ЕЛЕНА ЛАРИНА, ВЛАДИМИР ОВЧИНСКИЙ

КРИПТОВАЛЮТА: СВЕТ И ТЕНИ

Сейчас тема криптовалют по популярности соперничает с батлами рэперов. Многие воспринимают криптовалютную лихорадку как что-то модное, преходящее. Многие гуру-экономисты тут же вспоминают Нидерланды XVII века, когда луковицы тюльпанов продавались по цене домов. Российскому населению, с изумлением наблюдающему за биткойном, на ум приходят МММ с С. Мавроди и другие пирамиды 90-х.

Однако о биткойне и блокчейне не стоит судить поверхностно. Они появились в нашей жизни не случайно. Пришли надолго. Прежде всего, детективная завязка. Биткойн появился в 2008 году. Это год глобального финансово-экономического кризиса. Его создал человек или группа людей, которые до сих пор не известны. Долгое время, вплоть до 2013 года про биткойн и криптовалюты слышали только шифропанки, хакеры и компьютерные фанаты. Да и то не все. Между тем, биткойн – это плод не просто огромной работы, а соединения идей, высказанных задолго до создания первой криптовалюты.

Чтобы понять важность этих идей и сложность их упаковки в один продукт, разберёмся, что такое биткойн и другие криптовалюты. Некоторые считают, что это компьютерный код. Другие полагают, что это своего рода мания, предмет спекуляции. Третьи что-то рассказывают про шифры. Четвёртые – про протоколы. В итоге, основная часть публики, не погружённая глубоко в программирование и хайтек, вообще не понимает, что происходит в глобальном масштабе у них на глазах. С испугом и растерянностью люди во всём мире наблюдают, как буквально за два года из ничего вырос огромный рынок. Сейчас он оценивается примерно в 120 млрд долларов.

По сути, биткойн и другие мощные криптовалюты – это огромный распределённый компьютер. Он состоит из связанных сетью и оснащённых специальными программами компьютеров всех, кто участвует в транзакциях. Теперь посмотрим, что нужно распределённому компьютеру для работы. Прежде всего, сами компьютеры, провайдеры, которые обеспечивают связь, и желание людей за компьютерами поддерживать сеть и что-то в ней делать. Выделим главные составляющие криптовалюты.

Первое. Как это ни парадоксально, криптовалютная революция – это не революция, а контрреволюция. Общедоступный интернет появился в мире на рубеже 80–90-х годов, а активно стал развиваться в начале 90-х годов. Интернет – это иерархическая структура. Он держится на корневых серверах, скрепляющих всю всемирную паутину. Это и есть сеть интернет. Однако задолго до интернета появились одноранговые сети. Это сети, где все участники обладали равными правами и передавали друг другу сигналы с компьютера на компьютер. Криптовалюты используют именно одноранговые, или, как

их ещё называют, P2P сети (равный к равному). В сети – как в жизни: если есть иерархия, то есть начальник или хозяин. Такие сети работают быстрее, тогда их участники полностью зависят от хозяев интернета.

Второе. Интернет в значительной степени стал тем, что он есть, благодаря протоколу передачи данных http. Обязательная составляющая любой криптовалюты – блокчейн – это и есть другой протокол. Он предназначен не для передачи гипертекстов (кликабельных текстов и др. информации), а для передачи транзакций (перевода денег, передачи прав собственности и т. п.). Блокчейн – это своеобразный интернет денег.

Третье. При любом взаимодействии есть ключевая проблема. Это проблема доверия. Вообще вся нынешняя экономика в значительной мере родилась в рамках решения проблемы доверия. Внутри семьи, особенно традиционной, такой проблемы нет. А даже между хорошо знакомыми людьми она возникает. Нынешняя денежная система, бухгалтерский учёт, да и юридические нормы решают в значительной степени проблему доверия. Решают путём писаных норм и наказаний за их нарушение. Биткойн с первых дней своего существования решал ключевую задачу – обеспечить взаимодействие кого угодно в условиях неполного доверия. Был написан программный код протокола – блокчейн, – который обеспечивает автоматическое выполнение транзакций (любых сделок, переводов) лишь тогда и если стороны выполняют предусмотренные программами условия. Они могут быть какие угодно.

Четвёртое. Бухгалтерский учёт. Бухгалтерия пронизывает всю нашу жизнь. Без неё мы никуда. Уже почти 500 лет мы пользуемся двойной бухгалтерией и сводим дебет с кредитом, убытки с доходами. При этом существуют огромные армии бухгалтеров и юристов. Они следят за тем, чтобы бухгалтерия велась правильно. Несмотря на это, ежегодно мир сотрясают скандалы, когда крупнейшим компаниям удаётся годами вести поддельную бухгалтерию. Ещё в конце 80-х годов прошлого века была создана трёхсторонняя бухгалтерия. К дебету и кредиту была добавлена третья запись – транзакция. По сути, сеть криптовалют – это не только огромный распределённый компьютер, но и огромная база данных, в том числе бухгалтерия. В ней запомнены все транзакции. Деньги просто не могут исчезнуть бесследно. Они всегда приходят с одного адреса на другой. Эту транзакцию невозможно забыть, стереть или подправить. Она общедоступна для всей сети.

