совершены только настоящими владельцами. Для большего понимания рассмотрим подробный пример использования цифровой подписи в БТ.

Каждому пользователю блокчейн сети принадлежит пара, открытого и закрытого ключей. Закрытый ключ пользователь использует для совершения сделок. Сделки, подписанные цифровой подписью, распространяются по всей блокчейн сети и с помощью открытых ключей можно получить доступ к ним. Открытые ключи доступны каждому пользователю блокчейн сети. На (рис. 3) продемонстрирован пример использования цифровых подписей в БС.

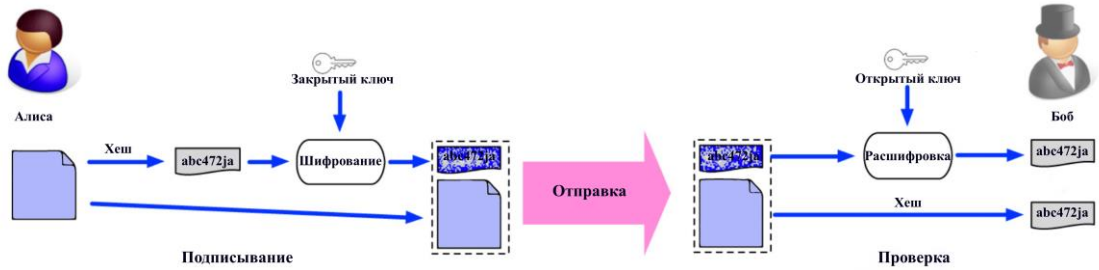

Рис. 3. Использование цифровой подписи в БТ

Базовый алгоритм подписания документа (сообщения) цифровой подписью включает два этапа: этап подписания и этап проверки. Рассмотрим пример, описанный на (рис. 3). Допустим, что Алиса хочет подписать транзакцию. Сначала ей необходимо вычислить хеш-значение самой транзакции. Используя свой закрытый ключ Алисе необходимо зашифровать полученное хеш-значение транзакции. Затем зашифрованный хеш с исходными данными Алиса отправляет Бобу. Для проверки подлинности полученных данных Бобу необходимо выполнить расшифрование данных с помощью открытого ключа Алисы. Затем Бобу нужно вычислить хеш-значение исходных данных, использовав ту же хеш-функцию, которой воспользовалась Алиса. И путём сравнения данных, полученных на этапе расшифрования и вычисления хеш-значения Боб, может сделать выводы о подлинности транзакции. В блокчейн сетях в качестве алгоритмов цифровых подписей используется Elliptic Curve Digital Signature Algorithm (ECDSA) [34].

1.2. Ключевые характеристики блокчейн-технологии

Блокчейн-технология обладает рядом преимуществ, в частности, можно выделить несколько ключевых характеристик, которые повлияли на ее развитие.

Децентрализация. Если рассматривать обычные централизованные системы (руководящие органы), то каждая транзакция должна быть подтверждена центральным доверенным звеном, например, в качестве такого звена может выступать центральный банк (ЦБ). В свою очередь это приводит к неизбежным затратам для обеспечения ИБ. Иначе говоря, транзакция в блокчейн сети может быть проведена между любыми двумя равными пользователями без проверки подлинности со стороны центрального сервера. Таким образом, применение

блокчейн-технологии может значительно снизить затраты на поддержание функционирования серверов (в том числе расходы на разработку и эксплуатационные расходы) и решить определённые задачи безопасности и обеспечения необходимой производительности.

Неизменность. Любая совершаемая транзакция в блокчейн сети подтверждается другими участниками данной сети и фиксируется в соответствующем блоке. Каждый узел сети располагает данными всех транзакций, совершенных в БС. Внести изменения в транзакции не представляется возможным, так как блоки и транзакции проверяются другими узлами. Если большинство узлов (пользователей) посчитает, что транзакция является действительной, то ее записывают в реестр. Это способствует обеспечению прозрачности и целостности информации. Таким образом, без согласия большинства узлов никто не сможет добавить блоки транзакций в распределённый реестр.

Анонимность. Каждый пользователь может взаимодействовать с блокчейн сетью с помощью сгенерированных адресов. Кроме того, пользователь может генерировать множество адресов, чтобы избежать однозначной идентификации. Отсутствует центральный сервер, хранящий идентификационные данные пользователей. Сей факт обеспечивает определённую степень конфиденциальности в отношении операций, включённых в БС. Анонимность достигается только в публичных блокчейн сетях, подробнее описано в следующем разделе.

Прозрачность. Так как каждая из транзакций в БС проверяется и записывается с меткой времени, пользователи могут легко проверить и отследить предыдущие записи. Например, в криптовалюте биткоин каждая транзакция может быть итеративно прослежена до предыдущих транзакций. Это улучшает прослеживаемость и прозрачность данных, хранящихся в БС.

1.3. Классификация блокчейн сетей

Как и любой свободный рынок, отрасль блокчейна развивается методом проб и ошибок – путём многочисленных экспериментов, конкурирующих или сотрудничающих друг с другом проектов, из которых постепенно выделяются наиболее жизнеспособные. Блокчейн-проекты постоянно видоизменяются и совершенствуются, и даже пользуются разработками друг друга, так как большинство из них основаны на открытом исходном коде. Это означает, что каждый из БС практически невозможно отнести к какому-либо классу. Однако почти у любой БС есть свои особенности и признаки, а также достаточно чётко очерченные рамки возможного применения [35].

Самым корректным разделением блокчейн сетей принято считать их разделение по степени открытости, таким образом их можно разделить на публичные (открытые) и закрытые сети. Степень открытости чаще всего зависит от нескольких факторов. Одним из наиболее значимых факторов является доступность исходного кода протокола БС. Обычно под этим подразумевается наиболее распространённый клиент для данной БС, например Bitcoin Core для биткоин сети.

Следующим наиболее значимым фактором является – возможность свободного подключения нового узла к сети без получения каких-либо разрешений. Данное свойство является основным определяющим отличием открытой блокчейн сети от закрытой. На сегодня большинство БС являются публичными и в большинстве из них для достижения консенсуса используется протокол Proof of Work (PoW), об этом более подробно описано в разделе алгоритмы консенсуса.

Для подключения новых пользователей в публичных блокчейн сетях достаточно лишь скачать совместимую с данной версией протокола клиентское приложение и установить связь с другими узлами сети. Уровень участия пользователя всегда определяется им самим и зависит только от его личных (финансовых и аппаратных) ресурсов. Необходимо также отметить, что никто из пользователей публичной БС не может отключить других пользователей от распределённой сети, так как все участники равноправны.

В закрытых БС подключение/отключение пользователей регулируются определёнными узлами или группой узлов, имеющие более высокий уровень полномочий по сравнению с остальными участниками сети [36]. Далее сравним публичные и закрытые блокчейн сети по следующим параметрам:

Достижение консенсуса. В публичных БС любой узел может принять участие в процессе достижения консенсуса. А в закрытых БС то она полностью контролируется одной организацией, которая может определить окончательный консенсус.

Прозрачность. Транзакции в публичных БС доступны общественности и каждый пользователь может проследить все действия, в то время как в закрытых БС чтение данных регулируется настройками сети.

Неизменность. Так как транзакции хранятся в распределённой сети, то практически невозможно изменить публичную БС. В закрытых БС при желании можно изменить транзакции это возможно благодаря управляющей организации.

Эффективность. Распространение транзакций и блоков в публичных БС занимает много времени, так как в сети имеется большое количество узлов. Поэтому значительно снижается пропускная способность сети. В закрытых БС количество узлов контролируется управляющей организаций тем самым можно повышать/снижать пропускную способность сети.

Децентрализованность. Основной отличительной особенностью между этими блокчейн сетями является то, что публичная БС сохраняет основную идею блокчейн-технологии (распределённость), в то время как закрытые БС полностью централизованы и контролируются определёнными группами узлов.

На таблице 1 приведены результаты сравнительного анализа блокчейн сетей.

Необходимо отметить, что не все публичные блокчейн сети обладают низкой эффективностью, так как для многих протоколов консенсуса, используемых в публичных БС, исследователи разрабатывают дополнительные механизмы увеличения производительности. В следующем разделе рассмотрены некоторые из них.

Таблица 1 – Результаты сравнительного анализа БС

Параметр	Публичная БС	Закрытая БС
Достижение консенсуса	Участвуют все узлы	Регулируется одной организацией
Прозрачность	Транзакции общедоступны	Транзакции могут быть общедоступными или ограниченными
Неизменность	Практически невозможно изменить данные	Существует возможность изменения данных
Эффективность	Низкая	Высокая
Централизованность	Отсутствует	Присутствует

1.4. Алгоритмы достижения консенсуса

Достижение консенсуса в распределённой среде сводится к решению задачи о византийских генералах. Формулировка задачи выглядит следующим образом.

Византийская армия, состоит из *n* легионов, каждым, из которых командует свой генерал, а также у армии есть главнокомандующий, которому подчиняются генералы легионов. Армия окружает город с целью нападения.

Благоприятный исход войны зависит от действий всех генералов. Генералам необходимо связаться, чтобы прийти к единому соглашению о том, атаковать город или нет. Однако среди генералов могут быть предатели, в том числе главнокомандующий. Предатель может посылать разного содержания приказы разным генералам [37].

Достижение консенсуса в данной обстановке является весьма непростой задачей. Решение задачи послужило основой математической модели построения и развития блокчейн-технологии. В блокчейн сетях нет центрального органа, который обеспечивал бы одинаковую работу на удалённых узлах. Таким образом, имеется потребность в протоколах обеспечения консенсуса между распределёнными узлами. Исследователи все чаще демонстрируют новые протоколы консенсуса, в большинстве случаев они являются некими модификациями основных существующих протоколов. Перед тем как рассмотреть наиболее часто используемые протоколы достижения консенсуса определим, что представляют из себя *вилки* (*forks*) в блокчейн сетях.

В децентрализованной сети могут одновременно генерироваться несколько действительных блоков. В результате создаются вилки. На (рис. 4) продемонстрирован сценарий разветвления блокчейн сети.

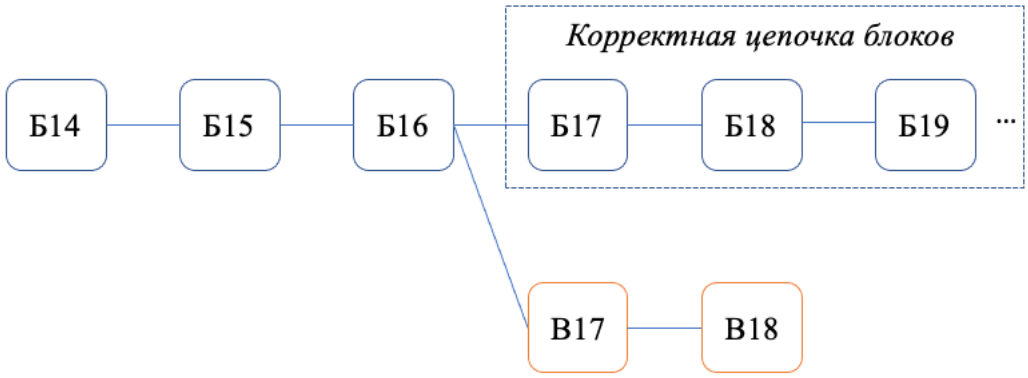

Рис. 4. Разветвление блокчейн сети (вилки)

Вилка – это изменение протокола или отклонение от предыдущей версии блокчейна. Существует два вида вилок: *мягкие* (*soft forks*) и *жёсткие* (*hard forks*) [38].

Soft fork – это обновление программного обеспечения (ПО), которое имеет обратную совместимость со старыми версиями [39]. Это означает, что участники, которые не перешли на новое ПО, все равно могут участвовать в процессах валидации и проверки корректности транзакций.

Реализовать soft fork гораздо проще чем hard fork, так, как только большинству участников необходимо обновить клиентское ПО. Все участники, независимо от того, обновили они или нет, будут продолжать распознавать новые блоки и поддерживать совместимость с сетью.

Однако следует отметить, что устаревшая версия ПО влияет на ее функциональность. Участники сети с устаревшим ПО по-прежнему могут видеть, что входящие новые транзакции действительны. Но проблема состоит в том, что при добавлении нового блока они будут отклонены блокчейн сетью.

