Федеральное государственное автономное образовательное учреждение высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет экономических наук

Национальный Расчетный депозитарии

Группа Московская биржа

СОВМЕСТНАЯ ПРОЕКТНАЯ РАБОТА

Распределенные реестры: мошеннические действия и технические ошибки

по направлению подготовки Экономика

образовательная программа «Экономика»

Кураторы:

Андрей Мигаленко

Николай Лудников

Выполнили:

Артемий Гусак

Максим Пешков

Натела Кордзахия

Людмила Латонова

Михаил Огородников

Москва 2020

Введение. Перспективы токенизации.

Технология распределенных реестров стала широко популярной после масштабного распространения и капитализации криптовалют. Однако функционирование криптовалют является далеко не единственным возможным применением этой технологии. Распределенные реестры могут помочь оптимизировать бизнес-процессы во многих отраслях экономики. Для Группы «Московская Биржа» токенизация активов с использованием распределенных реестров может стать одним из перспективных направлений работы по ряду причин.

Во-первых, токенизация в перспективе может значительно удешевить торговлю физическими активами и привлечение инвестиций. Распределённые реестры позволяют обрабатывать транзакции быстрее, а также частично убирают недоверие между контрагентами при проведении сделок, делая их максимально прозрачными. Это позволяет снизить издержки на процедуры взаимных проверок. Токенизация также позволяет легко торговать активами без необходимости их физического перемещения, что существенно повышает их ликвидность. Всё это может привлечь новых клиентов, которым недоступны обычные биржевые инструменты торговли в силу высокой стоимости их применения, а также держателей неликвидных активов.

Во-вторых, развитие в данном направлении уже осуществляется многими компаниями, причём не только биржами, но ещё и сырьевыми, что говорит об их заинтересованности в подобных площадках. Совсем недавно проект по выпуску security-активов iSTOX[1] от Сингапурской биржи получил лицензию Центрального банка Сингапура[2]. Норильский Никель разрабатывает собственную платформу Atomyze для токенизации его продукции, а в последствии и других физических активов. Также австрийской компанией Alukoenigstahl разрабатывается аналог этой платформы Steel But Smart[3], направленный на токенизацю стали. Это позволяет сделать вывод, что сырьевые компании нуждаются в новых технологических платформах для продажи их продукции. Более того, то, что они самостоятельно занимаются их разработкой, показывает, что они видят в этом нечто большее, чем просто платформу для размещения только собственных активов, а значит, в этих площадках должно быть заинтересовано гораздо больше компаний. Например, Владимир Потанин отмечал, что это позволит «*популяризировать их металлы благодаря переходу на цифровые методы торговли*»[4], то есть создание имиджа и нового видения продукта этих компаний также подталкивает их к дальнейшему развитию в этом направлении.

---

[1] iSTOX. 2020. URL: https://istox.com
[2] Центробанк Сингапура выдал лицензию платформе по выпуску security-токенов. Bloomchain. 2020. URL: https://bloomchain.ru/newsfeed/tsentrobank-singapura-vydal-litsenziyu-platforme-po-vypusku-security-tokenov/
[3] Steel But Smart. 2020. URL: https://www.steelbutsmart.com
[4] «НорНикель» станет первым эмитентом платформы для токенизации промышленных активов Atomyze. Норильский никель. 2020. URL: https://www.nornickel.ru/news-and-media/press-releases-and-news/nornikel-stanet-pervym-emitentom-platformy-dlya-tokenizatsii-promyshlennykh-aktivov-atomyze/

В-третьих, руководитель «Норильского никеля» Владимир Потанин ранее заявлял о намерении запустить свою платформу даже в случае, если в России не будут приняты необходимые нормативные акты[5]. Отсюда следует два вывода: 1) платформа будет запущена в другой стране, если это будет невозможно в России, а значит, это лишь подтверждает заинтересованность «Норильского Никеля» (и других потенциальных эмитентов) в создании и функционировании данной платформы; 2) подобное заявление должно подтолкнуть российских депутатов быстрее принять документ, который бы регулировал управление цифровыми активами – также Потанин ожидает, что первые коммерческие операции на платформе начнут совершаться уже в конце 2020 года[6]. Вкупе с тем фактом, что австрийцы также ведут разработку подобной платформы, а Сингапурская биржа уже получила лицензию на свой аналогичный проект, логично предположить, что российские депутаты должны быстрее принять необходимые нормативные акты, потому что иначе очень перспективная российская Atomyze могла бы быть запущена за рубежом ввиду того, что «Норильский никель» тоже не захочет давать лишнее время своим австрийским конкурентам. Стоит также отметить, что после успешного тестирования Atomyze в «песочнице» Центробанка, регулятором были представлены необходимые рекомендации относительно закона о цифровых активах[7]. Слова из разных заявлений председателя Государственной Думы по финансовому рынку Анатолия Аксакова только подтверждают, что скоро закон будет принят со всеми необходимыми правками, так как не только Госдума участвует в его разработке: «*Могу с уверенностью в 99,9% сказать, что в весеннюю сессию мы этот закон примем* [о законе о цифровых активах]»[8], возможно, он будет уже в марте этого года: «*Сейчас готовится текст, и если этот текст после рассылки соответствующие институты, ЦБ и компетентные органы, правовое управление поддержат, то мы в марте, я полагаю, можем выйти с таким законопроектом на рассмотрение во втором, третьем чтениях*»[9]. Всё это создает благоприятный фон для развития площадок по обороту цифровых активов.

В-четвёртых, запуск подобной платформы может быть стратегически важным для Московской биржи, так как это выведет её на новый уровень на международной арене. Подобные введения неизбежно будут происходить на мировых площадках, поэтому Московская биржа может стать одним из первопроходцев по внедрению токенизации. В начале февраля 2020 года

---

[5] Центробанк одобрил блокчейн-проект «Норникеля». РБК. 2020. URL: https://www.rbc.ru/business/17/02/2020/5e469c089a794755bbd0989c

[6] Bloomberg рассказал подробности блокчейн-проекта Потанина // Ведомости. 2020. URL: https://www.vedomosti.ru/technology/news/2020/02/25/823756-podrobnosti-blokchein-proekta-potanina

[7] Российская торговая платформа Atomyze на блокчейне запущена в тестовом режиме. SharesPro. 2020. URL: https://sharespro.ru/news/5694-torgovaya-platforma-atomyze

[8] Аксаков назвал дату принятия закона о криптовалютах. РБК. 2020. URL: https://www.rbc.ru/crypto/news/5e1c769c9a79475f3356cc26

[9] В марте Госдумой может быть принят закон о цифровых активах. Версия. 2020. URL: https://versia.ru/gosduma-mozhet-v-marte-prinyat-zakon-o-cifrovyx-finansovyx-aktivax

сингапурский проект iSTOX по выпуску security-токенов, одним из акционеров которого является Сингапурская биржа, получил лицензию от Центробанка Сингапура – очередное подтверждение наличия актуальности данной разработки. Пока такие платформы не стали рядовыми самостоятельными площадками отдельных компаний и/или частями бирж по всему миру, Московская биржа имеет уникальный шанс стать одним из мировых центров по выпуску токенов, так как данное направление не является освоенным и его развитие находится только в самом начале.

Впрочем, технология распределённых реестров пока еще имеет слабые места, позволяющие совершать мошеннические действия. В качестве основных проблем применения технологии мы выделяем возможности для компрометации данных, отмывания денег, проведения кибератак и манипулирования ценами. В этой работе будет представлен обзор этих проблем и их потенциальные решения.

Компрометация данных

Распределенные реестры обеспечивают сохранность и неизменность внесенных в них данных, однако серьёзной проблемой является проверка их истинности. Технология не может гарантировать соответствие информации, записанной в реестре, и физического мира. Это открывает возможности для мошенничества. В качестве одного из примеров можно представить некий блокчейн-проект в сфере логистики. Его целью может быть контроль за состоянием перевозимых товаров пути. Контроль может осуществляться при помощи смарт-контрактов: например, в реестр в течение доставки может вноситься информация о температуре внутри грузового отсека, и при её превышении некоторого значения сработает смарт-контракт, выставив штраф перевозчику. Это гарантирует наступление ответственности за нарушение условий перевозки, однако перевозчик может компрометировать данные, которые вносятся в реестр. Так, он может расположить датчик в ином пространстве, в котором вообще нет перевозимого груза, например, поместив его в некий охлаждаемый кейс, и избежать ответственности. Подобные возможности для мошенничества могут возникнуть везде, где в распределённый реестр вносится информация из реального мира. При этом неважно вносит её человек или аппаратное устройство[10].

Пример показывает, что распределённые реестры могут не защитить их пользователя от нечестности контрагента, и этот факт является серьёзным вызовом для технологии, поскольку в качестве одной из целей применения блокчейна декларируется преодоление отсутствия доверия между различными сторонами. В настоящее время улучшение технологий проверки и выбора

[10] Karl Wüst, Arthur Gervais. Do you need a Blockchain? IACR. 2017. URL: https://eprint.iacr.org/2017/375.pdf

информации для её поставщиков в распределённые реестры, так называемых оракулов, является приоритетной задачей для многих специалистов. Одним из возможных решений может стать развитие интернета вещей и RFID меток. В перспективе RFID метки будут способны отслеживать различные параметры: температуру, влажность, давление, содержание химических элементов и прочее. При этом развитие технологии сделает метки меньше и дешевле, а также затруднит их радиообнаружение[11]. Это позволит расположить большое число датчиков и затруднит компрометацию данных. Кроме того, при помощи технологии Интернета вещей может быть создана единая сеть из множества таких RFID меток. Она сможет определить попытку мошенничества: если один или несколько датчиков будут регистрировать отличающиеся от других данные или будут перемещены от положения основного числа меток, то это будет обнаружено системой.