Пятое. Для того, чтобы гигантский распределённый компьютер работал, у его участников должен быть интерес. Кто-то должен расходовать электроэнергию, использовать свои компьютеры для поддержания работы сети, осуществления шифрования для того, чтобы никто не мог подделать ни одну транзакцию. Вот в этом-то пункте к протоколу и всему остальному добавляется криптовалюта.

Как предположили авторы данной статьи в нашей книге “Кибервойны XXI века. О чём умолчал Сноуден”, группа очень непростых и неслучайных разработчиков и людей из элит связала создание и поддержание сети с интересом. Чтобы была сеть, недостаточно провайдера. Надо, чтобы работали компьютеры и использовались их мощности. Тогда создатель (-ли) блокчейна и придумали биткойн. Они предусмотрели дополнительно к протоколу программу, по сути, код, которому придаётся определённая ценность. Как только появляется ценность (неважно, в чём она выражена), и люди соглашаются, что это – именно ценность, они начинают тратить свои ресурсы (в данном случае – использовать свой компьютер) на то или иное дело. Теперь просто понять, что такое майнинг. Это работа определённой программы на компьютере, которая поддерживает существование и развитие сети блокчейн. И ничего больше. Если говорить грубо, то биткойн – это внутренняя валюта сети блокчейн биткойна, виртуальная цифровая валюта, предмет интереса и вожделения майнеров. Сейчас появились другие протоколы блокчейна, привязанные к иным цифровым монетам, – Ethereum, Ripple и др.

Почему речь сначала пошла о внутренней валюте? Почему биткойн связывается с преступниками? Нельзя ли разделить блокчейн и анонимность? Здесь заключена ещё одна тайна биткойна. С первых дней существования интернета значительная часть наиболее продвинутых айтишников боролась против диктата государств и их контроля над сетью. При этом чем дальше, тем больше в борьбу были вовлечены лучшие мозги. Хакеры, одним словом. Поэтому естественно, что при разработке биткойна был сделан упор на шифрование

и анонимность. Если почитать первые обсуждения биткойна на форумах 2010–2012 годов, можно увидеть, что на тему криптовалют общались в основном хакеры, шифропанки, компьютерные анархисты и т. д. Не зря биткойн появился после восхода звезды Джулиана Ассанжа, а фантастический первый взлёт его капитализации произошёл после откровений Э. Сноудена и всемирной мании приватности.

Строго говоря, блокчейн может существовать и уже существует как шифрованный, невзламываемый, неанонимный протокол.

Более того, неанонимный блокчейн – это мечта любого правоохранителя. В мире неанонимного блокчейна не только все знают, какие транзакции происходят, но и кто кому переводит, и даже – при определённых условиях – кто, сколько и какой криптовалюты или фиатных денег (долларов, евро, франков и т. п.) имеет в кошельках.

Суть важнейшей задачи, которую решил условный Накамото*, в следующем. Для каждой сети главное – её поддержание и рост. Придумав внутреннюю валюту блокчейна – биткойн, – он заинтересовал продвинутых разработчиков, хакеров, шифропанков использовать ресурсы собственных компьютеров для поддержания сети. Для этого надо было только скачать приложение и превратить свой компьютер в элемент всемирного распределённого компьютера. При этом вначале вознаграждение было получить в разы легче, чем сейчас. В будущем будет совсем сложно.

Хитрость Накамото в том, что на программном уровне он заранее программно установил, сколько всего может быть сгенерировано биткойнов за всю историю. Кстати, именно по этой причине классический биткойн стал лишь первой ступенью ракеты, а не космическим кораблём полностью. Один биткойн никогда не сможет покрыть потребности мировой экономики.

Когда разработчики разобрались в новом программном чуде, они стали на протоколе биткойна – блокчейне – придумывать свои варианты валют. Их появилось в 2012–2014 годах немерено. Большая часть из них не выжила, поскольку ничего интересного в себе не содержала. Однако события, связанные с выпуском криптовалют "на коленке", сарафанное радио, вирусный маркетинг сделали своё дело. Информация о чём-то новом, непонятном, с какой-то внутренней ценностью стала доступной не только узким кругам продвинутых айтишников, но и преступникам, отмывателям денег, биржевым спекулянтам.

В 2014 году случился первый экспоненциальный подъём курса биткойна. Менее чем за год он поднялся с 200 до 1200 долларов и превысил цену унции золота. Затем пошёл вниз. Из внутренней валюты биткойн-блокчейна он превратился в криптовалюту – инвестиционный актив, который может купить или продать любой желающий. Прежде всего, не для того, чтобы биткойном за что-то расплачиваться, хотя это было и остаётся важной функцией, а главное, чтобы им спекулировать – покупать и продавать. В итоге биткойн де факто стал деньгами. Правда, в мире почти никто не признаёт криптовалюты за деньги. В первую очередь, не признают центральные банки. Банки и правительства называют биткойн и другие криптовалюты инвестиционным активом или особым классом товаров, но, по сути, появились именно деньги. Деньги – это не просто средство обмена. Вот что пишет о деньгах в книге "eMoney. Неофициальная биография денег" банкир и публицист Феликс Мартин: "Можно сказать, что в центре новой теории денег лежит идея кредита. Деньги – не средство обмена, а социальная конструкция, состоящая из трёх фундаментальных элементов. Первый из них – абстрактные единицы ценности, в которых измеряются деньги. Второй – система счетов, благодаря которым можно вести учёт долгов и кредитов физических лиц или учреждений и осуществлять торговлю между ними. Третий – возможность передачи кредитором полученного обязательства третьей стороне для погашения другого долга".

