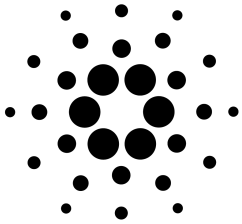

ЗАЧЕМ МЫ РАЗРАБАТЫВАЕМ CARDANO

Личное мнение

ЧАРЛЬЗ ХОСКИНСОН

<Charles.Hoskinson@iohk.io>

<C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66>

Международная лицензия Creative Commons Attribution 4.0

1. Введение

Мотивы

В 2015 году мы запустили проект Cardano, чтобы попытаться изменить то, как разрабатываются и проектируются криптовалюты. Цель, которая объединяет конкретные инновации — сконструировать устойчивую сбалансированную экосистему, которая лучше отвечает нуждам своих пользователей и лучше подходит для интеграции с другими системами, чем существующие.

Как часто бывает в случае проектов с открытым исходным кодом, у Cardano изначально не было ни четкого плана развития, ни даже солидного технического описания. У нас был просто набор принципов проектирования, передовых практик разработки и направлений исследования. Например:

- Разделить бухгалтерию и компьютерные расчеты (это должны быть отдельные уровни).

Международная лицензия Creative Commons Attribution 4.0

- Реализовать ключевые компоненты с использованием модульного функционального кода.

- Небольшие группы ученых и разработчиков должны параллельно проводить независимые рецензированные исследования одних и тех же тем.

- Подключить команды из других дисциплин — например, обратиться к специалистам по информационной безопасности на ранних этапах развития проекта.

- Быстро переключаться между созданием технических описаний, их реализацией и новыми исследованиями, необходимыми по результатам анализа выполненной работы.

- Встроить возможность вносить изменения в уже запущенные системы без разрушения существующей сети.

- Разработать механизм децентрализованного финансирования для дальнейшей работы.

- Проектировать криптовалюту с оглядкой на будущее — это позволит запускать ее на мобильных устройствах с удобным и понятным пользователю интерфейсом.

- Привлекать стейкхолдеров к разработке и поддержке криптовалюты, которой они пользуются.

- Принять во внимание необходимость учета различных активов в одном реестре.

- Добавить возможность включать в транзакции метаданные для лучшего соответствия нуждам существующих систем.

- Аккумулировать опыт около 1000 существующих альтернативных валют и заимствовать удачные решения.

- Использовать стандартоориентированный процесс по примеру IETF (Internet Engineering Task Force, рус. Инженерный совет Интернета) для утверждения окончательного вида протокола.

Международная лицензия Creative Commons Attribution 4.0

- Исследовать социальные аспекты коммерческой деятельности.

- Найти разумный компромисс между регулирующими органами и субъектами, осуществляющими коммерческую деятельность, сохранив верность ключевым принципам, унаследованным от Bitcoin.

Вооружившись таким неструктурированным списком идей, основатели Cardano начали изучение литературы по криптовалютам и разработку нужных абстракций. Результатом этих исследований стали: обширная библиотека статей IOHK, многочисленные результаты опросов — например, обзор скриптовых языков или Ontology of Smart Contracts (рус. "Онтология умных контрактов"), а также проект Scorex. Индустрия криптовалют переживает необыкновенно бурное развитие, и в некоторых случаях оно не идет ей на пользу.

Во-первых, в отличие от многих успешных протоколов — например, TCP/IP — при проектировании криптовалют редко уделяют внимание разделению на уровни. Причина тому — желание сохранить единый взгляд на факты и события, записанные в одном реестре, вне зависимости от того, оправданное это решение или нет.

Например, Ethereum в попытках превратиться в универсальный мировой компьютер стал слишком сложным — но при этом страдает от тривиальных проблем, которые могут мешать ему быть средством накопления. Нужно ли всем программам получать одинаковые ресурсы вне зависимости от их экономической ценности, расходов на содержание или требований законодательства?

Во-вторых, современные исследования в области криптовалют редко опираются на предыдущие находки в области криптографии. Например, в защите Bitshares по методу proof of stake можно было бы сделать простую и надежную генерацию случайных чисел с использованием техники подбрасывания монеты с гарантированной производительностью, которая была известна еще с восьмидесятых (см. оригинальную статью авторов Rabin и Ben-Or).

В-третьих, большинство альтернативных валют (за некоторыми исключениями вроде Tezos) не учли необходимость вносить изменения в будущем. Возможность успешно провести софтфорк или хардфорк ("мягкую" или "жесткую" модификацию протокола) — залог долгосрочного успеха любой криптовалюты.

Естественно, корпоративные пользователи не могут доверить ресурсы стоимостью в миллионы долларов протоколам, в которых план развития и стоящие за ним взгляды

Международная лицензия Creative Commons Attribution 4.0

людей недальновидны, ограничены или слишком радикальны. Для того, чтобы сформировать общественный консенсус по поводу того, как развивается протокол, необходим эффективный процесс. Если этот процесс слишком сложен, то неизбежна фрагментация, которая может привести к расколу сообщества.

Наконец, деньги — это исключительно общественное явление. Пытаясь обеспечить анонимность и уменьшить количество посредников, Bitcoin и его современники решили не обращать внимания на то, какое значение имеют идентификация личности, передача метаданных и репутация в коммерческих транзакциях. Добавление метаданных посредством централизованных решений исключает прозрачный аудит, доступность по всему миру и неизменяемость, а именно из-за этих качеств и стоит использовать блокчейны (распределенные базы данных).

Существующие финансовые системы, например, на основе SWIFT, FIX или ACH, добавляют в транзакции множество метаданных. Недостаточно просто знать, какое количество стоимости переместилось с одного счета на другой. Кроме этого, законы зачастую требуют идентификацию лиц, совершающих транзакцию, персональные данные, отчеты о подозрительной активности и другую информацию или действия. В некоторых случаях метаданные транзакции более важны, чем сама транзакция.

Итак, разумно предположить, что изменение метаданных транзакции может нанести такой же вред, как подделывание валюты или переписывание истории транзакций. Отказ предоставить участникам системы возможность по их желанию включать эти данные в транзакцию выглядит непродуктивным с точки зрения популяризации системы и защиты прав пользователей.

Вкратце о концепции

Мы исследовали область криптовалют, ища возможности реализовать эти принципы, и результатом стали два набора протоколов. Это криптовалюта, использующая защиту proof of stake [1][2] с математически доказанной эффективностью, которую мы назвали Cardano Settlement Layer или CSL (рус. "Уровень заключения сделок"), а также набор протоколов Cardano Computation Layer или CCL (рус. "Вычислительный уровень").

При проектировании мы уделяем особенное внимание общественной природе криптовалют. Поэтому мы создали два уровня, разделив бухгалтерский учет и машинные вычисления, а также учли нужды регулирующих органов в соответствии с рядом

Международная лицензия Creative Commons Attribution 4.0

непреложных принципов[1]. Кроме этого, при необходимости мы подвергаем предлагаемые протоколы рецензированию и проверяем код на соответствие формальным спецификациям.

Защита по методу proof of stake

По поводу использования метода proof of stake для криптовалют ведутся ожесточенные споры. Мы решили его использовать, потому что он предоставляет возможности для безопасного голосования, легче масштабируется и позволяет воплотить большее количества нестандартных премиальных схем.

Наш протокол, основанный на методе proof of stake, называется Ouroboros (рус. "Уроборос"). Его разработала команда талантливых криптографов из пяти научных учреждений[2], которую возглавляет профессор Aggelos Kiayias из Эдинбургского университета. Кроме того, что безопасность протокола математически доказана с использованием точной криптографической модели, новизна протокола состоит в его гибкой модульной реализации. Таким образом можно создавать множество протоколов в зависимости от того, какая нужна функциональность.

Модульность дает такие возможности, как делегация, сайдчейны (sidechains), улучшенные структуры данных для облегченных клиентов, различные формы генерации случайного числа и даже различные допущения для синхронизации. Когда количество пользователей в сети вырастает с тысяч до миллионов и даже миллиардов, требования к алгоритму консенсуса для этой сети тоже меняются. Поэтому в систему должна быть заложена гибкость, необходимая для адаптации к таким изменениям. Только так ядро криптовалюты выдержит проверку временем.

Социальные аспекты денег

Криптовалюты хорошо иллюстрируют социальные аспекты денег. Если говорить только о технической стороне криптовалют, то различий между Bitcoin и Litecoin не так уж много.

[1] Список можно найти в разделе "Регулирование"
[2] Коннектикутский университет, Афинский университет, Эдинбургский университет, Орхусский университет, Токийский технологический институт

Международная лицензия Creative Commons Attribution 4.0

Еще меньше их между Ethereum и Ethereum Classic. Но и Litecoin, и Ethereum Classic — проекты с большой рыночной капитализацией, динамичным сообществом, а также собственными социальными обязательствами.

Можно сказать, что огромная часть ценности криптовалюты — это ее сообщество, то, как оно использует криптовалюту, и уровень вовлеченности сообщества в развитие валюты. Продолжая эту мысль, валюты вроде Dash встроили прямо в протокол системы, которые позволяют сообществу решать, что именно разрабатывать и спонсировать.

Анализируя огромное количество криптовалют, можно четче увидеть их социальные аспекты. Случается, что сообщество не достигает соглашения по вопросам философии или финансовой политики или возникают разногласия между ключевыми разработчиками — это ведет к фрагментации и изменениям протокола. В отличие от криптовалют, обычные бумажные валюты супердержав переживают и смены власти, и различные разногласия — и все это без валютных кризисов или массового ухода пользователей.

Таким образом можно предположить, что в привычных валютных системах есть некоторые элементы, отсутствующие в криптовалютах. Мы утверждаем — и даже внесли это в план развития Cardano — что у пользователей протокола должна быть мотивация понимать общественный контракт, стоящий за этим протоколом, а также свобода предлагать продуктивные изменения. Эта свобода касается всех аспектов системы обмена стоимостью — от решений по регулированию рынков до решений по спонсированию проектов. Однако это нельзя реализовать путем введения какого-то централизованного органа или специальных разрешений, которые может приобрести хорошо обеспеченное меньшинство участников.

Cardano введет систему оверлейных протоколов на основе CSL, чтобы отвечать потребностям своих пользователей.

Вне зависимости от успешности краудсейл-продаж для начала разработки средства рано или поздно закончатся. Поэтому в Cardano будет включен децентрализованный фонд[3], который будет финансироваться посредством постепенно уменьшающейся инфляции и комиссий за транзакции.

