ВИТАЛИК БУТЕРИН

БОЛЬШЕ ДЕНЕГ

ЧТО ТАКОЕ ETHEREUM И КАК БЛОКЧЕЙН МЕНЯЕТ МИР

Виталик Бутерин

Больше денег: что такое Ethereum и как блокчейн меняет мир

Серия «Individuum»

http://www.litres.ru/pages/biblio_book/?art=69165661
Больше денег. Что такое Ethereum и как блокчейн меняет мир:
ISBN 978-5-6048295-8-5

Аннотация

В 2013 году девятнадцатилетний программист Виталик Бутерин опубликовал концепцию новой платформы для создания онлайн-сервисов на базе блокчейна. За десять лет Ethereum стал не только второй по популярности криптовалютой, но и основой для целого мира децентрализованных приложений, смарт-контрактов и NFT-искусства. В своих статьях Бутерин размышляет о развитии криптоэкономики и о ключевых идеях, которые за ней стоят, – от особенностей протокола Ethereum до теории игр, финансирования общественных благ и создания автономных сетевых организаций. Как блокчейн-сервисы могут помочь людям добиваться общих целей? Могут ли криптовалюты заменить традиционные финансовые инструменты? Ведут ли они к построению прекрасного нового мира, в котором власть

будет принадлежать не правительствам и корпорациям, а людям, объединенным общими ценностями и интересами, или служат источником неравенства и циничных финансовых спекуляций? В этой книге Бутерин предстает увлеченным мыслителем, глубоким социальным теоретиком и активистом, который рассуждает о том, что гораздо больше денег, не боится задавать сложные вопросы и предлагать решения противоречивых проблем.

В формате PDF A4 сохранен издательский макет книги.

Содержание

Виталик Бутерин
Больше денег. Что такое Ethereum и как блокчейн меняет мир

Copyright © 2022 by Vitalik Buterin
Introduction and notes © 2022 by Nathan Schneider
Originally published in English by Seven Stories Press, Inc. New York, U.S.A.
© Инна Проворова, перевод, 2023
© ООО «Индивидуум Принт», 2023

Посвящается маме и папе: потрясающим родителям, предпринимателям и повелителям мемов

Введение

НАТАН ШНАЙДЕР

До того как в возрасте 19 лет он создал новую экономическую инфраструктуру интернета; до того как стал миллиардером, ночующим на диванах у друзей, Виталик Бутерин хотел писать тексты. Он заинтересовался биткойном с подачи отца, с которым еще ребенком эмигрировал из России в Канаду. И даже первые криптомонеты достались ему в качестве оплаты за текст: в 2011 году он предложил на онлайн-форуме написать статью о биткойне с оплатой в биткойнах.

Предложение нашло отклик, и в итоге Бутерин дописался до того, что стал одним из основателей Bitcoin Magazine – печатного и онлайн-издания о новостях тогда еще крошечной и разрозненной субкультуры. Этот новый вид денег, которые было почти невозможно потратить, интересовал Бутерина куда больше учебы на первом курсе университета. Уже с первых текстов Бутерин развивал свои идеи в непрерывном диалоге со всеми заинтересованными. И все же в его публикациях, сделанных за несколько лет в разных блогах, форумах и твиттере, заметен собственный авторский голос. Этот голос сыграл не последнюю роль в том, с каким энтузиазмом сообщество приняло его изобретение – Ethereum. Вполне может случиться так, что Ethereum и его сообщество оправдают возложенные на них ожидания, став всепроника-

ющей инфраструктурой. И потому стоит тщательно изучить – и критически осмыслить – его идеи.

В этой книге мы познакомимся с Виталиком Бутериным как писателем.

Когда 2008 году начался глобальный финансовый кризис, некто под псевдонимом Сатоши Накамото анонсировал прототип биткойна – валюты, функционирующей на базе криптографических компьютерных сетей, а не государственных или банковских систем. Этот вид денег он назвал криптовалютой. Компьютерщиков-шифропанков и либертарианских «золотых жуков»[1] манили новые идеи: цифровой майнинг, ограниченная эмиссия, эквивалент наличных транзакций, которые могут быть безопасными и конфиденциальными. Бутерин отлично знал эту аудиторию. Он все больше и больше увлекался биткойном, но к концу 2013 года начал понимать, что технология блокчейна, на базе которой существует криптовалюта, может дать нечто большее: возможность создавать в интернете организации, компании и даже целые экономики. И он решил об этом написать. Первый вайтпейпер[2] Ethereum, включенный в эту книгу, пролил свет на еще крошечную на тот момент криптовалютную вселенную. Вместо зависимости от корпораций, инвесторов и за-

[1] В экономике «золотыми жуками» называют сторонников золотого стандарта и тех, кто предпочитает вкладываться в золото. – *Прим. пер.*

[2] Вайтпейпер (англ. white paper) – документ, излагающий суть, цели и принципы работы криптовалютного проекта. – *Прим. ред.*

конов Старого Света, регулирующих работу серверов, предлагалось отдать управление в руки самих пользователей. Если майнинг биткойна метафорически сравнивали с добычей золота, то культура Ethereum скорее перекликается с эстетикой любимых футболок Бутерина: роботами, единорогами и радугами, которые стали талисманами новой криптовалюты.

Ethereum запустился в 2015 году. С тех пор появилось много блокчейнов-конкурентов, способных различными путями выполнять сходные задачи, но Ethereum среди них остается крупнейшим. Его валюта, известная как эфир или ETH, по капитализации уступает только биткойну, но если добавить сюда токены всех продуктов и сообществ, созданных на базе Ethereum, на них придется крупнейшая доля в этой странной новой экономике. Бутерин, нравилось ему это или нет, во время первых тестов проекта постепенно превращался в «великодушного диктатора» Ethereum: не столько из-за своих официальных полномочий, сколько из-за доверия, которое ему оказывали. В формирование этого доверия немалый вклад внесли и собранные здесь статьи.

Но есть тут и некое противоречие. Бутерин хочет сделать шаг к радикальному переосмыслению того, как человеческие существа могут взаимодействовать в условиях самоорганизации, но при этом сохраняет строго агностическое отношение к их способности распоряжаться такой властью. Как объясняется в одном из эссе в этой книге, система Ethereum создавалась по принципу «доверительного нейтра-

литета» – этот же принцип определяет лидерскую роль Бутерина. С первых кадровых решений и до последних важных обновлений – и, возможно, вопреки его собственной воле – его стиль управления неотделим от самого Ethereum. Хотя эфир и подобные системы основаны на представлении о том, что все люди эгоистичны, его основатель – аскет, которому словно не нужно ничего, кроме криптобудущего.

При этом нет никаких гарантий, что к этому будущему стоит стремиться. Когда в 2014 году Бутерин впервые публично представил Ethereum на биткойн-конференции в Майами, он закончил перечислять все потенциальные чудеса этой системы, упомянув Скайнет – искусственный интеллект из фильмов о Терминаторе, восставший против людей, которые его создали. Он часто повторял эту шутку, в которой, как и во многих заезженных шутках, есть доля правды. Ethereum может стать и утопией, и антиутопией, и гибридом того и другого. В криптомире полно противоречий.

◊ Он умышленно создает дефицит, ограничивая доступность токенов, но он же позволяет сообществам генерировать, а затем использовать и контролировать огромный капитал.

◊ Он отсеивает людей, которые не могут себе позволить купить волатильную интернет-валюту и использовать ее, и он же стимулирует развитие новых систем управления, которые снимают сословные ограничения и отменяют властные привилегии.

◊ Его функционирование требует огромного количества энергии, и он же предлагает новые способы контролировать выбросы вредных веществ в атмосферу, в то время как правительства бездействуют.

