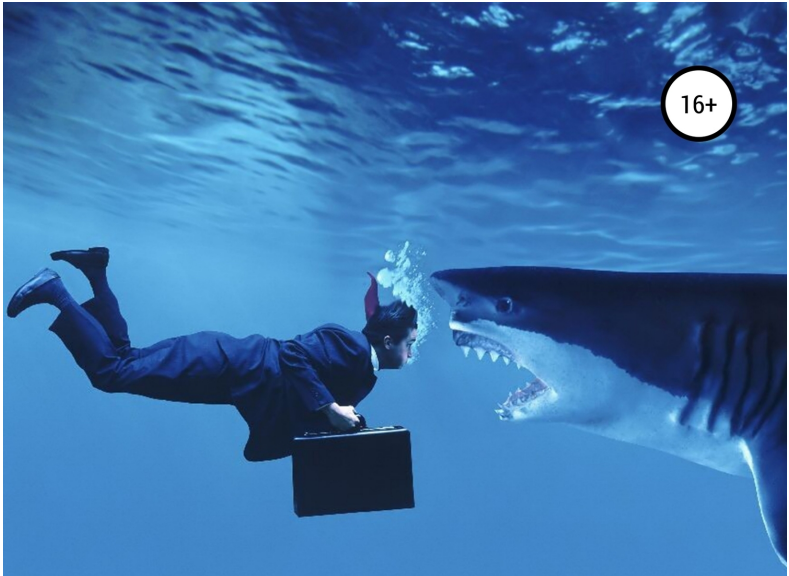

Александр Самарин

Новичок в ICO

Техника финансовой гигиены

Александр Михайлович Самарин

Новичок в ICO. Техника финансовой гигиены

http://www.litres.ru/pages/biblio_book/?art=24721063
SelfPub; 2020
ISBN 978-5-532-04336-7

Аннотация

Для новичка вложения в ICO обещают немыслимую прибыль и он, сломя голову, несется к своему компьютеру покупать волшебные токены ICO, не зная о рисках, которые несут биржа, брокер и трейдеры. Книга рассматривает вопросы о возникновении доверия к компании ICO, перечисление рисков, заставляет рассмотреть некоторые аспекты безопасности, включая информационную. Как не потерять деньги инвестору в начавшейся кампании ICO и определить объект достойный вложения средств? Эта книга ответит на ряд непростых вопросов о вложениях в блокчейн проекты. Praemonitus praemunitus – предупрежден, значит вооружен.

Содержание

Новичок в ICO. Техника финансовой гигиены.

Некоторые отличия IPO и ICO

Базовая информация о проекте ICO

Самостоятельная удаленная проверка компании ICO и вэб-сайта

Технологии криптовалют, как фактор риска в проекте ICO

Аудит информационной безопасности проекта ICO

Безопасность собственного рабочего места участника ICO

Коммуникации (общение), поиск и мониторинг событий

Словарь криптовалютных терминов

Список основных криптовалют (аббревиатуры)

Автор выражает
искреннюю благодарность
своим коллегам и друзьям, которые
помогли написать эту книгу.

Некоторые отличия IPO и ICO

Развитие информационных технологий делает весь финансовый мир теснее, устраняя посредников в виде банков, страховщиков и нотариусов. Старейшие биржи, ядром которых являлись торговые площадки продавцов и покупателей, уходят в интернет и трансформируются в виртуальные сообщества. Если раньше классические биржи привлекали инвесторов через размещение акций, то и сегодня этот механизм подвергается существенным изменениям, обходя преграды и кордоны столетиями возводимые государством. Особенно процесс изменения заметен при сравнении IPO и ICO, когда инвестором, вместо искушенного финансового брокера, становится простой пользователь компьютера.

IPO *(Initial Public Offer)* – привлечение средств, путем продажи акций через уполномоченных посредников, которые (не безвозмездно) делают ценные бумаги эмитента доступными для любого клиента, имеющего финансовые средства. Следует отметить, что на биржу IPO компании выходят с уже известным брэндом, готовым продуктом и их активность, в большинстве случаев, соответствует требованиям государственных регуляторов. Зачастую инвесторы посредством приобретения акций покупают долю в компании, которая им уже хорошо знакома, имеет специальные лицензии и некоторый рынок, развивающийся или расширяющий-

ся, чтобы впоследствии его захватить, о чем говорят реальные и прогнозируемые экономические показатели. И вдруг, появляется новый механизм ICO.