Hard fork – это обновление ПО, которое не имеет обратной совместимости [40]. Всем участникам необходимо перейти на новое программное обеспечение для того, чтобы продолжить участвовать в создании новых блоков. Те, кто не обновился, будут отделены от сети и в дальнейшем не смогут проверять новые транзакции. Это разделение приводит к постоянному расхождению блокчейн сетей. До тех пор, пока в цепочке меньшинств есть поддержка в виде участников майнинга, то две цепочки будут существовать одновременно (например: Bitcoin и Bitcoin Cash).

1.4.1. Протокол доказательства выполнения работы

Proof of Work (PoW, доказательство выполнения работы). Как упоминалось ранее протокол PoW связан с появлением криптовалюты биткоин [1]. PoW является одним из ресурсоёмких протоколов консенсуса. В данном протоколе каждому узлу необходимо вычислять значение хеша постоянно меняющегося заголовка блока. В распределённой среде все узлы непрерывно вычисляют значение хеша, используя различные случайные последовательности, называемые «nonce». В частности, решением является следующее:

$$H(n \vee H(b)) < t,$$

где: H – это криптографическая хеш-функция (например, SHA-256), n – значение «nonce», b – это текущее содержимое блока и t – время, затрачиваемое на нахождение нового блока.

Насколько быстро создаётся блок, зависит от того, насколько сложна головоломка. В биткоин сети значение t, эквивалентна 10 мин. Litecoin и ZCash уменьшают t до нескольких минут для достижения меньшего среднего времени генерации нового блока. Значение t не может быть произвольно маленьким, так как это приводит к лишним вилкам в блокчейн сети. Вилки не только приводят к расточительному расходованию ресурсов, но и имеют негативные последствия для безопасности, так как позволяют реализовать атаку двойного расходования.

После получения целевого значения хеша остальным участникам необходимо взаимно подтвердить корректность хеша. Тогда транзакции, хранящиеся в новом блоке, могут быть проверены в случае мошенничества. Таким образом появляется новый блок в цепочке, который тесно связан с предыдущим. Узлы, вычисляющие значение хешей, называются *майнерами* (*miners*), а сама процедура PoW называется *майнингом* (*mining*). Так как вычисление хешей является трудоёмким процессом, то реализован механизм стимулирования, например, в сети биткоин узел получает некую часть данной криптовалюты.

В данном протоколе при возникновении вилок легитимной считается та цепь, которая длиннее. В качестве примера обратимся к (рис. 4). Рассмотрим две вилки, созданные одновременно проверенными блоками Б17 и В17. Майнеры работают в обеих вилках и добавляют к одной из них вновь созданный блок. Когда новый блок (допустим, Б18) добавляется к блоку Б17, майнеры, работающие на вилке В17-В18, переключаются на Б18. Блок В18 в вилке В17-В18 становится *«сиротским блоком»* (*orphan block*), так как он больше не будет увеличиваться.

Так как майнерам приходится проделывать большое количество компьютерных вычислений, которые приводят к трате ресурсов (электроэнергии) были разработаны более эффективные PoW протоколы. Например, в работе [41] ищут специальные цепочки простых чисел, которые можно использовать в математических исследованиях.

1.4.2. Протоколы доказательства владения долей

Proof of Stake (PoS) – доказательство владения долей, является более эффективной альтернативой PoW. В протоколе PoS пользователям вместо того, чтобы вычислять корректный «nonce» как в PoW необходимо доказать право собственности на некоторое количество цифровых токенов. Считается, что пользователи с большим количеством токенов менее склонны к атакам на блокчейн сеть. В свою же очередь протокол PoS является несправедливым, так как один пользователь с большим количеством токенов обязательно будет доминировать в сети. В связи с этим разработаны новые модификации отбора узла сети для генерации следующего нового блока. В частности, в Blackcoin используется механизм рандомизации для прогнозирования следующего генератора (узла) блока [42]. Используется формула, цель которой является нахождение

наименьшего значения хеша в комбинации с размером доли. В работе [43] узлы с большим количеством старых токенов имеют большую вероятность для генерации нового блока. Многие блокчейн сети изначально использовали PoW для достижения консенсуса, но постепенно начали переходить на PoS. Например, Ethereum планируется привести к новой реализации Casper которая в конечном итоге преобразует Ethereum в блокчейн PoS (также известный как Ethereum 2.0) [44]. Также можно отметить протокол Nxt – гибрид двух протоколов PoW и PoS [45]. Отличительной особенностью является то, что отбор узла для генерации следующего блока и право подтверждения предыдущего блока вычисляется алгоритмом, который зависит от: хеша идентификатора предыдущего блока и открытого ключа, создавшего предыдущий блок; количества токенов на счету пользователя, подключённого к блокчейн сети. Вероятность формирования очередного блока выше у пользователя с большим эффективным балансом на счету. Эффективным балансом считается количество токенов на счету пользователя, не менявшееся последние 1440 блоков.

Delegated Proof of Stake (DPoS) – делегированное доказательство владения долей, является альтернативой консенсусам PoW и PoS. Протокол DPoS был разработан в 2014 г. в рамках проекта Graphene и впервые был задействован в проекте Bitshares, позже в проекте Steemit [46-48].

Основной принцип работы протокола DPoS выглядит следующим образом: реализовано разделение голосующих и валидирующих узлов, то есть участники сети, которые имеют право голоса в системе (держатели токенов) не являются при этом валидаторами транзакций. Таким образом, одно подмножество участников выбирает другое подмножество, которое в свою очередь будет формировать блоки. Условия, в которых работает данный алгоритм консенсуса, кардинально отличаются от условий, в которых работают протоколы PoW и PoS. А именно, валидаторам необходимо раскрыть свои личности и заявить о готовности бесперебойно поддерживать работу полноценного узла сети, своевременно выполнять верификацию транзакций и формировать новые блоки.

В DPoS-сетях, в отличии от Peercoin, токены пользователей, могут одновременно участвовать в голосовании и при этом использоваться для переводов. При изменении баланса вес в голосовании будет изменяться соответственно [49].

1.4.3. BFT-ориентированные протоколы

До сих пор были рассмотрены протоколы консенсуса, используемые в открытых БС, которые работают в публичной среде и нацелены на децентрализацию. Применение вышерассмотренных протоколов в корпоративном секторе не является возможным так как они обладают низкой пропускной способностью. Для увеличения производительности был придуман новый класс протоколов консенсуса – Byzantine Fault Tolerance (PBFT), в которых анонимность не является важным аспектом, то есть узлы знают некую информацию о друг друге (изначально узлы аутентифицированы). Благодаря этому можно оптимизировать алгоритмы консенсуса и достичь намного большей пропускной способности. Фактически скорость может увеличиться в 10 раз, от сотен до тысяч транзакций в секунду, что отлично подходит для корпоративных реалий.

Practical Byzantine Fault Tolerance (PBFT) – реализация протокола задачи византийских генералов является быстрым и легко масштабируемым протоколом консенсуса. Широко используется в проекте Hyperledger Fabric в качестве протокола консенсуса так как может обрабатывать до 1/3 нелегитимных транзакций [50]. Принцип работы протокола выглядит следующим образом: на вход валидатору поступает сообщение, по которому ему нужно принять решение – считать его истинным или нет. Для этого валидатор выполняет внутренние проверки, затем поочерёдно опрашивает остальные узлы, действительна ли транзакция. Если 2/3 участников проголосуют за эту транзакцию как корректную, валидатор принимает её и передаёт своё решение в блокчейн сеть другим валидаторам. Также необходимо отметить, что в PBFT отсутствует процедура хеширования [51].

Delegated Byzantine Fault Tolerance (DBFT) – это делегированный алгоритм консенсуса византийской отказоустойчивости с большим масштабированием сети. Данный алгоритм предложила команда разработчиков NEO во главе с Эриком Чжаном, а в 2016 г. применили его в проекте NEO [52]. Принцип работы такой, что держатели крипто-токенов выбирают узлы согласования, которые делятся на спикеров и делегатов. Узлы-спикеры отвечают за проведение транзакций и формирование блоков в сети, а узлы-делегаты отвечают за проверку первых (узлов-спикеров) для достижения консенсуса. Поэтому алгоритм стал удачным решением, которое сочетает в себе безопасность и масштабирование сети. Но на фоне скорости присутствует вероятность централизации. Это связано с тем, что большая половина узлов может быть сосредоточена в одних руках [53].

Federated Byzantine Agreement (FBA) – федеративное византийское соглашение. FBA не требует разрешения или заранее известного набора участников, в отличие от PBFT и других вариаций BFT. Транзакции в этом протоколе проверяются фиксированным количеством участников, которые выбираются из списка узлов сети, находящихся в активном состоянии. Необходимо отметить, что по правилам FBA существуют *шлюзы* (*gateways*) и *мэйкеры* (*market-makers*), которые обеспечивают честность и ликвидность сети. Первые выступают в роли традиционных банков, владеющих финансовыми средствами и создающих их эквивалент в цифровых токенах. Вторые – ведут учётные записи с многочисленными шлюзами и сразу в нескольких валютах [54].

XRP Ledger Consensus Protocol (XRP Ledger) – это алгоритм консенсуса сети XRP Ledger, который отвечает за достижение согласия между серверами. Алгоритм способен достичь консенсуса без полного согласия относительно того, какие узлы являются членами сети. Разработчиком алгоритма стала компания «Ripple Labs Inc», которая запустила его в 2012 г. [55]. Принцип работы такой, что реестр XRP Ledger состоит из серверов отслеживания и валидаторов. Сервера отслеживания распределяют транзакции и отвечают на запросы о состоянии реестра, валидаторы отвечают за обработку транзакций. XRP Ledger использует процесс консенсуса, для обеспечения того, что транзакции обрабатываются, а проверенные реестры являются согласованными по распределённой сети.

1.5. Сравнительный анализ протоколов достижения консенсуса

Каждый протокол консенсуса имеет преимущества так и недостатки. В таблице 2 приведены результаты сравнительного анализа рассмотренных протоколов консенсуса.

Таблица 2 – Сравнительный анализ протоколов консенсуса

Протокол консенсуса	Тип блокчейн сети	Производительность	Разработанные решения
PoW	открытая	низкая	Bitcoin-NG [56], Byzcoin [57], Bitcoin [1] и др.
PoS	открытая	высокая	Tendermint [58], Ethereum [44] и др.
DPoS	открытая	высокая	EOS [59], BitShares [60] др.
BFT	закрытая	высокая	Hyperledger Fabric 1.0 [50] и др.
PBFT	закрытая с разрешениями	высокая	Hyperledger [50], Chain [61] и др.
PBFT-ориентированные	закрытая	высокая	Parallel BFT [62], Optimistic BFT [63] и др.
DBFT	закрытая	очень высокая	NEO [64], TON [65] и др.
FBA	закрытая	высокая	Stellar [66] и др.
XRP	закрытая	высокая	Ripple [67] и др.
Другие	открытые	–	Другие протоколы, основанные на PoW, имеют форму Proof of X, например: Proof of Space [68] Proof of Activity [69], Proof of Authority [70] и др.

Хороший протокол консенсуса должен быть в идеале эффективным, безопасным и удобным в использовании. В распространённых протоколах консенсуса до сих пор исследователи находят уязвимости, которые могут негативно повлиять на работоспособность блокчейн сети. Поэтому разрабатываются новые решения, направленные на устранение найденных недостатков.

Следует отметить, что появление смарт-контрактов в БС позволило БТ перейти на новый уровень развития.

Смарт-контракт – инструмент, который формализует и защищает компьютерные сети путём объединения протоколов с пользовательским интерфейсом [71]. Применительно к БТ, смарт-контракты позволяют создавать доверительные протоколы. Это означает, что обе стороны могут взять на себя обязательства через блокчейн сеть, без знания или доверия друг к другу. Участники данного процесса могут не беспокоиться о правильности выполнения обязательств, поскольку если условия не будут удовлетворены, то контракт аннулируется.

2. Примеры использования блокчейн-технологии

БТ может найти практическое применение во многих прикладных сферах. В данном разделе рассматриваются лишь перспективные блокчейн-решения, которые уже внедрены в массовый сегмент или же находятся на стадии тестирования.