Любой пользователь должен иметь право запросить средства из фонда, используя специальную систему, а стейкхолдеры CSL проголосуют за то, кто именно их получит. Этот процесс обеспечивает полезную обратную связь, как в других криптовалютах с

[3] Она также известна как treasury system (рус. "система казначейства").

Международная лицензия Creative Commons Attribution 4.0

системами инвестиций/фондов, например, Dash. Таким образом начинается диалог о том, кого именно следует спонсировать.

Дискуссии о распределении фондов обеспечивают понимание краткосрочных и долгосрочных целей, общественного контракта криптовалюты, ее приоритетов, а также уверенность в том, что определенные предложения создают стоимость. Этот диалог означает, что сообщество постоянно оценивает и обсуждает свои убеждения относительно возможных путей развития.

Во-вторых, мы надеемся, что в Cardano со временем появится формальная система на основе блокчейна, чтобы предлагать изменения и голосовать по поводу софтфорков и хардфорков. Bitcoin и обсуждения размера блоков, Ethereum и хардфорк DAO — многие криптовалюты в свое время вели или все еще ведут долгие споры о техническом и моральном направлении развития кода.

Здесь можно и нужно сказать, что многие из подобных разногласий и расколы сообщества, следующие за ними возникают именно потому, что не существует стандартного процесса для обсуждения изменений.

Что нужно сделать, чтобы убедить пользователей Bitcoin принять софтфорк Segregated Witness? Как главным разработчикам Ethereum понять, насколько сообщество настроено спасать организацию DAO? Если в сообществе происходит раскол — криптовалюта уже не подлежит восстановлению?

В худшем случае право каждого пользователя принимать решения по поводу криптовалюты заменится на права тех, у кого есть штат разработчиков, связи и деньги — и их решения не будут отражать пожелания большинства членов сообщества. А если значительная часть членов сообщества не хочет или не может выразить свое мнение или исключена из процесса в результате каких-либо решений^{[4](#footnote4)}, как узнать, что они думают по поводу этих решений?

Некоторые криптовалюты, к примеру, Tezos, предлагают интересную модель, в которой протокол криптовалюты — это конституция, состоящая из трех разделов (Транзакция, Консенсус и Сеть) и набора формальных правил и процессов по изменению конституции. Тем не менее в этой модели еще нужно провести огромную работу с премиальными схемами и с тем, как моделировать и изменять криптовалюту, применяя формальный язык.

Международная лицензия Creative Commons Attribution 4.0

Использование формальных методов, понятных компьютеру спецификаций, а также использование казначейства в этом процессе для премиальных схем — вот направления, в которых, возможно, стоит работать. В конце концов, даже возможность открыто и без цензуры предложить изменение протокола уже улучшит процесс, даже если не получается придумать более элегантные решения.

Проектирование по уровням. Cardano Settlement Layer (Уровень заключения сделок)

Если вы хотите спроектировать по-настоящему хороший протокол или язык программирования, смотреть нужно не в будущее, а в прошлое. История знает множество идей, которые прекрасно выглядели на бумаге, но почему-то не прижились — примером тому стандарт Open Systems Interconnection. Истории также известны и счастливые случайности — от TCP/IP до JavaScript.

И вот некоторые принципы, которым учит нас история:

1. Будущее предсказать невозможно, поэтому всегда оставляйте место для маневра
2. Сложность выглядит красиво на бумаге, но выигрывает обычно простота
3. У семи нянек дитя без глазу
4. Стандарт, принятый первым, скорее всего приживется — даже если он не самый оптимальный
5. Из плохой идеи на самом деле можно сделать хорошую — было бы желание

Cardano — финансовая система, которая учитывает собственную общественную природу. Такая система должна обладать невероятной гибкостью и уметь обрабатывать транзакции пользователя произвольной степени сложности. Если проект будет успешным, понадобится огромное количество вычислительных мощностей, памяти и сетевых ресурсов, чтобы обрабатывать миллионы транзакций одновременно.

Но на выручку не придет этакий цифровой децентрализованный Робин Гуд, который отберет у богатых узлов и воздаст бедным, чтобы в нашей сети все получилось по справедливости. И не стоит полагаться на человеческое милосердие — люди не будут альтруистически жертвовать своими интересами во имя процветания сети. Итак, Cardano берет у TCP/IP концепцию "разделения обязанностей".

Международная лицензия Creative Commons Attribution 4.0

Блокчейны — это прежде всего базы данных, которые упорядочивают факты и события, гарантируя их неизменяемость и верные временные отметки. Если говорить о финансовой стороне, блокчейны упорядочивают данные о принадлежности активов. Добавление возможности сложных вычислений путем хранения и запуска программ — это совершенно другая задача. Итак, мы хотим просто узнать, сколько денег Алиса передает Бобу, или же нам нужно узнать всю полную историю транзакции и сколько стоимости пересылается в итоге?

Хочется выбрать второй вариант, как и сделали в Ethereum, потому что этот вариант обеспечивает больше гибкости. Но это — нарушение принципов проектирования, описанных выше. Если мы хотим знать историю транзакции, это значит, что один и тот же протокол должен понимать произвольные события, создавать произвольные транзакции, обеспечивать арбитраж в случаях мошенничества — и даже, возможно, отменять транзакции после получения некоторой ранее недоступной информации.

Придется принимать сложные решения о том, какие именно метаданные следует хранить для каждой транзакции. Какие элементы полной истории, стоящей за транзакцией от Алисы к Бобу, для нас важны? Будут ли они оставаться важными всегда? Когда можно будет удалить некоторые данные? Не нарушит ли удаление этих данных законы некоторых стран?

Кроме того, некоторые вычисления сами по себе не подлежат огласке. Например, если нужно рассчитать среднюю зарплату сотрудника в офисе, мы, возможно, не захотим раскрывать информацию о том, сколько каждый из них зарабатывает по отдельности. А если любая информация о вычислениях известна любому желающему? Что, если такая публичность влияет на порядок вычислений, меняя конечный результат?

Поэтому мы придерживаемся позиции, что расчет передаваемой стоимости должен производиться отдельно от истории того, почему именно произошла передача стоимости. Другими словами, следует разделять передачу стоимости и вычисления. Такое разделение не означает, что Cardano не будет поддерживать умные контракты. Напротив, поскольку мы явно разделяем эти уровни, система становится более гибкой в том, что касается проектирования, использования, конфиденциальности и исполнения умных контрактов.

Реестр стоимостей называется Cardano Settlement Layer. Поскольку его задача — перемещение стоимости, в плане развития указаны следующие цели:

Международная лицензия Creative Commons Attribution 4.0

1. Поддержка двух наборов скриптовых языков — один для перемещения стоимости, другой для улучшения поддержки оверлейных протоколов
2. Поддержка протокола KMZ sidechains[4] для связи с другими реестрами
3. Поддержка различных типов подписей, включая квантово-устойчивые подписи, отвечающие высоким требованиям безопасности
4. Поддержка различных активов, выпущенных пользователями
5. Возможность масштабирования — чем больше присоединяется пользователей, тем больше ресурсов у системы

Скрипты

Начиная со скриптовых языков программирования, для совершения транзакции между адресами в реестре нужен определенный скрипт — сценарий, который выполняется для проверки подлинности транзакции. В идеале мы не хотим, чтобы Ева получила доступ к деньгам Алисы, и, конечно, не хотим, чтобы плохо составленный скрипт случайно послал деньги на нерабочий адрес без возможности восстановления средств.

В таких системах, как Bitcoin, есть очень жесткий скриптовый язык. На нем сложно разрабатывать транзакции, о которых говорится выше, его сложно читать и понимать. Но языки общего назначения, подобные Solidity, очень усложняют систему, и их можно использовать только для небольшого количества участников.

Учитывая все это, мы решили спроектировать новый язык Simon[5], названный в честь его автора Саймона Томпсона (Simon Thompson) и автора концепции, лежащей в его основе — Саймона Пейтона Джонса (Simon Peyton Jones). Simon — специфичный для области (domain-specific) язык, основанный на статье Composing contracts: an adventure in financial engineering.

Ключевая идея — финансовые транзакции состоят из набора основных элементов[6]. Если собрать финансовую "таблицу элементов", то можно будет поддерживать сколь угодно большой набор сложных транзакций. В этот набор войдет большинство распространенных типов транзакций (или даже все распространенные транзакции), и для этого не понадобится универсальная программируемость.

---

[4] Скоро в статье авторства Kiayias, Zindros и Miller
[5] Подробности можно будет найти в готовящейся к выпуску статье. Полная версия языка будет поддерживаться после релиза Shelley CSL, который запланирован на четвертый квартал 2017 года
[6] Проект ACTUS предоставляет более подробную информацию.

Международная лицензия Creative Commons Attribution 4.0

Самый главный плюс — будет понятно, почему система безопасна и как она работает. Можно написать доказательства для проверки правильности шаблонов и предотвращения мошенничества при помощи транзакций — например, создания новых денег из воздуха или деформации транзакций. Во-вторых, таким образом остается возможность добавлять новые элементы, используя софтфорки, если понадобится новая функциональность.

И все-таки всегда будет необходимость соединять CSL с оверлейными протоколами, старыми финансовыми системами и специализированными серверами. Поэтому мы разработали Plutus — одновременно в качестве и универсального языка программирования для умных контрактов, и специализированного языка для совместимости с другими системами.

Plutus — типизированный функциональный язык программирования, основанный на концепциях из Haskell, который можно использовать для написания произвольных скриптов транзакций. В контексте CSL этот протокол будет использоваться для сложных транзакций, чтобы добавить поддержку для других уровней, к которым нужно подключаться — например, к системе сайдчейнов.

Сайдчейны

Для работы с сайдчейнами Cardano будет поддерживать новый протокол авторов Kiayias, Miller и Zindros (KMZ sidechains). Протокол основан на предыдущих результатах доказательств proof of work. Описание устройства протокола выходит за пределы этой статьи; скажем лишь, что его концепция позволяет передать средства из CSL в любой другой блокчейн, поддерживающий этот протокол — например, Cardano Computation Layer.

Протокол KMZ sidechains заключит сложность в системе внутри себя. Реестры с регулятивными требованиями, конфиденциальные операции, различные скриптовые языки и другие особые случаи остаются для CSL "черными ящиками", но пользователь CSL получает определенные бухгалтерские гарантии и возможность отозвать транзакцию после того, как расчеты окончены.

Подписи

Международная лицензия Creative Commons Attribution 4.0

Чтобы безопасно передать стоимость от Алисы к Бобу, Алисе нужно подтвердить, что у нее есть право на передачу этой стоимости. Самый прямой и надежный способ подтверждения — использовать схему получения электронно-цифровой подписи с помощью открытого ключа, в которой средства привязаны к открытому ключу, а у Алисы есть соответствующий закрытый ключ.