Деньгам не обязательно быть золотом или серебром. Уже в XVIII веке они сбросили вещественную форму и стали бумажными. Затем валюты превратились в программный код, передаваемый сигналами, ничем не отличающимися (за исключением юридической нормы) от биткойна. Различие в том, что эмиссии, то есть выпуск денег, могут делать только центральные банки государств или групп государств (ЕС). Больше никаких отличий сегодня нет. Более

---

* Сатоши Накамото – псевдоним человека или группы лиц, разработавших протокол криптовалюты биткойн.

того, биткойн, объём которого ограничен, хотя бы этим отличается от эмиссии долларов, евро и т. п.

О блокчейн-технологиях

Напомним, что блокчейн-технологии базируются на децентрализованных или P2P сетях с открытым исходным кодом, которые используют криптографические средства проверки транзакций и обеспечения работы сети, не полагаясь на стороннюю компанию. Криптоактивы функционируют как форма цифровых средств, позволяющих осуществлять прямые платежи и иные транзакции силами самих участников сети между собой. Они предоставляют вычислительные мощности своих компьютеров и получают за это вознаграждение в виде так называемых токенов.

В настоящее время технология блокчейн наиболее широко используется в инвестиционной сфере. Блокчейн-технология имеет также громадные перспективы за пределами инвестиционно-финансовой сферы для хранения распределённых ресурсов различного рода, проведения референдумов и голосований, повышения надёжности логистических сетей и т. п. В 2018 году по оценкам исследовательской группы Всемирного экономического форума в Давосе наиболее быстро развиваются не привычные – открытые – блокчейн-сети, типа эфириума, биткойна и т. п., а закрытые корпоративные и государственные блокчейн-сети, базирующиеся на своих уникальных протоколах. Эти сети не проводят ICO, их токены невозможно купить на криптообменных биржах, их платёжные средства не котируются в криптообменниках.

По состоянию на начало июля 2018 года общая капитализация криптовалютного рынка составила примерно 280 млрд долларов, что на порядки больше, чем в мае 2017 года. На рынке крипторесурсов продолжает доминировать биткойн, на долю которого приходится примерно две пятых от общей капитализации рынка криптовалют. При этом его доля снижается. В начале 2017 года на биткойн приходилось почти четыре пятых.

Любая инновация, а тем более высокая технология используется как в законных, так и в криминальных целях. Мало кто знает, что, например, автомобиль в США впервые был использован сначала преступниками, чтобы гарантированно оторваться от погони, а уж затем поступил в распоряжение правоохранителей. Блокчейн-технологии как технологический пакет, включающий математические, программные, юридические, финансово-экономические и социальные инновации, также используются, с одной стороны, бизнесом, государствами, гражданским обществом, а с другой – преступниками и террористами.

О противоречивых оценках криптовалюты и блокчейна свидетельствует следующий любопытный факт. В мае 2018 года одной группой экспертов Европарламента был подготовлен весьма тревожный доклад об использовании преступниками и террористами криптовалюты и технологии блокчейн. А уже в июле 2018 года другой экспертной группой для того же Европарламента выпущен доклад, в котором содержится вывод о том, что криптовалюту следует признать полноценным финансовым инструментом, а технология блокчейн делает криптовалютные транзакции относительно безопасными, прозрачными и быстрыми.

Если криптовалюты и блокчейн – это “наше всё” в “чудном новом цифровом мире”, то почему тогда всё чаще такие организации, как Интерпол, Европол, FATF (международная группа разработки финансовых мер по борьбе с отмыванием денег) бьют тревогу по поводу криминальных явлений вокруг криптовалюты и блокчейна? А Управление по наркотикам и преступности ООН вопрос об использовании преступниками криптовалюты и технологии блокчейн поставило в число первоочередных на рассмотрение очередного – 14-го Конгресса ООН по предупреждению преступности и уголовному правосудию, который состоится в 2020 году в Киото (Япония)? И почему 3 июля 2018 года пять стран – Австралия, Канада, Нидерланды, Великобритания и США объявили о создании Международного альянса J5 по борьбе с серьёзными международными преступлениями, отмыванием денег и киберпреступностью посредством использования криптовалют?

Первое, на что следует обратить внимание: основной оборот криптоактивов сегодня связан не с их использованием в качестве платёжных средств

либо ключей доступа к приложениям и сервисам, а в спекулятивных целях. Великие инвесторы, например, Уоррен Баффет и Джон Богл, чётко различают на финансовых рынках инвесторов и спекулянтов. Инвесторы вкладывают деньги на долгосрочную перспективу, стремятся так или иначе способствовать улучшению управления компанией, чьи акции они приобрели, повышению её экономических показателей. Спекулянтов же интересует только прибыль, полученная за счёт разницы цен покупки и продажи, раньше на интервале дней и часов, а с появлением торговых роботов — минут и секунд.