2.1. Финансовый сектор

Текущая ситуация связанная с криптовалютами все больше оказывает огромное влияние на традиционные модели финансовых услуг. До недавнего времени многие финансовые организации высказывались негативно в отношении использования криптовалют в банковской сфере, но спустя некоторое время начали активно использовать БТ и даже начали разрабатывать собственные криптовалюты. Далее рассмотрим финтех проекты с использованием БТ.

В 2020 г. «Сбербанк», «Альфа-Банк» и «М.Видео» начали использовать блокчейн для автоматического обмена документацией по факторинговым сделкам. Со стороны автоматизация данного процесса выглядит следующим образом: операторы «М. Видео» загружают в единую систему файл, в котором все данные о товаре записаны в специальном формате, затем смарт-контракты (Ethereum) автоматически обрабатывают эти данные и определяют статус поставки. В случае несоответствия объёмов или других данных по поставке товара платформа оповещает банк о необходимости дополнительной проверки [72].

Ещё одним примером использования БТ в финансовой сфере является проект от телекоммуникационной компании «Мегафон». В 2017 г. «Мегафон» выпустил облигации на 500 млн рублей, учёт прав по которым осуществлялся на блокчейне. Покупателем облигаций стал АО «Райффайзенбанк», а разработчиком децентрализованной платформы является Национальный расчётный депозитарий. Система для проведения сделки создана на блокчейн-платформе Hyperledger Fabric 1.0. Для неё развёрнуто три узла децентрализованного реестра – в НРД, «Райффайзенбанке» и «Мегафоне» [73].

Также следует отметить проект «S7» и «Газпромнефть-Аэро» который направлен на автоматизацию оплаты топлива. Эти компании разработали и внедрили совместные смарт-контракты (Aviation fuel smart contracts – AFSC). Это первый для российского авиарынка опыт использования технологий распределённых реестров [74].

Помимо этого, в 2019 г. АО «Первоуральскбанк» стал первым среди банков и небанковских факторинговых компаний организацией, которая провела полный цикл финансирования через блокчейн-платформу «Факторин». В работе платформы используются технологии распределённых реестров и файлового хранилища. В ходе сделки осуществляется автоматический обмен данными между ИТ-системами участников. Данные доступны только участникам сделки [75].

Среди зарубежных стран также можно выделить перспективные блокчейн проекты. Например, Южнокорейская компания «LG CNS» разработала систему проведения платежей в криптоактивах. На данный момент компания тестирует систему среди сотрудников и в ближайшем будущем планирует внедрить в повседневную жизнь граждан [76].

Сингапурский банк «DBS Bank» использует торговую платформу Contour на основе технологии Corda R3 для проведения расчётов по аккредитивам с помощью БТ. Клиенты «DBS» могут проводить переговоры с заявителями и получателями денег в режиме реального времени, что повышает точность выпуска аккредитивов. Транзакции также отслеживаются в режиме реального времени и проходят аудиторскую проверку, что обеспечивает дополнительную прозрачность, а при возникновении расхождений – помогает более эффективно их устранять [77].

Китайская телекоммуникационная компания «China Telecom» интегрировала БТ в 5G-системы для повышения эффективности распределения доходов, выставления счетов и платежей за услуги связи – например, роуминга (для пользователей) или совместного использования телекоммуникационной инфраструктуры (для других операторов). Среди плюсов интеграции БТ и 5G компания отметила улучшение услуг международного роуминга, так как информация пользователей каждого оператора мобильной сети безопасно и беспрепятственно передаётся в блокчейне без участия посредников, что делает возможным автоматическое выставление счетов и платежей [78].

2.2. Государственные и муниципальные сервисы

Технология распределённых реестров широко используется в государственных и муниципальных службах. Существует огромное количество блокчейн-проектов, которые внедрены в повседневную жизнь граждан нашей страны. Рассмотрим наиболее значимые из них.

В апреле 2020 г. Федеральная налоговая служба Российской Федерации запустила блокчейн-платформу для льготного кредитования малого и среднего бизнеса, пострадавшего от пандемии COVID-19. К системе присоединились «ВТБ» и «Сбербанк». Схема работы системы выглядит следующим образом: у каждого участника системы формируется свой узел в рамках распределённых реестров, который генерирует последовательные записи. Система гарантирует безопасность данных, при этом обеспечивая доступ к ним всем участникам проекта. Прозрачность платформы исключает выдачу повторных кредитов [79].

Суд по интеллектуальным правам стал первым судом России, внедрившим в работу технологию блокчейн. В 2018 г. государственный орган стал узлом блокчейн-инфраструктуры IPChain [80], что позволило размещать информацию о спорах и принятых по ним решениях. Результатом данного проекта стала возможность для участников рынка оперативно получать последние данные о транзакциях с интеллектуальной собственностью [81].

Примеру суда по интеллектуальным права последовал Верховный суд Российской Федерации. БТ использовали для организации электронного голосования на дистанционном пленуме. Разработчиком выступила компания «Лаборатория Касперского», систему развернули на базе российского облачного хранилища от компании «Softline» [82].

Помимо судов блокчейн-технологию также начали использовать для предоставления дипломов об окончании ВУЗов. Пензенский государственный университет начал предоставлять выпускникам электронные дипломы. Выдача,

хранение и проверка цифровых дипломов осуществляется при помощи решения компании «Credentia», основанного на блокчейне Ethereum [83].

Среди зарубежных блокчейн проектов в области предоставления государственных и муниципальных услуг также можно выделить пару успешных проектов.

Южнокорейская телекоммуникационная компания «SK Telecom» запустила блокчейн-систему для хранения и управления цифровыми государственными сертификатами SK Wallet. Оно поддерживает хранение и управление электронными сертификатами, которые выпускает ведомство (Министерство общественной администрации и безопасности). Система позволяет хранить цифровые копии регистрационных карточек резидентов страны и документов о медицинском страховании, иммиграционные свидетельства, а также другие документы, которые ранее выдавались на бумаге. Также SK Wallet позволяет отправлять документы в государственные и частные учреждения [84].

В 2020 г. Бюро фискальной службы (подразделение Казначейства США) реализовала блокчейн-проект для прозрачной раздачи грантов. Одна из проблем прослеживаемости грантов заключается в том, что многие из них проходят через третьи лица. Ключевая цель проекта – обеспечить прозрачность платежей субполучателей. В то же время использование блокчейна должно упростить субполучателям получение оплаты или предоставить все необходимые данные о задержках. Проект находится на стадии тестирования и в конце 2021 г. разработчики планируют опубликовать полученные результаты [85].

Примечательное решение предложила канадская компания «Emerge», в частности «Emerge» разработала блокчейн-приложение Citivas для борьбы с эпидемией COVID-19 в Латинской Америке. В данном решении разработчики реализовали проверку идентификационного номера жителя с записями, хранящимися в реестре. Это позволило регуляторам определять, может ли человек безопасно покинуть свой дом. Приложение также помогает определить наиболее безопасное время для похода в магазин за необходимыми покупками для разных категорий людей [86].

2.3. Промышленность и сельское хозяйство

К сожалению, в России в сфере промышленности и сельского хозяйства реализовано малое количество успешных проектов. Например, на территории Климовского трубного завода Московской области группа «Полипластик» осуществила запуск пилотного проекта по внедрению в производство полимерных труб системы маркировки на базе блокчейн-платформы Exonum от «Bitfury». Принцип работы платформы заключается в том, что информация о произведённых трубах заносится в реестр, а паспорт качества помечается специальным QR-кодом, соответствующим идентификационному номеру готового продукта. Контроль качества осуществляется посредством сверки достоверности данных, подлог которых оказывается невозможным благодаря блокчейн-технологии. Проект позволяет достичь прозрачности действий каждого участника проекта, а также простоту аудита и непрерывного доступа к информации [87].

С целью сокращения времени взаиморасчётов между потребителем и поставщиком, повышения прозрачности рынка электроэнергии «Россети Урал» реализовали проект использования технологии блокчейн в электроэнергетике. База данных в виде реестра не хранится локально у владельца, а распределена между участниками сети, в данном случае игроками розничного рынка электрической энергии. В результате изменить что-либо невозможно. В качестве пилотной зоны был выбран один из районов Екатеринбурга, где в нескольких жилых домах установлено 250 приборов учёта. Показания счётчиков снимаются каждые 30 минут, информация в онлайн-режиме поступают в распределённый реестр [88].

Компания по производству фруктов и овощей без участия человека с использованием искусственного интеллекта в партнёрстве с компанией «Bitfury» внедрила технологическую систему контроля качества на основе БТ. Проект находится на стадии тестирования и разработчики ожидают положительных результатов от функционирования системы, в частности оптимизацию контроля производства на фермах [89].

Как известно в странах Европейского союза хорошо развиты направления, связанные с источниками генерации возобновляемой энергии. В данной области предложены множества блокчейн-проектов. Наиболее интересный проект предложена компанией «Sonnen Group». Данная компания запустила в Германии новую виртуальную электростанцию (Virtual Power Plant, VPP), которая хранит любую избыточную энергию, рассматривающую как «отходы». VPP работает на блокчейне, и участники программы осуществляют платежи в цифровой валюте. VPP — представляет из себя сеть децентрализованных и распределённых энергоблоков, таких как ветряные электростанции, солнечные парки и системы хранения. VPP Sonnen в северо-восточной Германии использует блокчейн для поглощения избыточной энергии ветра путём зарядки батарей. Когда генерируется больше возобновляемой энергии, чем необходимо. «Sonnen» использует блокчейн приложение, созданное EW Origin, чтобы сопоставить прогнозируемый избыток энергии ветра с ёмкостью хранения VPP. Как только сетевой оператор сообщит об ожидаемой избыточной энергии, VPP Sonnen будет активно поглощать часть ее и использовать EW Chain для финансового расчёта. Решение использует стабильную монету EWDai в сети Ethereum [90].

Схожий проект предложили Французская энергетическая компания «ekWateur» и разработчик блокчейн-решений «Power Ledger». Компании запустили торговую платформу, которая позволяет отслеживать и сертифицировать продажи энергии из возобновляемых источников. Также торговая платформа позволяет клиентам компании «ekWateur» выбирать источник приобретаемой энергии, поскольку портфель активов компании объединяет проекты в ветряной, солнечной и гидроэнергетике. Таким образом, клиенты получают гарантию того, что они поддерживают конкретный выбранный проект в области альтернативной энергетики. Для отслеживания и сертификации сделок используется криптовалюта POWR token [91].

Блокчейн-технология также нашла применение в процессе контроля и оптимизации выбросов углекислого газа. Компания по добыче металла и нефти

«BHP» протестировала блокчейн в совместном эксперименте с японской судоходной компанией «NYK». Компания «GoodFuels», специализирующаяся на устойчивом биотопливе, представила свой продукт для эксперимента, а «BLOC», разработчик блочных приложений для морской промышленности, создал децентрализованную экосистему для его отслеживания. В ходе испытания биотопливо «GoodFuels» было доставлено на сухогруз «Frontier Sky», а экономия углекислого газа была подтверждена с помощью блокчейн-платформы контроля качества топлива. Устойчивое биотопливо, используемое в эксперименте, служит альтернативой традиционному морскому газойлю на основе ископаемого топлива [92].

В Китае «EBL» продемонстрировала платформу для оптимизации процессов учёта углеродных активов на основе технологии блокчейн. Так как в Китае ограничен объем углеродных выбросов, поэтому крупные неэкологичные компании покупают квоты на выбросы у других фирм. Результаты тестирования платформы показали значительное сокращение цикла освоения квот и снижение стоимости работы с углеродными активами на 20-30% [93].

2.4. Безопасность и приватность

В России некоторые учёные начали анализировать потенциал применения блокчейн технологии при обеспечении информационной безопасности (ИБ). До сих пор отечественные производители ИБ решений не анонсировали какие-либо продукты, в которых использовалась бы блокчейн-технология. Отечественными учёными предложены лишь теоретические работы, но данные работы пока что не нашли практического применения [94-96]. В отличии от России Азербайджанская Республика преуспела в данном направлении. ЦБ Азербайджанской Республики в 2020 г. запустил цифровую систему идентификации под названием «BankID», которая позволит гражданам и юридическим лицам страны безопасно пользоваться онлайн-услугами банков. Система работает на основе блокчейна, созданной компанией «IBM» с использованием Hyperledger Fabric. Система построена на базе программно-определяемой и виртуализируемой инфраструктуры и работает по принципу «знай своего клиента». Она позволяет банкам проверять, действительно ли клиент является тем, за кого себя выдаёт, соблюдает ли он действующие законы. Благодаря данному решению граждане Азербайджана могут управлять своими цифровыми удостоверениями в онлайн-режиме. Это позволяет повысить точность данных и минимизирует возможные риски мошенничества [97].