ICO (Initial Coin Offer) – привлечение средств, обычно без посредников (их упраздняет Интернет), для реализации проекта путём продажи запатентованной цифровой валюты – токенов, причем, эта цифровая валюта (криптовалюта) может еще не участвовать в обращении в финансовом мире. В общем случае, токены имеют определенную ценность, иногда могут продаваться на бирже или предоставлять различные преференции и даже приносить доход их покупателям. Но – это обусловлено доверием, которое в нашем мире формируется рекламой, новостями о компании ICO, ее технологиях или составе участников. Биржу заменил Интернет, брокеры отсутствуют, государственный регулятор только начинает задумываться о словарном определении криптовалют, которых уже несколько тысяч. Отметим, что сравнительна легкая реализация и доступность процесса ICO является одним из главных преимуществ перед IPO.

Для инвестора-обывателя вложения в ICO обещают немыслимую прибыль и он, сломя голову, несется к своему компьютеру покупать волшебные токены ICO, не зная о рисках, которые в IPO несут биржа, брокер и всевидящий регулятор.

Базовая информация о проекте ICO

Рассматривая вопрос о возникновении доверия к компании ICO, постараемся представить множество рисков и рассмотреть некоторые аспекты безопасности, включая финансовую и информационную.

Начнем с лица компании ICO, с ее вэб-сайта, если такой существует. Для примера возьмем вымышленную компанию «БУМ», которая вышла на рынок ICO с токеном «бумкоин».

Введение, описание проекта, для чего создан «бумкоин»

Наивно надеяться на объективность рекламы при вложении финансов даже в популярные, раскрученные проекты. Консалтинговые агентства, привлекая инвестиции в ICO, используют самые разнообразные методики для вовлечения клиентов. И все же существуют общие этапы реализации ICO проекта, которые дают возможность понять, кто и для чего собирает деньги инвесторов.

Наиболее типичный случай, когда реальные компании или предприниматели привлекают дополнительные инвестиции для перевода части своего бизнеса на технологию блокчейн. В качестве первого шага в большинстве проектов выполняется проработка экономической модели, где происхо-

дит экономическое обоснование и осмысление необходимости появления токена, как выгодного продукта. Какие услуги может предоставить токен, кто является потенциальным потребителем этих услуг, в чем выгода вложения средств и каковы перспективы развития данного проекта ICO?

Уделив этим вопросам пристальное внимание, инвестор получит положительные или отрицательные аргументы для решения о вложении средств.

Следующим шагом является маркетинговое исследование рынка, которое определяет соответствующие ниши выпускаемого токена. Аналитики ICO проекта редко раскрывают реальные показатели предполагаемого рынка. И это понятно. Любой конкурент может применить информацию маркетингового исследования в свою пользу, тем более, если имеет превосходящую финансовую поддержку. Таким образом, частному инвестору стоит самостоятельно проводить анализ и учитывать любые намеки на потенциал, который может скрывать рыночная ниша выпускаемого токена ICO.

Финальным этапом является собственно вывод ICO проекта в свет. Скорость и оперативность тщательно подготовленного выпуска нового токена являются сами по себе прекрасными показателями перспективности идеи и проекта. Если объем и/или количество выпускаемых токенов ограничено, то адекватное решение инвестору необходимо принимать быстро. Но, с учетом выявленных рисков, согласно вашему чек-листу.

Параметры ICO. Сроки проведения, участники

Коммерческий потенциал ICO проекта является одним из важнейших параметров и имеет свои составляющие, которые проявляются явно или косвенно.

Например, показательно, каким образом владельцы проекта освещают обоснованность проведения ICO? Какими средствами организуют диалог с потенциальными инвесторами? Хорошо, если владельцы проекта четко обозначают сумму инвестиций, которую они хотят получить в ходе проведения ICO, а также публично представляют персоналии ключевых участников проекта. Это может вызвать определенную степень доверия у инвесторов, если личности хорошо знакомы и популярны.

