МВД России
Санкт-Петербургский университет

ТЕХНОЛОГИИ КРИПТОВАЛЮТ

Монография

Санкт-Петербург
2023

План-график 2023, поз. 85

УДК 336.7:347.7
ББК 65.262:67.402
Т38

Т38 Технологии криптовалют : [монография] / А. И. Примакин, А. И. Локнов, И. Н. Васильева, В. Н, Родин [и др.]. – Санкт-Петербург : СПбУ МВД России, 2023. – 158 с. : ил., табл. ; 21 см. – 50 экз.

Авторы

Примакин А. И. – введение, заключение, главы 1 и 4 (в соавт.);
Локнов А. И. – главы 2 и 4 (в соавт.), разделы 2.1 и 2.2;
Васильева И. Н.— глава 2 (в соавт.); Родин В. Н. глава 3 (в соавт.);
Чудаков О. Е. глава 3 (в соавт.), разделы 3.3 и 3.4

ISBN 978-5-91837-713-0
EDN XJXKTL

Монография подготовлена в связи с необходимостью проведения учебных занятий в рамках дополнительного профессионального образования повышения квалификации сотрудников территориальных органов МВД России, служебная деятельность которых имеет отношение к расследованию преступлений, связанных с использованием криптовалют в противоправных целях. Позволяет сформировать у слушателей теоретические знания об основах криптографии, алгоритме формирования криптовалют, технологии блокчейна и процессе майнинга биткойнов. Рассмотрены алгоритмы формирования и применения открытого и закрытого ключей ассиметричной криптографической системы для создания биткойн-кошелька.

Издание может быть полезно для курсантов, слушателей, адъюнктов, научно-педагогического состава образовательных организаций высшего образования системы МВД России, интересующихся вопросами выявления и расследования преступлений, связанных с использованием криптовалют и других виртуальных активов.

УДК 336.7:347.7
ББК 65.262:67.402

Рецензенты:
Симаков А. А., кандидат технических наук, доцент
(Омская академия МВД России);
Назаров А. К., кандидат физико-математических наук
(Краснодарский университет МВД России)

ISBN 978-5-91837-713-0

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В Приказе МВД России от 25 ноября 2019 г. № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км 27 Декабря 2019 «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий» отмечалось, что «Приобретают все большую актуальность вопросы совершенствования кадровой политики и организации подготовки для органов внутренних дел специалистов в сфере информационных технологий».

Обеспечение эффективности борьбы с преступлениями в сфере информационных технологий предполагает решение ряда принципиально новых задач, связанных с появлением криптовалюты. В силу своей новизны и актуальности эта проблема, на наш взгляд, заслуживает отдельного, более пристального рассмотрения[1].

Постановка проблемы обусловлена, прежде всего, отсутствием либо недостаточностью законодательного регулирования использования криптовалют и криптотехнологий в экономике и администрировании цифрового пространства России.

В данной монографии делается попытка разобрать технологии, лежащие в основе понятия «криптовалюта» (глава 1).

Прежде всего, термин «криптовалюта» (англ. *cryptocurrency*) переводится в буквальном смысле как виртуальная валюта, защищенная криптографией. По этой причине, во второй главе монографии рассматриваются принципы и основные положения криптографии, лежащие в основе криптовалюты.

В широком научном плане криптовалюта — это цифровые счетные единицы, учет которых децентрализован. Принцип децентрализации напрямую связан с технологией блокчейна, которая представлена в третьей главе данной монографии.

В криптовалютах используются открытые и закрытые ключи для перевода валюты от одного (физического или юридического) лица другому, и для перевода криптовалюты каждый раз требуется криптографическая подпись. Технологии электронной подписи и процедуры хеширования (хэш-функции) представлены во второй главе монографии.

---

[1] Криптовалюты на территории стран Содружества: оценка вероятных криминальных рисков и угроз / И. Б. Колчевский, А. Г. Кузнецов. Москва: ФГКУ «ВНИИ МВД России», 2018. 15 с.

Синтез перечисленных выше технологий позволяет определить понятие «криптовалюта», как децентрализованная виртуальная валюта, основанная на математических принципах пиринговыми виртуальными валютами с открытым исходным кодом, у которых нет центрального администратора, и отсутствуют централизованный контроль или надзор.

Отсутствие контроля и надзора делает привлекательным данную сферу экономики для киберпреступности и криминального использования виртуальной валюты[1].

Впервые о рисках использования продуктов технологии блокчейн заговорила Европейская полицейская организация (Европол). В своем отчете за 2015 год он проанализировал тренды оборота криптовалюты и заключил, что наибольшую популярность новые финансовые инструменты приобретают в криминальной сфере (коррупционные преступления, торговля наркотиками, психоактивными веществами и порнографией). Чаще всего криптовалюта используется в нелегальном Интернете (даркнете) при покупке изъятых из оборота веществ и продуктов. К концу 2018 года число направлений криминального использования криптовалюты существенно увеличилось, но по-прежнему на первом месте находится использование цифровых денег, как средства расчетов на теневых Интернет-рынках[2].

В конце 2018 года рынок незаконной деятельности с биткойном[3], пиринговой платёжной системой, использующей одноимённую единицу для учёта операций, составил примерно 76 млрд долларов США в год (46 % биткойн-транзакций), что по объемам близко к масштабам американского и европейского рынков незаконного

---

[1] См.: Иванцов С. В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А., Берёзкин Ю. М. [и др.] // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 85–93.

[2] См., например: Сидоренко Э. Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. Т. 10, № 6. С. 147–155; Спасенников Б. А. Актуальные проблемы уголовного права: обзор литературы // Актуальные вопросы образования и науки. 2015. № 1-2 (47–48). С. 36–38; Williams K. S. Textbook on Criminology. Oxford: Univ. Press, 2012. 640 p.

[3] Транскрипция «Биткойн», соответствующая правилам англо-русской практической транскрипции, используемой для передачи английских собственных имён, а также других лексических единиц, непосредственно заимствуемых из английского языка (например, терминов), для которых не существует исторически сложившейся (традиционной) передачи на русский язык (см.,: Грамоту.ру: справочно-информационный Интернет-портал «Русский язык» [сайт]. URL: http://new.gramota.ru/spravka/buro/search-answer/?s=биткойн (дата обращения: 24.04.2023)); применён в заявлении Банка России (Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн: информация Банка России от 27 января 2014 г. Доступ из прав.-правовой системы «КонсультантПлюс»).

оборота наркотиков. Кроме того, примерно четвёртая часть (23 %) от общей долларовой стоимости транзакций и примерно половина биткойн-кошельков (49 %) так или иначе, связаны с незаконной деятельностью с использованием криптографических алгоритмов[1].

По данным бизнес-школы Сиднея, оборот психоактивных веществ с использованием виртуальной валюты на протяжении пяти лет сохраняет тенденцию к росту (показатель прироста от 5 до 15 %) со спецификацией на отдельных направлениях деятельности. Каждый год проводится около 40 млн криминальных сделок на сумму, превышающую 76 млн долларов США. Если исходить из того, что сегодня насчитывается около 22 млн владельцев цифровой валюты, то можно говорить о том, что примерно четверть из них хотя бы раз применяли криптовалюту в нелегальных расчетах[2].

Популярность нового финансового инструмента в криминальной среде объясняется тем, что до настоящего времени не выработаны юридические параметры криптовалюты и не установлены границы ее безопасного оборота. Во многом это обусловливается недопониманием со стороны отечественных и международных экспертов важности исследования криптовалюты в рамках риск-ориентированного подхода, когда одновременно соотносятся экономические преимущества и криминогенный потенциал криптоинструментов[3]. Отсутствие комплексных исследований трендов криминального использования криптовалюты с неизбежностью влияет на результативность работы в сфере предупреждения криптопреступлений[4].

В целях предупреждения дальнейшего развития киберпреступности важно разработать такую модель правового регулирования виртуальных валют, в которой одновременно были бы решены две задачи: предупреждение совершения корыстных преступлений и поддержка инновационного развития российской экономики.

---

[1] URL: https://www.group-ib.ru/media/gib-crypto-summary / (дата обращения: 17.08.2021).

[2] URL: https://utmagazine.ru/posts/21785-kriptovaly-uty-v-nelegalnoy-deyatelnosti / (дата обращения: 12.08.2021).

[3] Popper N., Ruiz R. Leading Online Black Markets Are Shut down by Authorities // The New York Times. — 2017. — July 20.

[4] См.: Архипов В.В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9. С. 69–90.

Глава 1
ПОНЯТИЕ КРИПТОВАЛЮТЫ

1.1. Классификация платежных систем

Прежде, чем рассматривать понятие «криптовалюта», необходимо разобраться в концепции денег, вспомнить их историю и предшествующие им средства обмена, а также положительные и отрицательные стороны до денежных систем. После этого станет понятно, что привело к идее *Bitcoin* (биткойн) и почему эту платежную систему называют самой революционной из всех когда-либо созданных[1].

Бартерная платежная система

Бартерную систему люди использовали 6 тыс. лет до н. э. Затем появились монеты — примерно в 650 г. до н. э. Люди начали применять первые формы печатной валюты приблизительно в 960 году, а первая форма чека появилась примерно в 1717 году. Впервые идея «электронных денег» была предложена американским специалистом по теории сложности Дэвидом Чоумом еще в конце 70-х гг. Первая система электронных денежных средств *PayPal* была представлена в 1998 году, в России — *WebMoney* также появилась в 1998 году. И, наконец, в 2008 году появилась идея биткойна.

Система бартера — первое средство обмена, известное человеку, — в своем зарождении была довольно простой и весьма логичной: любой человек производил тот товар или услугу, на которой он специализировался, и обменивал свой товар или услугу на те, которые ему требовались. Эта система отлично работала некоторое время, но в ней присутствовали недостатки, о которых стало известно позже. Рассмотрим пример, чтобы это понять. Представим два лица — А и Б. А — производит пшеницу, а у Б есть стадо коз. А и Б решили обменяться — 10 центнеров пшеницы за одну козу. В данный конкретный момент А и Б решили, что одна коза по стоимости равняется 10 центнерам пшеницы. Однако завтра это может измениться, и пшеница, принадлежащая лицу А, может не стоить столько же у третьего лица. Предположим, лицу А нужны бананы, он ищет того, кто их производит, и теперь ему придется предлагать разную общую стоимость каждый раз, когда он хочет приобрести разные товары. Поэтому первым

[1] См.: Бикмаев Ш. Р. Развитие рынка платежных карт в современных условиях // Финансы и кредит. 2011. № 41 (473). С. 65–71.

и главным недостатком системы бартера было отсутствие общей единицы стоимости.

Следующий недостаток состоял в том, что товары легко портятся. Козы, пшеница — это все продукты, подверженные порче. У них короткий срок жизни. Однако, если сегодня есть пшеница, а нужна коза, но через год, то пшеница не доживет до этого момента. Поэтому в данной системе всегда существовал разрыв во времени между спросом и предложением.

Следующим недостатком была неэффективная система перевозки товаров. К примеру, перевозка крупных товаров всегда становилась проблемным моментом.

И, наконец, в бартерной платежной системе не обеспечивалась безопасность — товары могли быть украдены и использованы кем-то другим, и у собственника этих товаров не было доказательства того, ресурсы принадлежат ему.

Монетная платежная система

Тем не менее, люди быстро поняли, что товаром-посредником может служить золото, которое ценилось всеми и прекрасно решило одну из основных проблем бартерной системы — отсутствие единицы общей стоимости. К тому же золотые монеты не подвержены быстрой порче и инфляции. Золотые запасы в мире всегда ограничены, а это значит, что спрос на золото всегда будет повышаться, в то время как предложение всегда будет ограничено. Это делает любые ресурсы не подверженными инфляции. Их стоимость будет только расти, и никогда не будет падать. Наконец, золото было легко транспортировать. Монеты были мелкими по размеру и чаще всего одинаковой формы. Людям больше не приходилось перевозить два разных по размеру товара.

Однако у золотых монет были и минусы, из-за которых люди перестали их использовать. Первый минус: добыча золота – затратное и нелегкое дело. Второй минус: несмотря на то, что золотые монеты были сравнительно мелкими по размеру, и их легко было перевозить, сравнения с современными бумажными деньгами они не выдерживали. И, наконец, в системе платежей золотыми монетами также не обеспечивалась безопасность: их мог украсть и использовать кто угодно. Это значит, что данная система не решала самую основную проблему бартера — не обеспечивала безопасность.

Итак, возникла необходимость решить вопрос безопасности

платежной системы с использованием золотых монет, поэтому люди стали отдавать монеты на хранение третьей стороне, которая в наши дни известна как банки. В обмен на это золото банки выпускали долговые расписки, которые подтверждали получение золота. Любой человек, имеющий такую расписку, мог где угодно обменять ее на товары. Таким образом, долговые расписки были ничем иным как первой формой бумажных денег. Однако их достоинства опирались на фактически существующее количество золота.

Бумажная платежная система

Существовало множество плюсов бумажной платежной системы. Во-первых, такие деньги были легче золотых монет, и их было проще производить. Во-вторых, эти деньги подкреплялись чем-то: на первых порах — физически существующим ценным ресурсом — золотом, а позже — неосязаемым ресурсом, таким, как доверие правительству, которое их выпускало.

Однако и у этой системы есть свои недостатки. И один из них заключается в том, что в системе бумажных денег не обеспечивается безопасность. Банкноты можно украсть и использовать. Второй недостаток — бумажные деньги подвержены инфляции. Итак, бумажные деньги — это валюта, подкрепленная нематериальным товаром, например, доверием правительству. Но по причине того, что какого-то осязаемого ресурса, подкрепляющего банкноты, не существует, правительство может выпустить столько бумажных денег, сколько возможно. Но из-за таких рыночных сил, как спрос и предложение, большее количество выпущенных банкнот со временем теряет свою стоимость.

Еще один недостаток бумажной платежной системы — это так называемые «грязные» деньги и теневая экономика. В то время не было способа отследить все денежные потоки, определить, на какие цели используются деньги, и кто ими владеет.

И, наконец, с золотомонетной системой в 1970-х гг. было покончено, потому что она снижала гибкость центрального банка в осуществлении кредитно-денежной и фискальной политик, требующихся для регулирования экономики страны.

Чековая платежная система

Чековая платежная система и система биткойн имеют много общего. Во-первых, в чековой платежной системе наконец улучшилась ситуация с безопасностью в средствах обмена: на чеках указывалось имя чекодателя, имя чекодержателя, а также их адреса. Этот момент

имеет очень большое значение для понимания системы биткойн. Во-вторых, в системе чеков использовалась базовая форма криптографии, именуемая «подписью», чтобы подтвердить, что именно чекодатель поручает провести операцию по чеку (еще одно важное свойство с точки зрения системы биткойн). И, наконец, пользователь мог поменять сумму на чеке — люди больше не опирались на определенную сумму, как в случае с бумажными деньгами.

Недостатки чековой платежной системы связаны с появлением формы чеков под названием «чек на предъявителя» — тот, кто предъявлял данный чек, мог получить сумму, указанную в нем. Это снижало уровень безопасности. Во-вторых, та форма криптографии, которая использовалась в чековой платежной системе, была довольно элементарной, и подписи можно было легко подделать. Наконец, самым большим недостатком чековой платежной системы являлось время верификации перевода денежных средств. Верификация происходила с большой задержкой. Чекодатель вручал чекодержателю чек, чекодержатель отправлялся в свой банк в любое удобное для него время и передавал чек банку. Банк чекодержателя связывался с разрешающей инстанцией, которая, в свою очередь, связывалась с банком чекодателя, чтобы подтвердить, что у чекодателя есть на счету требуемая сумма и операция по переводу средств может состояться. Проблема же заключалась в том, что во время перевода денег чекодержатель был вынужден отдавать чекодателю товар в обмен на его чек, не имея при этом никаких гарантий того, что у чекодателя есть на счету сумма для завершения сделки.

Платежная система электронных кошельков[1]

На первый взгляд эта система кажется идеальной — она не требует наличия «живых» денег, людям больше не нужно носить с собой кошелек. С развитием индустрии смартфонов и Интернета и повышением уровня применяемой криптографической защиты безопасность электронных кошельков стала гораздо выше. В наши дни практически в любом смартфоне есть сканер сетчатки и сканер отпечатка пальца, что может служить средством подтверждения банковских операций, а это гораздо более технически продвинутые способы, чем подпись. Благодаря быстроте, эффективности и удобству этих способов верификация операции занимает несколько секунд, что решает

[1] См.: Пухов А. В., Мацкевич А. Ю., Рего А. В., Ушанов П. В. Электронные деньги в коммерческом банке: практическое пособие. Москва: Изд-во КноРус. 2015. 208 с.

самую большую проблему системы платежей банковскими чеками. Наконец, возможность учета операций посредством электронных кошельков в финансовой системе гораздо выше. Электронные кошельки позволяют регулирующим органам отслеживать денежные потоки, контролировать, сколько у кого денег, и для чего эти деньги используются. Эта система дает возможность снизить количество «грязных» денег и денег, используемых в противозаконных целях.

Итак, с первого взгляда система электронных кошельков кажется идеальной. Но возникает вопрос: почему возникла необходимость в альтернативной системе — новой, усовершенствованной системе под названием биткойн? Потому что главная проблема системы электронных кошельков – это то, что не очевидно даже сейчас: эта система является частью существующей финансовой инфраструктуры.

В 2008 году мир увидел недочеты и недостатки существующей финансовой инфраструктуры. Обнаружилось, что действующая финансовая система неэффективна и коррумпирована. Произошел кризис субстандартного ипотечного кредитования, из-за которого финансовые рынки обрушились по принципу домино, крупные инвестиционные банки стали банкротами, правительствам пришлось предоставить финансовую помощь многим банкам. К тому же на мировых финансовых рынках был зарегистрирован крупнейший с 1929 года спад деловой активности. Но это были экономические последствия, а существовали еще и эмоциональные — люди потеряли веру в финансовую систему.

Вся суть банков состояла в том, что они являлись третьей стороной, которая надежно хранит материальные ценности и является лучшей альтернативой, чем хранение денег дома. Люди доверяли банкам сохранность своих средств, но банки не справились, — они неправильно использовали эти деньги и потеряли все. Тогда люди поняли, что альтернативной и надежной системы хранения денег не существует. Начался массовый вывод средств с банковских счетов, и стало понятно, что замены существующей системы нет. Люди оказались перед выбором: либо хранить все деньги дома, что в сегодняшних обстоятельствах не самая лучшая идея, либо отдавать их банку, которому они больше не доверяли. Возникла нужда в альтернативной системе.

В конце 2008 года лицо или группа лиц под псевдонимом Сатоси Накамото опубликовал документ под названием «Биткойн: одноранговая валютная система». Этот революционный документ бросал вызов самой концепции денег и всей идее существования посредника,

который занимается деньгами. В этом и заключается причина того, что биткойн — это самая продуманная и подрывающая все устои технология из всех когда-либо созданных[1].

Криптовалюта представляет собой цифровую валюту, защищенную с помощью криптографических технологий. Её главной особенностью является то, что физического аналога у этих денежных единиц нет, они существуют только в виртуальном пространстве. Весь её оборот: покупка, продажа, осуществляется только в информационно-телекоммуникационной сети «Интернет». Современные платёжные средства, такие как: *ЮMoney, PayPal, WebMoney* и другие электронные деньги оперируют уже имеющимися валютами, например, долларом, евро, рублём. У криптовалют нет привязки к каким-то ценным ресурсам, как, например, к золоту. Но, тем не менее, криптовалюта это, по сути, цифровое золото, так как почти все их свойства между собой совпадают:

– ограниченное количество;
– необходимость добывать;
– независимость;
– дробимость;
– невозможность скопировать.

В алгоритме криптовалюты «Биткойн» заложено максимальное количество монет, которое может быть выпущено — 21 млн, после чего он так же продолжит свою работу, но новые монеты в систему поступать уже не будут.

Необходимость добывать заключается в том, что для появления каждой новой монеты пользователи сети должны выполнить определённый ряд действий, заключающийся в решении математической задачи, сложность которой зависит от набора различных факторов и так же регулируется внутри системы. Этот процесс называется майнингом[2].

Независимость биткойн представляет под собой отсутствие того, кто бы мог контролировать работу системы биткойн и влиять на её дальнейшее развитие. Все решения об изменении принимаются по принципу 50 % + 1 человек, то есть по принципу голосования большинства.

---

[1] См.: Аммус С. Краткая история денег, или все, что нужно знать о биткоине. Москва: Изд-во «Манн, Иванов и Фарбер». 2019. 272 с.

[2] Биткоин (Bitcoin). Криптовалюта. URL: https://www.tadviser.ru/index.php/Статья:Биткоин_(Bitcoin)_ Крипто-валюта (дата обращения: 30.03.2022).

Дробимость заключается в том, что один биткойн можно разделить на 100 млн сатоши. Сатоши — самая маленькая единица биткойн, которая может храниться в блокчейн.

Такой популярности биткоину позволил достичь ряд его преимуществ перед привычными нам платёжными системами:

– децентрализованность;

– полная анонимность;

– высокий уровень безопасности;

– фиатность;

– неподверженность инфляции.

Каждая из вышеперечисленных особенностей обеспечивается разными технологиями, которые лежат в основе криптовалюты, а именно — биткойна. Так, например, децентрализованность достигается благодаря внедрению блокчейна и вместе с ним возможности достижения консенсуса между всеми пользователями. Полная анонимность и высокий уровень безопасности обеспечивается за счёт криптографии – ассиметричного шифрования и использования хеш-функций[1].

1.2. Понятие и алгоритм работы системы биткойна

Биткойн — это цифровая, децентрализованная, без посредников, без внешних гарантов, фиатная (то есть не обеспеченная золотом) валюта. Все эти определения по отдельности имеют очень важное значение в описании этой платежной системы[2].

Рассмотрим алгоритм работы системы биткойн на простом примере из жизни.

Допустим, есть шесть друзей — А, Б, В, Г, Д, Е. Они регулярно встречаются и любят ходить в бар, в котором расплачиваются каждый за себя. Однако бары в их районе обычно отказываются делать для каждого отдельный счет, потому что это неудобно. Поэтому каждый раз, когда друзьям приносят счет, расплачивается кто-то один и сохраняет чек, чтобы позже разобраться, кто, сколько должен (рисунок 1).

---

[1] Магомагазиев А. А. Рынок криптовалюты. История и сферы влияния криптовалюты // Форум молодых учёных. 2021. № 12 (64). С. 143.

[2] Афанасьева Ю. Как заработать биткоины: главные способы, плюсы и минусы. URL: https:https://www.finam.ru/publications/item/kak-zarabotat-bitkoiny-glavnye-sposoby-plyusy-i-minusy-20190605-16420/ (дата обращения: 24.08.2021).

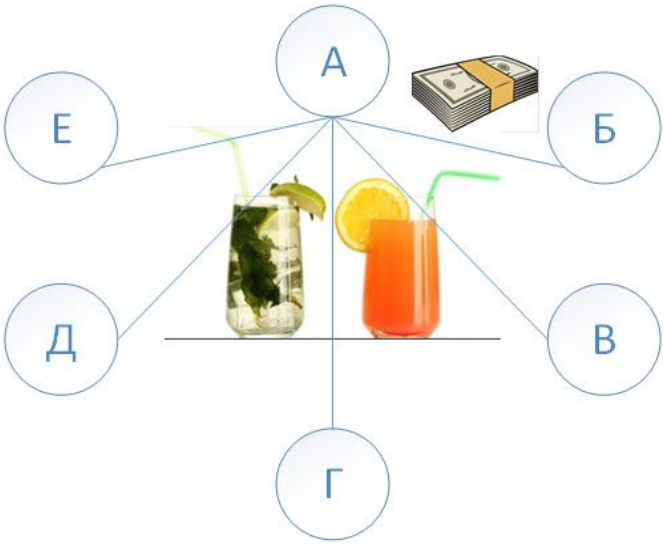

Рисунок 1 – «А» платит за друзей в баре

Какое-то время эта система работала, но скоро друзья начали ссориться. Некоторые из них были не согласны с суммой, которую были должны, другие пили больше, чем могли себе позволить, и позже не могли расплатиться. Тогда А решил, что они должны вести совместные записи в блокноте. Они создали общую книгу записей в блокноте и обновляли записи после каждого похода в бар. Блокнот хранился там, куда имел доступ каждый из них (рисунок 2).

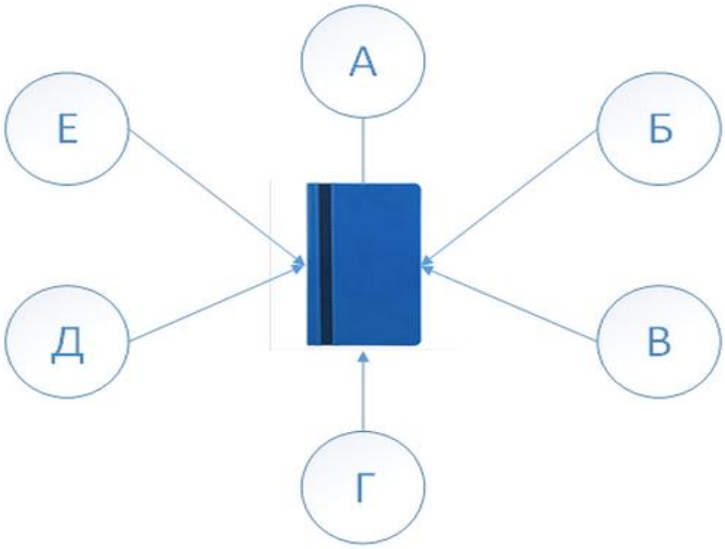

Рисунок 2 – Совместные записи в блокноте

Но однажды А обнаружил, что некоторые цифры не сходятся, а некоторые суммы подправлены. Это означало, что доверять друг другу они больше не могут, и А понял, что иметь общий гроссбух недостаточно. Он много думал, и в конце концов ему в голову пришла

блестящая идея. На следующий день он позвал всех друзей на встречу, чтобы познакомить их с новой системой.

Он сказал: «Я придумал безотказный метод, чтобы справиться с этой проблемой. Каждому из вас я вручаю блокнот. Мы все будем вести записи по каждому счету и по тому, кто, сколько и кому должен. Таким образом, мы все будем знать, сколько у каждого средств на счету, должны ли вы действительно кому-то эти деньги и т. д. В следующий раз, например, если В должен Е общую сумму за последние два похода в бар, мы проверим наши записи, чтобы понять, так ли это на самом деле. А когда мы это сделаем, то подытожим общую сумму, после чего подсчитаем оставшийся баланс. Но мы не будем это запоминать. Если более чем 51 % — это большинство из нас — согласны, что предложенная операция верна, мы одобрим ее и обновим информацию в наших блокнотах маркером, а потом заверим это обновление нашими подписями. Это будет означать, что ни одна запись не была стерта и все записи были нами проверены и утверждены. Записи могут быть изменены только путем предложения всем нам новой операции. В этом случае, если кто-то хочет обмануть систему, он должен будет изменить записи, по меньшей мере, в четырех блокнотах, в данном случае — без разрешения их владельцев. Усилия и затраты, которые он в это вложит, сведут на нет любую прибыль, которую он надеется получить. Таким образом, нам больше не нужно доверять друг другу – нам нужно довериться системе».

Если представить, что то, чем они обмениваются, — это не физические деньги, а некая форма цифровой и вымышленной валюты, то это и есть биткойн. Вот некоторые характеристики, которые упоминались в определении биткоина.

Биткойн — цифровая валюта. У биткойна нет физической формы, эта валюта полностью цифровая. Тем не менее, в общем понимании биткойн немного отличается от цифровой валюты. Цифровая валюта утверждается в местной валюте, а биткойн — это любая валюта, у которой есть собственная ценность, устанавливаемая в пересчете на каждую валюту, например, на юани, рупии, йены или доллары.

Биткойн — децентрализованная валюта. Группа из вышеприведенного примера перешла от общего блокнота с записями к индивидуальным блокнотам. Это и называется «децентрализованной системой базы данных»[1].

[1] См.: Антонопулос, А. М. Осваиваем биткойн: программирование блокчейна. Москва: ДМК Пресс, 2018. 428 с.

Биткойн — это система без посредников. В центре этой системы нет никого, кто контролировал бы одобрение транзакции. Каждый в группе вовлечен в этот процесс одобрения, и требуется минимальный консенсус в 51 %, чтобы одобрить транзакцию.

Система биткойн не создает напряжения у участников из-за недоверия друг к другу и полностью анонимна: членам группы не обязательно быть друзьями и доверять друг другу, чтобы принимать участие в системе, — доверять нужно только самой системе. Система биткойн, в отличие от вышеприведенного примера, не имеет идентификаторов личности — все личности скрыты. Идентификаторами служит набор алфавитно-цифровых символов, генерируемых случайным образом. Это достигается за счет процесса, который называется «криптографической хэш-функцией»[1].

Система биткойн неизменна. Это значит, что ни одна из предыдущих транзакций не может быть изменена, чтобы отменить ее действие или в тот момент времени, когда она должна быть предложена системе.

Как и большинство свободных рыночных валют сегодня, биткойн — фиатная валюта. Она не подкреплена какими-либо осязаемыми ресурсами, только неосязаемым — доверием. Биткойн имеет ценность просто потому, что члены группы верят в то, что он имеет ценность. Они верят в то, что все члены группы, объединенные сетью, примут ценность валюты биткойн и будут использовать ее как законное средство платежа, как любую другую валюту. (Принятый для любой валюты неосязаемый ресурс — доверие государству, которое выпускает ее.)

Дешевизна валюты биткойн. Так как в этой платежной системе нет посредников, а члены группы используют свою собственную валюту, они могут менять деньги с минимальными затратами — без оплаты участия посредника.

В системе биткойн обеспечивается высокий уровень безопасности. В вышеприведенном примере друзья используют подписи, чтобы идентифицировать себя в производимых транзакциях. Однако система биткойн, как ужу говорилось, с той же целью использует гораздо более сложный криптографический метод — криптографическую хэш-функцию.

[1] См.: Васильева, И. Н. Криптографические методы защиты информации. Москва: Юрайт, 2019. 349 с.

Биткойн — это валюта, не подверженная инфляции. Существует лимит в 21 миллион биткойнов, которые, когда-либо, могут быть добыты. К тому же каждый биткойн может быть разделен на 10 млн единиц, и это подтверждает, что эта валюта не станет жертвой инфляции и что биткойнов достаточно для всех транзакций.

Это не первый случай в истории, когда предпринимаются попытки создать цифровую валюту. Однако предыдущие попытки провалились в процессе решения так называемой проблемы «двойной траты». Одна единица цифровой валюты может копироваться, позволяя пользователю использовать ее более одного раза. Биткойн решает эту проблему применением децентрализованной модели верификации.

1.3. Экономическая сторона и анализ системы биткойн

Биткойн похож на любую свободно конвертируемую валюту на рынке. Его стоимость определяется рыночным спросом и предложением (рисунок 3).

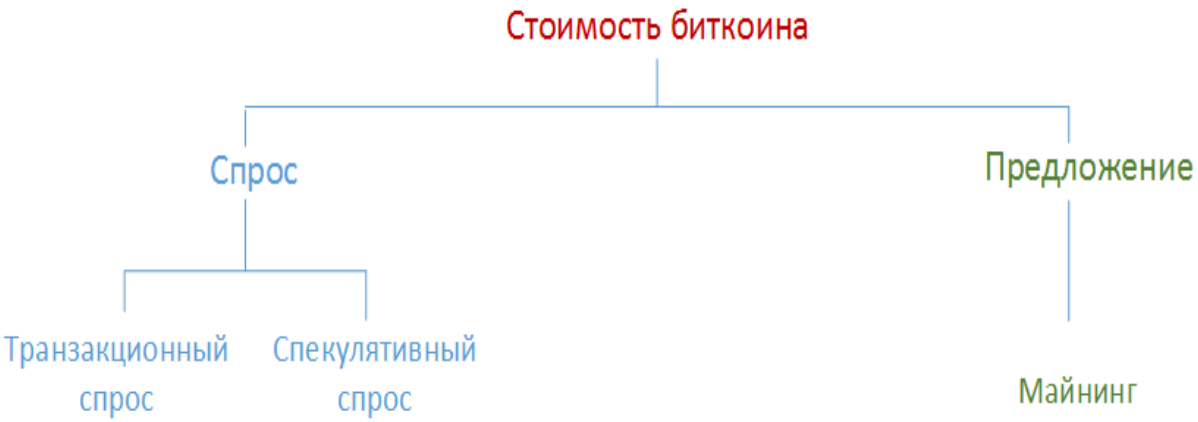

Рисунок 3 – Формирование стоимости биткоина

Для биткойна существует два основных источника спроса, как для любой другой валюты. Первый источник спроса — *транзакционный*. В некоторых странах биткойн был принят в качестве законного платежного средства. Люди в этих странах используют биткоины для своих ежедневных покупок, начиная с кофе и заканчивая автомобилями.

Второй источник спроса — *спекулятивный*. Игроки на бирже используют дефляционную природу биткойна, чтобы заработать на ней. Больший процент спроса валюты биткойн проистекает из ее активности, таким образом, делая ее более непостоянной. Валюта

биткоин ослабевает, когда происходят биржевые продажи с целью получения прибыли или так называемые «панические продажи».

Существуют некоторые социально-экономические факторы, влияющие на ценность биткойна.

О первом факторе сказано выше — это спрос и предложение.

Второй фактор — интерес к биткоину. Помимо специалистов, изначально привлеченных системой биткойн, как решением технических, экономических и политических проблем, интерес к этой системе среди широкой публики в силу исторических обстоятельств подогревался банковскими блокадами и кризисом фиатной валюты.

Третий фактор — банковские блокады: вероятно, первый подобного рода прецедент произошел в конце 2010 года — банковская блокада *WikiLeaks*, во время которой *Visa, MasterCard, Western Union* и *PayPal* прекратили переводить благотворительные вклады на счет *WikiLeaks*. По просьбе Сатоси Накамото Джулиан Ассанж воздерживался от принятия вкладов в биткоинах до середины 2011 года. Тем не менее, это событие пролило свет на биткойн, на его ценность как единственной электронной валюты, не поддающейся контролю. Самая последняя такая блокада имела место, когда *MasterCard* и *Visa* внесли в черный список сайты и, которые среди прочего размещали объявления об интим-услугах. Из-за блокады поставщики интим-услуг, чья жизнедеятельность зависит от объявлений, размещенных на подобных ресурсах, оказались не способны оплачивать размещение объявлений ничем, кроме биткойнов. Торговая площадка *Silk Road* стала еще одним примером случая, когда биткоины использовались для оплаты противозаконной деятельности.

Четвертый фактор — кризис фиатной валюты. Ранее упоминалось, что биткойн-кошелек гораздо безопаснее, чем банковский счет. Жители Кипра узнали об этом, получив негативный опыт, когда в начале 2013 года их сбережения были конфискованы. Это событие стало причиной резкого скачка стоимости биткойна, так как владельцы сбережений узнали, что работа с биткойном гораздо более безопасна, чем работа с банками. Следующей стала Греция, где в 2015 году ввели строгий контроль за движением капитала. Граждан Греции обязали выводить со счетов не более 60 евро в сутки. Биткойн снова продемонстрировал свою ценность как валюта, не подлежащая централизованному контролю. Вскоре после кризиса в Греции Китай начал девальвировать юань. По отчетам того времени, владельцы вкладов в Китае обратились к биткоину, чтобы защитить свои накопления.

Пятый фактор — манипулирование рынком. Самый высокий курс биткойна — около 1 000 долларов США — был частично достигнут за счет автоматизированных систем торгов или бирж, работающих на компанию *Mt. Gox*. Все свидетельствует в пользу того, что такие биржи действуют мошеннически, под управлением биржевого спекулянта Марка Карпелеса, который накручивал цены на несуществующие средства.

Шестой фактор — нарушение ценообразования. Иногда обменный курс может существенно отличаться от согласованного курса, что и происходило в определенный момент времени в компании *Mt. Gox* перед ее банкротством, а в середине ноября 2015 года — на биткойн-бирже братьев *Винклвосс Winklevoss Gemini Exchange*. Биткойн стоил 220 долларов США, в то время как на других площадках его цена составляла около 330 долларов США. Эти торги в дальнейшем были аннулированы. Такие события очень часто происходят на биржах либо из-за ошибок персонала, либо из-за сбоев программного обеспечения.

Теперь о биткойне как классе активов. Как уже упоминалось ранее, в последние годы биржевые спекулянты использовали биткойн для вложений. Однако из-за прочной позиции предложения биткойн на рынке остается нестабильным и зависит от «настроений» рынка. Проблемы в том, что, так как весь 21 мл биткойнов еще не выпущен, эта валюта на данный момент больше находится под воздействием спекулятивного спроса, чем транзакционного.

Потенциальные инвесторы рассматривают биткойн, как класс активов, представляющий альтернативу ценным бумагам и доле в капитале. Тем не менее, более дальновидным было бы хранить большую часть вложений в ценных бумагах и долях в капитале и играть на биткойн-биржах с оглядкой на то, что это рискованные инвестиции в расчете на экономический рост. Целесообразно использовать технические параметры исследований, основанных на качественных показателях цены и объема, и искать макроэкономические пусковые механизмы, например, такие, как победа Дональда Трампа на выборах в ноябре 2016 года, повысившая шансы инвесторов на большой куш.

1.4. Особенности системы биткойн

Особенности системы биткойн, прежде всего, проявляются в тех вопросах, ответы на которые представлены ниже.

Как создаются новые биткойны

Новые биткоины генерируются в ходе конкурирующего и децентрализованного процесса под названием «майнинг». Этот процесс также подразумевает, что частные лица получают вознаграждение за то, что объединяются в сеть и предоставляют свои услуги. «Добытчики» биткойнов производят транзакции и обеспечивают безопасность сети с помощью специального оборудования, взамен чего получают новые биткоины. Протокол биткойн создан таким образом, что новые биткоины создаются с фиксированной скоростью. Все это делает майнинг биткойнов конкурентоспособным бизнесом. Когда большое количество майнеров присоединяются к сети, становится значительно сложнее получить прибыль. Меж тем майнеры должны быть заинтересованы в эффективности, чтобы сократить свои производственные издержки. Центральная власть или учреждения не могут контролировать систему или повлиять на нее, чтобы увеличить прибыль.

Любая криптовалюта будет отклонять все, что не соответствует правилам, по которым должна работать эта система. Биткоины создаются со снижающейся и предсказуемой ставкой. Количество новых биткойнов, создающихся каждый год, автоматически уменьшается наполовину через какое-то время — до тех пор, пока количество выпущенных биткойнов не достигнет ровно 21 млн, после чего их выпуск будет прекращен. На этом этапе добытчики биткойнов, возможно, будут финансово поддерживаться исключительно за счет небольших процентов от транзакций.

Может ли биткойн обесцениться?

В мире существуют валюты, которые вышли из обращения и больше не используются, — например, немецкая марка времен Веймарской республики или переставший существовать сравнительно недавно доллар Зимбабве. Хотя предыдущие случаи обесценивания валют случались, как правило, из-за гиперинфляции — проблема, с которой биткойн не столкнется, – всегда существует потенциальная возможность технического сбоя, валют-конкурентов, политических проблем и т. д. Как показывает практика, ни одна валюта не может быть рассмотрена как абсолютно защищенная от обесценивания или сложных ситуаций. За прошедшие с момента ее возникновения годы валюта биткойн показала свою надежность, у нее огромный потенциал к росту и развитию. Однако не стоит забывать, что любая валюта, даже не подверженная инфляциям, может обесцениться, когда она

перестает считаться законным средством платежа. Это может случиться и с биткойном, если все больше и больше правительств будут запрещать эту валюту.

Является ли проблемой конечное количество биткойнов?

Валюта биткойн уникальна, так как всего может быть выпущен 21 млн биткойнов. Однако это ни в коем случае не ограничение, так как транзакции могут быть выражены в меньших единицах биткойнов, таких как битцент. Один биткойн может быть разделен на миллион частей и на более мелкие части вплоть до 0,00 000 001 (восьми десятичных знаков), а потенциально и на более мелкие части, если это когда-либо потребуется в будущем при уменьшении размера транзакции.

Может ли валюта биткойн попасть в дефляционную спираль?

Теория дефляционной спирали гласит, что если ожидается падение цен, то люди откладывают покупки на будущее, чтобы остаться в плюсе за счет низких цен. Это падение спроса в свою очередь заставит продавцов снизить цены, чтобы стимулировать спрос, тем самым усугубляя проблему, что приведет в итоге к падению экономики. Хотя эта теория – популярный способ оправдать инфляцию среди центральных банков, она не производит впечатление верной и считается довольно противоречивой даже среди экономистов. Бытовая техника, например, представляет собой пример сегмента рынка, где цены постоянно падают, но этот сегмент не находится в упадке. Аналогичным образом стоимость биткойнов возрастает по прошествии времени, и соответственно вырастет размер экономики биткойн. В 2009 году стоимость валюты биткойн и развитие ее экономики начались с нуля. Биткойн — доказательство, показывающее, что иногда теория ошибочна. Несмотря на это, биткойн создан не для того, чтобы быть дефляционной валютой; правильнее было бы сказать, что биткойн, предназначенный для того, чтобы вызывать инфляцию в ранние годы своей работы, позже стабилизируется. Единственный случай, когда количество биткойнов в обращении может упасть, — это если люди потеряют свои электронные кошельки в случае неудачного резервного копирования. Со стабильной монетарной базой и стабильной экономикой стоимость валюты биткойн должна оставаться неизменной.

Устойчивость валюты биткойн

Для стабилизации стоимости биткойнов крупномасштабная экономика должна выстраивать отношения с большим количеством предприятий и пользователей. Чтобы развивать крупномасштабную экономику, предприятия и пользователи будут стремиться к стабильности цен. К счастью, волатильность не воздействует на основные суммарные выгоды биткойна как платежной системы для перевода денег из пункта А в пункт Б. Предприятия могут переводить платежи в биткоинах в свою местную валюту сразу без привязки к колебанию курсов. Так как биткойн предлагает много полезных и уникальных функциональных особенностей, и свойств, эту валюту выбирают многие пользователи. С такими технологическими решениями и стимулами вполне возможно, что биткойн достигнет определенного уровня и настолько усовершенствуется, что волатильность его стоимости станет незначительной.

Возможен ли одновременный выкуп всех существующих в мире биткойнов?

Лишь часть биткойнов, выпущенных на сегодняшний день, находится на биржах и доступна для продажи. Рынки биткойнов конкурентны, то есть стоимость биткойна растет или падает в зависимости от спроса и предложения. К тому же в ближайшие десятилетия выпуск новых биткойнов продолжится. Таким образом, даже самый целеустремленный покупатель не сможет купить все существующие биткоины. Ситуация, однако, не предполагает того, что рынки защищены от манипулирования ценами. До сих пор не нужно было много средств, чтобы повышать или понижать биржевой курс. Таким образом, по состоянию на сегодняшний день биткойн остается неустойчивым ресурсом.

Может ли быть создана криптовалюта лучше, чем биткойн?

На самом деле, существует тысячи криптовалют помимо биткойна, но на сегодняшний день биткойн остается, вне всякого сомнения, самой популярной децентрализованной виртуальной валютой. Однако никаких гарантий, что он удержит эту позицию, не существует. В наше время создано множество альтернативных валют, вдохновленных валютой биткойн, — например, *IOTA, Ripple* и т. д. Однако для того, чтобы новая валюта могла обойти биткойн в условиях сформировавшегося рынка (несмотря на то, что рынок остается

крайне непредсказуемым), для нее требуются существенные улучшения. Биткойн также может перенимать улучшения валюты-конкурента до тех пор, пока они не потребуют изменения основных частей его протокола.

Меняют ли криптовалюты систему бартера?

По существу, система биткойн предоставляет услуги и товары и получает товары и услуги взамен. Стоимость этих товаров и услуг конвертируется в новую форму криптовалюты. Это может выглядеть как система бартера, но на самом деле не очень отличается от системы, которой пользуются сегодня. Для того чтобы определять количество и согласовывать различные виды товаров и услуг, используется общая единица стоимости. Можно назвать систему биткойн системой бартера, имеющей преимущества современной системы и избавленной от ее недостатков, что делает ее более точной, более прозрачной и предоставляющей больше возможностей людям.

1.5. Виды систем управления

Понятие управления[1]

Поскольку в следующих разделах разговор пойдет о системе блокчейн, в этом разделе монографии будут рассмотрены разновидности систем управления. Уникальность блокчейн состоит в том, что это система относится к распределенным системам. Поэтому сначала необходимо понять, как работают разные типы систем, и определить их плюсы и минусы. Но прежде всего, следует уяснить, что такое «управление». Для этого термина существуют общие определения, которые можно найти в Интернете или в различных словарях, например:

– «власть или право отдавать приказы, принимать решения и требовать повиновения»[2];

– «лицо или организация, у которой есть полномочия или контроль в отдельной, обычно политической или административной, сфере»[3];

– «власть влиять на других, особенно по причине главенствующего положения или потому, что у лица есть общепризнанные навыки в какой-либо сфере»[4].

---

[1] Цыпленкова М. В., Моисеенко И. В., Гуремина Н. В., Бондарь Ю. А. Основы менеджмента: учебное пособие. URL: http://www.rae.ru/monographs/211-6578 (дата обращения: 17.08.2021).

[2] Там же.

[3] Там же.

[4] Там же.

Три системы управления, о которых будет рассказано дальше, отличаются друг от друга наличием одного или нескольких центров управления или же их отсутствием.

Централизованные системы

Централизованные системы имеют только одну точку управления, в которой сосредоточен весь контроль за системой (рисунок 4). Все процессы выполняются только в этой точке, в ней же принимаются и все решения. Однако это делает систему чрезвычайно подверженной падениям: любой перебой — и этот единственный центр управления может обрушить всю систему.

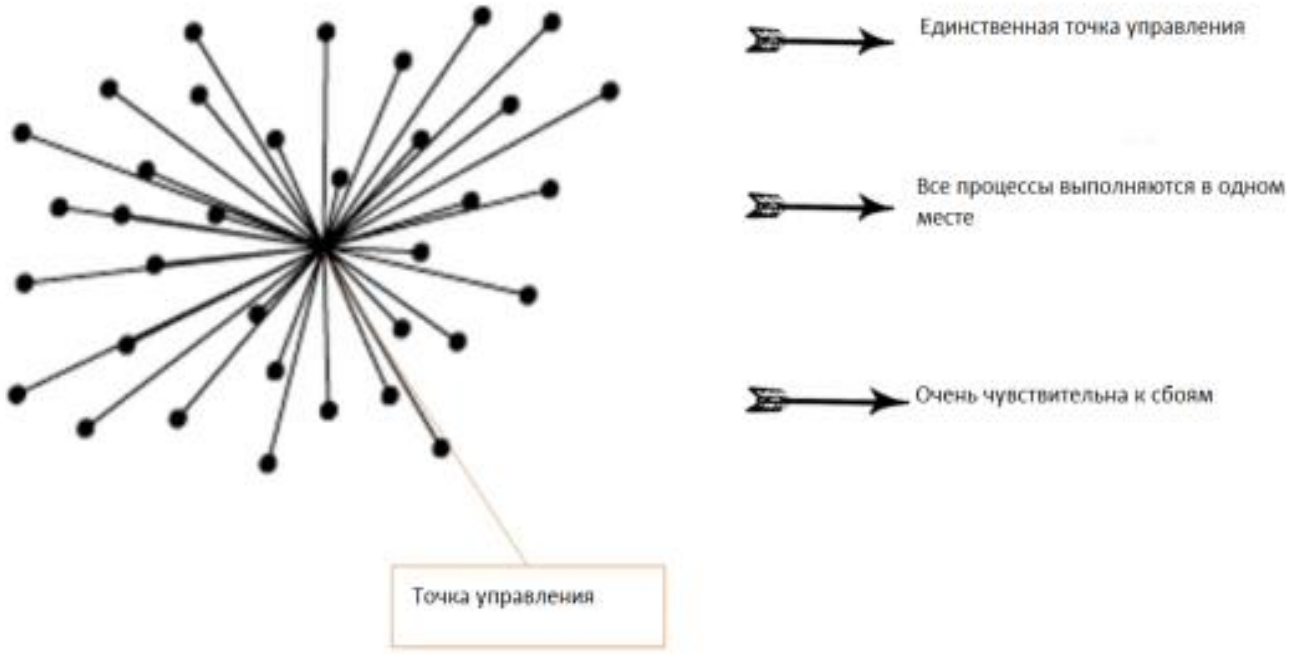

Рисунок 4 – Централизованные системы

Плюсы централизованной системы:

1. Она легко реализуема и все решения принимаются намного быстрее. Так как в ней только одна точка управления, в которой сосредоточен весь контроль за системой, консенсуса не требуется.