В 2020 г. были опубликованы итоги пилотного проекта по применению блокчейна для оказания экстренной помощи в польском городе Ольштын. В рамках пилота пожарные, сотрудники скорой помощи и полицейские в экстренных ситуациях благодаря смарт-ключам могли беспрепятственно попадать в защищённые объекты или дома, не дожидаясь разрешения владельцев здания. Проект реализован с применением трёх решений: блокчейн-платформы Ethereum, электронного ключа Teltonika и коннектора SmartKey [98].

3. Проблемы и недостатки блокчейн-технологии

К сожалению, как и любая другая технология, БТ имеет свои преимущества так и недостатки. В данном разделе рассмотрены типовые и специфические проблемы БТ.

3.1. Типовые проблемы блокчейн-технологии

3.1.1. Уязвимость «51%»

Взаимное доверие в блокчейн-сетях достигается благодаря алгоритму консенсуса. Однако алгоритмы консенсуса имеют уязвимость «51%», которая может быть эксплуатирована нарушителями с целью захвата контроля над всей блокчейн-сетью. Рассмотрим пример эксплуатации данной уязвимости в блокчейн-сетях, в которых используется протокол PoW. Эксплуатация уязвимости «51%» возможна тогда, когда мощность одного майнера составляет более 50% от общей мощности всей блокчейн-сети. Если рассматривать блокчейн-сети на основе PoS, то эксплуатация уязвимости доступна при условии владения более 50% крипто-токенов от общего количества крипто-токенов. Благодаря данной уязвимости нарушителю доступно следующее [99]:

- двойные траты;
- менять порядок очерёдности транзакций;
- препятствовать майнингу крипто-токенов;
- вторгаться в процесс подтверждения транзакций.

3.1.2. Двойные траты

В блокчейн-сетях существует возможность эксплуатации уязвимости, связанной с двойной тратой крипто-активов [100]. Двойные траты означают, что пользователь использует один и тот же крипто-токен несколько раз для совершения транзакций. Данная уязвимость легко эксплуатируема в блокчейн-сетях на основе протокола PoW, поскольку нарушитель для осуществления атаки может использовать промежуточное время между процессами инициации и подтверждения двух транзакций. Вследствие этого нарушителю удаётся отправить вторую транзакцию перед получением результата по первой транзакции, что приводит к двойным тратам.

3.1.3. Безопасность закрытых ключей

Как ранее упоминалось у пользователей блокчейн-сети есть пара ключей (открытый и закрытый), в свою очередь закрытый ключ выступает в качестве «удостоверения личности», так как с помощью закрытого ключа пользователь может получить доступ к свои активам. Генерация и обеспечение безопасности закрытого ключа полностью возложена на пользователя. Часто пользователи для генерации пары ключей используют различные крипто-кошельки. Группа исследователей обнаружили уязвимость в схеме ECDSA которая используется при генерации пары ключей. Данная уязвимость позволяет нарушителю восстановить закрытый ключ пользователя, поскольку ECDSA не генерирует до-

статочно качественную псевдослучайную последовательность [101]. Спустя некоторое время в 2019 г. чешскими учёными были обнаружены новые уязвимости в различных реализациях алгоритма создания цифровой подписи. Их эксплуатация позволяет нарушителям восстановить значение закрытого ключа на основе анализа утечек сведений об отдельных битах, всплывающих при применении методов анализа по сторонним каналам [102].

Следует отметить, что при потере закрытого ключа его восстановление не представляется возможным. Также возможны сценарии, когда закрытый ключ пользователя украден нарушителями или скомпрометирован.

3.1.4. Анонимность транзакций

В большинстве блокчейн-сетей существует возможность прослеживания поведения пользователей. Нарушитель на основе данных о транзакциях может прийти к выводу о том, что все поступления крипто-активов получает один и тот же пользователь. Например, в блокчейн-сети Monero реализован механизм защиты *Mixins* (*чеканные монеты*), чтобы нарушитель не смог сделать выводы о связи крипто-активов с пользователем.

К сожалению, предпринимаемые разработчиками меры безопасности не надёжны. В работе [103] приводятся результаты исследования механизма Mixins. Результаты исследования показывают, что около 66% всех транзакций не содержат никаких чеканных монет, что приводит к утечке конфиденциальной информации об отправителе.

За короткое время стоимость некоторых видов криптовалют выросла в несколько раз, тем самым привлекла внимание людей ранее не связанных с криптовалютами. Большинство людей в целях быстрого заработка денежных средств покупают крипто-активы и ждут подходящего момента (повышения стоимости) для их продажи. Самый лёгкий способ покупки крипто-активов предлагают крипто-биржи. Практически во всех крипто-биржах для покупки крипто-активов прежде всего необходимо пройти процесс идентификации. Для успешного прохождения процесса идентификации пользователю необходимо предоставить скан-копию документа, удостоверяющего личность (паспорт, водительское удостоверение и т. д.) и «селфи» с данным документом. Сей факт даёт возможность крипто-биржам прослеживать дальнейшие транзакции пользователя. Также необходимо отметить, что перемещение денежных средств с одного адреса на другой несёт дополнительные комиссионные затраты и не каждый пользователь готов понести расходы во благо обеспечения анонимности. Помимо этого, появляются дополнительные риски компрометации персональных данных со стороны крипто-бирж.

3.1.5. Криминальная деятельность

В любых блокчейн-сетях пользователь при желании может генерировать несколько адресов для хранения и проведения различных транзакций. Таким образом крипто-активы могут быть использованы в незаконной деятельности. Например, через сторонние торговые платформы, пользователи могут покупать или продавать любые товары. Зачастую таким способом осуществляются сдел-

ки, противоречащие законодательству (работорговля, покупка военной амуниции и т. д.). Такое поведение пользователей трудно отследить, не говоря уже о том, чтобы подвергать их законным санкциям. Далее рассмотрим сценарии использования биткоина в преступных целях:

1. Вымогательство. Часто нарушители используют различные вредоносные программы с целью вымогательства денежных средств и в качестве валюты используют биткоин. В 2017 г. программа-вымогатель WannaCry (также известная как WannaCrypt) [104] за два дня заразила около 230 000 жертв в 150 странах мира. Она использовала уязвимость в системе Windows для распространения вредоносного ПО и шифровала файлы пользователей с целью дальнейшего получения выкупа в биткоинах.

2. Подпольный рынок. Часто биткоин используется в качестве валюты на различных торговых платформах. Например, в сети Tor можно воспользоваться онлайн платформой «Silk Road» на которой можно приобрести различные товары/услуги начиная с наркотических средств и заканчивая заказными убийствами [105].

3. Отмывание денег. Некоторые исследователи утверждают, что использовать биткоин в целях отмывания денег не имеет смысла, но другие предлагают готовые решения для осуществления отмывания денег. Например, исследователи предложили решение «DarkWallet», которое может провести операцию полностью в незаметном и конфиденциальном режиме [106]. Данное решение шифрует информацию о транзакции и смешивает действительные токены пользователя с чеканными монетами, вследствие значительно облегчается процесс отмывания денег.

3.2. Специфические проблемы блокчейн-технологии

3.2.1. Уязвимости в смарт-контрактах

Смарт-контракты, выполняемые в блокчейн-сетях, могут иметь уязвимости, которые возникают при некачественном написании кода. В работе [107] рассмотрены типичные уязвимости, возникающие при написании смарт-контрактов. Также проделаны работы по созданию инструментов, которые направлены на поиск 4 видов потенциальных ошибок в смарт-контрактах [108]. Данным инструментом исследователи проанализировали 19366 смарт-контрактов в сети Ethereum. В результате проверки обнаружилось, что 8833 из них являются уязвимыми.

3.2.2. Неоптимизированные смарт-контракты

При взаимодействии пользователя со смарт-контрактами в блокчейн-сети Ethereum взимается определённое количество «газа» (*gas*).

Газ – это деноминированная единица в сети Ethereum, служащая для оплаты транзакций.

К сожалению, многие смарт-контракты не оптимизированы должным образом. В работе [109] авторы классифицировали проблемы, связанные с избыточными тратами газа. Также исследователи разработали решение «Gasper», которое в автоматическом режиме может обнаружить некоторые классы про-

блем: мёртвый код (dead code), скрытый предикат (opaque predicate), дорогостоящие операции в цикле (expensive operations in a loop).

4. Перспективы развития блокчейн-технологии

На основе блокчейн-проектов рассмотренных в разделе 2, можно обозначить направления, в которых наблюдается активное применение БТ. На (рис. 5) приведены области использования блокчейн-технологии. В России активное использование БТ наблюдается всего лишь в трёх областях (выделены оранжевым цветом). А в странах ЕС, США и Китае БТ нашла более широкое применение в отличие от России (выделены жёлтым цветом).

Рис. 5. Области применения блокчейн-технологии

Как упоминалось ранее, работы отечественных учёных направленных на разработку ИБ-решений с применением БТ носят теоретический характер, поэтому данное направление развито слабо в отличие от других (выделено красным цветом).

Использование БТ в ИБ-проектах может положить начало к появлению совершенно новых решений. Например, благодаря свойству децентрализации можно реализовать замену для классической системы доменных имён, тем самым стали бы существенно затруднены реализации атак типа «отказ в обслуживании» (DDoS-атаки). Также БТ можно использовать в задачах хранения ключевой информации. Ключевой информацией могут являться секретные ключи для административного доступа, пароли, кодовые слова, секрет и т. д. [110].

Помимо разработки новых ИБ-решений с применением БТ можно выделить дополнительные направления исследовательских работ в этой области.

1) На сегодняшний день наиболее популярным протоколом консенсуса, является PoW. Однако для работы данного протокола требуются большие вычислительные ресурсы. Для решения данной проблемы разработчики Ethereum пытаются реализовать гибридный протокол консенсуса на основе PoW и PoS. Разработка более эффективных протоколов консенсуса может вывести БТ на новый уровень.

2) Смарт-контракты активно применяются в различных распределённых приложениях. К сожалению, смарт-контракты обладают недостатками, которые могут привести нарушению неприкосновенности частной жизни.

3) В блокчейн-сетях хранится большое количество данных (транзакции, байт-код смарт-контрактов и т. д.). Однако не все данные, хранящиеся в сети, являются действительными. Существует множество смарт-контрактов, не содержащих исполняемого кода или полностью идентичных. Также многие смарт-контракты никогда не выполняются после развёртывания. Поэтому необходимы эффективные инструменты для обнаружения и очистки данных видов смарт-контрактов.

Заключение

Представлен обобщённый обзор современного состояния развития блокчейн-технологии. Проведён сравнительный анализ публичных и закрытых блокчейн-сетей, а также 3-х типов протоколов достижения консенсуса. Также рассмотрены успешные отечественные блокчейн-проекты и выявлены сферы, в которых данная технология пользуется спросом. Помимо этого, определены основные проблемы и недостатки данной технологии и предложены новые направления для проведения исследовательских работ, связанных с обеспечением безопасности блокчейн-технологии.

Результаты исследования могут быть полезны для начинающих исследователей, выбравших блокчейн-технологию областью своих интересов.

Литература

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system // Bitcoin.org [Электронный ресурс]. 2008. – URL: https://bitcoin.org/bitcoin.pdf (дата обращения 11.01.2021).

2. Xu D., Xu L., Li L. Industry 4.0: state of the art and future trends // International Journal of Production Research. 2018. Vol. 56. № 8. pp. 2941-2962.

3. Collins R. Blockchain: a new architecture for digital content // EContent. 2016. Vol. 39. № 8. pp. 22-23.

4. Chung M., Kim J. The internet information and technology research directions based on the fourth industrial revolution // KSII Transactions on Internet and Information Systems. 2016. Vol. 10. № 3. pp. 1311-1320. doi: 10.3837/tiis.2016.03.020.