Также в реальном мире объект, к которому привязан токен блокчейна, может быть серьёзно изменён, или он может вовсе прекратить своё существование. При этом распределённый реестр не может отследить это, если соответствующая запись не будет занесена и одобрена. Это открывает дополнительные возможности для мошенничества. Так, в 2018 году WWF запустил блокчейн-проект в Океании по отслеживанию перемещения тунца после отлова. Он должен помочь покупателям избежать приобретение рыбы, добытой незаконным путем. На легально добытую рыбу помещается метка, и далее записи по каждому перемещению рыбы вносятся в распределённый реестр, таким образом покупатель может отсканировать метку и увидеть весь путь тунца, убедившись, что он был выловлен законно[12]. Однако метка может быть перенесена на нелегально добытую рыбу на одном из этапов транспортировки, пока рыба жива, а легальный тунец может быть заново передан рыболовам, имитируя новую добычу. Подобная операция в текущих условиях не отразится в распределённом реестре, и технология не выполнит задачу, для решения которой она была применена. В случае токенизации активов базовый актив может быть подменён на менее качественный или вовсе украден или уничтожен до того, как будет потребован владельцем токена. В настоящий момент отсутствие чёткого нормативного определения цифрового актива теоретически позволяет совершать подобные действия и избегать ответственности.

Одним из решений этой проблемы может стать усовершенствование меток, расположенных на физическом объекте и контролирующих его неизменность и общее состояние. Эти метки должны быть чувствительны к собственному перемещению с одного объекта на другой и направлять соответствующую запись в реестр, если произошло некое несогласованное

---

[11] Обзор технологий и стандартов RFID систем. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича. 2018. URL: http://www.sut.ru/doci/nauka/review/20185/1-11.pdf

[12] WWF использует блокчейн для борьбы с браконьерством. Bit Journal. 2018. URL: https://bitjournal.media/29-01-2018/wwf-ispolzuet-blokchejn-dlya-borby-s-brakonerstvom/

изменение в физическом мире. Это отсылает к предыдущему примеру и тоже зависит от развития интернета вещей и технологии RFID. Также необходимо принятие новых регуляторных норм. В законодательстве должно быть чётко прописано, какими правами обладает владелец токена, а также какие обязательства перед ним имеет эмитент. В частности, должны быть определены права требования базового физического актива. Также в законодательстве может быть определен центральный контрагент, который будет обеспечивать сохранность базового актива и нести за него ответственность. В настоящее время в России еще не принят базовый закон, дающий понятие цифрового актива, к которому относятся токены, используемые в распределенных реестрах. Из-за этого пока сложно говорить о дальнейшем развитии законодательной базы, которая может устранить возможности для такого мошенничества.

Наконец, мошеннические действия широко распространены при проведении ICO: около 20% таких публичных предложений токенов имеют признаки мошенничества[13]. Ключевым фактором, способствующим этому, опять же является разрыв между физическим и виртуальным мирами. Блокчейн-система, к которой привязан токен может обеспечивать всё то, что гарантирует инвестору инициатор ICO, например, получение части прибыли в виде дивидендов или гарантированных будущих платежей. Однако владелец не может контролировать или даже наблюдать за реальным положением дел компании, выпустившей токен. Мошенники могут использовать в описании ICO скомпрометированные или вовсе скопированные у других проектов документы, указывать несуществующих людей как членов своей команды и привлекать инвесторов надуманными перспективами. Собрав деньги, компания перестает вести какую-либо деятельность, а ее владельцы – выходить на связь. Из-за этого её токен обесценивается, а инвесторы теряют вложенные деньги, почти не имея возможности вернуть их в силу отсутствия законодательства и судебных прецедентов. По такой схеме, например, прошло ICO компании «Полибиус»[14].

Решением этой проблемы должно стать применение регулирующего законодательства, которого в России пока нет. Одним из лидеров по качеству регулирования токенизации является Сингапур. В нормативах этой страны определены различные требования для многих видов эмитируемых токенов и сумм, на которые они размещаются. Объём затрат и обязательств эмитента при проведении ICO зависит от типа токена и суммы эмиссии. Так, если выпуск не превышает 5 миллионов сингапурских долларов, эмитент не обязан регистрировать проспект

[13] Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud. The Wall Street Journal. 2018. URL: https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115
[14] Как я потерял 1000 $ на ICO. Тинькофф Журнал. 2019. URL: https://journal.tinkoff.ru/icofail/

эмиссии у регулятора, что значительно удешевляет финансирование через ICO для малых компаний[15].

При этом любой эмитент обязан раскрыть следующую информацию:

- обоснование ICO;
- риски (операционные и кибербезопасность), возникающие из ICO;
- использование привлеченных средств;
- процедуры учета и оценки для ICO;
- система «Знай своего клиента» проверяет риски нарушения правил AML/CFT;
- порядок учета и оценки для ICO;
- использование существующих средств эмитента для проведения ICO;
- финансовое влияние на эмитента в результате выпуска токена;
- любое влияние на права существующих акционеров.

Также после проведения ICO в Сингапуре зарегистрированные эмитенты должны своевременно информировать своих акционеров о существенной информации, разработке ICO и цифровых токенов, а также об использовании доходов ICO. Кроме того, эти компании должны также согласиться со своими установленными законом обязательствами в отношении объема аудита, который должен обеспечить уверенность в том, что ICO должным образом учтено в их финансовой отчетности, и что соответствующие риски были должным образом учтены[16]. Все это в достаточной мере защищает права инвесторов.

Отмывание средств

Проекты, созданные на основе распределённых реестров, часто используются для легализации доходов, полученных преступным путём, и финансирования терроризма. Борьба с отмыванием денег посредством криптовалют главным образом заключается в деанонимизации криптовалютных транзакций. Чтобы достичь этого, регуляторы пытаются применять на рынке криптовалют те же самые механизмы контроля, что и на обычном финансовом рынке.

Ключевое решение – создание законодательства, регулирующего движение цифровых активов и действия поставщиков криптовалютных услуг. Так, согласно выпущенным в 2019 году рекомендациям Международной группы разработки финансовых мер по борьбе с отмыванием денег (FATF – financial action task force), биткоин-биржи и другие поставщики криптовалютных услуг (VASPs - virtual asset service providers) обязаны соблюдать процедуры AML (anti-money laundering) и CFT (combating the financing of terrorism) по аналогии с традиционными финансовыми компаниями. Таким образом, биткоин-биржи обязаны функционировать в

[15] Регулятор Сингапура представил руководство по ICO. vc.ru. 2017. URL: https://vc.ru/crypto/29089-regulyator-singapura-predstavil-rukovodstvo-po-ico
[16] Криптоактивы и блокчейн в сингапуре. IQ Decision. 2020. URL: https://iqdecision.com/kriptoaktivy-i-blokchejn-v-singapure/

соответствии с Know Your Transaction (KYT): удостоверять имя отправителя и получателя, данные о их цифровых кошельках, адресе, паспортные данные или пользовательский идентификатор, который привязывает человека к компании, дате или месту рождения. Поставщики криптовалютных услуг обязаны раскрывать информацию о бенефициарах, а также проходить процедуру лицензирования своей юрисдикции[17].

Если же смарт-контракты криптовалюты не позволяют отследить транзакции (например, валюты, основанные на доказательстве с нулевым разглашением (Zero-knowledge proof)), крипто-бирже следует провести делистинг такой монеты, как это произошло с Dash, Monero и Zcash на нескольких крупных азиатских биржах[18]. Данные меры повышают вероятность раскрытия преступных схем, но в то же время влекут за собой значительные издержки для криптовалютных сервисов, а также их частичный уход в теневой бизнес. «Есть ожидание, что сопротивление части криптовалютного сообщества тренду на прозрачность и деанонимизацию может стимулировать разработку и распространение по-настоящему децентрализованных бирж (DEX), которые на текущий момент так и не снискали массовой популярности из-за сложного интерфейса. Правда, тут есть вероятность, что создателей подобных площадок также могут привлечь к ответственности за способствование отмыванию денег, на что сослались разработчики той же IDEX.»[19] Децентрализованная биржа IDEX решила ввести обязательную верификацию всех пользователей. Платформа оценила риск того, что разработчики могут быть привлечены к ответственности за незаконные операции, согласно заявлению члена Комиссии по торговле товарными фьючерсами США (CFTC - Commodity Futures Trading Commission) Брайана Квинтенса. То есть достаточно крупным площадкам не удастся уйти в теневой сектор при уже налаженной работе с клиентами, легче будет приспособиться под новые требования.

Некоторые страны уже начали вводить необходимые законы в соответствии с рекомендациями FATF. Законодательство Мальты[20] является одним из самых проработанных в криптообласти, в нем достаточно чётко описаны регуляторные правила относительно криптоактивов, они могут быть ориентиром для готовящихся законопроектов в других странах. Для управления криптоактивами создана специальная государственная структура MDIA (Malta Digital Innovation Authority), которая тестирует проекты на основе распределённых реестров,

---

[17] FATF решила ужесточить контроль над биткоин-индустрией // Forklog. 2019. URL: https://forklog.com/fatf-reshila-uzhestochit-kontrol-nad-bitkoin-industriej-nesmotrya-na-predosterezheniya-ekspertov-o-neblagopriyatnyh-posledstviyah/

[18] Ждет ли Monero, Dash, Zcash и другие анонимные криптовалюты массовый делистинг, и к чему готовиться? Forklog. 2019. URL: https://forklog.com/zhdet-li-monero-dash-zcash-i-drugie-anonimnye-kriptovalyuty-massovyj-delisting-i-k-chemu-gotovitsya/

[19] Тоже плачут. Как криптобиржи противостоят преступникам. РБК. 2019. URL: https://www.rbc.ru/crypto/news/5d9dadf79a79472106eec0a1

[20] Юрисдикция Мальты – одно из лучших мест для запуска ICO и развития криптобизнеса. International Wealth. 2018. URL: https://internationalwealth.info/cryptocurrency/malta-one-of-the-best-places-for-launching-ico-and-developing-crypto/

сертифицирует их, а также осуществляет надзорную деятельность за ними. Функционирует государственная структура в соответствии с законами:

- «О цифровой инновационной деятельности»

Согласно этому закону, Управление по цифровым инновациям (далее Управление) осуществляет тестирование и сертификацию проектов на основе распределённых реестров

- «Об инновационных технологиях и услугах»;

Дает определение понятиям "инновационная технология" и "инновационные услуги"; в соответствии с критериями, данными в определениях, регламентируется механизм сертификации цифровых инноваций

- «О виртуальных финансовых активах» (Virtual Financial Asset Act (VFAA)).