◊ Он породил новый класс нуворишей, которые сорят деньгами и разгоняют инфляцию в «налоговых гаванях», выживая оттуда местных жителей, и он же представляет собой безграничную, принадлежащую самим пользователям финансовую систему, которая доступна каждому, у кого есть смартфон.

◊ Он дает преимущества технически подкованной элите, которая раньше успела воспользоваться новыми возможностями, и он же предлагает реальный шанс подорвать позиции доминирующих технологических компаний.

◊ Сначала он породил спекулятивную финансовую систему, а вовсе не реальную экономику полезных вещей, но при этом он в гораздо бóльшей степени принадлежит людям, создающим реальную ценность, чем фондовые активы.

◊ Он обеспечил огромные выплаты за коллекционные токены, не имеющие очевидной стоимости, но в результате появилась новая бизнес-модель для создания и распространения культуры открытого доступа.

◊ Он дает первым владельцам возможность обогатиться за счет следующих, и он же предлагает новым участникам набор инструментов, ценность которых зависит от их собственных поступков.

Помня об этих противоречиях, читатель должен сам делать выводы для себя и своего сообщества. Противоречия давят своей неопределенностью, но они же могут мотивировать к действию. В конце концов, вся эта сфера только развивается и еще не обрела окончательную форму.

В основе любой блокчейн-системы вроде биткойна или Ethereum лежит механизм консенсуса. Это процесс, посредством которого компьютеры согласовывают общий набор данных – будь то список транзакций в биткойне или память мирового компьютера Ethereum – и защищают его от махинаций. Достичь консенсуса без централизованного управления непросто. Биткойн использует механизм под названием proof of work, где много компьютеров тратят много энергии на решение математических задач и тем самым доказывают, что они вкладываются в обеспечение безопасности системы. За это они получают плату, но при этом поглощают столько же электроэнергии, сколько способна потребить целая страна[3], что неизбежно сопровождается выбросами CO_2. Поскольку на тот момент альтернатив не было, Ethereum тоже использовал proof of work, но еще до запуска проекта Бу-

[3] Согласно оценке Bitcoin Mining Council, глобальные затраты электричества на майнинг биткойна превышают энергопотребление в таких крупных странах, как Австралия, Испания и Турция. – *Прим. ред.*

терин начал говорить о переходе на другой механизм, proof of stake, когда это станет технически возможно. В proof of stake участники доказывают свою ценность для сети не вычислительной мощностью, а вложенными токенами. Этот механизм расходует минимальное количество энергии, а риск потерять активы удерживает участников от махинаций.

В этой книге механизмы консенсуса имеют еще и метафорическое, а не только техническое значение. Они символизируют трудолюбие, решимость, уверенность и сотрудничество, что отражено в собранных здесь эссе. Вместе с тем они демонстрируют и противоречия: инновации и безрассудство, демократию и плутократию, сплоченное сообщество и полное недоверие. Как и сами механизмы консенсуса, эти символы отвергают идеализм и подчеркивают компромиссы, без которых реальный мир никогда не сможет даже приблизиться к нашим желаемым представлениям.

Эссе, которые мы вместе с Бутериным собрали в этой книге, показывают его с новой стороны – как социального теоретика и активиста, человека, который действует, не забывая перед этим подумать о последствиях. Криптокультура – преимущественно мужская, молодая и привилегированная – может казаться очень далекой от проблем, которые она намеревается решить. И Бутерин – живое воплощение этой культуры. Местами он слишком увлекается техническими подробностями, но в приведенных здесь работах их куда меньше, чем в других, которые зачастую предназначались только для

коллег-разработчиков. Понять технические аспекты может оказаться непросто, но, если попытаться, потраченные усилия непременно окупятся. Даже когда в них встречаются математические формулы, эти тексты остаются ясными и увлекательными.

При публикации эти эссе подверглись небольшой редактуре для достижения стилистического единообразия, а также были очищены от гиперссылок, недоступных в книжном формате. Поскольку эти тексты изначально предназначались для узкой аудитории, к ним добавлены комментарии, делающие их понятными читателям, которые не знакомы с криптосферой.

По мере проникновения криптовалют в экономический мейнстрим все чаще разгораются дебаты о том, стоит ли вернуть этого джинна обратно в бутылку, если это вообще возможно. Может быть, после прочтения книги люди, задающиеся этим вопросом, заметят, что их, как и Бутерина, интересует уже не столько «стоит ли» это делать, сколько все более разнообразные варианты ответа на вопрос, как с этим жить. Если мы действительно наблюдаем рождение новой социальной инфраструктуры, то создающиеся вокруг нее политические и культурные привычки будут иметь огромные последствия. Размышления Бутерина показывают, что вопрос «как» пока остается в значительной степени открытым.

.

Часть 1
Премайнинг

В январе 2014 года Бутерин сообщает в своем блоге, что «холодным ноябрьским днем в Сан-Франциско после нескольких месяцев размышлений и часто безрезультатной работы»[4] он подготовил вайтпейпер Ethereum. В те месяцы он был полужурналистом (в своем Bitcoin Magazine), полуразработчиком (в нескольких стартапах, связанных с биткойном), общался с либертарианцами в Нью-Гемпшире, иммигрантами в Цюрихе, программистами в Тель-Авиве и жителями Калафа, «посткапиталистической колонии» в разрушающемся заводском комплексе неподалеку от Барселоны. В свое время биткойн анонсировали именно в форме вайтпейпера, где техническое описание сочетается с манифестом, и последующие криптопроекты унаследовали этот формат. В 2013 году такой жанр прекрасно подошел журналисту-разработчику Бутерину. Статья «Ethereum: криптовалюта следующего поколения и децентрализованная платформа для приложений» – прекрасный конспект полного текста вайтпейпера, который можно найти в приложении к этой книге. Еще за полтора года до первого релиза Ethereum

[4] Vitalik Buterin, «Ethereum: Now Going Public», Ethereum Foundation blog (January 23, 2014).

он размышляет об Ethereum 2.0 и proof of stake, хотя окончательно эти идеи созреют только к 2021 году.

Премайнинг – это выпуск токенов еще до публичного релиза блокчейна. Продав на базе вайтпейпера предварительно добытые эфиры, Бутерин и его первые партнеры сумели собрать больше 18 миллионов долларов. Тогда это был рекорд среди краудфандинговых онлайн-кампаний, в дальнейшем побитый проектами на базе самого Ethereum. Вопреки призывам более опытных партнеров создать коммерческую компанию, Бутерин настоял на некоммерческой сущности Ethereum. Но это не была благотворительная организация: в случае успеха ему и соучредителям доставалась солидная прибыль от токенов, полученных в результате премайнинга.

В этих эссе прослеживается эволюция Бутерина от адепта киберлибертарианства до прагматичного, открытого разным идеям разработчика инфраструктуры. Поначалу он хвалит проекты на основе биткойна – в то время очень модные и в большинстве случаев не дожившие до сегодняшнего дня. Но позднее, в статье «Об изолированных системах», Бутерин явно остужает свой пыл и отказывается искать все ответы

в каком-то единственном проекте. Чтобы переписать общественный договор, утверждает он, потребуется инструментарий, не привязанный к какой-либо конкретной идеологии.

В преддверии релиза Ethereum Бутерин спрашивает себя: «В чем же его основная польза?» Он разрабатывает теорию перемен, вызванных не столько великими технологическими прорывами, сколько решением частных задач. Мотивация разработчиков этой технологии, предрекает он, будет зависеть оттого, что с ее помощью создадут другие. Готовясь к публичному релизу, он все больше размышляет о том, что никто не может знать или контролировать. – Н. Ш.