2. Экономия на масштабе избавляет от необходимости двойной работы, которая иногда делается при наличии нескольких точек управления. Так как в системе только одна точка управления, не нужно заставлять множество точек выполнять одни и те же функции, что дает экономию на масштабах.

Минусы централизованной системы:

1. Зависимость от одной точки управления. Наличие лишь одной точки управления делает систему беззащитной, так как любая атака на эту единственную точку управления дестабилизирует всю систему. Несложно представить себе ситуацию с сервером, когда атакуется единственный источник информации и нет никаких резервных копий, — информация в этом случае будет потеряна.

2. Система с одной точкой управления бюрократична по своей сути, что добавляет в нее множество слоев и иерархий.

3. Эта система непрозрачна и потому имеет предрасположенность к мошенничеству. Недостаток прозрачности будет провоцировать безответственность на высшем уровне, так как именно там сконцентрирована вся власть (рисунок 5).

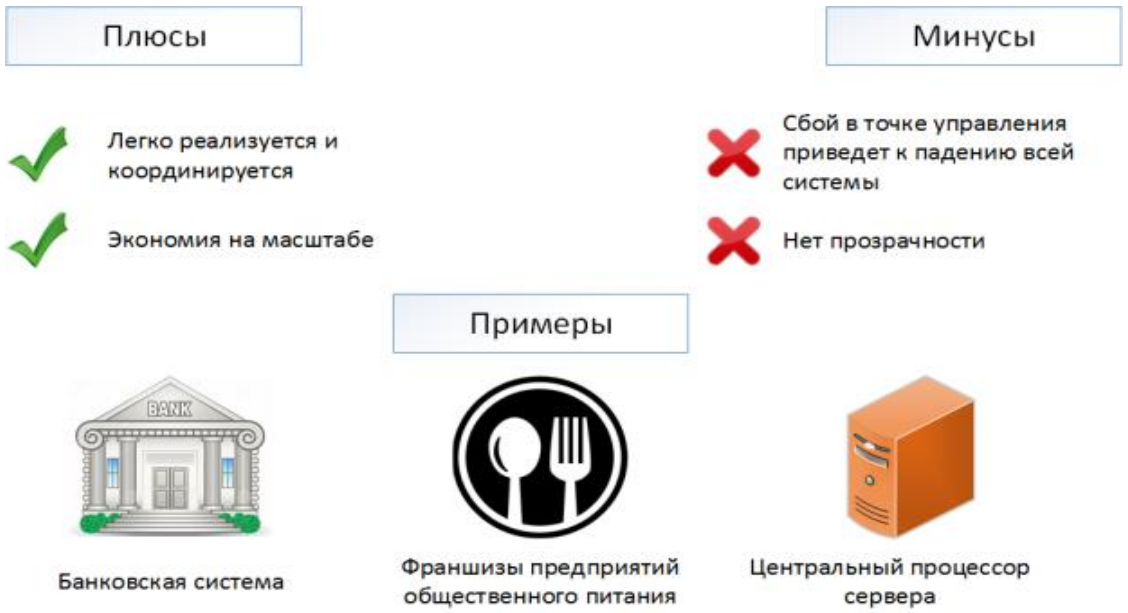

Рисунок 5 – Плюсы и минусы централизованной системы

Примеры централизованных систем: банковские системы; франшизы предприятий общественного питания («Макдональдс»); центральный процессор сервера.

Децентрализованные системы

Децентрализованные системы — системы, в которых существует несколько точек управления и полномочия диверсифицированы (рисунок 6). Это делает систему менее чувствительной к сбоям, так как выход из строя одной точки управления не приведет к падению всей системы. Иерархия такой системы больше приближена к горизонтальной по сравнению с централизованной системой.

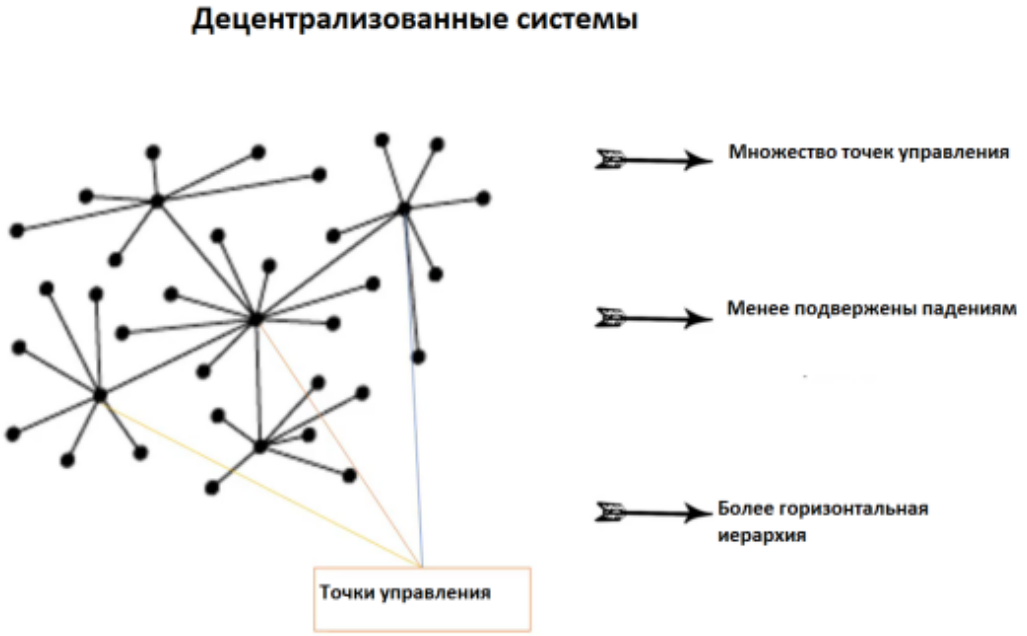

Рисунок 6 – Децентрализованные системы

Минусы децентрализованной системы:

1. Отрицательный экономический эффект, связанный с увеличением масштабов системы. В такой системе из-за увеличения количества точек управления можно получить проблему дублирования задач.

2. Несмотря на то, что децентрализованные системы надежнее централизованных, они все равно подвержены сбоям, поэтому их нельзя назвать полностью надежными (рисунок 7).

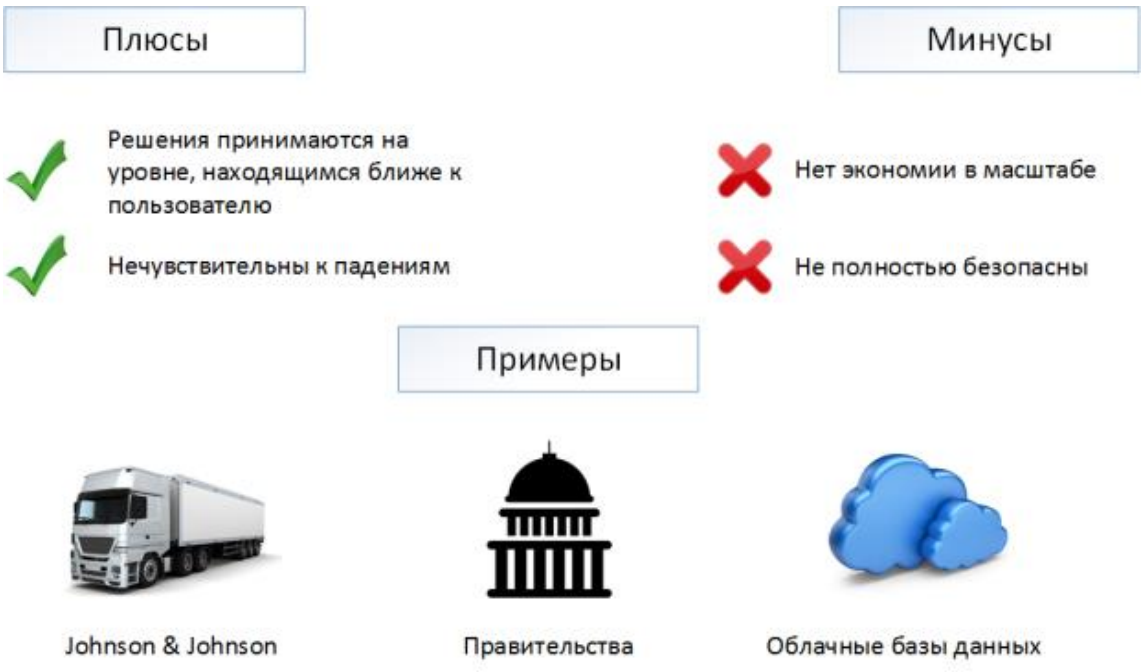

Рисунок 7 – Плюсы и минусы децентрализованной системы

Плюсы децентрализованной системы:

1. Решения в ней принимаются на уровне, более приближенном к пользователю. Таким образом, у органов (точек), принимающих решения, гораздо больше информации о конечном пользователе (если речь идет о продукте) или о людях (если речь идет о правительстве).

2. Эта система меньше подвержена отказам и сбоям, так как теперь в ней несколько точек управления. Сбой в одной точке не приведет к дестабилизации всей системы, как в случае с централизованной системой.

Примеры децентрализованных систем: системы снабжения, такие как *Johnson & Johnson*; правительства, где есть центральные и местные органы власти; облачные базы данных.

Распределенные системы

В распределенных системах любая точка — это точка управления (рисунок 8). Поэтому такие системы фактически невосприимчивы к падениям. Это не значит, что их не будут взламывать, однако, чтобы вывести из строя такую систему, злоумышленник должен взять под контроль или изменить более 50 % точек управления. Затраты на то, чтобы сделать подобное самостоятельно, сведут на нет большую часть прибыли и сделают экономически нецелесообразным попытки взлома. Иерархия таких систем полностью горизонтальна. Каждая точка управления равна любой другой точке управления, и любой субъект, любой участник системы является точкой управления. Итак, все равны, что и приводит к горизонтальной иерархии.

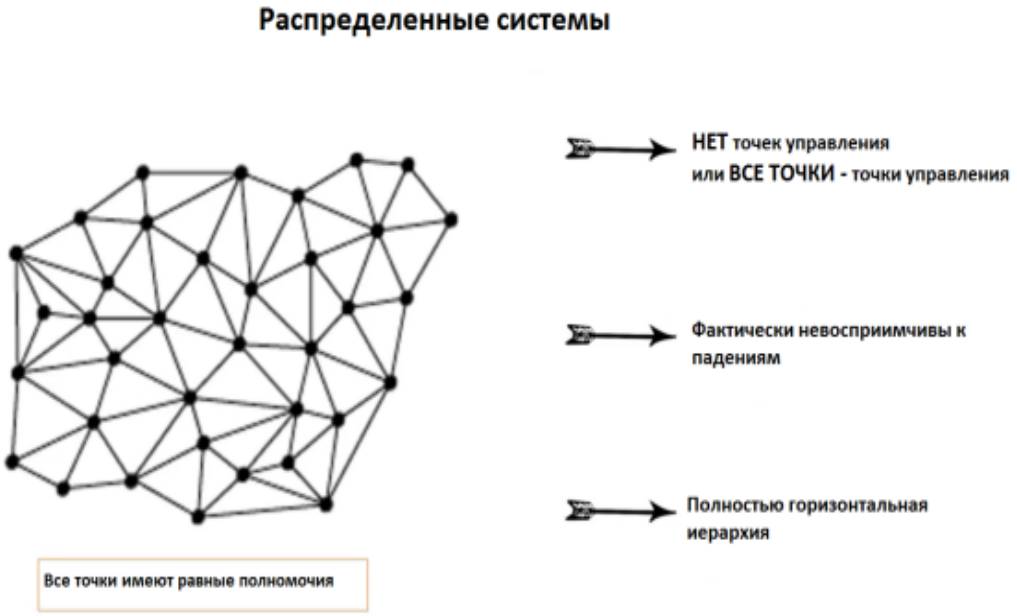

Рисунок 8 – Распределенные системы

Плюсы распределенной системы:

1. Отсутствие необходимости в посредниках.

2. Эту систему экономически нецелесообразно взламывать, что делает ее чрезвычайно надежной и самой безопасной из трех рассмотренных в этой лекции систем.

3. Распределенная система полностью прозрачна, благодаря чему совершение мошенничества становится маловероятным, так как это довольно сложно.

Минусы распределенной системы:

1. Такие системы до сих пор считаются новыми, и их технологии находятся в процессе зарождения.

2. Для стабилизации таких систем потребуется много времени и существенные вложения. Со временем получится сэкономить на масштабе, но на первых порах эти системы довольно дороги.

Примеры распределенных систем представлены на рисунке 9 (криптовалюты, сети блокчейн).

Рисунок 9 – Плюсы и минусы распределенной системы

Далее будут рассмотрены основы системы блокчейн, которую называют «самой революционной технологией века».

1.6. Основы системы блокчейн

Рассмотрим концепцию блокчейна и некоторые из ее основных возможностей, а также ее конкурентоспособные преимущества по сравнению с другими системами. Итак, что такое блокчейн?

1. Блокчейн — это распределенная система управления базами данных.

2. Блокчейн — это распределенный одноранговый регистр. Ранее говорилось о том, что распределенные системы — единственные, где каждый участник является точкой управления и все участники по сути своей равны, а система поддерживается взаимодействием участников друг с другом.

1. Любой участник в системе имеет полную версию базы данных, или, выражаясь техническим языком, регистр транзакций. Поэтому каждому участнику доступны полный список и история транзакций, которые были произведены в данной конкретной сети. Это то, что положено в основу фактора прозрачности системы блокчейн.

2. Любая транзакция объявляется подтвержденной строго после того, как она была одобрена большинством участников сети. Чтобы разрешить транзакцию, требуется консенсус. Это делается с помощью алгоритмов консенсуса и посредством криптографической хэш-функции, благодаря чему взламывать систему злоумышленникам становится экономически невыгодно, и через нее проходят только те транзакции, которые разрешены большинством участников.

3. С помощью системы блокчейн можно передавать любые ценности, это не обязательно должна быть криптовалюта или информация. Любой ресурс или права могут быть переданы через сеть.

4. Блокчейн — это технология, которая лежит в основе системы биткойн. В 2008 году, когда Сатоси Накамото выпустил документ об одноранговой системе, названной биткойн, люди сначала экспериментировали с идеей биткоин, а затем поняли, что базовая технология этой системы может использоваться для других целей. Эта технология и стала известна как блокчейн.

5. Блокчейн — это не биткойн. Порой люди не могут разграничить понятия «биткойн» и «блокчейн» и понять, что это не одно и то же. Можно сказать, что блокчейн — это прикладная система для системы биткойн. Блокчейн — это технология, которая предлагает множество вариантов ее использования в разных видах деятельности, о которых

будет рассказано в следующих лекциях. И биткойн является таким приложением, т. е. использует технологию блокчейн (рисунок 10).

Рисунок 10 – Блокчейн и Биткойн — не одно и то же

Итак, блокчейн позволяет пользователям передавать любые ценности. Это могут быть криптовалюты, автомобили, информация, интеллектуальная собственность. Все пользователи соединены между собой. Система хранит множество копий записей, что обеспечивает ее прозрачность и надежность. Отсутствие посредника в этой системе снижает расходы. Таким образом, все эти характеристики делают блокчейн более безопасным, надежным и дешевым средством для совершения транзакций.

Основные преимущества системы блокчейн (рисунок 11):

1. Отсутствие посредника. Система уравновешена и зависит от большого количества пользователей, что обеспечивает ее бесперебойное функционирование. Для того чтобы подтверждать транзакции, не требуется посредник или какая-то третья сторона. Это довольно важно, так как в противоположной ситуации посредник увеличивает расходы и снижает эффективность, а также замедляет работу системы.

2. Расширяет полномочия пользователей. Все пользователи имеют равные полномочия и отсутствует какая-либо иерархия. Каждый пользователь ответственен за подтверждение транзакций и поддерживает самостоятельность системы.

3. Целостность процессов. Существует систематизированная процедура подтверждения транзакций, что позволяет каждому пользователю доверять системе.

4. Прозрачность и неизменность. Идея неизменности гласит, что любая предыдущая запись или транзакция не может быть стерта. Это дает гарантии отсутствия какого-либо мошенничества, потому что никто не может вернуться к предыдущей записи, изменить стоимость или какую-то конкретную запись для своей выгоды. Чтобы изменить предыдущие записи, сети нужно предложить новую транзакцию, которую должен одобрить каждый ее участник.

5. Более быстрые транзакции. На сегодняшний момент это не совсем так, так как транзакции *Visa* и *MasterCard* гораздо быстрее, но сети блокчейн становятся быстрее и развиваются. Как уже говорилось, эта технология все еще находится в процессе становления, но по мере того, как все больше и больше пользователей присоединяются к сети, возрастает количество добытчиков, и время проведения транзакции сокращается. Существуют мнения, что блокчейн превзойдет по этому показателю существующие системы и станет самой быстрой из доступных систем — стоит только достаточному количеству пользователей присоединиться к сети.

6. Низкие расходы на транзакции. Система дешевле, так как в ней нет посредника, и это снижает расходы (рисунок 11).

Рисунок 11– Основные преимущества системы блокчейн

Итак, блокчейн, возможно, самая дешевая, надежная и прозрачная система из всех существующих, которая к тому же скоро станет самой быстрой. Она наделяет пользователей большими полномочиями, при этом сокращая полномочия посредников, а порой и полностью

лишая их полномочий. В современном мире посредники существуют везде, начиная с банков и заканчивая правительством. Долгое время существовало мнение, что их функция во всех технологических процессах очень важна. Если бы был способ передать технологиям их функции, это принесло бы обоюдную пользу и производителю, и потребителю. Это время наступило: блокчейн — технология, которая снизит зависимость от посредников.

1.7. Бизнес-среда структуры блокчейн

Представим краткий анализ бизнес-среды структуры блокчейн, стадии процесса ее принятия, а также инвестиции в нее, которые делают компании, работающие в данной сфере.

Как уже говорилось ранее, блокчейн — это децентрализованный цифровой реестр с открытым исходным кодом. Он существует в виде распределенной базы данных, которая содержит постоянно увеличивающийся список упорядоченных записей.

Какова же краткая история становления системы блокчейн, что такое процесс принятия, каков прогресс этой структуры и когда, по мнению экспертов, эта технология будет полностью принята? Хронологию событий, связанных с возникновением и развитием системы блокчейн, можно найти на сайте *MarhsClearSight*.

В 2008 году Сатоси Накамото опубликовал документ о новой криптовалюте под названием биткойн, основанной (хотя в то время об этом никто не знал) на использовании технологии блокчейн.

В 2013 году началось пристальное изучение вариантов использования технологии блокчейн. Были запущены такие проекты, как *Ethereum* и *Bitcoin 2.0. Ethereum* — это платформа на основе народно-общественного финансирования (краудфандинг), которая позволяет любому желающему внедрить технологию блокчейн. *Ethereum* схожа с блокчейн, но в нее внесены некоторые изменения.

В 2015 году отдельные игроки рынка, включая такие сообщества, как *R3* и *DHA*, положили начало сотрудничеству, направленному против крупнейших финансовых институтов с целью создать сети на основе блокчейн для осуществления финансовых операций.

В 2016 году начинающие компании и банки начали инвестировать средства в развитие системы блокчейн. Участники стартапов посвящали свое время поиску путей использования системы блокчейн, банки делали в нее инвестиции.

Сейчас эксперты считают, что скоро начнут применяться распределенные приложения, а к 2023 году система блокчейн полностью заменит существующие системы. Эксперты также полагают, что к 2026 году технология блокчейн будет широко распространена во всех сферах деятельности.

К 2015 году в блокчейн было вложено около 1,4 млрд долларов. Количество инвестиций, сделанных венчурными инвестиционными фондами (*VC*), в 2015 году резко возросло. Число сделок достигло пика в 2014 году и с тех пор снижается. Это происходит из-за того, что венчурные инвестиционные фонды и фонды прямого инвестирования признали ведущих игроков данного рынка и начали фокусировать инвестиции исключительно на этих компаниях. Это объясняет, почему в 2015 году суммы инвестиций выросли, а количество сделок уменьшилось. В 2016 году и суммы инвестиций, и количество сделок упали. В одном исследовательском отчете называется причина этого: венчурные фонды ожидают, что компании добьются внедрения блокчейн, а не будут использовать опытные образцы (рисунок 12).

Рисунок 12 – Хронология и перспективы блокчейн

Было проведено исследование — с сайта *blockchain.info* загрузили некоторую информацию о размерах инвестиций 400 инвесторов в блокчейн, которую распределили по порядку — от самых крупных к мелким, начиная с институциональных инвестирований, таких как хэдж-фонды и инвестиционные банки, и заканчивая компанией *National Health Investments*. Самые крупные игроки — D*ata Collective, Mitsubishi UFJ Capital, Andreessen Horowitz* (еще один венчурный фонд, который специально фокусировался на блокчейн), — делали

серьезный упор на эту новую технологию. Также в списке были такие фонды, как *Union Square Ventures* и *Greylock Partners* — они возглавляли эти списки.

Куда же пошли все эти деньги?

Для того чтобы проанализировать это, была собрана информация о самых крупных компаниях с учетом полученных ими сумм. Эту группу возглавляет компания *Circle Internet Financial*, которая получила более чем 200 млн долларов. За ней следуют компания *Ripple Lab*, у которой есть своя криптовалюта и которая работает в сфере транзакций между компаниями, и *Coinbase* с одноименным электронным кошельком. Нетрудно заметить, что большинство этих компаний работают в сфере биткойн. Почему? Ведь, как говорилось ранее, биткойн — это не технология блокчейн, у которой может быть множество вариантов применения. Дело в том, что эти компании появились гораздо раньше, а применение технологии блокчейн начали искать после появления системы биткойн. Поэтому причина того, что все инвестиции ушли в эти компании, — в том, что все они какое-то время работали с биткойн.

Так как технология блокчейн сравнительно новая, у всех этих компаний хорошие перспективы. Применение технология все еще находится на стадии экспериментов. Поэтому большинство ведущих компаний в области блокчейн работают с системой биткойн, будь то перевод денег между компаниями, транзакции и т. д.

Вот некоторые ведущие компании, не использующие систему биткойн, но работающие с системой блокчейн:

1. *Coin Desk*. Это новостное биткойн-агентство, которое предоставляет новости о цифровых валютах и их аналитические обзоры. На сайте агентства можно найти много важной информации и отслеживать ее обновления, поэтому он полезен тем, кто хочет быть в курсе последних событий в сфере биткойн.

2. *Ethereum*. Платформа с открытым исходным кодом, с помощью которой можно создавать децентрализованные приложения на базе блокчейн. Это одна из самых революционных компаний века, начиная с концепции, с которой они работают, и, заканчивая техникой финансирования. Компания работает на основе народно-общественного финансирования и уверяет, что инвесторы ее не подводят. *Ethereum* — ведущая компания эры общественного использования технологии блокчейн.

3. *Ripple*. Компания предлагает дешевые международные платежные решения для различных компаний.

4. *Poloneix Exchange*. Биткойн-биржа, предлагающая более 100 торговых пар для обмена.

Необходимо подчеркнуть, что это лишь некоторые из ведущих компаний.

Не стоит забывать и о компаниях-добытчиках (майнерах), поддерживающих сеть. Если майнеры исчезнут, сеть просто перестанет работать. Майнинг-пул (объединение добытчиков) — это инфраструктура, установленная компанией с целью добычи (майнинга) биткойнов или майнинга транзакций, а также их подтверждения. Большинство майнинг-пулов сегодня работает в сфере биткойн. Согласно данным хэшрейта, список майнеров возглавляют компании *DiscusFish* и *AntPool*. Хэшрейт — это количество хэшей, которые вычисляются за определенный период времени. Фактически, хэшрейт может быть использован как показатель того, насколько активен тот или иной майнинг-пул. Поэтому *DiscusFish* и *AntPool* (*AntPool* в настоящее время известна как финансовая группа *Ant*) — это некоторые из самых активных компаний в области майнинга.

Лучше всего характеризуют бизнес-среду блокчейн компании *Frost & Sullivan* и *Outlier Ventures*. Они поделили блокчейн с учетом различных вариантов использования в разных сферах деятельности. Изучение деятельности этих и подобных компаний дает представление о различных вариантах использования блокчейн.

Глава 2
КРИПТОГРАФИЯ, ЛЕЖАЩАЯ В ОСНОВЕ КРИПТОВАЛЮТ

2.1. Основные понятия и определения криптографии

Цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. При использовании криптографических методов посторонний наблюдатель может довольно легко обнаруживать сами сообщения, при этом очевиден факт их секретности[1].

Наука о методах и алгоритмах шифрования называется криптографией. Людей, занимающихся криптографией, зовут криптографами. Криптоаналитики являются специалистами в области криптоанализа — науки о вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным. Раздел науки, объединяющий криптографию и криптоанализ, именуется криптологией.

Попытка криптоанализа называется криптоаналитической атакой. Успешная криптоаналитическая атака, в результате которой противнику становится известным содержание зашифрованного сообщения, называется взломом, или вскрытием (раскрытием) шифра.

Различные криптографические алгоритмы обладают разной надежностью, чаще называемой стойкостью алгоритма шифрования или стойкостью шифра. Стойкость зависит от того, насколько легко криптоаналитик может взломать шифр.

Криптографическое преобразование информации — взаимнооднозначное математическое преобразование, зависящее от секретного параметра — ключа. Обычно криптографическое преобразование ставит в соответствие открытой информации, представленной в некоторой цифровой кодировке, зашифрованную информацию, также в цифровой кодировке (рисунок 13).

Процесс преобразования открытого текста с целью сделать непонятным его смысл для посторонних называется шифрованием. В результате шифрования сообщения получается шифртекст (криптограмма). Причем шифрование различных открытых текстов с использованием одного и того же ключа дают разные шифртексты.

---

[1] Васильева И. Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата. – Москва: Издательство Юрайт, 2019. 349 с.

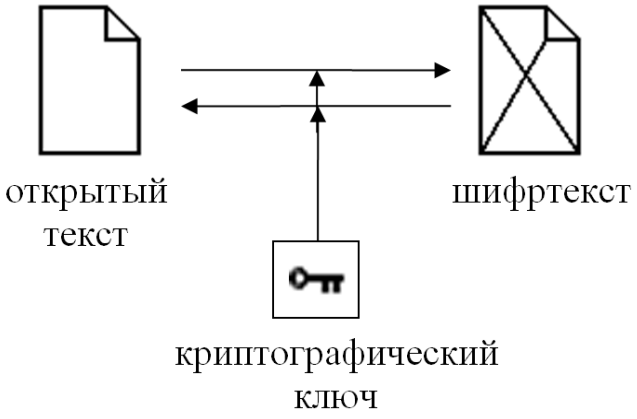

Рисунок 13– Криптографическое преобразование

Процесс обратного преобразования шифртекста называется расшифрованием. Расшифрование — процесс извлечения открытого текста из криптограммы при условии знания секретного параметра шифра — ключа. При этом открытый текст должен однозначно определяться по известному шифртексту и ключу шифрования.

Дешифрование — процесс извлечение открытого текста из криптограммы без знания ключа (при неизвестном ключе и, возможно, неизвестном алгоритме шифрования).

Термин «дешифрование» обычно применяется к процессу криптоанализа шифртекста.

Каждое криптографическое преобразование однозначно определяется ключом и описывается некоторым криптографическим алгоритмом.

История криптографии насчитывает тысячелетия, однако ее теоретическое обоснование было дано сравнительно недавно — лишь в XX веке. Одной из основополагающих теоретических работ по криптографии является статья Клода Шеннона (*Claude Shannon*) «Теория связи в секретных системах», опубликованная в открытой печати в 1949 году.

Ниже изображена предложенная Шенноном схема секретной системы (рисунок 14).

На стороне отправителя (A) имеются два источника информации — источник сообщений и источник ключей. Источник ключей выбирает из множества всех возможных ключей один ключ *k*, который будет использоваться в этот раз. Ключ передается отправителю и получателю (B) сообщения таким образом, что его невозможно перехватить. То есть канал передачи ключа является закрытым (защищенным). Этот канал абсолютно надежен и недоступен для других.

В то же время основной канал обмена сообщениями является общедоступным. Противник (E) может перехватывать передаваемые сообщения, то есть канал передачи шифртекстов является открытым.

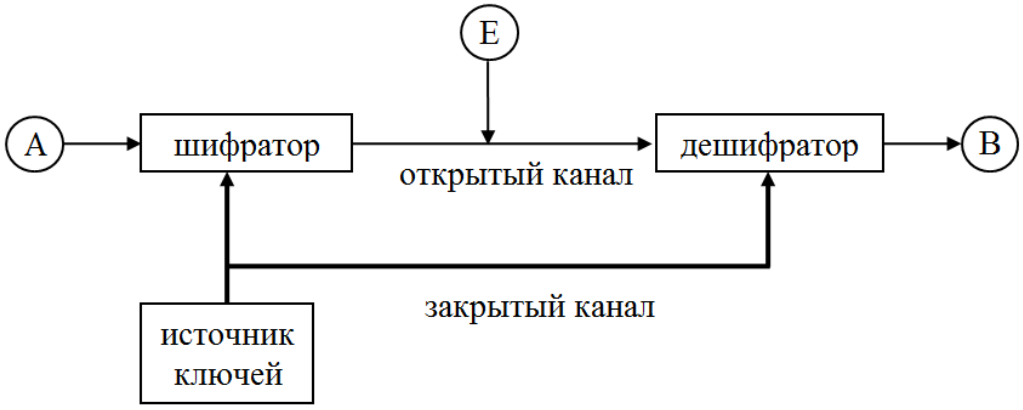

Рисунок 14 – Классическая схема секретной системы

Секретная система, или в современной терминологии — криптосистема, шифр (рисунок 15), определяется как семейство взаимнооднозначных отображений множества возможных сообщений X во множество криптограмм Y, проиндексированное элементами k из множества ключей:

$$\{Fk: X \rightarrow Y, k \in K\}, \quad (1)$$

где K — *пространство ключей* — набор всех возможных значений ключа k.

$$K = \{k\}, \quad (2)$$

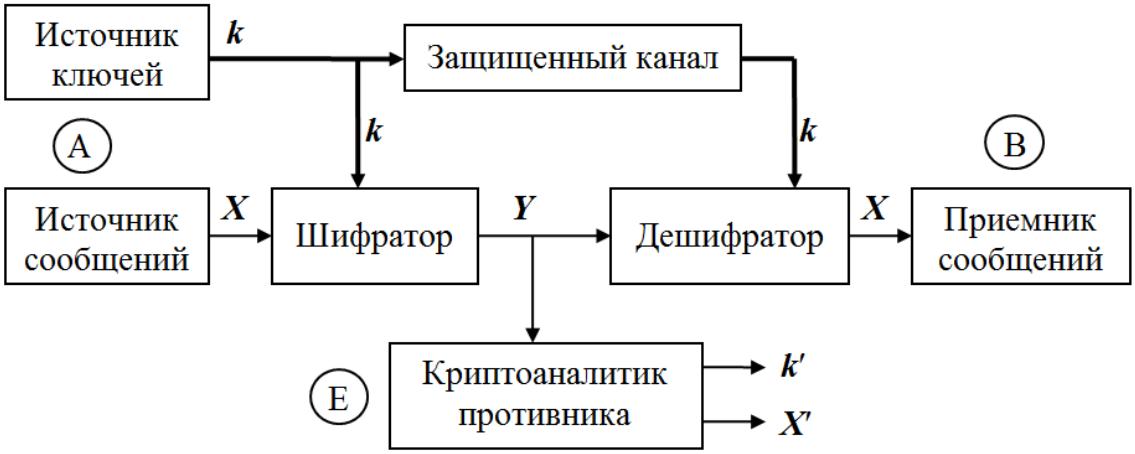

Рисунок 15 – Подробная схема секретной системы

Предполагается, что противнику известна используемая криптографическая система, то есть семейство криптографических преобразований и вероятности выбора различных ключей. Однако он не знает, какой именно ключ k выбран, и остальные возможные ключи столь же важны для него, как и истинный.

Под противником понимается любой субъект, не имеющий права ознакомления с содержанием передаваемой информации. В качестве противника может выступать криптоаналитик, владеющий методами раскрытия шифров.

Процесс расшифрования сообщения для легального получателя информации состоит в применении криптографического отображения, обратного по отношению к отображению, использованному при шифровании.

Процесс дешифрования для противника представляет собой попытку определить сообщение (или конкретный ключ), имея в распоряжении только криптограмму и априорные вероятности различных ключей и сообщений.

2.2. Симметричные и асимметричные шифры

Симметричным называют криптографический алгоритм, в котором как для шифрования, так и для и расшифровки, применяют один и тот же ключ. Такие алгоритмы именуются одноключевыми, или алгоритмами с секретным ключом (рисунок 16).

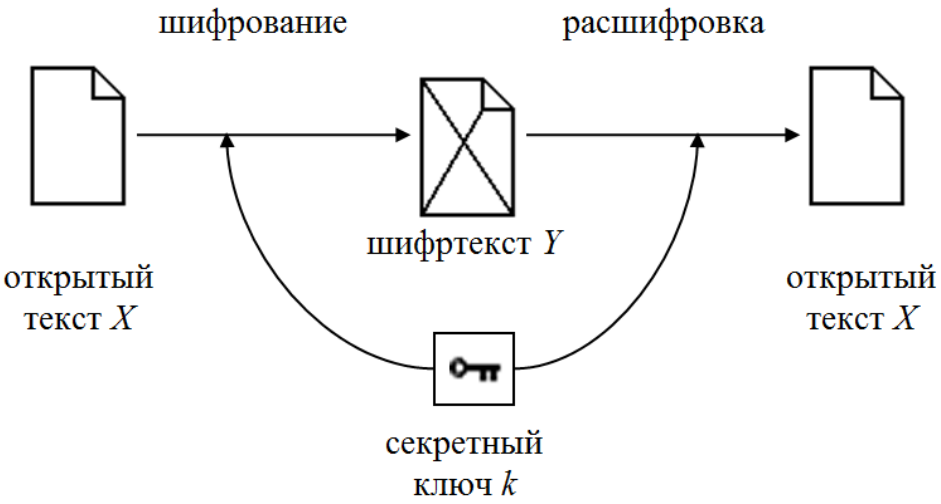

Рисунок 16 – Симметричная схема шифрования

Одно из главных преимуществ симметричных методов — их производительность (быстрота шифрования и расшифровки), а главный недостаток — проблема распределения ключей (необходимость надежной передачи секретного ключа получателю при обмене сообщениями). Применение шифрования обусловлено тем, что абоненты не доверяют каналу передачи данных. Неизбежно возникает вопрос: как передать ключ в не доверенной среде и при этом не позволить злоумышленникам перехватить его.

Преимущества криптографии с симметричными ключами:

– Высокая производительность. Высокая производительность позволяет использовать алгоритмы симметричной криптографии для шифрования данных в режиме реального времени.

– Высокая стойкость. При прочих равных условиях стойкость криптографического алгоритма определяется длиной ключа. В настоящее время для современных блочных алгоритмов симметричного шифрования считается достаточной длина ключа в 128 бит, в то время как асимметричные системы используют ключи не менее 1 024 бит, криптография на эллиптических кривых — ключи длиной 256 бит.

Недостатки криптографии с симметричными ключами:

– Проблема распределения ключей. Так как для шифрования и расшифровки используется один и тот же ключ, требуются очень надежные механизмы для их распределения между абонентами.

– Масштабируемость. Так, как и отправитель, и получатель используют единый ключ, количество необходимых ключей возрастает в геометрической прогрессии в зависимости от числа участников коммуникации. Для организации обмена зашифрованными сообщениями между N пользователями потребуется порядка $N^2/2$ ключей. Для двух пользователей достаточно одного ключа, для трех — потребуется три, а для четырех — шесть ключей. 10-и пользователям необходимо иметь 45 ключей, а для 1 000 пользователей потребуется уже 499 500 ключей.

Ограниченное использование. Криптография с секретным ключом только конфиденциальность (секретность) защищаемой информации, с ее помощью невозможно обеспечить такие свойства информации, как подтверждение или невозможность отказа от авторства (аутентичность и неотрекаемость).

Несмотря на достижения в области симметричной криптографии, к середине 1970-х гг. стала остро осознаваться проблема неприменимости данных методов для решения целого ряда задач.

Во-первых, при использовании симметричных шифров необходимо отдельно решать часто нетривиальную задачу распределения ключей. Несмотря на использование иерархий ключей и центров распределения, в какой-то начальный момент ключ (или мастер-ключ) все равно должен быть передан по безопасному каналу. Но такого канала может просто не быть, или он может быть достаточно дорогостоящим.

Во-вторых, при использовании методов симметричного шифрования подразумевается взаимное доверие сторон, участвующих во взаимодействии. Если это не так, совместное использование одного и того же секретного ключа может быть нежелательно.

Третья проблема связана с необходимостью проведения аутентификации информации и защиты от угроз, связанных с отказом отправителя (получателя) от факта отправки (получения) сообщений.

Перечисленные проблемы являются весьма существенными, и работа над их решением привела к появлению асимметричной криптографии, также называемой криптографией с открытым ключом. Эти системы являются двухключевыми и характеризуются тем, что для шифрования и для расшифрования используются разные ключи, связанные между собой некоторой зависимостью.

Любое сообщение, зашифрованное с использованием одного из этих ключей, может быть расшифровано только с использованием парного ему ключа.

Один из ключей (например, ключ шифрования) может быть сделан общедоступным — открытым (*public key*), и в этом случае проблема получения общего секретного ключа для связи отпадает. Поскольку один ключ из пары делается общедоступным, такие системы получили также название криптосистем с открытым ключом.

Открытый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью этого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует второй — личный ключ (*private key*), который держится в секрете.

Естественно потребовать, чтобы знание открытого ключа (ключа шифрования) не давало бы возможности определить парный ему личный ключ (ключ расшифрования).

В асимметричной схеме передачи шифрованных сообщений оба ключа являются производными от единого порождающего мастер-

ключа. Когда два ключа (открытый и личный) сформированы на основе одного мастер-ключа, они зависимы в математическом смысле, однако в силу вычислительной сложности ни один из них не может быть вычислен на основании другого.

После того, как сформированы оба ключа (и открытый, и личный закрытый), мастер-ключ уничтожается, и таким образом пресекается любая попытка восстановить в дальнейшем значения производных от него ключей.

Обозначим отправителя сообщения как А, а получателя — В. для обеспечения секретности (рисунок 17) отправитель А шифрует сообщение открытым ключом получателя ОК (В), а получатель В расшифровывает полученное сообщение своим личным ключом ЛК (В). Поскольку никто, кроме получателя не знает его личного ключа ЛК (В), расшифровать сообщение сможет только он один.

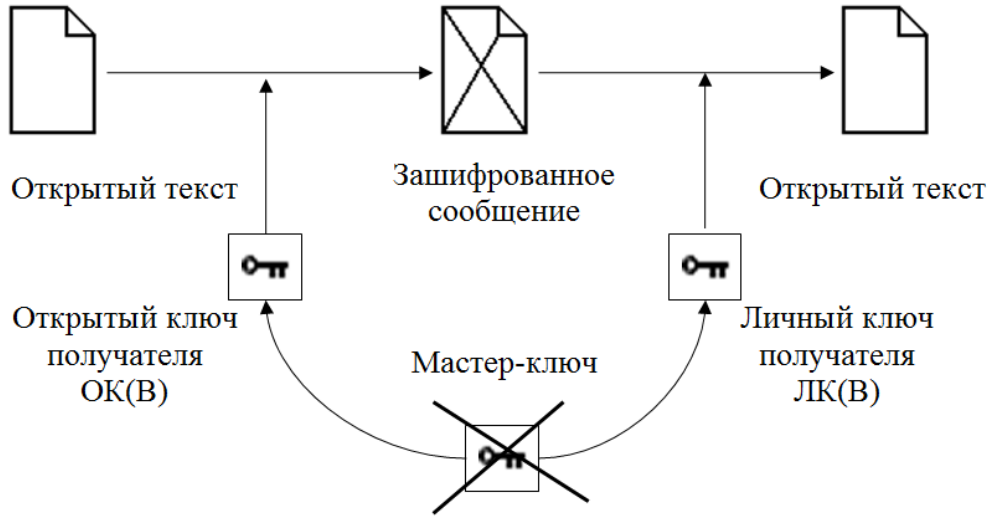

Рисунок 17 – Криптография с открытым ключом: обеспечение секретности

Если сделать общедоступным ключ расшифрования, то на базе полученной системы можно построить систему аутентификации передаваемых сообщений. В этом случае (рисунок 18) шифрование производится с помощью личного ключа отправителя ЛК (А), расшифровать же сообщение и таким образом проверить подлинность отправителя А может любой абонент с помощью известного открытого ключа ОК (А).

В отличие от симметричных криптосистем, базирующихся на двусторонних функциях, центральным понятием в теории криптографических систем с открытым ключом является понятие односторонней функции.

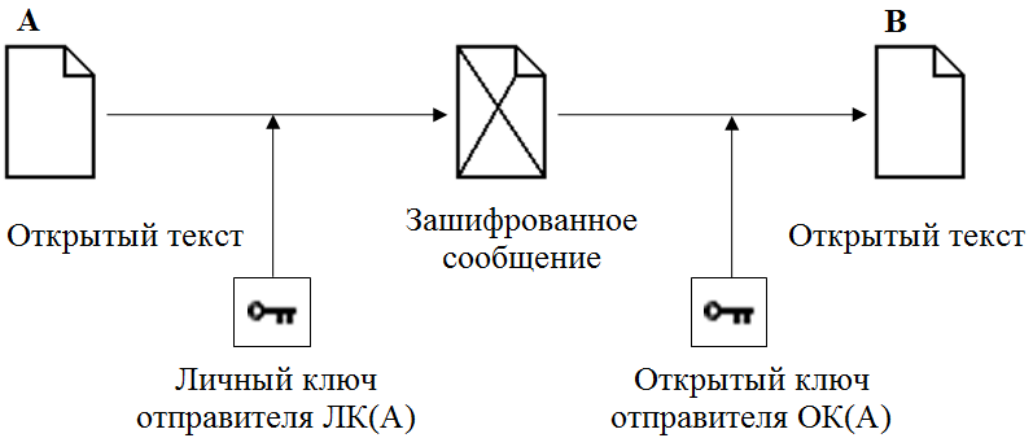

Рисунок 18 – Криптография с открытым ключом: обеспечение аутентичности и неотрекаемости

Пусть дана функция f: $X \to Y$, $y = f(x)$, определенная на конечном множестве X, $x \in X$, для которой существует обратная функция $x = f^{-1}(y)$, $y \in Y$.

Функция f называется односторонней (однонаправленной), если выполняются следующие условия:

– для всякого $x \in X$ легко вычислить значение функции $y = f(x)$;

– для произвольного $y \in Y$ нахождение значения $x \in X$, такого, что $x = f^{-1}(y)$ (то есть вычисление обратной функции) является трудной вычислительной задачей.

Односторонней функцией с секретом (функцией-ловушкой) называется односторонняя функция, для которой обратную функцию вычислить просто, если имеется некоторая дополнительная информация, и сложно, если такая информация отсутствует.

Односторонней функцией с секретом k, называется такая функция fk: $X \to Y$, для которой выполняются следующие условия:

– для всякого $x \in X$ легко вычислить значение функции $y = fk(x)$, где $y \in Y$, даже в том случае, если значение k неизвестно;

– не существует легкого (эффективного) алгоритма вычисления обратной функции $fk^{-1}(y)$ без знания секрета k;

– при известном k вычисление $fk^{-1}(y)$ для $y \in Y$ не представляет существенной сложности.

В качестве задач, приводящих к односторонним функциям, можно привести:

1. Разложение числа на простые сомножители. Вычислить произведение двух простых чисел очень просто. Однако, для решения

обратной задачи в общем случае — разложения любого заданного числа на простые сомножители — эффективного алгоритма в настоящее время не существует.

2. Дискретное логарифмирование в конечном простом поле (проблема Диффи-Хеллмана). Допустим, задано большое простое число p и пусть x — целое число: $0 < x < p$. Тогда для любого заданного x вычислить $y = a^x \bmod p$ — просто, а нахождение дискретного логарифма $x = \log_a y \bmod p$ по заданным y и p является сложной вычислительной задачей.

Криптосистемы с открытым ключом основываются на односторонних функциях с секретом. При этом открытый ключ определяет конкретную реализацию функции, а личный ключ дает информацию о секрете. Любой, знающий секрет, может легко вычислять функцию в обоих направлениях, но тот, у кого такая информация отсутствует, может производить вычисления только в одном направлении.

В частности, односторонняя функция с секретом может быть использована для шифрования информации. Пусть M — исходное сообщение. Получатель выбирает одностороннюю функцию с секретом, и тогда любой, кто знает эту функцию, может зашифровать сообщение для данного получателя, вычислив значение криптограммы $C = fk(M)$. Расшифровать же данную криптограмму сможет только законный получатель, которому известен секрет k.

Таким образом, прямое направление односторонней функции с секретом используется для шифрования и для верификации цифровых подписей, а обратное — для расшифровки и выработки цифровой подписи.

Во всех криптосистемах с открытым ключом, чем больше длина ключа — тем выше стойкость, определяемая различием между усилиями, необходимыми для вычисления функции в прямом и обратном направлениях тому, кто не обладает информацией о секрете.

Все практические криптосистемы с открытым ключом основываются на функциях, считающихся односторонними, но это свойство не было доказано в отношении ни одной из них. Это означает, что теоретически возможно создание алгоритма, позволяющего легко вычислять обратную функцию без знания секрета. В этом случае, криптосистема, основанная на этой функции, станет бесполезной.

Асимметричные криптосистемы идеально сочетаются с использованием общедоступных сетей передачи данных, решая задачу распределения ключей.

Недостатком криптографии с открытым ключом является ее низкая производительность (большие затраты процессорного времени на шифрование и расшифровку), что затрудняет ее использование для оперативного обмена пространными сообщениями в режиме диалога. Поэтому в мировой практике шифрование с открытыми ключами в чистом виде обычно не применяется.

Наиболее широкое распространение получили смешанные (гибридные) методы, сочетающие достоинства обеих криптографических систем. Принцип работы смешанных методов шифрования заключается в следующем:

1. Для очередного сеанса обмена сообщениями генерируется симметричный (сеансовый) ключ.

2. Затем этот ключ зашифровывается с помощью асимметричной криптосистемы и пересылается другой стороне взаимодействия.

3. После передачи секретного ключа шифрование всех последующих сообщений выполняется с помощью симметричной криптографии.

4. При завершении текущего сеанса связи симметричный ключ уничтожается.

Применение криптографических алгоритмов в технологиях криптовалют заменяет собой привлечение стороннего посредника при осуществлении блокчейн-транзакций.

В этом контексте важно провести различие между двумя компонентами блокчейн-адреса, а именно закрытым ключом и открытым ключом.

Открытый ключ можно использовать для просмотра истории транзакций пользователя, но для того, чтобы произвести транзакцию, нужно знать еще и закрытый ключ. Закрытый ключ необходим для получения доступа к счету и выполнения транзакции.

2.3. Криптографические решения в криптовалюте (биткойн)

Криптовалюта (биткойн) использует в своей системе защиты популярные и надёжные криптографические решения, а именно, криптографию на эллиптических кривых (*Elliptic curve cryptography, ECC*). Она основана на особой математической функции — эллиптической кривой[1].

[1] URL: https://habr.com/ru/post/319868/ (дата обращения: 17.08.2021).

Сегодня криптосистемы на эллиптических кривых используются в *TLS, PGP* и *SSH*, важнейших технологиях, на которых базируются современный веб и мир информационных технологий, не говоря уже о биткойнах и других криптовалютах.

До того, как *ECC* стала популярной, почти все алгоритмы с открытым ключом основывались на *RSA, DSA* и *DH*, альтернативных криптосистемах на основе модулярной арифметики. *RSA* и компания по-прежнему популярны, и часто используются вместе с *ECC*. Однако, несмотря на то, что магия, лежащая в фундаменте *RSA* и подобных ей алгоритмов легко объяснима и понятна многим, а грубые реализации пишутся довольно просто, основы *ECC* всё ещё являются для большинства людей загадкой.

В этом разделе монографии рассмотрим основы мира криптографии на эллиптических кривых. Наша цель — не создание полного и подробного руководства по *ECC* (в Интернете полно информации по этой теме), а простой обзор *ECC* и объяснение того, почему её считают безопасной.

В частности, рассмотрим следующие темы:

1. Эллиптические кривые над вещественными числами.
2. Эллиптические кривые над конечными полями.
3. Генерирование пар ключей и два алгоритма *ECC*: *ECDH* и *ECDSA*.