По сути, ещё не реализовав свою заявленную функцию, токены становятся предметом спекуляции. Более того, есть основания полагать, что значительная часть токенов вплоть до своей естественной кончины так и останется предметом операций купли-продажи между криптовалютными спекулянтами и никогда не перейдёт в функциональную фазу. Токены так и не станут реально используемыми платёжными средствами, ключами, обеспечивающими доступ к действительно работающим и нужным приложениям или электронной формой подтверждения права собственности на любой актив, признанной регуляторами.

Согласно отчёту ФБР, опубликованному в апреле 2018 года, примерно 85% токенов, в настоящее время обращающихся на криптовалютных биржах, не подкреплены какими-либо инфраструктурными решениями, пытаются реализовать заведомо ненужные потребителю проекты либо не обладают достаточным уровнем квалификации команд разработчиков. Причиной такого положения ФБР называет беспрепятственное проведение первичных предложений монет (ICO).

ICO представляют собой способ сбора средств, альтернативный венчурному капиталу. По мнению ФБР, подавляющее число инициаторов ICO уже в момент его проведения знают о нереализуемости проекта. Сотрудники ФБР, а также представители налоговых органов ряда англоговорящих государств провели анализ использования средств, полученных от ICO руководителями команд блокчейн-проектов. Выяснилось, что значительная часть средств инвесторов тратится либо на личные цели — покупку машин, домов и даже самолётов, — либо на рекламные цели, поддерживающие интерес инвесторов и широкой публики к данному токену.

Криптоактивы используются не только в мошеннических целях, но и как способ оплаты, предназначенный для криминальных онлайн и оффлайн рынков. Начиная с 2014 года IOCTA Европола пытается оценить направления и масштабы использования киберпреступниками криптовалют как платёжных средств. Согласно докладу IOCTA 2017 года, уже сегодня анонимные криптовалюты стали главным инструментом оплаты в сфере электронного вымогательства с использованием кибервирусов. Хакеры требуют биткойны в качестве оплаты при вымогательстве. По данным Европола, только в 2016 году полицейскими органами государств ЕС было зафиксировано более 50 крупномасштабных вымогательств со стороны киберпреступников. Средний размер требуемого ими выкупа составлял примерно 2 млн долларов. В 2016 году почти 16% монет были связаны с вредоносными программами, такими как Locky. В 2017 году это были WannaCry и NotPeya.

Американская компания по кибербезопасности Chainanalysis обнаружила, что в первой половине 2017 года на американских криптовалютных биржах было безвозвратно украдено 75 млн долларов. Криптообменные платформы, хотя и называют себя биржами, действуют не только вне правового поля, но и в условиях отсутствия программно-аппаратного аудита их инфраструктуры. Поэтому ежегодно несколько крупных криптовалютных бирж объявляют о своей кончине, забирая десятки миллионов долларов своих пользователей, либо сообщают о крупномасштабных кражах из кошельков, открытых пользователями биржи. В отчёте компании CipherTrace, которая выявляет финансовые преступления на основе анализа криптовалютных транзакций, за первое полугодие 2018 года с криптобирж было украдено криптовалюты в три раза больше, чем за весь 2017 год.

Ещё одной прибыльной формой киберпреступности является криптоджекинг. Преступники скрытно устанавливают на компьютере, гаджете жертвы собственное программное обеспечение и используют сторонние компьютеры, как свои собственные. Главным образом, жертвами оказываются не столько

частные лица, сколько компании и корпорации. Согласно индексу глобальной оценки угроз Агентства Reuters, как минимум 55% компаний Великобритании стали жертвами криптоджекинга. Их компьютерные мощности были задействованы киберпреступниками для проведения криминальных операций. Если несколько упростить реальную ситуацию, то можно сказать, что в то время как проекты falecoin и golem только реализуются, киберпреступники уже создали свой вариант аналогичных блокчейн-технологий и активно используют их в преступных целях. Британский Национальный Центр кибербезопасности и Национальное Агентство по борьбе с преступностью указали, что в 2018–2020 годах криптоджекинг станет одной из главных форм высокоорганизованной преступности. Первоначально криптоджекинг возник как форма использования сторонних вычислительных ресурсов для проведения майнинга. Затем майнинг был расширен на другие сферы, в том числе создание распределённых бот-сетей или компьютерных распределённых мощностей для проведения DDoS атак и других кибернападений.

Криптовалюты также являются предпочтительно формой оплаты в dark web и конкретно в сети Tor. Согласно данным Интерпола, в 2010–2016 годах в сети Tor было реализовано оружия, наркотиков, контрафактных изделий, поддельных паспортов, педофильского контента на сумму более 2 млрд долларов исключительно в криптовалютах. На ранней стадии исключительным платёжным сервисом был биткойн. Начиная с 2014 года, стала расти доля других анонимных платёжных средств, в первую очередь, Monero и Dash. Практически полностью в криптовалютах существует наиболее быстроразвивающийся криминальный рынок – сервис "преступление как услуга". Этот рынок работает подобно Amazon или eBay, что позволяет клиентам отслеживать репутацию преступных провайдеров услуг.