Рынки, институты и валюты – новый метод социального стимулирования

BITCOIN MAGAZINE
10 января 2014 года

До сих пор подступиться к проблеме стимулирования производства можно было, по сути, только с двух сторон: со стороны рынков или институтов. Рынки в чистом виде полностью децентрализованы и состоят из бесконечного числа агентов, которые взаимодействуют друг с другом так, чтобы каждый остался в выигрыше. Институты, в свою очередь, устроены иерархически: верхушка определяет, какие действия в определенный момент будут наиболее эффективны, и назначает вознаграждение за их выполнение. С одной стороны, централизация помогает институтам стимулировать производство общественных благ, которые приносят пользу тысячам или даже миллионам людей, хотя их польза для каждого отдельного человека может быть крайне мала; с другой стороны, она сопряжена с известными внутренними рисками. В сущности, в последние 10 000 лет именно эти два механизма отвечали за стимулирование производства. Однако с появлением биткойна и его производных все может измениться. И то, что мы наблюдаем сейчас, – это, возможно, зарождающаяся третья форма стимулирования: валюты.

ДРУГАЯ СТОРОНА МОНЕТЫ

В обществе валюта выполняет три фундаментальные функции. Она служит средством обмена, позволяя людям покупать и продавать товары за деньги, а не искать кого-то, кто одновременно и заинтересован в вашем товаре, и может предложить взамен нужный вам товар. Также валюта работает как средство сбережения, позволяя людям производить и потреблять блага в разное время. Наконец, это средство подсчета и измерения, с помощью которого мы можем вычислить постоянный «объем производства». Но мало кто знает о существовании четвертой роли валюты, важность которой скрывалась от нас большую часть истории: сеньораж.

Формально сеньораж можно определить как разницу между рыночной и внутренней стоимостью валюты, то есть стоимостью, которую имела бы валюта, если бы никто не использовал ее в качестве таковой. У древнейших валют вроде зерна сеньораж был практически равен нулю, но по мере развития экономики эта «фантомная стоимость», создаваемая деньгами будто из ниоткуда, все больше росла. В итоге она достигла точки, где сеньораж представляет собой всю стоимость валюты – как, например, у доллара или биткойна.

Но куда уходит этот сеньораж? В случае валют, основанных на природных ресурсах, – например, золота – бóльшая часть стоимости просто теряется. На каждый грамм золота

приходится труд того, кто его добывает. Возможно, первые добытчики и получают неплохую прибыль, но потом, когда рынок исчерпывает все легкие пути, стоимость производства этой валюты приближается к доходу от нее. Конечно, существуют хитрые способы и дальше получать сеньораж от золота; например, в древних обществах короли чеканили золотые монеты и пускали их в ход дороже обычного золота, поскольку закладывали в них гарантию подлинности металла. Однако обычно эта ценность не доставалась никому конкретно. Американский доллар немного изменил положение вещей: часть его сеньоража шла правительству США. Это был одновременно и большой шаг вперед, и своего рода незавершенная революция – валюта, получив преимущества централизованного сеньоража, также столкнулась с рисками, неизбежными при работе с одним из крупнейших централизованных институтов в истории человечества.

И ПОЯВИЛСЯ БИТКОЙН

Пять лет назад появился новый вид денег – биткойн. Как и у доллара, у него нет внутренней стоимости, и его производство ничего не стоит. Куда же в этом случае идет сеньораж? Часть достается майнерам, а остальное покрывает издержки функционирования самой системы – обеспечивает ее безопасность. Так возникла валюта, сеньораж которой идет непосредственно на общее благо – поддержание без-

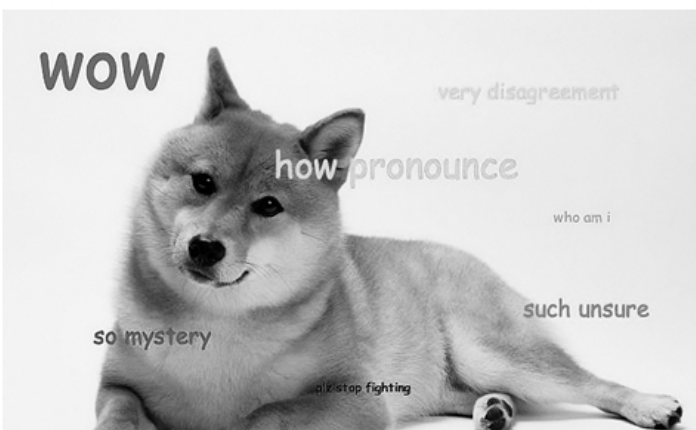
опасности сети биткойна. Эта ее особенность несправедливо обделена вниманием, ведь именно за счет нематериальной «фантомной» ценности, возникающей из самого использования биткойна как средства хранения и обмена, мы получаем уникальный процесс стимулирования: децентрализованный, не нуждающийся в контроле или управлении и создающий общественное благо.

Потом появился праймкойн (primecoin) – первая валюта, сеньораж которой попытались пустить на поддержку чего-то еще, кроме ее самой: если для создания биткойна майнерам приходится вычислять совершенно бесполезные хеши SHA256, то здесь им нужно было искать цепочки простых чисел Каннингема, что одновременно помогает развивать очень узкое направление научных вычислений и подталкивает производителей компьютеров искать новые способы оптимизировать микросхемы для арифметических операций. Праймкойн рос в цене с завидной скоростью и по сей день остается одиннадцатой среди самых популярных криптовалют[5], хотя многие другие, куда менее известные системы гарантируют пользователю такую же непосредственную практическую выгоду – создание блока за одну минуту[6].

---

[5] Информация актуальна на момент написания статьи. – *Прим. ред.*

[6] Чем меньше время создания блока, тем быстрее проходят транзакции. – *Прим. ред.*



Буквально через несколько месяцев, в декабре, с поразительным успехом выстрелила еще более необычная валюта – дожкойн [7](dogecoin). Дожкойн (тикер – DOGE) в техническом плане почти полностью идентичен лайткойну (litecoin) и отличается лишь большей максимальной эмиссией монет: 100 миллиардов против 84 миллионов. И все же рыночная капитализация дожкойна достигла 14 миллионов долларов,

[7] В русском языке не закрепилось единственное произношение названия Dogecoin. В русскоязычном интернете варианты «догекойн»/«догикойн» популярны примерно так же, как и «дожкойн» (так название этой криптовалюты произносит ее главный апологет – Илон Маск). – *Прим. ред.*

сделав его шестой по величине криптовалютой в мире. Даже пресса – Business Insider и Vice – не обошла его стороной. Что же такого особенного в DOGE? Все началось с мема. Слово «doge» – производное от «dog» – впервые появилось в 2005 году в кукольном шоу Homestar Runner и разрослось до глобальной тенденции накладывать разноцветные надписи вроде «wow», «so style» и «such awesome» шрифтом Comic Sans на изображение собаки породы сиба-ину. Этот мем отражает весь брендинг дожкойна: изображениями сиба-ину пестрят его сайты (в том числе официальный) и форумы, тред на Bitcointalk, который заводит любая уважающая себя криптовалюта[8], а также сабреддиты r/dogecoin и r/dogecoinmarkets. Этого оказалось вполне достаточно, чтобы капитализация клона лайткойна выросла до 14 миллионов долларов.

Наконец, третий пример выводит нас за пределы мира криптовалют. Более традиционная, централизованная валюта Ven подкрепляется набором товаров и услуг вроде предметов потребления, национальных валют и фьючерсов. Недавно этот набор пополнился фьючерсами на выбросы углекислого газа, что сделало Ven первой валютой, в некотором роде «привязанной к окружающей среде». Произошло это благодаря грамотному экономическому ходу: цена

[8] В то время Bitcointalk, созданный Сатоши Накамото, был онлайн-доской объявлений и главным форумом для обсуждений криптовалют. Любая новая криптовалюта создавала там свой тред. – *Далее примечания редактора англоязычного издания следуют без дополнительных пометок*.