Косвенно на успех размещения будет влиять некоторая информация, которую инвестору довольно сложно проверить. Например, сообщения о том, что собираемые средства будут вложены в развитие бизнеса, или существует некая декларация о намерении депонировать часть токенов на длительный срок с целью сохранить потенциал на старте проекта, а в дальнейшем регулировать спрос на размещаемые и существующие токены проекта.

Некоторую информацию можно извлечь, анализируя спецификацию криптовалюты (после размещения токенов). До-

полнительные детали могут быть скрыты в символике, алгоритме майнинга и адресе пула (если токен майнится). Не лишним будет обратить внимание на биржи для размещения, ограничения на этих биржах и прочие скрытые детали и особенности.

Whitepaper (белая бумага)

Whitepaper является обязательным атрибутом любого ICO проекта. Это публичный всеобъемлющий документ рассказывающий, каким образом будет работать технологический механизм блокчейн-проекта. Немного найдется желающих инвестировать в проект без внятного грамотного описания ключевых принципов работы денежных вложений.

Для доверительного общения с инвесторами владельцы проекта часто излагают реальную или правдоподобную историю, с чего всё начиналось. Ретроспективная информация может психологически преувеличивать темпы роста и изобразить фантастический прорыв в будущее. Будьте внимательны к своим эмоциям. Внимательно проверяйте информацию. Если есть возможность, обратитесь к истории идеи проекта и сделайте это тщательно. Идея может оказаться устаревшей или даже иметь другого создателя.

Whitepaper должна представить описание ниши рынка и применимость технологии блокчейна на данном рынке. Развернутая информация должна дать вам понимание, что ана-

лиз рынка выполнен качественно, что существует реальный потенциал рынка и его, в момент запуска проекта, не захватили более продвинутые конкуренты.

Об отношении к инвесторам прямо говорит подробное описание продукта, перечисление особенностей сервисов, реализуемых в ходе проекта, а также детальные таблицы или графики, отражающие тенденции показателей и степень продвижения проекта. Хорошим тоном можно назвать информирование инвесторов о прошлых или будущих практиках применения токенов, аналогичных токену стартовавшего проекта ICO.

Обратите внимание на то, что называется предварительным привлечением инвестиций (pre-ICO). Сопоставление результатов pre-ICO и показателей, декларируемых в Whitepaper, может дать дополнительную ценную информацию о рисках или перспективах, которые повлияют на решение инвестора.

Важнейшей частью Whitepaper является описание команды, работающей над проектом. Опыт и авторитет инженеров блокчейна и ключевых сотрудников, реализующих идею проекта, дает инвестору понимание и некоторую уверенность в том, что проект будет успешным. Команда является интеллектуальным ядром проекта и от конструктивного взаимодействия ее членов, включая лидера, зависит эффективность достижения цели и конечный результат. Отмечайте потенциал команды ICO проекта в вашем чек-листе.

Road Map – дорожная карта

Весомой составляющей Whitepaper или даже самостоятельной частью описания динамики проекта ICO является Road Map – дорожная карта. По существу, Road Map есть детализированный план развития, во главу которого ставится рентабельность проекта. Комплексное отражение перечня всех этапов и последовательных шагов, реализуемых создателями и разработчиками, с указанием промежуточных целей (milestones), позволяет инвесторам оценить темпы продвижения и выполнения краеугольных задач проекта.

Любой план-график основных этапов ICO, с указанием времени реализации, является свидетельством адекватных ориентиров в будущем. Сохраните ваш впервые увиденный вариант Road Map проекта ICO и внимательно отслеживайте продвижение проекта по дорожной карте, если оно происходит или надвигается по шкале времени к отметке очередного дорожного столба (milestone). Road Map должна оставаться неизменной, как географическая карта, а поэтому нехорошим сигналом для инвестора и, возможно, всего проекта, являются изменения в этом важном документе. Оцените реальность Road Map проекта в вашем чек-листе.

Самостоятельная удаленная проверка компании ICO и вэб-сайта

Осмотр домена сайта с помощью сервиса Whois

Постараемся получить полезную информацию о компании ICO, проводящей размещение токена «бумкоин», которая расположена за рубежом, на другом континенте. Интернет и компьютер дают такую возможность.