Имеются также данные, свидетельствующие, что криптовалюты всё чаще используются в схемах отмывания денег организованными преступными группами. По данным Европола, через криптовалюты ежегодно отмывается 3-4 млрд евро или 3-4% незаконных доходов, отмываемых ежегодно через ЕС и Великобританию. Общая сумма отмываемых средств составляет в настоящее время примерно 100 млрд долларов ежегодно, а доля использования криптовалют растёт по экспоненте. В прессе сообщалось, что колумбийские и мексиканские наркокартели широко используют анонимные криптовалюты, прежде всего, Monero и Dash для отмывания доходов, полученных в Европе от поставок из Колумбии, и США – из Мексики.

На состоявшихся в феврале-марте 2018 года встречах руководства FATF с руководством Интерпола и Европола была подтверждена полная и безусловная поддержка FATF со стороны Европола и Интерпола в работе по анализу и прогнозированию криптоэкономики и криптофинансов. Руководители Европола и Интерпола заверили, что приложат все усилия, чтобы правоохранительные органы всех стран, входящих в эти организации, в качестве приоритетной рабочей задачи занимались анализом криптоэкономики и других финансовых инноваций и пресечением их использования мошенниками, преступниками, террористами и другими деструктивными субъектами, разрушающими глобальную финансовую и экономическую систему.

Оценка рисков использования террористами и киберкриминалом криптовалют

За исключением операции ФБР по ликвидации онлайн рынка "Шёлковый путь" в сети Tor и ещё нескольких незначительных случаев, у правоохранительных органов в мире имеется лишь небольшое количество подтверждённых примеров использования криптовалют для отмывания денег и финансирования терроризма. В этой связи у экспертов, изучающих новые формы преступности, часто возникает вопрос, почему киберпреступники и террористы, активно использующие достижения высоких технологий, применительно к криптовалютам ведут себя робко и мало используют эту технологическую возможность?

В недавнем исследовании взаимосвязи криптовалют и терроризма, проведенном для Европарламента (май 2018 года), называются террористические акторы, которые должны были бы активно использовать криптовалюты, но не делают этого:

– одиночные акторы, которые не имеют официальных связей с центральными преступными или террористическими группировками, но действуют в соответствии с их призывами. Многие одиночные акторы, особенно в Европе и Северной Америке, обладают высоким уровнем компетенций в области информационных технологий и активно используют их для кибернападений;

– небольшие группы и состоящие из них сети, которые связаны с преступными ядрами и центрами террористических группировок лишь посредством онлайн связей;

– организация командования и управления без единого центра. Например, Аль-Каида – группа, контролирующая определённые территории, через такие группировки, как Боко Харам, Аль-Шааб и т. п.

Все они сосредотачивают свою активность в финансовой сфере на следующих операциях:

– сбор средств различными путями, включая криминальный краудфандинг, сбор пожертвований или изъятие средств легальных бизнесов на добровольной либо принудительной основе;

– перемещение средств в основном путём перевода финансовых ресурсов через международную банковскую структуру или официальные и неофициальные системы перевода наличных средств;

– хранение средств. Например, путём создания резервов наличных денег или размещения безналичных финансовых ресурсов в наиболее защищённых офшорных зонах типа Лихтенштейна, Арубы и Сингапура.

Согласно данным Европола, из 76 случаев террористических и преступных операций, связанных с использованием оружия в 2015–2017 годах, в 72 фигурировало использование наличных денег, а в оставшихся 4 – перевод на безналичные фиатные счета. Ни в одном из случаев не были использованы криптовалюты.

В Соединённых Штатах на сегодняшний день установлен только один случай использования криптовалют для поддержки терроризма. В июне 2015 года молодой человек из Вирджинии Али Шукри Амин был осуждён в США за предоставление материальной поддержки ИГИЛ. Получив информацию из Твиттера о закрытом портале в Tor, он перевёл несколько биткойнов на указанный на портале счёт ИГИЛ.

Что касается финансировании текущих операций крупных террористических групп, например, таких, как Аль-Каида и ИГИЛ, а также организованных преступных группировок, в 2017 – начале 2018 года не было установлено ни одного случая использования для этой цели криптовалют. Причина этого вполне очевидна. С одной стороны, подобного рода группировки, как правило, получают деньги от взимания своего рода незаконного налога с бизнесов на контролируемых территориях или возглавляемых людьми, симпатизирующими этим организациям. Всё это происходит в наличных деньгах. С другой стороны, эти сети давно установили связи с легальными банковскими институтами, через которые и проводят текущие операции. Более того, эксперты полагают, что финансовые институты знают о преступном происхождении средств и, тем не менее, открывают счета таким акторам.

По мнению экспертов Европарламента, главная причина незначительного использования террористами и организованной преступностью криптовалют заключена в нескольких обстоятельствах.

Во-первых, террористы и преступники с подозрением относятся к криптовалютам, поскольку считают биткойн созданием американского разведывательного сообщества, в состав которого входит ФБР. Они подозревают, что одной из целей создания криптовалют является перемещение преступных и террористических транзакций в эту сферу с установлением, в конечном счёте, отправителей и получателей денежных средств.

Во-вторых, террористические сети возглавляются людьми, чей средний возраст попадает в основном в промежуток от 35 до 50 лет. Эти люди не понимают сути криптовалют и, соответственно, испытывают к ним недоверие, а потому отрицательно реагируют на предложения более молодых членов террористических и преступных организаций использовать криптовалюты.