фьючерсов на выбросы обратно пропорциональна стоимости Ven, так что ценность валюты становится выше, когда общество отказывается от производств с повышенным выбросом CO_2 и разрешения на выбросы CO_2 становятся менее рентабельными. Таким образом, каждый держатель Ven имеет финансовый стимул – пусть и небольшой – заботиться об окружающей среде, и отчасти именно это привлекает интерес к Ven.

Все эти примеры показывают, что привлекательность альтернативных валют практически полностью зависит от низового маркетинга. Никто не стал бы покупать биткойн, праймкойн, дожкойн или Ven, если бы их просто навязывали всем без разбора или уговаривали продавцов принимать их в качестве оплаты. Не только техническое превосходство валюты определяет ее успех – идеалы имеют не меньшее значение. Именно идеалы биткойна убедили WordPress, Mega, а теперь и Overstock принимать его в качестве валюты. Возможно, по той же причине монета Ripple, несмотря на техническое превосходство над биткойном (в частности, пятисекундное подтверждение транзакции), не возымела такого же успеха: модель полуцентрализованного протокола, поддерживаемого корпорацией, которая забрала себе 100 % эмиссии его валюты, делает Ripple малопривлекательным для криптоэнтузиастов с их стремлением к справедливости и децентрализации. Сегодня праймкойн и DOGE продолжают успешно существовать именно благодаря верности своим

идеалам. В первом случае это наука, во втором – юмор.

КРИПТОВАЛЮТЫ КАК ЭКОНОМИЧЕСКАЯ ДЕМОКРАТИЯ

Эти примеры, наряду с идеей фантомной ценности сеньоража, очерчивают приблизительные контуры нового вида «экономической демократии», где можно создавать валюты, сеньораж или эмиссия которых пойдут на поддержку конкретных целей, а люди смогут поддержать эти цели, используя ту или иную валюту в своей предпринимательской деятельности. Если у человека нет своего бизнеса, он сможет участвовать в маркетинговых инициативах и добиваться, чтобы другие компании начали принимать эти монеты. Можно также выпускать свои SocialCoin[9], как это уже ежемесячно делают 1000 человек по всему миру, и, если достаточному количеству людей понравится идея и они начнут ее реализовать, в мире появится гражданская программа дивидендов, не требующая централизованного финансирования. Мы также можем создавать валюты для стимулирования медицинских исследований, освоения космоса и даже поддержки

[9] SocialCoin – созданная в 2013 году криптовалюта, основанная на идее добрых дел. Человек получал монету, когда ему чем-то помогли, и таким же образом передавал ее другому. Каждый описывал в общей сети, что именно для него сделали. Каждая монета имела физический аналог и существовала три месяца. – *Прим. пер.*

искусства – уже сегодня о создании собственных валют подумывают некоторые художники, музыканты и авторы подкастов.

Говоря о конкретном общественном благе – вычислительных исследованиях, – мы можем пойти еще дальше и автоматизировать процесс распределения. Стимулировать вычислительные исследования можно посредством механизма, который пока не был применен в реальности, но в теории был описан создателем пиркойна и праймкойна Санни Кингом. Речь идет о proof of excellence, «доказательстве достижениями». Идея proof of excellence заключается в том, что ваше вознаграждение и ваша доля в децентрализованном пуле голосования зависят не от вычислительной мощности вашего компьютера или количества монет, а от возможности вашего устройства решать сложные математические или алгоритмические задачи, ответы на которые принесут пользу всему человечеству. Например, если кто-то хочет стимулировать исследования в области теории чисел, он может внедрить в валюту задачи по факторизации RSA-чисел и первому, кто предоставит решение, автоматически назначить награду в 50 000 единиц и, например, дать возможность голосовать за валидацию блоков в процессе майнинга. Теоретически это может даже стать стандартным элементом эмиссионной модели любой валюты.

Конечно, такой подход к валютам существовал и раньше: «социальные валюты» начали циркулировать в локаль-

ных сообществах еще в начале XX века. Однако после пика популярности интерес к ним пошел на спад, в первую очередь из-за того, что они просто не смогли выйти за границы локальных сообществ, к тому же они плохо вписывались в растущую банковскую систему, которая предпочитала работать с более серьезными валютами вроде доллара США. Однако для криптовалют это уже не помеха – они по определению охватывают весь мир и работают на основе невероятно мощной цифровой банковской системы, встроенной непосредственно в их исходный код. Возможно, настал идеальный момент для грандиозного возвращения социальных валют в технически усовершенствованном виде, причем в новой роли движущей силы мировой экономики.

Так что же будет дальше? На примере DOGE мы убедились, как на самом деле просто выпустить собственную валюту, а совсем недавно разработчик биткойна Мэтт Коралло создал сайт coingen.io, единственная цель которого – позволить пользователям быстро создавать клоны биткойнов или лайткойнов с несколько измененными параметрами. Даже с ограниченным на сегодняшний день набором опций сайт оказался довольно популярным и, несмотря на комиссию в 0,05 BTC, подарил жизнь сотням валют. Как только Coingen позволит пользователям добавлять майнинг на основе proof of excellence и передавать часть эмиссии определенной организации или фонду, а также расширит возможности индивидуального брендинга, вполне возможно, на

наших глазах появятся уже тысячи криптовалют. Оправдают ли они наши надежды? Станут ли они децентрализованным и демократичным способом объединять наши средства и поддерживать общественные проекты и инициативы, ведущие человечество к лучшему будущему? Может, да, а может, и нет. Но почти каждый день на свет появляется новая криптовалюта, приближая нас к ответу на этот вопрос.

Ethereum: криптовалюта следующего поколения и децентрализованная платформа для приложений

23 ЯНВАРЯ 2014 ГОДА

В минувшем году все чаще и чаще можно было услышать о так называемых протоколах «Bitcoin 2.0». Эти альтернативные блокчейны, вдохновленные биткойном, стремятся предложить на основе той же технологии более широкую функциональность, чем просто валютные операции. Впервые эта идея была реализована в неймкойне – созданной в 2010 году биткойноподобной валюте для децентрализованной регистрации доменных имен. Недавно появились цветные монеты (colored coins), позволяющие пользователям создавать собственные валюты на основе биткойна, и продвинутые протоколы вроде Mastercoin, Bitshares и Counterparty с функциями финансовых деривативов, сберегательных кошельков и децентрализованного обмена валют. Однако все существующие на сегодня протоколы имеют слишком узкую специализацию: как правило, это наборы конкретных функций для конкретных отраслей или приложений, чаще всего финансового характера. Но сегодня группа разработчиков – и я в их числе – решила подойти к этому с другой стороны и создать максимально универсальную криптовалютную сеть,

на основе которой любой сможет разработать специализированные приложения практически для любых целей, которые только можно себе вообразить. Мы назвали ее Ethereum.

КРИПТОВАЛЮТНЫЙ ПРОТОКОЛ НАПОМИНАЕТ ЛУКОВИЦУ…

В дизайне многих криптовалютных протоколов второго поколения прослеживается общая идея: протокол, как и интернет, работает лучше при разделении на слои. Если развить эту мысль, протокол биткойна можно представить как своего рода TCP/IP для криптовалютной экосистемы, а протоколы следующего поколения создаются поверх биткойна. То же самое мы наблюдали с TCP в качестве общего базового слоя и созданными поверх него SMTP для электронной почты, HTTP для веб-страниц и XMPP для чатов.