Открываем главную страницу сайта www.nic.ru и в закладке «Домены» ищем популярный сервис Whois, который позволяет получить основную информацию о регистрации домена компанией ICO. Например, дату регистрации, возраст домена, детальные контакты, по которым можно связаться с компанией или с администратором, чей домен вас заинтересовал.

В строке поиска https://www.nic.ru/whois/?searchWord= вводим имя домена компании ICO:

– «www.бумкоин.домен» занят. Это позитивная новость, так как домен существует;

– Registrar URL: http://www.fastdomain.com, – сведения о регистраторе домена, обычно крупный интернет-провайдер,

предоставляющий имена доменов;

– Creation Date: 2018-03-11T19:07:34Z – дата регистрации «бумкоин.домен»;

– Registry Expiry Date: 2019-03-11T19:07:34Z – дата окончания регистрации «бумкоин.домен»;

– Registrar Abuse Contact Email: legal@fastdomain.com – адрес э-почты, для жалоб или информации о злоупотреблениях со стороны «бумкоин.домен»;

– Registrar Abuse Contact Phone: +1.602.2262389 – контактный телефон, для жалоб или информации о злоупотреблениях со стороны «бумкоин.домен»;

– Domain Status: clientTransferProhibited – статус домена «бумкоин.домен»;

– Registrant Organization: The Endurance International Group, Inc. – организация заявитель регистрации домена;

– Registrant State/Province: Massachusetts – местонахождение организации заявителя;

– Registrant Country: US – страна заявителя.

Исходя из полученных данных понятно, что домен токена «бумкоин», действующий. Страна размещения компании – США, а не Зимбабве. Есть контакты регистратора домена, а вот контакты администратора домена «бумкоин.домен» отсутствуют, что несет некоторые риски при обращении к компании ICO токена «бумкоин». Внимательно знакомимся с каждой строкой сервиса Whois. Заполняем соответствующий чек-лист, делаем выводы.

Осмотр SSL-сертификата домена сайта

SSL-сертификат – это цифровая подпись сайта, реализующая безопасное соединение между сервером домена и браузером пользователя. Обеспечивает надежную защиту данных – информация передается в закодированном виде по протоколу https. Расшифровать ее можно с помощью специального ключа, известного только владельцу сертификата.

SSL-сертификаты выдаются удостоверяющими центрами. Чем более известен и компетентен удостоверяющий центр, тем меньше риск, условно говоря, перехвата данных при общении с сайтом домена. Некоторые наиболее профессиональные:

– SSL-сертификаты Symantec;
– SSL-сертификаты Comodo;
– SSL-сертификаты GeoTrust;
– SSL-сертификаты Thawte;
– SSL-сертификаты RU-CENTER и другие.

Найдите сертификат сайта «бумкоин.домен» в левом верхнем углу открытой страницы браузера. Нажмите на «зеленый» замок, убедитесь в актуальности сертификата. Прочитайте кем, когда и кому выдан SSL-сертификат домена, распространяющего ICO токены. Сомнения должны быть развеяны.

Анализ структуры сайта ICO

Продолжая пассивно исследовать сайт токена ICO, можно применить некоторые следующие вполне легальные инструменты.

Монитор защищенности сайтов webbez.ru предоставляет услуги по обнаружению и исправлению типичных уязвимостей и недостатков вэб-сайтов для их владельцев. Ресурс предлагает получить расширенное досье на сайт за 15 секунд. На странице PageScan ресурса вводим имя исследуемого сайта «бумкоин.домен», получаем техническую информацию о структуре сайта, программах, на которых он базируется и ошибках, если такие имеются. По этой информации ИТ-специалист сможет определить некоторые уязвимости сайта токена ICO.

В Интернете можно найти целый ряд онлайн-сканеров для анализа, интересующего нас, вэб-сайта. Другой онлайн ресурс для тесного знакомства с сайтом токена ICO это *rescan.pro*. Этот сканер верхнего уровня сообщает об опасных кодах, вирусах в скриптах, о наличии сайта в списке вредоносных и прочих ошибках на ссылках и страницах исследуемого сайта.

Прекрасным автономным инструментом для всестороннего анализа вэб-сайта является бесплатная утилита *FOCA Free 3.0* для Windows. Полученный с помощью FOCA по-

дробный отчет, передайте для анализа специалисту. Он оценит риски для сайта в пределах своей компетенции, а вы получите информацию, которая вам необходима для безопасного инвестирования в новый проект.