Направлен на регламентирование проведения ICO. Выделяет 4 категории токенов: в зависимости от того, как Управление оценило экономическую значимость, токену присваивается та или иная степень регулирования:

Виртуальные токены, жетоны (Utility) не подлежат регулированию, владельцы токенов перед правительством Мальты не имеют никаких обязательств или прав до тех пор, пока токен будет являться сервисным символом.

Виртуальные монеты или деньги (coin), используемые в финансовых услугах, подлежат регулированию законом Мальты об инвестиционных услугах и Директивой ЕС «О финансовых инструментах» (MiFIDII) №39 от 2004 года.

Электронные деньги регламентируются Директивой ЕС «Об электронных денежных средствах» №110 от 2009 года.

Цифровые финансовые активы (криптовалюты) регулируются новым законом (VFAA) от 4/07/2018 года.

Также регулируется деятельность: поставщиков виртуальных кошельков, криптобирж и брокеров, управляющих активами и инвестиционных консультантов. Например, в отношении борьбы с отмыванием доходов важным нормативом стало обязательное для эмитентов цифровых активов назначение независимого агента VFAA, который осуществляет контроль за деятельностью эмитента, тестирует виртуальные активы на предмет определения экономического значения, представляет в MFSA (Malta Financial Service Authority) отчёт о технической документации на предмет соответствия сертифицированных эталонов с текущими техническими данными, а также сообщает в MFSA о выявлении нарушений со стороны

эмитента[21]. Агент VFA должен быть адвокатом, бухгалтером, аудитором или любым другим лицом, обладающим необходимыми полномочиями, квалификацией и опытом

Вышеуказанные нормы дополняются законом, регулирующим традиционный сектор финансовых услуг (MFSA). Каждая компания, организовывающая ICO, должна в специальном документе, который обычно называется «White paper», публично и подробно описывать проведение проекта, а также финансовую историю своей компании.

Если сертификат на инновации выдаёт Управление по инновациям (MDIA), то физические и юридические лица, собирающиеся стать поставщиками финансовых услуг, должны пройти тестирование для получения лицензии в Управлении финансовыми услугами (MFSA).

Чётко прописанные этапы прохождения лицензирования, указание конкретных случаев, в которых поставщики криптоуслуг подотчётны правительству, обязательные внутренние системы контроля, управления рисками, верификации клиентов, включая идентификацию пользователя и проверку личности с помощью паспорта или других документов - всё эти действия являются эффективным решением в борьбе с отмыванием доходов и мошенническими действиями в сфере крипто-активов. Мальта имеет высокую репутацию в сфере криптобизнеса, поэтому, систему регулирования в данной стране можно счесть эталонной.

Существует критика попыток введения рекомендаций FATF: в них нет смысла, пока не будет создана управляемая правительствами глобальная система наблюдения за криптовалютой[22]. Глобальные финансовые учреждения используют свою собственную систему безопасного обмена сообщениями под названием SWIFT (Society for Worldwide Interbank Financial Telecommunications) для обмена информацией о финансовых операциях и противодействию отмывания денег. Сейчас криптовалютные биржи находятся под давлением со стороны регуляторов, чтобы создать подобную систему. В рекомендациях FATF указано, что всякий раз, когда пользователь отправляет криптовалюту стоимостью более 1000 долларов или евро другому пользователю, инициирующий обмен должен «незамедлительно и безопасно» обмениваться идентифицирующей информацией как об отправителе, так и о предполагаемом получателе. Эта информация также должна предоставляться «соответствующим органам власти по запросу», а также доступна всем странам G20, согласно FATF.

На данный момент компания CipherTrace разработала проект Travel Rule Information Sharing Architecture (TRISA), который позволит проводить процедуры KYC (Know your client), KYV (Know Your VASP), включая скрининг против санкционных списков, а также отслеживать

---

[21] Юрисдикция Мальты – одно из лучших мест для запуска ICO и развития криптобизнеса. International Wealth. 2018. URL: https://internationalwealth.info/cryptocurrency/malta-one-of-the-best-places-for-launching-ico-and-developing-crypto/

[22] New money-laundering rules change everything for cryptocurrency exchanges. MIT Technology Review. 2019. URL: https://www.technologyreview.com/s/614164/new-money-laundering-rules-change-everything-for-cryptocurrency-exchanges/

сомнительные операции без изменения блокчейн- и криптопротоколов. *«TRISA предоставляется бесплатно как ПО с открытым исходным кодом. Услуга аутентификации и защиты VASP предлагаются CipherTrace, но могут также предоставляться другими компаниями, правительственными агентами или консорциумами из-за открытого характера TRISA и её модели независимого управления».* [23]

По мнению крупных криптобирж, таких как Binance[24], TRISA может стать жизнеспособным аналогом SWIFT среди поставщиков криптоуслуг.

Несмотря на введение правовой основы, государство не может повлиять на функционирование крипто-миксеров. Хотя крупные биржи работают в поле законов KYC и AML, но при поступлении на их депозиты денег с сайтов-миксеров они неэффективны. Поправки FATF, конечно, предусматривают принудительное сотрудничество крипто-миксеров с правительством, однако как это будет реализовываться – непонятно, учитывая саму суть в анонимизации транзакций в этих сервисах и их децентрализованный характер. Тут мы сталкиваемся с проблемой неэффективности мер традиционного финансового рынка в отношении криптовалют, в данном случае необходимы высокотехнологичные решения. Однако, многие из популярных биткоин-миксеров могут расшифровываться с высокой вероятностью. Это происходит благодаря технике под названием «Анализ кластеризации». Компании Chainalysis и Bitfury разработали алгоритмы, которые могут идентифицировать адреса, связанные друг с другом, с высокой степенью точности[25]. Также, например, получить доступ к серверу, который предположительно связан с отмыванием криптовалют можно посредством фаззинга (передача приложению на вход неправильных, неожиданных или случайных данных), виды которого со временем становятся всё более прогрессивными. Так, например, спецслужбам США удалось успешно применить этот процесс в поимке главы онлайн-рынка наркотиков Silk Road[26]. но данная мера также должна быть закреплена в законодательстве, чтобы исключить неправовой характер действий спецслужб (в данном случае ФБР обвинили в использовании незаконных, секретных инструментов Агентства национальной безопасности).

Также эффективным методом отслеживания криптопотоков становятся сервисы, помогающие криптовалютным компаниям соответствовать требованиям AML. EXMO недавно заключили партнерское соглашение со компанией CipherTrace. Система отслеживает криптовалютные потоки и присваивает кошелькам уровень риска от 1 до 10 в зависимости от

---

[23]Travel Rule Information Sharing Architecture for Virtual Asset Service Providers (TRISA). August 22, 2019. Version 4. https://ciphertrace.com/wp-content/uploads/2019/08/TRISA-Enabling-FATF-Travel-Rule-V4.pdf

[24] CipherTrace unveils open source solution for crypto Travel Rule compliance TRISA. Tokenpost. 2019. URL: https://tokenpost.com/CipherTrace-unveils-open-source-solution-for-crypto-Travel-Rule-compliance-TRISA-3369

[25] Анонимность в сети Биткоин. Мифы и реальность. Cryptor. 2017. URL: https://cryptor.net/bitkoin-dlya-chaynikov/anonimnost-v-seti-bitkoin-mify-i-realnost

[26] The FBI revealed how it found the Silk Road servers. Was the search legal? Quartz. 2014. URL: https://qz.com/261961/the-fbi-revealed-how-it-found-the-silk-road-servers-was-the-search-legal/

того, получал или отправлял ли этот адрес средства, которые ранее были замечены в использовании магазинами наркотических средств, террористическими организациями, скам-проектами или миксерами. Если сотрудничество с подобными проектами будет вводиться повсеместно, то поставщики криптовалютных услуг хотя бы смогут вычислять те токены, которые прошли анонимизацию и заморозить их дальнейшее движение до выяснения происхождения. Также набирает популярность Chainalysis — блокчейн-стартап, который занимается вопросами цифровой идентификации пользователей и борьбы с отмыванием денег. Используя наработки Chainalysis, Федеральное бюро расследований США смогло продвинуться в расследовании по вышеупомянутому делу анонимной торговой платформы Silk Road. Также благодаря Know Your Transaction оно смогло выяснить дополнительные обстоятельства банкротства Mt. Gox, поскольку именно специалисты Chainalysis обнаружили исчезнувшие 650 тысяч биткоинов. Результаты мониторинга были открыто оглашены на слушании в Конгрессе[27].

Кибератаки

Создавая новую платформу на основе распределенных реестров, необходимо осознавать какие риски будут при реализации этого проекта. Сюда следует включить различные кибератаки как на пользователей сети, так и на саму сеть в целом, ведь на сегодняшний день злоумышленники имеют множество способов украсть деньги в условиях распределенного реестра. Далее рассмотрим основные виды таковых и предложим способы решения по минимизации рисков потери средств от кибератак.

В первую очередь, необходимо раскрыть виды атак на непосредственно пользователей. Здесь имеется в виду кража средств из кошелька владельцев с помощью вируса-трояна. Оно осуществляется в том случае, когда на компьютер пользователя был загружен вирус, меняющий действительный адрес в транзакции на адрес мошенника в буфере обмена. Также другой вирус может вытаскивать конфиденциальную информацию о пароле к кошельку из облачного хранилища при помощи алгоритмов распознавания фотографий и передавать его хакеру для опустошения счета клиента. Однако существует и другой способ сделать это: современные вирусы-вымогатели CryptoLocker или CryptoWall шифруют файлы на компьютере и требуют выплатить выкуп в Bitcoin. Более сложным является вирус, который добывает резервную копию файлов компьютера и отправляет злоумышленнику со старыми паролями, которые обычно не меняют пользователи. Что же касается вирусов, напрямую связанных со сделками по криптовалюте, то существует несколько вариантов таковых. К первым относятся вирусы,

[27] Анонимность криптовалют под ударом. БрокерТрибунал. 2020. URL: https://brokertribunal.com/blog/post/anonimnost-kriptovalyut-pod-udarom

которые начинают использовать ресурсы компьютера для майнинга в скрытом виде, примером таковых был Miner Bitcoin, распространенный через Skype. К другим относятся более затратные и тяжело реализуемые вирусы, которые за пользователя отправляют несколько платежей, передающих один и тот же актив, создавая конфликтующие транзакции, хотя в итоге совершится только одна из них, то есть будет осуществлена «двойная трата», требующая, на самом деле, большого контроля над счетом пользователя, о чем будет более детально рассмотрено в одном из следующих видов атак[28].