Наконец, в-третьих, ОПГ и террористы видят особо пристальный интерес международных и национальных финансовых организаций и правоохранительных структур к сфере криптовалют. Соответственно, они не хотят оказаться в поле зрения их интересов.

В то же время эксперты Европарламента полагают, что буквально в ближайшие год-два положение изменится. Террористические сети и международные преступные группировки имеют распределённый характер и действуют не только в разных странах, но и на разных континентах. Одним из главных направлений блокчейн-технологий является резкое удешевление при сохранении высокого уровня надёжности межгосударственных финансовых транзакций. Для террористических и преступных организаций так же, как и для законного бизнеса, является весьма ощутимой разница между 5–7% и 1,5-2%, которые берут за перевод соответственно банки и традиционные процессинговые компании, – с одной стороны, и платёжные системы, базирующиеся на Ripple и Stellar, – с другой. В первую очередь, использование террористами и организованной преступностью криптовалют будет происходить по линии платёжных систем, базирующихся на блокчейне.

Кроме того, из-за слабой подготовленности правоохранительных органов к работе в сфере криптовалют международная общественность, возможно, не знает о том, что организованная преступность и террористы уже активно вовлечены в сферу криптовалют, но не как пользователи технологии блокчейна, а как хозяева групп, которые в 2016–2018 годах провели ICO. Согласно оценке Банка международных расчётов, примерно 90% ICO носят либо мошеннический, либо дилетантский характер. При этом, только в 2017 году за счёт ICO было извлечено 8 млрд долларов. Поскольку ICO никак не регулируются, то команды, проводившие ICO, не несут никакой ответственности перед лицами, вложившими деньги.

Всего в 2017–2018 годах была сделана попытка реализовать почти 960 проектов ICO. 194 проекта не справились и закрылись либо на стадии предпродажи токенов, либо сразу после проведения неудачного ICO. 282 проекта перестали обновлять свои сайты, публиковать новости в блогах, не отвечают на контакты. Таким образом, половина проектов ICO приказала долго жить. По нашим данным, включающим и первый квартал текущего года, сумма прямых потерь инвесторов составила 140–150 млн долларов. Кроме указанных проектов, по нашим данным, ещё 131 проект имеют незначительное число подписчиков в социальных сетях и коммуникаторах, общаются с сообществами от случая к случаю и не обновляют блоги. С чрезвычайно высокой степенью вероятности можно говорить, что эти проекты так же уверенно двигаются по пути к катастрофе. Таким образом, почти две трети, а точнее – около 63% блокчейн-проектов, осуществивших ICO, либо уже мертвы, либо отправятся в ближайшее время на цифровое кладбище.

Политические экстремисты гораздо чаще, чем террористы, используют высокие технологии. По данным ФБР, на конец 2016 года ультраправые американские экстремисты активно использовали биткойны и анонимные криптовалюты для сбора средств. В последнем докладе Европола о ситуации с терроризмом, выпущенном в 2017 году, отмечается, что правые политические нерелигиозные экстремисты собирают пожертвования на закрытых сайтах в биткойнах и Dash.

По мнению экспертов Европарламента, наиболее вероятным направлением использования террористическими акторами блокчейн-решений будут уже во второй половине 2018 года основанные на блокчейне платёжные сервисы. Террористов и организованных преступников, помимо дешевизны, к подобного рода сервисам влечёт отсутствие регулятора. Не только банковские и карточные платёжные сервисы предусматривают контроль со стороны центральных банков либо министерств финансов, но и такие платёжные электронные сервисы, как PayPal. Блокчейн платёжные сервисы реализуются в протоколах P2P и не позволяют правоохранительным органам или органам банковского контроля отслеживать, а тем более блокировать подобного рода транзакции.

Наибольшую опасность в этом плане представляют беженцы из районов Ближнего и Среднего Востока – от Сирии до Афганистана.

Согласно исследованиям Корнельского и Бристольского университетов, эмигрантам с Ближнего Востока в среднем необходимо два-три года для полной адаптации в местах нового проживания, обретения навыков использования в полном масштабе даров информационно-коммуникационных технологий. Поскольку поток мигрантов в Европу начался в 2011 году, а массовые масштабы принял с 2014-м, то в 2018 году можно ожидать, что значительная часть платежей легальных и нелегальных мигрантов из Европы в страны

Ближнего Востока будет так или иначе контролироваться террористическими сетями и албанскими и другими ОПГ с господствующим мусульманским вероисповеданием в странах ЕС.

Что касается высокотехнологичного бизнеса, то здесь ситуация иная. Например, ФБР стало известно, что мексиканский наркокартель Зетас, основное ядро которого составляют бывшие военные и полицейские, в настоящее время контролирует сеть из нескольких десятков банкоматов, где можно обменять биткойны и другие криптовалюты на мексиканские песо. Известно, что колумбийские наркоторговцы в 2017 году зондировали вопрос о приобретении базирующейся в Польше криптовалютной биржи. Благодаря усилиям польской полиции и Европола, эта попытка была пресечена.