5. Underwood S. Blockchain beyond bitcoin // Community ACM. 2016. Vol. 59. № 11. pp. 15-17. doi: 10.1145/2994581.

6. Buterin V. Ethereum white paper // Ethereum.org [Электронный ресурс]. 2013. – URL: https://ethereum.org/en/whitepaper (дата обращения 11.01.2021).

7. Hileman G., Rauchs M. Global cryptocurrency benchmarking study // Cambridge Centre for Alternative Finance. 2017. № 33. pp. 33-113.

8. Haferkorn M., Diaz M. Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin // Enterprise Applications and Services in the Finance Industry. 2014. № 1. pp. 106-120.

9. Schwartz D., Youngs N., Britto A. The Ripple Protocol Consensus Algorithm, Ripple Labs Inc White Paper // Ripple Labs Inc [Электронный ресурс]. 2018. – URL: https://ripple.com/files/ripple_consensus_whitepaper.pdf (дата обращения 11.01.2021).

10. Часовских В. П., Лабунец В. Г., Воронов М. П. Технология «блокчейн» (blockchain) в образовании вузов и цифровой экономике // Эко-потенциал 2017. Т. 2. № 18. С. 99-105.

11. Sharples M., Domingue J. A distributed system for educational record, reputation and reward // Adaptive and Adaptable Learning. 2016. pp. 490-496. doi: 10.1007/978-3-319-45153-4_48.

12. Skiba J. The potential of blockchain in education and health care // Nursing education perspectives. 2017. Vol. 38. № 4. pp. 220-221. doi: 10.1097/01.nep.0000000000000190.

13. Hoy B. An introduction to the blockchain and its implications for libraries and medicine // Medical reference services quarterly. 2017. Vol. 36. №. 3. pp. 273–279. doi: 10.108 0/02763869.2017.1332261.

14. Khan A., Salah K. IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems. 2018. Vol. 82. pp. 395-411.

15. Reyna A., Martín C., Chen J., Soler E., Díaz M. On blockchain and its integration with IoT. Challenges and opportunities // Future generation computer systems. 2018. Vol. 88. pp. 173-190.

16. Panarello A., Tapas N., Merlino G., Longo F., Puliafito A. Blockchain and IoT integration: A systematic survey // Sensors. 2018. Vol. 18. № 8. pp. 2575.

17. Дорожная карта развития «сквозной» цифровой технологии «Системы распределённого реестра» от 10 октября 2019 // Официальный интернет-портал Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. 2019. – URL: https://digital.gov.ru/uploaded/files/07102019srr.pdf (дата обращения 11.01.2021).

18. Miraz H., Ali M. Applications of blockchain technology beyond cryptocurrency // Annals of Emerging Technologies in Computing (AETiC). 2018. Vol. 2. № 1. pp. 20-26.

19. Liu Z., Luong C., Wang W., Niyato D., Wang P., Liang YC., Kim DI. A survey on blockchain: A game theoretical perspective // IEEE Access. 2019. Vol. 7. pp. 47615-47643.

20. Conti M., Kumar S., Lal C., Ruj S. A survey on security and privacy issues of bitcoin // IEEE Communications Surveys & Tutorials. 2018. Vol. 20. № 4. pp. 3416-3452.

21. Khalilov M., Levi A. A survey on anonymity and privacy in bitcoin-like digital cash systems // IEEE Communications Surveys & Tutorials. 2018. Vol. 20. № 3. pp. 2543-2585.

22. Zheng Z., Xie S., Dai N., Chen X., Wang H. Blockchain challenges and opportunities: Survey // International Journal of Web and Grid Services. 2018. Vol. 14. № 4. pp. 352-375.

23. Lao L., Li Z., Hou S., Xiao B., Guo S., Yang Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling // ACM Computing Surveys (CSUR). 2020. Vol. 53. № 1. pp. 1-32.

24. Butun I., Osterberg P., Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures // IEEE Communications Surveys & Tutorials. 2019. Vol. 22. № 1. pp. 616-644.

25. Ferrag A., Shu L., Yang X., Derhab A., Maglaras L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges // IEEE access. 2020. Vol. 8. pp. 32031-32053.

26. Трегубов В. Н. Реализация автономной логистики на основе технологий интернета вещей и блокчейн // Современные информационные технологии и ИТ-образование. 2019. № 3. URL: https://cyberleninka.ru/article/n/realizatsiya-avtonomnoy-logistiki-na-osnove-tehnologiy-interneta-veschey-i-blokcheyn (дата обращения: 13.03.2021).

27. Перекальский И. Н., Кокин С. Е. Применение технологий распределённого реестра (blockchain) в электроэнергетических системах // Вестник Южно-Уральского государственного университета. Серия: Энергетика. 2020. № 1. URL: https://cyberleninka.ru/article/n/primenenie-tehnologiy-raspredelennogo-reestra-blockchain-v-elektroenergeticheskih-sistemah (дата обращения: 13.03.2021).

28. Salah K., Rehman MH., Nizamuddin N., Al-Fuqaha A. Blockchain for AI: Review and open research challenges // IEEE Access. 2019. vol. 7. pp. 10127-10149.

29. Dinh N., Thai T. AI and blockchain: A disruptive integration // Computer. 2018. Vol. 51. № 9. pp. 48-53.

30. Karafiloski E., Mishev A. Blockchain solutions for big data challenges: A literature review // IEEE EUROCON 2017-17th International Conference on Smart Technologies. 2017. pp. 763-768.

31. Hassani H., Huang X., Silva E. Big-crypto: Big data, blockchain and cryptocurrency // Big Data and Cognitive Computing. 2018. Vol. 2. № 4. pp. 34.

32. Nofer M., Gomber P., Hinz O., Schiereck D. Blockchain // Business & Information Systems Engineering. 2017. Vol. 59. № 3. pp. 183-187.

33. Merkle C. A certified digital signature // Conference on the Theory and Application of Cryptology. 1989. pp. 218-238.

34. Johnson D., Menezes A., Vanstone S. The elliptic curve digital signature algorithm (ECDSA) // International journal of information security. 2001. Vol. 1. № 1. pp. 36-63.

35. Niranjanamurthy M., Nithya N., Jagannatha S. Analysis of Blockchain technology: pros, cons and SWOT // Cluster Computing. 2019. Vol. 22. № 6. pp. 14743-14757.

36. Scherer M. Performance and scalability of blockchain networks and smart contracts // Umea University. 2017. pp. 1-41.

37. Castro M., Liskov B. Practical Byzantine fault tolerance and proactive recovery // ACM Transactions on Computer Systems (TOCS). 2002. Vol. 20. № 4. pp. 398-461.

38. Lin C., Liao C. A survey of blockchain security issues and challenges // IJ Network Security. 2017. Vol. 19. № 5. pp. 653-659.

39. Zamyatin A., Stifter N., Judmayer A., Schindler P., Weippl E., Knottenbelt J. A wild velvet fork appears! inclusive blockchain protocol changes in practice // International Conference on Financial Cryptography and Data Security. 2018. pp. 31-42.

40. Puddu I., Dmitrienko A., Capkun S. μchain: How to forget without hard forks // IACR Cryptology [Электронный ресурс]. 2017. – URL: https://eprint.iacr.org/2017/106.pdf (дата обращения 12.02.2021).

41. King S. Primecoin: Cryptocurrency with Prime Number Proof-of-Work // PS University [Электронный ресурс]. 2013. – URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.694.5890&rep=rep1&type=pdf (дата обращения 14.02.2021).

42. Vasin P. Blackcoin's Proof-of-Stake Protocol v2 // Whitepaper.io [Электронный ресурс]. 2018. – URL: https://whitepaper.io/document/327/blackcoin-whitepaper (дата обращения 20.01.2021).

43. King S., Nadal S. Peercoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake // Self- Published Paper. 2012.

44. Buterin V., Griffith V. Casper the friendly finality gadget // Cornell University [Электронный ресурс]. 2017. – URL: https://arxiv.org/abs/1710.09437 (дата обращения 09.01.2021).

45. NXT. Nxt Whitepaper // Nxt community [Электронный ресурс]. 2016. – URL: https://nxtdocs.jelurida.com/Nxt_Whitepaper (дата обращения 14.01.2021).

46. Yang F., Zhou W., Wu Q., Long R., Xiong N., Zhou M. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism // IEEE Access. 2019. Vol. 7. pp. 118541-118555.

47. Ozisik P., Andresen G., Bissias G., Houmansadr A., Levine B. Graphene: A new protocol for block propagation using set reconciliation // In Data Privacy Management, Cryptocurrencies and Blockchain Technology. 2017. pp. 420-428.

48. Schuh F., Larimer D. Bitshares 2.0: general overview // Cryptonomex.com [Электронный ресурс]. 2017. – URL: https://pdfs.semanticscholar.org/c5c6/eefc414d32637890dbe40a1440e46f68e10f.pdf (дата обращения 13.02.2021).

49. Skriabin B. Описание работы Delegated Proof-of-stake // Distributed Lab [Электронный ресурс]. 2017. – URL: https://distributedlab.com/blog/ru/description-of-delegated-proof-of-stake (дата обращения18.01.2021).

50. Hyperledger. Hyperledger Project // Linux Foundation [Электронный ресурс]. 2015. – URL: https://www.hyperledger.org/ (дата обращения 18.01.2021).

51. Sukhwani H., Martínez M., Chang X., Trivedi S., Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network

(hyperledger fabric) // IEEE 36th Symposium on Reliable Distributed Systems (SRDS). 2017. pp. 253-255.

52. Gao S., Yu T., Zhu J., Cai W. T-PBFT: An Eigen Trust-based practical Byzantine fault tolerance consensus algorithm // China Communications. 2019. Vol. 16. № 12. pp. 111-123.

53. Wang Q., Yu J., Peng Z., Bui C., Chen S., Ding Y., Xiang Y. Security Analysis on dBFT protocol of NEO // International Conference on Financial Cryptography and Data Security. 2020. pp. 20-31.

54. Mazieres D. The stellar consensus protocol: A federated model for internet-level consensus // Stellar Development Foundation [Электронный ресурс]. 2015. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.93&amp=&rep=rep1&amp=&type=pdf (дата обращения 25.02.2021).

55. Chase B., MacBrough E. Analysis of the XRP ledger consensus protocol // Cornell University [Электронный ресурс]. 2018. – URL: https://arxiv.org/abs/1802.07242 (дата обращения 11.02.2021).

56. Eyal I., Gencer E., Sirer G., Van Renesse R. Bitcoin-ng: A scalable blockchain protocol // 13th USENIX symposium on networked systems design and implementation (NSDI'16). 2016. pp. 45-59.

57. Kogias K., Jovanovic P., Gailly N., Khoffi I., Gasser L., Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing // 25th USENIX security symposium (USENIX security'16). 2016. pp. 279-296.

58. Kwon J. Tendermint: Consensus without mining // GitHub [Электронный ресурс]. 2014. – URL: https://github.com/tendermint/tendermint/wiki (дата обращения 18.01.2021).

59. Grigg I. Eos-an introduction // White paper [Электронный ресурс]. 2017. – URL: https://whitepaperdatabase.com/eos-whitepaper (дата обращения 15.02.2021).

60. Schuh F., Larimer D. Bitshares 2.0: Financial smart contract platform // WeuseCoins.com [Электронный ресурс]. 2015. – URL: www.weusecoins.com/assets/pdf/library/Bitshares%20Financial%20Platform.pdf (дата обращения 24.02.2021).

61. Crypto.org Chain. The next generation public Blockchain // Crypto.org [Электронный ресурс]. 2017. – URL: https://crypto.org/docs/chain-details/introduction.html#design-goals (дата обращения 15.01.2021).

62. Zbierski M. Parallel byzantine fault tolerance // Soft Computing in Computer and Information Science. 2015. pp. 321-333.

63. Zhao W. Optimistic byzantine fault tolerance // International Journal of Parallel, Emergent and Distributed Systems. 2016. Vol. 31. № 3. pp. 254–267.

64. Lokhava M., Losa G., Mazières D., Hoare G., Barry N., Gafni E., Jove J., Malinowsky R., McCaleb J. Fast and secure global payments with stellar // Proceedings of the 27th ACM Symposium on Operating Systems Principles. 2019. pp. 80-96.

65. Durov P. Telegram open network platform (TON) // Telegram Open Network [Электронный ресурс]. 2020. – URL: https://ton-telegram.net (дата обращения 01.03.2021).