Вышеупомянутые вирусы осуществляются из-за невнимательности и неосторожности людей, поэтому чтобы предотвратить такие следует постоянно обновлять систему и часто менять пароли, установить проверенные антивирусы и плагины против майнеров (к таким относятся плагин AdBlock, «Лаборатория Касперского», встроенный скрипт NoCoin и другие)[29], осуществлять дополнительную цифровую подпись транзакции (в том числе использование биометрических данных личности)[30], разбиение секретного ключа на несколько частей и шифрование их. Это необходимые меры по собственной защиты от вирусов, но также существуют приложения, которые способны защитить горячие кошельки (подключенные к сети ежедневно) от хакеров, так называемые аппаратные кошельки, например, Trezor или SatoshiLabs[31].

Однако даже такие меры не смогут защитить от атак на сетевое взаимодействие, к которым относят атака Сивиллы (Sybil attack), атака «затмения» (Eclipse attack), DDoS-атака, которые являются наиболее популярными сегодня. Каждую из них рассмотрим отдельно, предлагая для них собственные способы защиты.

Атака «Сивиллы» подразумевает формирование множества фальшивых узлов, которые будут захватывать сообщения, искажать информацию, удалять её, использовать недостоверные сведения в системе репутации протокола. Тем самым, атака Сивиллы позволяет полностью ограничить взаимодействие в сети между другими пользователями, однако это естественно требует больших затрат. Если же говорить о крупной атаке Сивиллы, позволяющей овладеть контролем в крупной распределённой сети, где можно извлечь больше прибыли, то введен термин «Google атака», который подтверждает, что даже такая крупная компания, как Google, на сегодня не способна осуществить атаку Сивиллы на децентрализованную сеть Bitcoin, так как не обладает достаточными мощностями. Таким образом, можно утверждать, что хорошим

---

[28] Соколова Т. Н., Волошин И. П., Петрунин И. А. Преимущества и недостатки технологии блокчейн //Экономическая безопасность и качество. – 2019. – №. 1 (34).
[29] 6 несложных способов защититься от скрытого майнинга. The Village. 2018. URL: https://www.the-village.ru/village/business/simple/306631-mining
[30] Не блокчейном единым: как работает электронная подпись. Bloomchain URL: https://bloomchain.ru/detailed/ne-blokchejnom-edinym-kak-rabotaet-elektronnaya-podpis/
[27] Трубач Г. Г. Виды атак на блокчейн и умные контракты //75-я научная конференция студентов и аспирантов Белорусского государственного университета. – 2018. – С. 278-281.

решением избежать атаку Сивиллы является увеличение объема сети, при котором хакерам будет невыгодно осуществлять таковую. Это же в свою очередь можно сделать двумя путями: создать финансовый интерес по развертыванию самой сети или самой организации, использующая распределенный реестр, выпускать новые узлы[32]. Первый метод успешно применяется в Dashcoine, где система поощряет за майнинг и подтверждение транзакций: награда за создание нового блока распределяется по 45% между майнерами и холдерами, а остальные 10% идут на развитие сети (DGBB - Decentralized Governance by Blockchain), где любой желающий может предложить свое предложение по изменению сети[33]. Второй же хотя и является дорогостоящим, но позволяет обезопасить пользователей от атаки Сивиллы, так как уже подсчитано, что для создания дополнительных 4000 нодов требуется 20 миллионов рублей, в то время как стоимость атаки на сеть Bitcoin вырастет на не меньше, чем 19 миллиардов рублей[34].

Похожей на атаку Сивиллы является атака «затмения», когда злоумышленник так же пытается получить контроль, создавая множество фальшивых нодов, но теперь его цель – ограничение взаимодействия одного участника сети с другими, то есть атака «затмения» направлена на «окружение жертвы». Однако в виду децентрализованности сети и рандомного распределения подключения узлов между собой злоумышленник, овладевая даже 70% узлов сети, имеет вероятность меньше 1% полностью овладеть контролем над единственным узлом. Из-за схожести принципов с атакой Сивиллы можно также говорить о возможных способах защиты – увеличение числа нодов путем вознаграждения пользователей или созданием собственных узлов в сети[35].

Еще одним способом ограничить взаимодействия в сети является DoS и DDoS атаки, при которой сервер отказывается обслуживать сеть, так как существует ограничение пропускной способности по обработке запросов. В итоге таких атаках некоторые запросы игнорируются, создаются возможности для злоумышленников обмануть сеть и все алгоритмы верификации в целом. Для проведения такой атаки необходимо отправлять большое количество запросов, для чего часто используют «зомби-сеть», то есть совокупность зараженных компьютеров для отправки спама и последующего парализованности сети. Так произошло с сетью Ethereum в 2018 году, когда весь реестр пришлось перезагружать для возобновления работы, что суммарно стоило

---

[32] Глотов В. И., Михайлов Д. М. Минимизация рисков в кредитно-финансовой сфере (блокчейн) //Экономика. Налоги. Право. – 2017. – №. 6.
[33] Криптовалюта Dash (DASH): обзор монеты, курс, майнинг и перспективы. Coinpost. 2018. URL: https://coinpost.ru/p/342-chto-nuzhno-znat-o-kriptovalyute-dash#loc-44
[34] Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6.
[35] Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты //LAP Lambert Academic Publishing. – 2017.

в 15 миллионов долларов[36]. Доступным решением обезопасить систему от DoS атаки является увеличение лимитов мощностей, позволяющей обрабатывать большее количество заявок. Именно поэтому с 2015 года постоянно идут дебаты об увеличении ограничения памяти блока до 3 МБ[37], которые теоретически уменьшат возможность такой атаки до нуля, но для проведения такой реформы требуются большие затраты, к которым не многие пользователи готовы. Однако существует и другой случай Dashcoin, в которой после общего голосования в децентрализованной сети приняли увеличение блока до 2 МБ, что привлекло новых пользователей[38]. Существует и другой способ борьбы – увеличение комиссии с транзакции, из-за чего Mempool становится менее загружен, ведь атакующим невыгодно создавать множество транзакций. Однако такой метод может дискриминировать других пользователей сети, поэтому редко применяется[39].

Главная причина, из-за которой такие атаки работают, является изначальное определение протоколов проверки транзакции: Proof-of-Work (алгоритм доказательства работы для майнинга, по которому узел может работать только после нахождения хеш-функции) или Proof-of-Stake (алгоритм подтверждения доли, при котором к майнингу допускаются согласно доле владения пользователя в сети). Для первой более опасной является DoS атака, а для второй атака Сивиллы, поэтому сейчас активно работают над различными гибридными методами проверки. Одной из самых перспективной выглядит Slasher, в котором для генерации блоков используют PoW, но при этом каждый блок отдельно проверяется по PoW и PoS, что уменьшает риски вышеупомянутых атак[40]. Более того, существует и алгоритм консенсуса Proof-of-Activity, используемая в Dashcoin. Ее суть заключается в том, что каждый блок является продуктом совместного участия как PoW, так и PoS-майнера. И основной момент здесь в том, что холдеры вступают в игру лишь после того, как некоторая работа произведена PoW-участниками. Иными словами, даже если существует некий владелец 50% монет, то он не может единолично управлять созданием новых блоков, что делает маловероятной атаку 51%[41].

Более того, в виде атак на блокчейн у злоумышленников взлом методов PoW и PoS непосредственно являются целью. Отсюда логично вытекают основные виды таких атак: атака

---

[36] Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6.
[37] У кого блок больше. Из-за чего враждуют Bitcoin и Bitcoin Cash. РБК. 2018. URL: https://www.rbc.ru/crypto/news/5b1a52fd9a7947151a4f6f09
[38] Криптовалюта Dash (DASH): обзор монеты, курс, майнинг и перспективы. Coinpost. 2018. URL: https://coinpost.ru/p/342-chto-nuzhno-znat-o-kriptovalyute-dash#loc-44
[39] Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты //LAP Lambert Academic Publishing. – 2017.
[40] Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты //LAP Lambert Academic Publishing. – 2017
[41] Криптовалюта Dash (DASH): обзор монеты, курс, майнинг и перспективы. Хабр. 2015. URL: https://habr.com/ru/post/266619/

на криптографию и DoS атака на блокчейн. Раскрывая атаку на криптографию, нужно сказать, что она подразумевает непосредственный взлом алгоритмов криптографии в самом реестре, чаще всего такое встречается в работе смарт-контрактов, так как только в них хакерам возможно изменить код, а если обращать внимание на другие распределенные реестры, то само определение системы не позволяет сделать какие-либо атаки на изменение сети (открытость между пользователями и многоуровневая валидация) или они являются дорогими и труднодоступными, как атака Сивиллы[42]. Аналогично и DDoS атака на блокчейн является более масштабной и направлена на непосредственно все ветки блоков. И хотя сейчас серьезные IT-компании работают над квантовым компьютером, но риск от его создания не такой большой, ведь никакая и так крупная организация не будет его использовать в частных целях обогащения. Кроме того, сейчас активно создаются новые квантовые и постквантовые виды криптографии, одни уже используются в России современным квантовым компьютером[43], а другие находятся на стадии разработки у компании Google[44]. Более того, в 2014 году была создана международная финансово-технологическая компания R3 CEV LLC, которая тщательно исследует возможности технологии блокчейн и его опасности для финансового и банковского сектора, причем такие общесистемные атаки рассматриваются в первую очередь, ведь если система не способная выдержать их, то она некачественная и не будет воплощена в жизнь. Поэтому можно смело утверждать, что такие риски на данный момент не представляют большой угрозы, ведь уже изначально система распределенных реестров на сегодняшний день создается, не допуская их[45].