Гораздо большую озабоченность вызывает феномен блокчейн-преступности. Сегодня с полным основанием можно говорить о том, что наряду с киберпреступностью появилась блокчейн-преступность. Блокчейн-преступность, строго говоря, не является частью киберпреступности. Объясняется это тем, что блокчейн – это не только программное решение, относящееся к киберсреде, но и одновременно финансовая, организационная, бухгалтерская и даже правовая инновация. Кроме того, в отличие от киберрешений, блокчейн фантастически привлекателен для поколения 20–30-летних как способ быстрого делания денег.

Для того чтобы дать представление о масштабах и темпах роста блокчейн-преступности, приведём некоторые цифры. По данным Британской банковской ассоциации, за 2012–2017 годы инвесторы из-за краж платёжных кошельков или взломов криптобирж потеряли средства, приближающиеся к 2,5 млрд долларов. В том же исследовании Британской банковской ассоциации указывается, что в 2015–2017 годах объём преступлений, связанных с блокчейн-проектами, рос темпами 370% в год. Приведённые данные показывают, что, по крайней мере, сегодня и на ближайшую перспективу главная проблема – это не использование террористами блокчейн-технологий, а использование блокчейн-технологий высокотехнологичными преступниками. Криптоэкономика, подобно любому экономическому сектору, создала возможности для появления внутренней преступности, которая действует в самом секторе, глубоко зная его писаные и неписаные традиции и разбираясь в хитросплетениях инноваций на порядок лучше правоохранителей.

В значительной степени сегодня для преступников и террористов возможность воспользоваться преимуществами децентрализации зависит от готовности блокчейн-предприятий, прежде всего, криптообменных бирж, принять на себя требования, предъявляемые к финансовым институтам в той или иной юрисдикции. Наибольший оборот криптообменов осуществляется на биржах США, Гонконга и Японии. Практически все эти биржи приняли на себя обязательства реализовывать правило “знай своего клиента” и предоставляют по требованию правоохранительным органам данные о транзакциях.

В то же время вызывают опасение планы создания криптообменных бирж в регионах, где не соблюдается международное законодательство и плохо реализуются меры по борьбе с оффшорами. В первую очередь, это относится к Центральной Америке и некоторым Латиноамериканским странам. Приведённые выше случаи, а также статистические данные свидетельствуют о небольших пока масштабах и спорадическом использовании криптовалют террористами, политическими экстремистами и низкотехнологичными организованными преступниками.

В настоящее время основные риски развития преступности лежат не вовне, а внутри блокчейн-экономики. Сама по себе блокчейн-экономика достаточно криминализирована. Террористические акторы, стремящиеся работать в онлайн средах, требующих комбинации анонимности и децентрализации, пока предпочитают пользоваться допотопной Хавалой и другими подобными схемами, а не технически сложными, требующими квалификации блокчейн-решениями. Однако это положение неизбежно в ближайшее время изменится.

Что делать?

В июне 2015 года FATF опубликовал подробные рекомендации по борьбе с отмыванием денег и рисками, связанными с использованием криптовалют. К настоящему времени эти рекомендации, особенно в части криптовалют,

по мнению многих экспертов уже несколько устарели. Поэтому FATF в этом году готовится выпустить новые стандарты противодействия легализации преступных доходов и финансирования терроризма с помощью криптовалютных операций.

В разных странах наблюдается разнобой в регулировании. Едва ли не самая противоречивая политика в отношении блокчейна и криптовалют реализуется в России. С одной стороны, российские правоохранительные органы и Министерство финансов требовали принятия законодательства, предусматривающего полный запрет частных блокчейн-сетей и проектов, а также установления табу на использование биткойна как "суррогата денег". В период с 2014-го по 2017 годы Центральный банк РФ постоянно предупреждал физических и юридических лиц о проблемах, с которыми они могут столкнуться не только со стороны блокчейн-мошенников, но и правоохранительных органов из-за анонимного характера криптовалют и высокой вероятности невольного вовлечения в незаконную деятельность, прежде всего, связанную с отмыванием денег. Руководители финансовых и правоохранительных органов в период с 2014-го по первую половину 2017 года выступали за введение уголовного наказания за использование анонимных криптовалют, а также за участие в ICO за пределами России без выплаты налогов.

С другой стороны, президент России В. Путин стал единственным лидером стран G20, который имел встречу с Виталиком Бутериным и представителями фонда "Эфириум". После встречи позиция ЦБ, Минфина и правоохранительных органов заметно изменилась. Она состоит в том, что токены рассматриваются не как денежные суррогаты, а как инвестиционные активы или инвестиционные товары, которые могут приобретаться, храниться, покупаться и продаваться российскими гражданами.

В настоящее время в Госдуме рассматривается три законопроекта – о цифровых финансовых активах (криптовалютах), о привлечении инвестиций с использованием инвестиционных платформ (краудфандинг). Первый законопроект даёт определение цифровых финансовых активов, относя к ним криптовалюту и токен, и законодательно закрепляет новый вид договора, заключаемого в электронной форме, – смарт-контракт, исполнение обязательств по которому осуществляется с использованием цифровых финансовых технологий. Второй законопроект регулирует отношения по привлечению инвестиций юрлицами или индивидуальными предпринимателями посредством инвестплатформ и определяет правовые основы деятельности операторов таких платформ. Третий – вводит в гражданское законодательство понятие "цифровое право" и "цифровые деньги" (в обиходе – криптовалюта). Согласно законопроектам, российским гражданам будет разрешено участвовать в криптоэкономике, а российским предпринимателям дадут возможность заниматься блокчейн-проектами в России и за рубежом. В целом нынешнее отношение России к криптовалютам можно считать инновационным и лояльным, даже более лояльным, чем в США.