До сих пор этой модели придерживались в основном три протокола: цветные монеты, Mastercoin и Counterparty. Принцип работы протокола цветных монет очень прост. Сперва пользователь приписывает определенным биткойнам конкретное значение и таким образом создает цветные монеты. Например, если Боб – эмитент золота, он может пометить некий набор биткойнов и сказать, что каждый сатоши в нем стоит 0,1 грамма золота и подлежит обмену по соответствующему курсу. Затем протокол отслеживает эти биткойны через блокчейн, и таким образом всегда можно вычис-

лить, кто владеет ими прямо сейчас.

Mastercoin и Counterparty в некотором роде более абстрактны. Они используют блокчейн Bitcoin для хранения данных, так что по сути их транзакция – это транзакция биткойна, но протоколы интерпретируют их совершенно иначе. Например, можно провести две транзакции Mastercoin, в первой отправив 1 MSC, а во второй – 100 000 MSC. Но с точки зрения пользователя Bitcoin, который не знает принципов работы протокола Mastercoin, обе они будут выглядеть как маленькие транзакции по 0,0006 BTC; метаданные Mastercoin кодируются в выходах транзакций. Затем, чтобы определить текущий баланс Mastercoin, клиенту потребуется выполнить поиск транзакций Mastercoin в блокчейне биткойна.

Мне довелось лично пообщаться со многими создателями цветных монет и протокола Mastercoin и принять участие в развитии обоих проектов. За два месяца исследований и совместной работы я понял, что все плюсы идеи создания высокоуровневых протоколов поверх низкоуровневых теряются из-за существенных недостатков в ее реализации, что может помешать этой идее вырасти в нечто большее.

И дело не в том, что сама задумка плоха. Задумка отличная, и реакция сообщества лишний раз доказала, насколько это востребовано. Причина скорее в том, что используемый протокол – биткойн – просто не очень подходит на роль базы для надстройки других протоколов. Это не делает бит-

койн ненужным или менее революционным изобретением: как протокол для хранения и передачи ценности он прекрасен, но в качестве низкоуровневого протокола – далеко не так эффективен. Если сравнивать его с другими протоколами, он похож не на TCP, поверх которого можно построить HTTP, а скорее на SMTP, который хорошо справится с конкретной задачей (для SMTP это работа с электронной почтой, а для биткойна – с деньгами), но едва ли подойдет в качестве основы для чего-либо еще.

Эта проблема объясняется конкретным свойством биткойна – его масштабируемостью. Сам по себе биткойн масштабируем ровно настолько, насколько это возможно для криптовалюты. Даже если размер блокчейна перевалит за терабайт, протокол под названием Simplified Payment Verification (SPV, «упрощенная проверка платежей»), описанный в вайтпейпере биткойна, позволит «легким клиентам» с пропускной способностью и объемом памяти всего в несколько мегабайт спокойно отслеживать прохождение транзакций. Однако с цветными монетами и Mastercoin эта возможность исчезает. Причина кроется в следующем: для определения цвета цветной монеты SPV будет недостаточно, и потребуется проследить весь ее путь вплоть до происхождения, на каждом этапе выполняя упрощенную проверку. Иногда обратное сканирование экспоненциально, и с протоколами метакойнов вовсе невозможно что-либо узнать без проверки каждой отдельной транзакции.

Именно эту проблему намерен решить Ethereum. Он задуман не как швейцарский нож с сотнями функций для удовлетворения любых потребностей, а как более совершенный базовый протокол, который заменит биткойн в качестве основы для других децентрализованных приложений, предложит им больше рабочих инструментов и позволит в полной мере использовать преимущества масштабируемости и эффективности Ethereum.

КОНТРАКТЫ НА ЧТО УГОДНО

Пока Ethereum еще разрабатывался, возрос интерес к финансовым контрактам на базе криптовалют. Основным типом контракта был «контракт на разницу цен» (CFD): в нем две стороны соглашаются внести некоторую сумму денег, а затем получить деньги в пропорции, которая зависит от стоимости некоторого базового актива. Например, Алиса вносит $1000, Боб – столько же, а через 30 дней блокчейн автоматически возвращает Алисе $1000 плюс $100 за каждый доллар, на который за это время выросла цена LTC/USD, а Бобу отправит оставшуюся сумму. Эти контракты позволяют людям спекулировать на активах с высоким кредитным плечом или, наоборот, защищать себя от волатильности криптовалют, избегая рисков без какого-либо централизованного обмена.

Однако сейчас ясно, что контракты на разницу цен – лишь

одна из имплементаций более глобальной идеи: контрактов по формуле. Недостаточно, чтобы контракт умел только брать у Алисы $x, у Боба $y, а затем возвращать Алисе $x + дополнительные $z за каждый доллар, на который подорожал данный актив. Он должен также уметь вернуть Алисе сумму, рассчитанную по любой математической формуле. Такая возможность позволит заключать контракты произвольной сложности. Если формула будет допускать любые входные данные, такие универсальные CFD можно использовать даже для p2p-игр. Чтобы выпустить CFD, Алисе нужно будет создать контракт, отправить на него криптовалюту на $1000 и дождаться, пока Боб примет контракт, также отправив транзакцию на $1000. Затем включится запрограммированный таймер, и через 30 дней они смогут отправить на контракт небольшую транзакцию, чтобы снова его активировать и разблокировать средства.

Пример кода контракта на Ethereum, написанный на высокоуровневом языке:

```
if tx.value < 100 * block.basefee:
stop
if contract.memory[1000]:
from = tx.sender
to = tx.data[0]
value = tx.data[1]
if to <= 1000:
stop
if contract.memory[from] < value:
```

```
    stop
    contract.memory[from] = contract.memory[from] –
value
    contract.memory[to] = contract.memory[to] + value
    else:          contract.memory[mycreator]          =
10000000000000000 contract.memory[1000] = 1
```

Но контрактами на разницу цен возможности не ограничиваются: вайтпейпер Ethereum описывает и другие виды транзакций, реализуемые с помощью его скриптов. Вот несколько из них.

▒ **ЭСКРОУ С МУЛЬТИПОДПИСЬЮ**, по духу напоминающий арбитражный сервис биткойна Bitrated, но с усложненными правилами. Например, подписавшимся не придется вручную обрабатывать частично подписанные транзакции: через блокчейн люди смогут асинхронно санкционировать вывод средств, и когда транзакцию подтвердит достаточное число участников, она совершится автоматически.

▒ Еще одна интересная функция – **СБЕРЕГАТЕЛЬНЫЕ СЧЕТА**. Предположим, Алиса хочет отложить крупную сумму, но не хочет рисковать всем, если ее приватный ключ потеряется или попадет в чужие руки. Она заключает контракт с Бобом, которому не готова довериться до конца, на следующих условиях: во-первых, Алиса может снять до 1 % в день; во-вторых, она может снять любую сумму с одобрения Боба; в-третьих, сам Боб может снять до 0,05 % в

день. Алиса не собирается снимать крупные суммы за один раз, а если захочет, то сможет сделать это через Боба, подтвердив ему свою личность. Если кто-то украдет приватный ключ Алисы, она поспешит обратиться к Бобу и переместить средства на другой контракт, пока вор не успел украсть больше 1 %. Если Алиса потеряет свой приватный ключ, Боб сможет восстановить ее средства, пусть это и займет какое-то время. А если сам Боб окажется злоумышленником, Алиса сможет вывести свои средства в 20 раз быстрее, чем он. Короче говоря, система защиты напоминает традиционный банкинг, но отличается от него тем, что основана не на одном лишь доверии к банку.

P2P-ИГРЫ. Любой вид протокола p2p-игр можно внедрить на базе Ethereum. Простейший из таких протоколов – контракт на разницу цен на основе случайных данных вроде хеша блока.