2.3.1. Эллиптические кривые над вещественными числами

Эллиптические кривые

Во-первых, что такое эллиптическая кривая? В *Wolfram MathWorld* есть отличное и исчерпывающее определение. Но для нас достаточно того, что эллиптическая кривая — это просто множество точек, описываемое уравнением: $y^2 = x^3 + ax + b$,где $4a^3 + 27b^2 \neq 0$ (это необходимо, чтобы исключить особые кривые).

Приведённое выше уравнение называется обычной формулировкой Вейерштрасса для эллиптических кривых[1].

В зависимости от значений a и b эллиптические кривые могут принимать на плоскости разные формы. Как можно легко увидеть и проверить, эллиптические кривые симметричны относительно оси X (рисунок 19).

[1] Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Москва: Ленанд, 2020. Кн. 2: Протоколы криптографии на эллиптических кривых. 376 с.

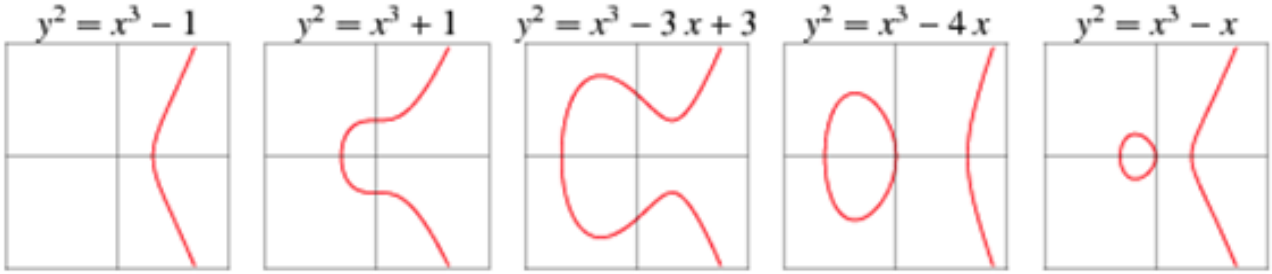

Рисунок 19 – Эллиптические кривые в зависимости от значений параметров *a* и *b*

Пусть есть две точки $P, Q \in \alpha$. Их суммой называется точка $R \in \alpha$, которая в простейшем случае определяется следующим образом: проведем прямую через P и Q — она пересечет кривую α в единственной точке, назовем ее $-R$. Поменяв у координату точки $-R$ на противоположную по знаку, мы получим точку R, которую и будем называть суммой P и Q, то есть $P + Q = R$ (рисунок 20).

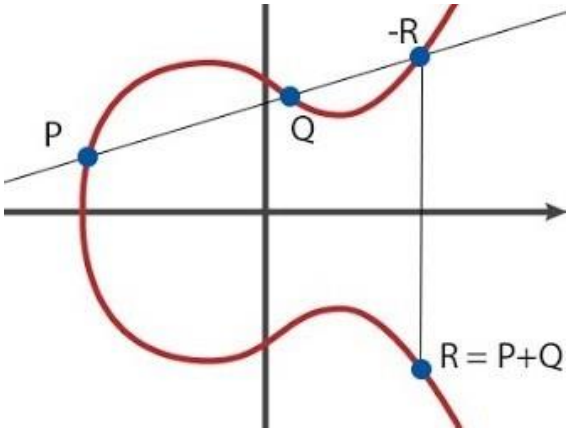

Рисунок 20 – Геометрические построения
для получения суммы двух точек
на эллиптических кривых

Важно понимать, что мы именно вводим такую операцию сложения — если будем складывать точки в привычном понимании, т. е. складывая соответствующие координаты, то получим совсем другую точку $R'(x_1 + x_2, y_1 + y_2)$, которая, не имеет ничего общего с R или $-R$ и вообще не лежит на кривой альфа.

В случае если провести прямую через две точки, имеющие координаты вида $P(a, b)$ и $Q(a, -b)$, то есть получится прямая, проходящая через них, будет параллельна оси ординат (третий график на рисунке 21).

В этом случае отсутствует третье пересечение с кривой альфа, которое обозначено как $-R$. Для того чтобы этого избежать, введем так называемую точку в бесконечности (*point of infinity*), обозначаемую

как *0*, как на рисунке 21. И будем говорить, что в случае отсутствия пересечения, $P + Q = O$.

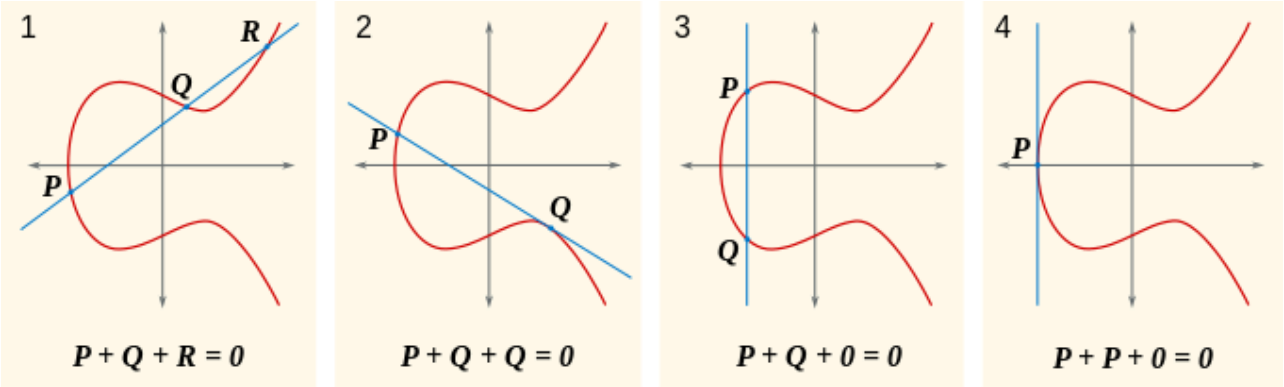

Рисунок 21 – Результаты сложения точек на эллиптических кривых

Особый интерес представляет случай, когда мы хотим сложить точку саму с собой (второй график, точка Q — см. рисунок 21). В этом случае просто проведем касательную к точке Q и отразим полученную точку пересечения относительно Y.

Теперь можно ввести операцию умножения точки на какое-то натуральное число. В результате получим новую точку $K = G*k$, т. е. $K = G + G + ... + G$, k раз. Графическое представление на рисунке 22.

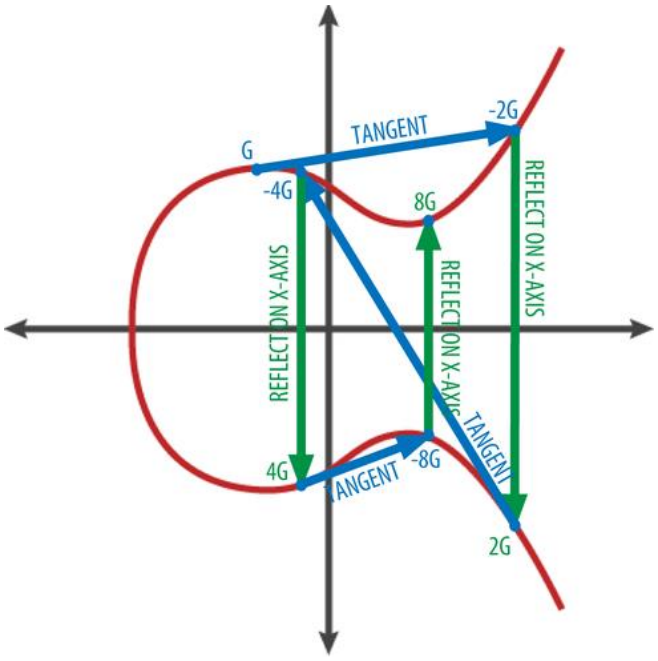

Рисунок 22 – Геометрические построения
для получения результата операции
умножения точки на натуральное число
на эллиптических кривых

2.3.2. Эллиптические кривые над конечными полями

В криптографии на эллиптических кривых используется точно такая же кривая, только рассматриваемая над некоторым конечным полем $F_p = Z / Z_p = \{0, 1, \ldots, p-1\}$, где p — простое число. То есть:

$$y^2 \bmod p = x^3 + ax + b (\bmod p), \qquad (2)$$

Все названные свойства (сложение, умножение, точка в бесконечности) для этой функции остаются в силе, хотя, если начертить данную функцию, то напоминать привычную эллиптическую кривую она будет лишь отдаленно. А понятие «касательной к функции в точке» в таком случае вообще теряет всякий смысл.

Пример, на рисунке 23 представлена функция $y^2 = x^3 + 7$ для $p = 17$:

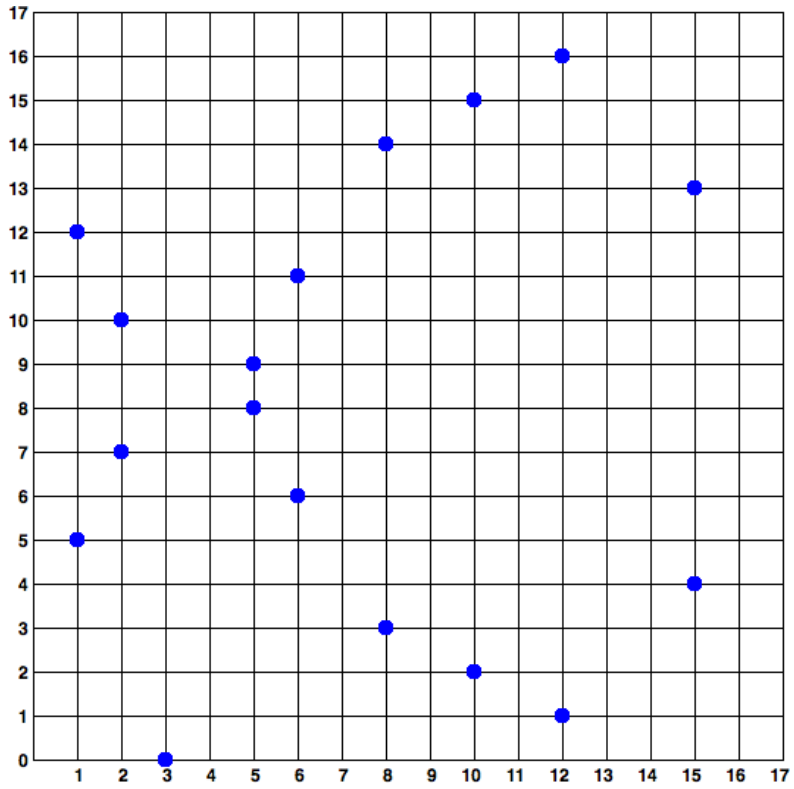

Рисунок 23 – Геометрическое представление функции $y^2=x^3+7$ для p=17

SECP256k1

Если говорить конкретнее о Bitcoin, в нем используется кривая *SECP256k1*. Она имеет вид $y^2 = x^3 + 7$ и рассматривается над полем *Fp*, где p — очень большое простое число, а именно $2^{256} – 2^{32} – 2^9 – – 2^8 – 2^7 – 2^6 – 2^4 – 1$.

Так же для *SECP256k1* определена так называемая *base point*, она же *generator point* — это просто точка, как правило, обозначаемая как *G*, лежащая на данной кривой. Она необходима для создания публичного ключа, о котором будет пояснено далее.

2.3.3. Криптография на эллиптических кривых. Генерирование пар ключей и два алгоритма *ECC*: *ECDH* и *ECDSA*

Цифровая подпись

Изложим основную идею технологии электронной подписи[1].

Определение с сайта *Wikipedia*: «Электронная подпись (ЭП) или электронная цифровая подпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость)».

Общая идея такая такова: Даша хочет перевести 1 BTC (один биткойн) Вове. Для этого она создает сообщение вида:

{«from»:1FXySbm7jpJfHEJRjSNPPUqnpRTcSuS8aN, // Адрес кошелька Даши to: 1Eqm3z1yu6D4Y1c1LXKqReqo1gvZNrmfvN, // Адрес кошелька Вовы amount: 1 // Отправить 1 BTC}.

Потом Даша использует свой приватный ключ (можно считать, что это число, известное только Даша), хэш-сообщения и функцию вида *sing_text (private_key, text)*. На выходе она получит подпись своего сообщения – в случае алгоритма цифровой подписи с использованием эллиптической кривой это будет пара целых чисел, для других алгоритмов подпись может выглядеть по-другому. После этого она рассылает всем участникам сети исходное сообщение, подпись и свой публичный ключ.

В результате, каждый пользователь при желании сможет взять эти данные, функцию вида *validate_signature (public_key, signature, text)* и проверить, действительно ли владелец приватного ключа подписывал это сообщение или же нет. Если внутри сети все пользователи знают, что публичный ключ принадлежит Даше, то возможно определить, отправила эти деньги она или же кто-то пытается сделать это от ее имени (рисунок 24).

[1] См.: Лаптев В. А., Чуча С. Ю. Электронное правосудие. Электронный документооборот. Москва: Проспект, 2021. 240 с.

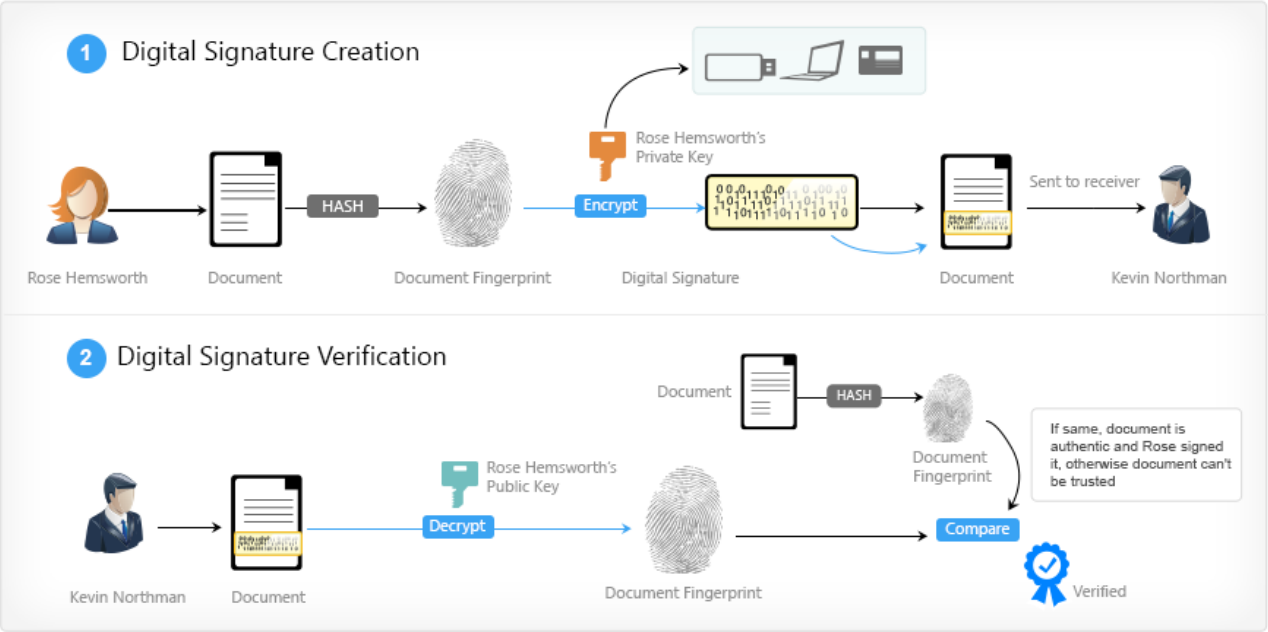

Рисунок 24 – Алгоритм формирования электронной подписи: процедуры подписания электронного документа и верификации ЭП

Затем, предположим, что нашелся человек, который перехватил сообщение Алисы и что-то в нем изменил, совершенно ничтожное количество информации. Но даже в этом случае проверка (верификация) подписи на валидность *validate_signature (public_key, signature, text')* покажет, что сообщение было изменено.

Это очень важная функция *Bitcoin*, потому как сеть распределенная. Мы не можем заранее знать, к кому на обработку попадет транзакция с требованием перевести 1 000 BTC. Но изменить ее (скажем, указать свой адрес в качестве получателя) он не сможет, т. к. транзакция подписана вашим приватным ключом, и остальные участники сети сразу поймут, что в транзакции ошибка.

В действительности процесс довольно сильно отличается от вышеописанного. Здесь наглядным образом показано, что из себя представляет ЭП и зачем она нужна. Транзакции в *Bitcoin* — тема для отдельного разговора.

Приватный ключ

Приватный ключ — это довольно общий термин и в различных алгоритмах электронной подписи могут использоваться различные типы приватных ключей.

Bitcoin используется алгоритм цифровой подписи с использованием эллиптической кривой — в его случае приватный ключ — это некоторое натуральное 256 битное число, то есть самое обычное целое число от 1 до 2^{256}. Технически, даже число 123 456 будет являться

корректным приватным ключом, но очень скоро вы узнаете, что ваши биткоины принадлежат вам ровно до того момента, как у злоумышленника окажется ваш приватный ключ, а значения типа 123 456 очень легко перебираются.

Важно отметить, на сегодняшний день перебрать все ключи невозможно в силу того, что 2^{256} — это невероятно большое число.

Публичный ключ

Пусть *k* — наш приватный ключ, *G* — *base point*, тогда публичный ключ *K = G*k*. То есть, фактически, публичный ключ — это некоторая точка, лежащая на кривой *SECP256k1*.

Два важных нюанса. Во-первых, несложно видеть, что операция получения публичного ключа определена однозначно, то есть конкретному приватному ключу всегда соответствует один единственный публичный ключ. Во-вторых, обратная операция является вычислительно трудной и, в общем случае, получить приватный ключ из публичного можно только полным перебором первого.

Точно такая же связь существует между публичным ключом и адресом, только там все дело в необратимости хэш-функций (рисунок 25).

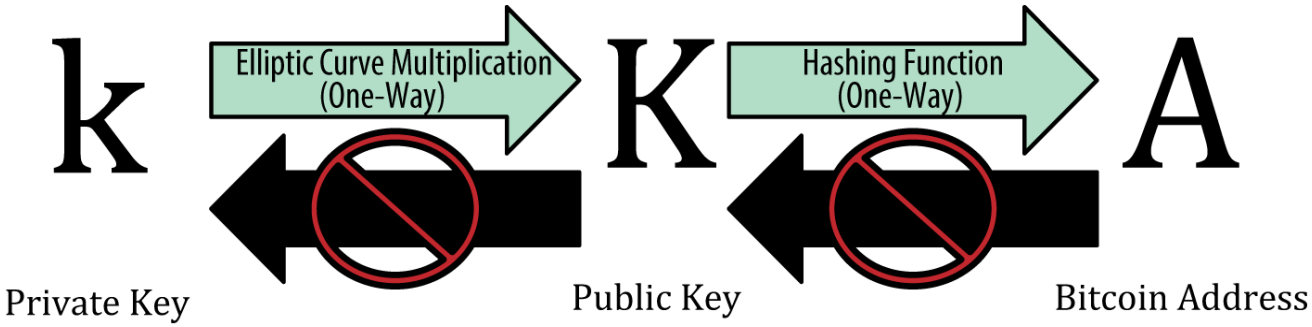

Рисунок 25 – Алгоритм, связывающий формирование приватного (*private*) и публичного (*public*) ключей с использованием эллиптической кривой (*elliptic curve cryptography, ECC*)

Форматы и адреса

Кодировка Base58Check — эта кодировка будет встречаться в реализации ключей постоянно, поэтому важно понимать, как она работает и зачем она вообще нужна.

Ее суть в том, чтобы максимально кратко записать последовательность байт в удобочитаемом формате и при этом сделать вероятность возможных опечаток еще меньше. В случае, когда речь идёт

о деньгах, безопасность лишней не бывает. Один неправильный символ и деньги уйдут на чужой адрес.

Краткость записи проще всего реализовать, используя довольно распространенную кодировку *Base64*, т. е. используя систему счисления с основанием 64, где для записи используются цифры 0, 1, ..., 9, буквы *a–z* и *A–Z* — это дает 62 символа, оставшиеся два могут быть чем угодно, в зависимости от реализации.

Первое отличие *Base58Check* в том, что убраны символы *0, O, l, I* на случай, если кто-нибудь решит их перепутать. Получается 58 символов.

Второе отличие — это тот самый *check*. В конец строки снова добавляется *checksum* — первые 4 байта, полученных в результате функции *SHA256*(*SHA256*(*str*)). В начало нужно добавить столько единиц, сколько ведущих нулей было до кодировки в *base58* (рисунок 26).

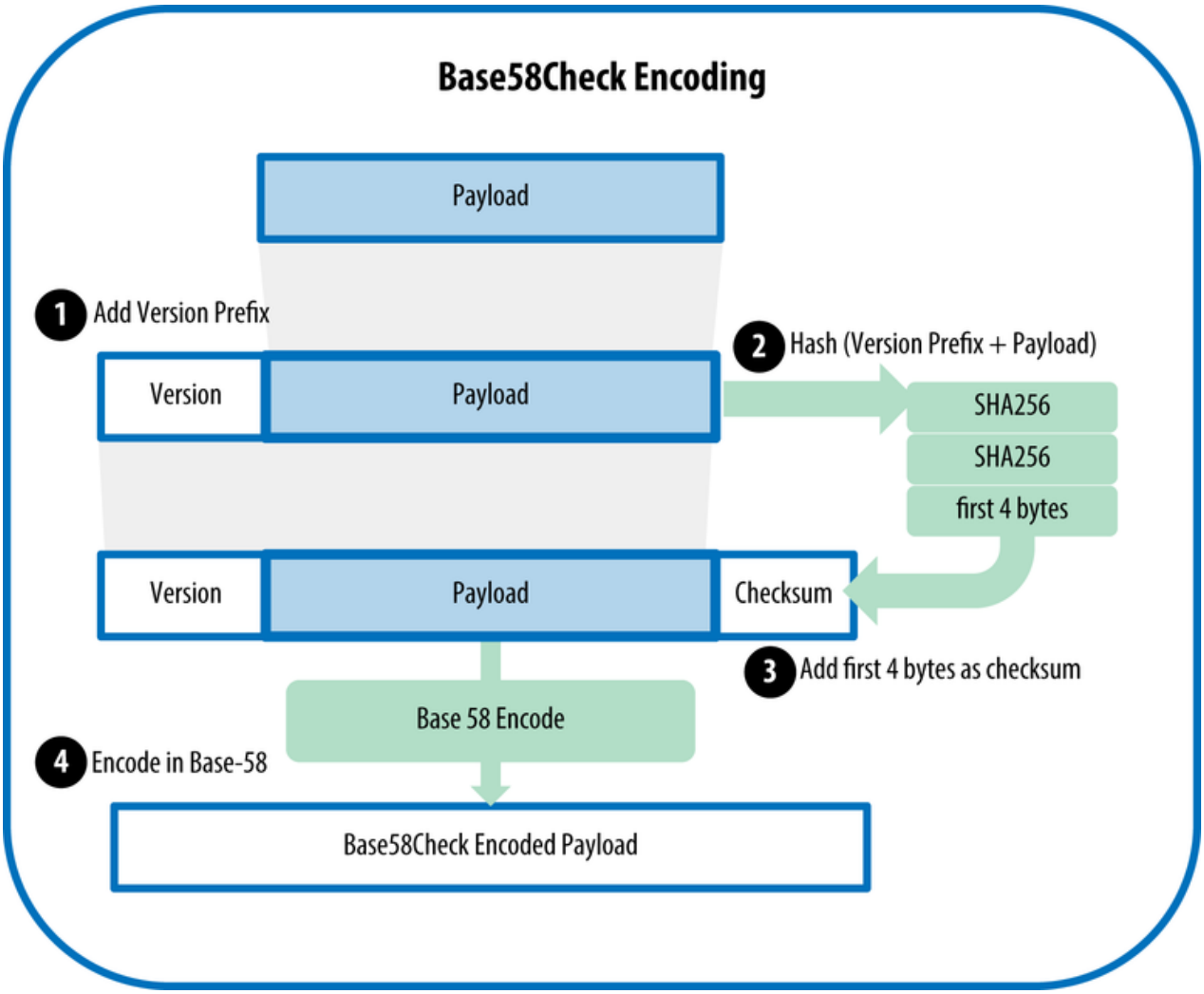

Рисунок 26 – Алгоритм кодировки *Base58Check*

Форматы приватного ключа

Самый очевидный способ хранить приватный ключ — это записать 256 бит в виде набора нулей и единиц. Но любой технически грамотный человек понимает, что будет гораздо проще представить ту же самую последовательность в виде 32 байт, где каждому байту соответствует два символа в шестнадцатеричной записи. В этой записи используются цифры 0, 1, ..., 9 и буквы A, B, C, D, E, F. Пример такого формата: *E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62*.

В этом примере байты разделены пробелом для большей наглядности.

Другой, более прогрессивный формат — *WIF* (*Wallet Import Format*). Строится он довольно просто:

1. Берем приватный ключ, например, *0C28FCA386C7A227600B 2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D*.

2. Записываем его в *Base58Check* с префиксом 0×80.

3. Конец.

Форматы публичного ключа

Публичный ключ — это точка на прямой *SECP256k1*. Самый распространенный вариант его записи — *uncompressed* формат, по 32 байта для *X* и *Y* координат. Чтобы не возникало путаницы, используется префикс 0 × 04, итого 65 байт.

Однако, это не самый оптимальный способ хранить публичный ключ.

Второй формат называется *compressed*. Суть его в следующем: публичный ключ — это точка на кривой, то есть пара чисел, удовлетворяющая уравнению (2). Значит можно записать только *X* координату, и если нам понадобится Y координата, то нужно просто решить уравнение. Тем самым размер публичного ключа уменьшается почти на 50 %.

Адреса

Как уже было сказано, адрес получается из публичного ключа однозначным образом. Более того, провести обратную операцию невозможно, так как используются криптографически стойкие хэш-функции — *RIPEMD160* и *SHA256*. Вот алгоритм перевода публичного ключа в адрес:

1. Возьмем приватный ключ, например, *45b0c38fa54766354cf340 9d38b873255dfa9ed3407a542ba48eb9cab9dfca67*.

2. Получим из него публичный ключ в *uncompressed* формате, в данном случае это *04162ebcd38c90b56fbdb4b0390695afb471c944a6003cb334bbf030a89c42b584f089012beb4842483692bdff9fcab8676fed42c47bffb081001209079bbcb8db*.

3. Считаем функцию *RIPEMD160* (*SHA256* (*public_key*)), получается *5879DB1D96FC29B2A6BDC593E67EDD2C5876F64C*.

4. Переводим результат в *Base58Check* с префиксом 0×00 — *17JdJpDyu3tB5GD3jwZP784W5KbRdfb84X*. Это и есть адрес.

Подпись и подтверждение

Для подписи создаются три точки (точка сообщения, случайная точка и случайная точка публичного ключа):

1. Точка сообщения (*Message Point*): Сообщение переводится в числовую последовательность (путем использования хэш-функции), и это число перемножается на G (*generator point*): (Точка сообщения) = Хэш из сообщения * G.

2. Случайная точка (*Random Point, RP*): Выбирается случайная точка: (Случайная точка) = Случайное число * G.

3. Случайная точка публичного ключа (*Random-Public Key Point, PKRP*): Перемножается *X*-координата случайной точки на публичный ключ, (Следует помнить, что, *X*-координата случайной точки является переменной): (Случайная точка публичного ключа) = *X*-координата случайной точки * (публичный ключ).

Подписывающий пользователь создает специальный путь к случайной точке с помощью точки сообщения и случайной точки публичного ключа. Ему необходимо вычислить коэффициент подписи таким образом, чтобы выполнялось условие: (Коэфф. подписи ∗ Точка сообщения) + (Коэфф. подписи ∗ Случайная точка публичного ключа) = Случайная точка.

Затем подписавший пользователь передает случайную точку и коэффициент подписи верификатору, который проверяет, воссоздает ли коэффициент подписи специальный путь к случайной точке с помощью «точки сообщения» и «случайной точки публичного ключа».

Этот способ довольно безопасен, так как:

1. Создание коэффициента подписи, который проверяется с помощью открытого ключа, невозможно без генератора открытого ключа.

2. Коэффициент подписи также используется вместе с хэшем сообщения, поэтому, если сообщение будет кем-либо изменяется, коэффициент подписи больше не будет действителен при воссоздании

пути к данной случайной точке. Как указано выше, о создании нового коэффициента подписи для работы с измененным сообщением не может быть и речи.

Алгоритмы эллиптических кривых работают в циклической подгруппе эллиптической кривой над конечным полем. Поэтому алгоритмам требуются следующие параметры:

1. Простое число *p*, задающее размер конечного поля.
2. Коэффициенты *a* и *b* уравнения эллиптической кривой.
3. Базовая точка *G*, генерирующая подгруппу.
4. Порядок *n* подгруппы.
5. Кофактор *h* подгруппы.

В результате параметрами области определения для алгоритмов является шестёрка (*p, a, b, G, n, h*).

Иногда приходится использовать дополнительный параметр области определения: порождающее значение (*seed*) *S*. Это случайное число, используемое для генерирования коэффициентов *a* и *b* или базовой точки *G*, или того и другого. Эти параметры генерируются вычислением хеша *S*. Хеши, как известно, «просто» вычислить, но «сложно» реверсировать.

Простая схема генерирования случайной кривой из порождающего значения: хеш случайного числа используется для вычисления различных параметров кривой (рисунок 27).

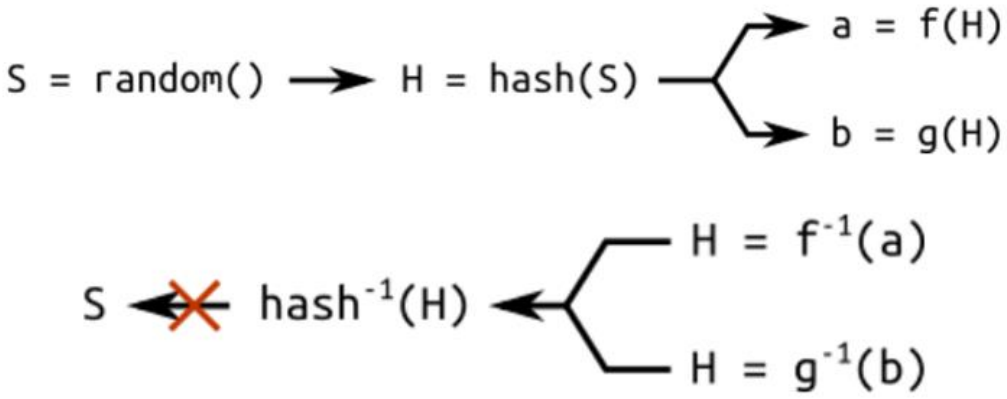

Рисунок 27 – Алгоритм генерирования случайной кривой из порождающего значения

Если бы мы хотели сжульничать и воссоздать хеш из параметров области определения, то нам пришлось бы решать «сложную» задачу: инверсирование хеша.

Таким образом, закрытый ключ — это случайное целое *d*, выбранное из *{1, ..., n - 1}*, где *n* — порядок подгруппы.

Открытый ключ — это точка $H = d*G$, где G — базовая точка подгруппы.

Если мы знаем d и G (вместе с другими параметрами области определения), то найти H «просто». Но если мы знаем H и G, то поиск закрытого ключа d является «сложной» задачей, потому что требует решения задачи дискретного логарифмирования.

Опишем два основанных на этом принципе алгоритма с открытым ключом: *ECDH* (*Elliptic curve Diffie-Hellman*, протокол Диффи-Хеллмана на эллиптических кривых), используемый для шифрования, и *ECDSA* (*Elliptic Curve Digital Signature Algorithm*), используемый для цифровых подписей.

Шифрование с помощью ECDH

ECDH — это разновидность алгоритма Диффи-Хеллмана для эллиптических кривых[1].

На самом деле это скорее протокол согласования ключей, а не алгоритм шифрования[2].

В сущности, это означает, что *ECDH* задаёт (в определённой степени) порядок генерирования ключей и обмена ими. Способ шифрования данных с помощью таких ключей мы можем выбирать сами.

Он решает следующую проблему: две стороны (обычно Алиса и Боб) хотят безопасно обмениваться информацией, чтобы третья сторона (посредник, *Man In the Middle*) мог перехватывать её, но не мог расшифровать. Например, это один из принципов *TLS*.

Вот как это работает[3]:

Сначала Алиса и Боб генерируют собственные закрытые и открытые ключи. У Алисы есть закрытый ключ d_A и открытый ключ $H_A = d_A*G$, у Боба есть ключи d_B и $H_B = d_B*G$. Заметьте, что и Алиса, и Боб используют одинаковые параметры области определения: одну базовую точку G на одной эллиптической кривой в одинаковом конечном поле.

Алиса и Боб обмениваются открытыми ключами H_A и H_B по незащищённому каналу. Посредник (*Man In the Middle*) перехватывает H_A и H_B, но не может определить ни d_A, ни d_B, не решив задачу дискретного логарифмирования.

---

[1] URL: https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0/ (дата обращения: 17.08.2021).

[2] URL: https://en.wikipedia.org/wiki/Key-agreement_protocol / (дата обращения: 10.08.2021).

[3] URL: https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0_%D0%B8_%D0%91%D0%BE%D0%B1/ (дата обращения: 11.08.2021).

Алиса вычисляет $S = d_A H_B$ (с помощью собственного закрытого ключа и открытого ключа Боба), а Боб вычисляет $S = d_B H_A$ (с помощью собственного закрытого ключа и открытого ключа Алисы). Учтите, что S одинаков и для Алисы, и для Боба. На самом деле:

$$S = d_A H_B = d_A (d_B G) = d_B (d_A G) = d_B H_A. \quad (3)$$

Однако посреднику известны только H_A и H_B (вместе с другими параметрами области определения) и он не сможет найти общий секретный ключ S. Это известно, как задача Диффи-Хеллмана, которую можно сформулировать следующим образом:

Каким будет результат abP для трёх точек P, aP и bP?

Или, аналогично:

Каким будет результат k^{xy} для трёх целых k, k^x и k^y?

(Последняя формулировка используется в исходном алгоритме Диффи-Хеллмана, основанном на модулярной арифметике).

Протокол Диффи-Хеллмана: Алиса и Боб могут «просто» вычислить общий секретный ключ, посреднику же придётся решать «сложную» задачу (рисунок 28).

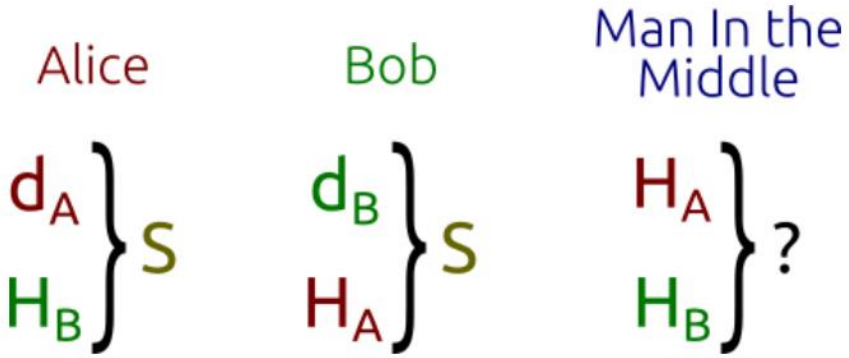

Рисунок 28 – Принцип, лежащий
в основе задачи Диффи-Хеллмана

Задача Диффи-Хеллмана для эллиптических кривых считается «сложной». Считается, что она так же «сложна», как задача дискретного логарифмирования, но математических доказательств этому нет. Можно только с уверенностью сказать, что она не может быть «сложнее», потому что решение задачи логарифмирования — это способ решения задачи Диффи-Хеллмана.

Получив общий секретный ключ, Алиса и Боб могут обмениваться данными с симметричным шифрованием.

Например, они могут использовать координату *X* ключа *S*, как ключ для шифрования сообщений такими безопасными шифрами, как *AES* или *3DES*[1].

Примерно это и делает *TLS*, разница в том, что *TLS* соединяет координату *X* с другими числами, относящимися к подключению, а затем вычисляет хеш получившейся строки байтов.

Иногда применяется эфемерное *ECDH*, а именно *ECDHE* («E» в *ECHDE* обозначает *Ephemeral* (эфемерное) и связано с тем, что передаваемые ключи временны, а не статичны). *ECDHE* используется, например, в *TLS*, где клиент и сервер генерируют свою пару закрытого-открытого ключа на лету, при установке соединения. Затем ключи подписываются сертификатом *TLS* (для авторизации) и передаются между сторонами.

Сценарий следующий: Алиса хочет подписать сообщение своим закрытым ключом (d_A), а Боб хочет проверить подпись с помощью открытого ключа Алисы (H_A). Никто, кроме Алисы не должен иметь возможности создать действительные подписи. Каждый должен иметь возможность проверить подписи.

Шифрование с помощью *ECDSA* (рисунок 29)

Алиса и Боб снова используют одинаковые параметры области определения. Мы рассмотрим алгоритм *ECDSA*, разновидность *Digital Signature Algorithm*, применённого к эллиптическим кривым[2].

ECDSA работает с хешем сообщения, а не с самим сообщением. Выбор хеш-функции остаётся за нами, но, очевидно, нужно выбирать криптографическую хеш-функцию[3].

Хеш сообщения необходимо урезать, чтобы битовая длина хеша была такой же, что и битовая длина n (порядок подгруппы). Урезанный хеш — это целое число, и оно будет обозначаться как *z*.

Алгоритм, выполняемый Алисой для подписания сообщения, работает следующим образом:

1. Берём случайное целое *k*, выбранное из {1, …, n - 1}, где *n* — это по-прежнему порядок группы.

[1] URL: https://ru.wikipedia.org/wiki/Triple_DES/ (дата обращения: 16.08.2021).

[2] URL: https://en.wikipedia.org/wiki/Digital_Signature_Algorithm / (дата обращения: 19.08.2021).

[3] URL: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%85%D0%B5%D1%88%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F/ (дата обращения: 18.08.2021).

2. Вычисляем точку $P = k*G$, где G — базовая точка подгруппы.

3. Вычисляем число $r = x_p \ mod \ n$, где x_p — это координата x_P).

Если $r = 0$, то выбираем другое k и пробуем снова.

4. Вычисляем $s = k^{-1}(z + rd_A) \ mod \ n$, где d_A — закрытый ключ Алисы, а k-1 — мультипликативная инверсия k по модулю n).

Если $s = 0$, то выбираем другое k и пробуем снова.

Пара (r, s) является подписью.

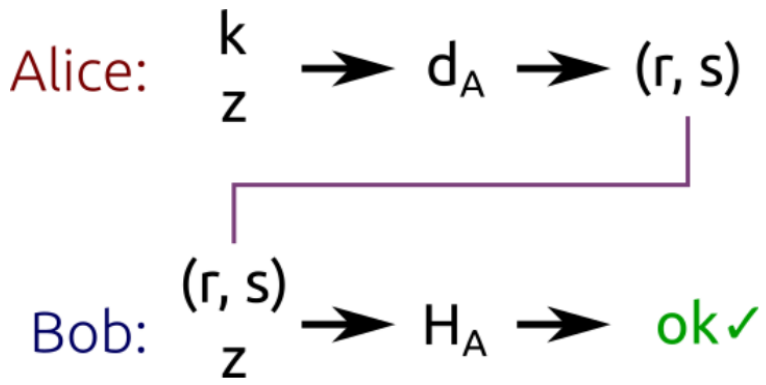

Рисунок 29 – Шифрование с помощью *ECDSA*

Алиса подписывает хеш z с помощью закрытого ключа d_A и случайного k. Боб проверяет правильность подписи сообщения с помощью открытого ключа Алисы H_A.

Проще говоря, этот алгоритм сначала генерирует секретный ключ (k). Благодаря умножению точек (которое, как мы знаем, является «простым» в одну сторону и «сложным» в обратную) секретный ключ прячется в r. Затем r привязывается к хешу сообщения уравнением $s = k^{-1}(z + rd_A) \ mod \ n$.

Необходимо учитывать, что для вычисления s вычислили обратную величину k по модулю n. Как было сказано выше, это гарантировано сработает только если n — простое число. Если подгруппа имеет порядок непростого числа, *ECDSA* использовать не удастся. Неслучайно все стандартизированные кривые имеют простой порядок, а имеющие непростой порядок неприменимы для *ECDSA*.

Проверка подписей

Для проверки подписи необходим открытый ключ Алисы H_A, (урезанный) хеш z и, очевидно, подпись (r, s).

1. Вычисляем целое $u_1 = s^{-1}z \ mod \ n$.

2. Вычисляем целое $u_2 = s^{-1}r \ mod \ n$.

3. Вычисляем точку $P = u_1G + u_2H_A$.

4. Подпись действительна, только если $r = x_P \ mod \ n$.

Корректность алгоритма

С первого взгляда логика алгоритма может быть неочевидной, однако если объединить все ранее записанные нами уравнения, всё становится понятнее.

Начнём с $P = u_1G + u_2H_A$. Из определения открытого ключа знаем, что $H_A = d_AG$, где d_A — закрытый ключ. Можно записать:

$$P = u_1G + u_2H_A$$
$$P = u_1G + u_2\, d_AG$$
$$P = (u_1 + u_2\, d_A)\, G$$

С учётом определений u_1 и u_2 можно записать:

$$P = (u_1 + u_2\, d_A)\, G$$
$$P = (s^{-1}z + s^{-1}rd_A)\, G$$
$$P = s^{-1}\, (z + rd_A)\, G$$

Здесь опустили «*mod n*», как для краткости, так и потому, что циклическая подгруппа, сгенерированная точкой G, имеет порядок n, то есть часть «*mod n*» избыточна.

Ранее мы определили $s = k^{-1}\, (z + rd_A)\ mod\ n$. Умножив обе части уравнения на k и поделив на s, получаем: $k = s^{-1}\, (z + rd_A)\ mod\ n$. Подставляя этот результат в наше уравнение для P, получаем:

$$P = s^{-1}\, (z + rd_A)\, G$$
$$P = kG$$

Это то же самое уравнение P, которое было у нас на шаге 2 алгоритма генерирования подписи! При генерировании подписей и при их проверке вычисляем одну и ту же точку P, просто разными наборами уравнений. Именно поэтому алгоритм работает.

Важность *k*

При генерировании подписей *ECDSA* важно хранить секретный k по-настоящему в тайне. Если бы мы использовали одну k для всех подписей или генератор случайных чисел оказался бы в какой-нибудь степени предсказуемым, то атакующий смог бы определить закрытый ключ.

Глава 3
ТЕХНОЛОГИЯ БЛОКЧЕЙНА

3.1. Общая характеристика технологий блокчейна

Блокчейн — это особая технология, на которой основаны платформы для проведения операций между равноправными участниками, действующими без посредников, и в которой применяется децентрализованное хранение информации для отражения всех данных об операциях. Это эффективная платформа для совершения транзакций в рамках сети, объединяющей равноправных участников[1].

Впервые технология «блокчейн» была использована в финансовом секторе, где она послужила основой для создания критповалюты «биткойн». В последнее время появляется все больше приложений, расширяющих ключевую функцию этой технологии — децентрализованное хранение данных о транзакциях — за счет интеграции механизмов, позволяющих децентрализовано проводить реальные сделки. Данные механизмы, получившие название «умных контрактов», работают на основе правил, установленных в индивидуальном порядке (например, конкретные требования в отношении количества, качества, цены) и позволяющих в автоматическом режиме подбирать потенциальных потребителей для поставщиков и, наоборот, на основе распределенных реестров.

Благодаря технологии блокчейна меняется порядок проведения операций: соответствующая транзакционная модель постепенно переходит от использования централизованной структуры (банки, биржи, торговые платформы, энергетические компании) к применению децентрализованной системы (конечные пользователи, потребители электроэнергии). В таких системах независимые посредники, в услугах которых сегодня нуждается большинство отраслей, больше не требуются (по крайней мере в соответствии с теорией блокчейна), поскольку операции могут быть инициированы и проведены напрямую «между равноправными участниками сети». Это позволяет сократить затраты и ускорить процессы. В результате вся система становится более гибкой, так как многие рабочие задачи, ранее выполнявшиеся вручную, теперь решаются в автоматическом режиме

[1] Дрешер Д. Основы блокчейна. Москва: ДМК Пресс, 2018. 312 с.

с использованием «умных контрактов». Таким образом, блокчейн обеспечивает снижение затрат, ускорение процессов и повышение уровня гибкости.

Обозначим факторы, препятствующие сегодня внедрению приложений на базе блокчейна[1].

Теоретически блокчейн-системы не нуждаются ни в посредниках, ни в централизованном управлении. Противоречия разрешаются на основе принципа «пчелиного роя», то есть исходя из коллективного мнения всех участвующих сторон. Однако сегодня реализовать такие модели на практике все еще трудно. Кроме того, имеется ряд требований нормативно-правового характера, которые должны быть соблюдены при реализации блокчейн-проектов. В любом случае сама технология, позволяющая выстраивать цепочки блоков транзакций (блокчейны), еще не достигла необходимого уровня зрелости и продолжает развиваться.

В секторе финансовых услуг технология блокчейна достигла определенного уровня зрелости, но в энергетике и других отраслях это направление пока находится на этапе формирования концепций.

Вокруг концепции биткойна сформировалась целая «экосистема» компаний, которые строят свою работу, используя виртуальную валюту и лежащую в ее основе технологию. Сегодня многие банки и стартапы разрабатывают и испытывают другие направления, в рамках которых эта технология может быть использована для финансовых целей.

В других отраслях технология блокчейна только начинает делать первые шаги. В настоящее время некоторые стартапы выходят на рынок с проектами на основе блокчейн-решений. В электроэнергетике испытания технологии проводятся в рамках очень небольшого количества пилотных проектов, часть из которых финансируются крупными электроэнергетическими компаниями. Например, в апреле 2016 года в Нью-Йорке впервые были осуществлены операции купли-продажи электроэнергии, произведенной в децентрализованном порядке, между соседями с помощью блокчейн-системы. Цель — создать полностью децентрализованную систему энергоснабжения, в рамках которой контракты на поставку электроэнергии заключаются напрямую

[1] См.: Цихилов А. Блокчейн. Принципы и основы. Москва: Изд-во «Интеллектуальная литература», 2019. – 286 с.

между производителями и потребителями электроэнергии (без участия сторонних посредников) и исполняются в автоматическом режиме.

Блокчейн обеспечивает следующие возможности для потребителей, являющихся одновременно и производителями.

Использование технологии блокчейна повышает роль отдельных потребителей и производителей на рынке. Технология позволяет потребителям электроэнергии, являющимся одновременно и ее производителями (т. е. домохозяйствам, которые не только потребляют, но и производят электроэнергию), продавать и покупать электроэнергию напрямую и практически в автономном режиме. В настоящее время в электроэнергетике действует четко определенная нормативно-правовая база для потребителей и потребителей, являющихся одновременно и производителями, которая обеспечивает правовую защиту на многих уровнях, особенно защиту прав потребителей. Однако в средне- и долгосрочной перспективе действующую нормативно-правовую базу, по всей вероятности, придется скорректировать с учетом потребностей децентрализованных транзакционных моделей.

Таким образом, блокчейн — это технология, которая позволяет проводить транзакции между равноправными участниками единой сети (*P2P*-сети — «пиринговая» сеть). Транзакции данного вида предполагают, что каждый участник сети может осуществлять транзакцию напрямую с любым другим участником сети без привлечения стороннего посредника.

Новшество технологии «блокчейн» заключается в том, что информация о транзакциях более не хранится в централизованной базе данных, а передается на компьютеры всех участников сети, которые хранят данные локально. Первым приложением на базе технологии блокчейна стало приложение «Биткойн» для так называемой криптовалюты (биткойн). В последние годы биткойн послужил основой для создания других блокчейн-приложений, большинство из которых в настоящее время разрабатываются в финансовой сфере. Совсем недавно был создан ряд компаний и запущены отдельные проекты, цель которых — применить принципы блокчейна в других отраслях, в том числе в электроэнергетике. В целом считается, что блокчейн-приложения представляют собой весьма перспективную технологию, однако пока они все еще находятся на ранних стадиях развития (рисунок 30).