Существуют сотни возможных решений с различными допущениями и параметрами безопасности. Некоторые из них полагаются на решение математических задач, связанных с эллиптическими кривыми, другие связаны с необычными концепциями, использующими решетки.

Но абстрактная цель всегда остается одной и той же. Существует сложная задача, которую нельзя решить без знания определенной информации. Тот, кто знает эту информацию, называется владельцем ключа, и только он может им пользоваться.

Существует две группы проблем, которые приходится решать, выбирая схему подписей. Во-первых, схема должна быть безопасной даже спустя долгое время. Некоторые криптографические схемы, использовавшиеся в 1970 и 1980 гг — к примеру, DES — на сегодняшний день уже взломаны. Следует решить, какое время схема должна гарантированно оставаться рабочей.

Во-вторых, существует много предприятий, правительств и других учреждений, которые предпочитают или предписывают использовать определенную схему. Например, Агенство национальной безопасности США использует набор протоколов NSA Suite B Cryptography. Есть стандарты ISO и даже рабочие группы W3C по криптографии.

Если для криптовалюты выбрана только одна схема подписей — приходится учитывать, что в определенный момент в будущем ее могут взломать, и кроме того, как минимум одна организация не сможет использовать эту криптовалюту из-за государственных или отраслевых ограничений. С другой стороны, криптовалюта не может поддерживать абсолютно все схемы — так каждый клиент должен будет понимать и проверять правильность любой из схем.

Для Cardano мы решили начать с использования криптографии на основе эллиптических кривых — в частности, кривой Ed25519. Также мы решили улучшить уже существующие библиотеки, добавив поддержку технологии HD wallets на основе спецификации Дмитрия Ховратовича и Джейсона Лоу (Jason Law)[7].

[7] Вот документация по реализации технологии HD Wallets в Cardano. Насколько нам известно, Cardano — первая криптовалюта, поддерживающая технологию Ed25519 HD Wallets

Международная лицензия Creative Commons Attribution 4.0

В будущем Cardano станет поддерживать и другие криптографические схемы. В частности, мы хотим интегрировать BLISS-B, чтобы добавить в нашу систему возможность использовать квантово-устойчивые подписи. Кроме того, мы хотели бы добавить SECP256k1, чтобы улучшить взаимодействие с существующими криптовалютами, например, Bitcoin.

При разработке в Cardano были добавлены специальные расширения, которые позволят добавлять схемы подписей через софтфорк. Мы будем добавлять их по необходимости во время крупных обновлений, указанных в плане развития[8].

Активы, выпускаемые пользователем (User Issued Assets, UIA)

В ранней истории Bitcoin быстро разрабатывались протоколы, позволяющие пользователям выпускать собственные активы. Эти активы работали на основе системы расчетов Bitcoin, отслеживая несколько разных криптовалют одновременно. Такие протоколы не поддерживались протоколом Bitcoin по умолчанию — они были добавлены с помощью разных хитрых решений.

В случае других криптовалют, основанных на Bitcoin, например, Colored Coins и Mastercoin (нынешнее название —Omni), облегченным клиентам приходится полагаться на доверенные сервера. Кроме того, комиссия за транзакции все равно выплачивается в биткоинах. Эти факты, а также наличие только одного канала для обработки всех транзакций делают Bitcoin неоптимальным для учета разных активов.

В случае Ethereum, который использует стандарт ERC20, есть больше свободы для реализации различных функций. Но для того, чтобы оплатить комиссию, все-таки нужен эфир. Кроме того, сеть Ethereum недостаточно масштабируема, чтобы отвечать требованиям всех существующих токенов ERC20.

Эта фундаментальная проблема состоит из трех частей: ресурсы, премиальные схемы и согласие. Говоря о ресурсах — если в один и тот же реестр мы добавляем другую криптовалюту, это значит, что теперь в реестре сосуществуют два независимых набора UTXO (unspent transaction inputs, "неистраченные входы транзакций"), которые делят между собой пропускную способность канала, мемпул и место в блоке. Узлам консенсуса, ответственным за обработку транзакций в этих валютах, нужна мотивация для того,

[8] См. cardanoroadmap.com

Международная лицензия Creative Commons Attribution 4.0

чтобы это делать. И не каждый пользователь криптовалюты будет — или должен — заботиться о какой-то другой валюте.

Таким образом, есть огромное преимущество в том, что основной токен реестра с несколькими активами может служить "связующей валютой" для формирования децентрализованного рынка. Специализированные активы можно издавать для дополнительных целей, например, активы с фиксированной стоимостью вроде Tether или MakerDAO, которые используются для кредитования и денежных переводов.

Учитывая имеющиеся сложности, в Cardano мы постарались прагматично подойти к учету нескольких активов одновременно. Разработка ведется поэтапно: первая задача — спроектировать инфраструктуру, необходимую для поддержки тысяч разных активов. В частности, необходимы следующие улучшения:

1. Специальные аутенцифицированные структуры данных, позволяющие отслеживать состояние огромного количества UTXO
2. Возможность сделать распределенный мемпул, способный хранить огромную очередь транзакций
3. Разделение блокчейна на части и поддержка контрольных точек — для того, чтобы сделать возможным появление огромного глобального блокчейна
4. Премиальная схема, которая будет мотивировать узлы консенсуса включать в блоки различные наборы транзакций
5. Механизм подписки, позволяющий пользователям решать, какие валюты они хотят отслеживать
6. Гарантия того, что пользовательские активы получают такую же безопасность, как и основной актив
7. Обеспечение децентрализованного поддержания двусторонних котировок для увеличения ликвидности между пользовательскими активами и основным токеном

Наши ранние попытки найти подходящую аутентифицированную структуру данных закончились созданием нового типа AVL+ дерева, совместно разработанного Leo Reyzin, IOHK и Waves. Необходимы дальнейшие исследования, но это фундаментальное улучшение уже будет включено в одну из следующих версий Cardano.

Распределенный мемпул можно реализовать, используя протокол RAMCloud Стэнфордского университета. В третьем квартале 2017 года мы начнем исследовать возможность интегрировать его с уровнем заключения сделок Cardano.

Международная лицензия Creative Commons Attribution 4.0

Остальные темы связаны между собой, и по ним уже ведутся исследования. По результатам этих исследований мы надеемся включить протокол для UIA в Cardano во время релиза CSL Basho в 2018 году.

Масштабируемость

Распределенные системы состоят из набора компьютеров (сетевых узлов), которые выполняют протокол или пакет протоколов, преследуя общую цель. Этой целью может быть распространение файла, как в протоколе BitTorrent, или фолдинг белка, как в протоколе Folding@Home.

В случае самых эффективных протоколов ресурсов становится больше, когда в сети появляются новые узлы. Например, средняя скорость скачивания файла с BitTorrent будет в среднем намного выше, если его качают одновременно много пиров. Скорость увеличивается, потому что пиры не только потребляют, но и предоставляют ресурсы. Именно эту характеристику имеют в виду, когда говорят, что распределенная система является масштабируемой.

Сложность со всеми уже существующими криптовалютами в том, что они изначально не проектировались как масштабируемые. Скажем, блокчейн в общем случае — это цепочка блоков, в которой блоки расположены один за другим. Безопасность и доступность в протоколе блокчейна обеспечивается тем, что у большого количества узлов есть полная копия всех данных блокчейна. Таким образом, один и тот же байт данных нужно копировать столько раз, сколько узлов в сети. Дополнительные узлы не предоставляют дополнительных ресурсов.

Это же касается и обработки транзакций, и передачи сообщений в системе. Добавление большего количества узлов в систему достижения консенсуса не создает дополнительного ресурса для обработки транзакций. На выполнение той же самой работы придется затрачивать большее количество ресурсов. Бывает, сообщения приходится передавать через несколько узлов, а значит, еще больше узлов будут передавать одно и то же сообщение, чтобы синхронизировать всю сеть с самым новым блоком.

С такой топологией криптовалюты не могут масштабироваться до глобального уровня с тем же успехом, что и традиционные финансовые системы. Инфраструктура традиционных финансовых систем хорошо масштабируется, и у них на порядок больше ресурсов для обработки и хранения информации. Добавим, что, например, Bitcoin —

Международная лицензия Creative Commons Attribution 4.0

очень маленькая сеть по сравнению с остальными платежными системами, но уже сейчас она с трудом справляется с нагрузкой.

В масштабировании Cardano очень поможет наш алгоритм консенсуса. Ouroboros позволяет децентрализованно выбрать кворум узлов консенсуса, а эти узлы запускают более привычные протоколы, разработанные за последние 20 лет для компаний с огромной инфраструктурой, например, Google или Facebook[9].

Избрание кворума для эпохи означает, что у нас есть проверенный набор узлов, занимающихся администрированием реестра на протяжении определенного времени. Можно просто избрать одновременно несколько кворумов и распределить транзакции между ними.

Такую же технику можно применять для расширения сети и сегментирования блокчейна. Мы запланировали применение методов масштабирования к алгоритму Ouroboros на 2018 год и продолжим работу над этой проблемой в 2019 и 2020.

Cardano Computation Layer (Вычислительный уровень)

Как отмечалось ранее, любая транзакция состоит из двух компонентов. Первый — механизм для передачи токенов и документирования их потока; второй — причины и условия перемещения токенов. Второй компонент может иметь произвольную сложность и включать терабайты данных, множество различных подписей и записей о случившихся событиях. А может быть очень простым — передача денег с одного адреса на другой, подтвержденная одной подписью.

При моделировании причин и условий, сопутствующих передаче стоимости, главная сложность заключается в том, что все они зависят от конкретных участников транзакции — и порой самым неожиданным образом. Область контрактного права рисует нам еще более нерадостную картину: действующие лица иногда и сами не в курсе, что транзакция не соответствует происходящему на рынке. Обычно мы называем это явление "семантический разрыв"[10].

Зачем разрабатывать криптовалюту с бесконечными уровнями сложности и абстракции? Это по сути сизифов труд — и на практике такая задумка очень наивна. Кроме того,

[9] Есть и другие протоколы, преследующие те же цели, например, Elastico и Bitcoin-NG.
[10] Loi Luu с соавторами освещают эту разницу в своей последней статье об умных контрактах, Making Smart Contracts Smarter.

Международная лицензия Creative Commons Attribution 4.0

любая абстракция имеет последствия — как с точки зрения закона, так и с точки зрения безопасности.