Более серьезной проблемой являются различные атаки двойной траты, в том числе и атака 51% и атака Финни. Каждая из них обладает своими особенностями, поэтому требует отдельного рассмотрения.

Вышеупомянутая атака 51% основана на том, что группа злоумышленников может овладеть более 51% всех вычислительных мощностей узлов, что дает ей право вето на определенные транзакции в децентрализованной системе, преимущество в создании новых блоков. Это осуществляется тем, что злоумышленник создает более сложное ветвление блоков с нужными ему транзакциями, после чего раскрывает эту секретную ветку в сеть, тогда все транзакции, не входящие в нее, будут аннулированы.

Данный вид атаки можно избежать несколькими способами. Во-первых, ведение глубокого мониторинга сети и транзакций, которые могут быть основаны на Cloud Federation –

---

[42] Что такое атака информационного затмения? Binance Academy URL: https://www.binance.vision/ru/security/what-is-an-eclipse-attack

[43] Физики из России создали первый в мире квантовый блокчейн. РИА Новости. 2017. URL: https://ria.ru/20170526/1495086879.html

[44] Постквантовая криптография и закат RSA — реальная угроза или мнимое будущее? Хабр. 2017. URL: https://habr.com/ru/company/neobit/blog/332942/

[45] Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6.

децентрализованная платформа по обмену информации между пользователями блокчейна, что обеспечивает открытость сделок и повышает доверие участников сети друг к другу[46]. Во-вторых, существуют различные методы их обработки (Slasher и Proof-of-Activity), которые уменьшают шансы успеха такой атаки[47]. Дополнительные валидации с использованием множества блоков, что только ограничивает возможности проведения такой атаки[48]. Однако такие методы не работают для малых блокчейнов, например, известен случай, как в 2013 году мощность пула BTC Guild превысила 50% хэшрейта сети, но даже тогда компания не использовала свои мощности для двойной траты, а продолжила делать 6 блоков подряд, поэтому в сети Биткоин теперь считается, что транзакция подтверждена, если создано выше 6 блоков сверху[49].

Более реализуемой считается атака Финни, которая включает в себя следующие действия: атакующий перед совершением транзакции создает параллельный блок, который в итоге публикует в сеть, если майнеры продолжат эту фальшивую ветвь, то продавец ничего не получит, а злоумышленник сможет использовать свои средства второй раз. В этом случае правильной защитой будет ожидания определенного подтверждения транзакции, что уменьшает вероятность такой атаки, но не полностью (может произойти атака затмения»). Если же говорить о масштабной защите от атаки Финни, то здесь необходим постоянный мониторинг сети и бдительность пользователей сети (выше приведен способ мониторинга – Cloud Federation), а также смогут помочь различные методы обработки транзакций (Slasher и Proof-of-Activity) и дополнительные их валидации[50].

Однако на сегодняшний день для распределенных реестров наибольший интерес представляют атаки на смарт-контракты, которые позволяют осуществлять различные транзакции с активами по написанному коду, из-за чего на них высокий спрос и требование к безопасности. Особенностью смарт-контрактов является то, что они не способны обрабатывать исключения, то есть при генерации исключения выполнение кода прекращаются, а все изменения отменяются, при этом раньше сжигался весь газ (плата за выполнение), но в новой версии языка Solidity такого больше нет, что сделало смарт-контракты более востребованными. Другой особенностью является синхронный вызов других смарт-контракта, причем можно наследовать их исключения, что позволяет делать несколько финансовых операций одновременно с высоким

---

[46] Ferdous M. S. et al. Decentralised runtime monitoring for access control systems in cloud federations //2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). – IEEE, 2017. – С. 2632-2633.
[47] Криптовалюта Dash (DASH): обзор монеты, курс, майнинг и перспективы. Хабр. 2015. URL: https://habr.com/ru/post/266619/
[48] Трубач Г. Г. Виды атак на блокчейн и умные контракты //75-я научная конференция студентов и аспирантов Белорусского государственного университета. – 2018. – С. 278-281.
[49] Суханов Е. Э., Штанг К. С., Алешко Р. А. Технология блокчейн: вызовы, ограничения, варианты совершенствования //Синергия наук. – 2017. – №. 14. – С. 540-546.
[46] Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты //LAP Lambert Academic Publishing. – 2017.

уровнем надежности[51]. Тем не менее, у того алгоритма, как смарт-контракт, существует модельный риск – риск того, что код изначально не предполагал каких-то условий, из-за чего весь контракт работает неправильно и несет убытки пользователю. Этот риск связан с различными атаками злоумышленников, о которых пойдет речь далее.

Из-за свойств смарт-контракта и среды блокчейн следует, что пользователь возможно будет вызывать через смарт-контракт другой, записанный злоумышленником алгоритм, причем пользователь не способен как-либо изменить его. Единственной защитой от этого является внимательность с использованием контрактов, которые будут расположены в открытом доступе на Github, то есть сам агент должен изначально убедиться в качестве смарт-контракта перед его активацией[52].

Другой угрозой является то, что вызывающий код ждет конца выполнения вызываемого кода до того, как продолжит свое выполнение. Такая особенность может стать причиной использования вызываемым контрактом промежуточного состояния вызывающего контракта. Такая ситуация не всегда очевидна при разработке, если не берутся во внимание возможные мошеннические действия со стороны вызываемого контракта. К тому же уже известны случаи использования такой уязвимости, когда произошел хардфорк Ethereum, а убытки оценивались в 50 миллионов долларов[53]. Поэтому следует проверять не только использованный один смарт-контракт, но и все те, которые он вызывает в процессе.

Если же обращать внимание на криптографию и возможность хранения у смарт-контракта приватной информации, то существует риск атаки на криптографию контракта. Естественной защитой будет использование других криптографических методов, например, современных гомоморфных методов криптографии, которые уже тестируются R3 в проекте Corda для финансового и банковского сектора[54], или других открытых смарт-контрактов, которые никак не затрагивают конфиденциальную информацию пользователя[55].

Еще одной уязвимостью является невозможность определения уровня состояния контракта, в отличие от транзакции, которая подтверждалась после процесса сборки блока, в смарт-контракте пользователь не может быть уверен, что транзакция будет выполнена при том же состоянии контракта, в котором он находился на момент отправки. Такое может произойти,

---

[51] Алиев И. А. Уязвимости смарт-контрактов блокчейн-платформы Ethereum //Научные записки молодых исследователей. – 2019. – №. 3.

[48] Алиев И. А. Уязвимости смарт-контрактов блокчейн-платформы Ethereum //Научные записки молодых исследователей. – 2019. – №. 3.

[53] Какие уязвимости смарт-контрактов бывают и как с ними бороться? 2018. URL: https://crypto-fox.ru/faq/uyazvimosti-smart-kontraktov-i-kak-s-nimi-borotsya/

[54] Гомоморфное шифрование и смарт-контракты — идеальное сочетание. BitNovosti. 2016. URL: https://bitnovosti.com/2016/05/19/homomorphic-encryption-and-smart-contracts/

[55] Алиев И. А. Уязвимости смарт-контрактов блокчейн-платформы Ethereum //Научные записки молодых исследователей. – 2019. – №. 3.

поскольку другие транзакции в том же блоке изменили состояние контракта. Это непосредственно является большой проблемой в использовании смарт-контрактов, но существует единственный выход – ручная проверка транзакций, включенных в смарт-контракт[56].

Но самой большой проблемой является невозможность изменения кода контракта. Это условие приводит к тому, что злоумышленники уже изначально знают код и могут искать ошибки в нем. Подобный случай произошел со смарт-контрактами с мультиподписью от компании Parity, когда одна группа злоумышленников в 2017 году смогла похитить с кошельков компании 30 миллионов долларов, а позже хакер Devops199 так же обнаружил этот критический баг и поставил на самоуничтожение смарт-контракты, что повлекло блокировку средств пользователей на более, чем 280 миллионов долларов[57].

Вышеупомянутые уязвимости ставят под вопрос полноценное использование смарт-контрактов, ведь, согласно Oyente, из выборки в 19366 контрактов около половины, 8833 контракта, обладали хотя бы одной из них[58]. Но высокая удобность для финансовых операций и проведения ICO влекут за собой большой спрос, поэтому предлагается использовать общепринятые меры по уменьшению таких рисков. Так как смарт-контракт не изменяется, то его изначальный код должен быть проверен различными способами, к которым относится фаззинг и стресс-тестинг. Фаззинг — это методика тестирования программного обеспечения, суть которой заключается в автоматизированном обнаружении ошибок реализации путем отправки заведомо неверных данных и анализе реакции программы на них, что позволяет автоматизировано тестировать код и собрать общее представление о его защищенности[59]. Но, на самом деле, фаззинг является частным примером стресс-тестинга, когда в модель вставляют некоторые шоки и смотрят, как она себя ведет под их воздействием, что постепенно позволяет улучшить качество результатов.

Подводя итог, следует сказать о том, что существуют различные виды кибератак, но против них существуют различные способы борьбы, в том числе улучшение цифровой грамотности и бдительности пользователей, увеличение масштабов распределенного реестра с качественным мониторингом сети и валидации транзакций и дополнительная проверка качества смарт-контрактов на их многочисленные уязвимости. И хотя многие методы уменьшения рисков могут обходиться дорого, но только с созданием высокого уровня инфраструктуры реестра будут возможны последующие действия по его внедрению в финансовый сектор.

---

[51] Алиев И. А. Уязвимости смарт-контрактов блокчейн-платформы Ethereum //Научные записки молодых исследователей. – 2019. – №. 3.

[57] Случайная активация бага в Ethereum-кошельке Parity заблокировала $280 000 000. Хакер. 2017. URL: https://xakep.ru/2017/11/08/parity-mess/

[58] Luu L. et al. Making smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM; 2016:254–269.