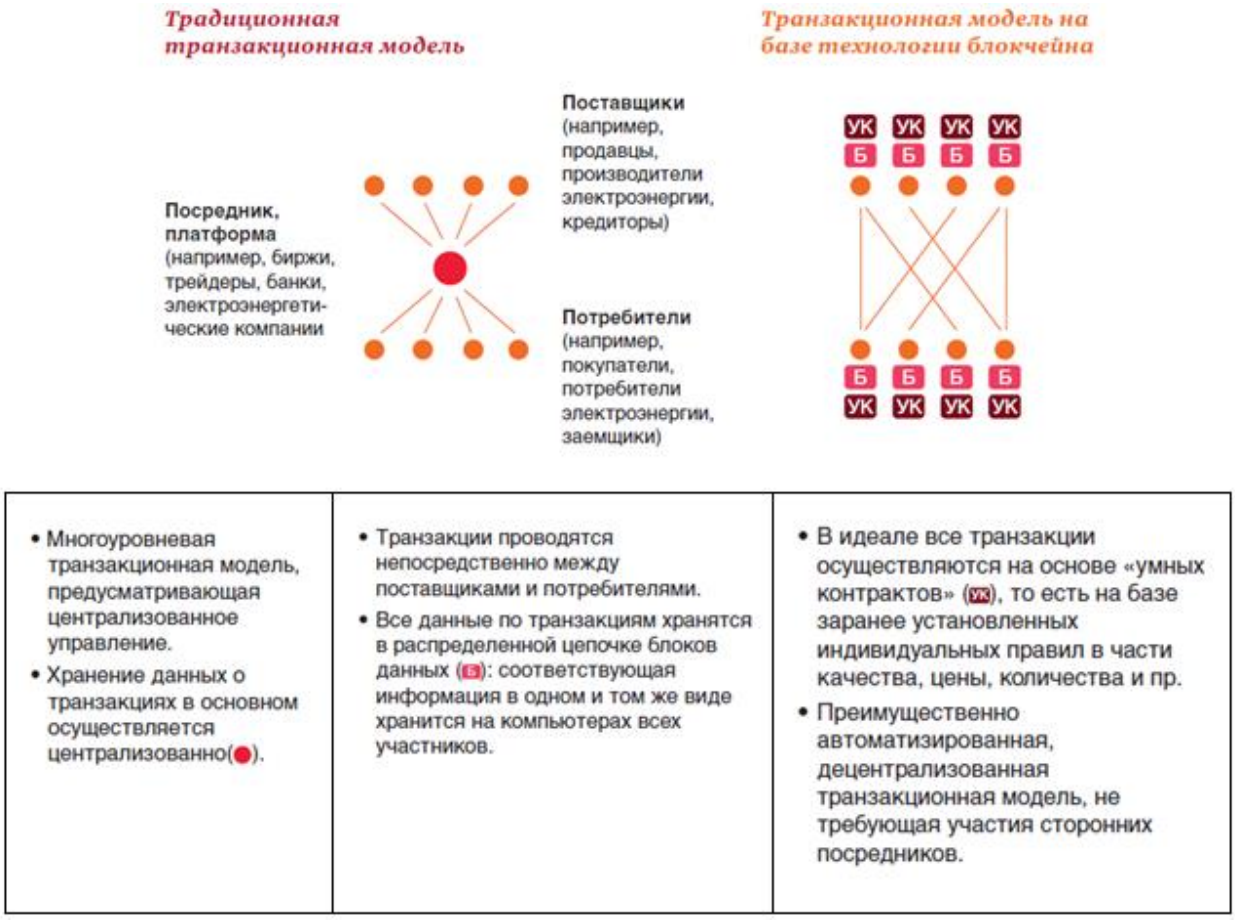

Рисунок 30 – Как благодаря технологии блокчейна меняется порядок проведения транзакций

3.2. Алгоритм работы блокчейна

Если поставщик и покупатель договорились осуществить транзакцию, они определяют переменные величины данной транзакции, указав получателя, отправителя и сумму транзакции, а также другую информацию. Вся информация, относящаяся к конкретной транзакции, затем объединяется с подробной информацией по другим транзакциям, проведенным в течение того же периода времени, для создания нового блока данных. Это сопоставимо с отправкой электронных писем, которые тоже разбиваются на отдельные блоки данных. Блокчейн отличается тем, что данный процесс относится к одной стандартизированной транзакции.

Информация по каждой транзакции зашифровывается и передается на большое число персональных компьютеров (участников сети *P2P*), на каждом из которых осуществляется локальное хранение данных. Участники сети автоматически подтверждают (верифицируют) транзакции, информация о которых хранится на персональных компьютерах (рисунок 31).

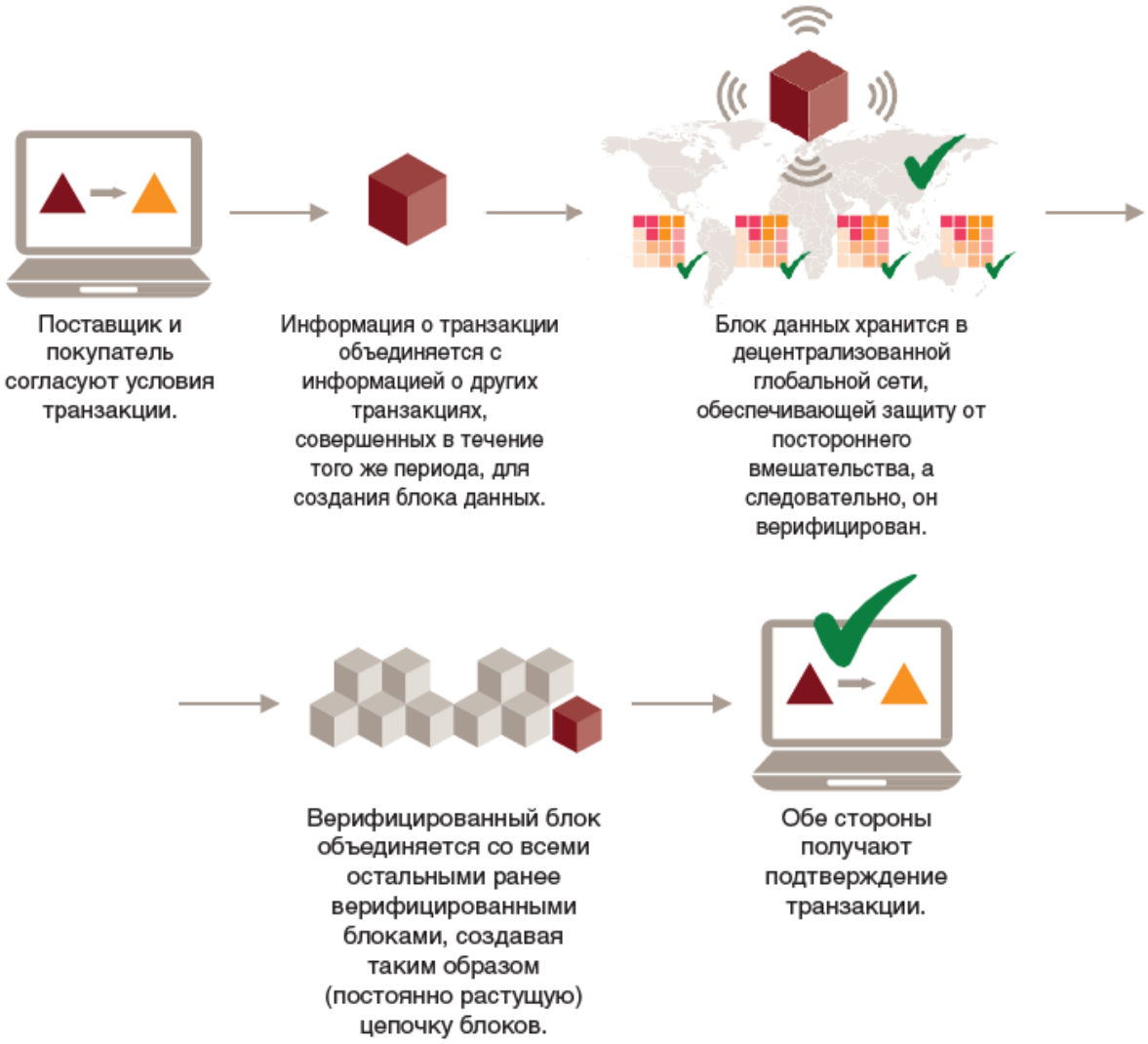

Рисунок 31 – Алгоритм работы блокчейна

Верификация данных, хранящихся в блоках, проводится с использованием алгоритмов, которые присваивают каждому блоку уникальный хеш-код. Каждый такой хеш-код представляет собой последовательность цифр и букв, которая создается на основе информации, хранящейся в соответствующем блоке данных. Если какая-либо информация, относящаяся к той или иной транзакции, в дальнейшем будет изменена в результате несанкционированного вмешательства или из-за ошибок передачи данных (например, точная сумма операции), то алгоритм, примененный к измененному блоку, уже не даст правильного хеш-кода, а, следовательно, сообщит об ошибке.

Все комбинации цифр и букв постоянно проверяются на предмет их корректности, и из отдельных блоков данных формируется цепочка блоков данных, то есть блокчейн. Благодаря тому, что эти комбинации цифр и букв последовательно связаны друг с другом,

целостность информации, хранящейся в цепочке блоков данных, невозможно нарушить (по крайней мере это потребует весьма значительных усилий). Непрерывный процесс верификации (называемый «майнингом») выполняется участниками блокчейна, которые получают вознаграждение за эту услугу в соответствии с тем, какой объем собственных вычислительных мощностей они израсходовали.

Процесс верификации гарантирует, что все участники могут пополнить цепочку блоков, но при этом последующее внесение изменений в записи невозможно (рисунок 32). Это позволяет осуществлять операции в сети *P2P* напрямую между лицами или организациями, которым ранее обычно требовались услуги посредника для того, чтобы на законных основаниях отразить свои операции. Например, если в настоящее время для проведения финансовой операции между двумя сторонами требуется участие банка в качестве посредника, то в случае использования технологии блокчейна такую же операцию смогут осуществить напрямую и сами ее документально оформить непосредственно две участвующие в операции стороны.

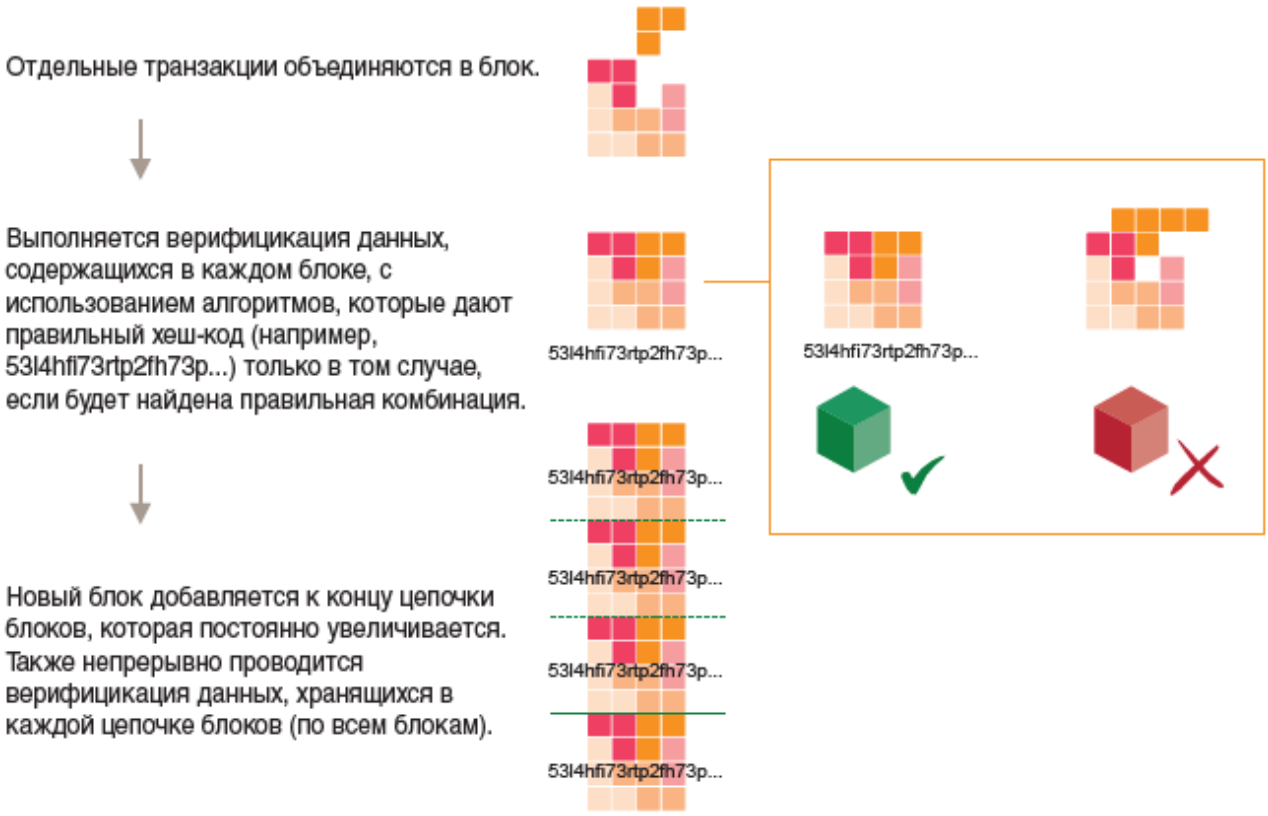

Рисунок 32 – Процесс верификации

История развития технологии «блокчейн»[1]

Существующие сегодня блокчейн-приложения можно разделить на три большие категории в зависимости от уровня разработки, а именно: блокчейн-приложения версий 1.0, 2.0 и 3.0.

Категория «Блокчейн 1.0» охватывает такие виртуальные валюты (или криптовалюты), как биткойн, которые могут быть использованы в качестве альтернативы реальным валютам (например, евро или доллару США). До настоящего момента биткойн по-прежнему остается блокчейн-приложением, которое наиболее хорошо знакомо широкой публике и популярность которого продолжает расти. Однако, несмотря на то, что у этой валюты появляется все большее число пользователей и объемы торговли в ней растут, доля операций с биткойнами на международных биржевых рынках в абсолютном выражении все еще остается минимальной. В настоящее время ничто не указывает на то, что биткойн сможет когда-либо хотя бы приблизиться к уровню других мировых валют.

Цель следующего этапа разработки — внедрить модели «умных контрактов», которые совместно называются «Блокчейн 2.0». «Умный контракт» представляет собой цифровой протокол, автоматически исполняющий заранее предопределенные процессы транзакции и не требующий участия третьей стороны (например, банка). Давайте вернемся к примеру, приведенному в начале этой главы. Например, станет возможным создание полностью автоматизированного «умного контракта» между производителем электроэнергии и потребителем, который будет регулировать в автономном и защищенном режиме, как поставки, так и платежи. В случае если покупатель, например, не сможет осуществить платеж, «умный контракт» автоматически обеспечит приостановку электроснабжения до момента получения платежа, при условии, что стороны заранее договорились о включении такого механизма в свой контракт. Такое развитие ситуации представляет собой угрозу для традиционных бизнес-моделей банков, которые рискуют быть вытесненными из рыночного сегмента платежных систем.

Компании и разработчики могут принять решение о том, будут ли они создавать свои приложения на основе открытых или закрытых цепочек блоков. В случае открытой цепочки блоков сохраняется анонимность всех участников системы. Примерами таких цепочек блоков

[1] См.: Дуглас С. Криптовалюта и блокчейн. Основы электронных валют. Москва: ЛитРес, 2021. 188 с.

являются платформы «Биткойн» и «Эфириум». В закрытых блокчейн-системах все участники известны и идентифицированы до того, как будет предоставлен доступ. Некоторые преимущества закрытых цепочек блоков заключаются в том, что они позволяют использовать более простые структуры корпоративного управления и стоимость обслуживания таких цепочек блоков ниже, чем открытых. Следовательно, банки и поставщики платежных услуг должны будут использовать закрытые цепочки блоков в рамках своих текущих бизнес-моделей, в частности потому, что это позволит им в некоторой степени сохранить контроль, а также потенциал генерирования выручки.

Технология блокчейна следующего поколения, которая называется «Блокчейн 3.0», пока еще существует только на уровне концепции. Блокчейн 3.0 — это этап развития технологии, на котором осуществляется дальнейшая проработка концепции «умного контракта» с целью создания децентрализованных, автономных организационных единиц, которые руководствуются собственными законами и действуют практически автономно.

Каждая цепочка блоков данных — это, по сути, так называемое приложение *DApp* («децентрализованное приложение»), которое работает на основе протокола *P2P* и имеет особую характеристику: обеспечивает функционал распределенного хранения для транзакционных данных.

Приложения *DApp* — это приложения с открытым исходным кодом, которые представляют собой контракт, заключенный между сетью и ее пользователями, и которые основаны на технологии так называемого распределенного реестра (*ledger*), например, блокчейны «Биткойн» или «Эфириум». Специфика этого приложения заключается в том, что ни одна организация не контролирует эти контракты и не имеет законного права требования в отношении них, а все решения (например, об адаптации протокола) принимаются в результате достижения пользователями консенсуса на основе компьютерного кода.

Приложение считается действительно децентрализованным, если и его протокол, и его данные хранятся в децентрализованной цепочке блоков (чтобы избежать наличия центральной точки отказа), находящейся в открытом доступе, а их правильность подтверждается путем использования механизма децентрализованной верификации (например, «доказательства выполнения работы»).

Децентрализованные должным образом приложения обеспечивают возможность хранения надежной учетной информации по всем транзакциям и деловым сделкам даже в том случае, если ключевые

веб-сайты и интерфейсы находятся в офлайн-режиме. Кроме того, в дальнейшем никто не сможет изменить или стереть записи в распределенном реестре.

Приложения *DApp* могут быть классифицированы следующим образом:

Тип 1: децентрализованные приложения, имеющие собственные цепочки блоков, например, *Bitcoin, Altcoin, Litecoin*.

Тип 2: децентрализованные приложения, использующие цепочку блоков *DApp* типа 1, например:

– протокол *Omni* (слой программного обеспечения, выстроенный поверх цепочки блоков «Биткойн»);

– приложения *DApps* типа 2 представляют собой протоколы и используют собственные токены.

Тип 3: децентрализованные приложения, использующие цепочку блоков *DApp* типа 2, например, сеть *SAFE*, использующая протокол *Omni* для выпуска токенов *safecoin2*.

Концепции доказательства выполнения работы и подтверждения доли

Цель процесса верификации — добиться консенсуса в отношении информации, содержащейся в распределенном реестре. Верификация на основе консенсуса представляет собой децентрализованный (то есть встроенный в саму цепочку блоков) и автоматизированный процесс.

Для достижения консенсуса наиболее широко используются следующие два механизма.

1. Доказательство выполнения работы.

Концепция доказательства выполнения работы — это механизм на основе консенсуса, который наиболее часто используется вместе с технологией блокчейна и который полагается на так называемых майнеров. Прежде чем информация по каждому блоку будет сохранена, проводится его верификация с помощью майнинга. Верификация данных, содержащихся в каждом блоке, осуществляется с использованием алгоритмов, которые присваивают каждому блоку уникальный хеш-код на основе хранящейся в нем информации.

Хеш-алгоритмы используются для конвертации данных произвольной длины в данные фиксированной длины, составляя таким образом хеш-код. Хеш-сумма представляет собой контрольную сумму, используемую для шифрования сообщения переменного размера с применением функции хеширования. Никакие два зашифрованных сообщения не могут быть основаны на одной и той же хеш-сумме,

равно как и хеш-сумма не может содержать подсказку в отношении представленной в сообщении информации.

Хеш-коды могут представлять собой обычные или криптографические хеш-комбинации. Сложность данной задачи заключается в обнаружении конкретного хеш-кода, соответствующего информации, которая содержится в блоке. Уровень сложности (трудности) гибко корректируется с учетом вычислительной мощности, имеющейся в сети майнеров, чтобы обеспечить возможность хеширования новых блоков с установленной периодичностью (Биткойн: 10 минут; Эфириум: 10 секунд). Даже если какая-то информация по какой-либо операции впоследствии меняется, например, если изменяется сумма операции в результате несанкционированного вмешательства или из-за ошибок передачи данных, применяемый к блоку алгоритм уже не будет генерировать правильный хеш-код. Хеш-коды, рассчитанные для того же блока, который был сохранен несколько раз в децентрализованной сети (как описано выше), сопоставляются таким образом, чтобы выявить измененные блоки и объявить их недействительными. Верифицированная правильная версия блока выявляется большинством участвующих компьютеров и добавляется к другим, ранее верифицированным блокам, увеличивая, таким образом, цепочку блоков. Как только блок, содержащий первоначальную операцию, добавляется к цепочке блоков и данное добавочное звено сохраняется достаточным количеством участников сети, операция подтверждается, о чем информируются обе стороны, участвующие в операции (рисунок 33).

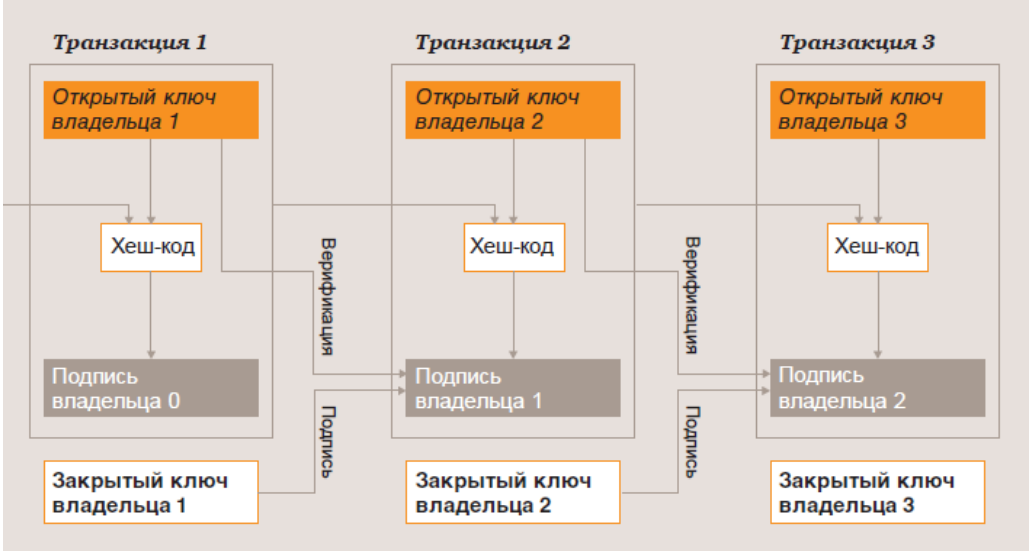

Рисунок 33 – Транзакции между участниками сети *P2P*

Процесс майнинга может быть также использован для принятия решений о внесении изменений в приложение *DApp*. Решения, принятые в соответствии с принципом доказательства выполнения работы, принимаются на основе объема работ, который выполнили отдельные заинтересованные лица для верификации блока данных[1].

2. Подтверждение доли.

Подход, основанный на подтверждении доли, упрощает процесс майнинга, в рамках которого необходимо верифицировать большое количество токенов. Если, согласно принципу доказательства выполнения работы, большая группа пользователей распределенной сети непрерывно проводит верификацию хеш-кодов по транзакциям в рамках процесса майнинга, с тем чтобы актуализировать текущий статус блокчейн-активов, то в случае концепции подтверждения доли пользователи должны периодически доказывать право владения своей собственной долей («долей участия») в соответствующей валюте. Если используется метод подтверждения доли, работа, необходимая для выполнения верификации, распределяется между отдельными участниками в соответствии с их долей, выраженной в процентах. Например, если пользователь владеет долей в 10 % от общей стоимости блокчейн-активов, находящихся в обращении, то этот пользователь должен будет выполнять 10 % всех необходимых майнинговых операций. Использование такого подхода позволяет снизить уровень сложности децентрализованного процесса верификации и, следовательно, может обеспечить большую экономию за счет снижения затрат на электроэнергию и операционных затрат.

Термин «токен» может обозначать несколько понятий:

– токен может использоваться для предоставления пользователям доступа к компьютерному приложению, которое может быть, как централизованным, так и децентрализованным;

– служить ключом к выполнению цифровых транзакций или представлять единицу валюты (например, биткойны).

Токены приложения *DApp* генерируются и распространяются с использованием стандартного алгоритма или набора критериев. Токены формируют основу для применения приложения, а кроме того, представляют собой вознаграждение за вклад пользователей. Тем не менее, токены не представляют какие-либо активы, равно как и не дают прав на дивиденды или обыкновенные акции. Хотя ценность

[1] См.: Максуров А. А. Блокчейн, криптовалюта, майнинг. Понятие и правовое регулирование: монография. Москва: Изд-во «Дашков и К°», 2022. 211 с.

токена приложения *DApp* с течением времени может увеличиваться или снижаться, было бы неправильно рассматривать токены как своего рода гарантию безопасности.

Какие же механизмы используются для распределения токенов?

Существует три общих механизма, которые могут использоваться в приложениях *DApp* (таких как «Биткойн» и «Эфириум») для распределения имеющихся у них токенов (например, биткойнов или эфиров): майнинг, привлечение средств и разработка.

Майнинг: токены распределяются в виде вознаграждения среди тех участников, которые наиболее оперативно осуществляют операции по верификации (при этом консенсус достигается методом доказательства выполнения работы). «Биткойн» — это один из примеров децентрализованного приложения *DApp*, генерирующего свои токены посредством майнинга.

Привлечение средств: токены распределяются между теми лицами, которые финансировали первоначальную разработку приложения *DApp*.

Разработка: токены генерируются с использованием заранее определенного механизма и имеются в наличии для целей будущих разработок приложения *DApp* (при этом консенсус достигается посредством подтверждения доли).

Транзакции между участниками сети *P2P* осуществляются следующим образом.

На рисунке 33 показано, как Владелец 1 передает токен Владельцу 2 посредством подписания в цифровом формате хеш-кода предыдущей транзакции и открытого ключа следующего получателя (цифровая подпись). Затем транзакция добавляется к блокчейну. Сторона, получающая информацию/платеж (Владелец 2), может верифицировать «цепочку владельцев» путем проверки достоверности подписей с использованием открытого ключа Владельца 1, хранящегося в цепочке блоков с открытым доступом. Однако они не могут проверить, был ли тот же токен уже использован предыдущим владельцем до момента совершения текущей транзакции («двойное использование»). Двойное использование может быть проверено либо централизованно (администратором), либо (в случае «Биткойна») в рамках процесса верификации, выполненного в децентрализованном порядке.

3.3. Использование блокчейн-приложений в качестве основы для криптовалют (биткойнов)

Платежная система «Биткойн» — это первое приложение, созданное на основе технологии блокчейна, а биткойны со временем стали самой ходовой криптовалютой. С 2009 года эта технология позволяет пользователям осуществлять переводы биткойнов друг другу без участия стороннего посредника, при этом само слово «биткойн» стало употребляться не только как название самой системы, но и как название денежной единицы.

Пользователям не требуется глубокое понимание системы для того, чтобы установить ее на своем устройстве и работать с ней. Даже неопытные пользователи могут относительно легко войти в систему. Более того, доступ к системе «Биткойн» ничем не ограничен. Любой пользователь может войти в систему и даже разработать новые приложения, используя в качестве основы цепочку блоков «Биткойн». При регистрации через веб-сайт «Биткойн» пользователи выбирают так называемый кошелек (который представляет собой их электронный бумажник) и адрес в системе «Биткойн». Биткойн-адреса аналогичны адресам электронной почты, с помощью которых пользователи могут посылать биткойны другим пользователям. Каждый раз, когда произведена транзакция, соответствующая информация передается по всей цепочке блоков «Биткойн» через связанную с ней сеть равноправных участников (*P2P*). Кошельки рассчитывают остатки по счетам на основании защищенной от постороннего вмешательства информации, которая хранится в цепочке блоков. Кошельки могут быть сконфигурированы таким образом, чтобы выполнялись только определенные транзакции, например, только в том случае, если отправитель распоряжается значительной суммой биткойнов. Это обеспечивает пользователям-получателям комплексную систему защиты от мошеннических действий или от неплатежей. Вместе с тем пользователи, особенно неопытные, также подвергаются некоторому риску при использовании системы «Биткойн», например, в случае, если они забудут свои реквизиты доступа, поскольку это означает, что активы, которые они хранили в этой системе, будут безвозвратно утеряны. Кроме того, в системе невозможно сторнировать ошибочно произведенные транзакции.

Платежи, произведенные в системе «Биткойн», могут быть четко и однозначно верифицированы, что означает невозможность возникновения в бухгалтерском учете ошибок, связанных с использованием этой системы. Вопреки распространенному мнению, такой

высокий уровень прозрачности также ведет к утрате анонимности. К каждому шагу процедуры любого перевода средств в системе «Биткойн» имеется открытый доступ через Интернет. Хотя все счета, а, следовательно, и пользователи, участвующие в транзакции, являются анонимными, но как только регистрационное имя пользователя (имя-псевдоним) становится известно, можно сразу найти всю историю транзакций пользователя в цепочке блоков и проследить транзакцию обратно вплоть до пользователя.

За семь лет работы системы никому не удалось изменить биткойн-транзакцию после того, как она была проведена, или организовать успешную атаку на сеть (либо хотя бы помешать ее работе). Тем не менее, в прошлом имели место инциденты, в частности случаи, когда биткойны были украдены посредством манипуляций с обменными операциями.

Если рассматривать не только виртуальную среду, где биткойны используются для оплаты покупок в интернет-магазинах и т. п., следует отметить, что растет число ресторанов, гостиниц и музыкальных магазинов, которые принимают биткойны в качестве платежного средства. Муниципалитет швейцарского города Цуг даже стал первым государственным административным органом, который начал принимать платежи в биткойнах. Однако обменять биткойны на «реальные» продукты по-прежнему трудно. Одна из имевшихся ранее проблем для пользователей, которая возникала в связи с существенными колебаниями обменного курса цифровой валюты по отношению к «реальным» валютам, в настоящее время уже в основном устранена благодаря приложениям, которые предлагают обмен биткойнов на евро в момент осуществления платежа.

Только будущее покажет, будет ли рядовой потребитель ценить (и если будет, то в какой мере) такие преимущества блокчейн-приложений (например, «Биткойна»), как повышенный уровень защиты от постороннего вмешательства и экономию (теоретическую) на затратах, считая их значимым и заметным шагом вперед по сравнению с традиционной платежной системой. Последняя уже сегодня обычно предлагает бесплатный перевод денег, обеспечивает высокие стандарты безопасности и значительно более высокую скорость обработки транзакций по переводу денежных средств (50 000 переводов в секунду в платежной системе *Visa* по сравнению с 7 переводами в секунду в случае системы «Биткойн»)[1].

[1] См.: Милушкин С. А. Майнеры. Москва: АСТ, 2020. 544 с.

3.4. Алгоритм процедуры майнинга криптовалюты (биткойнов)

Словом «майнинг» (от англ. *mining* — добыча полезных ископаемых) называют процесс подтверждения транзакций и их последующее добавление в распределенный публичный регистр (блокчейн); во время этого процесса и происходит эмиссия биткойнов. Верификация транзакций осуществляется посредством решения компьютерами сложных математических задач. Этот процесс был определен в протоколе криптовалюты (биткойна) его создателем Сатоши Накамото и остается неизменным. Участников системы «Биткойн», которые занимаются майнингом, называют майнерами.

Не все участники сети добывают биткоины. Тем не менее, при желании майнером может стать каждый, у кого имеются определенные знания в этой области, доступ в интернет и подходящее оборудование.

За присоединение каждого нового блока к блокчейну майнеру начисляется награда — собственно, криптовалюта.

Немного цифр:

– величина награды уменьшается вдвое каждые 210 000 добытых блоков;

– изначально награда составляла 50 BTC;

– на добычу одного блока уходит около десяти минут;

– добыча 210 000 блоков по времени занимает около четырех лет;

– всего будет выпущено 21 млн BTC (рисунок 34).

Рисунок 34 – Динамика выпуска BTC
и размера вознаграждений за процесс майнинга

В 2018 году награда за блок составляет 12,5 BTC, а с 23 мая 2020 г. она будет равняться 6,25 BTC. Последний биткойн будет добыт в 2140 году, но уже в 2018 году в обороте находится 80 % от общего количества биткойнов, а к 2036 году пользователи намайнят более 99 %.

Блок представляет из себя следующую конструкцию: заголовок (*header*), а затем список всех транзакций текущего блока (*payload*).

Заголовок состоит из хеша предыдущего («родительского») блока и хеша транзакций текущего блока, а также некоторой служебной информации (дата и время создания блока, его версия) (рисунок 35).

Рисунок 35 – Структура блока в системе «Биткойн» и добавление нового блока в блокчейн

Хеш предыдущего блока используется для проверки нового блока на подлинность. Таким образом, платежи в системе «Биткойн» подтверждаются раз в десять минут — только тогда, когда находится новый блок. Подтверждаются не все транзакции, а только те, которые выберет майнер из очереди (мемпула). Например, часто майнеры запрограммированы выбирать транзакции с большей комиссией, так как комиссия – его оплата за работу; у отправителя же часто есть возможность определять ее размер.

Понятия хеш-сумма и хеш-функция[1]

Хеш, или хеш-сумма — это результат компьютерной обработки строки символов. Строка обрабатывается некой математической хеш-функцией таким образом, что из полученного результата невозможно получить исходные данные.

Хеш-функция — это сложная математическая функция, которая шифрует строку данных с помощью определенного алгоритма (*SHA256* в случае с Биткойном). С его помощью из одной и той же строки данных получается бесконечное число разных вариантов.

[1] См.: Антонопулос А. М. Осваиваем биткойн: программирование блокчейна. Москва: ДМК-Пресс, 2018. 428 с.

Майнер «ищет» правильный вариант — ту хеш-сумму, которая будет записана в следующий блок. Для этого он устанавливает на свой компьютер специальное программное обеспечение с открытым кодом — программу, вычисляющую правильный хеш для блока, который может быть добавлен в блокчейн. Когда ему это удается, другие компьютеры в системе «Биткойн» получают сигнал и проверяют данные на подлинность. Если хеш-сумма правильная, в блокчейн добавляется новый блок (рисунок 36).

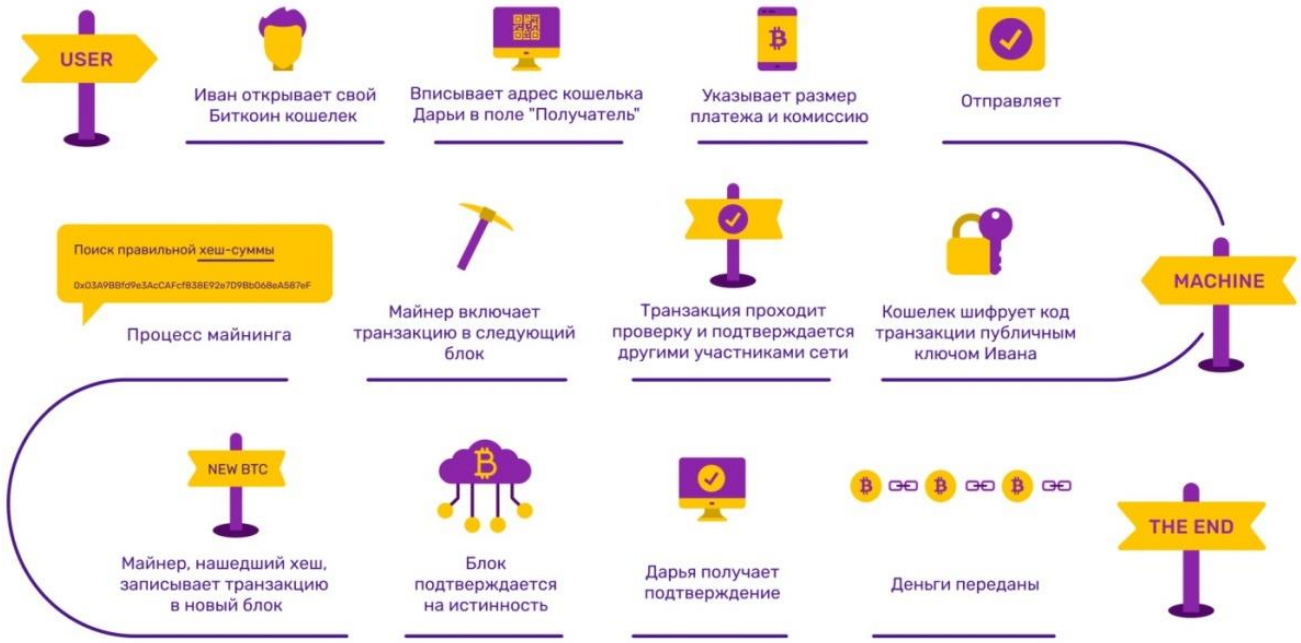

Рисунок 36 – Алгоритм транзакции в системе «Биткойн»

Протокол Биткойн предусматривает, что правильная хеш-сумма будет находиться раз в десять минут. Этот параметр не меняется с самого начала работы сети и не зависит от количества участников и их хешрейта.

Понятие хешрейта[1]

Хешрейт — это скорость, с которой майнер обрабатывает информацию, она соответствует количеству хешей, которое он находит в секунду. Чем выше хешрейт участника сети, тем больше вероятность того, что именно он найдет верную хеш-сумму и получит вознаграждение. Таков принцип распределения вознаграждения между участниками сети — *Proof-of-Work*, или доказательство работы.

[1] Что такое хешрейт и сложность майнинга криптовалют? URL: https://forklog.com/chto-takoe-heshrejt-i-slozhnost-majninga-kriptovalyut (дата обращения: 19.08.2021).

За годы существования в системе «Биткойн» количество точек в блокчейн-сети, основные функции которых сводятся к распределению данных между другими узлами (нодами) выросло в тысячи раз, мощность производимого оборудования также значительно увеличилась. Если бы в протоколе не было прописано правило о добыче блока раз в десять минут, он находился бы гораздо быстрее из-за высокого хешрейта участников. Однако этого не происходит из-за изменения сложности сети (рисунок 37).

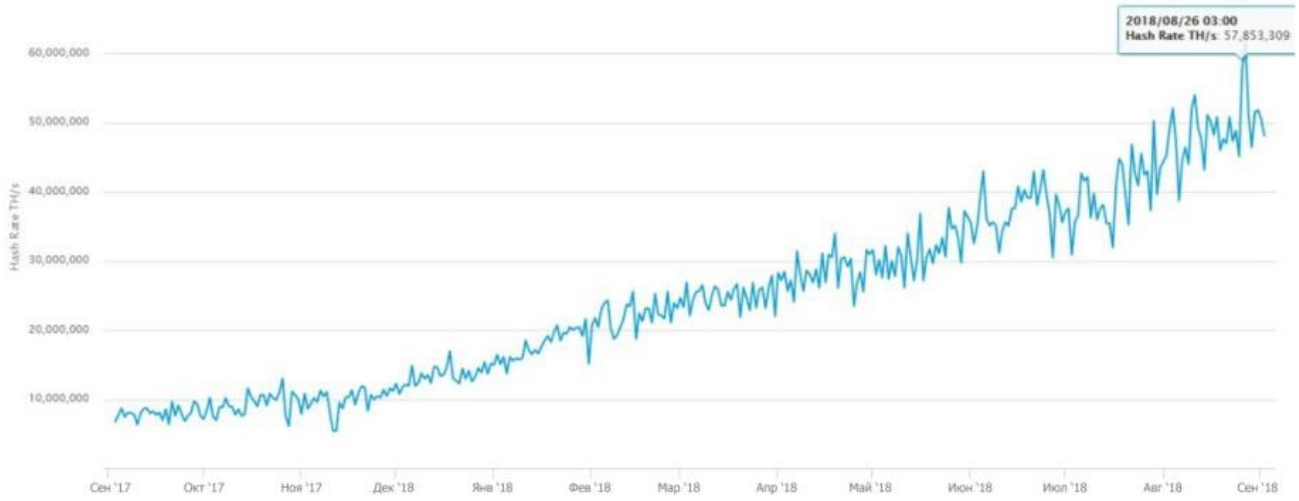

Рисунок 37 – График изменения хешрейта в системе «Биткойн» за год с сентября 2017 по сентябрь 2018 гг. (данные с сайта *Blockchain.com*)

Понятие сложности сети

Сложность сети, или *Bitcoin Difficulty* — это параметр, используемый для регулирования скорости нахождения нового блока. Каждые 2016 блоков система автоматически проверяет хешрейт сети, и, если он заметно изменился, меняется и сложность. Например, если добавился новый участник с высоким хешрейтом, он может находить новые блоки быстрее, таким образом, возрастет общий показатель хешрейта сети. В этом случае система отрегулирует скорость повышением сложности сети, чтобы эмиссия (выпуск монет) оставалась равномерной.

Хешрейт сети таков, что вероятность добывания блока рядовым участником с обычным, пусть даже мощным персональным компьютером, стремится к нулю. Поэтому получить биткойны можно двумя путями:

– организовать собственную майнинговую ферму — объединить большое количество устройств и получить таким образом высокий хешрейт;

– присоединиться к пулу для майнинга.

Первый вариант достаточно дорогой, но более прибыльный, в то время как второй более доступен, поэтому многие выбирают именно его.

Понятие пула для майнинга

Это группа устройств для майнинга, объединенная с целью повышения вероятности нахождения нового блока. Хешрейт всех подключенных к пулу компьютеров суммируется, и таким образом повышается шанс нахождения правильной хеш-суммы. Вознаграждение за присоединение блока распределяется между участниками по определенному пулом алгоритму, который учитывает хешрейт участника, время майнинга и другие факторы.

3.5. Хранение и обработка ключей в криптовалютных кошельках

Очередной задачей в организации работы биткоин сети является решение вопроса о том, где и как хранить пользователю свой личный ключ. С конца 2008 года сложилось несколько подходов к решению этого вопроса:

– хранение и управление на выделенном сервере (рисунок 38);

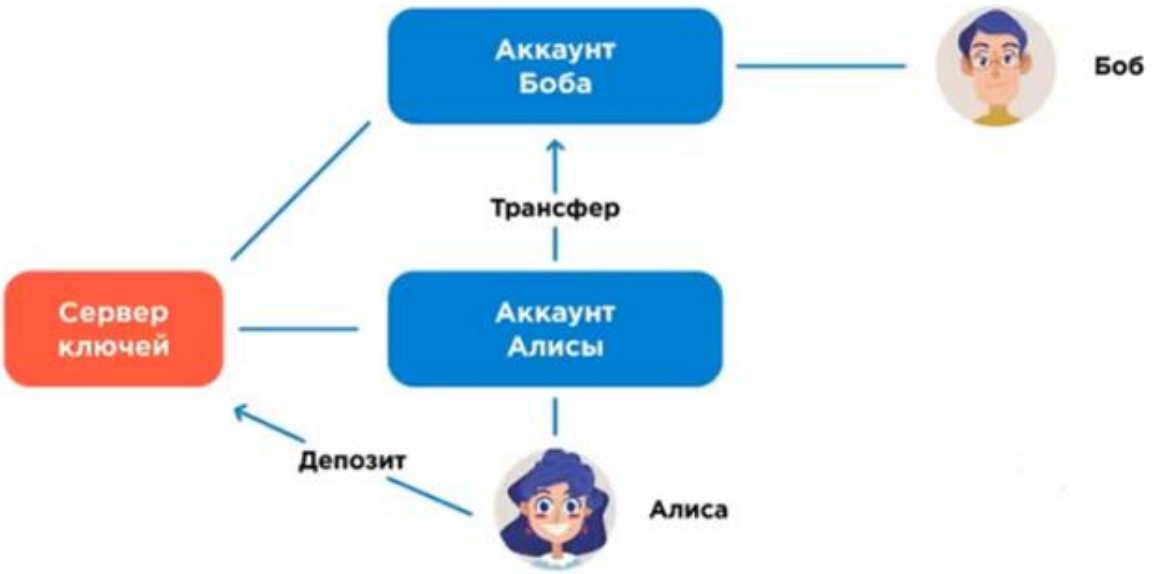

Рисунок 38 – Хранение и управление на выделенном сервере

– хранение на выделенном сервере, управление на устройстве;

– хранение и управление на устройстве (рисунок 39);

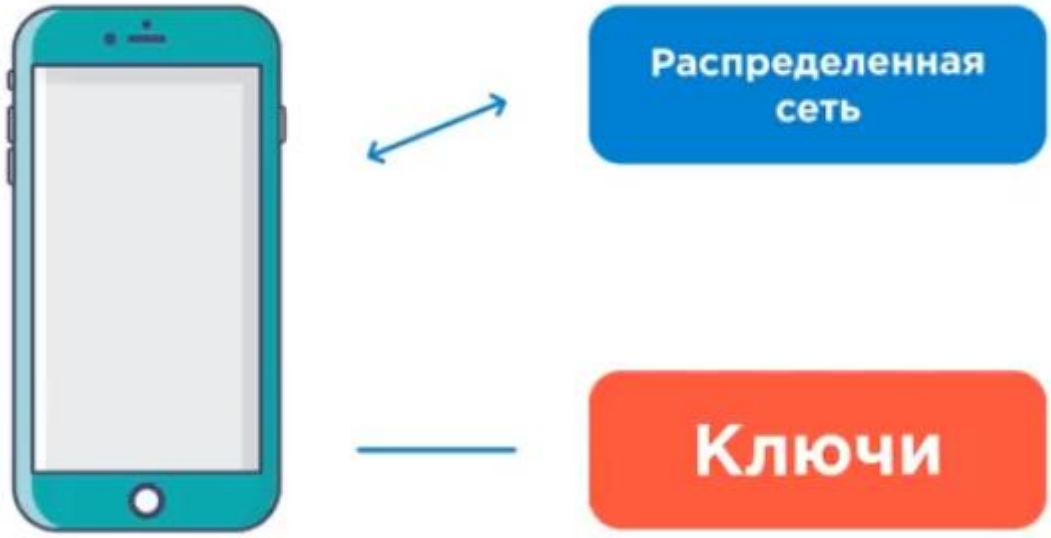

Рисунок 39 – Хранение и управление ключами на устройстве

– смешанное с использованием мультиподписи (рисунок 40).

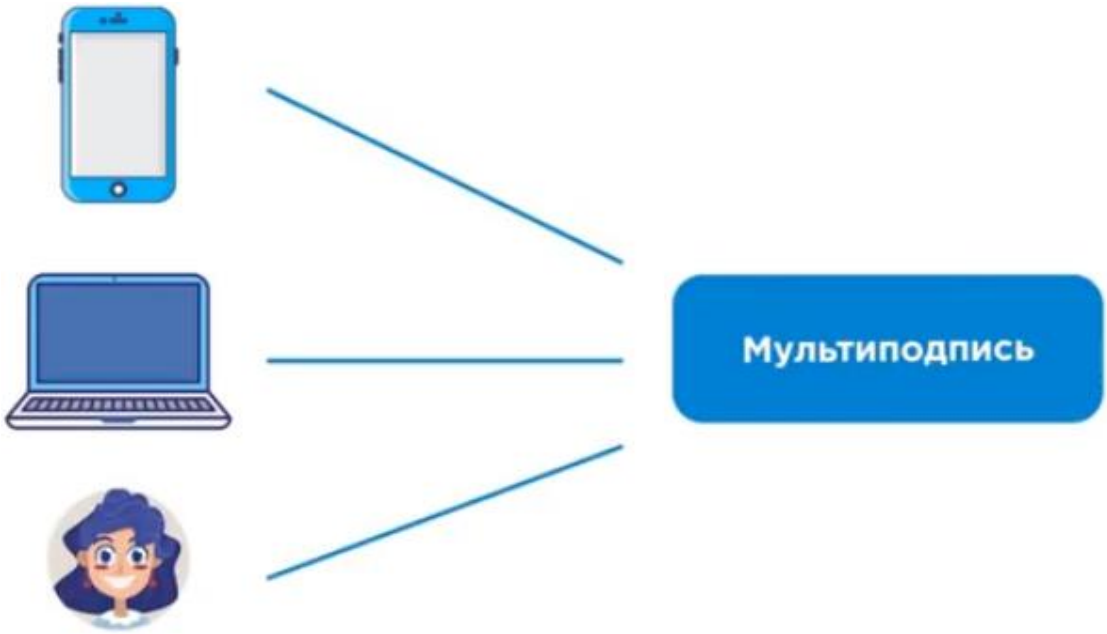

Рисунок 40 – Смешанное с использование мультиподписи

В первом случае все данные, процесс их обработки и изменения происходит на удалённом сервере. Выходит, ситуация, когда сервис, который предоставляет услугу такого кошелька, полностью контролирует

ключи. Данный подход на уровне клиента почти схож с любым интернет-банкингом.

Такой кошелёк имеет множества своих личных ключей, которые хранятся и используются только самим сервисом, пользователи доступа к ним не имеют. Получается, что они «не владеют» реальной криптовалютой. Ведь вся валюта хранится на дата-центрах сервера, а клиент видит лишь отображение своих денег в переводе на определённую криптовалюту по текущему курсу на рынке или бирже.