Поиск дополнительной информации с помощью Google

Значительный объем информации о компании ICO можно получить из открытых источников. Для сбора информации и последующей оценки риска можно использовать не только Google, но и другие поисковые системы, например, Yahoo, Bing и т.п. Для эффективного сбора и выявления интересующих данных рекомендуем грамотно применять операторы поиска. С приемами использования операторов поиска Google можно ознакомиться по этой ссылке http://www.google.com/help/basics.html. Важно отметить, что сайт токена ICO и сайт компании, проводящей ICO, могут различаться между собой.

В нашем примере, следующим шагом можно направить фокус поиска, применив оператор site. Наберите в строке поиска Google строку *site:бумкоин.домен* , тем самым представляется возможным ограничить вывод результатов только внутренней информацией домена «бумкоин.домен».

Добавьте в ту же командную строку ключевые слова «уязвимость», «взлом» или другие, значимые по вашему мне-

нию, и тогда станут доступны негативные или позитивные сведения с сайта «бумкоин.домен». Например, *"site:бумкоин.домен взлом"*.

В Интернете можно найти множество профессиональных ресурсов и программ для исследования сайтов, но разумно ограничиться поиском в рамках требуемых целей и задач. Изучите некоторые операторы поиска и комбинируйте их с ключевыми словами. Пробуйте поисковые ресурсы, отличные от Google, для получения информации разными поисковиками (достаточно полный список можно найти на *http://www.searchenginecolossus.com*).

Проверка личного кабинета на сайте ICO токена

Для первого и последующих контактов с компанией ICO заведите специальный уникальный почтовый ящик. Финансовые вложения через Интернет и переписка по этим вопросам должны быть надежно защищены и отделены от личной почты. Это разумно, легко и, к тому же, бесплатно.

Начните регистрацию в личном кабинете на сайте токена ICO с помощью вашего нового уникального почтового ящика. Решите, указывать ли полные настоящие персональные данные. Напишите короткое приветственное письмо на адрес службы поддержки сайта, указанный в вашем личном кабинете. Оцените ответ, который вы получите, а также быст-

роту и время ответа на ваше письмо. Сделайте выводы, если ответа не получите вовсе.

Внимательно осмотрите ваш личный кабинет. Важно, чтобы имелась обязательная возможность смены (change password) первоначального пароля для входа, с которым вы регистрировались. Измените первоначальный пароль, прежде чем вкладывать финансовые средства. Тема выбора пароля особенно критична, так как одинаковые пароли к вашим различным кабинетам (почта, вход в компьютер, логины в другие удаленные ресурсы и пр.) недопустимы. Установив по привычке «старый» пароль, вы приобретаете существенный риск взлома вашего личного кабинета для токенов ICO. Это происходит потому, что степень защищенности у различных ресурсов может значительно отличаться. Один слабый скомпрометированный пароль к почтовому ящику с новостями потянет за собой «на дно» ваши финансовые проекты, если пароли у личных аккаунтов будут одинаковые.

Настоятельно рекомендуем пароль длиной не менее 12 символов и включающий в себя три алфавита (a, A, @). Пароль обычно не хранится на серверах проекта ICO, поэтому, если вы забудете его, восстановление будет невозможно. Запишите пароль на бумажный лист, положите в конверт и спрячьте в личный сейф. При смене пароля, потрудитесь внести измененные данные в тот же лист. Верните лист в конверт, конверт в сейф.

Если в личном кабинете существует опция 2-шаговой

(двойной) верификации, то непременно воспользуйтесь ею. При некоторых неудобствах подтверждения вашей личности, опция двойной верификации (э-почта, смс, Google-идентификатор и пр.) дает многократное повышение безопасности доступа в ваш личный кабинет.

В личном кабинете вам будет представлен номер кошелька (один или несколько) – это ваш уникальный идентификатор. Он полностью индивидуален и будет использоваться вами для финансовых операций со средствами кошелька. Не сообщайте никому ID своего кошелька, если не проводите конкретную операцию покупки/продажи криптовалюты.