В Сети существует множество видов деятельности, которые весь мир считает незаконными или недостойными: скажем, работорговля, распространение детской порнографии, продажа государственных секретов. Создание устойчивой децентрализованной инфраструктуры одновременно создает и канал для подобных видов деятельности, уровень устойчивости к цензуре в котором такой же, как для обычных денежных переводов. С юридической точки зрения неясно, станут ли узлы консенсуса (которые мотивированы со временем объединяться для более эффективной работы) считаться ответственными за содержимое, которое они хранят.

Судебный процесс над операторами Tor, жестокое обращение с оператором Silk Road и отсутствие ясности в законах насчет защиты участников протокола — все довольно туманно. Несложно представить, чему еще может поспособствовать достаточно развитая криптовалюта (см. Ring of Gyges). Разумно ли принуждать всех пользователей криптовалюты одобрять — или хотя бы делать возможным — все самое худшее, что может водиться в Сети?

К сожалению, на этот вопрос нет четких ответов, которые бы помогли создателям криптовалюты. Здесь нужно выбрать позицию и ее придерживаться. И у Cardano, и у Bitcoin есть общее преимущество, которое состоит в том, что в них проблемы разделяются по уровням. У Bitcoin есть Rootstock. У Cardano — Cardano Computation Layer.

Так ограничение функциональности может предоставить пользователям разумную защиту. Большинство из существующих правительств не считают использование или поддержку криптовалют незаконным действием. Следовательно, у большинство пользователей будет возможность поддерживать реестр, который сравним по функциональности с платежной системой.

Если кому-то понадобится расширить функциональность — есть два варианта. Первый — функциональность расширяется усилиями группы единомышленников и по природе своей временна (например, партия в покер). Второй — функциональность расширяется за счет реестра с возможностями, сравнимыми с Ethereum. В обоих случаях события отдаются на обработку другому протоколу.

В случае частного, временного события разумно отойти от парадигмы блокчейна и ограничить усилия созданием библиотеки MPC-протоколов (протоколов

Международная лицензия Creative Commons Attribution 4.0

конфиденциального вычисления), которые при желании может воспользоваться группа единомышленников. Расчеты и другая деятельность координируются частной сетью, а CSL используют только в качестве безопасной "доски объявлений" и — если это понадобится — канала передачи сообщений.

Ключевое новшество здесь — согласие: концепция, объединяющая обязательства и конфиденциальность. CSL используется в качестве электронной площадки для сбора и общения пользователей — как парк может быть местом для проведения какого-либо частного события, но не участвовать в его организации. Использование специальных MPC-протоколов позволяет взаимодействие с низкой задержкой без накладных расходов, которые бы повлекло применение блокчейна. Это помогает масштабированию всей системы.

Исследования Cardano по этой библиотеке проводятся в нашей лаборатории в Токийском техническом институте при помощи иностранных ученых. Мы назвали библиотеку "Tartaglia" в честь одного математика, современника Cardano, и предполагаем, что первая ее итерация будет доступна в первом квартале 2018 года.

Во втором случае нужен блокчейн с виртуальной машиной, набор узлов консенсуса и механизм, обеспечивающий коммуникацию между двумя блокчейнами. Мы начали процесс строгой формализации Ethereum Virtual Machine с использованием K-framework[11] в сотрудничестве с командой из Иллинойского университета.

Результаты проведенного анализа укажут наиболее оптимальный путь для проектирования размноженной, а потом и распределенной виртуальной машины[12] с понятной операционной семантикой и гарантией корректной реализации в соответствии со спецификацией. Другими словами, виртуальная машина действительно делает то, что предписывает код, а риски по безопасности минимизированы.

Остаются нерешенными вопросы про газовую экономику, предложенную Ethereum, и ее связь как с учитывающим ресурсы ML (автор Jan Hoffmann и др.), так и в целом с исследованиями про оценку ресурсов, расходуемых при вычислениях. Нам также интересно, насколько виртуальная машина должна зависеть от используемого языка. Например, проект Ethereum выразил желание перейти с их нынешней виртуальной машины на WebAssembly.

---

[11] K — это универсальный фреймворк для машиноисполняемых семантик, не зависящих от языка программирования. До нашей работы его использовали для моделирования C, Java и JavaScript

[12] Предполагая, что на различных узлах консенсуса запущены разные умные контракты. Также известно под названием "state sharding" ("разделение статусов")

Международная лицензия Creative Commons Attribution 4.0

Следующим шагом станет разработка подходящего языка программирования для контрактов с отслеживанием состояния (stateful contracts), которые децентрализованные приложения смогут вызывать как службы. Для этой цели мы, во-первых, будем поддерживать традиционный язык для умных контрактов Solidity для приложений с низким уровнем гарантий, а во-вторых — разработаем новый язык под названием Plutus для приложений с более высоким уровнем гарантий, которым нужна формальная верификация.

Как и в случае с Zeppelin project, который основан на Solidity, IOHK разработает свою библиотеку кода на Plutus, чтобы разработчики приложений использовали ее в своих проектах. Мы также создадим специальный набор инструментов для формальной верификации, на идею которого нас натолкнула работа из проекта Liquid Haskell Калифорнийского университета в Сан-Диего.

Если говорить о консенсусе, Ouroboros достаточно модульный, чтобы поддерживать выполнение умных контрактов. Таким образом, в основе CSL и CCL лежит один и тот же алгоритм консенсуса. Дело в том, что Ouroboros может использоваться как в контролируемых, так и неконтролируемых реестрах — зависит от распределения токенов.

В случае CSL сгенерированные токены Ada были распределены между покупателями в Азии. Они будут постепенно перепродавать токены на вторичном рынке. Это значит, что алгоритм консенсуса CSL контролируется разнообразным и со временем все более децентрализованным набором участников или их делегатов. При помощи CCL можно создать специализированный токен, принадлежащий делегатам конкретного реестра — это могут быть регулируемые организации. Таким образом получается контролируемый реестр.

Гибкость подобного подхода позволяет настраивать CCL для каждого конкретного случая с разными правилами выполнения транзакций. Например, можно ограничить деятельность, связанную с азартными играми, если для транзакции отсутствуют данные KYC/AML — просто внести в черный список транзакции без соответствующих аттрибутов.

И, наконец, еще один штрих нашего проекта — добавить в наш стек протоколов аппаратные модули безопасности (hardware security module, HSM). Добавление этих возможностей в протокол дает нам два огромных преимущества. Во-первых, использование HSM увеличивает производительность[13], сохраняя требуемый уровень

[13] См. статью http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/ (Корнеллский университет)

Международная лицензия Creative Commons Attribution 4.0

безопасности (приходится доверять только производителю модуля). Во-вторых, используя технологию Sealed Glass Proofs (SGP), HSM позволяют верифицировать данные и затем уничтожить их, гарантируя, что данные не будут копироваться и не смогут попасть в руки злоумышленникам.

Насчет второго пункта — SGP могли бы оказать революционное влияние на соблюдение законодательных требований. Обычно, если потребитель предоставляет персональные данные, чтобы подтвердить свою личность и доказать право участия в чем-либо, эта информация передается третьей стороне с надеждой на то, что третья сторона не является злоумышленником. Эта деятельность по своей природе централизована — тот, кто предоставляет данные, теряет над ними контроль, а также подпадает под действие различных законов.

Возможность выбрать доверенных аттестаторов и поместить персональные данные в защищенный аппаратный модуль значит, что любой человек с подходящим HSM сможет верифицировать данные других пользователей, и результат проверки нельзя будет подделать — но при этом он не сможет узнать личность этих пользователей. Например, Боб не является резидентом США. Алиса — аккредитованный инвестор. Джеймс является налогоплательщиком в США и должен посылать облагаемую налогом прибыль на счет X.

Стратегия Cardano в отношении HSM состоит в том, чтобы внедрить специализированные протоколы за следующие два года, используя Intel SGX и ARM Trustzone. Оба этих модуля встроены в миллиарды бытовых устройств, от ноутбуков до мобильных телефонов, и не требуют от пользователя никаких дополнительных усилий для работы. Кроме того, они подвергались различным испытаниям, отлично спроектированы и являются результатом многих лет работы самых лучших команд, занимающихся аппаратной защитой.

Регулирование

Суровая реальность всех современных финансовых систем состоит в том, что когда они вырастают до определенного предела, то нуждаются в регулировании — или хотя бы склоняются в его сторону. В основном это результат того, что периодически халатность отдельных участников рынка приводит к финансовым кризисам.

Например, за Банковской паникой 1907 года последовало учреждение Федеральной резервной системы в 1913 году как кредитора-спасителя. Другой пример — события в двадцатых годах в США, которые привели к ужасному финансовому кризису, Великой

Международная лицензия Creative Commons Attribution 4.0

депрессии. Этот кризис подтолкнул США к созданию Комиссии по ценным бумагам и биржам в 1934 году, которая была призвана предотвращать подобные события в будущем или хотя бы привлекать виновников к ответственности.

Можно спорить о необходимости или эффективности регулятивных мер, но невозможно отрицать само существование регулирования — и настойчивость, с которой правительства его вводят. Однако по мере того, как мир все больше глобализуется, а деньги становятся электронными, регулирование превращается в обоюдоострое оружие.

Во-первых, какой набор законов нужно применять, если мы имеем дело с несколькими юрисдикциями? Старое понятие Вестфальской системы международных отношений разваливается на части, когда одна транзакция может затронуть три десятка стран за одну минуту. Должны ли мы предпочесть законы тех стран, которые имеют большее геополитическое влияние?

Во-вторых, технологии сохранения конфиденциальной информации постоянно улучшаются, что приводит к цифровой "гонке вооружений". Все сложнее и сложнее будет понять, кто принял участие в транзакции, не говоря уже о том, кто владеет определенным количеством стоимости. Как организовать эффективное регулирование в мире, где активы на сумму в миллионы долларов можно контролировать всего лишь секретным ключом-мнемоникой из 12 слов[14]?

Как и в любой финансовой системе, в протоколе Cardano должна быть заложена идея о том, что такое "честно" и "разумно". Мы решили разделять права физических лиц и права рынка.

У физического лица всегда должен быть доступ к принадлежащим ему средствам без ограничений или конфискаций. Такое право необходимо ввести потому, что не всем правительствам можно доверять: некоторые используют власть для собственной выгоды, как происходит, например, в Венесуэле или Зимбабве. При разработке криптовалют необходимо ориентироваться на наименьший общий знаменатель.

Второй принцип: историю менять нельзя. Блокчейн должен обеспечивать неизменяемость. Если разрешить откатывать историю назад или изменять официальные записи, это будет слишком большим соблазном — можно изменить записи для личной выгоды конкретного участника.