Чтобы воспользоваться таким видом криптокошелька, пользователю необходимо сначала выбрать один из множества сервисов, предоставляющих подобный вид услуг, и создать там аккаунт под своими или же чужими данными. В современном мире многие сервисы запрашивают данные, подтверждающие личность, с целью возможности просмотра и контроля транзакций пользователя, тем самым пресечения возможных противозаконных действий. По сути, клиент управляет своими средствами через аккаунт, на котором имеется свой виртуальный счёт для каждой криптовалюты.

При переводе валюты вне системы, то есть не между пользователями одинакового сервиса, сервис самостоятельно создаёт транзакцию и отправляет со своих ключей на внешний кошелёк. И в коде транзакции, следовательно и в блокчейне отражаются личные ключи не конкретного пользователя, а ключи, сгенерированные сервисом и принадлежащие ему[1].

К плюсам такого вида организации и хранения личных ключей можно отнести: моментальные переводы без комиссии между участниками системы, простой доступ к аккаунту с нескольких устройств, простое восстановление аккаунта при утере пароля.

Скорость перевода между пользователями одного сервиса достигается за счёт того, что на программном уровне требуется лишь перезаписать значения валют на двух аккаунтах — вычесть из имеющихся у отправителя и прибавить к старому значению у получателя. За счёт такой системы достигается и отсутствие комиссии при переводе.

Наличие одного аккаунта и пароля к нему снимают необходимость отдельного хранения своего личного ключа на одном устройстве, что приводит к удобству входа и возможности управления своими

[1] Milosh D. V., Gerasenko V. P. Digital of financial assets: current state and forecast of development at the global level on the example of cryptocurrencies // Corporate governance and innovative economic development of the north: bulletin of research center of corporate law, management and venture investment of syk-tyvkar state university. – 2020. – № 4. – P. 99–104.

средствами с любого устройства. Требуется только логин и пароль, как, например, для входа в социальную сеть или интернет-магазин.

К минусам данного похода относятся: отсутствие контроля над своими ключами, а вследствие и средствами, максимальная зависимость от сервиса.

В случае технических неполадок или же осуществления кибератаки на сервера, которым дано разрешение на управление средствами пользователя и их хранение, доступ к ним утрачивается. Клиент не имеет возможности осуществить любой перевод, либо же вывести деньги из системы, также есть риск на кражу хакерами средств, которые хранились на сервере.

При выборе второго способа — хранение на сервере и управление на устройстве — уменьшается зависимость от сервиса и риск полной потери своих средств.

При этом методе хранения ключей, пользователь генерирует на своём устройстве личный ключ, далее его зашифровывает паролем и отправляет на сервер ключей. Этот сервер хранит в себе все ключи пользователей, которые к нему подключены. В случае, когда клиенту требуется управление счётом, например, осуществить транзакцию, он заходит в свой аккаунт, запрашивает у сервера свой зашифрованный ключ, на своём устройстве его расшифровывает и работает непосредственно на самом девайсе.

Такой подход позволяет повысить уровень безопасности и не отказываться от всех удобств использования облачного хранения данных. Плюсами являются: простой доступ к аккаунту с нескольких устройств, наличие прямого контроля над своими ключами.

Но здесь всё также остаётся высокая зависимость от сервера ключей, ведь при любой неполадке или, непосредственно, аварии на самом сервере, пользователь теряет доступ к своей криптовалюте. А если после какого-либо происшествия сотрутся сами данные, то доступ будет утерян навсегда.

Рассматривая третий способ, где хранение и управление ключами происходит на самом устройстве пользователя, сразу выделяется ряд ярких преимуществ и недостатков перед предыдущими способами.

Полный контроль над ключами является неотъемлемым плюсом, ведь при таком подходе исчезает зависимость от сервера и того, что может с ним произойти. Все ключи и данные хранятся непосредственно на накопителе, установленном в устройство, и возможность достать их злоумышленнику, резко уменьшается, а при осуществлении

определённых действий и соблюдении принципов информационной безопасности эту возможность можно привести близкой к нулю.

Также к плюсам можно отнести возможность офлайн работы и полную независимость от программного обеспечения.

Необходимость в ручном переносе между устройствами, в случае их смены или же надобности использования другого, а также ручное создание резервных копий кошелька, вытекает прямо из «определения» рассматриваемого подхода.

Для того, чтобы всё это проводить без ошибок и дальнейших сбоев, требуется обладать определённым уровнем знаний, который на порядок выше того, что необходим для лёгкого хранения и управления ключами на выделенном сервере.

Последний возможный способом управления своими средствами в криптовалютном кошельке — это смешанное использование предыдущих методов с применением мультиподписи (

Рисунок).

Данную технологию рассмотрим на примере.

Пользователь имеет свой личный ключ, который сгенерировал с помощью аппаратных средств, он его делит, например, на три части и делает мультиподпись $^{2}/_{3}$.

Пользователь решает хранить и управлять одной такой частью через удалённый сервер, вторую он решает хранить на одном устройстве, а третью — на другом устройстве. Получаем ситуацию, что при мультиподписи $^{2}/_{3}$ для отправки транзакции ему требуется сначала поставить подпись на одном устройстве, потом переслать её на другое, там завершить подпись и уже после можно отправить в сеть. Или сначала подписать часть через сервис, отправить на одно из устройств и там поставить вторую необходимую для полного формирования транзакции подпись.

При выбранном методе имеется возможность совместить преимущества хранения личных ключей на сервере и на физическом устройстве, таким образом сглаживая минусы каждого из способов по отдельности.

3.6. Синхронизация кошельков с Биткойн-сетью

Для получения всего ряда возможностей Биткойн необходимо решить вопрос работы в распределённой сети, ведь она является достаточно сложной темой, в которой встречаются со следующими проблемами.

Одна из них заключается в способе проверки данных из распределённой сети, а вторая – в оптимизации хранения всех этих данных. Возникает конфликт между этими двумя запросами: с одной стороны, чем больше объём хранимых данных, тем более качественную проверку новых транзакций мы можем осуществить, но с другой — это противоречит требованию в оптимизации хранения таких данных.

Еще одна проблема заключается в следующем. Чтобы получить историю транзакций по определенному адресу на полном узле сети, придется проверить весь блокчейн, что достаточно долго, поскольку это большой объем данных, а грубый перебор — малоэффективный подход. Для оптимизации запросов применяются специальные надстройки над обычным узлом сети, которые помогают индексировать блокчейн и кэшировать некоторые данные для ускорения поиска по популярным метрикам. По такому принципу работает любой *blockchain explorer*, который достаточно быстро возвращает данные практически о любом адресе и любой транзакции[1].

Отсюда вытекают несколько кардинально разных подходов к решению вопроса о взаимодействии с внешней сетью и синхронизацией с ней.

Первый подход: кошелёк — полный узел сети (*full node*) (рисунок 41).

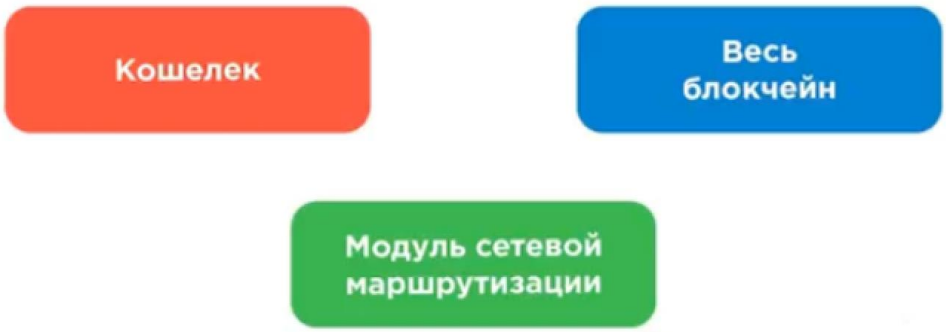

Рисунок 41 – Кошелёк — полный узел сети

В таком случае кошелёк имеет сразу два модуля, один из которых выступает в роли хранилища под весь блокчейн и обновляет его при появлении очередного блока. Он синхронизируется и создаёт

[1] Syporyatov V. A., Maskaev A. I. Evolution of the institutional structure of private money in the form of cryptocurrencies — development models and controversy with Hayek's = Эволюция институциональной структуры частных денег в форме криптовалют — модели развития и полемика с позицией Хайека // Journal of economic regulation (Вопросы регулирования экономики). 2020. Vol. 11. № 3. P. 40–43.

соединение с подобными модулями других пользователей сети посредством доступа в Интернет сеть, который предоставляет ему модуль сетевой маршрутизации.

Такой способ обычно применяют в деятельности пользователи, которым необходимо регулярно принимать и отправлять платежи на большие суммы, что влечёт за собой потребность в постоянном онлайн режиме и повышенном уровне безопасности личных средств.

Стоить отметить, что при подходе хранения и управления биткойном на выделенном сервере, рассмотренном во втором параграфе данной работы, сервер, которому мы доверяем свои деньги и логины с паролями, обязательно прибегает к работе с полным узлом сети.

За счёт сосредоточения всех необходимых элементов для работы непосредственно на устройстве пользователя появляется ряд возможностей, например, осуществление офлайн работы, лишь с периодическим выходом в сеть для обновления базы блокчейна. Либо возможность полного контроля над проверкой всех данных.

К недостаткам такого подхода относятся высокие требования аппаратной составляющей устройства, так как необходимо обеспечить достаточно большой объём памяти для хранения всего блокчейна, повышенное потребление трафика и вычислительных мощностей.

Второй способ: использование доверенного узла сети (*trusted node*).

В таком подходе логика кошелька и логика проверки транзакций разносится посредством использования доверенного узла сети, что является главным отличием от предыдущего метода. Такой узел может поддерживать кто угодно, например, друг пользователя, которому он доверяет процесс проверки своих транзакций.

Зачастую такой подход используют *IT*-компании в своих цифровых кошельках. Они обещают пользователям качественную проверку транзакций и клиенты, фактически веря обещаниям, доверяют им. Способность хранить свои личные ключи самостоятельно и заверять ими транзакции у пользователей не пропадает, но статус подтвержденности транзакций клиент сам не проверит, а спрашивает его у доверенного узла.

Для такого вида кошелька необходима реализация дополнительной надстройки для кеширования блокчейна, которая помогает индексировать его, что ускоряет доступ с клиентских приложений. Такое кеширование требует немалое количество памяти, обеспечение доступа к которой ложится на плечи компании разработчика, как и высокие требования к стабильности в работе. Как только пропадает

доступ к доверенному узлу, пользователь утрачивает возможность выхода в сеть и общения с ней.

Ещё одной из проблем для компании-разработчика, которую необходимо решить, является передача данных между кошельком и сервером по защищённому каналу связи. При таком подходе появляются угрозы атаки *Main in the middle*, которая заключается в получении злоумышленником доступа к тексту сообщения и изменении его в своих целях, посредством перехвата данных в канале связи. Пользователь, в случае изменения сообщения при передаче ему, этого не обнаружит, ведь сообщения пришло из доверенного им источника[1].

Проблема замыкания на одном узле и угрозы потери доступа к общей сети решается использованием сразу нескольких таких. В один момент времени мы остаёмся подключенными к одному конкретному узлу, но в случае потери к нему доступа, благодаря программному обеспечению, случайным образом выбирается другой доверенный узел, и работа продолжается.

Третий подход: использование облегчённого узла сети (*Simplified Payment Verification — SPV*).

В случае использования *SPV* (рисунок 42) нет необходимости в запуске своих полных узлов или же выборе доверенных. Кошелёк фактически выбирает несколько десятков чужих полных узлов и поддерживает с ними постоянное общение, обмениваясь с ними *p2p* сообщениями.

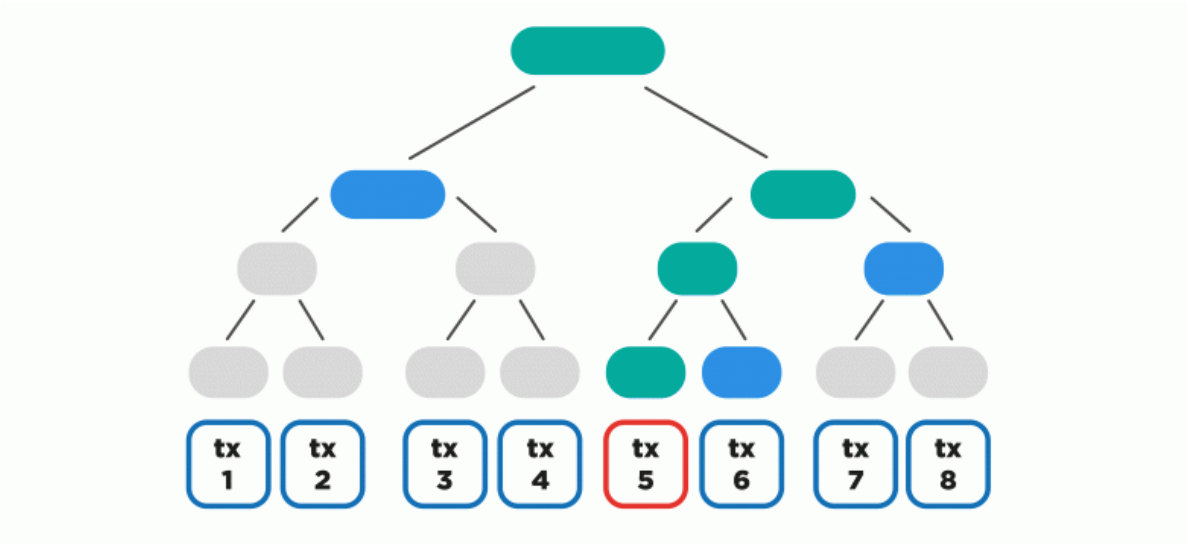

Рисунок 42 – *Merkle Tree*

[1] Целых А. А., Целых А. Н., Котов Э. М. Современные технологии противодействия финансовым преступлениям: учебное пособие. Ростов-на-Дону: Южный федеральный университет, 2019. С. 91–94.

На вход такой узел получает не сами блоки, а их заголовки, что резко уменьшает размер необходимой памяти, ведь заголовок занимает всего 80 байт. В каждом таком заголовке есть поле, называемое *Merkle Root*, в котором записывается хеш-значение всех транзакций, рассчитанное по схеме *Merkle Tree*.

Такая схема позволяет убедиться, входит ли хеш-значение определённой транзакции в блок, не имея данных обо всех остальных транзакциях этого блока.

Таким образом, кошелёк, который использует схему *SPV*, имея одну из веток *Merkle Tree*, которую в свою очередь можно запросить у полного узла сети, может убедиться в подтвержденности нужной транзакции в её блоке.

Недостаток состоит в том, что на таком клиенте проверка осуществляется не полностью, он лишь удостоверяется в факте проверки транзакции полными узлами сети. Всё опять сводится к доверию, что большинство вычислительных мощностей используется в честных целях, ведь возможность атаки 51 % тут также присутствует.

Для минимизации возможности получения данных от злоумышленников используется соединение с максимальным количеством полных узлов сети, чем их больше, тем меньше шансов стать жертвой хакеров.

SPV-узлы требовательны к стабильной работе сетевого соединения, тем не менее, часто применяются даже в мобильных приложениях. Этот подход синхронизации с платежной сетью достаточно широко распространен и используется в ряде популярных Биткойн кошельков.

Глава 4
КРИМИНАЛИЗАЦИЯ ОБЩЕСТВЕННО ОПАСНОЙ ДЕЯТЕЛЬНОСТИ В ОТНОШЕНИИ ИЛИ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ И ДРУГИХ ВИРТУАЛЬНЫХ АКТИВОВ

4.1. Нормативно-правовое обеспечение криптовалюты

Растущий спрос на глобальные социально-политические и экономические реформы приводит к значительным изменениям не только в так называемом общественном договоре, но и во всей международной правовой системе. Одним из ключевых инструментов в этой эволюции стали виртуальные валюты (криптовалюты). Попытки эффективного регулирования криптовалют не только создают оптимальную правовую платформу для криптовалютного бизнеса, но и наглядно иллюстрируют проблемы, с которыми сталкиваются национальные власти по всему миру при попытке определить и понять феномен децентрализованных систем в целом. Этот случай также иллюстрирует тот исторический факт, что государства, возглавлявшие мировую финансовую экономику, не смогли адекватно отреагировать на инновации и технологические достижения.

Вместе с тем ситуация в сфере оборота криптовалют хорошо коррелирует с несистемными попытками регулирования многих других инновационных явлений, таких как внедрение децентрализованной сети блокчейн. Не так давно основной вопрос о статусе криптовалют в России и за рубежом упирался в главную дилемму: запрещать или не запрещать криптовалюты? Регулировать их оборот или наблюдать за процессом? Облагать налогами или нет? В Российской Федерации эти ключевые вопросы пока остаются неразрешенными. Следовательно, криптовалюта в настоящее время находится в некоем правовом вакууме. Для того чтобы максимально точно установить правовой режим криптовалютой деятельности в России и определить статус самих криптовалют, на наш взгляд, необходимо рассмотреть опыт зарубежных стран, как положительный, так и отрицательный, на основании которого выработать оптимальный путь для нашего государства в сфере регулирования оборота криптовалюты.

Появление первых видов криптовалют в мире было воспринято

различными государствами негативно, ведь, по сути, правительства лишались основного своего преимущества — эмиссии денег. И действительно, на первоначальном этапе возникновения криптовалют отношение к ним со стороны правительств было резко отрицательным, после чего многие государства стали их просто-напросто запрещать и вводить ответственность за расчеты в криптовалюте. Затем, поняв, что процесс эмиссии криптовалют невозможно контролировать, государства предприняли попытки регулирования их оборота и налогообложения. И вот в настоящее время ситуация радикально изменилась: международные законодатели склонны рассматривать криптовалюты как новое перспективное направление в экономике, а не как неопределенный валютный суррогат в теневом секторе экономики.

Большинство международных регуляторов продолжают наблюдать за развитием криптовалютой индустрии, не предпринимая активных действий по ее легализации, но предупреждая собственных граждан о рисках, связанных с ее использованием. Так, например, Австралия, стремясь обеспечить благоприятные условия для развития криптовалютой индустрии и создания собственных финансово-технологических центров, демонстрирует намерение стать одной из наиболее прогрессивных юрисдикций и не исключает использования технологий децентрализованной сети блокчейн в различных сферах государственного регулирования (например, в управлении наземным транспортом).

Возможность применения блокчейна рассматривает и почта Австралии. Активно развиваются и негосударственные проекты, связанные с цифровыми деньгами. Резервный банк Австралии в 2013 году определил криптовалюту биткойн, как альтернативу валютам разных стран и платежную систему.

При этом Комиссией по ценным бумагам и инвестициям Австралии цифровая валюта (криптовалюта) не рассматривается как финансовый продукт, и криптовалютная деятельность, т. е. деятельность, прямо или опосредованно связанная с криптовалютами, например, майнинг, или ее использование в качестве средства платежа или обмена не подлежат лицензированию.

Согласно Австралийскому кодексу поведения для игроков индустрии цифровых валют (*Australian Digital Currency Industry Code of*

Conduct), разработанному Ассоциацией цифровых валют и коммерции Австралии (*Australian Digital Currency & Commerce Association*), надлежащие стандарты ведения криптовалютного бизнеса установлены и являются обязательными к исполнению только для членов указанной Ассоциации. Сама организация в случае нарушения ее членами положений Кодекса может накладывать на них штрафные санкции.

В 2014 году Налоговая служба Австралии (*Australian Taxation Office*) отметила возможность введения налогообложения криптовалютных операций. В настоящее время операции с криптовалютой, криптовалютные транзакции в Австралии облагаются стандартным подоходным налогом и налогом на прибыль (*Income Tax, Corporate Tax*). В то же время при использовании криптовалюты как инвестиций не возникает необходимость уплаты налога на прирост капитала (*Capital Gains Tax*). При этом в Австралии существует легальная возможность выплачивать заработную плату в криптовалюте, но только при наличии договора между работником и работодателем. Кроме того, в Австралии с 2016 года Активно разрабатывается и законодательство в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, регулирующее деятельность криптовалютных бирж, которое являлось бы эффективным противодействием преступлениям, совершаемым с использованием криптовалюты. Однако до настоящего момента каких-либо нормативных правовых актов и уголовно-правовых запретов не введено.

Великобритания — лидер криптовалютой интеграции и наиболее благоприятная юрисдикция для ведения криптовалютного бизнеса — на государственном уровне оказывает поддержку криптовалютному сообществу и стартапам, связанным с криптовалютой. Начиная с 2014 года Банком Англии (*Bank of England*) проводились исследования гипотетических рисков для кредитно-денежной системы от цифровых валют, в частности от их использования в качестве основной платежной единицы, и был сделан вывод о том, что риски настолько минимальные, что возможное регулирование криптовалют предотвратит их преступное использование и поддержит инновации в данной сфере.

Управление по финансовому регулированию и контролю

Великобритании указало, что криптовалюта — это и не деньги, и не валюта, поэтому не может регулироваться финансовым законодательством Великобритании. Таким образом, в настоящее время криптовалюту в Великобритании считают уникальной комбинацией цифр, полученной в результате сложных математических вычислений и алгоритмов. Соответственно, она не подпадает под действие Закона Великобритании о легализации (отмывании) доходов, полученных преступным путем (*Money Laundering Regulations*).

По другому пути пошел Европейский Союз в правовом регулировании криптовалютного бизнеса, хотя государства — члены Европейского Союза традиционно считаются благоприятными для его ведения. Ни один из регуляторов (органов) Европейского Союза не принял никаких специальных правил регулирования криптовалютной деятельности.

В 2012 году Европейский центральный банк (*European Central Bank*) опубликовал отчет, в котором заявил, что традиционное регулирование финансового сектора неприменимо к биткойнам. Сам биткойн в документе был определен как конвертируемая децентрализованная виртуальная валюта. Европейская служба банковского надзора (*European Banking Authority*) обратила внимание на то, что криптовалютные биржи — не банки, а их деятельность в настоящее время не урегулирована, поэтому пользователи не защищены от денежных убытков в случае их закрытия. В 2016 году Европейская комиссия объявила о планах по ужесточению стандартов отчетности для криптовалютных бирж и компаний, предоставляющих криптовалютные кошельки пользователям. В частности, Еврокомиссия планировала обязать европейские криптовалютные биржи и провайдеров криптовалютных кошельков проводить обязательную идентификацию пользователей.

В свою очередь, Комитет Европарламента по экономическим и монетарным вопросам (*European Parliament's Committee on Economic and Monetary Affairs*) указал, что следует воздержаться от прямого регулирования криптовалют, однако возможно приведение правового положения криптовалют в соответствие с существующими нормами по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Тогда же Европейская комиссия предложила принять Директиву о предупреждении использования финансовой системы для целей отмывания преступных

доходов и финансирования терроризма (2015/849/ЕС)[1].

Вместо термина «криптовалюта» европейскими регуляторами используется термин «цифровая валюта». При этом она рассматривается в большей степени как средство обмена. Таким образом, операции по купле и продаже биткойна за традиционные фиатные валюты не должны облагаться налогом на добавленную стоимость. До этого национальные регуляторы по-разному относились к обложению криптовалюты этим налогом.

Порядок обложения криптовалюты и операций с ней другими налогами регулируется национальным законодательством государств-членов в зависимости от природы криптовалютной операции. При этом, как правило, цифровая валюта в целях налогообложения рассматривается как нематериальный актив или товар, а не как валюта или деньги.

Так, например, в Норвегии, Финляндии и Германии криптовалюта облагается налогом на прирост капитала (*Capital Gains Tax*) и налогом на богатство (*Wealth Tax*). В Болгарии цифровая валюта рассматривается как финансовый инструмент и облагается соответствующими налогами. В Австрии криптовалюта рассматривается налоговыми органами в качестве нематериального актива, а ее майнинг — как операционная деятельность.

Следовательно, доход, полученный в результате ее отчуждения, облагается подоходным налогом (*Income Tax*). В целом правовое регулирование криптовалюты и операций с ней в Европейском Союзе осуществляется в рамках политики противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Соединенные Штаты Америки в отношении криптовалют пошли по пути регулирования налогообложения в сфере криптовалютной торговли, заставив все американские криптовалютные биржи проводить верификацию своих клиентов. При этом США — одна из наиболее удобных стран в мире для ведения криптовалютного бизнеса.

[1] Директива (ЕС) № 2015/849 Европейского парламента и Совета ЕС о предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии. Доступ из прав.-правовой системы «КонсультантПлюс».

Но правовое регулирование цифровой валюты в США при этом не менее сложное, чем в Европе. В основном это обусловлено особенностями правовой системы государства (наличием, как федерального права, так и права штатов) и отсутствием единой позиции среди регуляторов относительно правового статуса криптовалюты.

В 2012 году Федеральное бюро расследований США (*Federal Bureau of Investigation*) (далее — ФБР) выпустило отчет «Виртуальная валюта биткойн, уникальные особенности которой представляют отдельные затруднения сдерживания незаконной деятельности»[1]. В нем ФБР выразило свою обеспокоенность возможностью осуществления незаконной деятельности в анонимной платежной системе биткойн. В 2013 году представители Федеральной резервной системы (*Federal Reserve System*) определили криптовалюту как «угрозу для банковской системы, экономической деятельности и финансовой стабильности».

Конституция США закрепляет федеративное устройство государства. Соответственно, общественные отношения, связанные с криптовалютой, регулируются не только федеральным правом, но и правом штатов. Криптовалютная деятельность подлежит лицензированию, если такое требование установлено правом штатов.

Относительно правового регулирования в Российской Федерации ведется ряд дискуссий о признании или не признании криптовалюты международным рынком, о статусе новой платежной системы, о способах регулирования, о подготовке и привлечении специалистов в области криптовалюты, о возможностях использования биткойна в качестве денежной единицы и многое другое.

Центробанк России занимает противоположную позицию относительно законного принятия криптовалют как средства платежа. Несмотря на это, в начале октября 2017 года глава Центрального Банка Эльвира Набиуллина говорила о потенциальной допустимости разработки национальной цифровой валюты на основе технологии блокчейн[2]. Глава Сбербанка Герман Греф положительно отзывался о развитии биткойна, а также о том, что криптовалюты в России необходимо узаконить[3].

Выступая на заседании Совета Безопасности Российской Федерации, секретарь Николай Патрушев говорил о том, что специалисты

[1] URL: https://habr.com/ru/articles/143587/(дата обращения: 17.08.2021).
[2] URL: https://www.interfax.ru/business/581900 (дата обращения: 17.08.2021).
[3] URL: https://iz.ru/news/717485?ysclid=lgxnuv8ikd408365541 (дата обращения: 17.08.2021).

полностью не определились с понятием и представлением криптовалюты, а значит, данная область остается полем деятельности для мошенников[1]. При этом руководитель рабочей группы по криптовалютам при Государственной думе Федерального собрания Российской Федерации, Элина Сидоренко отметила, что Н. Патрушев во время своей речи упомянул об угрозе использования криптовалюты — способствование процветанию преступных доходов и теневого интернета[2].

Однако, несмотря на такое расхождение во мнениях, государство не может игнорировать такое явление в международной экономической сфере. Поэтому Президент Российской Федерации Владимир Путин по итогам прошедшего в октябре 2017 года в Сочи совещания посвященному внедрение цифровых технологий в финансовой, банковской сфере, использование инновационных финансовых инструментов поручил Правительству Российской Федерации сконструировать законодательство в сфере криптовалют в России. В. В. Путин акцентировал внимание на том, что регулирование криптовалюты необходимо производить без построения преград для их использования, а также с учетом гарантий и защиты прав граждан, предпринимателей и государства[3].

В январе 2018 года Министерство финансов Российской Федерации разместило на своем официальном сайте проект федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[4]. Цель закона заключается в регулировании производства, оборота, обмена, хранения и получения прибыли от цифровых финансовых активов, а также осуществления прав и исполнения обязательств по смарт-контрактам. Законопроект содержит обще используемые ключевые понятия, такие как цифровой финансовый актив, цифровая транзакция, реестр цифровых транзакций, криптовалюта, майнинг и другие, а также особенности выпуска токенов и обращения цифровых активов.

---

[1] URL: https://cryptowiki.ru/article/nikolai-patryshev-rasskazal-ob-otnoshenii-sovbeza-rf-k-kriptovalutam.html?ysclid=lgxo3tv5zs347250493 (дата обращения: 17.08.2021).

[2] URL: https://news.myseldon.com/ru/news/index/177667657 (дата обращения: 17.08.2021).

[3] URL: http://www.kremlin.ru/events/president/transcripts/deliberations/55813 (дата обращения: 17.08.2021).

[4] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: законопроект № 419059-7 // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество»). URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения: 17.08.2021).

Под цифровым финансовым активом понимается имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств. Права собственности на данное имущество удостоверяются путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта, токен. Цифровые финансовые активы не являются законным средством платежа на территории Российской Федерации.

Из данного определения, которое содержится в статье второй законопроекта «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», исходит то, что Российская Федерация старается узаконить инновационные платежные системы, с осторожностью, без причинения вреда экономической сфере государства и для устранения ажиотажа, возникшего на международном рынке в связи с появлением криптовалюты, а также с целью обезопасить ее использование участниками данных отношений и предотвратить возрастание преступности и теневых операций, связанных с созданием, оборотом и хранением цифровых финансовых активов.

Рассматриваемый законопроект «О цифровых финансовых активах», в своей терминологии, раскрывает два вида цифровых финансовых активов: криптовалюта и токен. Разница, исходя из текста части 3 статьи 3, состоит в том, что токен может производиться юридическим лицом или индивидуальным предпринимателем с целью привлечения прибыли. Теперь, вся связанная с этим деятельность будет детализироваться путем ведения цифровых транзакций, где необходимо будет указывать информацию о передаче прав на электронную валюту от одного участника к другому, посредником такого обмена может быть только оператор цифровых активов, а именно, юридическое лицо, обладающее правом осуществлять подробные сделки, то есть быть дилерами, форекс-дилерами и брокерами или организаторами торговли, имеющими лицензию биржи или торговой системы. Помимо данного законопроекта, регулирование деятельности таких операторов подлежит Федеральному закону от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах»[1], а действия, совершаемые этими субъектами отношений, устанавливаются согласованно с Правилами организованных торгов цифровыми финансовыми активами, зарегистрированными в Центральном банке Российской Федерации.

[1] Об организованных торгах: Федеральный закон от 21 ноября 2011 г. № 325-ФЗ. Доступ из прав.-правовой системы «КонсультантПлюс».

Все данные, связанные с оборотом цифровых активов, будут храниться в реестре цифровых транзакций, а любой участник, пользующийся данной электронной системой, сможет ознакомиться с ней через свой, постоянно обновляемый, распределенный реестр. Это поможет отслеживать течение криптовалюты в системе, а также ее переход от одного владельца к другому.

Предоставление прав и удовлетворение обязанностей по поводу цифровых финансовых активов определяются договором, устанавливающим переход валюты посредством цифровых транзакций и последующим фиксированием в реестре цифровых транзакций, вход к которому пользователю сети открывается при помощи цифрового кошелька, отражающего осуществление всех пользовательских финансовых операций.

Непосредственная угроза криптовалют, как платежных средств или же средств накопления, состоит в том, что при закупке или обмене как биткойнов, так и иных видов электронных валют, существует риск их кражи или утери держателями без возможности защиты своих прав в судебном или административном порядке, в силу отсутствия в законодательстве мер регулирования оборота валюты и защиты нарушенных интересов.

Отсутствием легализации биткойнов и иных криптовалют пользуются мошенники, которые рекламируют, так называемый, легкий способ обогатиться при помощи оборота биткойнов. Примером этого служит покупка биткойнов через иностранную валюту на предложенном мошенниками интернет-сайте, потом перепродавать их, а полученную прибыль забирать в рублях через онлайн-обменник криптовалюты. Заманивают обычно тем, что после исполнения данных операций на счет держателя придут деньги с учетом прибыли от разницы стоимости валют, однако, происходит так, что мошенник завладевает чужими деньгами.

Существует иной способ получения денег от пользования криптовалютой. Так, в Костромской области Российской Федерации впервые в судебной практике было возбуждено уголовное дело по ч. 2 ст. 172 Уголовного кодекса Российской Федерации[1] «Незаконная банковская деятельность». Как было сказано на официальном сайте газеты «Ведомости», сотрудники правоохранительных органов Костромской области и спецслужбы региона задержали трех человек,

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Доступ из прав.-правовой системы «КонсультантПлюс».

которые занимались незаконной банковской деятельностью, используя, в частности, одну из международных систем и площадки для обмена биткойнов.

По данным возбужденного уголовного дела, злоумышленники зарегистрировали более 300 банковских карт и *SIM*-карт на подставных лиц, с помощью которых наладили обмен и перевод криптовалюты. После они обналичили более 500 млн рублей. Подозреваемые были оставлены под подписку о невыезде, а дело было передано в суд на рассмотрение.

Все вышеописанные процедуры, в том числе легализация цифровых финансовых активов, как электронную валюту, объясняются невозможностью игнорирования технического и компьютерного прогресса на уровне государственной политики, и заданным курсом на устранение пробелов в праве, а также определения категорий «законное» и «незаконное» использование продуктов майнинга с целью извлечения выгоды, а равно, защита от мошеннических действий преступного характера. Актуальным в последующем считается отграничение преступлений и правонарушений в сфере получения, обмена, хранения и обналичивания цифровых финансовых активов, а также установление пределов юридической ответственности в зависимости от характера и степени общественной опасности деяния.

Вступивший в силу с 1 января 2021 г. Закон о цифровых финансовых активах и цифровой валюте[1] (далее — Закон № 259-ФЗ), хотя и содержит в своем названии оба этих понятия, и дает их определения, не сильно помог криптосообществу с точки зрения понимания сущности и условий использования криптовалют в нашей стране.

Абсолютное большинство норм Закона № 259-ФЗ посвящены цифровым финансовым активам (далее — ЦФА), под которыми понимаются цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг. Установлены правила выпуска, учета и обращения ЦФА, требования к операторам

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ. Доступ из прав.-правовой системы «КонсультантПлюс».

информационных систем, в которой выпускаются ЦФА, операторам обмена ЦФА, порядок деятельности таких операторов. Как отметил в ходе онлайн-конференции издательского дома «Коммерсантъ» председатель Комитета Госдумы по финансовому рынку Анатолий Аксаков, «принятие Закона № 259-ФЗ должно поспособствовать более активному использованию технологии блокчейн для выпуска ЦФА с целью привлечения инвестиций под реализацию различных проектов»[1].

Таким образом, можно прийти к выводу, что необходимо быстро и качественно обеспечить правовое регулирование принципиально новой платежной системы, с учетом ее особенностей применения, искоренить лазейки для преступного промысла получения денег и конфиденциальной информации пользователей.

Сейчас правительство рассматривает возможность использования цифровых валют во внешнеторговой деятельности.

31 мая 2022 г. первый зампред Центрального Банка Российской Федерации (далее — Центробанк России) Ксения Юдаева заявила, что Центробанк России не против криптовалютных расчетов в международных сделках и международной финансовой инфраструктуре[2].

За несколько дней до этого Министерство финансов Российской Федерации (далее — Минфин России) внес изменения в законопроект «О цифровой валюте», разрешающие использовать цифровые валюты для оплаты внешнеторговой деятельности.

Такая возможность активно обсуждалась российскими властями в последние месяцы. Так, в апреле Федеральная налоговая служба Российской Федерации (далее — ФНС России) предложила разрешить российским компаниям расчеты за экспортно-импортные операции в криптовалюте, а Торгово-промышленная палата Российской Федерации направила письмо председателю правительства с предложением вести расчеты со странами Африки в криптовалюте.

При этом еще в феврале 2022 года Центробанк России предлагал полностью запретить оборот криптовалют в России. Минфин России занял более мягкую позицию и выступил за интегрирование цифровых валют в экономику страны.

---

[1] URL: https://www.garant.ru/news/1448450/?ysclid=lgxp23c1vh973972938 (дата обращения: 31.05.2022).

[2] URL: https://tass.ru/ekonomika/14781541?ysclid=lgxpfqd4sh78507928&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 31.05.2022).

Сейчас в Государственной думе Российской Федерации на рассмотрении находится проект федерального закона «О цифровой валюте». Документ предусматривает создание комплексного регулирования криптовалютного рынка, включая порядок совершения операций с цифровыми валютами.

Причины повышенного внимания к международным расчетам в криптовалюте

Основная причина использования цифровых валют для внешнеторговых расчетов — это текущее отсутствие возможности расплачиваться по сделкам у крупнейших российских компаний и импортеров[1], по мнению партнера, руководителя практики *FinTech & Crypto* юридической фирмы *DRC* Михаила Быстрова. Он отметил, что все подобные сделки ранее проводились и обслуживались как раз теми банками, которые сейчас находятся под прямыми санкциями США и Европейского Союза (далее — ЕС, *прим. автора*), — ВТБ, Альфа-Банком, Сбером, Промсвязьбанком[2].

«Расчеты в криптовалюте в международных сделках могут спасти ситуацию и позволить российским компаниям, не попавшим под санкции, рассчитываться с контрагентами в криптовалюте», — согласился основатель компании *LFCS Legal Support* Юрий Брисов[3].

Причиной такой ранее немыслимой лояльности Центробанка России послужила геополитическая напряженность, санкции, фактически создавшие новую реальность, в которой бизнесу функционировать крайне сложно[4], подтверждает юрист юридической компании РКТ Елена Волчек. По ее словам, именно эта новая реальность стала импульсом к революции в системе расчетов и к переменам в последовательной позиции регулятора по отношению к криптовалюте[5].

«Ранее ЦБ крайне резко отрицал какую-либо возможность внедрения криптовалюты в экономическую систему России, ссылаясь на существенные риски и невозможность контроля. Минфин, в свою

[1] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

[2] Там же.

[3] Там же.

[4] URL: https://cryptocurrency.tech/chto-dumayut-eksperty-o-predlozhenii-vvedeniya-mezhdunarodnyh-raschetov-v-kriptovalyute-v-rf/?ysclid=lgxqrn7rg3719341757 (дата обращения: 01.06.2022).

[5] Там же.

очередь, напротив, исходил из невозможности закрыть глаза на цифровизацию рынка и предлагал более лояльные условия для функционирования криптовалюты в России»[1], — напомнила эксперт.

Волчек уточнила, что теперь регулятор и Минфин объединены общей целью и им предстоит найти формулу баланса между существующими рисками и необходимостью поддержки внешнеторговых отношений, в которой нуждаются все стороны, включая иностранных контрагентов[2].

«Поэтому инициатива представляется обнадеживающей, даже при невозможности предоставления абсолютной свободы в расчетах»,[3] — подчеркнула Е. Волчек.

Актуальность нововведений

Изменения будут актуальны для всех компаний, ведущих внешнюю экономическую деятельность,[4] уверен основатель компании *LFCS Legal Support* Ю. Брисов. Он считает, что сейчас жизнь российских предпринимателей на иностранном рынке очень затруднена[5].

По мнению партнера *DRC* М. Быстрова, основными интересантами таких нововведений в первую очередь станут крупные импортеры, поскольку российская экономика достаточно сильно зависит от импорта, а полноценное производство по программе «импортозамещения» предстоит налаживать еще «минимум пару десятилетий»[6].

«Несмотря на кажущийся позитив этой новости, я вижу глобальные проблемы с такими сделками. США и ЕС уже неоднократно публично заявляли, что Россия попытается использовать криптовалюты для обхода санкций, и в этом случае будут предприниматься жесткие меры»,[7] — говорит эксперт.

«Криптовалюта рассматривается, как один из инструментов обхода санкций, а любая криптоплощадка — как потенциальный

---

[1] Там же.

[2] Там же.

[3] Там же.

[4] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

[5] Там же.

[6] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

[7] Там же.

помощник России в их обходе, достаточно вспомнить недавний конфликт между регуляторами в США и компанией *BitRiver*»,[1] — привел пример М. Быстров.

В конце апреля 2022 года оператор дата-центра для майнинга *BitRiver* попал под санкции США. Министерство финансов США подчеркнуло, что компании, работающие в индустрии добычи криптовалют, помогают России монетизировать ее природные ресурсы, которые не могут быть экспортированы из-за санкций. В ответ в *BitRiver* пообещали подготовить и летом 2022 года подать иск к американскому Минфину.

М. Быстров указал, что ЕС планирует вводить уголовную ответственность уже на уровне себя самого за любую помощь России в обходе санкций.[2] «Это означает, что даже если какие-либо поставщики и бизнес в ЕС теоретически будут готовы принимать российскую криптовалюту за товары, работы, услуги, то они стопроцентно будут отказываться сотрудничать из-за угрозы уголовного преследования их самих»[3], — уверен юрист.

«Так что инициатива наших законотворцев может быть актуальна только для расчетов с очень ограниченным числом поставщиков из стран Латинской Америки, Африки и, возможно, Азиатско-Тихоокеанского региона, но явно не США и ЕС» [4], — заключил он.

Возможные проблемы

«Основной вопрос заключается в отсутствии легального рынка криптовалюты»[5], — уверен Ю. Брисов. По его словам: «доступ российских юрлиц на иностранные биржи закрыт, российских аналогов не существует»[6].

Эксперт допустил, что для покупки криптовалюты юрлицами будут возможны «костыльные» конструкции, вроде договоров поручения сотруднику компании получить деньги из кассы, открыть счет на бирже и купить криптовалюту. Однако остается непонятным, как ФНС России и иные проверяющие органы отнесутся к таким сделкам[7].

---

[1] URL: https://cryptocurrency.tech/chto-dumayut-eksperty-o-predlozhenii-vvedeniya-mezhdunarodnyh-raschetov-v-kriptovalyute-v-rf/?ysclid=lgxqrn7rg3719341757 (дата обращения: 01.06.2022).

[2] Там же.

[3] Там же.

[4] Там же.

[5] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

[6] Там же.

[7] Там же.

«Еще более сложная ситуация с получением валюты в качестве оплаты по международным сделкам. Сейчас это прямо запрещено статьей 14 закона «О ЦФА». Но даже если и этот закон подвергнется редакции, по-прежнему непонятно, как юридические лица должны менять криптовалюту на рубли» [1], — объяснил специалист.

По мнению партнера юридической группы *Guskov & Associates* Игоря Гуськова, главный вопрос состоит в том, признавать ли вообще в российском праве оплату криптовалютой. Уже на этапе концепции законодатель дал понять, что такая опция возможна только при выполнении двух условий:

– доступа государства к информации о держателях криптоактивов и всех совершаемых транзакциях;

– контроля государства и наличие властных полномочий по отношению к криптокошелькам[2].

«Прежде всего, речь о наложении ареста на активы и обращении на них взыскания, поскольку на сегодняшний день исполнимость таких судебных актов выглядит туманно. Особенно в случае с «холодными» кошельками» [3], — рассказал юрист.

«Законопроект «О цифровой валюте» обеспечивает оба критерия»[4], — считает И. Гуськов. Он поясняет, что все легальные криптоактивы будут храниться в электронных кошельках на информационной площадке, созданной регулятором и находящейся под администрированием банков[5].

«Однако в этом случае утрачиваются плюсы, которые привлекают большинство пользователей блокчейн-платформ. По сути, расчеты криптовалютой отождествляются с типичными безналичными денежными перечислениями, а значит с наличием аналогичных проблем (блокировки, запросы дополнительных документов и проч.)»[6], — признал эксперт.

«На внутреннем обороте криптовалют это нововведение не отразится»[7], — сказал М. Быстров. Он разъяснил, что «текущая версия законопроекта о регулировании оборота цифровых валют дословно

---

[1] Там же.

[2] URL: https://cryptocurrency.tech/chto-dumayut-eksperty-o-predlozhenii-vvedeniya-mezhdunarodnyh-raschetov-v-kriptovalyute-v-rf/?ysclid=lgxqrn7rg3719341757 (дата обращения: 01.06.2022).

[3] Там же.

[4] Там же.

[5] Там же.

[6] Там же.

[7] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

повторяет установленный статьи 14 259-ФЗ о ЦФА запрет на прием цифровой валюты за передаваемые товары, выполняемые работы, оказываемые услуги. Использование криптовалюты для расчетов по внешнеторговым операциям — всего лишь изъятие из этой запретительной нормы»[1].

Юрист указывает, что «обязательным условием в таких случаях является использование адреса-идентификатора, предоставленного оператором цифровой торговой платформы. Это означает, что перед любой внешнеторговой сделкой юридическое лицо или ИП будет обязано получить такой адрес-идентификатор у оператора цифровой торговой платформы (ОЦТП). Однако, есть нюанс — в полномочия ОЦПТ, согласно законопроекту, входит только организация торгов цифровыми валютами, но не обслуживание внешнеторговых сделок»[2].

«По этой причине, законодателям придется разъяснить и то, каким образом и посредством какой платформы российские ИП и юрлица должны будут проводить или регистрировать подобные сделки для целей контроля»[3], — уверен М. Быстров.

Законодательные перспективы

Существенным корректировками подвергнутся нормы, касающиеся криптобирж и криптообменников. Это один из самых сложных в регулировании вопросов, в котором переплетается масса противоречивых интересов[4], считает член комиссии по правовому обеспечению цифровой экономики Московского отделения Ассоциации юристов России Ефим Казанцев.

«В текущей редакции законопроект вряд ли будет принят. Думаю, впереди его ждет еще ни одна итерация»[5], — добавил Е. Казанцев.

«С учетом уже внесенных изменений текущая версия законопроекта будет далеко не последней, спрогнозировал партнер»[6], — руководитель практики *FinTech & Crypto* юридической фирмы *DRC*. По его прогнозам, более или менее согласованную между госорганами

[1] Там же.
[2] Там же.
[3] Там же.
[4] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv914 7172668 (дата обращения: 01.06.2022).
[5] Там же.
[6] Там же.

версию мы в лучшем случае увидим не ранее, чем осенью 2022 года[1].

«Следует рассмотреть целый комплекс мер, которые с учетом существующей реальности создадут для юридических лиц возможность покупать и продавать криптовалюту, не опасаясь негативных последствий»[2], — полагает Ю. Брисов.

Эксперт пояснил, что «поскольку нет четких разъяснений, приходится перестраховываться на каждом шагу и терпеть большие транзакционные издержки»[3].

«Рассчитывать на то, что криптовалюта может стать универсальным расчетным инструментом пока не приходится, поскольку помимо обеспечения такой возможности с российской стороны, необходимо учитывать ограничения стран контрагентов, а также ужесточение контроля для российских граждан на зарубежных криптоплатформах»[4], — предупредила юрист РКТ Е. Волчек. Она заключила, что «в любом случае российский бизнес должен подготовиться к возможным рискам, связанным с последующим доказыванием оплаты»[5].

4.2. Опыт создания и применения криптовалюты

Однако, как известно, методы познания бывают не только теоретические, но и эмпирические, т. е. основанные на опыте. В данном параграфе приводится личный опыт авторов монографии по созданию (майнингу) и применению криптовалюты[6].

На официальном сайте биткойна представлены четыре этапа использования этой криптовалюты: разобраться, выбрать кошелек, получить биткоины, потратить биткоины[7]. Собственно, с выбора кошелька мы и начнем наше эмпирическое исследование. Поскольку криптовалюты и биткойн являются частью цифрового информационного поля, то и средства их хранения относятся к программным или аппаратно-программным. К первым относятся программы для раз-

---

[1] URL: https://cryptocurrency.tech/chto-dumayut-eksperty-o-predlozhenii-vvedeniya-mezhdunarodnyh-raschetov-v-kriptovalyute-v-rf/?ysclid=lgxqrn7rg3719341757 (дата обращения: 01.06.2022).

[2] URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

[3] Там же.

[4] Там же.

[5] Там же.

[6] Локнов А. И., Примакин А. И., Хлебников А. М. Особенности и алгоритмы формирования и применения криптовалют // Региональная информатика и информационная безопасность: сб. трудов. – Санкт-Петербург: СПОИСУ, 2020. Вып. 8. – С. 151–154.

[7] Как использовать Биткойн // Новичку о Биткойне. Bitcoin Project 2009–2019. URL: https://bitcoin.org/ru/gettingstarted (дата обращения: 29.10.2019).

личных платформ на базе мобильных устройств (в первую очередь, под управлением операционных систем (далее — ОС) *Android* и *IOS*) и персональных компьютеров (*ОС MacOS, Windows, Unix*). Также к программным относятся кошельки, работающие через web-браузеры, как обычные интернет-страницы. Интерфейс работы с программным кошельком *Totalcoin* на базе *ОС Android* представлен ниже (рисунок 43).