Ознакомьтесь с предложениями по проекту и с дополнительными опциями в личном кабинете, где таковые имеются. Особенное внимание обратите на комиссионные платежи при операциях и условия вывода средств. Оцените риск «замораживания» ваших финансовых средств без движения. Лучше иметь возможность вывести средства с комиссией, чем оставить средства навсегда в случае краха проекта ICO по независящим от вас причинам.

О безопасности собственного рабочего места участника ICO мы расскажем позже в главе 6.

Технологии криптовалют, как фактор риска в проекте ICO

Методики консенсусов в криптовалютах и их основные риски

Мир цифровых коммуникаций стремительно меняется и причиной тому расцвет публичных блокчейнов в финансах, торговле, юриспруденции, здравоохранении. Чтобы функционировать в мировом масштабе, практичный повсеместно используемый взаимозачет нуждается в блокчейне с эффективными, функциональными и безопасными соглашениями. Реализация методик этих соглашений должна стремиться к отсутствию рисков. Рассмотрим различные типы методик достижения консенсуса, которые могут участвовать в проекте ICO, от наиболее востребованных до экзотических.

Доказательство работы (proof of work, PoW)

Наиболее распространена методика, такая как «доказательство работы» в биткойне, с которой мы чаще всего сталкиваемся и взаимодействуем. Она выполняет две вещи: дает гарантию, что следующий блок в блокчейне (цепочке) всегда уникален и притом является единственно верным артефактом, что и удерживает всесильных участников-оппонентов

от подмены системы и возможного разветвления блокчейна (цепи блоков).

Починяясь «доказательству работы» создатели монет (майнеры) конкурируют за добавление следующего блока (набора транзакций) в цепочку, участвуя в соревновании посредством решения чрезвычайно сложной криптографической задачи. Первый, кто решил головоломку, выигрывает эту лотерею. За свои усилия в качестве вознаграждения майнер получает цепочку из 12,5 новых биткойнов и небольшую комиссионную плату.

Хотя это уникально само по себе, тем не менее методика, применяемая в биткойне, не совсем совершенна. Важным моментом является обязательное существование большой совокупной мощности сети для защиты от одного потенциального злоумышленника, желающего завладеть 51% ресурсов сети.

Разрастаясь, класс криптовалют с «доказательством работы» превратился в чудовище, пожирающее электричество в гонке за прибыльностью майнинга. Серьезные претензии о бесполезной трате электроэнергии небезосновательны, но пока практически игнорируются.

Основные критические замечания состоят в том, что такой методический подход требует огромных вычислительных ресурсов, что он недостаточно оптимизирован (подтверждение транзакции занимает около 10-60 минут), и что большая часть добычи централизована в районах мира с деше-

вым электричеством.

Неуловимый автор Bitcoin (BTC) Сатоши Накамото воодушевил нас потенциалом блокчейна, но это не значит, что у нас отсутствует способность продолжить поиск более быстрых, менее централизованных и более энергосберегающих процессов с методиками, перспективными в будущем.

Опишем далее нескольких альтернативных подходов, которые прорастают в мире криптовалют и ICO проектов.

Доказательство доли (proof of stake, PoS)

После «доказательства работы» наиболее распространенной является методика «доказательство доли». В этом согласующем процессе вместо того, чтобы инвестировать в дорогостоящее компьютерное оборудование по соревнованию добытых блоков, собственник опирается на инвестиции в «монеты» системы.

Поясним появление термина «собственник». Поскольку в «доказательстве доли» не существует никакой добычи монеты (майнинга), а все монеты уже созданы с самого начала процесса, то собственники (также называемые участниками, потому что они держат долю в системе) получают платежи строго как сборы за выполнение транзакций.

В «доказательстве доли» шанс быть выбранным для генерации следующего блока зависит от величины доли монет в системе (или отложенной для получения). Собственник 200 монет имеет в двадцать раз больше шансов быть выбранным, чем собственник 10 монет.

По сути, процесс «доказательства доли» является таким же случайным, как и «доказательство работы». Однако, он не содержит необходимости «платить» вычислительной мощностью за выигрыш. Перебор вариантов для выигрыша происходит среди ограниченного множества комбинаций и почти не зависит от производительности CPU. На вероятность выиграть влияет суммарное число монет собственника и сложность существующей сети. Кроме того, атака на 51% монет (а не захват мощности сети) заставит рынок реагировать на скупку быстрым ростом цены, потому что одноразовое приобретение 51% монет выполнить практически невозможно.