[14] См. BIP39 https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Международная лицензия Creative Commons Attribution 4.0

В-третьих, нельзя ограничивать движение стоимости. Контроль капитала и другие искусственно возведенные стены идут вразрез с человеческими правами. Кроме того, что такой контроль бесполезен[15], в глобальной экономике со множеством участников из менее развитых стран, которые переезжают в другие страны в поисках средств на жизнь, ограничение потока капитала сильнее всего бьет по самым бедным.

Итак, принципы озвучены, но права рынков и права физических лиц — это совершенно разные вещи. Создатели Cardano верят в права личности. Но мы также верим в то, что у любого рынка есть право открыто заявить о своих правилах и условиях, и если физические лица соглашаются сотрудничать с этим рынком — они должны придерживаться его правил ради сохранения целостности всей системы.

Основная сложность всегда заключалась в стоимости и практичности претворения в жизнь требований закона. Мелкие межъюрисдикционные транзакции в традиционных финансовых системах слишком дорого отменять в случаях, если произошло мошенничество или торговый спор. Если кто-то пошлет деньги нигерийскому принцу^{[17](#footnote17)}, то возвращать их назад обычно слишком дорого.

Мы полагаем, что в случае Cardano можно внести в существующий процесс новое на трех уровнях. Во-первых, используя умные контракты, можно тщательнее контролировать условия коммерческих отношений. Если все активы электронные и могут быть выражены средствами CSL, мы можем дать уверенную гарантию коммерческих сделок без мошенничества.

Во-вторых, HSM предоставляют возможность использовать персональные данные для аутентификации, при этом исключая их утечку. Так получится глобальная система репутации, и можно будет сильно снизить затраты на регулируемые виды деятельности — например, азартные игры онлайн, к которым автоматически применяется налоговое законодательство, или децентрализованные биржи.

И наконец, в плане развития Cardano есть создание инструмента для модульного регулирования — DAO, децентрализованной автономной организации. DAO можно настроить для работы с умными контрактами, созданными пользователем, что добавит системе гибкости, защитит потребителей и облегчит арбитраж. Мы очертим объем и содержание этого проекта в статье, которую выпустим позднее.

[15] Иллюстрацией мер против утечки капитала является финансово-расчетная система Хавала (Hawala Banking System).

Международная лицензия Creative Commons Attribution 4.0

Зачем все это нужно?

Cardano — долгоиграющий проект, полагающийся на сотни блестящих умов как в криптовалютной отрасли, так и за ее пределами. Мы постоянно совершенствуемся, активно используем рецензирование и бесстыдно воруем великие идеи, как только их заметим.

В оставшихся главах мы поочередно опишем конкретные ключевые аспекты, из которых состоит наш проект. Некоторые из них мы выбрали потому, что хотим улучшить технологии, использующеся в нашей отрасли. Некоторые связаны конкретно с эволюцией Cardano.

Ни один проект не может выполнить все на свете цели или удовлетворить нужды всех на свете потребителей. Но мы стараемся создать концепцию, видение того, как должна выглядеть самоподдерживающаяся финансовая система, для юрисдикций, у которых этого видения нет. В конечном итоге суть криптовалют не в том, что они полностью заменят традиционные финансовые системы. Традиционные финансовые системы отлично справляются с тем, чтобы адаптироваться к переменам и сохранять свое устройство и функциональность.

Скорее стоит искать места, где слишком дорого внедрять существующие банковские системы, где многие живут на несколько долларов в день, не имеют удостоверения личности, и где невозможно взять кредит.

В таких местах возможность объединить платежную систему, права на собственность, удостоверение личности, кредитование и защиту от рисков в одном приложении, которое можно запустить на мобильном телефоне, не просто полезна — она меняет жизни. Мы разрабатываем Cardano, потому что считаем, что можем создать или хотя бы улучшить такую концепцию для развивающихся стран.

Даже если у нас не получится достичь этой цели — уже изменение того, как криптовалюты проектируют, развивают и спонсируют, будет большим достижением.

Международная лицензия Creative Commons Attribution 4.0

2. Наука и разработка

Искусство постоянных улучшений

Криптовалюта — это протокол, реализованный в виде приложения. Протокол — это просто умная беседа между участниками. Программное обеспечение — это в конечном итоге оперирование данными с какой-либо целью. Но что отличает устойчивое и надежное программное обеспечение, а также полезные и безопасные протоколы? А разница в людях.

Хорошему программному обеспечению нужна прозрачность и отчетность, четкие бизнес-требования, воспроизводимые процессы, тщательное тестирование и постоянные улучшения. Кроме того, хорошее программное обеспечение делают талантливые разработчики с глубокими знаниями в своей области, достаточными, чтобы создать систему, которая может решить все стоящие перед ней задачи.

Если говорить о полезных и безопасных протоколах — в особенности о тех, которые используют криптографию и распределенные системы — то их разработка начинается в более академической и стандартизированной манере. Рецензирование, бесконечные дискуссии и четкая концепция компромиссов — все это обязательно для уверенности в том, что протокол будет удобным и полезным. Но только этого недостаточно: протоколы нужно еще реализовать и протестировать в реальной жизни.

Отрасль криптовалют уникальна тем, что в ней две абсолютно разные философии скомканы в одну без должного применения гегелевского синтеза. Здесь тезис — это подход стартапа, "Главное — сделать быстро", где царствуют юность, алчность и страсть. Антитезисом станет неспешный, методичный и академический подход, основывающийся на желании упрочнить инновации нашей отрасли в удобной нише, где можно найти достойное финансирование и престиж.

В итоге многие криптовалюты описаны или только "на бумаге" (что годится разве что для строчки в резюме), или написанным на скорую руку кодом. Ни одна из десяти[16] криптовалют, на данный момент лидирующих по показателю рыночной капитализации, не

[16] На coinmarketcap.com можно найти наглядный список криптовалют, отсортированный по рыночной доле.

Международная лицензия Creative Commons Attribution 4.0

имеет в своей основе протокола, прошедшего рецензирование. Ни одна из этих десяти криптовалют не была создана на основе формальной спецификации[17].

А на счету эквивалент миллиардов долларов. После того, как криптовалюта введена в эксплуатацию, изменить что-то в ней очень сложно. Как пользователь может быть уверен в том, что он использует безопасную систему? Как пользователь может быть уверен в честности рекламных заявлений? А что, если предложенный протокол никогда не достигнет обещанного?

Недостаточная синхронизация, недостаточное следование четким процессам — вот одна из первых причин, по котором в IOHK решили сделать Cardano. Мы надеемся создать проект, на который можно будет ориентироваться при работе в нашей отрасли, чтобы делать все более эффективно, разумно и честно.

Цель не в том, чтобы предложить полностью новый способ разработки программного обеспечения и протоколов, а в том, чтобы признать, что отличные программы и отличные протоколы существуют — и мы можем воспроизвести условия, в которых они создавались. Кроме того, следует сделать знание об этих условиях достоянием общественности, а в случаях, когда это возможно — и с открытым кодом, чтобы эти решения могли повторять на благо всей отрасли.

Факты и мнения

Другой важный вопрос — где заканчиваются факты и начинаются мнения. Существуют сотни языков программирования, десятки парадигм разработки и более чем одна философия управления проектами. В научных кругах много своих проблем, которые возникают из-за того, что ученые не думают о практичности и о коммерческой стороне вопроса.

В случае Cardano мы попробовали сначала найти очевидные инженерные недоработки, которые по общему согласию было бы хорошо исправить. Криптография и распределенные системы — сферы, в которых слишком много примеров того, как неопытные руки могут совершить ужасные ошибки. Таким образом, любой протокол,

[17] У Ethereum есть полуформальная спецификация, известная под названием Yellow Paper. Однако в ней не полностью прописана семантика EVM (виртуальной машины Ethereum), и этого недостаточно для точной реализации протокола.

Международная лицензия Creative Commons Attribution 4.0

относящийся к этим сферам, должен проектироваться признанным экспертом в этой области, а работу должны оценивать другие эксперты.

Протокол Ouroboros — наше первое исследование в данной области. Он спроектирован командой криптографов с огромной, разносторонней и общепризнанной историей публикаций. Его создатели использовали стандартную криптографическую методологию с использованием доказательств, допущений о безопасности, а также модели угроз. Доказательства прошли проверку на конференциях[18], а также независимую проверку доказательными вычислениями, написанными на языке Isabelle командой Кембриджского университета[19].

Но одно это не предоставляет никаких гарантий полезности протокола — просто тщательная проверка модели безопасности с некоторыми допущениями. Чтобы проверить полезность протокола, нужно его реализовать и протестировать. Наши разработчики реализовали протокол и на Haskell, и на Rust. Эта работа показала, что следует сосредоточить больше усилий на модели синхронизации, и это привело к созданию Ouroboros Praos.

Искусство постоянных улучшений — вот что нужно для создания отличных протоколов. Каждый шаг ведет к новым урокам и необходимости перепроверить предыдущий шаг[20]. Это требует вложений и времени, и иногда очень нудно и утомительно, но без этого нельзя проверить, что протокол сделан правильно.

Протоколы — особенно те, которыми будут пользоваться миллиарды людей — живут долго и развиваются неспешно. Предполагается, что их будут использовать годами или даже десятилетиями. Кажется разумной мысль о том, что прежде чем обременить мир новой финансовой системой, с которой мы все будем жить следующие 100 лет, ее создатели должны хорошенько попотеть и потрудиться.

Функциональные огрехи

Тема, которую мы будем обсуждать, достаточно субъективна: инструменты, языки программирования и методологии, используемые в разработке — все это больше вопрос

[18] Принятая статья номер 71 на ежегодной криптоконференции IACR (International Association for Cryptologic Research, рус. Международная ассоциация криптологических исследований) в Калифорнии

[19] Автор — Kawin Worrasangasilpa, супервизор —профессор Lawrence Paulson

[20] Слегка отвлекаясь от темы — развлечения ради стоит посмотреть видеоролик Professor Halmos's discussion about how to write a math textbook

Международная лицензия Creative Commons Attribution 4.0

"приверженства религии", чем объективной реальности. Исходный код — это как проза. У всех есть мнение насчет того, что такое "хорошо" — и то, что говорится, зачастую не так важно, как то, как это говорится.

Нам придется согрешить, выбрав одну сторону — и эта сторона хотя бы одному человеку наверняка покажется неправильной. Как бы то ни было, мы можем очень подробно обосновать наш выбор.

Протоколы, делающие возможным создание Cardano, реализованы на Haskell. Пользовательский интерфейс воплощен форком Electron, который мы назвали Daedalus. Мы решили использовать веб-архитектурную модель там, где это возможно, а для нашей базы данных выбрали парадигму key-value с использованием RocksDB.