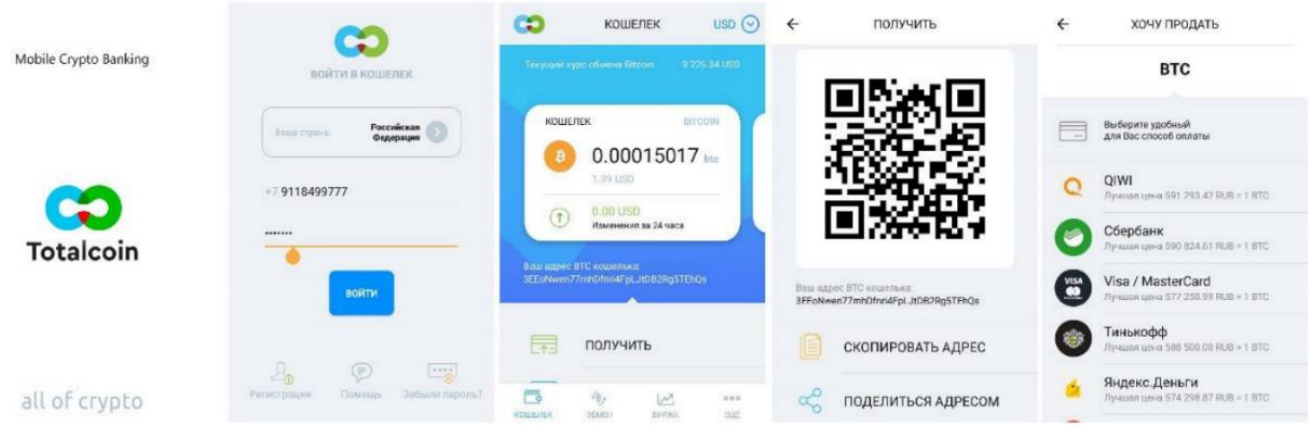

Рисунок 43 – Интерфейс работы с программным кошельком *Totalcoin* на базе *ОС Android*

Для покупки или продажи криптовалюты достаточно выбрать удобный способ оплаты по предлагаемому курсу. Стоит отметить, что, как и на любом рынке, стоимости покупки и продажи криптовалюты отличается. Разница между этими курсами на языке торговцев на финансовых биржах (трейдеров) называется спред. В случае с торговлей биткойнами через кошелек *Totalcoin* спред на момент исследования составлял от 3,89 % до 26,56 %. То есть купив на один условный рубль биткоины и тут же продав их можно было вернуть от 0,73 до 0,96 рубля (соответственно потеряв от 27 до 4 копеек). Самый выгодный курс обмена оказался у Сбербанка России (продажа по курсу 617 тыс. рублей за 1 биткойн, покупка — 590,8 тыс. рублей), а самый невыгодный — у американской платежной системы *PayPal* (726,7 и 575 тыс. рублей — соответственно). Простота обмена биткойна говорит о высокой ликвидности этого актива, в связи с чем, его популярность неуклонно растет.

Отдельного внимания заслуживает крайне изменчивый курс криптовалют. Его колебания могут достигать десятков процентов только в течение одних суток. Так, авторы этого текста покупали биткоины при курсе около 8 тыс. долларов США за 1 единицу, на следующий день курс упал до 7 400 долларов США (потери около 8 %), а еще через

день курс превысил 10 тыс. долларов США за 1 биткойн (рост более 25 % от цены покупки). Динамика курса биткойна в последней декаде октября 2019 года представлена на рисунке 44.

Рисунок 44 – Динамика курса биткойна
в последней декаде октября 2019 года

Вообще же за всю историю существования биткойна (с 5 октября 2009 г.) его курс менялся с 0,0008 до 20 тыс. долларов США за 1 биткойн, т. е. амплитуда колебаний составила около 2,5 млрд процентов! Известен случай, когда американец Ласло Ханич в мае 2010 года за 10 000 биткойнов купил 2 пиццы (стоимостью около 25 долларов США каждая). На сегодняшний день эта сумма в биткоинах эквивалентна 90 млн долларов США или почти 6 млрд рублей. Очевидно, что подобный финансовый инструмент относится к высоко рискованным активам и сегодня широко используется на финансовых рынках, в том числе как пример спекулятивного вложения финансов для извлечения сверхприбыли.

Кроме того, к рискам работы с криптовалютами стоит отнести вредоносные программы, т. к. большинство криптокошельков это не более чем компьютерные программы, в связи с чем, возможен их взлом и потеря имеющихся финансов. Указанного недостатка практически лишены аппаратные кошельки, являющиеся, по сути, физическими носителями информации и напоминающие обычные *USB*-флешки или *USB*-ключи — токены, использующиеся для идентификации владельца, как, например, при работе с порталом Госуслуги или сервисами ИСОД МВД России. Подобные аппаратные устройства

целесообразно использовать при работе со значительными суммами криптовалют, и они не столь широко применяются на практике, в том числе по причине относительно высокой стоимости (около 100 долларов США). Образец такого устройства, рекомендованного на официальном сайте биткойна, представлен на рисунке 45.

Рисунок 45 – Аппаратный криптокошелек
BitBox02

К проблемам криптовалют также относятся хакерские атаки, отсутствие законодательной базы и юридические риски, банкротство и закрытие бирж, отсутствие гарантий на возмещение убытков, потеря секретного кода и ошибочная транзакция пользователя[1].

Последние две проблемы стоит рассмотреть отдельно. Известно, что общее количество биткойнов искусственно ограничено его создателями. Предполагается, что общее количество «монет» составит 21 млн. Если разделить эту сумму на все население планеты (7,74 млрд. чел.[2]), то получится около 0,00 271 биткойна или 271 317 сатоши (в одном биткоине 100 млн. сатоши) на каждого жителя Земли. На сегодняшний день эта сумма эквивалентна 25 долл. США или 1500 руб. Очевидно, что заложив подобное ограничение общего количества биткойнов, создатели пытались создать аналогию с золотом, которого за всю историю человечества было добыто немногим больше 160 тыс. т[3]. Кроме искусственного ограничения количества биткойнов создатели предусмотрели необходимость «добычи» этого ресурса или так называемого «майнинга» (от англ. *mining* — добыча

[1] 10 проблем и рисков криптовалют // НПП «ГАРАНТ-СЕРВИС» [сайт], 05.12.2017. URL: https://www.garant.ru/article/1150927 (дата обращения: 01.11.2019).

[2] World Population Clock: 7.74 Billion People // Worldometers, 2019. URL: www.worldometers.info (дата обращения: 01.11.2019).

[3] Золото // Википедия, свободная энциклопедия. URL: https://ru.wikipedia.org/?oldid=102742182 (дата обращения: 01.11.2019).

полезных ископаемых). Здесь опять же усматривается аналогия с золотом, ценность которого обусловлена в том числе и сложностью добычи. Однако в отличии от добычи полезных ископаемых сложность майнинга биткойнов также создана искусственно. Смысл майнинга заключается в решении компьютером какой-то математической задачи, за решение которой происходит вознаграждение в виде пополнения счета. Сравнивая золото и биткойн можно отметить, что объемы добычи золота с ростом производительности труда имеют параболический тренд и фактически не ограничены, в отличие от биткойна, объем которого асимптотически приближается к отметке 21 млн. ед., что представлено на рисунке 46.

Рисунок 46 – Сравнение добычи биткойна и золота

Первые биткоины не требовали сложных вычислений и добывались на обычных компьютерах, однако, с ростом популярности этой криптовалюты и ее курса, желающих добывать биткоины становилась все выше. А поскольку количество ежедневно получаемых биткойнов строго ограничено и, более того, постоянно уменьшается, то алгоритм этой системы просто постоянно усложняет задачи и для достижения результата майнерны, конкурирующие между собой, используют все более мощные вычислительные ресурсы. Сейчас под такие вычислительные мощности выделяют целые помещения или даже здания, получившие название майнинг-ферм. Самые крупные из таких «ферм» занимают гектары земли и размещаются, как правило, в ангарах.

Также дефицит биткойнов создает утрата имен и паролей кошельков, в т. ч. в связи со смертью владельцев, которые никому не оставили информацию о доступе, что также постоянно поднимает стоимость этого актива. Однако стоит иметь в виду, что само количество

криптовалют ничем не ограничено. Тысячи энтузиастов, вдохновившись примером биткойна, пытаются создать свои криптовалюты, однако только немногим из них удается выйти на финансовые рынки и получить популярность, отличную от круга общения создателей. Вместе с тем уже сейчас на биржах торгуется несколько тысяч различных криптовалют. По данным сайта *Investing.com* на момент написания статьи торговалось 2 824 вида криптовалют с общей капитализацией более 250 млрд долларов США, из которых на долю биткойна приходится более 66 %. В десятку популярных криптовалют также входят Эфириум, Рипл, *Bitcoin Cash, Tether*, Лайткоин, *Binance Coin, EOS, Bitcoin SV, Stellar*[1].

Проблема ошибочной транзакции обусловлена тем, что платежи в системе биткойна безвозвратны, т. е. если ошибочно перевести деньги на какой-либо кошелек, то не предусмотрено обращение куда-либо с этой проблемой, так как в основе криптовалют лежит принцип блокчейна, т. е. децентрализации, когда вся информация не сосредоточена в каком-то одном месте, а распределена между всеми участниками и каждый пользователь, его вычислительные ресурсы, являются объектом хранения информации в системе. Какой-то головной организации или структуры нет. Здесь уместно провести аналогию с торрентом — протоколом обмена информацией между пользователями, когда доступ к информации предоставляется всеми пользователями, имеющими такую информацию, что многократно повышает скорость получения необходимой информации по сравнению с системами, где информация хранится централизованно. Принцип блокчейна повышает устойчивость всей системы к вмешательству, так как практически невозможно подменить информацию на неопределенном количестве вычислительных ресурсов всех пользователей, которые и являются хранилищем системы.

Вообще блокчейн получает все большее распространение и в России. Многие компании, в том числе такие, как Сбербанк, Ростелеком уже используют эту технологию. Не обошли вниманием этот принцип обменом информации и государственные структуры. Так, Росреестр в начале 2018 года одним из первых зарегистрировал договор долевого участия строительстве жилья в Ленинградской области. Также блокчейн уже используют Федеральная антимонопольная

[1] Все криптовалюты // Финансовые новости = Fusion Media Limited. URL: https://ru.investing.com/crypto/currencies (дата обращения: 01.11.2019).

служба Российской Федерации, ФНС России и др.[1].

Однако вернемся к биткоину и его практическому применению. Ведь позиционируется это инструмент, в первую очередь, как универсальное платежное средство. Так, что и где можно приобрести на биткоины? Поисковые интернет-системы предлагают воспользоваться сайтом coinmap.org, на котором наглядно можно найти необходимые торговые точки, принимающие электронную валюту. И вот тут владелец биткойнов в России сталкивается с реальной трудностью — даже в многомилионном Санкт-Петербурге едва ли наберется три десятка магазинов, которые готовы обменять свои товары и услуги на электронные записи в системе блокчейна.

Возможно такая ситуация связана с тем, что, согласно ст. 140 Гражданского кодекса Российской Федерации[2] (далее — ГК РФ), законным платежным средством, обязательным к приему по нарицательной стоимости на всей территории Российской Федерации, является только российский рубль.

Но почему же биткоин и другие криптовалюты неизменно связывают с криминальным миром? Существует даже мнение, что создатели подобных финансовых инструментов шли на поводу у преступников и создавали подобные системы в угоду преступному сообществу. Сторонники подобных теорий приводят в пример широкую популярность биткойна и других криптовалют при обороте запрещенных веществ и предметов. Однако авторы настоящей монографии не могут согласится с подобным высказыванием, так как следуя подобной логике, если преступные группы используют какую-либо другую валюту или даже, например, российский рубль в своих запрещенных законом операциях, то это не должно означать, что, например, ФРС США или Центробанк России являются преступными элементами, как эмитенты указанных платежных средств.

Одна из особенностей биткойна и многих других криптовалют — анонимность. Идентификация владельца происходит только по номеру электронного кошелька, который, как правило, не привязан к персональным данным владельца. В приведенном выше примере использования программы *Totalcoin* авторизация происходит по номеру телефона, однако, есть кошельки, в которых не используются

[1] Росреестр использовал технологию блокчейн // Ведомости (Vedomosti), 08.02.2018. URL: https://www.vedomosti.ru/economics/articles/2018/02/08/750276-rosreestr_blokchein (дата обращения: 02.11.2019).

[2] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Доступ из прав.-правовой системы «КонсультантПлюс».

эти данные, позволяющие идентифицировать пользователя, — все, что нужно знать для доступа к кошельку — это имя кошелька и пароль (ключ). Именно эта особенность биткойна и его ликвидность сделали этот инструмент чрезвычайно популярным в преступной среде, где анонимность чрезвычайно ценна.

Так, где же и как можно применить биткоины в незаконных целях? Известно, что согласно Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ[1] Роскомнадзор ограничивает на территории Российской Федерации доступ к сайтам, содержащим запрещенную информацию. Технически ограничение накладывает Интернет-провайдер на IP-адрес ресурса, доступ к которому должен быть ограничен. Однако, как известно, существуют интернет-технологии, позволяющие обойти блокировку от Роскомнадзора и Интернет-провайдеров. Использование подобного программного обеспечения позволяет получить доступ к даркнет (англ. *DarkNet*, также известна как «Скрытая сеть», «Тёмная сеть», «Теневая сеть», «Тёмный веб»), где механизм покупки и продажи абсолютно анонимен — все сделки происходят в биткоинах по текущему рублевому курсу. Как говорится, комментарии излишни.

Судя по всему, на сегодняшний день злоумышленники на шаг опережают государственные органы в области использования цифровых технологий для своих преступных целей. Ужасно, что даже ребенок несколькими кликами мышкой может попасть в нашей стране на нежелательный ресурс. Очевидно, что необходима реакция государства на подобные вызовы. С 1 ноября 2019 г. вступили в силу поправки в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»[2], предусматривающие создание национальной системы маршрутизации интернет-трафика, инструментов централизованного управления и др. Среди прочих мер закон предусматривает, что обмен трафиком на территории страны будет осуществляться только через специально одобренные и внесённые в соответствующий реестр точки обмена. Операторы, не исполняющие указания Роскомнадзора или правоохранительных органов, могут быть отключены от точек обмена.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из прав.-правовой системы «КонсультантПлюс».

[2] О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ. Доступ из прав.-правовой системы «КонсультантПлюс».

Об эффективности этих мер пока рано говорить. Хочется верить, что законодательные и исполнительные органы государственной власти смогут справиться с представленной выше проблемой.

4.3. Анализ преступлений, совершаемых в отношении или с использованием криптовалют

Тренды 2022 года: число криминальных транзакций достигло рекордного объема за всю историю и рекордного минимума по доле от общей криптовалютной активности.

В 2021 году криптовалютная преступность достигла нового исторического максимума: в течение года криминальные кошельки получат 14 млрд долларов США по сравнению с 7,8 млрд долларов США в 2020 году (рисунок 47).

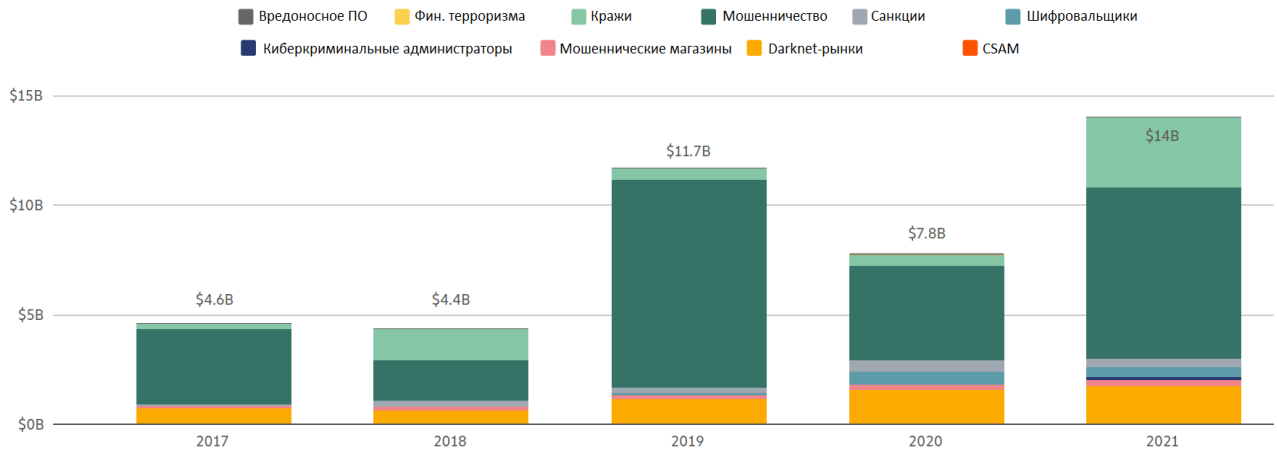

Рисунок 47 – Объем криптовалюты, полученной криминальными кошельками в период 2017–2021 гг.

«Киберкриминальный администратор» относится к кошелькам, которые были приписаны лицам, связанным с управлением киберкриминальной организацией, например, с торговой площадкой в *Darknet*.

Но эти цифры не раскрывают всей картины. Использование криптовалют растет быстрее, чем когда-либо прежде. По всем криптовалютам, отслеживаемым *Chainalysis*, общий объем транзакций в 2021 году вырастет до 15,8 трлн долларов США, что на 567 % больше, чем в 2020 году. Учитывая такой стремительный рост,

неудивительно, что все больше киберпреступников используют криптовалюты. Тот факт, что рост объема криминальных транзакций составил всего 79 % — почти на порядок меньше, чем общий рост рынка – может стать самым большим сюрпризом. На самом деле, поскольку рост легального использования криптовалют значительно опережает рост криминального использования, доля незаконной активности в общем объеме криптовалютных транзакций еще никогда не была такой низкой.

Транзакции с использованием криминальных счетов составили всего 0,15 % от объема криптовалютных транзакций в 2021 году, несмотря на то, что «чистый» объем криминальных транзакций достиг самого высокого уровня за всю историю (см. рисунок 48).

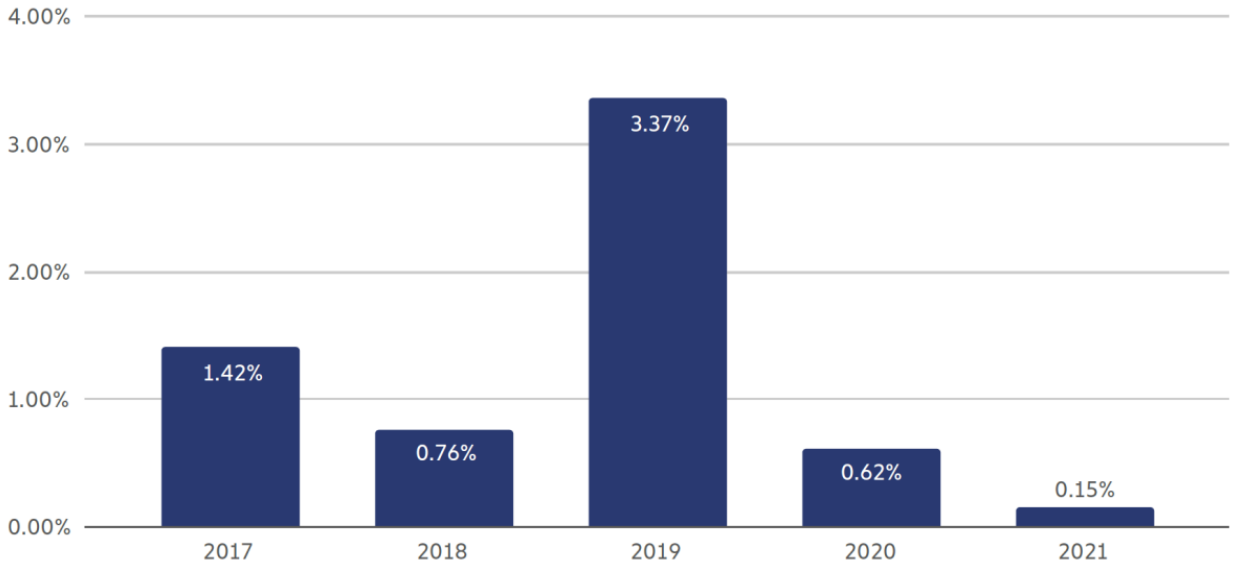

Рисунок 48 – Доля криминальной активности в объеме всех криптовалютных транзакций в период 2017–2021 гг.

Необходимо отметить, что эта цифра, скорее всего, будет расти по мере того, как *Chainalysis* будет выявлять все больше криптосчетов, связанных с криминальной деятельностью, и включать их транзакционную активность в нашу статистику. Ранее было обнаружено, что 0,34 % объема криптовалютных транзакций за 2020 год было связано с незаконной деятельностью – сейчас этот показатель вырос до 0,62 %. Тем не менее, ежегодные тенденции показывают, что за исключением 2019 года — экстремального года для криптовалютной преступности, в основном из-за схемы Понци *PlusToken* — преступность становится все меньшей частью криптовалютной экосистемы.

Возможности правоохранительных органов по борьбе с криптовалютными преступлениями также развиваются. В 2021 году мы видели несколько примеров этого: от предъявления *CFTC* обвинений нескольким инвестиционным мошенникам до уничтожения ФБР распространенного штамма шифровальщика *REvil* и введения *OFAC* санкций в отношении *Suex* и *Chatex* — двух российских криптовалютных сервисов, серьезно замешанных в отмывании средств.

Однако мы также должны сбалансировать положительные моменты роста легального использования криптовалют с пониманием того, что криминальная деятельность на сумму 14 млрд долларов США представляет собой серьезную проблему. Злоупотребление криптовалютами создает огромные препятствия для дальнейшего их развития, повышает вероятность введения ограничений со стороны правительств, и, что самое страшное, жертвами становятся невинные люди по всему миру. В этом отчете мы объясним, как и где именно выросла криптовалютная преступность, рассмотрим последние тенденции среди различных типов киберпреступников и расскажем, как криптовалютные компании и правоохранительные органы по всему миру реагируют на это. Но сначала давайте рассмотрим несколько основных тенденций в сфере криптовалютного криминала.

Рост *DeFi*-платформ предоставляет преступникам новые возможности.

Что изменилось за последний год? Для начала давайте посмотрим, какие виды преступлений больше всего выросли в 2021 году по объему транзакций (см. рисунок 49).

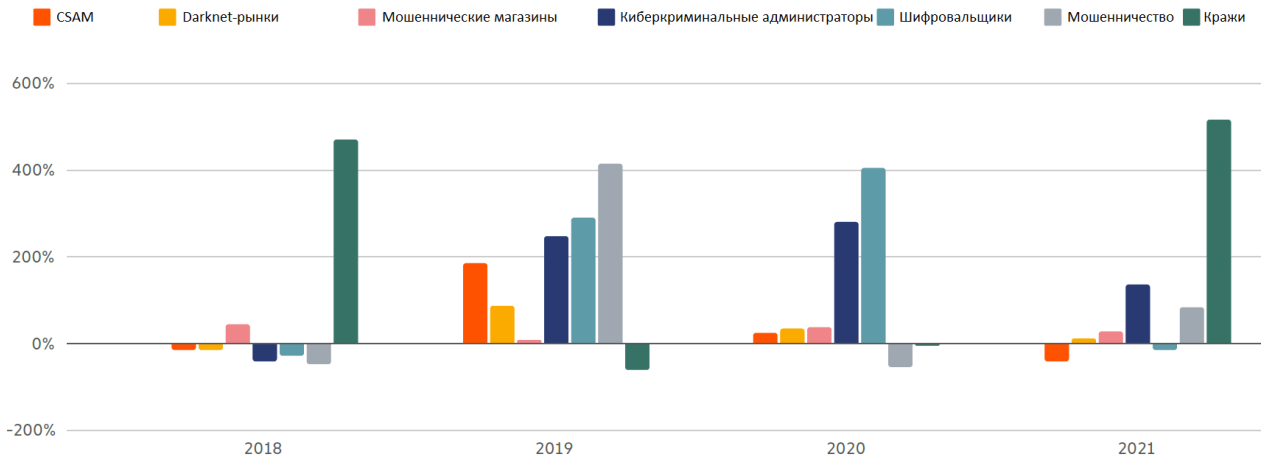

Рисунок 49 – Годовое процентное изменение полученных объемов криптовалют по видам преступлений в период 2018–2021 гг.

Две категории выделяются своим ростом: кражи и, в меньшей степени, мошенничество. В обеих категориях большую роль играют *DeFi*-платформы.

Начнем с мошенничества. В 2021 году доходы от мошенничества выросли на 82 % и составили 7,8 млрд долларов США в различных криптовалютах. Более 2,8 млрд долларов США из этой суммы — что почти равно росту по сравнению с 2020 годом — поступило от «ковровых афер» (*Rug Pull*), относительно нового вида мошенничества, в котором разработчики создают видимость легальных криптовалютных проектов — т.е. они делают нечто большее, чем просто создают кошельки для приема криптовалюты, скажем, для мошеннических инвестиционных операций – а затем забирают деньги инвесторов и исчезают. Следует также помнить, что приведенные цифры потерь от ковровых афер отражают только объем похищенных средств инвесторов, а не потери от последующей потери стоимости *DeFi*-токенов.

Следует отметить, что примерно 90 % от общей суммы, потерянной в результате ковровых афер в 2021 году, можно отнести на счет одной мошеннической централизованной биржи *Thodex*, генеральный директор которой исчез вскоре после того, как биржа приостановила возможность пользователей выводить средства. Однако все остальные мошеннические действия, отслеженные *Chainalysis* в 2021 году, были связаны с проектами *DeFi*. Почти во всех этих случаях разработчики обманом заставляли инвесторов покупать токены, связанные с проектом *DeFi*, а затем выводили предоставленные инвесторами средства, в результате чего стоимость токена падала до нуля.

Мы считаем, что мошенничества в *DeFi* распространены по двум причинам: Первая — ажиотаж вокруг этого пространства. Объем транзакций *DeFi* вырос на 912 % в 2021 году, а невероятная доходность децентрализованных токенов — таких как *Shiba Inu* — вызывает у многих желание спекулировать токенами. В то же время тем, кто обладает необходимыми техническими навыками, очень легко создать новые токены *DeFi* и зарегистрировать их на биржах, даже без аудита кода. Аудит кода — это процесс, в ходе которого сторонняя компания или биржа анализирует код смарт-контракта, лежащего в основе нового токена или другого проекта *DeFi*, и публично подтверждает, что правила управления контрактом железные и не содержат механизмов, которые позволили бы разработчикам нажиться на средствах инвесторов. Многие инвесторы, вероятно, могли бы избежать потери средств если бы они придерживались проектов *DeFi*, прошедших аудит кода — или если бы платформы требовали аудита

кода перед листингом токенов.

Кражи криптовалют выросли еще больше: в 2021 году было украдено криптовалют на сумму около 3,2 млрд долларов США, что на 516 % больше, чем в 2020 году. Примерно 2,2 млрд долларов США из этих средств — 72 % от общего объема 2021 года — были украдены с помощью платформ *DeFi*. Рост числа краж, связанных с *DeFi*-платформами, представляет собой ускорение тенденции, которую мы выявили в прошлогоднем отчете по криптопреступности.

В 2020 году с платформ *DeFi* было похищено криптовалют на сумму чуть менее 162 млн долларов США, что составило 31 % от общей суммы краж за год и на 335 % больше, чем в 2019 году. В 2021 году эта цифра выросла еще на 1 330 %. Другими словами — по мере того, как платформы *DeFi* продолжают расширяться, растет и проблема краж. Как мы подробнее рассмотрим далее в отчете, большинство случаев кражи средств из платформ *DeFi* можно отследить по ошибкам в коде смарт-контрактов, управляющих этими платформами, которые хакеры используют подобно уязвимостям, позволяющим совершать ковровые аферы (см. рисунок 50).

Мы также наблюдаем значительный рост использования *DeFi* для отмывания криминальных средств — практика, разрозненные примеры которой мы видели в 2020 году, и которая стала более распространенной в 2021 году. На графике ниже показан рост криминальных средств, полученных различными типами сервисов в 2021 году по сравнению с 2020 годом (см. рисунок 51).

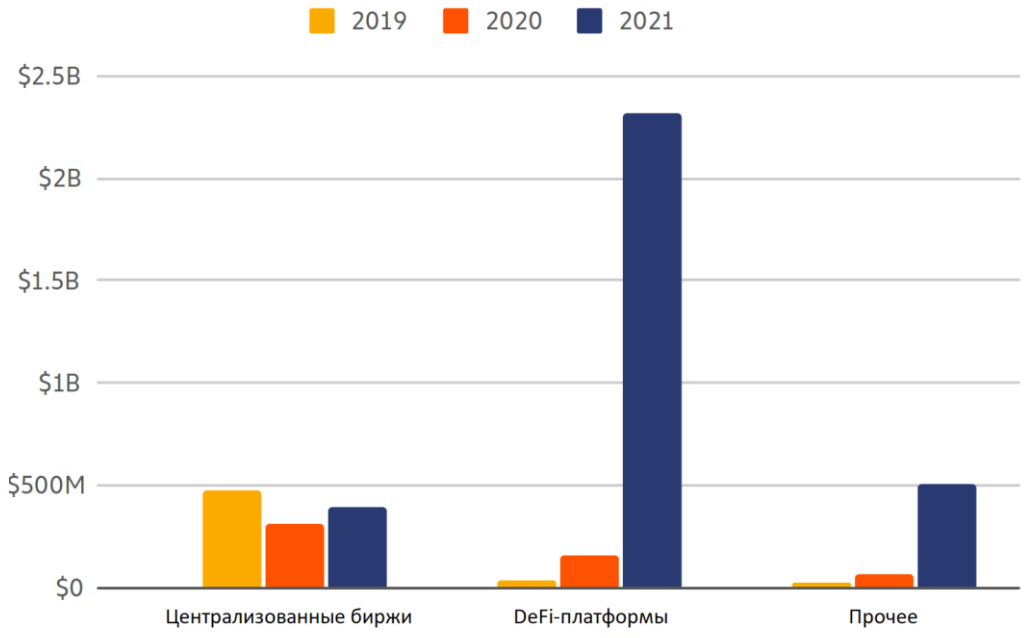

Рисунок 50 – Ежегодный общий объем похищенной криптовалюты по типам жертв в период с января 2019 по декабрь 2021 гг.

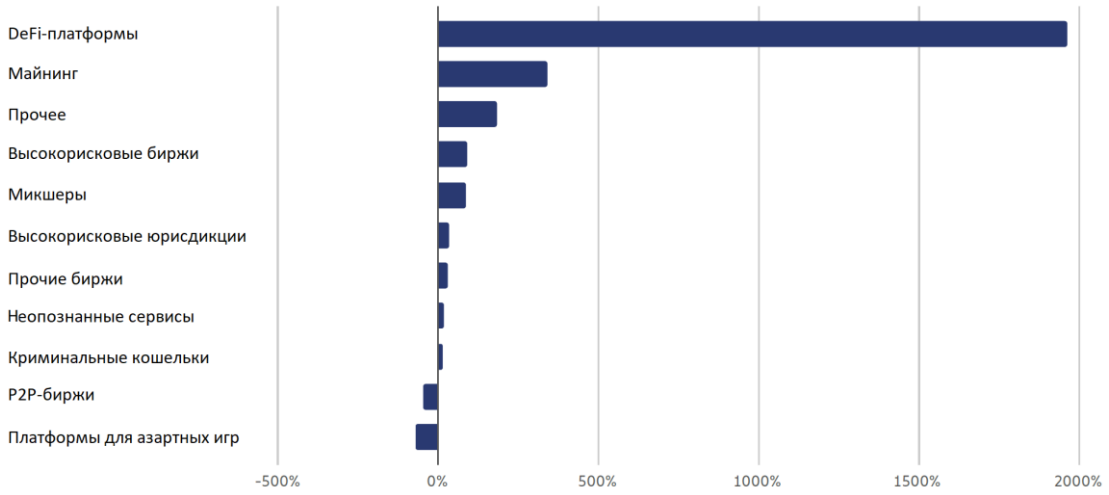

Рисунок 51 – Годовой процентный рост стоимости, полученной сервисом от криминальных счетов в период 2020–2021 гг.

DeFi-платформы показали наибольший рост использования для отмывания средств — 1 964 %.

DeFi — одна из самых интересных областей широкой криптовалютной экосистемы, открывающая огромные возможности как для предпринимателей, так и для пользователей криптовалют. Однако *DeFi* вряд ли сможет полностью реализовать свой потенциал, если децентрализация, которая делает ее такой динамичной, также позволит широко распространиться мошенничеству и воровству. Одним из способов борьбы с этим является улучшение коммуникаций — как частный, так и государственный сектор должны сыграть важную роль в том, чтобы помочь инвесторам узнать, как избежать сомнительных проектов. В долгосрочной перспективе отрасли, возможно, придется принять более решительные меры, чтобы не допустить размещения на крупных биржах токенов, связанных с потенциально мошенническими или небезопасными проектами.

Объемы криминальных криптовалют растут. Что могут сделать правоохранительные органы?

Одним из перспективных направлений в борьбе с криптовалютной преступностью является растущая способность правоохранительных органов изымать незаконно полученную криптовалюту. Например, в ноябре 2021 года отдел уголовных расследований *IRS* объявил, что в 2021 году изъял криптовалют на сумму более 3,5 млрд долларов США – все в рамках неналоговых расследований, — что составляет 93 % от всех средств, изъятых отделом за этот период времени. Мы также видели несколько примеров успешного изъятия

средств другими ведомствами, включая 56 млн долларов США, изъятых Министерством юстиции США в ходе расследования криптовалютного мошенничества, 2,3 млн долларов США, изъятых у группы разработчиков шифровальщиков, стоявшей за атакой *Colonial Pipeline*, и нераскрытую сумму, изъятую Национальным бюро по борьбе с финансированием терроризма Израиля в ходе дела, связанного с финансированием терроризма.

В связи с этим возникает интересный вопрос: Сколько криптовалюты в настоящее время находится у преступников? Невозможно знать наверняка, но мы можем оценить это на основе текущих балансов криптосчетов, которые *Chainalysis* определяет как связанные с криминальной деятельностью. По данным на начало 2022 года, на криминальных кошельках хранятся криптовалюты на сумму не менее 10 млрд долларов США, причем подавляющее большинство этой суммы находится на кошельках, связанных с кражей криптовалют. Кошельки, связанные с *Darknet*-рынками и мошенничеством, также вносят значительный вклад в эту сумму. Как мы рассмотрим далее в этом отчете, большая часть этой криптовалюты получена не непосредственно в результате преступной деятельности, а от последующего роста цен на хранящиеся криптоактивы.

Мы считаем, что правоохранительным органам важно понимать эти оценки, поскольку они развивают свои следственные возможности в блокчейне, и особенно по мере развития своих возможностей по изъятию незаконной криптовалюты.

Преступления, связанные с *DeFi*, и криминальные запасы криптовалют – это лишь одни из областей, которым посвящен наш отчет. Мы также рассмотрим последние данные и тенденции в отношении других форм преступлений, связанных с криптовалютой, в том числе:

– постоянное развитие угроз шифровальщиков;

– отмывание средств с помощью криптовалют;

– роль национальных государственных субъектов в криптовалютной преступности;

– криминальная деятельность в *NFT*.

Поскольку криптовалюты продолжают расти, крайне важно, чтобы государственный и частный секторы работали вместе, чтобы пользователи могли безопасно совершать сделки, а преступники не могли злоупотреблять этими новыми активами. Мы надеемся, что данный отчет будет способствовать достижению этой цели

и предоставит правоохранительным органам, регуляторам и специалистам по соблюдению нормативно-правового соответствия знания для более эффективного предотвращения, смягчения последствий и расследования преступлений на основе криптовалют.

Отмывание криминальных средств.

Платформы *DeFi* играют все более серьезную роль в отмывании средств, но небольшая группа централизованных сервисов все еще доминирует.

Киберпреступники, работающие с криптовалютой, преследуют одну общую цель: перевести свои незаконно нажитые средства в сервис, где они будут надежно защищены от властей и в конечном итоге конвертированы в наличные. Именно поэтому отмывание средств — фундамент всех других форм криптовалютных преступлений. Если нет возможности получить доступ к средствам, то нет и стимула совершать преступления с использованием криптовалют.

Деятельность по отмыванию в криптовалютах также сильно сконцентрирована. Хотя ежегодно с криминальных счетов перемещаются миллиарды долларов, большая часть оказывается в удивительно небольшой группе сервисов, многие из которых, судя по истории транзакций, специально созданы для отмывания средств. Правоохранительные органы могут нанести серьезнейший удар по криптовалютной преступности и существенно ограничить возможности преступников по доступу к своим цифровым активам, прервав работу этих сервисов. Мы наблюдали пример в прошлом году, когда Управление по контролю за иностранными активами Министерства финансов США (*OFAC*) наложило санкции на два самых опасных сервиса по отмыванию средств — *Suex* и *Chatex* — за прием средств от операторов шифровальщиков, мошенников и других киберпреступников. Однако, как мы рассмотрим ниже, многие другие сервисы по отмыванию остаются активными.

Криптовалютная деятельность по отмыванию средств в кратком изложении

В целом, если судить по количеству криптовалюты, отправленной с криминальных счетов на различные сервисы, в 2021 году киберпреступники отмыли криптовалют на сумму 8,6 млрд долларов США (см. рисунок 52).

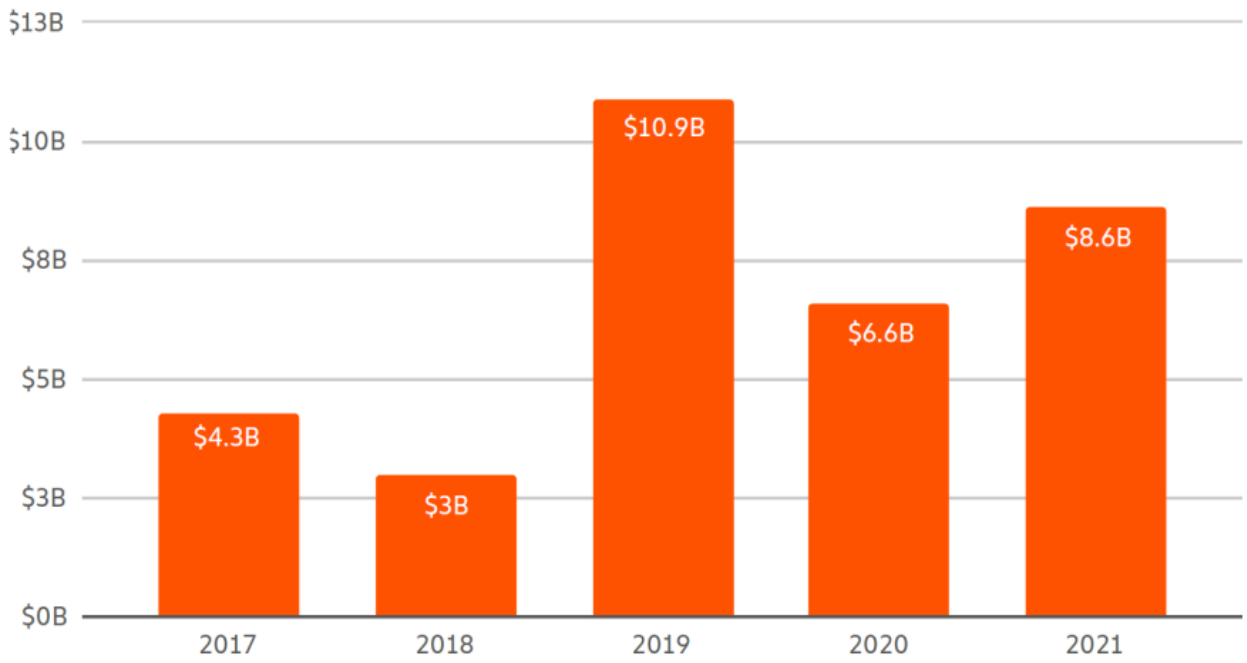

Рисунок 52 – Общий объем отмытых криптовалют
по годам в период 2017–2021 гг.

Это рост на 30 % по сравнению с 2020 годом, что неудивительно, учитывая значительную активизацию как законной, так и незаконной криптовалютной деятельности в 2021 году. Следует также отметить, что эти цифры учитывают только средства, полученные от «криптовалютно-нативных[1]» преступлений, то есть киберпреступной деятельности, такой как торговля на *Darknet*-рынках или атаки с использованием шифровальщиков, в которых прибыль практически всегда получается в криптовалюте, а не в фиатной (наличной) валюте. Сложнее измерить, сколько фиатной валюты, полученной от офлайн-преступлений — например, традиционного наркотрафика — конвертируется в криптовалюту для отмывания. Тем не менее, мы знаем, что это происходит, и далее в этом разделе приводим пример из практики.

В целом, с 2017 года киберпреступники отмыли криптовалюты на сумму более 33 млрд долларов США, при этом большая часть общего объема со временем переместилась на централизованные биржи. Для сравнения, по оценкам Управления ООН по наркотикам и преступности, ежегодно отмывается от 800 млрд долларов США до 2 трлн фиатной валюты — это около 5 % мирового ВВП. Для сравнения, в 2021 году

[1] Нативные монеты — это родные криптовалюты блокчейнов, а токены создаются с помощью смарт-контрактов поверх существующего блокчейна. У нативной монеты блокчейна и нового токена этого блок-чейна может быть один адрес (прим. автора).

на отмывание пришлось всего 0,05 % от всего объема криптовалютных транзакций. Мы приводим эти цифры не для того, чтобы преуменьшить проблемы криптовалют, связанные с преступностью, а скорее для того, чтобы указать на то, что отмывание средств — это чума практически для всех форм экономической деятельности, а также для того, чтобы помочь специалистам правоохранительных органов и комплаенс-служб осознать, какой объем деятельности по отмыванию средств теоретически может переместиться в криптовалюты по мере распространения этой технологии.

Самая большая разница между отмыванием фиатных и криптовалютных средств заключается в том, что благодаря присущей блокчейн прозрачности мы можем легче отследить, как преступники перемещают криптовалюты между кошельками и сервисами, пытаясь превратить свои средства в наличные (см. рисунок 53). На какие криптовалютные сервисы опираются преступники?

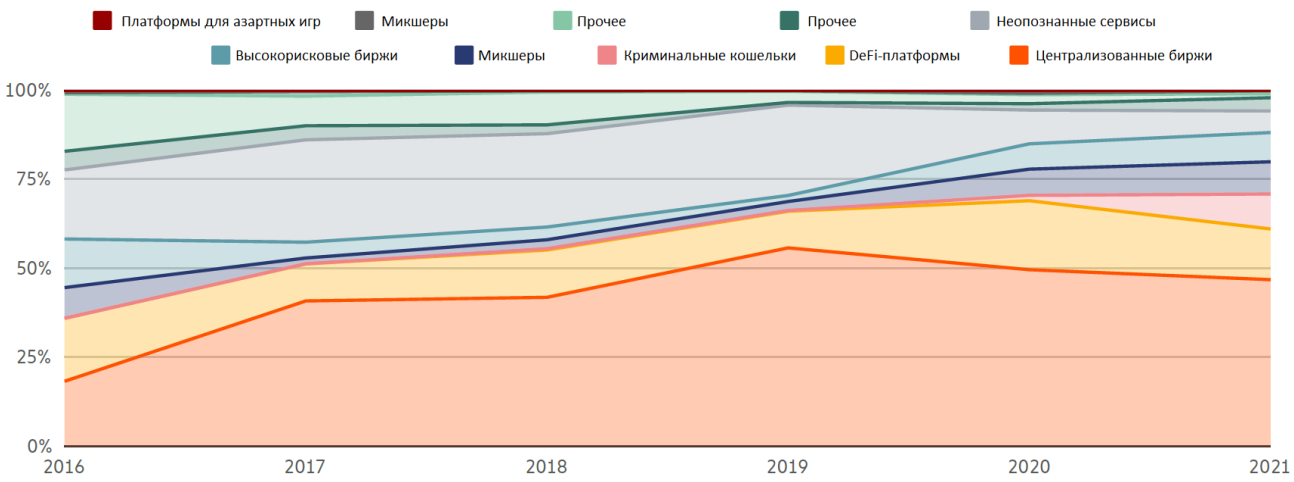

Рисунок 53 – Назначение средств, уходящих с криминальных криптосчетов в период 2016–2021 гг.

Впервые с 2018 года централизованные биржи не получили большую часть средств, отправленных с криптосчетов преступников в прошлом году, приняв лишь 47 %. Куда киберпреступники отправляли средства вместо этого? Большую часть разницы составили платформы *DeFi*. *DeFi* получили 17 % всех средств, отправленных с криминальных счетов в 2021 году, по сравнению с 2 % в предыдущем году (рисунок 54).

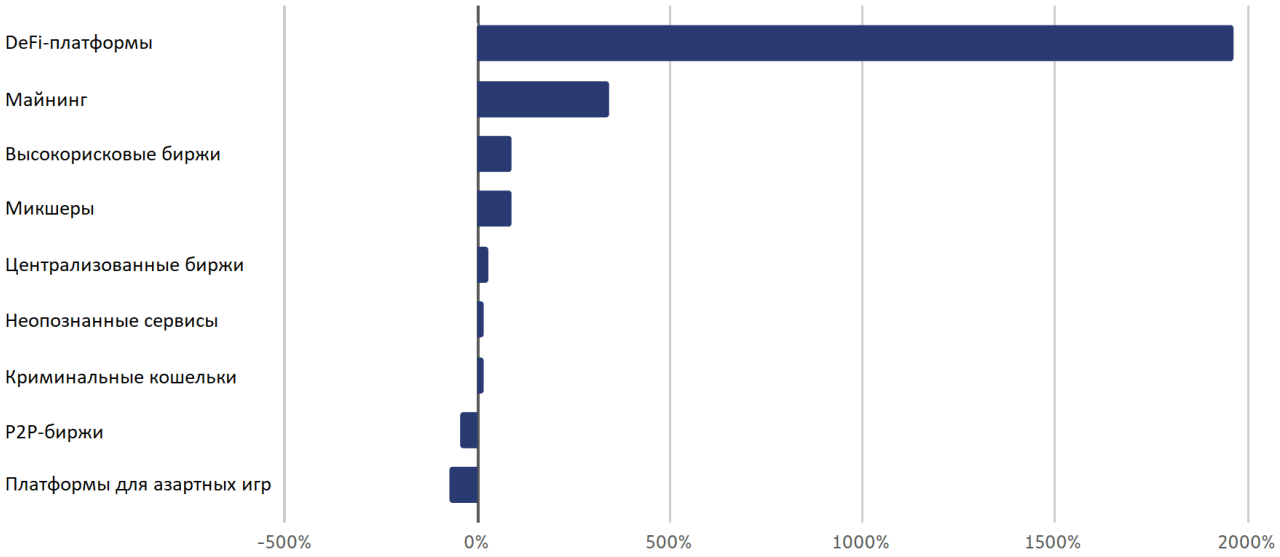

Рисунок 54 – Годовой процентный рост объема криптовалюты, полученной с криминальных счетов, по категориям сервисов в период 2020–2021 гг.

Это означает рост общих сумм, полученных платформами *DeFi* с криминальных счетов, на 1 964 % по сравнению с предыдущим годом, и в 2021 году они достигают 900 млн долларов США. Майнинговые пулы, высоко рисковые биржи и микшеры также продемонстрировали значительный рост криминальных поступлений.

Мы также видим закономерности в том, какие виды сервисов используют различные типы киберпреступников для отмывания криптовалют (см. рисунок 55).