СОЗДАНИЕ СОБСТВЕННОЙ ВАЛЮТЫ. На базе внутренней памяти Ethereum вы можете создать внутри него совершенно новую валюту. Возможности создания валют позволяют сделать так, чтобы они взаимодействовали друг с другом, обеспечивали децентрализованный обмен и поддерживали множество других передовых функций.

В этом и есть главное преимущество кода Ethereum: его скриптовый язык создавался так, чтобы не иметь ограничений кроме системы комиссий, и поэтому на его основе можно закодировать любой вид правил. На блокчейне можно

даже управлять сбережениями целых компаний: создать, к примеру, контракт, по которому перемещение средств возможно только с разрешения 60 % акционеров (а 30 %, например, могут распоряжаться суммой максимум в 1 % в день). Возможны и другие структуры, менее традиционные для капиталистической реальности: например, демократические организации, членом которых можно стать только с согласия двух третей ее состава.

НЕ ТОЛЬКО ФИНАНСЫ

Но финансовые приложения – лишь малая доля того, на что способны Ethereum и созданные на нем протоколы. Хотя именно финансовые приложения Ethereum в первую очередь привлекают криптосообщество, не менее интересно предположить, какой результат может дать взаимодействие с нефинансовыми p2p-протоколами. Одна из главных проблем таких протоколов – отсутствие стимулов: они, в отличие от централизованных коммерческих платформ, не предлагают участникам финансовых выгод. Конечно, иногда участие в проекте – само по себе награда. Именно поэтому люди продолжают создавать софт с открытым исходным кодом, писать статьи для «Википедии», вести блоги и оставлять развернутые комментарии на форумах. Но вот в контексте p2p-протоколов увлеченность проходит очень быстро: процесс

поглощает безмерное количество ресурсов, демон[10] может без остановки работать в фоновом режиме, из-за чего процессор перегружается и расходует очень много электроэнергии.

Например, уже давно существуют протоколы данных вроде Freenet, готовые предоставить каждому нецензурируемый хостинг статического контента. По факту же Freenet работает очень медленно, и мало кто выделяет на него ресурсы. Все файлообменные протоколы преследует одна и та же проблема: если нашумевшие блокбастеры распространяют на них с завидным альтруизмом, то на что-то менее популярное энтузиазма уже не хватает. Парадоксально, но выходит, что обмен файлами между пользователями порой не просто не препятствует централизации развлекательной и медийной продукции, но даже ее усиливает. Однако все эти проблемы можно решить с помощью стимулов: дать людям возможность создавать в сети не только некоммерческие проекты, но и доходный бизнес.

ПООЩРИТЕЛЬНОЕ ХРАНЕНИЕ ДАННЫХ. Проще говоря, децентрализованный Dropbox. Идея такая: если пользователь захочет хранить в сети файл размером в 1 Гб, он создаст структуру данных, известную как дерево Меркла. Затем он заложит корень дерева вместе с 10 ETH в контракт и загрузит файл в другую сеть, за сообщениями

[10] Демон – программа, работающая в фоновом режиме без прямого взаимодействия с пользователем. – *Прим. пер.*

которой будут следить узлы, готовые сдать в аренду место на своих жестких дисках. Каждый день контракт будет автоматически выбирать случайную ветку дерева (например, «left – > right – > left – > left – > left – > right – > left»), заканчивая блоком файла, и выдавать 0,01 ETH первому узлу этой ветки. Узлы будут хранить весь файл целиком, чтобы максимально увеличить шанс получить вознаграждение.

BITMESSAGE И TOR. Bitmessage – это протокол электронной почты нового поколения, который одновременно и полностью децентрализован, и зашифрован, благодаря чему можно безопасно отправлять сообщения любому другому пользователю Bitmessage и не полагаться на третью сторону (кроме самой сети). Тем не менее у Bitmessage есть один большой недостаток в удобстве использования: вместо отправки сообщений на простой и понятный адрес вроде «bob@gmail.com» придется иметь дело с корявым 34-значным адресом Bitmessage (например, «BM-BcbRqcFFSQUUmXFKsPJgVQPSiFA3Xash»). Вот какое решение предлагает Ethereum: люди могут регистрировать свои имена при помощи специального контракта Ethereum, а клиенты Bitmessage – запрашивать блокчейн Ethereum предоставить адрес Bitmessage из 34 символов, секретно привязанный к любому имени. Эта схема может пригодиться и в анонимной сети Tor, пользователи которой тоже столкнулись с этой проблемой.

СИСТЕМЫ ИДЕНТИФИКАЦИИ И РЕПУТА-

ЦИИ. Раз в блокчейне можно зарегистрировать имя, логика подсказывает следующий очевидный шаг: создать на базе блокчейна систему Web of Trust (WOT, сеть доверия). Web of Trust – ключевой элемент эффективной коммуникативной инфраструктуры p2p: ведь вам нужно не просто знать, что конкретный публичный ключ связан с конкретным человеком, но и понимать, можно ли этому человеку вообще доверять. Решением становится использование соцсетей. Если вы доверяете А, А доверяет Б, а Б доверяет В, тогда есть большая вероятность, что вы хотя бы отчасти можете доверять В. Ethereum может стать слоем хранения данных для полностью децентрализованной системы репутаций, а в перспективе – полностью децентрализованной торговой площадкой.

Многие из вышеупомянутых кейсов – это реальные p2p-протоколы и проекты, которые уже активно разрабатываются. Мы намерены привлечь к сотрудничеству как можно больше подобных проектов и помочь им финансированием в обмен на вклад в экосистему Ethereum. Мы хотим помочь не только криптосообществу, но и p2p-сообществу в целом, включая файлообмен, торренты, хранение данных и ячеистые сети. Мы уверены, что существует множество проектов, потенциально ценных для сообщества, особенно в нефинансовой сфере, которые недополучают финансирование как раз из-за сомнений в их финансовом потенциале. Ethereum может помочь десяткам таких проектов сделать

долгожданный шаг вперед.

Почему все эти приложения можно построить на базе Ethereum? Ответ кроется во внутреннем программном языке. Проведем аналогию с интернетом. В 1996 году в сети не было другого языка, кроме HTML, и на нем можно было создавать лишь статические веб-страницы на сайтах вроде Geocities. Затем люди решили, что им нужна возможность отправлять формы в HTML, и добавили в него такую функцию. Получилось что-то вроде «цветных монет» для веб-протоколов: чтобы решить конкретную проблему, они дополнили слабый протокол, вместо того чтобы копнуть глубже. Но вскоре появился Javascript – язык программирования внутри веб-браузера. Именно он решил эту проблему: будучи универсальным, полным по Тьюрингу языком программирования, он подошел для создания приложений произвольной сложности. Gmail, Facebook и даже биткойн-кошельки – все это было создано с помощью Javascript. И дело не в том, что разработчики этого языка мечтали подарить людям Gmail, Facebook и биткойн-кошельки. Они просто хотели создать язык программирования. Возможности этого языка ограничиваются лишь нашим воображением, и именно этот дух мы хотим привнести в Ethereum. Задача Ethereum – стать не финалом инноваций в криптосфере, а их началом.

ДРУГИЕ ИННОВАЦИИ

Хотя Ethereum прежде всего ценен своим полным по Тьюрингу, универсальным скриптовым языком, он также имеет ряд преимуществ над другими блокчейнами.