На уровне компонентов эта абстракция означает, что техобслуживание будет проще, можно будет заменять технологии на более новые без лишних усилий, и что наш стек технологий частично связан с разработкой Github и Facebook.

Выбор WebGUI позволит нам использовать React и разрабатывать фронтенд при помощи инструментов, знакомых сотням тысяч JavaScript-разработчиков. Использование веб-архитектуры означает, что с компонентами можно работать как со службами, а модель безопасности достаточно разумна.

Самым сложным решением оказалось выбрать Haskell для разработки протокола. Даже в мире функциональных языков программирования выбора достаточно. Более гибкие языки, но с побочными эффектами — например, Clojure, Scala and F# — пользуются огромными библиотеками из экосистем Java и .Net и при этом сохраняют некоторые из лучших черт функционального программирования.

Есть более академически ориентированные языки, например, Agda и Idris. Они тесно связаны с техниками, которые позволяют строго верифицировать корректность. Но им не хватает нужных библиотек, и на них неудобно вести разработку на нужном нам уровне.

В случае Cardano мы выбирали из Ocaml и Haskell. Ocaml — прекрасный язык с отличным сообществом, хорошими инструментами, приятным опытом разработки на нем и прекрасным наследием в области формальных верификаций (см. Coq[21]). Так почему же мы выбрали Haskell?

[21] Раз уж мы об этом говорим, у IOHK вообще-то есть проект на Ocaml под названием Qeditas, который нам передал некто под псевдонимом Bill White

Международная лицензия Creative Commons Attribution 4.0

Почему Haskell?

Протоколы, из которых состоит Cardano, — распределенные, связаны с криптографией и должны обладать высокой отказоустойчивостью. Даже при самом удачном раскладе все равно будут "византийские генералы", искаженные сообщения и неисправные клиенты, невольно устраивающие в сети разгром.

Во-первых, мы хотели язык с мощной системой типов, где мы бы могли с легкостью использовать инструменты вроде QuickCheck и более сложные техники вроде Refinement Types, при этом предполагая достаточную степень отказоустойчивости. OTP model в стиле Erlang удовлетворяет последнему требованию, а языки вроде Haskell и Ocaml — первому.

С появлением Cloud Haskell Haskell унаследовал множество преимуществ Erlang, не потеряв собственных плюсов. Кроме того, модульность и компонуемость Haskell позволила нам использовать для Cardano специальную облегченную библиотеку под названием Time Warp.

Во-вторых, последние несколько лет библиотеки Haskell быстро развивались благодаря масштабной работе коммерческих компаний, например, Galois, FP Complete и Well-Typed. В итоге Haskell можно использовать для написания промышленных приложений.[22]

В-третьих, быстрое развитие PureScript привело к появлению давно ожидаемого моста к миру JavaScript — так язык Clojurescript многое дал Clojure. Мы ожидаем, что PureScript будет особенно полезен, когда нам нужно будет заставить Cardano работать в браузере, а также при разработке мобильных кошельков.

В-четвертых, разрешение зависимостей в Haskell в последние годы значительно улучшилось в результате значительных общественных и технологических усилий, возглавленных такими специалистами, как Michael Snoyman. Эти работы велись с помощью платформы Stackage, которую легко использовать, а также она поддерживается компанией FP Complete.

[22] Bryan O'Sullivan отлично рассказывает о промышленном применении Haskell здесь.

Международная лицензия Creative Commons Attribution 4.0

В-пятых, кроме адекватного разрешения зависимостей мы хотим, чтобы сборки нашего программного обеспечения были воспроизводимыми. Другими словами, с теми же значениями конфигурации и версиями зависимостей всегда должны получаться те же самые результаты. При помощи технологии Stackage мы использовали NixOps и достигли потрясающей воспроизводимости.

Кроме того, по сравнению с другими похожими языками сообщество Haskell располагает множеством прекрасных разработчиков с нужным соотношением академического и производственного опыта. Этот факт работает как фильтр: вряд ли получится найти опытных разработчиков на Haskell, не имеющих глубоких знаний по информатике.

Формальная спецификация и верификация

Огромный плюс разработки протокола с использованием доказуемо корректной модели безопасности — для него существует гарантированный лимит возможностей злоумышленника. У пользователя есть гарантия того, что пока протоколу следуют и доказательства корректны, злоумышленник не может обойти заявленные меры безопасности.

Если на вышесказанное посмотреть внимательнее, то оно оказывается еще более важным. Злоумышленники могут быть сколь угодно умными и талантливыми. Сказать, что всех злоумышленников можно победить лишь математической моделью — исключительное по своей сути заявление. И, конечно, не совсем верное.

В реальном мире существуют факторы и обстоятельства, которые мешают создать утопию полной безопасности и правильного поведения системы. Реализация может быть неправильной. В технике могут найтись возможности для атак, о которых раньше не было известно. Модель безопасности может быть неполной и не совпадающей с использованием в реальной жизни.

Для того, чтобы решить, насколько подробной должна быть спецификация и сколько труда и проверок следует вложить в протокол, приходится применять интуицию. Например, такие проекты, как SeL4 Microkernel project, являются отличной иллюстрацией того, как попытки избежать неопределенности потребовали почти 200 тысяч строк кода на

Международная лицензия Creative Commons Attribution 4.0

Isabelle для проверки менее 10 тысяч строк кода на C. Но ядро операционной системы — важнейшая часть инфраструктуры, и если ее реализовать неправильно, может получиться серьезная брешь в безопасности.

Нужны ли подобные геркулесовы подвиги всякий раз, когда мы разрабатываем криптографическое программное обеспечение? Или можно выбрать менее сложный путь и получить тот же результат? Так ли уж важно, что протокол идеально реализован, если окружение, в котором он запущен, очень уязвимо — например, это Windows XP?

В случае Cardano мы пришли к следующему компромиссу. Во-первых, поскольку сферы криптографии и распределенных вычислений достаточно сложны, доказательства обычно очень запутанные, длинные и иногда довольно технические. Из этого следует, что проверки вручную могут быть утомительными, и в них могут закрасться ошибки. Поэтому мы считаем, что все важные доказательства в описании ключевой инфраструктуры должны пройти автоматические тесты.

Во-вторых, для проверки кода на Haskell на соответствие нашему техническому описанию мы можем выбрать два распространенных варианта: работать с SMT-решателями при помощи LiquidHaskell или использовать Isabelle/HOL.

SMT-решатели (от "satisfiability modulo theories" — задача выполнимости формул в теориях) решают задачу нахождения переменных, которые удовлетворяют уравнению или неравенству, или показывают, что подобные параметры не существуют. Как обсуждалось авторами De Moura и Bjørner, SMT могут использоваться в различных случаях, но главное — эти очень мощные техники могут значительно уменьшить количество неполадок и семантических ошибок.

С другой стороны, Isabelle/HOL — более выразительный и гибкий инструмент, который можно использовать и для описания, и для проверки реализации протокола. Isabelle — классический инструмент для доказательства теорем, он работает с логическими конструкциями высшего порядка и способен представлять множества и другие математические объекты для использования их в доказательствах. Isabelle можно совмещать с доказателем теорем Z3 SMT, если необходимо работать с задачами, в которых есть соответствующие ограничения.

Оба подхода имеют свои преимущества, поэтому мы решили использовать их оба поэтапно. Написанные человеком доказательства мы превратим в код на Isabelle, чтобы убедиться в их корректности и удовлетворить требование о машинных проверках. А

Международная лицензия Creative Commons Attribution 4.0

потом мы собираемся постепенно вводить Liquid Haskell в исходный код Cardano на протяжении 2017 и 2018 года.

И наконец, формальная верификация хороша настолько, насколько хороша сама спецификация и доступный набор технических средств. Одна из главных причин, по которым мы выбрали Haskell — это отличный баланс между практикой и теорией. Спецификация на основе технического описания выглядит очень похоже на код на Haskell, и связать их воедино намного проще, чем было бы в случае императивного языка программирования.

Это не отменяет того, что написать хорошую спецификацию невероятно сложно и приходится постоянно держать ее в актуальном состоянии, когда происходят обновления и исправляются ошибки; но это не уменьшает ее ценности. Если есть намерение заложить доказуемую безопасность в основу проекта, реализация должна быть именно такой, как предлагается в документации.

Прозрачность

И наконец, еще один вопрос при обсуждении теории и практики разработки криптовалюты — что делать с прозрачностью. Проектно-технологические решения не являются разработчикам во снах, внезапно становясь каноном. Они являются результатом опыта, дискуссий и уроков, полученных из предыдущих ошибок.

Проблема тут в том, что полностью прозрачный процесс разработки может сделать дискуссии больше театральными, чем основанными на фактах. Самомнение, попытки завоевать симпатию сообщества и страх показаться глупым — все это может сделать обсуждения пустыми и непродуктивными.

Кроме того, сторонние участники могут влиться в беседу и увести ее в бесполезное (но интересное им) русло. У каждого есть своя священная корова.

Как совместить прозрачный процесс разработки, который нужен сообществу, доверившемуся нашей команде разработчиков, и возможность открыто высказывать свое мнение, ничего не боясь?

В случае Cardano мы решили использовать стандартоориентированный контролируемый процесс. Сообщество должно знать, что научная основа и сам код хорошо продуманы, проверены и действительно делают именно то, что заявили разработчики. Что касается научной основы, рецензирование должно полностью удовлетворить это требование —

Международная лицензия Creative Commons Attribution 4.0

именно для этого оно и предназначено, и именно так сформировался мир современной науки.

С кодом все не так просто. Мы доверили организации Cardano Foundation право быть конечным аудитором работы IOHK. В частности, у этой организации следующие обязанности:

1. Регулярная проверка исходного кода в Github-репозитории Cardano на качество, полноту тестов, подробные комментарии и завершенность
2. Проверка всей документации Cardano на корректность и полезность
3. Проверка того, что протоколы, разработанные учеными, полностью реализованы

Для выполнения этого задания IOHK будет предоставлять регулярные и своевременные отчеты Cardano Foundation и уполномоченным этой организацией третьим сторонам. Cardano Foundation, в свою очередь, будет публиковать для сообщества Cardano доклад по итогам надзорной деятельности как минимум раз в квартал.

Это первая попытка начать широкое обсуждение того, как децентрализованный проект может нести ответственность за результат. Надзор за разработкой, выполняемый доверенной третьей стороной — мощный инструмент, если мы хотим убедиться, что разработчики следуют плану. Но он не может стопроцентно гарантировать, что на проекте всегда будут успешно решаться нужные задачи.