Против «доказательства доли» часто звучит мнение, что этот процесс «делает богатых богаче». И в самом деле: тот, у кого больше всех монет, будет находить больше всех блоков и получать больше всех прибыли, увеличивая число этих монет. Очевидно, что в таком ключе этот упрек можно высказать и методике «доказательства работы»: ведь тот, кто вложил большие деньги в железо, будет получать отдачу в виде большего дохода. Представителями «доказательства доли» являются криптовалюты Waves (WAVES) и Lisk (LSK).

Peercoin (PPC) был первой монетой, с выполнением «доказательства доли», за которой последовали BlackCoin (BLK) и Nxt (NXT). Ethereum (ETH) в самом начале опирался на «доказательство работы», но планирует перейти к «доказательству доли» (проект Casper).

Доказательство депозита (proof of deposit, PoD)

Разновидностью процесса «доказательства доли» является «доказательство депозита», где майнеры блокируют определенное количество монет (депозит), которые они не могут потратить в период своей работы, причем собственник, вбросивший в сеть некорректный блок не только лишается права на майнинг, но и автоматически лишается права на свой депозит. Одной из таких систем является Tendermint, где сила голоса майнера пропорциональна количеству монет, которые он внес на депозит.

После создания блока собственником, этот блок все равно должен быть привязан к цепочке блоков. Различные системы проверки подлинности характеризуются тем, как они справляются с проверкой. В системе Tendermint каждый узел системы должен подписывать блок до тех пор, пока не будет достигнуто большинство голосов, тогда как в других системах выбрана случайная группа подписантов.

Теперь у нас возникает проблема. Что должно препятствовать собственнику создать два блока и требовать два набора транзакционных сборов? А также, что можно противопоставить подписанию двух этих блоков?

Особенность майнинга с методикой «доказательства доли» – суть обычное голосование. Оно ничего не стоит, не требует ресурсов или физических затрат. Участникам выгодно майнить несколько параллельных альтернативных ветвей. Они просто могут это делать бесплатно, с ненулевыми

шансами на успех, а значит – увеличить вероятность дохода. С «доказательством работы» такое невозможно в принципе: любой проверенный хэш цепочки №1 не может являться проверенным хэшем цепочки №2 (иначе они идентичны). «Доказательство доли» позволяет желающим производить перебор во всех интересуемых «параллельных цепочках» сразу, причем в любом времени, в том числе и в прошлом. Как результат – в чистой методике «доказательства доли» однозначно гарантировать соглашение, консенсус всех участников, не получается. С одной стороны, энергия не расходуется, а с другой – без расхода энергии распределенный консенсус выглядит уязвимым.

Делегированное доказательство доли (delegated proof of activity, DPoS)

В растущей области «криптоэкономики» инженеры блокчейна устранили возможную уязвимость распределенного консенсуса, совершив новый шаг в эволюции блокчейна с методикой «доказательства доли». Один из шагов – введение делегатов, внутреннего сообщества пользователей, список которых меняется по определенным правилам. Делегаты подписывают вновь подтвержденный блок.

Другой шаг – требование для собственника депонировать свою валюту в виртуальном хранилище. Если собственник пытается удвоить подписание или разветвить систему, то эти монеты хранилища будут у него отобраны. Делегированное доказательство доли реализовано в криптовалюте BitShares

(BTS).

Доказательство активности (proof of activity, PoA)

Во избежание гиперинфляции (она происходит, когда слишком много монет наводняет систему), Bitcoin будет производить только 21млн биткойнов. Это означает, что в какой-то момент субсидии за майнинг биткойна закончатся, а биткойн-майнеры получат только транзакционные сборы за переводы.

Предполагается, что возможно возникновение проблемы безопасности, называемой «трагедией общин»[1]

[1] Трагедия общин -явление, связанное с противоречием между интересами индивидов относительно блага общего пользования. В общем случае «трагедия» состоит в том, что свободный доступ к экономическому ресурсу (например, пастбищу) уничтожает или истощает ресурс из-за чрезмерного его использования.

Конец ознакомительного фрагмента.