КОМИССИИ. Функциональные возможности полноты по Тьюрингу допускают злоупотребления в транзакциях вроде пожирателей памяти или закольцованных скриптов. Контракты Ethereum будут предотвращать их благодаря комиссиям за транзакцию на каждом вычислительном этапе исполнения сценария. Более дорогие операции – например, доступ к хранению и криптографические операции – будут обходиться дороже, а также будет отдельная плата для каждого элемента хранения, который заполняет контракт. Чтобы стимулировать контракты «убирать за собой», например если они сокращают объем памяти, будет взиматься дополнительная, «негативная» комиссия. Более того, специальный опкод SUICIDE позволит аннулировать контракт и вернуть все сбережения и значительные «негативные» комиссии владельцу.

АЛГОРИТМЫ МАЙНИНГА. Многие ждут появления криптовалют, ограничивающих майнинг на специализированном оборудовании. Тогда люди с обычными компьютерами могли бы поучаствовать в этом процессе без каких-либо вложений, что позволило бы избежать централизации.

До сих пор главным противоядием был алгоритм майнинга Scrypt, который требует очень много вычислительной мощности и памяти. Но его требований к памяти недостаточно, к тому же некоторые компании производят устройства специально под этот алгоритм. Мы же хотим предложить Dagger – тестовый алгоритм proof of work с еще бóльшими требованиями к памяти, чем у Scrypt, а также тестовые алгоритмы proof of stake – например, Slasher, который вовсе не сталкивается с проблемой майнинга. Но рано или поздно мы собираемся провести конкурс, подобный тем, что определили стандарты для AES и SHA3. Мы пригласим исследовательские группы из университетов всего мира, чтобы разработать лучший из возможных майнинговых алгоритмов, устойчивых к специализированному оборудованию.

GHOST. Это новый протокол распространения блоков, впервые предложенный Авивом Зоаром и Йонатаном Сомполински. Он помогает блокчейну подтверждать блок гораздо быстрее, в идеале – в диапазоне 3–30 секунд, при этом избегая проблем с централизацией и задержкой записи транзакций, типичных при быстром подтверждении блоков. Ethereum – первая крупная криптовалюта, которая интегрирует в свой протокол упрощенную одноуровневую версию GHOST.

ПЛАН

Ethereum – крупное и масштабное начинание, и на его разработку уйдут месяцы. Поэтому запуск разделится на несколько этапов. Первый – публикация вайтпейпера – уже состоялся, у проекта появились форумы, википедия и блог, где любой желающий может зарегистрироваться и оставлять комментарии. 25 января на конференции в Майами запускается 60-дневный сбор средств, во время которого любой желающий сможет приобрести ETH – внутреннюю валюту Ethereum – за биткойны, как это было с Mastercoin. За 1 биткойн можно будет приобрести 1000 ETH, хотя для более ранних инвесторов курс будет примерно в два раза выше – в качестве компенсации за повышенный риск, на который они пошли, поддержав проект на ранних стадиях. Участники сбора средств получат не только эфиры, но и дополнительные вознаграждения: билеты на конференции, хранилище в 32 байта для первичного блока, а крупнейшие спонсоры – даже возможность придумать название для трех единиц исчисления валюты (вроде «микробиткойна» у биткойна).

Эмиссия ETH будет осуществляться не по какому-либо единому механизму: мы остановились на компромиссном варианте, сочетающем преимущества сразу нескольких подходов. Вот как это будет выглядеть.

- Эмиссия ETH состоится в рамках сбора средств по це-

не 1000–2000 ETH за BTC, причем первые спонсоры получат более выгодный курс в качестве компенсации за повышенный риск участия на более ранней стадии. Минимальный взнос составит 0,01 BTC. Предположим, что таким образом мы выпустим X эфиров.

- 0,225X ETH отправятся доверенным членам и самым первым спонсорам, которые существенно помогли проекту еще до начала сбора средств. Эта доля будет храниться на контракте с блокировкой по времени: около 40 % можно будет потратить через один год, 70 % – через два года и 100 % – через три года.
- 0,05X ETH уйдут на поощрение тех, кто помог во время сбора средств: эти средства пойдут на оплату расходов и вознаграждения в ETH поддержавшим проект между началом сбора средств и запуском валюты.
- 0,225X ETH войдут в долгосрочный резервный фонд для оплаты расходов, заработной платы и вознаграждений в ETH после запуска блокчейна.
- После этого каждый год будет добываться одинаковое количество ETH – 0,4X.

В отличие от биткойна и большинства других криптовалют, эмиссия ETH не ограничена. Модель «перманентной линейной инфляции» разработана таким образом, чтобы эфир не был подвержен ни инфляционным, ни дефляционным процессам. Отказ от лимита на эмиссию должен ослабить влияние спекуляций и имущественного неравен-

ства, которому подвержены существующие криптовалюты. В то же время линейная, а не традиционная экспоненциальная инфляционная модель подразумевает, что эффективная ставка инфляции со временем будет стремиться к нулю. Кроме того, поскольку валюта начнет свое существование не с нуля, увеличение валютной массы в первые восемь лет будет происходить медленнее, чем это было у биткойна, что даст ранним спонсорам и участникам сбора средств шанс получить значительную выгоду в среднесрочной перспективе.

Примерно в феврале мы готовим релиз централизованной тестовой сети – сервера, с помощью которого каждый сможет отправлять транзакции и создавать контракты. За ним последует децентрализованная тестовая сеть, в которой мы будем тестировать различные алгоритмы майнинга, проверять безопасность и работоспособность p2p-демона, а также проводить измерения, чтобы в дальнейшем оптимизировать скриптовый язык. Наконец, когда мы будем уверены в том, что протокол и клиент полностью безопасны, мы выпустим первичный блок и запустим процесс майнинга.

ЧТО ДАЛЬШЕ

Поскольку Ethereum использует полный по Тьюрингу скриптовый язык, можно математически доказать, что он способен на все, на что может быть способна криптовалюта на основе блокчейна, подобная биткойну. И все же про-

токол в его нынешнем виде не лишен недостатков. Например, Ethereum не решает фундаментальную проблему масштабируемости всех криптовалют на основе блокчейна: каждый полный узел должен хранить весь баланс и проверять каждую сделку. Ethereum несколько смягчает проблему за счет концепции разделения «дерева состояний» и «списка транзакций», заимствованной у Ripple, но никаких фундаментальных прорывов в этой области он пока предложить не может. Для этого необходима технология вроде Secure Computational Integrity and Privacy (SCIP) Эли Бен-Сассона, которая пока находится в стадии разработки.

Кроме того, Ethereum не предлагает никаких улучшений в области традиционного майнинга proof of work со всеми его недостатками, а возможности proof of excellence и консенсуса в стиле Ripple пока остаются неисследованными. Если выяснится, что proof of stake или какой-либо другой алгоритм proof of work предлагает лучшее решение, то будущие криптовалюты смогут перейти на такие алгоритмы proof of stake, как MC2 и Slasher. Если дело дойдет до Ethereum 2.0, то в первую очередь улучшения произойдут именно в этих областях. В конце концов, проект Ethereum не предполагает конечной цели, и при достаточном финансировании мы сможем запустить Ethereum 2.0 самостоятельно, перенеся балансы с первоначальных счетов в обновленную сеть. Как гласит девиз нашей платформы, мы ограничены лишь воображением.

Самоисполняемые контракты и фактическое право

БЛОГ ETHEREUM

24 февраля 2014 года

Многие концепции, которые мы предлагаем в Ethereum, могут показаться совершенно фантастическими, а иногда даже жуткими. Одна из них – так называемые смарт-контракты, которые исполняются самостоятельно, без необходимости или даже без возможности человеческого вмешательства. Роль человека ограничивается тем, что он создает напоминающие Скайнет «децентрализованные автономные организации», которые полностью существуют в облаке и управляют мощными финансовыми ресурсами. Такие виртуальные контракты могут сподвигнуть людей на вполне реальные действия в физическом мире – например, на создание децентрализованной «правовой системы на основе математики» или на реализацию утопической на первый взгляд модели общества, которая не строится на доверии к централизованным институтам. Неосведомленному пользователю, особенно если он не слышал даже о старом добром биткойне, трудно вообразить, как такое возможно и для чего это нужно. В этой серии статей мы разберем основные концепции Ethereum, объясним их значение, обсудим свойства, преимущества и недостатки.