[59] Фаззинг — важный этап безопасной разработки. Хабр. 2019. URL: https://habr.com/ru/company/dsec/blog/450734/

Манипулирование

Рынок цифровых активов постоянно развивается, но несмотря на активную интеграцию распределённых реестров в работу крупных организаций, активы крипторынка отличаются низкой ликвидностью и высокой волатильностью. Это связано с тем, что данная отрасль всё ещё не до конца изучена инвесторами и им может быть сложно управлять цифровыми активами. Не каждый брокер или финансовое учреждение берётся за взаимодействие с блокчейном и его инструментами, так как данная сфера влечёт за собой высокие риски. Более того, виртуальные активы всё ещё не считаются государственными органами достаточно надёжными, а также ещё не создан прочный правовой фундамент для работы на данном рынке. Всё это влечет за собой нестабильность рынка, а это также приводит к низкой ликвидности и высокой волатильности. В свою очередь эти факторы создают возможности для манипулирования криптоактивами.

Под манипулированием рынком чаще всего подразумевают умышленные действия участников рынка, имеющие целью ввести в заблуждение остальных участников торгов, в результате которых рыночные цены искусственно поддерживаются на выгодном для отдельно взятых участников рынка уровне. Обычно выделяют три вида ценовых манипуляций: повышение, снижение и стабилизация цен, также манипуляции на крипторынке можно классифицировать, выделив несколько часто встречающихся видов:

1) **Манипуляция, в основе которой лежат действия (action-based manipulation)**

В этом виде манипуляторы (обычно высокоранговые сотрудники компании) предпринимают какие-либо действия (например, закрывают производство), что влияет на цену актива. Ярким примером такой манипуляции можно назвать ситуацию с ICO немецкой компании Savedroid, создатели проекта которой 18 апреля 2018 года объявили проект закрытым, но на следующий день опровергли закрытие, назвав данную ситуацию «шуткой» и призвав инвесторов более внимательно относиться к своим вложениям, так как на рынках часто происходят скамы[60]. Данный кейс является примером того, как действия со стороны эмитента ICO сильно могут повлиять на рыночную ситуацию с токенами, ведь на фоне подобных новостей владельцев токенов может охватить паника, и они будут стараться продать их практически по любой цене, что, в свою очередь, может привести к обратному выкупу токенов по бросовой цене. Если такое произойдет, то можно утверждать о ценовой манипуляции над токеном посредством действий глав компании.

2) **Манипуляция, в основе которой лежит информация (information-base manipulation)**

[60] Экзит-скам, которого не было? Немецкий проект Savedroid преподал жестокий урок ICO-инвесторам. Forklog. 2018. URL: https://forklog.com/ekzit-skam-kotorogo-ne-bylo-nemetskij-proekt-savedroid-prepodal-zhestokij-urok-ico-investoram/

В этом виде манипуляторы распространяют слухи или неверную информацию, чтобы повлиять на цены активов. Можно выделить несколько ее типов:

a) **Манипуляция, основанная на инсайдерской информации (insider trading).** Сотрудники компании или любые другие лица, имеющие доступ к внутренней (инсайдерской) информации, используют её с целью получения собственных выгод. Зная заранее о важных решениях, манипулятор, обычно через подконтрольных участников рынка, покупает или распродает актив (в зависимости от положительного/отрицательного воздействия инсайда).

b) **Манипуляция информационно-финансовыми показателями**. На фондовом рынке это означает, что манипулятор умышленно искажает информацию, в том числе представленную в финансовой отчетности, затем, чтобы создать более благоприятное представление о состоянии компании и повлиять за счёт этого на курс акций.

Примером инсайдерской торговли на рынке криптоактивов можно назвать ситуацию с листингом Bitcoin Cash крупной компанией Coinbase в декабре 2017 года. За пару дней до анонса новости объёмы сделок и цена данного криптоактива резко увеличились (за 2 дня в 146%)[61]. В связи с этим, на Coinbase было подано сразу два коллективных иска — за инсайдерскую торговлю при листинге Bitcoin Cash и за нарушение закона штата Калифорния о невостребованном имуществе[62]. Описать работу манипулирования информационно-финансовыми показателями на цифровом рынке можно через пример биотехнической компании Riot Blockchain, цена акции которой увеличились с $4,5 до более $38,6 после того, как компания изменила своё название и добавила в конце слово «blockchain» (данную ситуацию можно сравнить с действиями фирм во время увеличения пузыря доткомов)[63]. В результате такой манипуляции инвесторы подали против Riot Blockchain три коллективных иска, обвинив фирму в «нарушении законов о ценных бумагах, манипулировании ценами на акции, а также предоставлении ложной и вводящей в заблуждение информации». Описанные выше кейсы являются примерами манипулирования, которое происходит не только на крипторынках – подобные случаи распространены на реальном фондовом рынке и регулируются правоохранительными органами. В некоторых странах, например, в США, данные случаи подходят под уже имеющуюся юрисдикцию и контролируются органами надзора за ценными бумагами.

3) Pump&Dump (Ramping)

Данный вид манипулирования ценами активов крайне распространен на крипторынке в силу

---

[61] Я знаю, что вы сделали прошлой ночью. DeCenter. 2017. URL: https://decenter.org/ru/ya-znayu-chto-vy-sdelali-proshloy-nochyu

[62] Coinbase Hit with SECOND Class Action Lawsuit for Violating ‘Unclaimed Property" Laws. Bitcoinist. 2018. URL: https://bitcoinist.com/coinbase-hit-second-class-action-lawsuit-violating-unclaimed-property-laws/

[63] Инвесторы подали три коллективных иска против Riot Blockchain. Forklog. 2018. URL: https://forklog.com/investory-podali-tri-kollektivnyh-iska-protiv-riot-blockchain/

сильной сосредоточенности большого пула активов в руках маленькой группы. Людей с крупным запасом криптоактивов называют «китами»: 20% всех криптовалют на планете находятся на 117 кошельках, владельцы которых и являются теми самыми «китами»[64]. Из-за этого крупные сделки, совершаемые данными инвесторами, могут сильно пошатнуть рынок в ту или иную сторону (в силу волатильности рынка). Но Pump&Dump характерен не только для крупных игроков, но и для объединений менее крупных владельцев активов. Pump&Dump заключается в том, что манипуляторы активно раздувают цены на активы, после чего создают в информационном пространстве инфоповод, обычно агрессивно тиражируемый, зачастую в несколько этапов и на различных информационных ресурсах. Затем, после повышения цен, они привлекают других инвесторов, чтобы купить акции в момент их ценового пика. Мошенники быстро продают токены по высокой цене, чтобы получить прибыль, после чего эти же токены буквально через несколько минут резко падают в цене, оставляя вторую волну инвесторов с убытками[65].

Достаточно часто пампы проводятся через группы в мессенджерах (очень много подобных каналов в Telegram). Манипуляторы покупают монеты по низкой цене (небольшими частями, чтобы резко не влиять на курс), затем искусственно повышают цену путем совершения сделок между счетами-марионетками участников памп-каналов. Цена монеты растёт, параллельно с этим по различным инфоканалам (обычно это чат биржи) участники пампа пытаются распространить ложную информацию об активе на фоне его роста. Это заставляет сторонних трейдеров ее купить, после чего манипуляторы продают ее с прибылью, обваливая цену. В качестве активов обычно используются низколиквидные альткоины с низкой капитализацией, а жертвами подобных действий нередко становятся и сами участники памп-каналов, которые не успели/не смогли сбросить актив вовремя[66].

4) Манипуляция, в основе которой лежат торги (trade-based manipulation)

Их можно разделить на несколько категорий сговора и/или практик манипулирования, согласно Глобальному кодексу валютного рынка[67]:

- практики, создающие ложное впечатление о рыночной цене, глубине или ликвидности рынка: фиктивные сделки, спаривание ордеров;

---

[64] Как биткоин-киты манипулируют крипторынком. Prometheus. 2018. URL: https://prometheus.ru/kak-bitkoin-kity-manipuliruyut-kriptorynkom/

[65] BI Prime 'Market manipulation 101': 'Wolf of Wall Street'-style 'pump and dump' scams plague cryptocurrency markets. Business Insider. 2017. URL: https://www.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11

[66] BI Prime 'Market manipulation 101': 'Wolf of Wall Street'-style 'pump and dump' scams plague cryptocurrency markets. Business Insider. 2017. URL: https://www.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11

[67] Глобальный кодекс валютного рынка. Центральный банк Российской Федерации URL: https://www.cbr.ru/Content/Document/File/32852/Global_code_currency_market.pdf

- ввод бида (bid) или аска/оффера (ask/offer) с намерением их отзыва до совершения сделки: спуфинг, флешинг, лееринг. Преимущественно используются в высокочастотной торговле.

Фиктивная сделка (wash trades). Операция, в которой нет изменения собственника актива или производного контракта, другими словами, манипулятор покупает и продает свои же ордера. Цель данного способа манипулирования состоит в том, чтобы создать видимость активности на рынке, искусственно завысив объёмы торгов и цены.

Двойная сделка/спаривание ордеров (matched orders). Разновидность фиктивной сделки. Сделки, в которых и ордера на покупку, и ордера на продажу вводятся в одно и то же время с теми же самыми ценой и количеством различными, но тайно вошедшими в сговор сторонами или между разными счетами (так называемые счета-марионетки) одного и того же манипулятора. Зачастую проводится на нескольких биржах, что усложняет их нахождение.

Спуфинг или «раскрашивание ленты» (spoofing/painting the tape). Выставление манипулятором большого количества заявок на покупку/продажу активов без намерения совершать сделки и отмена этих заявок до исполнения. Целью является сбор информации о спросе и предложении, привлечение внимания участников рынка, искусственное создание благоприятного впечатления о торговой активности или ценовом движении актива.

Флешинг (flashing). Кратковременный показ котировок на рынке без намерения заключить сделку с целью создать ложное представление о действительных рыночных ценах.

Лееринг (layering). Выставление манипулятором многочисленных заявок на покупку/продажу актива на различных уровнях с намерением их последующей отмены до исполнения с целью влияния на цену и ликвидность торгового инструмента.