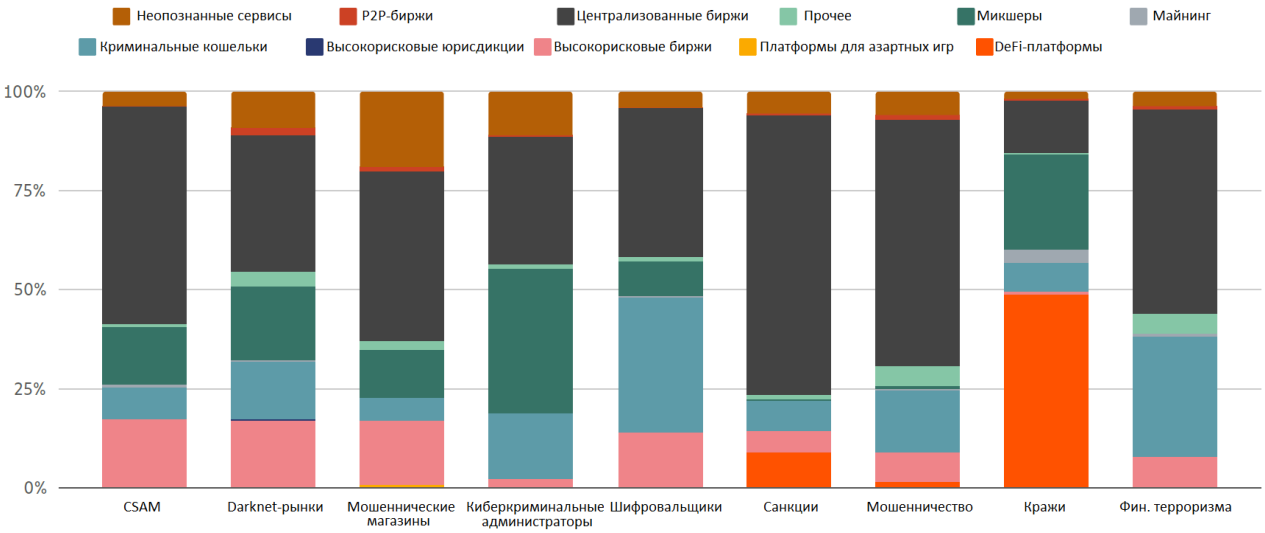

Рисунок 55 – Назначение средств, уходящих с криминальных счетов, по видам преступлений в 2021 году

Бросается в глаза разница в стратегиях отмывания средств между двумя наиболее прибыльными видами преступлений в 2021 году: кражами и мошенничеством. Счета, связанные с кражей, отправили чуть меньше половины украденных средств на платформы *DeFi* — всего криптовалюты на сумму более 750 млн долларов США. Связанные с Северной Кореей хакеры, ответственные за взломы криптовалютных активов на сумму 400 млн долларов США, довольно часто использовали платформы *DeFi* для отмывания средств. Это может быть связано с тем, что с *DeFi* было украдено больше криптовалюты, чем с любого другого типа сервисов. Мы также видим значительное использование микшеров для отмывания краденых средств.

С другой стороны, мошенники отправляют большую часть своих средств на централизованные биржи. Это может отражать относительную неискушенность мошенников. Для взлома криптовалютных платформ с целью кражи средств, требуется больше технических знаний, чем для осуществления большинства наблюдаемых нами афер, поэтому логично, что продвинутые киберпреступники будут использовать более совершенную стратегию отмывания.

Необходимо также подчеркнуть, что мы не можем отследить всю деятельность по отмыванию средств, измеряя суммы транзакций, отправленных с известных преступных счетов. Как было сказано выше, некоторые преступники используют криптовалюту для отмывания средств, полученных в результате преступлений, совершенных вне сети, и существует множество активных криминальных счетов, которые еще предстоит идентифицировать. Однако мы можем объяснить некоторые из более скрытых случаев отмывания путем поиска моделей транзакций, позволяющих предположить, что пользователи пытались избежать выявления правилами мониторинга. Например, в связи с такими нормативными актами, как *Travel Rule*, криптовалютные компании во многих странах должны проводить дополнительные проверки на соответствие требованиям, предоставлять отчетность и обмениваться информацией о транзакциях стоимостью свыше 1 000 долларов США. Как и следовало ожидать, криминальные криптокошельки отправляют непропорционально большое количество переводов на биржи, находящиеся чуть ниже этого порога. (см. рисунок 56).

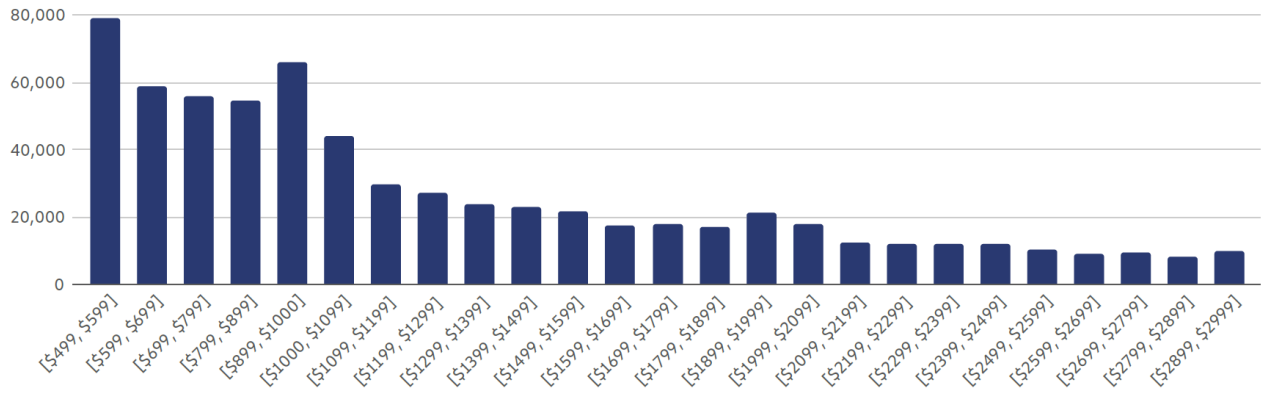

Рисунок 56 – Количество переводов с криминальных счетов на биржи в зависимости от размера перевода в 2021 году

Биржи, использующие *Chainalysis*, смогут увидеть, что средства поступают с криминальных счетов, независимо от размера перевода. Но в более общем плане командам по соблюдению нормативно-правового соответствия следует рассмотреть возможность более тщательного подхода к пользователям, которые постоянно отправляют или получают транзакции такого размера. Повторяющиеся транзакции чуть ниже порога могут указывать на то, что пользователи занимаются так называемым «*структурированием*», то есть намеренно разбивают крупные платежи на более мелкие, не превышающие порог мониторинга, чтобы обмануть комплаенс-команды.

Деятельность по отмыванию средств все еще остается высоко-концентрированной, но в меньшей степени, чем в 2020 году.

Как мы уже сообщали ранее, деятельность по отмыванию криминальных средств в значительной степени сосредоточена всего в нескольких сервисах. Ниже мы можем увидеть, как эта концентрация менялась с течением времени (рисунок 57).

При меньшем количестве сервисов, используемых в 2021 году, концентрация отмывания средств первоначально, по-видимому, немного увеличилась. 58 % всех средств, отправленных с криминальных счетов, в прошлом году перешли на пять сервисов, по сравнению с 54 % в 2020 году.

Однако деятельность по отмыванию лучше рассматривать на уровне счетов, а не на уровне сервисов. Причина этого заключается в том, что многие сервисы по отмыванию, используемые киберпреступниками, являются «вложенными» сервисами — т. е. используют счета, размещенные на более крупных сервисах — чтобы использовать ликвидность и торговые пары этих крупных сервисов.

Внебиржевые брокеры, например, часто функционируют как вложенные сервисы, счета которых размещаются на крупных биржах. На графике ниже (рисунок 58) мы рассматриваем все счета депозитов, которые получили какие-либо криминальные средства в 2021 году, в разбивке по диапазону полученных криминальных средств.

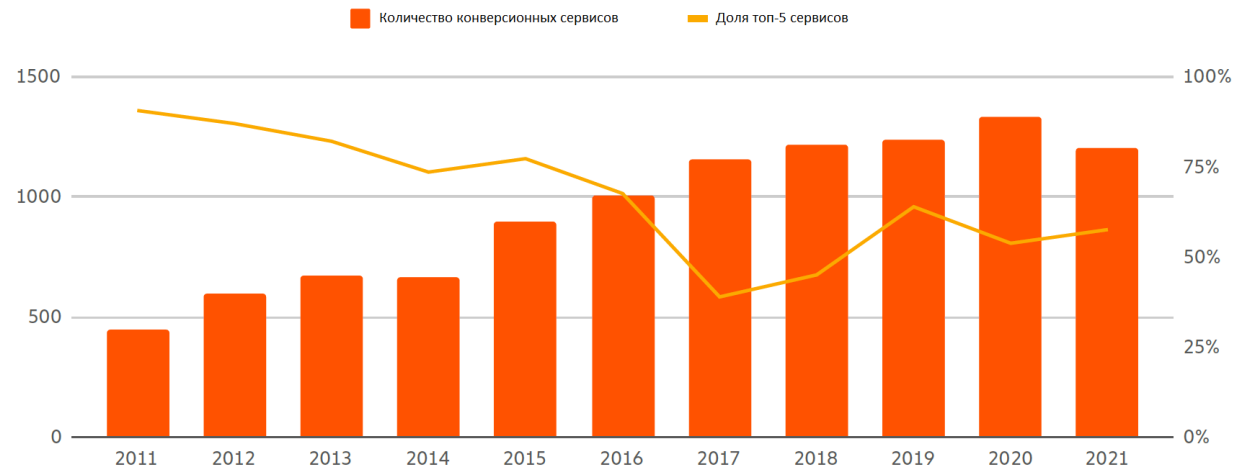

Рисунок 57 – Доля криминальной криптовалюты, поступающей в пять крупнейших сервисов, и общее количество уникальных сервисов, получающих криминальную криптовалюту в период 2011–2021 гг.

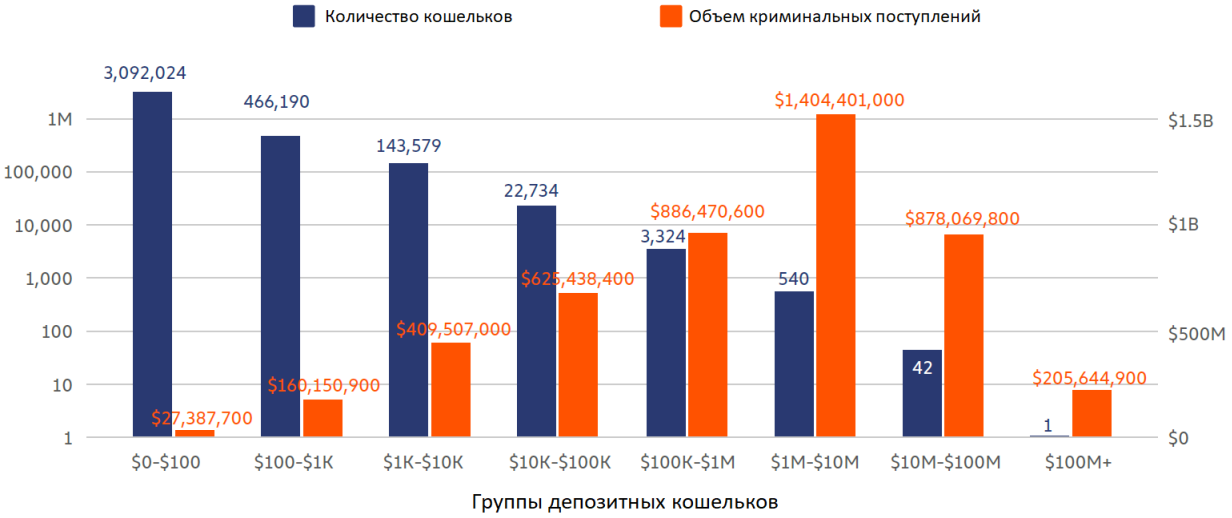

Рисунок 58 – Объемы криминальной криптовалюты, полученные счетами депозитов (по общему объему поступлений в 2021 году)

На этом графике показаны счета сервисных депозитов, разбитые по количеству криминальной криптовалюты, полученной каждым счетом по отдельности в 2021 году (см. рисунок 58). Каждая синяя полоса представляет собой количество депозитных счетов в группе,

а каждая оранжевая полоса — общую стоимость криминальной криптовалюты, полученной всеми депозитными счетами в группе. На примере первой группы мы видим, что 3 092 024 депозитных счета получили от 0 до 100 долларов США криминальной криптовалюты, а все вместе эти депозитные счета получили в общей сложности 27,4 млн долларов США.

Группа из всего 583 депозитных счетов получила 54 % всех средств, отправленных с криминальных счетов в 2021 году. Каждый из этих 583 счетов получил от криминальных счетов не менее 1 млн долларов США, а всего они получили криптовалюты на сумму чуть менее 2,5 млрд долларов США. Еще меньшая группа из 45 счетов получила 24 % всех средств, отправленных с криминальных счетов, на общую сумму чуть менее 1,1 млрд долларов США. Один депозитный счет получил чуть более 200 млн долларов США, и все это с криптосчетов, связанных с аферой *Finiko*.

Хотя деятельность по отмыванию остается достаточно концентрированной, она менее активна, чем в 2020 году. В том году 55 % всей криптовалюты, отправленной с криминальных счетов, поступило всего на 270 счетов сервисных депозитов. Одной из возможных причин снижения концентрации деятельности по отмыванию могут быть действия правоохранительных органов. Как мы уже упоминали выше, в прошлом году *OFAC* наложило санкции на *Suex*, российского внебиржевого брокера, который получил криптовалюты на десятки миллионов долларов со счетов, связанных с программами-шифровальщиками, мошенничеством и другими формами киберпреступной деятельности. Вскоре после этого *OFAC* также ввела санкции против *Chatex*, *P2P*-биржи, основанной тем же человеком, что и *Suex*, с аналогичным профилем клиентов. Хотя в то время мы не могли сообщить их имена, счета, связанные с обоими сервисами, появились в списке 270 счетов, которые мы определили как крупнейших отмывателей в прошлогоднем отчете.

Возможно, что некоторые сервисы отмывания прекратили свою деятельность после того, как увидели эти и другие действия, предпринятые против криминальных платформ, что заставило киберпреступников перераспределить свою активность по отмыванию средств в пользу других операторов. Возможно также, что сервисы отмывания продолжали работать, но распределяли свою деятельность по большему количеству депозитов, что способствовало бы уменьшению концентрации, которую мы видим выше.

Мы также видим различные уровни концентрации в отмывании в зависимости от актива (см. рисунок 59).

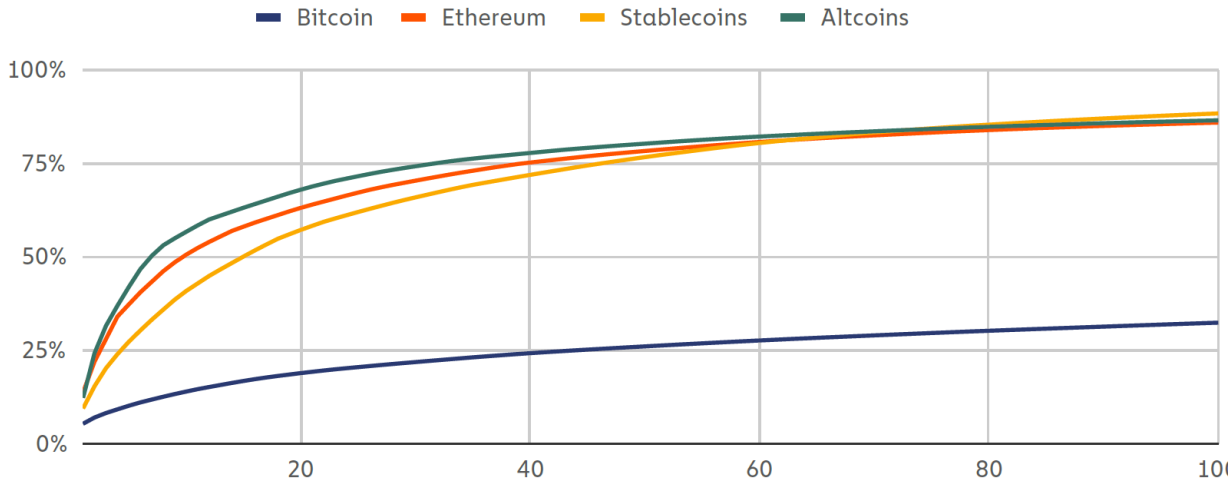

Рисунок 59 – Концентрация отмывания средств:
доля общей криминальной криптовалюты,

полученной ведущими депозитными счетами, по активам 2021 года

Деятельность *Bitcoin* по отмыванию средств является наименее концентрированной. 20 крупнейших депозитных счетов, занимающихся отмыванием средств, получают всего 19 % от всех *Bitcoin*, отправленных с криминальных криптосчетов, по сравнению с 57 % для *stablecoin*, 63 % для *Ethereum* и 68 % для *altcoin*.

Мы также видим различия в уровне концентрации отмывания средств для разных типов киберпреступников. На диаграмме ниже разбиты по категориям преступности все счета, получившие в 2021 году более 1 млн долларов США в криминальной криптовалюте, и доля всех средств, отправленных из этих категорий преступников, приходящаяся на эти счета.

Больше всего бросается в глаза то, насколько меньше концентрация деятельности по отмыванию у мошенников и продавцов и администраторов торговых площадок в *Darknet* по сравнению с другими категориями преступников. Это может отражать тот факт, что преступная деятельность этих категорий сама по себе менее концентрирована. В продажах и мошенничестве на *Darknet*-рынках участвует гораздо больше киберпреступников разного уровня продвинутости, поэтому логично, что средства этих киберпреступников распределены по большему количеству депозитных счетов для отмывания — каждый игрок может следовать своей собственной стратегии. Что касается более сложных форм киберпреступности, таких как шифровальщики,

то на администраторов крупнейших штаммов шифровальщиков приходится большая доля всей активности, поэтому можно ожидать, что и отмывание средств будет более концентрированным (рисунок 60).

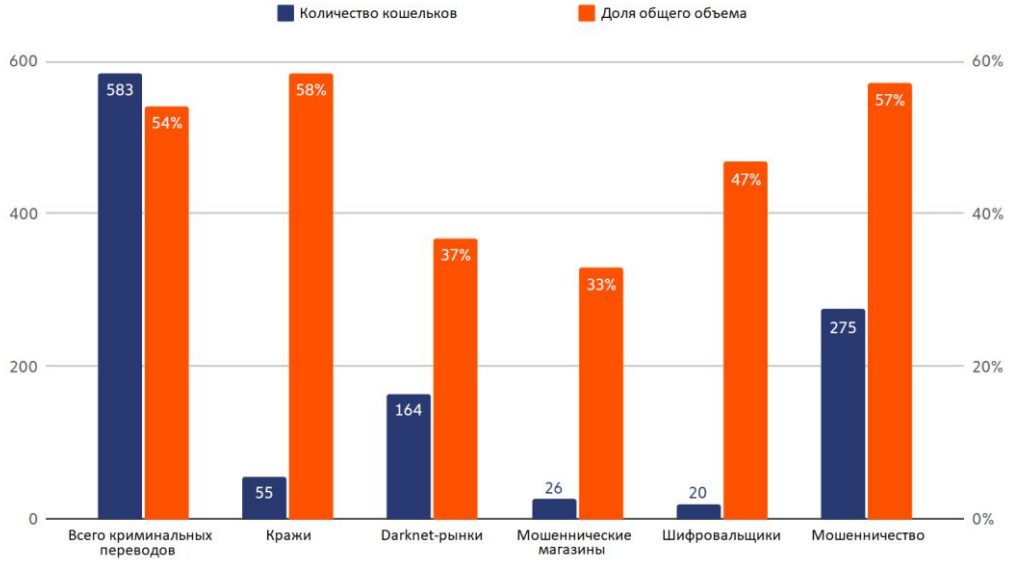

Рисунок 60 – Количество депозитных счетов, получивших более $1 млн. криминальной криптовалюты в разбивке по категориям преступности и доля всех отправленных средств по категориям преступности 2021 года

Кейс: *Spartan Protocol* использует *DeFi*-платформы и прыжки по цепочке для отмывания средств.

Как мы уже говорили выше, использование платформ *DeFi* для отмывания средств резко возросло в 2021 году. Взлом *Spartan Protocol* служит хорошим примером того, как выглядит эта деятельность (рисунок 61).

В мае 2021 года один или несколько хакеров воспользовались уязвимостью в коде, чтобы украсть из платформы криптовалюту на сумму более 30 млн долларов США — в основном его родной токен *SPARTA*. Затем хакер конвертировал большую часть этих средств в *anyETH* и *anyBTC*, которые представляют собой композиты *Ethereum* и *Bitcoin*, соответственно, построенные на отдельных блокчейнах, отличных от оригиналов. Затем часть *anyBTC* была обменена на *Bitcoin*, перейдя таким образом на блокчейн *Bitcoin*, что привело нас к транзакциям, показанным на графике *Chainalysis Reactor* ниже (рисунок 62).

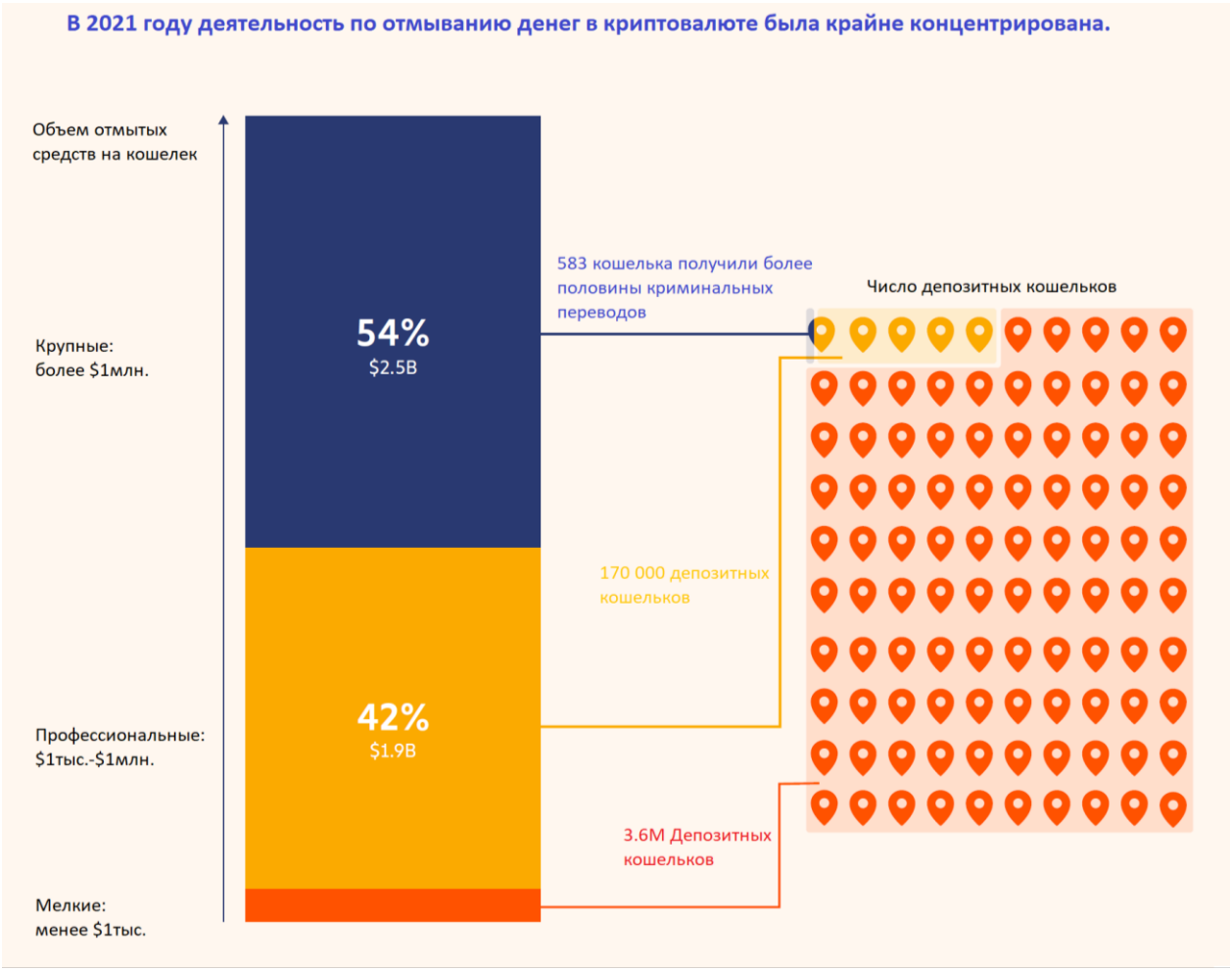

Рисунок 61 – Концентрация активности по отмыванию криминальных средств 2021 года

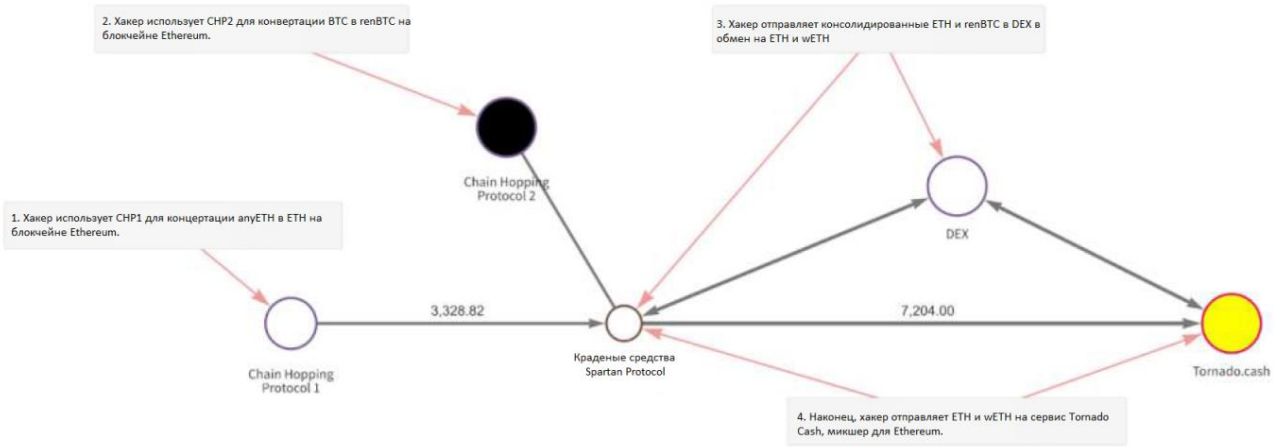

Рисунок 62 – Схема транзакций взлома *Spartan Protocol*

Используя две *DeFi*-платформы, которые специализируются на кроссчейн-транзакциях, хакер перешел на блокчейн *Ethereum*, конвертировав средства в *Ethereum* и *renBTC*. Затем хакер отправил

эти средства на *DEX*, обменяв их на новый *Ethereum* и *wrapped Ethereum*. Наконец, хакер перевел эти средства в *Tornado Cash*, микшер для блокчейна *Ethereum*.

Хотя большинство этих операций было проведено в дни, непосредственно следующие за взломом в начале мая, некоторые из них состоялись несколько месяцев спустя, причем хакер продолжал отмывать средства вплоть до октября. Такая ситуация менее вероятна в случае централизованных сервисов, которые, в отличие от платформ *DeFi*, обычно запрашивают у клиентов *KYC*-информацию при регистрации и имеют больше возможностей для замораживания средств из подозрительных источников. Взлом сервиса *Spartan* — отличный пример не только того, почему *DeFi* привлекателен как механизм отмывания средств, но и того, насколько сложным может стать расследование, когда киберпреступники используют *DeFi* — особенно платформы с переходом по цепочке.

Для раскрытия дел, подобных взлому *Spartan Protocol*, правоохранительные органы должны хорошо разбираться в анализе транзакций *DeFi*, но создающие платформы *DeFi* команды также должны работать над тем, чтобы предотвратить злоупотребление их продуктами со стороны киберпреступников. Одним из способов сделать это является проверка счетов, взаимодействующих с их смарт-контрактами, на предмет предыдущих транзакций с известными криминальными криптосчетами. С помощью *API Chainalysis* разработчики *DeFi* могут автоматизировать процесс проверки и убедиться, что их сервисы не используются для содействия отмыванию средств.

Кейс: Наркоторговцы из Великобритании сотрудничают с брокером для отмывания наркоденег с применением *bitcoin*.

Как мы уже говорили ранее, трудно оценить роль криптовалют в отмывании средств, полученных от традиционных, офлайновых преступлений. Это связано с тем, что в таких случаях криптовалюта не перемещается со счетов, которые мы ранее определили, как связанные с преступностью, а скорее изначально размещается как фиатная валюта без каких-либо доказательств ее криминального происхождения, видимых в блокчейне. Кто-то может узнать о происхождении этих средств только в том случае, если уже расследует криминальную деятельность, и мы знаем, что, по крайней мере, некоторые преступники пользуются этим механизмам. Следователи по-прежнему могут использовать *Chainalysis Reactor* для расследования таких дел, и мы покажем вам пример того, как это делается, в следующем примере

успешного расследования деятельности группы наркоторговцев из Великобритании.

Схема была проста: Группа поставляла наркотики по всей северной Англии и передавала их уличным дилерам, которые затем продавали их за наличные, которые затем доставлялись обратно в преступную группу. Затем курьер забирал наличные и доставлял их брокеру, который организовывал конвертацию средств в *Bitcoin*. Затем брокер отправлял *Bitcoin* на счет, указанный преступной группой, беря небольшую комиссию в размере 4 %. Сеть *Bitcoin* используется в качестве системы передачи средств, и дальнейший анализ показал, что валюта в конечном итоге была отправлена на внебиржевой сервис, вложенный в популярную криптовалютную биржу.

Группа по борьбе с тяжкими и организованными преступлениями полиции Большого Манчестера обнаружила роль *Bitcoin* в операции по отмыванию после того, как остановила одного из курьеров, которого они ранее заметили за сбором наличных на конспиративной квартире, и обнаружила в его автомобиле 170 000 британских фунтов наличными. Полиция арестовала подозреваемого за отмывание и изъяла два мобильных телефона. Последующая цифровая экспертиза этих устройств показала наличие различных сообщений в *WhatsApp* и *Telegram* с подробным описанием плана, а также *Bitcoin*-кошельков и скриншотов хэшей транзакций.

С этой информацией офицеры смогли использовать анализ блокчейна, чтобы увидеть движение средств. Используя *Chainalysis Reactor*, мы можем увидеть активность, о которой говорится на скриншоте (рисунок 63).

Эквивалент 174 900 фунтов за вычетом 4 % комиссии брокера был отправлен на *Bitcoin*-счет, указанный наркоторговцами. Это относительно низкий процент по сравнению с более традиционными видами отмывания средств, что говорит о том, что отмывание с помощью *Bitcoin* может стать все более привлекательным для традиционных преступников. Затем средства отправляются на кошелек посредника, после чего поступают на внебиржевой сервис, вложенный в популярную криптовалютную биржу. Анализ других транзакций позволил установить, что курьер, работавший на группировку наркоторговцев, используя эти методы, отмыл не менее миллиона фунтов в нескольких *Bitcoin*-транзакциях.

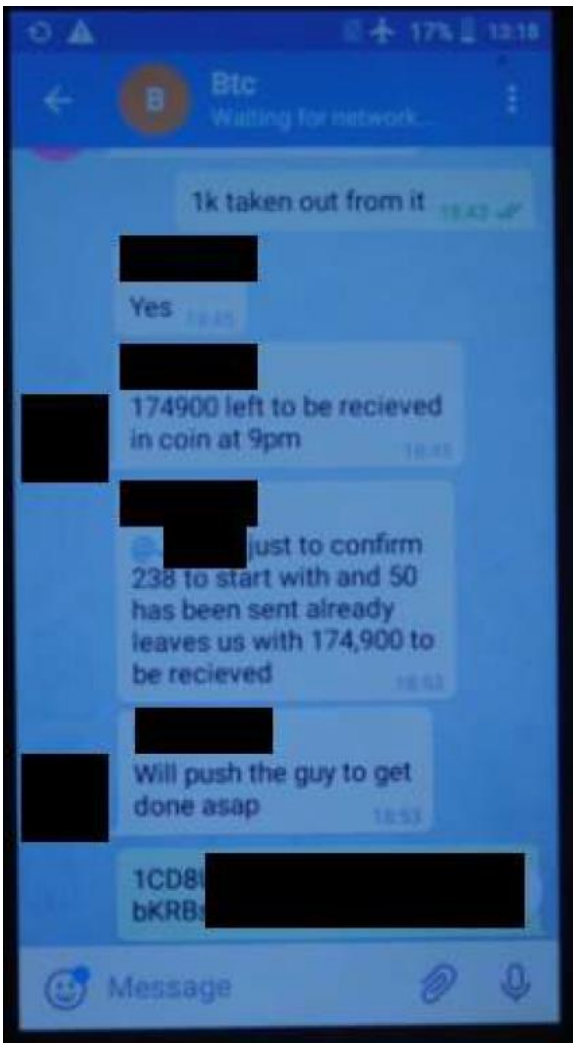

Рисунок 63 – Telegram-переписка по кейсу

Этот случай показывает, насколько важно всем следователям по уголовным делам — не только тем, кто занимается киберпреступлениями — разбираться в криптовалютах и анализе блокчейна. Оно также служит примером того, как анализ блокчейна может дополнить более устоявшиеся методы расследования, которыми уже хорошо владеют правоохранительные органы. В данном случае сотрудники использовали цифровую экспертизу для обнаружения криптовалютных связей, а затем смогли проанализировать транзакции на блокчейне, чтобы понять схему отмывания денег наркоторговцами, что привело к их успешному судебному преследованию.

Финансовый баланс киберпреступников

Криминальные «киты» удерживают более 25 млрд долларов США в криптовалюте из множества преступных источников.

Одним из позитивных событий последнего года стала растущая способность правоохранительных органов изымать криптовалюту

у преступников. В 2021 году мы увидели несколько примеров этого, в том числе:

– Минюст США изъял криптовалюты на сумму 2,3 млн долларов США у операторов шифровальщика *DarkSide*, ответственных за атаку на компанию *Colonial Pipeline*, о чем мы подробно рассказываем в нашем разделе о шифровальщиках.

– В течение 2021 года служба *IRS-CI* конфисковала криптовалюты на общую сумму более 3,5 млрд долларов США.

– Столичная полицейская служба Лондона (MPS) произвела крупнейшую в Великобритании конфискацию криптовалюты, изъяв у подозреваемого в отмывании средств 180 млн долларов США.

Совсем недавно, в феврале 2022 года, минюст США конфисковал *Bitcoin* на сумму 3,6 млрд долларов США по делу взлома *Bitfinex* в 2016 году, что на данный момент является крупнейшим в истории возвратом краденных активов в криптовалюте или фиате.

Эти истории важны не только потому, что позволяют получить финансовую компенсацию жертвам криптовалютных преступлений, но и потому, что опровергают мнение о том, что криптовалюта — это не отслеживаемый, не поддающийся идентификации актив, идеально подходящий для преступлений. Если киберпреступники будут знать, что правоохранительные органы способны изъять их криптовалюту, это может снизить стимул использовать ее в будущем.

Эти кейсы также поднимают важный вопрос: Сколько криптовалюты в настоящее время хранится в блокчейне у известных криминальных структур, и поэтому теоретически может быть изъято правоохранительными органами? Ответ на этот вопрос зависит не только от криптовалютных доходов от преступлений в 2021 году, но и от нелегальных доходов за все время, которые все еще хранятся по видимым счетам. Ниже мы рассмотрим, как общую сумму криптовалютных активов, которые можно отследить до незаконных источников, так и общий баланс криминальных «китов», то есть преступников, владеющих криптовалютой на сумму от 1 млн долларов США.

Краденные средства доминируют в общем балансе преступников.

Начнем с анализа остатков криминальных средств на конец года за последние пять лет в разбивке по видам незаконной деятельности, в результате которой они были получены. В данном анализе под криминальными остатками подразумеваются любые средства, которые в настоящее время хранятся на счетах, приписываемых *Chainalysis* криминальным субъектам. Эти счета могут принадлежать криминальным сервисам, например, *Darknet*-рынкам, но в некоторых слу-

чаях на них также могут располагаться частные кошельки, например, в случаях с кражами (рисунок 64).

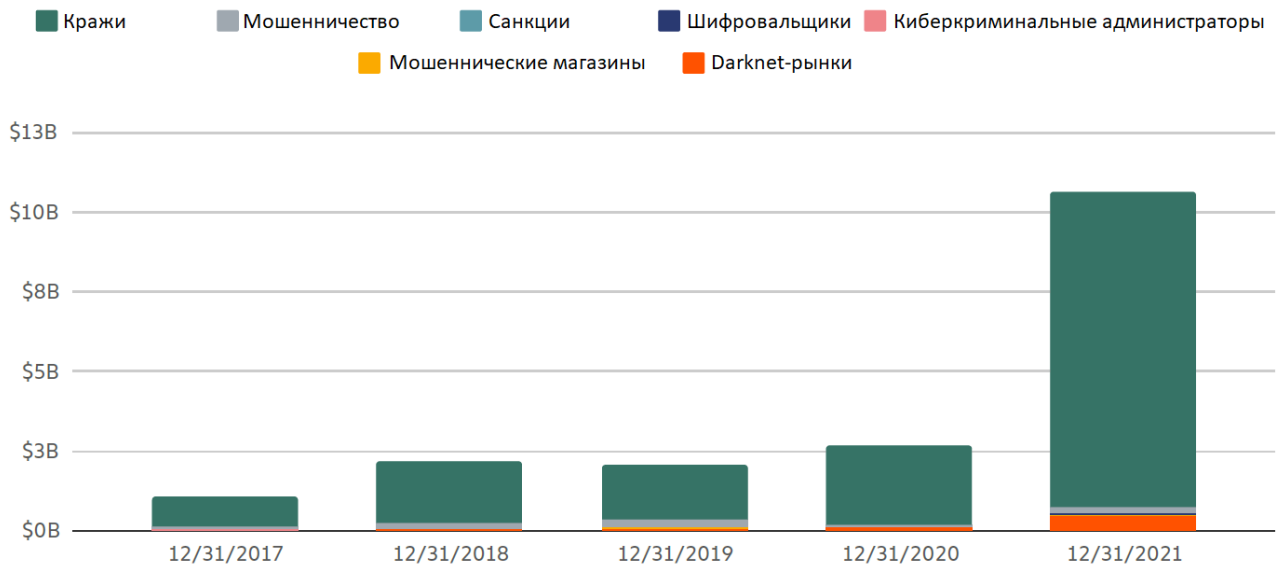

Рисунок 64 – Криминальный финансовый баланс на конец года за период 2017–2021 гг.

Больше всего выделяются две вещи: первая — огромный рост криминальных накоплений в 2021 году — на конец года преступники держали средства из известных незаконных источников на сумму 11 млрд долларов США, тогда как на конец 2020 года этот показатель составлял всего 3 млрд долларов США. Вторая причина заключается в том, насколько сильно преобладают украденные средства. По состоянию на конец 2021 года на краденные средства приходится 93 % всех остатков преступных средств — 9,8 млрд долларов США (рисунок 65).

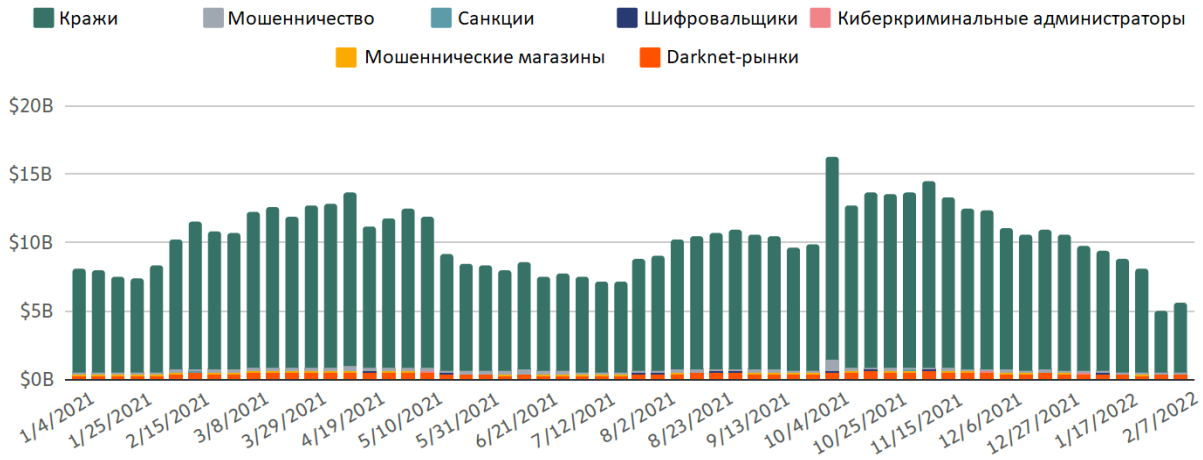

Рисунок 65 – Общий недельный баланс по видам преступлений (2021 год)

«Киберкриминальные администраторы» означает счета, которые были приписаны лицам, связанным с управлением киберпреступной организацией, такой как *Darknet*-рынок.

Далее следуют фонды торговых площадок в *Darknet* — 448 млн долларов США, затем мошенничества — 192 млн долларов США, мошеннические магазины — 66 млн долларов США и шифровальщики — 30 млн долларов США. Криминальные балансы также колебались в течение года: от минимума в $6,6 млрд долларов США в июле до максимума в 14,8 млрд долларов США в октябре. Эти колебания напоминают о важности скорости в криптовалютных расследованиях, поскольку криминальные средства, успешно отслеженные в блокчейне, могут быть быстро ликвидированы. Конечно, криминальные балансы могут падать и по веским причинам. Значительное падение криминальных накоплений, которое мы видим выше в феврале 2022 года, связано с конфискацией минюстом США 3,6 млрд долларов США в *Bitcoin*, похищенных в результате взлома *Bitfinex* в 2016 году. После этого изъятия, по состоянию на 9 февраля 2022 г., криминальные балансы составляют около 5 млрд долларов США.

Давайте посмотрим, какие типы киберпреступников дольше всего хранят свои средства (рисунок 66).

Рисунок 66 – Среднее время хранения криптовалюты для криминальных счетов за 2021 год

Если рассматривать тенденции за все время, то продавцы и администраторы *Darknet*-рынков дольше всего держат свои средства перед ликвидацией, а кошельки с краденными средствами хранятся наименьшее время. Последнее может вызвать удивление — как кра-

денные средства могут храниться так мало по времени, но при этом составлять подавляющее большинство суммы криминальных накоплений? Оказывается, большинство этих средств принадлежат очень крупным счетам, которые хранят средство дольше, чем другие счета в категории краденных средств. Но что действительно бросается в глаза, так это то, насколько сократилось время хранения по всем категориям — среднее время хранения в 2021 году по крайней мере на 75 % меньше, чем в прошлом во всех категориях. Операторы шифровальщиков, в частности, являются примером этой тенденции, поскольку теперь они держат средства в среднем всего 65 дней, прежде чем ликвидировать их. Возможно, это реакция на растущее давление правоохранительных органов, с которым сталкиваются злоумышленники, использующие программы-вымогатели.

Криминальные киты показывают больше вариаций.

Вопрос, который естественным образом вытекает из нашего исследования криминальных накоплений: Какие преступники хранят больше всего криптовалюты? Мы решили провести исследование, проанализировав балансы криминальных китов. Однако обратите внимание, что мы рассчитываем балансы несколько иначе, чем общие накопления преступников, о которых мы говорили выше. Мы определяем «криминального кита» как любой частный кошелек с криптовалютой на сумму от 1 млн долларов США, который получил более 10 % средств с криминальных счетов.

Следует понимать, что поскольку баланс криминальных китов рассчитывается на основе данных о частных кошельках, а общий криминальный баланс рассчитывается на основе данных о счетах, помеченных как незаконные (то есть они могут включать средства, хранящиеся на сервисах в дополнение к частным кошелькам), баланс криминальных китов, обсуждаемый здесь, не будет совпадать с общим криминальным балансом, рассчитанным выше.

В целом, *Chainalysis* выявил 4 068 криминальных китов, владеющих криптовалютой на сумму более 25 млрд долларов США. Криминальные киты составляют 3,7 % от всех криптовалютных китов — то есть частных счетов, на которых хранится криптовалюта на сумму более 1 млн долларов США (рисунок 67).

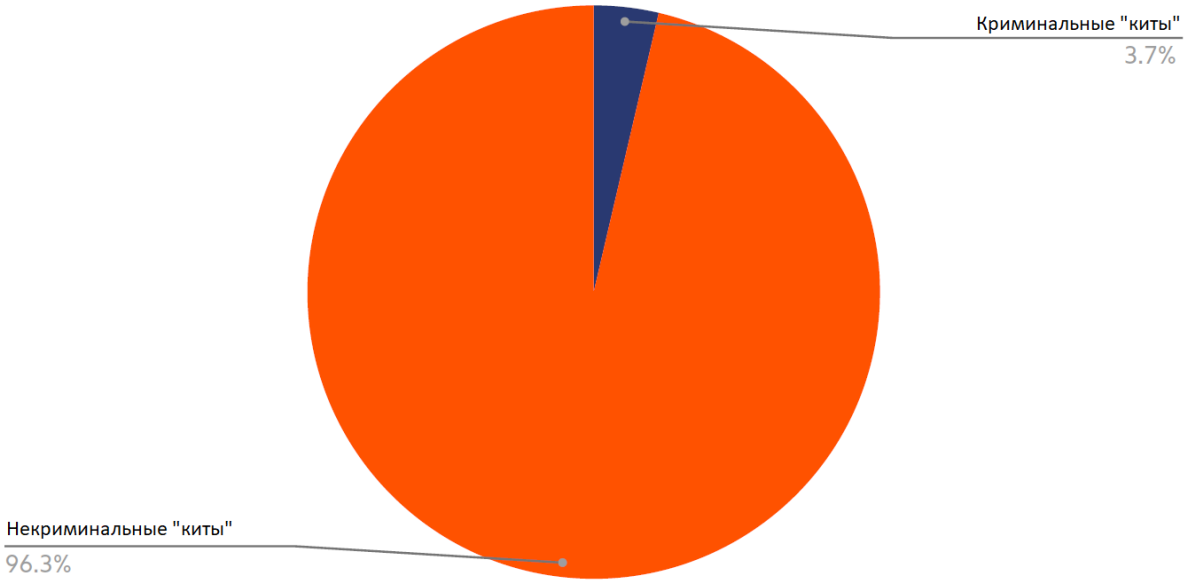

Рисунок 67 – Доля всех криптовалютных «китов»,
получивших 10 % и более средств с криминальных счетов

Интересная картина вырисовывается, когда мы разбиваем криминальных китов по доле их общих средств, имеющих незаконное происхождение: большинство криминальных китов, получали либо относительно небольшую, либо чрезвычайно большую долю своего общего баланса с криминальных счетов (рисунок 68).

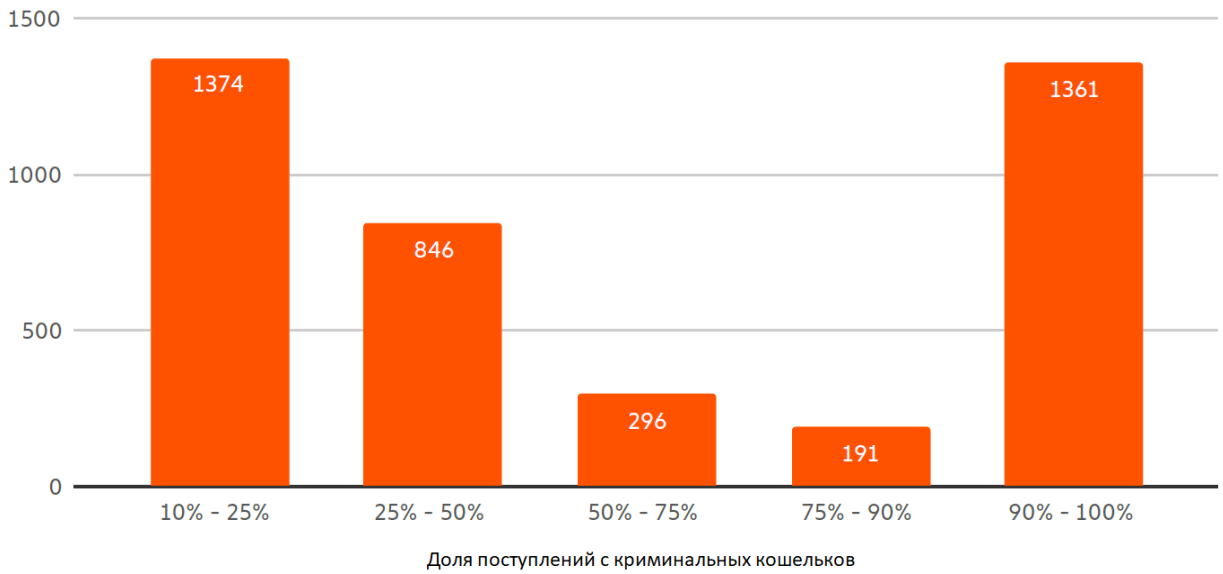

Рисунок 68 – Криминальные «киты» по доле всех средств,
полученных с криминальных счетов

Выше мы распределили всех криминальных китов по доле всех полученных ими криптовалют, поступивших с криминальных счетов. 1 374 криминальных кита получили от 10 до 25 % от общего баланса с криминальных счетов. Однако самый крупная группа находится близко позади: 1 361 счет получил от 90 до 100 % своего общего баланса с криминальных счетов. В целом, 1 333 криминальных кита получили от 25 до 90 % всех средств с криминальных счетов.