И поэтому после того, как в CSL появится система казначейства, Cardano Foundation наймет дополнительные команды разработчиков для создания альтернативных клиентов по формальной спецификации, разработанной в сотрудничестве с IOHK. Разнообразие в разработке — отличная техника, которую использовал проект Ethereum, чтобы избежать формирования монокультуры вокруг одного набора идей или одной команды разработчиков.
Если говорить о спецификациях, то многое можно почерпнуть из стандартоориентированных процессов, которым следуют WC3 и IETF. Но каждый протокол, который используется в Cardano, требует спецификации, которая не ссылается на научные работы или исходный код. Она должна быть в подходящем формате, например, RFC.

Одна из важнейших задач Cardano Foundation — выступать в качестве комитета стандартов для протоколов Cardano и создавать условия для ведения дискуссий по обновлению, добавлению и изменению стандартов, имеющих отношение к Cardano. Если интернет — продукт стандартов — с помощью IETF смог достигнуть согласия по поводу

Международная лицензия Creative Commons Attribution 4.0

того, какие ключевые протоколы использовать, то вполне разумно предположить, что специализированный орган может помочь решить ту же задачу.

В завершение скажем, что интересно было бы попробовать переместить подобные обсуждения в децентрализованную сущность на базе блокчейна. Эта концепция называется decentralized autonomous organization, DAO (децентрализованная автономная организация), и на данный момент мы ведем предварительные работы в этой области. IOHK собирается разработать эталонную DAO-модель для сущностей, взаимодействующих с Cardano, чтобы при желании можно было ей воспользоваться. Cardano Foundation решит, следует ли включать ее в требования по стандартам.

3. Операционная совместимость

Великая недальновидность

Финансы и в целом идея коммерческой деятельности — исключительно человеческое изобретение. Существуют великолепные языки, очень точные инструменты для выражения сути и бесконечные лабиринты техник для обращения за помощью в случае неудач, а также тысячелетняя история законов, призванных обеспечить честную торговлю. Одними из самых ранних найденных нами письменных документов были торговые договоры.

И нельзя исключать человеческий фактор, даже несмотря на уменьшение количества посредников благодаря логике, компьютерам или ограничениям правительств, наделенными огромной мощью. В этом и состоит великая недальновидность криптовалют. В основном они оторваны от реальности, в которой живут люди.

Люди делают ошибки. Люди меняют свои мнения. Люди не всегда полностью понимают условия сделки, которую готовы заключить. Людей обманывают и вводят в заблуждение. На личном и государственном уровне могут меняться обстоятельства, требуя принятия особых решений. Для этого в большинстве контрактов есть разделы о форс-мажоре.

Криптовалюты, однако, пытаются заменить человеческое понимание, сочувствие и правосудие на бесстрастного электронного судью, идеально следующего конституции без

Международная лицензия Creative Commons Attribution 4.0

оглядок на результат. Учитывая тот факт, что люди всегда пытались и будут пытаться изменить правила для собственной выгоды, приятно будет наконец пользоваться системой, в которой не будет коррупции.

Но что случится, если пользователю придется совмещать новые финансовые системы с традиционными? Что будет в человеческом мире, а не в мире компьютеров? Например, права на собственность — скажем, земельная регистрация — существуют исключительно в реальном мире. Даже если привязать земельные участки к токенам, все равно потребуется участие специалистов в этой области.

Еще один аргумент — слиток золота сам себя не никому не передаст. Электронный судья может принять решение о его передаче, но сделать это без людей, которые выполнят решение, он не может. В этом месте электронный реестр может расходиться с реальностью.

Таким образом, создатель протокола решает, насколько его криптовалюта должна учитывать условия, в которых находятся реальные люди. Чем больше гибкости, тем меньше соответствия абсолюту стоит ожидать от системы. Чем сильнее мы защищаем потребителя, тем больше понадобится механизмов для отката транзакций, возмещения средств и редактирования истории.

Эта глава и следующая глава — о регулировании — раскрывают прагматический подход Cardano к этой теме. Если говорить об операционной совместимости — тут есть две большие группы. Во-первых, совместимость с традиционными финансовыми системами (не криптовалютами). Во-вторых, совместимость с другими криптовалютами.

Традиционные системы

FinTech не ограничивается одним стандартом или даже одним языком программирования. Есть огромная разница в подходах, множество субъектов, ответственных за различные расчеты, и бизнес-процессов, и огромное разнообразие в других сферах, связанных с бухучетом и перемещением стоимости.

Недальновидно предполагать, что если какая-то технология окажется лучше прочих, остальные области экосистемы просто признают свое поражение и сдадутся. Например, спустя 16 лет после выхода Windows XP некоторые люди все еще ею пользуются. Это как если бы кто-то пользовался в 2000 году компьютером Macintosh, который выпустили в 1984.

Международная лицензия Creative Commons Attribution 4.0

Если даже отставить в сторону поведение пользователей — предприятия меняются еще медленнее. Бэкенд многих банков до сих пор написан на Cobol. Когда понятно, что инфраструктура работает и отвечает требованиям бизнеса, больше нет стимула обновлять или улучшать программное обеспечение и протоколы ради пользователей — разве что ради соблюдения законов или из-за проблем с безопасностью.

В случае Cardano нужно разобраться: что принесет нам совместимость с традиционными финансовыми системами? На какие системы, стандарты, сущности и протоколы следует ориентироваться, чтобы быть достаточно уверенными в операционной совместимости? Можно ли сделать интеграционные мосты для взаимодействия с традиционными системами федеративными или децентрализованными? Станут ли они, подобно биржам, подсобьем для хакеров, злоумышленников и слишком ревностных регуляторов?

Здесь есть три проблемы, на которые следует обратить внимание. Во-первых, репрезентация информации и уверенность в ее точности. Во-вторых, репрезентация стоимости и владения ею. В-третьих, репрезентация организаций, а также уровня доверия к этим организациям — как для отдельного пользователя, так и для общего доверия всех пользователей.

Чтобы приносить пользу, информация и стоимость должны иметь возможность свободно перемещаться между традиционными финансовыми системами и Cardano. Результаты этого процесса нужно фиксировать, чтобы собирать данные о репутации и иметь возможность обратиться за помощью. Но обычно такие вещи зависят от участников процесса. Если их встроить в блокчейн, это сделает их глобальными и постоянными.

Кроме того, не всегда можно свободно перемещать стоимость в мире традиционных финансовых систем. Эмбарго, санкции, контроль капиталов и судебные решения могут замораживать активы. Если мы хотим обеспечить совместимость, то нельзя создавать постоянно открытый путь утечки стоимости.

Кроме того, бренд и репутация организаций — один из краеугольных камней коммерческих отношений. Миллиарды долларов тратятся ежегодно на маркетинговые компании, чтобы придумывать, поддерживать и обновлять бренды. Если в адрес физического лица или организации были сделаны клеветнические, лживые или дезинформирующие заявления, то у этого лица или организации есть право обратиться в суд. Но блокчейн пытается хранить историю вечно.

Международная лицензия Creative Commons Attribution 4.0

Здесь та же история, что с выбором языка программирования: нет идеального решения, которое бы позволило Cardano однозначно решить эти проблемы. Нам опять приходится сделать выбор в пользу какого-то решения и его придерживаться.

Если говорить о потоке информации, такой поток называется "достоверным потоком данных" (англ. "trusted data feed"). У него есть источник и содержание. У источников есть некоторое понятие доверия и поводы обманывать или, наоборот, оставаться честными. Содержание может быть закодировано произвольным образом.

Учитывая, что мы хотим реализовать в нашем протоколе поддержку доверенного аппаратного обеспечения, мы решили исследовать добавление поддержки для протокола Town Crier профессора Ari Juel с коллегами. При условии, что существует набор источников данных, заслуживающих доверия, протокол Town Crier позволяет безопасно собирать данные из интернета для использования в умных контрактах и других приложениях.

Начальный список источников предоставят компании Emurgo, IOHK и Cardano Foundation. Позже этот список будет заменен на другой список источников — их порекомендует сообщество, используя механику по принципу системы казначейства Cardano. У хороших источников данных будет формироваться хорошая репутация, и так образуется цепь положительной обратной связи, постепенно улучшающая надежность информации из источника.

Представление стоимости — более сложная тема. В отличие от информации (где можно однажды добиться правильности, своевременности и полноты, и протоколы будут вести себя надежно и предсказуемо), со стоимостью дела обстоят запутаннее.

Как только стоимость привязали к токену, она должна вести себя как уникальный объект. Информацию можно копировать и передавать дальше, но токен, который дает право на владение чем-либо (скажем, право на владение транспортным средством), нельзя копировать и передавать в двух разных реестрах одновременно. Это уничтожит целостность всей системы.

Обеспечить совместимость с традиционными финансовыми системами при работе с токенизированной стоимостью сложно: дело в том, что когда токены перемещаются из одного реестра в другой, то допущения, степени надежности и условия для проведения аудита меняются. Например, у Боба есть некоторое количество биткоинов и он решает обменять их на другую валюту. Теперь у Боба есть аналог биткоинов в другом реестре. В

Международная лицензия Creative Commons Attribution 4.0

случае биржи криптовалют Mt. Gox пользователи потеряли все, поскольку реестр биржи не соответствовал реальности.

Задача еще больше усложняется тем, что традиционные системы должны уметь работать с токенами в реестрах криптовалют. Как упоминалось ранее, предприятия обычно сопротивляются изменениям в программном обеспечении и принятию новых протоколов. Вот почему в этой ситуации сложно придумать решение.

В случае Cardano мы надеемся дать пользователям возможность прикреплять к транзакции обширный набор метаданных, после чего подождем формирования стандартов в этой области и будем им соответствовать. На этот счет есть некоторые подвижки, например, рабочая группа Interledger, инициативы вроде R3Cev и международные распоряжения насчет обновления старых финансовых протоколов.

Самая большая сложность в том, чтобы определять количество и качество стоимости, перемещаемой из традиционной системы в реестр криптовалюты. Например, Боб — владелец банка. Он издает токен, поддерживаемый долларом, после чего всегда может устроить мост для перемещения своих токенов в реестр вроде Cardano, где они станут пользовательскими активами.

Cardano может точно отслеживать принадлежность активов и предлагает возможность добавить метки времени и провести аудит. Но ни одна криптовалюта не сможет гарантировать, что Боб — честный банкир. Он всегда может создать в своем банке частичный резерв, не полностью обеспечив все токены долларом. И это нельзя будет обнаружить средствами криптовалюты, если только доллар сам по себе не будет являться токеном в цифровом реестре[23].