По состоянию на первое полугодие 2018 года ЕС имеет наиболее развитое и непротиворечивое законодательство по блокчейн-экономике. Главная направленность этого законодательства – блокировка возможностей для высокотехнологичных преступников развернуть в Европе блокчейн-преступность или использовать криптовалюты в операциях киберпреступников или террористов.

ЕС и Европол поддерживают, и более того – считают необходимым создание в ближайшее время общеевропейских и национальных частно-государственных партнёрств содействия блокчейн-экономике. Одной из главных функций этих партнёрств должно стать очищение отрасли от криминала, связей с терроризмом и недопущение превращения криптоэкономики в базу блокчейн-преступности. Имеется в виду, что такой подход позволит сочетать имеющиеся у правоохранительных органов информационные, расследовательские и силовые возможности с программно-аппаратной базой и финансовыми ресурсами, которыми располагает блокчейн-отрасль.

Также Европол и ряд комиссий ЕС полагают необходимым ввести в официальный оборот тщательно отредактированный термин "блокчейн-криминал", выделив его из киберпреступности. Блокчейн-криминал имеет собственные отличительные черты, сферу деятельности – блокчейн-экономику – и специфические формы реализации – мошеннические ICO, манипуляции рынками токенов, кражу клиентских средств и т. п.

По мнению Европола, определение, а тем более борьба с блокчейн-преступностью не должны быть делом исключительно правоохранительных и судебных органов и структур ЕС. К этой работе изначально должны быть привлечены как равные партнёры представители блокчейн-бизнеса, университеты и исследовательские центры, анализирующие криптоэкономику и подготавливающие новые решения в области одноранговых транзакций, криптографии, юридических решений, связанных со смарт-контрактами и т. п.

Анализ практики развития криптоотрасли предполагает, что законодатели и правоохранители должны перестать видеть в криптоиндустрии неизбежное зло, с которым надо бороться всеми возможными методами, непрерывно ужесточая законодательство и практику правоприменения. Сегодня, а тем более завтра главной задачей становится вычленение внутри криптоиндустрии технологий, сегментов и практик, которые использует уже сформировавшаяся блокчейн-преступность и в которых заинтересована киберпреступность, традиционные ОПГ, коррумпированное чиновничество, отмывающее деньги, и террористы всех мастей. Отрасль уже накопила эмпирические данные, позволяющие правоохранительным и законодательным органам вести целевую адресную работу по сокращению, а в идеале — по пресечению блокчейн-технологий и организационных решений, порождающих криптопреступность, и необходимых для террористов и организованной преступности.

Криптоотрасль развивается на основе комплекса сложных технологий, которые должны регулироваться принципиально новыми правоохранительными нормами и процедурами.

К сожалению, приходится констатировать, что на сегодняшний день незаконные субъекты, прежде всего, криптопреступники адаптируются, и более того, в каком-то смысле развивают блокчейн-технологии существенно быстрее, чем правоохранительные и законодательные органы вникают и понимают эти технологии, а соответственно — принимают решения.

Поэтому сегодня крайне важно, в том числе и для России, чтобы государство обеспечило эффективную работу по повышению уровня компетенций сотрудников правоохранительных органов в области блокчейн-экономики.

Необходимо разработать учебные программы и практические базовые технические курсы для всех правоохранителей, занятых борьбой с блокчейн-преступностью. Следует поддержать предложения Европола сформировать в полиции государств Европы специализированные группы или межведомственные команды по борьбе с блокчейн-преступностью, укомплектовав их специалистами, обладающими профессиональными знаниями блокчейн-технологий.

Целесообразно на международном и национальном уровне создать постоянно пополняемые базы данных, касающиеся всех аспектов блокчейн-криминала как в плане используемых технологий, так и в контексте субъектов преступности, включая ОПГ и отдельных криптопреступников.

Наряду с учётной и информационно-аналитической компонентами повышения уровня готовности правоохранителей противодействию блокчейн-преступлениям и использованию криптоотрасли террористами, большое значение имеет разведывательная работа. Благодаря специфике блокчейн-отрасли, у правоохранителей есть все необходимые предпосылки для качественного улучшения разведывательной работы и повышения уровня осведомлённости.

В блокчейн-отрасли, как ни в одной другой сфере высоких технологий, популярны локальные и глобальные, закрытые и открытые встречи, симпозиумы, конференции, хакатоны по различным аспектам криптоиндустрии и блокчейн-экономики. Кроме того, существует множество медиа и распределённых социальных площадок для обмена мнениями по вопросам криптоэкономики и блокчейн-инвестирования. До настоящего времени правоохранительные органы явно недостаточно используют возможность работы в открытой среде. Без изменения положения создать обширную, постоянно пополняемую и детальную базу данных по блокчейн-криминалу и сращиванию блокчейн-индустрии в лице отдельных её представителей и команд с ОПГ и криминалом не представляется возможным. Поэтому наряду со сквозным обучением, созданием информационным банков, оперативно-розыскная деятельность должна стать третьим основным направлением работы в ближайшее время.