Незаконные средства, полученные криминальными китами, также поступают из более разнообразных источников, чем средства, составляющие общий баланс преступников (рисунок 69).

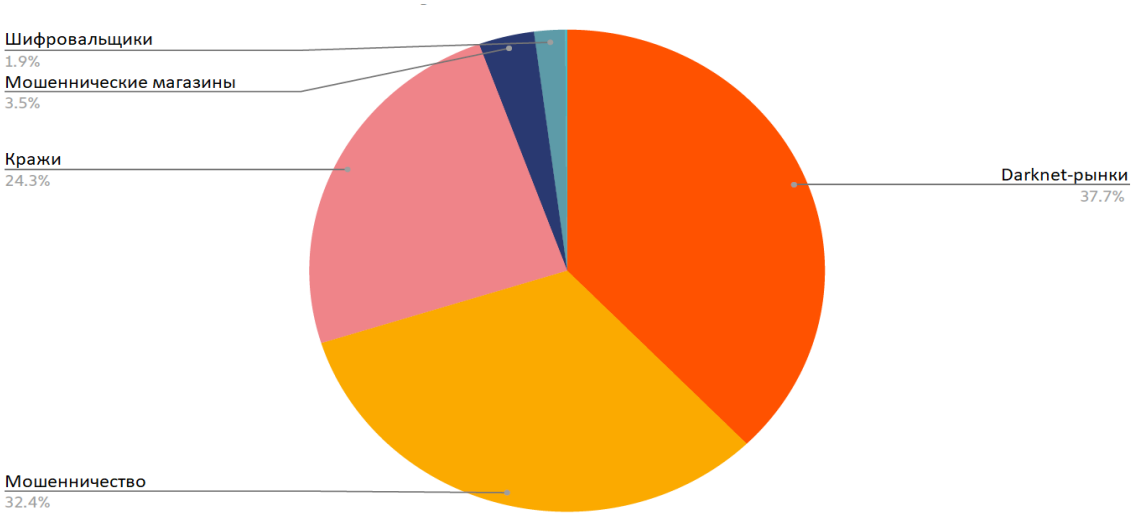

Рисунок 69 – Источники средств,
получаемых криминальными «китами»

В то время как краденные средства доминируют в общем балансе преступников, *Darknet*-рынки являются крупнейшим источником криминальных средств, направляемых криминальным китам, на втором месте — мошенничество, на третьем — краденные средства.

Наконец, мы также можем использовать анализ часовых поясов, чтобы попытаться приблизительно определить местоположение криминальных китов. На приведенном ниже графике мы присвоили часовые пояса криминальным китам, чьи кошельки обладают достаточной активностью, чтобы мы могли сделать точную оценку (рисунок 70).

Временные зоны UTC 2, 3 и 4, по оценкам, содержат больше всего криминальных китов, в то время как временные зоны 1 и -9 также имеют большое количество. Часовые пояса UTC 2, 3 и 4 включают большую часть России, в том числе крупные населенные пункты,

такие как Москва и Санкт-Петербург, что особенно интересно в контексте огромной роли России в криптовалютной преступности, о чем мы рассказываем в других разделах этого отчета. Однако часовые пояса, конечно, позволяют нам оценить только продольное местоположение, поэтому вполне возможно, что некоторые из криминальных китов базируются в других странах в пределах часовых поясов 2, 3 и 4, таких как Южная Африка, Саудовская Аравия или Иран.

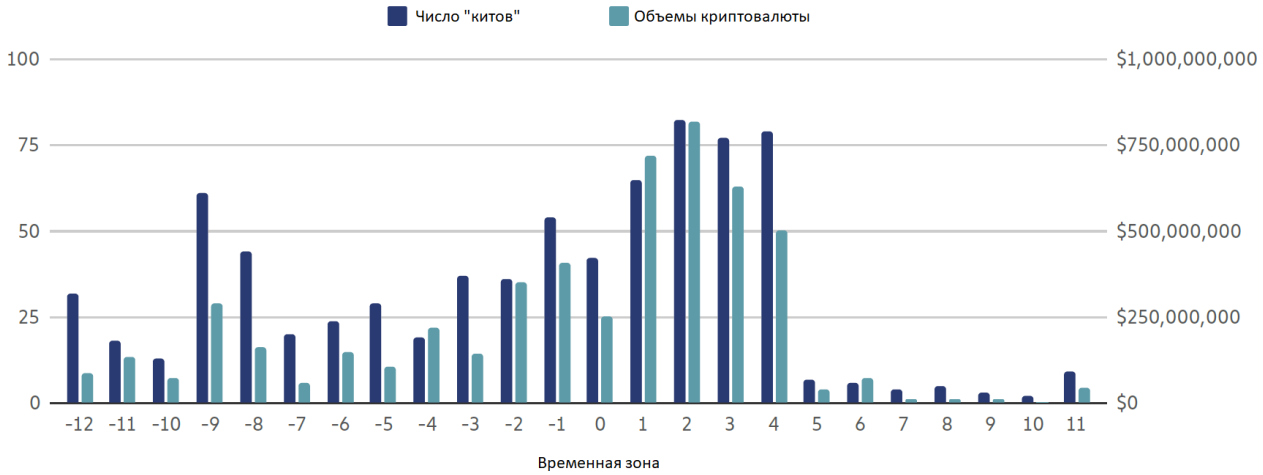

Рисунок 70 – Предполагаемый часовой пояс криминальных «китов»

Возможность эффективно отслеживать криминальных китов и количественно оценивать их активы на основе одного публичного набора данных является основным отличием криптовалютной преступности от фиатной. В фиате преступники с самым высоким чистым капиталом используют мутные сети иностранных банков и подставных корпораций, чтобы скрыть свои активы. Но в криптовалюте транзакции сохраняются в блокчейне для всеобщего обозрения. Расследование преступных китов представляет собой отличную возможность для государственных органов по всему миру продолжить череду успешных конфискаций и привлечь к ответственности крупнейших бенефициаров криптовалютных преступлений.

Криминал и NFT

Исследователи *Chainalysis* выявили значительные объемы «серых» сделок и некоторые случаи отмывания средств в этом новом классе активов.

Non-fungible tokens (*NFT*) стали одной из самых громких историй в криптовалюте в 2021 году. *NFT* — это цифровые элементы на основе блокчейна, которые разработаны таким образом, чтобы быть уникальными, в отличие от традиционных криптовалют, которые предназначены для взаимозаменяемости. *NFT* могут хранить данные на блокчейне — большинство проектов *NFT* построены на та-

ких блокчейнах, как *Ethereum* и *Solana* — и эти данные могут быть связаны с изображениями, видео, аудио, физическими объектами, членством и бесчисленными другими развивающимися вариантами использования. *NFT* обычно дают владельцу право собственности на данные или медиа, с которыми связан токен, и обычно покупаются и продаются на специализированных торговых площадках.

Популярность *NFT* резко возросла в 2021 году. *Chainalysis* отследил минимум 44,2 млрд долларов США криптовалюты, отправленной в контракты *ERC-721* и *ERC-1155* — два типа смарт-контрактов *Ethereum*, связанных с рынками и коллекциями *NFT* — по сравнению со всего лишь 106 млн долларов США в 2020 году (рисунок 71).

Рисунок 71 – Еженедельный объем криптовалют и средняя стоимость транзакции на *NFT*-платформы в 2021 году

Однако, как и в случае с любой новой технологией, *NFT* не исключает возможности злоупотреблений. Важно, чтобы по мере того, как наша индустрия рассматривает все способы, которыми этот новый класс активов может изменить то, как мы связываем блокчейн с физическим миром, мы также создавали продукты, которые делают инвестиции в *NFT* максимально безопасными и надежными. Ниже мы рассмотрим две формы криминальной деятельности, которую мы наблюдали в *NFT*:

- отмывочная торговля для искусственного повышения стоимости *NFT*;

– отмывание средств через покупку *NFT*.

Давайте погрузимся в этот вопрос.

Некоторые продавцы *NFT* наживаются на «отмывочной» торговле.

Еще одной областью, вызывающей беспокойство *NFT*, является «отмывочная торговля», то есть проведение сделки, в которой продавец выступает на обеих сторонах сделки, чтобы создать ложное представление о стоимости и ликвидности актива. Исторически сложилось так, что криптовалютные биржи пытаются создать видимость больших объемов торгов, чем есть на самом деле. В случае с «отмывочной торговлей» *NFT*, цель состоит в том, чтобы сделать свои *NFT* более ценным, чем он есть на самом деле, «продав» его на новый кошелек, который также контролирует первоначальный владелец. Теоретически, это было бы относительно просто с *NFT*, поскольку многие торговые *NFT*-платформы позволяют пользователям торговать, просто подключив свой кошелек, без необходимости идентифицировать себя.

Однако с помощью анализа блокчейна мы можем отследить отмывочную торговлю *NFT*, проанализировав продажи *NFT* на самофинансируемые счета, то есть были профинансированные либо продающим криптосчетом, либо счетом, который первоначально профинансировал продающий счет. Анализ продаж *NFT* на самофинансируемые счета показывает, что некоторые продавцы *NFT* провели сотни отмывочных сделок.

Давайте более подробно рассмотрим продавца 1, самого «плодовитого» продавца *NFT*, который совершил 830 продаж на самофинансированные счета (рисунок 72). На скриншоте *Etherscan* ниже показана транзакция, в которой этот продавец, используя счет, начинающийся с 0×828, продал *NFT* на счет, начинающийся с 0×084, за 0,4 *Ethereum* через торговую площадку *NFT* (рисунок 73).

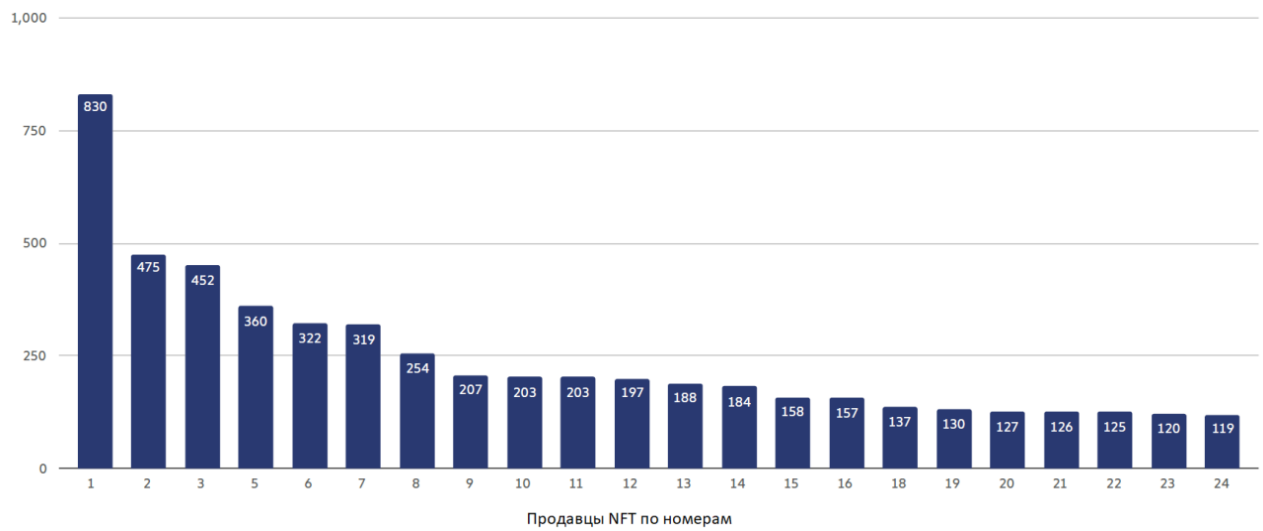

Рисунок 72 – Продавцы *NFT* по количеству продаж
на самофинансируемые счета 2021 года

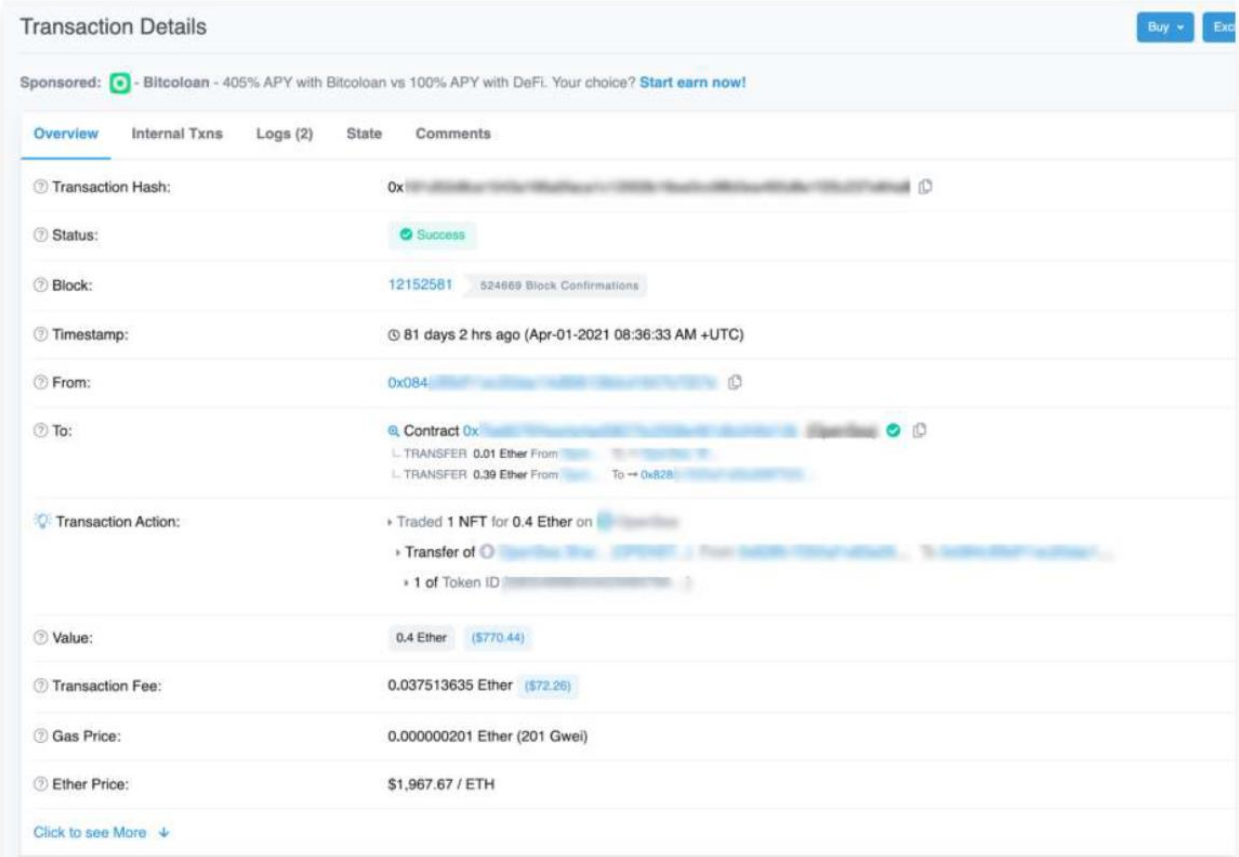

Рисунок 73 – Скриншот Etherscan

На первый взгляд все выглядит нормально. Однако график *Chainalysis Reactor* ниже показывает, что счет 0×828 незадолго до этой продажи отправил 0,45 *Ethereum* на счет 0×084 (рисунок 74).

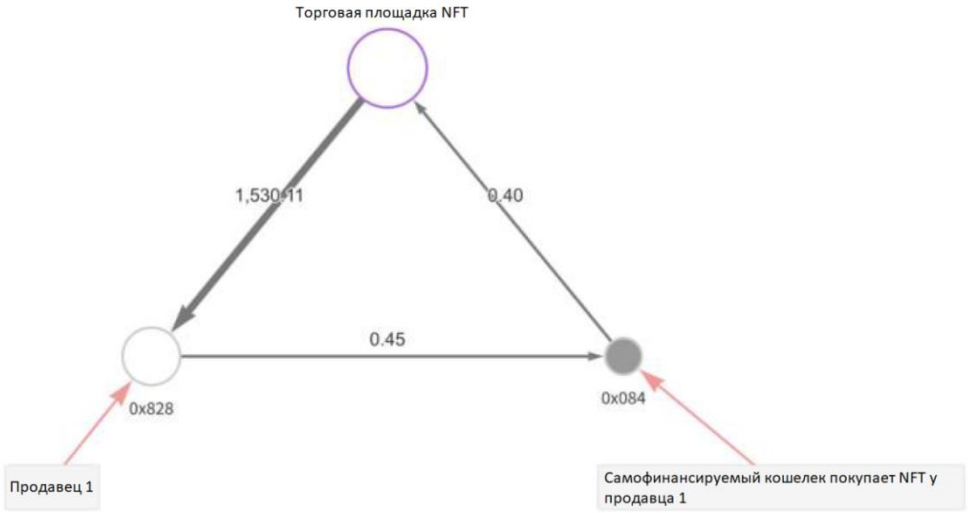

Рисунок 74 – Транзакции продавца *NFT*

Эта активность соответствует шаблону Продавца 1. На графике *Reactor* ниже (рисунок 75) показаны аналогичные отношения между продавцом 1 и сотнями других счетов, на которые он продавал *NFT*.

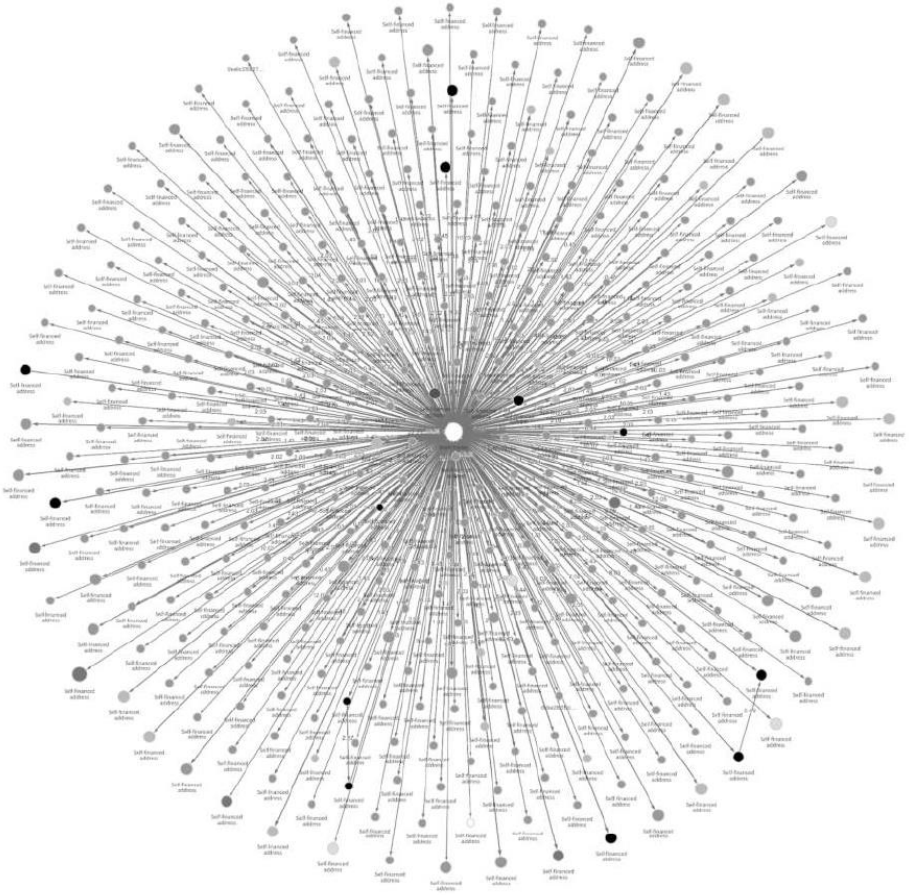

Рисунок 75 – График из системы *Chainalysis Reactor*

Продавец 1 — это счет в центре. Все остальные счета на этом графике получили средства от основного счета Продавца 1 до покупки *NFT* с этого счета. Однако пока что Продавец 1, похоже, не извлек прибыли из своей активной отмывочной торговли. Если мы подсчитаем сумму, которую продавец 1 заработал на продаже *NFT* счетам, которые он сам не финансировал — и которые, как мы можем предположить, являются жертвами, не знающими о том, что *NFT*, которые они покупают, были отмыты — это не компенсирует сумму, которую им пришлось потратить на комиссию во время сделок отмывочной торговли (таблица 1).

Таблица 1 – Подсчёт суммы, которую продавец 1 заработал на продаже *NFT* счетам

Кошелек продавца 1	Сумма комиссионных, $	Доход от продажи NFT, $	Общий баланс, $
0×828...	-35,642	27,258	- 8,383

Однако история меняется, если мы посмотрим на более крупную часть экосистемы *NFT*. Используя анализ блокчейна, мы выявили 262 пользователя, которые продали *NFT* на самофинансируемый счет более 25 раз. Хотя мы не можем быть на 100 % уверены, что все случаи продажи *NFT* на самофинансируемые кошельки предназначены для отмывочной торговли, порог в 25 транзакций дает нам большую степень уверенности в том, что эти пользователи являются постоянными отмывочными трейдерами. Как и в случае с одним трейдером, мы рассчитали общую прибыль этих 262 трейдеров, вычтя сумму, потраченную ими на комиссию, из суммы, которую они заработали на продаже *NFT* ничего не подозревающим покупателям. Одна оговорка для этого анализа заключается в том, что он охватывает только сделки, совершенные в *Ethereum* и *Wrapped Ethereum*, так что, вероятно, существует деятельность по отмыванию, которую мы здесь не рассматриваем.

Тем не менее, вырисовывается интересная история: Большинство отмывочных схем в *NFT* были убыточными, но успешные отмыватели получили такую прибыль, что в целом эта группа из 262 человек является крайне доходной (таблица 2).

Таблица 2 – Соотношение групп, количества счетов и доходов

Группа по отмыванию средств	Количество счетов	Доходы, $
Прибыльные группы	110	8 875 315
Бесприбыльные группы	152	-416 984
Всего	262	8 458 331

110 прибыльных трейдеров получили в общей сложности почти 8,9 млн долларов США прибыли от этой деятельности, что значительно превышает убытки в размере 416 984 долларов США, понесенные 152 убыточными трейдерами. Что еще хуже, эти 8,9 млн долларов США, скорее всего, получены от продаж ничего не подозревающим покупателям, которые считают, что *NFT*, которые они покупают, растут в цене, продаваясь от одного коллекционера к другому.

Отмывочная торговля *NFT* существует в серой правовой зоне. В то время как отмывочная торговля запрещена в отношении обычных ценных бумаг и фьючерсов, в *NFT* она еще не стала предметом судебного преследования. Однако ситуация может измениться, когда регулирующие органы сместят фокус и применят существующие

полномочия по борьбе с мошенничеством к новым рынкам *NFT*. В целом, отмывочная торговля в *NFT* может создать криминальный рынок для тех, кто покупает искусственно завышенные в цене токены, а ее существование может подорвать доверие к экосистеме *NFT*, препятствуя будущему росту. Мы призываем торговые площадки *NFT* максимально препятствовать такой деятельности. Данные анализа блокчейна позволяют легко обнаружить пользователей, продающих *NFT* на счета, которые они самостоятельно финансировали, поэтому площадки могут рассмотреть возможность запрета или других наказаний для самых злостных нарушителей.

Деятельность по отмыванию средств незначительна, но заметна в *NFT*. Используют ли киберпреступники незаконные средства для покупки NFT? Давайте проанализируем (рисунок 76).

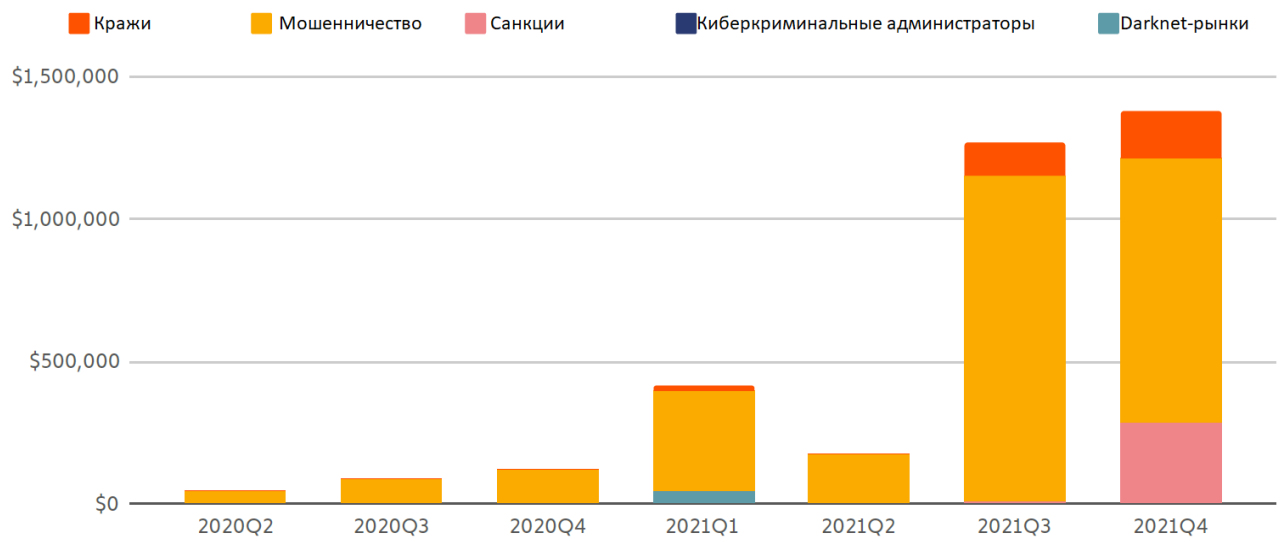

Рисунок 76 – Объемы криминальной криптовалюты,
полученной платформами *NFT*
(период со 2 квартала 2020 по 4 квартал 2021 гг.)

В третьем квартале 2021 года объем средств, отправленных на торговые площадки *NFT* с криминальных счетов, значительно вырос, превысив отметку в 1 миллион долларов США в криптовалюте. В четвертом квартале этот показатель снова вырос, достигнув отметки чуть менее 1,4 млн долларов США. В обоих кварталах подавляющая часть этой активности исходила от связанных с мошенниками счетов, отправляющих средства на торговые площадки *NFT* для совершения покупок. В обоих кварталах также наблюдались значительные суммы краденых средств, отправленных на торговые площадки. Возможно, наиболее тревожным является тот факт, что в четвертом

квартале на торговые площадки *NFT* с криптосчетов с санкционным риском было отправлено криптовалюты на сумму около 284 000 долларов США. Все это было связано с переводами с *P2P*-биржи *Chatex*, которую управление по контролю за иностранными активами (*OFAC*) США в прошлом году включило в список особо опасных лиц.

Примеры различных типов преступников, покупающих *NFT*, мы можем увидеть на графике *Reactor* ниже (рисунок 77).

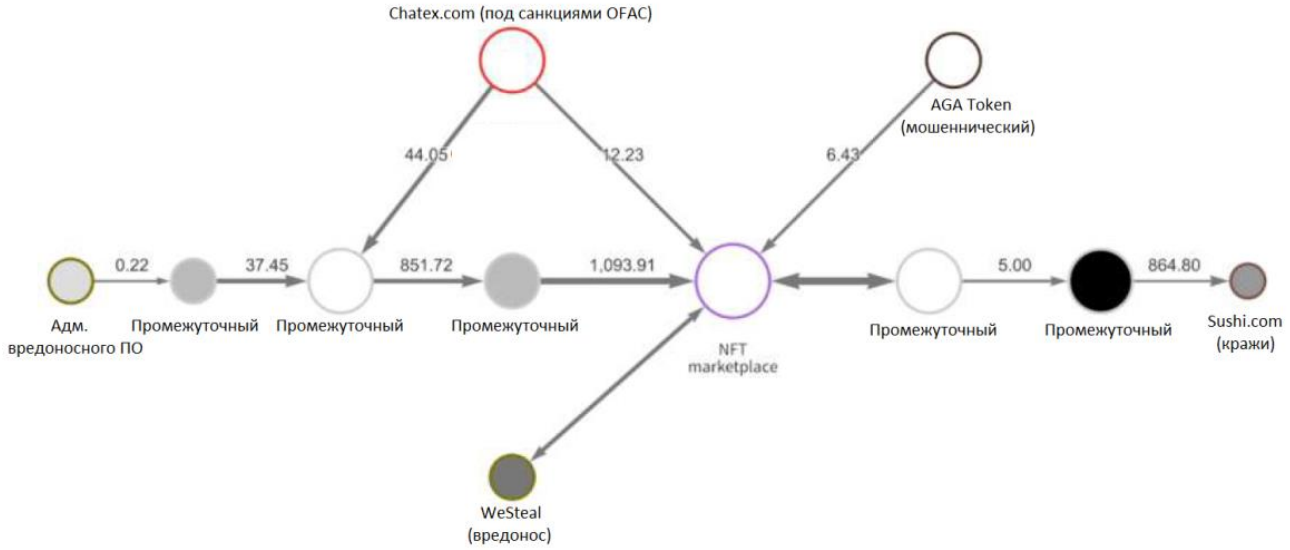

Рисунок 77 – Схема криминальных транзакций с участием *NFT*

Здесь мы видим счета, связанные с несколькими различными типами киберпреступников, отправляющих средства на популярную торговую площадку *NFT*, включая операторов вредоносных программ, мошенников и *P2P*-биржу *Chatex*.

Вся эта деятельность представляет собой каплю в море по сравнению с отмыванием криптовалютных средств на сумму 8,6 млрд долларов США, которое мы отследили за весь 2021 год. Тем не менее, отмывание, и в частности переводы от криптовалютных компаний, находящихся под санкциями, представляют собой большой риск для укрепления доверия к *NFT*, и должны более тщательно отслеживаться торговыми площадками, регуляторами и правоохранительными органами.

ЗАКЛЮЧЕНИЕ

В заключение приведенного выше анализа информационных технологий, применяемых в криптовалютах и других цифровых активах, важно подчеркнуть, что современная криптопреступность демонстрирует негативную качественную и количественную трансформацию на фоне очевидной неготовности правоохранительных органов разработать единые стандарты предупреждения такого рода преступлений, а законодателей — определить правовой статус криптовалюты и других цифровых продуктов блокчейна. Для криптопреступности характерно увеличение динамики, углубление специализации компаний и «опривычивание» криминального использования виртуальной валюты.

В целях предупреждения дальнейшего развития криптопреступности важно разработать такую модель правового регулирования оборота, в которой одновременно были бы решены две задачи: предупреждение совершения корыстных преступлений и поддержка инновационного развития российской экономики.

Целесообразно обозначить некоторые приоритетные направления правового регулирования новых финансовых инструментов с одновременным обеспечением безопасности участников рынка:

– включение криптовалюты в число объектов гражданских прав (ст. 128 ГК РФ) с одновременным определением в специальных нормативных правовых актах пределов безопасности использования модели коллективного инвестирования (краудфандинга);

– введение требования об обязательной идентификации владельцев цифровых активов и иных лиц, участвующих в их обороте;

– установление режима конвертации цифровой криптовалюты в фиатную;

– определение правовых критериев и стандартов предупреждения отмывания криминальных доходов, в том числе с использованием криптовалюты[1];

– введение уголовной и административной ответственности

[1] См.: Иванцов С. В., Новиков С. В. Преступления на рынке ценных бумаг: криминологическая характеристика и предупреждение. Москва: Юнити-Дана, 2012. 119 с.

за нарушение стандартов оборота криптоинструментов[1];

– создание международной базы данных о лицах, занимающихся незаконным оборотом и применением цифровых финансовых активов[2], в контексте используемых технологий и субъектов криптопреступности;

– определение модели налогового администрирования криптовалюты и иных цифровых активов[3];

– лицензирование профессиональной деятельности, связанной с созданием и оборотом новых цифровых активов.

Вступивший в силу 1 января 2021 г. закон о цифровых финансовых активах и цифровой валюте (Закон № 259-ФЗ), хотя и содержит в своем названии оба этих понятия, и дает их определения, не сильно помог криптосообществу с точки зрения понимания сущности и условий использования криптовалют в нашей стране. Как отметил председатель Комитета Государственной Думы Российской Федерации по финансовому рынку А. Аксаков, принятие Закона № 259-ФЗ должно поспособствовать более активному использованию технологии блокчейн для выпуска цифровых финансовых активов с целью привлечения инвестиций под реализацию различных проектов[4].

---

[1] См.: Ларина Е., Овчинский В. Криптовалюта: свет и тени // Наш современник. 2018. № 8. С. 214–224.

[2] См.: Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А. П. Суходолов [и др.] // Всероссийский криминологический журнал. 2017. Т. 11, № 1. С. 13–21.

[3] См., например: Cox J. Staying in the Shadows: The Use of Bitcoin and Encryption in Cryp-tomarkets // The Internet and Drug Markets. Lisbon: EMCDDA, 2016. P. 41–47; Foley S., Karlsen J. R., Putnins T. J. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? URL: https://papers.ssrn.com /sol3 / papers.cfm?abstract_id=3102645. (дата обращения: 02.11.2019).; Сидоренко Э. Л., Шайдуллина В. К., Киракосян С. А. Токенизация угольной промышленности: экономические и криминологические риски // Уголь. 2018. № 12. С. 54–59.

[4] См.: Обручев В. Закон о криптовалюте: Федеральный закон «О цифровой валюте и цифровых финансовых активах». Москва: Эксмо, 2021. 64 с.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ *

1. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А. П. Суходолов [и др.]. – Текст : непосредственный // Всероссийский криминологический журнал. – 2017. – Т. 11, № 1. – С. 13–21. – Библиогр.: с. 20 (10 назв.).

2. Аммус, С. Краткая история денег, или все, что нужно знать о биткоине / Сейфедин Аммус ; пер. с англ. М. Сухотиной ; [науч. ред. Н. Решетник]. – Москва : Издательство «Манн, Иванов и Фарбер». 2019. – 272 с. – ISBN: 978-5-00117-918-4 – Текст : непосредственный.

3. Антонопулос, А. М. Осваиваем биткойн: программирование блокчейна. / Андреас М. Антонопулос ; [пер. с англ. А. В. Снастина]. – [2-е изд.]. – Москва : ДМК Пресс, 2018. – 428 с. – ISBN 978-5-94074-965-3. – Текст : непосредственный

4. Архипов, В. В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр / В. В. Архипов. – Текст : непосредственный // Закон. – 2014. – № 9. – С. 69–90. – Библиогр.: с89–90 (36 назв.).

5. Афанасьева, Ю. Как заработать биткоины: главные способы, плюсы и минусы // URL : https://www.finam.ru/publications/item/kak-zarabotat-bitkoiny-glavnye-sposoby-plyusy-i-minusy-20190605-16420/?ysclid =lgz5t89hz341805135 (дата обращения: 24.08.2021).

6. Бикмаев, Ш. Р. Развитие рынка платежных карт в современных условиях / Ш. Р. Бикмаев. – Текст : непосредственный // Финансы и кредит. – 2011. – № 41 (473). – С. 65–71. – Библиогр.: с. 71 (4 назв.).

7. Биткоин (Bitcoin). Криптовалюта [Электронный ресурс]. URL : https://www.tadviser.ru/index.php/Статья: Биткоин_(Bitcoin)_Криптовалюта (дата обращения: 30.03.2022).

8. Болотов А. А. Элементарное введение в эллиптическую криптографию : Книга 2 : Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. Москва : Ком-Книга, 2020. – 376 с. – Текст : непосредственный.

* Нормативно-правовые акты представляются в соответствии со справочно-правовой системой «КонсультантПлюс».

9. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум [для академического бакалавриата] / И. Н. Васильева. – Текст: электронный // Образовательная платформа «Юрайт» [сайт]. – Москва : Юрайт, 2019. – 349 с. – ISBN 978-5-534-02883-6. – URL : https://urait.ru/bcode/433610 (дата обращения: 24.08.2021).

10. Все криптовалюты // Финансовые новости = Fusion Media Limited. – URL : https://ru.investing.com/crypto/currencies (дата обращения: 01.11.2019).

11. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ.

12. Директива (ЕС) № 2015/849 Европейского парламента и Совета ЕС о предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской комиссии.

13. Дрешер, Д. Основы блокчейна /Даниэль Дрешер ; [пер. с англ. А. В. Снастина]. – Москва : ДМК Пресс, 2018. – 312 с. – ISBN 978-5-97060-591-2 – Текст : непосредственный.

14. Дуглас, С. Криптовалюта и блокчейн. Основы электронных валют / Саймон Дуглас. – Москва : ЛитРес, 2021. – 188 с. – Текст : непосредственный.

15. Золото. – Текст : электронный. // Википедия, свободная энциклопедия [сайт]. – Сан-Франциско : Фонд Викимедиа, 2019. – URL : https://ru.wikipedia.org/?oldid=102742182 (дата обращения: 01.11.2019).

16. Иванцов, С. В. Преступления на рынке ценных бумаг: криминологическая характеристика и предупреждение / С. В. Иванцов, С. В. Новиков. – Москва : Юнити-Дана, 2012. – 119 с. – ISBN 978-5-238-02317-5 – Текст : непосредственный.

17. Иванцов, С. В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С. В. Иванцов, Э. Л. Сидоренко, Б. А. Спасенников, Ю. М. Берёзкин [и др.]. – Текст : непосредственный // Всероссийский криминологи-

ческий журнал. – 2019. – Т. 13. – № 1. – С. 85–93. – Библиогр.: с. 93 (20 назв.).

18. Как использовать Биткойн // Новичку о Биткойне. Bitcoin Project 2009–2019. – URL : https://bitcoin.org/ru/gettingstarted (дата обращения: 29.10.2019).

19. Криптовалюты на территории стран Содружества: оценка вероятных криминальных рисков и угроз / И. Б. Колчевский, А. Г. Кузнецов. – Москва : ФГКУ «ВНИИ МВД России», 2018. – 15 с. – Текст : непосредственный.

20. Лаптев В. А. Электронное правосудие. Электронный документооборот : научно-практическое пособие / В. А. Лаптев, С. Ю. Чуча ; под общ. ред. С. Ю. Чучи. – Москва : Проспект,2021. – 240 с. – ISBN 978-5-392-30031-0 – Текст : непосредственный.

21. Ларина, Е. Криптовалюта: свет и тени / Е. Ларина, В. Овчинский. – Текст : непосредственный // Наш современник. – 2018. – № 8. – С. 214–224. – ISSN 0027-8238.

22. Локнов, А. И. Особенности и алгоритмы формирования и применения криптовалют / А. И. Локнов, А. И. Примакин, А. М. Хлебников. – Текст : непосредственный // Региональная информатика и информационная безопасность : сборник трудов. – Санкт-Петербург : СПОИСУ, 2020. – Вып. 8. – С. 151–154. – ISBN 978-5-907223-87-5.

23. Магомагазиев, А. А. Рынок криптовалюты. История и сферы влияния криптовалюты / А. А. Магомагазиев. – Текст : непосредственный // Форум молодых учёных. – 2021. – № 12 (64). – С. 142–144. – Библиогр.: с. 144 (3 назв.).

24. Максуров, А. А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование : монография. – 3-е изд. – Москва : Издательство «Дашков и К°», 2022. – 211 с. – ISBN 978-5-394-04756-5 – Текст : непосредственный.

25. Милушкин, С. А. Майнеры. – Москва : АСТ, 2020. – 544 с. – ISBN 978-5-17-114952-9 – Текст : непосредственный.

26. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ.

27. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ.

28. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : законопроект № 419059-7 // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») [официальный сайт]. – URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения: 17.08.2021).

29. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ.

30. Об организованных торгах : Федеральный закон от 21 ноября 2011 г. № 325-ФЗ.

31. Обручев В. Закон о криптовалюте: Федеральный закон «О цифровой валюте и цифровых финансовых активах» – Москва : Эксмо, 2021. – 64 с. – ISBN 978-5-04-120429-7 – Текст : непосредственный.

32. Пухов, А. В. Электронные деньги в коммерческом банке : практическое пособие / А. В. Пухов, А. Ю. Мацкевич, А. В. Рего, П. В. Ушанов. – Москва : Издательство КноРус. – 2015. – 208 с. – ISBN 978-5-406-04397-4 – Текст : непосредственный.

33. Росреестр использовал технологию блокчейн. – Текст : электронный // Ведомости (Vedomosti) : электронное периодическое издание, 08.02.2018. – URL : https://www.vedomosti.ru/economics/articles/2018/02/08/750276-rosreestr blokchein (дата обращения: 02.11.2019).

34. Сидоренко, Э. Л. Криминологические риски оборота криптовалюты / Э. Л. Сидоренко. – Текст : непосредственный // Экономика. Налоги. Право. – 2017. – Т. 10. – № 6. – С. 147–154. – Библиогр.: с. 154 (7 назв.).

35. Сидоренко, Э. Л. Токенизация угольной промышленности: экономические и криминологические риски / Э. Л. Сидоренко, В. К. Шайдуллина, С. А. Киракосян. – Текст : непосредственный // Уголь. – 2018. – № 12. – С. 54–58. – Библиогр.: с. 57–58 (13 назв.).

36. Спасенников, Б. А. Актуальные проблемы уголовного права: обзор литературы / Б. А. Спасенников. – Текст : непосредственный //

Актуальные вопросы образования и науки. – 2015. – № 1-2 (47-48). – С. 36–38. – Библиогр.: с. 38 (6 назв.).

37. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ.

38. Целых, А. А. Современные технологии противодействия финансовым преступлениям: учебное пособие / А. А. Целых, А. Н. Целых, Э. М. Котов; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2019. – С. 91–94. – ISBN: 978-5-9275-3285-6 – Текст : непосредственный.

39. Цихилов, А. Блокчейн. Принципы и основы. – Москва : Интеллектуальная литература, 2019. – 192 с. – ISBN 978-5-6042880-1-6 – Текст : непосредственный.

40. Цыпленкова, М. В. Основы менеджмента : учебное пособие. [Электронный ресурс]. / М. В. Цыпленкова, И. В. Моисеенко, Н. В. Гуремина, Ю. А. Бондарь // URL : http://www.rae.ru/monographs/211-6578 (дата обращения: 17.08.2021).

41. Что такое хешрейт и сложность майнинга криптовалют? – URL : https://forklog.com/chto-takoe-heshrejt-i-slozhnost-majninga-kriptovalyut (дата об-ращения: 19.08.2021).

42. 10 проблем и рисков криптовалют // НПП «ГАРАНТ-СЕРВИС» [сайт], 05.12.2017. – URL : https://www.garant.ru/article/1150927 (дата обращения: 01.11.2019).

43. Cox J. Staying in the Shadows: The Use of Bitcoin and Encryption in Cryptomarkets / J. Cox // The Internet and Drug Markets. – Lisbon : EMCDDA, 2016. – P. 41–47.

44. Foley S. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? [Electronic resource] / S. Foley, J. R. Karlsen, T. J. Putnins. – URL : https://papers.ssrn.com /sol3/papers.cfm?abstract_id=3102645 (дата обращения: 17.08.2021).

45. Milosh, D. V. Digital of financial assets: current state and forecast of development at the global level on the example of cryptocurrencies / D. V. Milosh, V. P. Gerasenko // Corporate governance and innovative economic development of the north: bulletin of research center of corporate law, management and venture investment of Syktyvkar State University. – 2020. – № 4. – P. 99–104.

46. Popper, N. Leading Online Black Markets Are Shut down by Authorities / N. Popper, R. Ruiz // The New York Times. – 2017. – July 20.

47. Syporyatov V. A., Maskaev, A. I. Evolution of the institutional structure of private money in the form of cryptocurrencies — development models and controversy with Hayek's = Эволюция институциональной структуры частных денег в форме криптовалют — модели развития и полемика с позицией Хайека / В. А. Сыропятов, А. И. Маскаев. – Текст : непосредственный // Journal of economic regulation (Вопросы регулирования экономики). – 2020. – Vol. 11. – № 3. P. 40–43. – Doi : 10.17835/2078-5429.2020.11.3.038-048.

48. Williams, K. S. Textbook on Criminology / K. S. Williams. – Oxford : Univ. Press, 2012. – 640 p.

49. World Population Clock: 7.74 Billion People // Worldometers, 2019. – URL : https://www.worldometers.info (дата обращения: 01.11.2019).

50. URL : https://www.group-ib.ru/media/gib-crypto-summary/ (дата обращения: 17.08.2021).

51. URL : https://utmagazine.ru/posts/21785-kriptovaly-uty-v-nelegalnoy-deyatelnosti / (дата обращения: 12.08.2021).

52. URL : https://habr.com/ru/post/319868/ (дата обращения: 17.08.2021).

53. URL : https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0/ (дата обращения: 17.08.2021).

54. URL : https://en.wikipedia.org/wiki/Key-agreement_protocol / (дата обращения: 10.08.2021).

55. URL : https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1% 81%D0%B0_%D0%B8_%D0%91%D0%BE%D0%B1 / (дата обращения: 11.08.2021).

56. URL : https://ru.wikipedia.org/wiki/Triple_DES/ (дата обращения: 16.08.2021).

57. URL : https://en.wikipedia.org/wiki/Digital_Signature_Algorithm / (дата обращения: 19.08.2021).

58. URL : https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%85%D0%B5%D1%88%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F/ (дата обращения: 18.08.2021).

59.URL : https://cbr.ru/Content/Document/File/104942/Directive%20(rus)%202015_849.pdf (дата обращения: 17.08.2021).

60. URL: https://cryptowiki.ru/article/nikolai-patryshev-rasskazal-ob-otnoshenii-sovbeza-rf-k-kriptovalutam.html?ysclid=lgxo3tv5zs347250493 (дата обращения: 17.08.2021).

61 URL: https://iz.ru/news/717485?ysclid=lgxnuv8ikd408365541 (дата обращения: 17.08.2021).

62. URL : https://habr.com/ru/articles/143587/ (дата обращения: 17.08.2021).

63. URL : https://www.interfax.ru/business/581900 (дата обращения: 17.08.2021).

64. URL : https://iz.ru/news/717485?ysclid=lgxnuv8ikd408365541 (дата обращения: 17.08.2021).

65. URL : https://cryptowiki.ru/article/nikolai-patryshev-rasskazal-ob-otnoshenii-sovbeza-rf-k-kriptovalutam.html?ysclid=lgxo3tv5zs347250493 (дата обращения: 17.08.2021).

66. URL: https://habr.com/ru/articles/143587/ (дата обращения: 17.08.2021).

67 URL: http://www.kremlin.ru/events/president/transcripts/deliberations/55813 (дата обращения: 17.08.2021).

68 URL: https://news.myseldon.com/ru/news/index/177667657 (дата обращения: 17.08.2021).

69. URL: https://minfin.gov.ru/ru/document/?id_4=121810-proekt-federalnogo-zakona_o_tsifrovykh_finansovykh_aktivakh&ysclid=lgxoqikua71640532 (дата обращения: 17.08.2021).

70. URL: https://www.garant.ru/news/1448450/?ysclid=lgxp23c1vh973972938 (дата обращения: 31.05.2022).

71. URL: https://tass.ru/ekonomika/14781541?ysclid=lgxpfqd4sh78507928&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 31.05.2022).

72. URL: https://www.rbc.ru/crypto/news/629734ef9a7947211379062f?ysclid=lgxqe1bvv9147172668 (дата обращения: 01.06.2022).

73. URL: https://cryptocurrency.tech/chto-dumayut-eksperty-o-predlozhenii-vvedeniya-mezhdunarodnyh-raschetov-v-kriptovalyute-v-rf/?ysclid=lgxqrn7rg3719341757 (дата обращения: 01.06.2022).

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Научное издание

Примакин Алексей Иванович,
доктор технических наук, профессор;
Локнов Алексей Игоревич,
кандидат технических наук;
Васильева Ирина Николаевна,
кандидат физико-математических наук, доцент;
Родин Владимир Николаевич,
кандидат технических наук, доцент;
Чудаков Олег Евгеньевич,
доктор технических наук, профессор

ТЕХНОЛОГИИ КРИПТОВАЛЮТ

Монография

Редактор *Артамонов Р. Е.*
Компьютерная верстка *Артамонов Р. Е.*
Дизайн обложки *Шеряй А. Н.*

ISBN 978-5-91837-713-0

EDN XJXKTL

Подписано в печать 05.05.2023. Формат 60×84 $^{1}/_{16}$
Печать цифровая. Объем 10 п. л. Тираж 50 экз. Заказ № 23/23

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1.