Некоторые криптобиржи используют подобные практики манипулирования для продвижения цены криптоактивов. Недавнее исследование[68] подтвердило факт Wash Sale биткоина двумя ботами (Willy и Markus) на бирже MtGox в 2013 году. Оба бота совершали фиктивные сделки объемом порядка 100 BTC в час с небольшими временными интервалами, не обладая при этом таким объёмом криптовалюты. В дни активной работы ботов наблюдалась повышенная активность торгов и на других биржах, а курс главной криптовалюты рос.

Некоторые исследования[69] также указывают на то, что более 90% объёмов торгов на крупнейших криптобиржах могут быть сфальсифицированы. Если предположить, что приведенные выше примеры с торговыми ботами — лишь малая часть всех действий с криптоактивами, то можно сделать вывод о том, что криптовалютная торговля на текущий

---

[68] Price Manipulation in the Bitcoin Ecosystem. WEIS. 2017. URL: https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_21.pdf

[69] Исследование: OKEx и другие криптовалютные биржи фальсифицируют торговые объемы. Forklog. 2018. URL: https://forklog.com/issledovanie-okex-i-drugie-kriptovalyutnye-birzhi-falsifitsiruyut-torgovye-obemy/

момент является крайне манипулятивной. Это создает серьёзное препятствие развитию эффективного рынка криптоактивов, вносит сложности в его анализ, но, с другой стороны, обеспечивает сверхволатильность и сверхдоходность (сверхубыточность) торговых операций.

Противодействие манипулированию

В первую очередь, криптобиржам следует постоянно отслеживать возможные манипуляции. На данный момент финтехкомпании уже готовы предложить ряд инструментов мониторинга. Так, израильская компания Nice Actimize разработала инструмент Cloud Markets Surveillance (CMS). Запатентованный корреляционный механизм NICE Actimize облегчает аналитику задач путем поиска миллиардов записей и автоматической корреляции и анализа торговых и коммуникационных данных (голос, электронная почта, чат, обмен мгновенными сообщениями), чтобы соединить всё вместе, решения поставляются на единой облачной платформе.[70]

Вслед за введением этого механизма на бирже Poloniex наблюдалось резкое падение торгов, что подтверждает их завышенные до этого объёмы. Также исключение низколиквидных криптовалют на этой бирже могло сыграть свою роль в борьбе с манипулированием, ведь такие активы часто используются для схем P&D[71].

У биржи Bitstamp, например, существовал собственный движок по сопоставлению заявок, однако сейчас она перешла к новой трейдинговой системе TRADExpress, созданной компанией Irisium, которая выполняет все те же функции, однако скорость сопоставления заявок на Bitstamp повысилась в 1250 раз, а пропускная способность – в 400 раз. Решения от Irisium для выявления подозрительной активности на рынке используют достаточно известные компании, включая сингапурскую биржу деривативов Asia Pacific Exchange Pte Ltd (APEX).[72]

Вводит меры и такая биржа как Bittrex. Биржа повысит требуемый минимум к объему торговли. Минимальная сумма увеличится с 50 000 сатоши (1 сатоши = 1/100 000 000 BTC), что составляет примерно 4 доллара, до 100 000 сатоши или около 8 долларов. «Несмотря на то, что изменения, несомненно, будут разочаровывать некоторых пользователей, которые привыкли иметь полную свободу отправлять микро-сделки по своему усмотрению, для многих это, безусловно, положительный признак того, что одна из наиболее крупных бирж заботится о защите своих пользователей от манипуляционных действий.»[73]

---

[70] Cloud-based Markets Surveillance. Nice Actimize. 2019 URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://info.nice.com/rs/338-EJP-431/images/NICE_Actimize_Markets_Surveillance_-_Brochure.pdf&ved=2ahUKEwjSifeYq5LoAhVw2aYKHe7_C3MQFjAGegQICRAB&usg=AOvVaw2ViFnUb__oM_JZMWTMPmm7&cshid=1583926959339

[71] Биткоин-биржа Poloniex исключит из листинга восемь криптовалют. Forklog. 2018. URL: https://forklog.com/bitkoin-birzha-poloniex-isklyuchit-iz-listinga-vosem-kriptovalyut/

[72] Биткоин-биржа Bitstamp задействует технологии для противодействия манипуляциям рынком. Forklog. 2018. URL: https://forklog.com/bitkoin-birzha-bitstamp-zadejstvuet-tehnologii-dlya-protivodejstviya-manipulyatsiyam-rynkom/

[73] Bittrex Takes Steps to Prevent Price Manipulation on its Platform. Finance Magnates. 2017. URL: https://www.financemagnates.com/cryptocurrency/exchange/bittrex-takes-steps-prevent-price-manipulation-platform/

В контексте правового регулирования рынка по снижению манипулирования криптоактивами необходимо сказать, что только с введением определений каждого вида токена на законодательном уровне будет возможна проработка государственной борьбы с мошенничеством. Нашей командой был проведен анализ имеющегося на данный момент законодательства США, на основе которого мы вывели предложение для уменьшения манипулирования на крипторынках. Мы считаем, что одним действенным методом борьбы с манипулированием может стать принятие аналога закона Додда-Франка[74], способствующего уменьшению количества незаконных операций на фондовом рынке, который будет стимулировать сообщать о готовящихся манипуляциях.

Одним из положений закона Додда-Франка является возможность поощрения осведомителей, направляющих регулятору информацию о готовящихся незаконных операция. Такая мера может быть применена и в контексте регулирования цифровых активов. Так, большинство манипуляций типа Pump&Dump происходят крупными анонимными объединениями манипуляторов, которые начинают раздувать цены на криптоактивы в определённый момент. Если осведомитель, интегрированный в данное анонимное сообщество, за определённое поощрение (возможно, превышающее гипотетическую прибыль от данного манипулирования) будет сообщать в правоохранительные органы о планируемой манипуляции, то регулятор биржи сможет предотвратить чрезмерное раздувание или падение цены.

Данный тип регулирования может быть реализован только после утверждения на юридическом уровне всех видов возможных манипуляций над каждым определенным видом криптоактива и после более детальной проработки данной системы в контексте как работы с осведомителем, так и взаимодействия с криптобиржами.

Заключение

В настоящий момент технология распределенных реестров имеет некоторые уязвимости, которые могут быть использованы для проведения мошеннических действий. Основными направлениями для злоумышленников могут являться компрометация данных в распределенных реестрах в силу неполной способности технологии контролировать несанкционированные изменения в реальном мире, отмывание денег через проекты на основе распределенных реестров, проведение кибератак и манипулирование рынками цифровых активов. Среди ключевых решений, которые могут устранить эти уязвимости, можно выделить развитие связанных технологий передачи и защиты информации от компрометации, например, Интернета вещей и RFID, а также технологий разработки ПО в целях повышения устойчивости к кибератакам.

---

[74] Закон Додда-Фрэнка, краткое содержание. Smart Lab. 2017. URL:https://smart-lab.ru/finansoviy-slovar/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%94%D0%BE%D0%B4%D0%B4%D0%B0-%D0%A4%D1%80%D1%8D%D0%BD%D0%BA%D0%B0

Примером такой технологии может стать фаззинг. С другой стороны, для противодействия мошенническим действиям и создания условий для успешного развития технологии необходимо принятие профильного законодательства. Здесь стоит ориентироваться на примеры оригинальных специально созданных нормативных актов, принятых, например, в Сингапуре, Швейцарии, Мальте и прочих государствах. Эти решения могут помочь технологии избавиться от уязвимостей и стать очень перспективной для применения во многих отраслях экономики.

Список источников:

1. «НорНикель» станет первым эмитентом платформы для токенизации промышленных активов Atomyze. Норильский никель. 2020. URL: https://www.nornickel.ru/news-and-media/press-releases-and-news/nornikel-stanet-pervym-emitentom-platformy-dlya-tokenizatsii-promyshlennykh-aktivov-atomyze/
2. Steel But Smart. 2020. URL: https://www.steelbutsmart.com
3. Как токенизация и цифровизация активов помогут вернуть «мертвый капитал» в экономику. IBM. 2020 URL: https://www.ibm.com/blogs/ibm-russia/2020/02/asset-tokenization-atomyze/
4. iSTOX. 2020. URL: https://istox.com
5. Центробанк Сингапура выдал лицензию платформе по выпуску security-токенов. Bloomchain. 2020. URL: https://bloomchain.ru/newsfeed/tsentrobank-singapura-vydal-litsenziyu-platforme-po-vypusku-security-tokenov/
6. Центробанк одобрил блокчейн-проект «Норникеля». РБК. 2020 URL: https://www.rbc.ru/business/17/02/2020/5e469c089a794755bbd0989c
7. Bloomberg рассказал подробности блокчейн-проекта Потанина // Ведомости. 2020 URL: https://www.vedomosti.ru/technology/news/2020/02/25/823756-podrobnosti-blokchein-proekta-potanina
8. Российская торговая платформа Atomyze на блокчейне запущена в тестовом режиме. SharesPro. 2020. URL: https://sharespro.ru/news/5694-torgovaya-platforma-atomyze
9. Аксаков назвал дату принятия закона о криптовалютах. РБК. 2020. URL: https://www.rbc.ru/crypto/news/5e1c769c9a79475f3356cc26
10. В марте Госдумой может быть принят закон о цифровых активах. Версия. 2020. URL: https://versia.ru/gosduma-mozhet-v-marte-prinyat-zakon-o-cifrovyx-finansovyx-aktivax
11. Karl Wüst, Arthur Gervais. Do you need a Blockchain? IACR. 2017. URL: https://eprint.iacr.org/2017/375.pdf
12. Обзор технологий и стандартов RFID систем. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича. 2018. URL: http://www.sut.ru/doci/nauka/review/20185/1-11.pdf
13. WWF использует блокчейн для борьбы с браконьерством. Bit Journal. 2018. URL: https://bitjournal.media/29-01-2018/wwf-ispolzuet-blokchejn-dlya-borby-s-brakonerstvom/
14. Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud. The Wall Street Journal. 2018. URL: https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115
15. Как я потерял 1000 $ на ICO. Тинькофф Журнал. 2019. URL: https://journal.tinkoff.ru/icofail/
16. Регулятор Сингапура представил руководство по ICO. vc.ru. 2017. URL: https://vc.ru/crypto/29089-regulyator-singapura-predstavil-rukovodstvo-po-ico
17. Криптоактивы и блокчейн в сингапуре. IQ Decision. 2020. URL: https://iqdecision.com/kriptoaktivy-i-blokchejn-v-singapure/