66. García-Pérez Á., Schett A. Deconstructing Stellar Consensus (Extended Version) // Cornell University [Электронный ресурс]. 2019. – URL: https://arxiv.org/pdf/1911.05145.pdf (дата обращения 01.03.2021).

67. Armknecht F., Karame O., Mandal A., Youssef F., Zenner E. Ripple: Overview and outlook // International Conference on Trust and Trustworthy Computing. 2015. pp. 163-180.

68. Park S., Pietrzak K., Kwon A., Alwen J., Fuchsbauer G., Gazi P. Spacemint: A cryptocurrency based on proofs of space // IACR Cryptology. 2015. pp. 528.

69. Bentov I., Lee C., Mizrahi A., Rosenfeld M. Proof of activity: Extending bitcoin's proof of work via proof of stake // ACM SIGMETRICS Performance Evaluation Review. 2014. Vol. 42. № 3. pp. 34-37.

70. De Angelis S., Aniello L., Baldoni R., Lombardi F., Margheri A., Sassone V. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain // University of Southampton [Электронный ресурс]. 2018. – URL: https://eprints.soton.ac.uk/415083/2/itasec18_main.pdf (дата обращения 19.02.2021).

71. Szabo N. Formalizing and securing relationships on public networks // First Monday. 1997. vol. 2. № 9. DOI: 10.5210/fm.v2i9.548.

72. М.Видео, Сбербанк Факторинг и Альфа-Банк создали первый в России коммерческий блокчейн-консорциум // Альфа-Банк пресс-центр [Электронный ресурс]. 2017. – URL: https://alfabank.ru/press/news/2017/10/13/41066.html (дата обращения 25.03.2021).

73. «МегаФон» НРД и Райффайзенбанк осуществили первую сделку по размещению рублёвых облигаций на блокчейне // Официальный сайт ПАО «Мегафон» [Электронный ресурс]. 2017. – URL: https://corp.megafon.ru/press/news/federalnye_novosti/20171002-0934.html (дата обращения 25.02.2021).

74. Gazprom Neft and S7 Airlines become the first companies in Russia to move to blockchain technology in aviation refuelling // Official site of «Gazprom» [Электронный ресурс]. 2018. – URL: https://www.gazprom-neft.com/press-center/news/gazprom-neft-and-s7-airlines-become-the-first-companies-in-russia-to-move-to-blockchain-technology-i/ (дата обращения 25.02.2021).

75. АО «Первоуральскбанк» провёл первый полный цикл финансирования через блокчейн-платформу // Официальный сайт АО «Первоуральскбанк» [Электронный ресурс]. 2019. – URL: https://www.pervbank.ru/news/725/ (дата обращения 25.02.2021).

76. LG тестирует платформу цифровых платежей на основе ИИ и блокчейна // BitNovosti [Электронный ресурс]. 2020. – URL: https://bitnovosti.com/2020/04/25/lg-testiruet-platformu-tsifrovyh-platezhej-na-osnove-ii-i-blokchejna/ (дата обращения 25.02.2021).

77. Граин В. DBS Bank внедрит блокчейн Contour для расчётов по аккредитивам // Bits.media [Электронный ресурс]. 2020. – URL: https://bits.media/dbs-bank-vnedrit-blokcheyn-contour-dlya-raschetov-po-akkreditivam/ (дата обращения 25.02.2021).

78. China Telecom внедряет блокчейн в системы 5G // Bits.media [Электронный ресурс]. 2020. – URL: https://bits.media/china-telecom-vnedryaet-blokcheyn-v-sistemy-5g/ (дата обращения 25.02.2021).

79. Даниил Егоров представил сервис для быстрого подтверждения льготных кредитов бизнесу на видео совещании с Президентом России // Официальный сайт ФНС России [Электронный ресурс]. 2020. – URL: https://www.nalog.ru/rn77/news/activities_fts/9744281/ (дата обращения 25.02.2021).

80. Paillisse J., Ferriol M., Garcia E., Latif H., Piris C., Lopez A., Kuerbis B., Rodriguez-Natal A., Ermagan V., Maino F., Cabellos A. IPchain: Securing IP prefix allocation and delegation with blockchain // 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2018. pp. 1236-1243.

81. Российский суд впервые использовал платформу блокчейн в делопроизводстве // TASS.RU [Электронный ресурс]. 2018. – URL: https://tass.ru/obschestvo/5865776 (дата обращения 25.02.2021).

82. Polys - система цифрового голосования // Kaspersky [Электронный ресурс]. 2020. – URL: kaspersky.ru/ihub/assets/POLYS.KASP.RUS_leaflet.pdf (дата обращения 25.02.2021).

83. Степанов Д. В России впервые выдали цифровые дипломы на блокчейне // CNews.ru [Электронный ресурс]. 2020. – URL: https://cnews.ru/news/top/2020-02-25_rossijskij_vuz_vpervye_vydast (дата обращения 25.02.2021).

84. Erazo F. South Korean telecom launches blockchain wallet for official documents // CoinTelegraph [Электронный ресурс]. 2020. – URL: https://cointelegraph.com/news/south-korean-telecom-launches-blockchain-wallet-for-official-documents (дата обращения 25.02.2021).

85. U.S. Treasury unveils blockchain grant project // Ledger Insights [Электронный ресурс]. 2020. – URL: https://www.ledgerinsights.com/us-treasury-unveils-blockchain-grant-project/ (дата обращения 25.02.2021).

86. Блокчейн массового поражения. Как криптомир победит эпидемию // РБК [Электронный ресурс]. 2020. – URL: https://www.rbc.ru/crypto/news/5e9ab5a69a79475e1af088ae?from=main (дата обращения 25.02.2021).

87. В борьбе с незаконным оборотом полимерных труб поможет блокчейн // Группа полипластик [Электронный ресурс]. 2019. – URL: https://www.polyplastic.ru/press/news/2019/05/27/item17663 (дата обращения 25.02.2021).

88. «Россети» запускают пилотный блокчейн-проект по биллингу на Урале // РБК+ [Электронный ресурс]. 2019. – URL:

https://ekb.rbc.ru/ekb/freenews/5df772cc9a794781fbf5e65a (дата обращения 25.02.2021).

89. FoodTech: как накормить людей с помощью цифровых технологий // iFarm [Электронный ресурс]. 2020. – URL: https://ifarmproject.ru/kostenko (дата обращения 25.02.2021).

90. Seven S., Yao G., Soran A., Onen A., Muyeen SM. Peer-to-Peer Energy Trading in Virtual Power Plant Based on Blockchain Smart Contracts // IEEE Access. 2020. Vol. 8. pp. 175713-175726.

91. Kim G., Park J., Ryou J. A study on utilization of blockchain for electricity trading in microgrid // IEEE International Conference on Big Data and Smart Computing (BigComp). 2018. pp. 743-746.

92. Clott C., Hartman B., Beidler B. Sustainable blockchain technology in the maritime shipping industry // Maritime Supply Chains. 2020. pp. 207-228.

93. Teufel B., Sentic A., Barmet M. Blockchain energy: Blockchain in future energy systems // Journal of Electronic Science and Technology. 2019. Vol. 17. № 4. 100011 P.

94. Волошин И. П. Управление доступом на основе блокчейн // Информационная безопасность регионов. 2017. № 3-4 С. 28-29.

95. Филяк П. Ю., Постников М. К., Федоров С. Е. Применение технологий blockchain для разработки корпоративной информационной системы в защищённом исполнении // Информация и безопасность. 2020. Т. 23. № 3. С. 399-408.

96. Юмашева Е. В., Юмашев Д. В., Тимонов Д. А. Информационная безопасность в системах электронного документооборота с применением технологии блокчейн // Современные наукоёмкие технологии. 2021. № 1. С. 63-68.

97. Agbede O. Strong Electronic Identification: Survey & Scenario Planning // School of Electrical Engineering [Электронный ресурс]. 2018. – URL:https://aaltodoc.aalto.fi/bitstream/handle/123456789/34352/master_Agbede_Oluwabunmi_2018.pdf?sequence=1 (дата обращения 25.02.2021).

98. SmartCitiesWorld news team. Olsztyn claims world-first by linking blockchain to emergency services // SmartCitiesWorld [Электронный ресурс]. 2020. – URL: https://smartcitiesworld.net/news/news/olsztyn-claims-world-first-by-linking-blockchain-to-emergency-services--5900 (дата обращения 25.02.2021).

99. Dye C., Li G., Cai H., Gu Y., Fukuda A. Analysis of security in blockchain: Case study in 51%-attack detecting // 5th International Conference on Dependable Systems and Their Applications (DSA). IEEE Access. 2018. pp. 15-24.

100. Karame O., Androulaki E., Roeschlin M., Gervais A., Čapkun S. Misbehavior in bitcoin: A study of double-spending and accountability // ACM Transactions on Information and System Security (TISSEC). 2015. Vol. 18. №. 1. pp. 1-32.

101. Mayer H. ECDSA security in Bitcoin and Ethereum: a research survey // CoinFaabrik. 2016. Vol. 28. pp. 126-127.

102. Security Lab. Обнаружен способ восстановить ключи ECDSA // Security Lab by positive technologies. [Электронный ресурс]. 2019. – URL: https://www.securitylab.ru/news/501553.php (дата обращения 05.03.2021).

103. Miller A., Moser M., Lee K., Narayanan A. An empirical analysis of linkability in the monero blockchain // arXiv preprint arXiv:1704.04299. 2017.

104. Ehrenfeld M. Wannacry, cybersecurity and health information technology: A time to act // Journal of medical systems. 2017. Vol. 41. № 7. pp. 104-105.

105. Christin N. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace // Proceedings of the 22nd international conference on World Wide Web. 2013. pp. 213-224.

106. Courtois T., Mercer R. Stealth Address and Key Management Techniques in Blockchain Systems // ICISSP. 2017. pp. 559-566.

107. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on ethereum smart contracts (sok) // International conference on principles of security and trust. 2017. pp. 164-186.

108. Luu L., Chu H., Olickel H., Saxena P., Hobor A. Making smart contracts smarter // Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. pp. 254-269.

109. Chen T., Li X., Luo X., Zhang X. Under-optimized smart contracts devour your money // 24th International Conference on Software Analysis, Evolution and Reengineering. 2017. pp. 442–446.

110. Носиров З. А., Щербинина О. В. Анализ криптографических схем разделения секрета для резервного хранения ключевой информации // Прикаспийский журнал: управление и высокие технологии. 2019. № 2. С. 126-134.

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Bitcoin.org*, 2008. Available at: https://bitcoin.org/bitcoin.pdf (accessed 11 January 2021).

2. Xu D, Xu L, Li L. Industry 4.0: state of the art and future trends. *International Journal of Production Research*, 2018, vol. 56, no. 8, pp. 2941-2962.

3. Collins R. Blockchain: a new architecture for digital content. *EContent*, 2016, vol. 39, no. 8, pp. 22–23.

4. Chung M., Kim J. The internet information and technology research directions based on the fourth industrial revolution. *KSII Transactions on Internet and Information Systems,* 2016, vol. 10, no. 3, pp. 1311-1320. doi: 10.3837/tiis.2016.03.020.

5. Underwood S. Blockchain beyond bitcoin. *Community ACM,* 2016, vol. 59, no. 11, pp. 15-17. doi: 10.1145/2994581.

6. Buterin V. Ethereum white paper. *Ethereum.org,* 2013. Available at: https://ethereum.org/en/whitepaper (accessed 11 January 2021).

7. Hileman G., Rauchs M. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance,* 2017, no. 33, pp. 33-113.

8. Haferkorn M, Diaz M. Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin. *Enterprise Applications and Services in the Finance Industry*, 2014, no. 1, pp. 106-120.

9. Schwartz D., Youngs N., Britto A. The Ripple Protocol Consensus Algorithm, Ripple Labs Inc White Paper. *Ripple Labs Inc*, 2018. Available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed 11 January 2021).

10. Chasovskih V. P., Labunec V. G., Voronov M. P. Tekhnologiya «blokchejn» (blockchain) v obrazovanii vuzov i cifrovoj ekonomike [Blockchain technology in university education and the digital economy]. *Eco-potential*, 2017, vol. 2, no. 18, pp. 99-105 (in Russian).