Первую статью серии мы посвятим так называемым смарт-контрактам. Сама идея смарт-контрактов витала в воздухе несколько десятилетий, но свое современное имя и концептуальные очертания приобрела в 2005 году, когда Ник Сабо представил ее вниманию заинтересованной в криптографии публики. Суть термина очень проста: смарт-контракт – это контракт, который исполняется без постороннего вмешательства. Другими словами, если обычный контракт – это лист бумаги (или PDF-документ) с текстом, согласно которому одна сторона должна отправить деньги (или другую собственность) другой стороне при соблюдении определенных условий, то смарт-контракт – это компьютерная программа, которая сама автоматически выполняет эти условия. Ник Сабо использовал пример с вендинговыми автоматами:

> *Классический пример из реальной жизни – простой вендинговый автомат, можно сказать, примитивный предшественник смарт-контрактов. Он принимает монеты в пределах определенной суммы (сумма в кассе не должна превышать затраты злоумышленников на ее взлом) и за счет простого механизма – на уровне задач для студентов-программистов первого курса – выдает товар и сдачу в соответствии с указанной ценой. Вендинговый автомат – это контракт на предъявителя, то есть обмен с ним может совершить любой, у кого есть достаточно монет. Замки и другие защитные механизмы оберегают товары и*

монеты от взломщиков, и этого вполне достаточно, чтобы продавцам было выгодно использовать такие автоматы.

В смарт-контрактах тот же принцип применяется для, скажем так, самых широких задач. Например, финансовые смарт-контракты могут автоматически перемещать деньги на основании заданных формул и условий; смарт-контракт на продажу доменного имени может автоматически отдать его первому, кто заплатит за него $200; возможны даже страховые смарт-контракты, которые контролируют банковские счета и автоматически осуществляют выплаты на основании данных о событиях в реальном мире из надежного источника (или источников).

УМНАЯ СОБСТВЕННОСТЬ

Здесь, однако, возникает очевидный вопрос: как эти контракты будут исполняться? Традиционный контракт не стоит и цены листа бумаги, на котором он написан, пока, например, судья, обладающий законной властью, не гарантирует его исполнение. Со смарт-контрактами все то же самое: чтобы возыметь силу, они должны быть «встроены» в какую-то систему. Самое старое и очевидное решение – специальное оборудование, известное также как «умная собственность». Вендинговый автомат Ника Сабо – хороший пример такого решения. Ведь внутри автомата находится, можно сказать,

протосмарт-контракт с примерно таким компьютерным кодом:

```
    if button_pressed == “Coca Cola” and money_inserted
>= 1.75:
    release(“Coca Cola”)
    return_change(money_inserted – 1.75)
    else if button_pressed == “Aquafina Water” and
money_inserted >= 1.25:
    release(“Aquafina Water”)
    return_change(money_inserted – 1.25)
    else if …
```

Этот контракт имеет четыре привязки к внешнему миру: входные переменные button_pressed (нажать кнопку) и money_inserted (вставить деньги) и выходные команды release (выдать) и return_change (вернуть сдачу). В разных автоматах эти функции могут быть реализованы по-разному, но на первой мы останавливаться не будем, поскольку нажатие кнопки – задача несложная. Попытка выполнить этот контракт на Android-смартфоне образца 2007 года ни к чему бы не привела: он не сможет узнать, сколько денег внес покупатель, и уж точно не выдаст сдачу и бутылку колы. А вот в вендинговом автомате этот контракт приобретает «силу» за счет запасов колы и физической защиты, которая не позволяет взять напиток просто так, без соблюдения условий контракта.

Можно представить и другое, более футуристическое во-

площение умной собственности – например, в сфере аренды автомобилей. Вообразите мир, где у каждого в смартфоне есть собственный приватный ключ, и, если отправить $100 на конкретный адрес, автомобиль в течение суток будет автоматически подчиняться командам, подписанным этим ключом. Тот же принцип можно применить и к домам. Если для вас это звучит нереально, напомню, что уже сегодня некоторые офисные здания функционируют как умная собственность: для входа в них нужна карта доступа, и то, какую именно дверь сможет открыть ключ, определяет код, привязанный к базе данных. Более того, если компания использует HR-систему, которая автоматически обрабатывает трудовые контракты и активирует карты доступа новых сотрудников, это тоже своего рода смарт-контракт.

УМНЫЕ ДЕНЬГИ И ФАКТИЧЕСКОЕ ОБЩЕСТВО

И все же возможности физической собственности весьма ограничены. Уровень ее защиты невысок, поэтому интересных опций на сумму, превышающую несколько десятков тысяч долларов, практически не существует. И, в конце концов, самые интересные контракты связаны с перемещением денег. Но как реализовать их на практике? Собственно, прямо сейчас – никак. Теоретически мы можем предоставить контрактам учетные данные для доступа к нашим банковским

счетам, чтобы затем контракт отправлял оттуда средства при выполнении определенных условий, но такой контракт нельзя будет назвать «самоисполняемым». Одна из сторон контракта в любой момент сможет отключить его до наступления срока оплаты, или опустошить свой банковский счет, или попросту изменить свой пароль. В сущности, неважно, как контракт интегрирован в систему, ведь любая сторона всегда сможет его отключить.

Как же решить эту проблему? Для широкой аудитории ответ может показаться радикальным, но для тех, кто знаком с биткойном, это уже не новость: нам нужны деньги нового типа. На сегодняшний день эволюция денег прошла три этапа: товарные деньги; деньги, обеспеченные товаром; фиатные деньги. Товарные деньги устроены очень просто: они имеют ценность, потому что сами представляют собой товар с некоторой «внутренней» потребительской стоимостью. Лучшие примеры – золото и серебро, а в более традиционных обществах в этом качестве могут использовать чай, соль (минутка этимологии: отсюда произошло слово «зарплата» [11]), ракушки и прочее. Потом возникли деньги, обеспеченные товаром, – банки выпускали сертификаты, которые можно было обменять на золото. Наконец, появились фиатные деньги. Слово «fiat» в фиатных деньгах – то же, что и в библейском «fiat lux» («да будет свет»), только тут говорит не бог, а го-

[11] Английское слово salary произошло от латинского salarium (зарплата), которое, в свою очередь, произошло от sal – соль. – *Прим. пер.*

сударство, и говорит оно: «да будут деньги». Ценность фиатных денег обусловлена исключительно тем, что их выпускает государство и оно же принимает их (и только их) в качестве налогов и пошлин, а также предоставляет им другие преимущества.

Но вместе с биткойном у нас появился новый вид денег: фактические деньги. Фиатные и фактические деньги различаются тем, что первые кто-то создает и поддерживает – в нашем случае государство, но теоретически это может быть и какой-то другой агент, – а фактические деньги просто существуют. Фактические деньги – это просто баланс с некоторым набором правил его обновления, и пользователи сами выбирают, пользоваться такими деньгами или нет. Первым примером фактических денег стал биткойн, но есть и другие. Например, если пользователь примет новое правило, по которому баланс будет пополняться только биткойнами из определенной «первичной транзакции», мы получим так называемые цветные монеты – еще один вид фактических денег (если только эти цветные монеты сами не будут фиатными или обеспеченными товаром).

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.