18. FATF решила ужесточить контроль над биткоин-индустрией // Forklog. 2019. URL: https://forklog.com/fatf-reshila-uzhestochit-kontrol-nad-bitkoin-industriej-nesmotrya-na-predosterezheniya-ekspertov-o-neblagopriyatnyh-posledstviyah/
19. Ждет ли Monero, Dash, Zcash и другие анонимные криптовалюты массовый делистинг, и к чему готовиться? Forklog. 2019. URL: https://forklog.com/zhdet-li-monero-dash-zcash-i-drugie-anonimnye-kriptovalyuty-massovyj-delisting-i-k-chemu-gotovitsya/
20. Тоже плачут. Как криптобиржи противостоят преступникам. РБК. 2019. URL: https://www.rbc.ru/crypto/news/5d9dadf79a79472106eec0a1
21. Юрисдикция Мальты – одно из лучших мест для запуска ICO и развития криптобизнеса. International Wealth. 2018. URL: https://internationalwealth.info/cryptocurrency/malta-one-of-the-best-places-for-launching-ico-and-developing-crypto/
22. New money-laundering rules change everything for cryptocurrency exchanges. MIT Technology Review. 2019. URL: https://www.technologyreview.com/s/614164/new-money-laundering-rules-change-everything-for-cryptocurrency-exchanges/
23. Travel Rule Information Sharing Architecture for Virtual Asset Service Providers (TRISA). August 22, 2019. Version 4. URL: https://ciphertrace.com/wp-content/uploads/2019/08/TRISA-Enabling-FATF-Travel-Rule-V4.pdf
24. CipherTrace unveils open source solution for crypto Travel Rule compliance TRISA. Tokenpost. 2019. URL: https://tokenpost.com/CipherTrace-unveils-open-source-solution-for-crypto-Travel-Rule-compliance-TRISA-3369
25. Анонимность в сети Биткоин. Мифы и реальность. Cryptor. 2017 URL: https://cryptor.net/bitkoin-dlya-chaynikov/anonimnost-v-seti-bitkoin-mify-i-realnost
26. The FBI revealed how it found the Silk Road servers. Was the search legal? Quartz. 2014. URL: https://qz.com/261961/the-fbi-revealed-how-it-found-the-silk-road-servers-was-the-search-legal/
27. Анонимность криптовалют под ударом. БрокерТрибунал. 2020. URL: https://brokertribunal.com/blog/post/anonimnost-kriptovalyut-pod-udarom
28. Соколова Т. Н., Волошин И. П., Петрунин И. А. Преимущества и недостатки технологии блокчейн //Экономическая безопасность и качество. – 2019. – №. 1 (34).
29. 6 несложных способов защититься от скрытого майнинга. The Village. 2018. URL: https://www.the-village.ru/village/business/simple/306631-mining
30. Не блокчейном единым: как работает электронная подпись. Bloomchain URL: https://bloomchain.ru/detailed/ne-blokchejnom-edinym-kak-rabotaet-elektronnaya-podpis/
31. Глотов В. И., Михайлов Д. М. Минимизация рисков в кредитно-финансовой сфере (блокчейн) //Экономика. Налоги. Право. – 2017. – №. 6.
32. Криптовалюта Dash (DASH): обзор монеты, курс, майнинг и перспективы. Coinpost. 2018. URL: https://coinpost.ru/p/342-chto-nuzhno-znat-o-kriptovalyute-dash#loc-44
33. Ferdous M. S. et al. Decentralised runtime monitoring for access control systems in cloud federations //2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). – IEEE, 2017. – С. 2632-2633.
34. Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6.
35. Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты //LAP Lambert Academic Publishing. – 2017.
36. У кого блок больше. Из-за чего враждуют Bitcoin и Bitcoin Cash. РБК. 2018. URL: https://www.rbc.ru/crypto/news/5b1a52fd9a7947151a4f6f09
37. Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты //LAP Lambert Academic Publishing. – 2017.
38. Криптовалюта Dash (DASH): обзор монеты, курс, майнинг и перспективы. Хабр. 2015. URL: https://habr.com/ru/post/266619/

39. Что такое атака информационного затмения? Binance Academy. 2020. URL: https://www.binance.vision/ru/security/what-is-an-eclipse-attack
40. Физики из России создали первый в мире квантовый блокчейн. РИА Новости. 2017. URL: https://ria.ru/20170526/1495086879.html
41. Постквантовая криптография и закат RSA — реальная угроза или мнимое будущее? Хабр. 2017. URL: https://habr.com/ru/company/neobit/blog/332942/
42. Трубач Г. Г. Виды атак на блокчейн и умные контракты //75-я научная конференция студентов и аспирантов Белорусского государственного университета. – 2018. – С. 278-281.
43. Суханов Е. Э., Штанг К. С., Алешко Р. А. Технология блокчейн: вызовы, ограничения, варианты совершенствования //Синергия наук. – 2017. – №. 14. – С. 540-546.
44. Алиев И. А. Уязвимости смарт-контрактов блокчейн-платформы Ethereum //Научные записки молодых исследователей. – 2019. – №. 3.
45. Какие уязвимости смарт-контрактов бывают и как с ними бороться? 2018. URL: https://crypto-fox.ru/faq/uyazvimosti-smart-kontraktov-i-kak-s-nimi-borotsya/
46. Гомоморфное шифрование и смарт-контракты — идеальное сочетание. BitNovosti. 2016. URL: https://bitnovosti.com/2016/05/19/homomorphic-encryption-and-smart-contracts/
47. Случайная активация бага в Ethereum-кошельке Parity заблокировала $280 000 000. Хакер. 2017. URL: https://xakep.ru/2017/11/08/parity-mess/
48. Luu L. et al. Making smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM; 2016:254–269.
49. Фаззинг — важный этап безопасной разработки. Хабр. 2019. URL: https://habr.com/ru/company/dsec/blog/450734/
50. Опасный токен: от ICO до тюрьмы — один шаг. Forbes. 2017. URL: https://www.forbes.ru/kompanii/349049-opasnyy-token-ot-ico-do-tyurmy-odin-shag
51. 80% прошлогодних ICO оказались обманом. РБК. 2018 URL: https://www.rbc.ru/crypto/news/5b4882f49a794762638113e6
52. Собрать необходимую сумму на ICO смогли лишь 8% российских проектов. РБК. 2017. URL: https://www.rbc.ru/rbcfreenews/5a3bc43c9a7947a7a926b8fd
53. Экзит-скам, которого не было? Немецкий проект Savedroid преподал жестокий урок ICO-инвесторам. Forklog. 2018. URL: https://forklog.com/ekzit-skam-kotorogo-ne-bylo-nemetskij-proekt-savedroid-prepodal-zhestokij-urok-ico-investoram/
54. Я знаю, что вы сделали прошлой ночью. DeCenter. 2017. URL: https://decenter.org/ru/ya-znayu-chto-vy-sdelali-proshloy-nochyu
55. Coinbase Hit with SECOND Class Action Lawsuit for Violating ‘Unclaimed Property" Laws. Bitcoinist. 2018. URL: https://bitcoinist.com/coinbase-hit-second-class-action-lawsuit-violating-unclaimed-property-laws/
56. Инвесторы подали три коллективных иска против Riot Blockchain. Forklog. 2018. URL: https://forklog.com/investory-podali-tri-kollektivnyh-iska-protiv-riot-blockchain/
57. Как биткоин-киты манипулируют крипторынком. Prometheus. 2018. URL: https://prometheus.ru/kak-bitkoin-kity-manipuliruyut-kriptorynkom/
58. BI Prime 'Market manipulation 101': 'Wolf of Wall Street'-style 'pump and dump' scams plague cryptocurrency markets. Business Insider. 2017. URL: https://www.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11
59. Глобальный кодекс валютного рынка. Центральный банк Российской Федерации URL: https://www.cbr.ru/Content/Document/File/32852/Global_code_currency_market.pdf
60. Price Manipulation in the Bitcoin Ecosystem. WEIS. 2017. URL: https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_21.pdf
61. Исследование: OKEx и другие криптовалютные биржи фальсифицируют торговые объемы. Forklog. 2018. URL: https://forklog.com/issledovanie-okex-i-drugie-kriptovalyutnye-birzhi-falsifitsiruyut-torgovye-obemy/

62. Cloud-based Markets Surveillance. Nice Actimize. 2019 URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://info.nice.com/rs/338-EJP-431/images/NICE_Actimize_Markets_Surveillance_-_Brochure.pdf&ved=2ahUKEwjSifeYq5LoAhVw2aYKHe7_C3MQFjAGegQICRAB&usg=AOvVaw2ViFnUb__oM_JZMWTMPmm7&cshid=1583926959339
63. Биткоин-биржа Poloniex исключит из листинга восемь криптовалют. Forklog. 2018. URL: https://forklog.com/bitkoin-birzha-poloniex-isklyuchit-iz-listinga-vosem-kriptovalyut/
64. Биткоин-биржа Bitstamp задействует технологии для противодействия манипуляциям рынком. Forklog. 2018. URL: https://forklog.com/bitkoin-birzha-bitstamp-zadejstvuet-tehnologii-dlya-protivodejstviya-manipulyatsiyam-rynkom/
65. Bittrex Takes Steps to Prevent Price Manipulation on its Platform. Finance Magnates. 2017. https://www.financemagnates.com/cryptocurrency/exchange/bittrex-takes-steps-prevent-price-manipulation-platform/
66. Закон Додда-Фрэнка, краткое содержание. Smart Lab. 2017. URL:https://smart-lab.ru/finansoviy-slovar/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%94%D0%BE%D0%B4%D0%B4%D0%B0-%D0%A4%D1%80%D1%8D%D0%BD%D0%BA%D0%B0