11. Sharples M., Domingue J. A distributed system for educational record, reputation and reward. *Adaptive and Adaptable Learning*, 2016, pp. 490-496. doi: 10.1007/978-3-319-45153-4_48.

12. Skiba J. The potential of blockchain in education and health care. *Nursing education perspectives*, 2017, vol. 38, no. 4, pp. 220-221. doi: 10.1097/01.nep.0000000000000190.

13. Hoy B. An introduction to the blockchain and its implications for libraries and medicine. *Medical reference services quarterly*, 2017, vol. 36, no. 3, pp. 273–279. doi: 10.108 0/02763869.2017.1332261.

14. Khan A., Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 2018, vol. 82, pp. 395-411.

15. Reyna A., Martín C., Chen J., Soler E., Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, 2018, vol. 88, pp. 173-190.

16. Panarello A., Tapas N., Merlino G., Longo F., Puliafito A. Blockchain and IoT integration: A systematic survey. *Sensors*, 2018, vol. 18, no. 8, pp. 2575.

17. Dorozhnaya karta razvitiya «skvoznoj» cifrovoj tekhnologii «Sistemy raspredelyonnogo reestra» ot 10 oktyabrya 2019 [Roadmap for the development of «end-to-end» digital technology «Distributed Register System» dated October 10, 2019]. *Official Internet portal of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation*, 2019. Available at: https://digital.gov.ru/uploaded/files/07102019srr.pdf (accessed 11 January 2021) (in Russian).

18. Miraz H., Ali M. Applications of blockchain technology beyond cryptocurrency. *Annals of Emerging Technologies in Computing (AETiC)*, 2018, vol. 2, no. 1, pp. 20-26.

19. Liu Z., Luong C., Wang W., Niyato D., Wang P., Liang YC., Kim DI. A survey on blockchain: A game theoretical perspective. *IEEE Access*, 2019, vol. 7, pp. 47615-47643.

20. Conti M., Kumar S., Lal C., Ruj S. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 4, pp. 3416-3452.

21. Khalilov C., Levi A. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 3, pp. 2543-2585.

22. Zheng Z., Xie S., Dai N., Chen X., Wang H. Blockchain challenges and opportunities: Survey. *International Journal of Web and Grid Services*, 2018, vol. 14, no. 4, pp. 352-375.

23. Lao L., Li Z., Hou S., Xiao B., Guo S., Yang Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Computing Surveys (CSUR)*, 2020, vol. 53, no. 1, pp. 1-32.

24. Butun I., Osterberg P., Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials,* 2019, vol. 22, no. 1, pp. 616-644.

25. Ferrag A., Shu L., Yang X., Derhab A., Maglaras L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE access*, 2020, vol. 8, pp. 32031-32053.

26. Tregubov V. N. Realizaciya avtonomnoj logistiki na osnove tekhnologij interneta veshchej i blokchejn [Implementation of autonomous logistics based on IoT and blockchain technologies]. *Modern information technology and IT education*, 2019. № 3. Available at: https://cyberleninka.ru/article/n/realizatsiya-avtonomnoy-logistiki-na-osnove-tehnologiy-interneta-veschey-i-blokcheyn (accessed 11 January 2021) (in Russian).

27. Perekal'skij I. N., Kokin S. E. Primenenie tekhnologij raspredelyonnogo reestra (blockchain) v elektroenergeticheskih sistemah [Application of blockchain technologies in electric power systems]. *Bulletin of the South Ural State University. Series: Energy*, 2020. № 1. Available at: https://cyberleninka.ru/article/n/primenenie-tehnologiy-raspredelennogo-reestra-blockchain-v-elektroenergeticheskih-sistemah (accessed 11 January 2021) (in Russian).

28. Salah K., Rehman MH., Nizamuddin N., Al-Fuqaha A. Blockchain for AI: Review and open research challenges. *IEEE Access*, 2019, vol. 7, pp. 10127-10149.

29. Dinh N., Thai T. AI and blockchain: A disruptive integration. *Computer*, 2018, vol. 51, no. 9, pp. 48-53.

30. Karafiloski E., Mishev A. Blockchain solutions for big data challenges: A literature review. *In IEEE EUROCON 2017-17th International Conference on Smart Technologies. IEEE Access,* 2017, pp. 763-768.

31. Hassani H., Huang X., Silva E. Big-crypto: Big data, blockchain and cryptocurrency. *Big Data and Cognitive Computing*, 2018, vol. 2, no. 4, pp. 34.

32. Nofer M., Gomber P., Hinz O., Schiereck D. Blockchain. *Business & Information Systems Engineering*, 2017, vol. 59, no. 3, pp. 183-187.

33. Merkle RC. A certified digital signature. *Conference on the Theory and Application of Cryptology*, 1989, pp. 218-238.

34. Johnson D., Menezes A., Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *International journal of information security,* 2001, vol. 1, no. 1, pp. 36-63.

35. Niranjanamurthy M., Nithya N., Jagannatha S. Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing,* 2019, vol. 22, no. 6, pp. 14743-14757.

36. Scherer M. Performance and scalability of blockchain networks and smart contracts. *Umea University*, 2017, pp. 1-41.

37. Castro M., Liskov B. Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS),* 2002, vol. 20, no. 4, pp. 398-461.

38. Lin C., Liao C. A survey of blockchain security issues and challenges // *IJ Network Security,* 2017, vol. 19, no. 5, pp. 653-659.

39. Zamyatin A., Stifter N., Judmayer A., Schindler P., Weippl E., Knottenbelt WJ. A wild velvet fork appears! inclusive blockchain protocol changes in practice. *International Conference on Financial Cryptography and Data Security*, 2018, pp. 31-42.

40. Puddu I., Dmitrienko A., Capkun S. μchain: How to forget without hard forks. *IACR Cryptology*, 2017. Available at: https://eprint.iacr.org/2017/106.pdf (accessed 11 January 2021).

41. King S. Primecoin: Cryptocurrency with Prime Number Proof-of-Work. *PS University*, 2013. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.694.5890&rep=rep1&type=pdf (accessed 11 January 2021).

42. Vasin P. Blackcoin's Proof-of-Stake Protocol v2. *Whitepaper.io*, 2018 Available at: https://whitepaper.io/document/327/blackcoin-whitepaper (accessed 11 January 2021).

43. King S., Nadal S. Peercoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. *Self- Published Paper*, 2012.

44. Buterin V., Griffith V. Casper the friendly finality gadget. *Cornell University*, 2017. Available at: https://arxiv.org/abs/1710.09437 (accessed 11 January 2021).

45. NXT. Nxt Whitepaper. *Nxt community*, 2016. Available at: https://nxtdocs.jelurida.com/Nxt_Whitepaper (accessed 11 January 2021).

46. Yang F., Zhou W., Wu Q., Long R., Xiong N., Zhou M. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 2019, vol. 7, pp. 118541-118555.

47. Ozisik P., Andresen G., Bissias G., Houmansadr A., Levine B. Graphene: A new protocol for block propagation using set reconciliation. *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 2017, pp. 420-428.

48. Schuh F., Larimer D. Bitshares 2.0: general overview. *Cryptonomex.com*, 2017. Available at: https://pdfs.semanticscholar.org/c5c6/eefc414d32637890dbe40a1440e46f68e10f.pdf (accessed 11 January 2021).

49. Skriabin B. Opisanie raboty Delegated Proof-of-stake [Job description Delegated Proof-of-stake]. *Distributed Lab*, 2017. Available at: https://distributedlab.com/blog/ru/description-of-delegated-proof-of-stake (accessed 11 January 2021) (in Russian).

50. Hyperledger. Hyperledger Project. *Linux Foundation*, 2015. Available at: https://www.hyperledger.org/ (accessed 11 January 2021).

51. Sukhwani H., Martínez M., Chang X., Trivedi S., Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). *IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, 2017, pp. 253-255.

52. Gao S., Yu T., Zhu J., Cai W. T-PBFT: An Eigen Trust-based practical Byzantine fault tolerance consensus algorithm. *China Communications*, 2019, vol. 16, no. 12, pp. 111-123.

53. Wang Q., Yu J., Peng Z., Bui C., Chen S., Ding Y., Xiang Y. Security Analysis on dBFT protocol of NEO. *International Conference on Financial Cryptography and Data Security*, 2020, pp. 20-31.

54. Mazieres D. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.93&amp=&rep=rep1&amp=&type=pdf (accessed 11 January 2021).

55. Chase B., Macbrough E. Analysis of the XRP ledger consensus protocol. *Cornell University*, 2018. Available at: https://arxiv.org/abs/1802.07242 (accessed 11 January 2021).

56. Eyal I., Gencer AE., Sirer EG., Van Renesse R. Bitcoin-ng: A scalable blockchain protocol. *13th USENIX symposium on networked systems design and implementation (NSDI'16),* 2016, pp. 45-59.

57. Kogias K., Jovanovic P., Gailly N., Khoffi I., Gasser L., Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing. *25th USENIX security symposium (USENIX security'16),* 2016, pp. 279-296.

58. Kwon J. Tendermint: Consensus without mining. *GitHub,* 2014. Available at: https://github.com/tendermint/tendermint/wiki (accessed 11 January 2021).

59. Grigg I. Eos-an introduction. *White paper,* 2017. Available at: https://whitepaperdatabase.com/eos-whitepaper (accessed 11 January 2021).

60. Schuh F., Larimer D. Bitshares 2.0: Financial smart contract platform. *WeuseCoins.com,* 2015. Available at: www.weusecoins.com/assets/pdf/library/Bitshares%20Financial%20Platform.pdf (accessed 11 January 2021).

61. Crypto.org Chain. The next generation public Blockchain. *Crypto.org*, 2017. Available at: https://crypto.org/docs/chain-details/introduction.html#design-goals (accessed 11 January 2021).

62. Zbierski M. Parallel byzantine fault tolerance. *Soft Computing in Computer and Information Science*, 2015, pp. 321-333.

63. Zhao W. Optimistic byzantine fault tolerance. *International Journal of Parallel, Emergent and Distributed Systems*, 2016, vol. 31, no. 3, pp. 254–267.

64. Lokhava M., Losa G., Mazières D., Hoare G., Barry N., Gafni E., Jove J., Malinowsky R., McCaleb J. Fast and secure global payments with stellar. *In Proceedings of the 27th ACM Symposium on Operating Systems Principles*, 2019, pp. 80-96.

65. Durov P. Telegram open network platform (TON). *Telegram Open Network*, 2020. Available at: https://ton-telegram.net (accessed 11 January 2021).

66. García-Pérez Á., Schett MA. Deconstructing Stellar Consensus (Extended Version). *Cornell University*, 2019. Available at: https://arxiv.org/pdf/1911.05145.pdf (accessed 11 January 2021).

67. Armknecht F., Karame GO., Mandal A., Youssef F., Zenner E. Ripple: Overview and outlook. *International Conference on Trust and Trustworthy Computing*, 2015, pp. 163-180.

68. Park S., Pietrzak K., Kwon A., Alwen J., Fuchsbauer G., Gazi P. Spacemint: A cryptocurrency based on proofs of space. *IACR Cryptology,* 2015, 528 p.

69. Bentov I., Lee C., Mizrahi A., Rosenfeld M. Proof of activity: Extending bitcoin's proof of work via proof of stake. *ACM SIGMETRICS Performance Evaluation Review*, 2014, vol. 42, no. 3, pp. 34-37.

70. De Angelis S., Aniello L., Baldoni R., Lombardi F., Margheri A., Sassone V. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. *University of Southampton*, 2018. Available at: https://eprints.soton.ac.uk/415083/2/itasec18_main.pdf (accessed 11 January 2021).

71. Szabo N. Formalizing and securing relationships on public networks. *First Monday,*1997, vol. 2, no. 9. doi: 10.5210/fm.v2i9.548.

72. M.Video, Sberbank Faktoring i Al'fa-Bank sozdali pervyj v Rossii kommercheskij blokchejn-konsorcium [M.Video, Sberbank Factoring and Alfa-Bank created the first commercial blockchain consortium in Russia]. *Alfa-Bank press center*, 2017. Available at: https://alfabank.ru/press/news/2017/10/13/41066.html (accessed 11 February 2021) (in Russian).

73. «MegaFon» NRD i Rajffajzenbank osushchestvili pervuyu sdelku po razmeshcheniyu rublyovyh obligacij na blokchejne [MegaFon NSD and Raiffeisenbank completed the first transaction to place ruble bonds on the blockchain]. *Official site of PJSC «Megafon*», 2017. Available at: https://corp.megafon.ru/press/news/federalnye_novosti/20171002-0934.html (accessed 11 February 2021) (in Russian).

74. Gazprom Neft and S7 Airlines become the first companies in Russia to move to blockchain technology in aviation refuelling. *Official site of «Gazprom»,* 2018. Available at: https://www.gazprom-neft.com/press-center/news/gazprom-neft-and-s7-airlines-become-the-first-companies-in-russia-to-move-to-blockchain-technology-i/ (accessed 11 February 2021).

75. AO «Pervoural'skbank» provyol pervyj polnyj cikl finansirovaniya cherez blokchejn-platformu [Pervouralskbank JSC carried out the first full cycle of financing through the blockchain platform]. *Official site of JSC «Pervouralskbank»*, 2019. Available at: https://www.pervbank.ru/news/725/ (accessed 11 February 2021) (in Russian).

76. LG testiruet platformu cifrovyh platezhej na osnove II i blokchejna [LG Tests AI and Blockchain Digital Payment Platform]. *BitNovosti,* 2020. Available at: https://bitnovosti.com/2020/04/25/lg-testiruet-platformu-tsifrovyh-platezhej-na-osnove-ii-i-blokchejna/ (accessed 11 February 2021) (in Russian).

77. Grain V. DBS Bank vnedrit blokchejn Contour dlya raschyotov po akkreditivam [DBS Bank will implement blockchain contour for settlements under letters of credit]. *Bits.media,* 2020. Available at: https://bits.media/dbs-bank-vnedrit-blokcheyn-contour-dlya-raschetov-po-akkreditivam/ (accessed 11 February 2021) (in Russian).

78. China Telecom vnedryaet blokchejn v sistemy 5G [China Telecom brings blockchain to 5G systems]. *Bits.media,* 2020. Available at: https://bits.media/china-telecom-vnedryaet-blokcheyn-v-sistemy-5g/ (accessed 11 February 2021) (in Russian).

79. Daniil Egorov predstavil servis dlya bystrogo podtverzhdeniya l'gotnyh kreditov biznesu na video soveshchanii s Prezidentom Rossii [Daniil Egorov

presented a service for quick confirmation of concessional loans to businesses in a video meeting with the President of Russia]. *Official website of the Federal Tax Service of Russia*, 2020. Available at: https://nalog.ru/rn77/news/activities_fts/9744281/ (accessed 11 February 2021) (in Russian).

80. Paillisse J., Ferriol M., Garcia E., Latif H., Piris C., Lopez A., Kuerbis B., Rodriguez-Natal A., Ermagan V., Maino F., Cabellos A. IPchain: Securing IP prefix allocation and delegation with blockchain. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1236-1243.

81. Rossijskij sud vpervye ispol'zoval platformu blokchejn v deloproizvodstve [The Russian court first used the blockchain platform in office work]. *TASS.RU*, 2018. Available at: https://tass.ru/obschestvo/5865776 (accessed 11 February 2021) (in Russian).

82. Polys - sistema cifrovogo golosovaniya [Polys - digital voting system]. *Kaspersky*, 2020. Available at: kaspersky.ru/ihub/assets/POLYS.KASP.RUS_leaflet.pdf (accessed 11 February 2021) (in Russian).

83. Stepanov D. V. Rossii vpervye vydali cifrovye diplomy na blokchejne [For the first time in Russia issued digital diplomas on the blockchain]. *CNews.ru*, 2020. Available at: https://cnews.ru/news/top/2020-02-25_rossijskij_vuz_vpervye_vydast (accessed 11 February 2021) (in Russian).

84. Erazo F. South Korean telecom launches blockchain wallet for official documents. *CoinTelegraph*, 2020. Available at: https://cointelegraph.com/news/south-korean-telecom-launches-blockchain-wallet-for-official-documents (accessed 11 February 2021).

85. U.S. Treasury unveils blockchain grant project. *Ledger Insights*, 2020. Available at: https://www.ledgerinsights.com/us-treasury-unveils-blockchain-grant-project/ (accessed 11 February 2021).

86. Blokchejn massovogo porazheniya. Kak kriptomir pobedit epidemiyu [Blockchain of mass destruction. How the crypto world will defeat the epidemic]. *RosBusinessConsulting*, 2020. Available at: https://rbc.ru/crypto/news/5e9ab5a69a79475e1af088ae?from=main (accessed 11 February 2021) (in Russian).

87. V bor'be s nezakonnym oborotom polimernyh trub pomozhet blokchejn [Blockchain will help fight illicit trafficking in polymer pipes]. *Polyplastic group*, 2019. Available at: https://polyplastic.ru/press/news/2019/05/27/item17663 (accessed 11 February 2021) (in Russian).

88. «Rosseti» zapuskayut pilotnyj blokchejn-proekt po billingu na Urale [Rosseti is launching a pilot billing blockchain project in the Urals]. *RosBusinessConsulting*, 2019. Available at: https://ekb.rbc.ru/ekb/freenews/5df772cc9a794781fbf5e65a (accessed 11 February 2021) (in Russian).

89. FoodTech: kak nakormit' lyudej s pomoshch'yu cifrovyh tekhnologij [FoodTech: How to digitally feed people]. iFarm, 2020. Available at: https://ifarmproject.ru/kostenko (accessed 11 February 2021) (in Russian).

90. Seven S., Yao G., Soran A., Onen A., Muyeen M. Peer-to-Peer Energy Trading in Virtual Power Plant Based on Blockchain Smart Contracts. *IEEE Access*, 2020, vol. 8, pp. 175713-175726.

91. Kim G., Park J., Ryou J. A study on utilization of blockchain for electricity trading in microgrid. *International Conference on Big Data and Smart Computing (BigComp)*, 2018, pp. 743-746.

92. Clott C., Hartman B., Beidler B. Sustainable blockchain technology in the maritime shipping industry. *Maritime Supply Chains*, 2020, pp. 207-228.

93. Teufel B., Sentic A., Barmet M. Blockchain energy: Blockchain in future energy systems. *Journal of Electronic Science and Technology*, 2019, vol. 17, no. 4, 100011 p.

94. Voloshin I. P. Upravlenie dostupom na osnove blokchejn [Blockchain-based access control]. *Information security of regions*, 2017, no. 3-4, pp. 28-29.

95. Filyak P. YU., Postnikov M. K., Fedorov S. E. Primenenie tekhnologij blockchain dlya razrabotki korporativnoj informacionnoj sistemy v zashchishchyonnom ispolnenii [The use of blockchain technologies for the development of a corporate information system in a secure execution]. *Information and security*, 2020, vol. 23, no. 3, pp. 399-408.

96. Yumasheva E. V., YUmashev D. V., Timonov D. A. Informacionnaya bezopasnost' v sistemah elektronnogo dokumentooborota s primeneniem tekhnologii blokchejn [Information security in electronic document management systems using blockchain technology]. *Modern high technologies*, 2021, no. 1, pp. 63-68.

97. Agbede O. Strong Electronic Identification: Survey & Scenario Planning. *School of Electrical Engineering*, 2018. Available at: https://aaltodoc.aalto.fi/bitstream/handle/123456789/34352/master_Agbede_Oluwabunmi_2018.pdf?sequence=1 (accessed 11 February 2021).

98. SmartCitiesWorld news team. Olsztyn claims world-first by linking blockchain to emergency services. *SmartCitiesWorld*, 2020. Available at: https://smartcitiesworld.net/news/news/olsztyn-claims-world-first-by-linking-blockchain-to-emergency-services--5900 (accessed 11 February 2021).

99. Dye C., Li G., Cai H., Gu Y., Fukuda A. Analysis of security in blockchain: Case study in 51%-attack detecting. *5th International Conference on Dependable Systems and Their Applications (DSA)*, 2018, pp. 15-24.

100. Karame O., Androulaki E., Roeschlin M., Gervais A., Čapkun S. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)*, 2015, vol. 18, no. 1, pp. 1-32.

101. Mayer H. ECDSA security in Bitcoin and Ethereum: a research survey. *CoinFaabrik*, 2016, vol. 28, pp. 126-127.

102. Security Lab. A way to recover ECDSA keys has been found // *Security Lab by positive technologies*. Available at: https://www.securitylab.ru/news/501553.php (accessed 05.03.2021).

103. Miller A., Möser M., Lee K., Narayanan A. An empirical analysis of linkability in the monero blockchain // *arXiv preprint.* arXiv:1704.04299. 2017.

104. Ehrenfeld JM. Wannacry, cybersecurity and health information technology: A time to act. *Journal of medical systems,* 2017, vol. 41, no. 7, pp. 104-105.

105. Christin N. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 213-224.

106. Courtois T., Mercer R. Stealth Address and Key Management Techniques in Blockchain Systems. *ICISSP*, 2017, pp. 559-566.

107. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on ethereum smart contracts (sok). *International conference on principles of security and trust*, 2017, pp. 164-186.

108. Luu L., Chu H., Olickel H., Saxena P., Hobor A. Making smart contracts smarter. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 254-269.

109. Chen T., Li X., Luo X., Zhang X. Under-optimized smart contracts devour your money. *24th International Conference on Software Analysis, Evolution and Reengineerin*g, 2017, pp. 442–446.

110. Nosirov Z. A., Sherbinina O. V. Analiz kriptograficheskih skhem razdeleniya sekreta dlya rezervnogo hraneniya klyuchevoj informacii [Analysis of cryptographic secret sharing schemes for backing up key information]. *Caspian journal: Control and high technologies,* 2019, no. 2, pp. 126-134 (in Russian).

Статья поступила 15 марта 2021 г.

Информация об авторах

Носиров Зафаржон Амрулоевич – соискатель учёной степени кандидата технических наук. Аспирант департамента «Информационная безопасность». Финансовый университет при Правительстве Российской Федерации. Область научных интересов: технологии распределённых реестров, Интернет вещей. E-mail: nosirovzafar@outlook.com

Фомичев Владимир Михайлович – доктор физико-математических наук, профессор. Профессор департамента «Информационная безопасность». Финансовый университет при Правительстве Российской Федерации. Область научных интересов: криптология, дискретная математика. E-mail: fomichev.2016@yandex.ru

Адрес: 125993, Россия, г. Москва, Ленинградский просп., 49.

Analysis of Blockchain Technology: Architectural Basics, Application Examples, Future Trends, Problems and Disadvantages

Z. A. Nosirov, V. M. Fomichev

Problem Statement. *Distributed ledger technology (blockchain technology) has important advantages: reliability, immutability and transparency. This technology is used in various fields providing services in finance, industrial Internet of Things (IoT), public and socially important services. Despite the large number of studies conducted on the application of blockchain in various fields of activity, there are still relevant complex studies from a technical and applied point of view.* ***The purpose of this paper*** *is to systematize knowledge about blockchain technology, to identify problems and drawbacks, as well as to propose new directions for development.* ***Results and novelty:*** *the paper presents a comprehensive overview of blockchain technology (technical features). A comparative analysis of public and closed blockchain networks, as well as 3 types of consensus protocols was carried out. In addition, the successful domestic blockchain projects are considered and the areas in which this technology is in demand are identified. The main problems and shortcomings of this technology were also identified and new directions for research work related to the security of blockchain technology were proposed.* ***Practical relevance.*** *The results of the study may be useful for novice researchers who have chosen blockchain technology as an area of interest. They may also be in demand by government agencies and large corporations of the Russian Federation engaged in the development and implementation of blockchain solutions in information systems.*

Key words: *blockchain, distributed ledger, blockchain technology, consensus protocols, consensus, key information, blockchain survey, distributed ledger technology.*

Information about Authors

Zafarzhon Amruloevich Nosirov – postgraduate at the Department of Information Security. Financial University under the Government of the Russian Federation. Field of research: distributed ledger technology, Internet of Things. E-mail: nosirovzafar@outlook.com

Vladimir Mikhailovich Fomichev – Dr. habil. of Physico-mathematical Sciences. Full Professor. Professor at the Department of Information Security. Financial University under the Government of the Russian Federation. Field of research: discrete mathematics, cryptology. E-mail: fomichev.2016@yandex.ru

Address: 125993, Russia, Moscow, Leningradskiy prospect, 49.