И наконец, репрезентация сущностей в сети — классическая сетевая проблема, известная с ранних дней интернета. Университеты, предприятия, правительственные ведомства — любые пользователи в какой-то момент сталкиваются с необходимостью подтвердить собственную личность.

На этот случай существуют такие решения, как Public Key Infrastructure (рус. "инфраструктура открытых ключей") и система DNS под администраторством ICANN. Учитывая то, что нынешним положением дел в Интернете мы довольны — эти решения и масштабируемы, и полезны. Но они не отвечают на более узкие, коммерческие вопросы

[23] С другой стороны, для цифровых реестров предлагается использовать метод защиты proof of reserve, который гарантирует верную работу в случаях, если обменная биржа работает только с криптовалютами.

Международная лицензия Creative Commons Attribution 4.0

надежности, достоверности и прочих дополнительных характеристик, возникающие тогда, когда необходимо решить, иметь ли дело с каким-либо предприятием.

Бизнес-модель многосторонних торговых площадок, например, eBay — предоставлять некоторые метаданные и помогать проведению транзакций. Суждения о качестве информации, событиях и фирмах часто формируются только на основе рейтинга из надежных онлайн-источников[24].

Во всем этом для Cardano важен вопрос централизованности данных о репутации. Одна из целей Cardano — предоставить набор финансовых инструментов развивающимся странам. Ключ к выполнению этой цели — возможность установить доверие между участниками, которые даже не знают друг друга.

Если только одно предприятие или даже консорциум предприятий контролируют, кого называть хорошим, а кого плохим — вместо того, чтобы это получалось в результате естественного взаимодействия в рамках сообщества — тогда они могут произвольно внести в черный список кого угодно и за что угодно. Такое положение вещей противоречит ценностям нашего проекта и делает бессмысленным использование криптовалюты.

К счастью, те же механизмы, которые используются для голосования за распределение казны, форков протокола и формирования списка достоверных потоков данных, можно применить и для организации пространства репутаций. Мы ведем исследования в этой области и надеемся сконструировать оверлейный протокол для децентрализованной сети доверия репутации в 2018-2019 году — после того, как стабилизируются центральные элементы инфраструктуры.

Совместимость с другими криптовалютами

Если перейти из мира традиционных финансовых систем в мир цифровых реестров, дела с операционной совместимостью пойдут куда лучше. У каждого реестра есть свой сетевой протокол, коммуникационные стандарты и допущения безопасности для соответствующего алгоритма консенсуса. Всему этому легко дать количественную оценку.

Информация передается путем подключения к другой сети и интерпретации ее сообщений. Перемещение стоимости можно осуществлять при помощи релейной

[24] Эти рейтинги даже влияют на собственно содержание информационных источников. Вот любопытная история о том, как сайт с кинообзорами Rotten Tomatoes повлиял на индустрию кино.

Международная лицензия Creative Commons Attribution 4.0

системы, технологии "atomic cross chain trading" (рус. "неделимые кросс-сетевые обменные операции") или схемы сайдчейнов. Поскольку централизованного оператора не существует, то репрезентация сущностей сводится к мета-обсуждению уровня доверия к разработчикам, майнерам и другим влиятельным участникам.

Для Cardano мы разрабатываем новый сайдчейн-протокол (авторы Kiayias, Miller и Zindros). Он дает неинтерактивную возможность безопасно перемещать стоимость между двумя отдельными сетями, поддерживающими этот протокол. Именно с помощью этого механизма в первую очередь будет осуществляться перемещение стоимости между уровнями CSL и CCL.

По мере того, как Cardano будет наращивать общую стоимость и базу пользователей, для других криптовалют сформируются интеграционные мосты. Для того, чтобы ускорить этот рост, Cardano SL поддерживает урезанную версию языка Plutus для скриптов совместимости. Во время релиза Shelley и последующих релизов CSL будут добавлены новые транзакции специально для этих нужд.

Лабиринт Дедала

Вопросы совместимости следует рассматривать с точки зрения глобальной перспективы. Специализированные протоколы, новые типы транзакций, системы оценки степени доверия и потоки информации — все это нельзя свести к одному контролеру или пользователю. Наоборот, все они должны быть доступны кому угодно — без цензуры или взимания платы.

Но что будет в случаях, когда Cardano не поддерживает какой-либо протокол, транзакцию или приложение, без которого пользователь не может обойтись? Опустим ли мы руки? Интернет уже сталкивался с подобной проблемой в девяностых.

Как ни странно, всемирная паутина предлагает два решения, которые можно применить к криптовалютам. Появление JavaScript дало возможность добавлять произвольную функциональность на любой веб-сайт. Плагины и расширения для браузеров добавили дополнительные возможности для пользователей . Оба этих подхода способствовали появлению всемирной сети — такой, какой мы ее знаем сейчас. Это же верно для всех проблем безопасности, существующих в ней.

Международная лицензия Creative Commons Attribution 4.0

Ethereum использует второй подход, давая пользователям возможность встраивать субпротоколы в свой блокчейн в виде умных контрактов. Cardano поддерживает такую функциональность при помощи парадигмы CCL. Но что насчет специализированных расширений?

Хорошим примером здесь будет трейдер на криптовалютной бирже. Представьте себе некий децентрализованный рынок, который поддерживает набор различных криптовалют. Трейдер хочет автоматизировать свои действия на этом рынке.

В случае фрагментированной экосистемы трейдеру придется установить десятки клиентов для каждой криптовалюты, после чего написать собственное программное обеспечение, которое взаимодействует с каждым из клиентов, координируя автоматизированные операции купли-продажи. Если один из клиентов обновится, то вся система может перестать работать. Более того, а что, если трейдер захочет продать это программное обеспечение?

Прямо как в веб-модели расширений — если интерфейс для различных криптовалют можно реализовать средствами веба, то задача трейдера очень упрощается. Можно сделать универсальный интерфейс. Установка в один клик. Распространять такое программное обеспечение можно так же, как это реализовано в веб-магазине Chrome.

Для Cardano мы решили поэкспериментировать с этой парадигмой, реализовав фронтенд нашего эталонного кошелька при помощи Electron. Electron — это проект Github с открытым исходным кодом, совмещающий в себе Node и Chrome. Билд Electron для Cardano мы назвали Daedalus (Дедал).

Daedalus первого поколения[25] будет вести себя как иерархически детерминированный кошелек (HD wallet) с поддержкой большинства ожидаемых функций бухгалтерии и безопасности по стандартам индустрии — например, паролей на расходные транзакции или мнемоник BIP39. В следующих поколениях Daedalus станет средой разработки приложений с магазином, универсальными интеграционными API и набором средств разработки.

Ключевыми новшествами будет упрощение разработки (программисты смогут использовать JavaScript, HTML5 и CSS3 для своих приложений) и унифицированный мост для коммуникации между приложениями. От сложного поведения, например, криптографии, распределенных сетей и механик баз данных, можно будет

[25] Он уже доступен по адресу daedaluswallet.io.

Международная лицензия Creative Commons Attribution 4.0

абстрагироваться. Разработчики смогут сосредоточиться исключительно на взаимодействии с пользователем и базовой логике приложения.

Поскольку предполагается, что Daedalus будет универсальной средой разработки, план развития этого проекта не зависит от плана развития Cardano. В 2017 году они еще тесно связаны, но позже Cardano будет просто одним из приложений для пользователя Daedalus. Мы также рассматриваем некоторые уникальные функции, например, универсальную службу управления ключами, которая работает целиком в Intel SGX.

Создавая протокол, мы не можем учесть абсолютно все нужды пользователей. Однако мы надеемся, что гибкость, которую предлагает Daedalus, и умные контракты с отслеживанием состояния, работающие под CCL, смогут удовлетворить те нужды, которые остались за рамками наших проектных решений. Кроме того, мы надеемся, что это позволит улучшить стандарты в нашей индустрии, и у всех криптовалют повысится уровень совместимости и безопасности.

4. Регулирование

Ложная дихотомия

Законодательство часто бывает запутанным и непонятным. В результате получаем нарушителей и гоняющихся за ними блюстителей закона. Законодательство — главный инструмент того, кто вершит правосудие. Но как любой инструмент, оно может быть недоработанным или устаревшим, его можно неправильно применить.

Криптовалюты не уберут из нашего уравнения человеческий фактор. Всегда найдутся мошенники, недобросовестные участники и вышедшие кому-то боком благие намерения. Криптовалюты могут убрать человеческую субъективность, но человеческое поведение никуда не денется.

Тот, кто проектирует криптовалюту, должен решить, каким инструментом он снабдит регулятивный орган для исправления негативных событий. Уникальная проблема, с

Международная лицензия Creative Commons Attribution 4.0

которой сталкиваются криптовалюты — они сами по себе являются результатом законодательных и финансовых провалов[26].

Исторически многие из тех, кто работает с криптовалютами, считают, что действия правительства могут быть коррумпированными, неадекватными или неэффективными. Поэтому у них не появляется ни уважения, ни терпения, ни желания предусматривать запасной ход для регулятивных органов на случай необходимости восстановить справедливость. Создание такого запасного хода — кощунство с точки зрения самой сути криптовалют.

С другой стороны, если учесть только сбои при обменных операциях и исторические события, более 10 процентов биткоинов было утеряно или похищено с момента запуска протокола — 3 января 2009 года. На 30 января 2017 года стоимость всех утерянных или похищенных биткоинов составила чуть больше 4 миллиардов долларов. И сюда не входят биткоины и другие токены, утерянные в результате мошенничества и плохо организованных ICO (первичных предложений монет).

Есть еще проблема с конфиденциальностью. На макроуровне стоимость перемещается по специальным каналам, которые регламентированы, богаты метаданными и активно наблюдаются правоохранительными органами, правительствами и международными регулирующими органами. Правила этой игры всем хорошо знакомы, и утечки случаются только при использовании наличных денег — что бывает все реже и реже, поскольку весь мир переходит на электронные деньги.[27]

Если бы криптовалюты не существовали, то, похоже, мир стал бы воспринимать финансовые тайны примерно как информацию в социальных сетях. Тайны не существует и с этим никто ничего бы не мог поделать. Таким образом мы получаем дилемму из двух очевидных вариантов.

Создатель криптовалюты может предать принципы и вписать в свой код все, что от него требует местное законодательство, таким образом ставя под удар конфиденциальность и неприкосновенность своих пользователей. Или он может остаться верным принципам, но это — анархический подход, нежелание сотрудничать с нынешними передовыми подходами и нынешним законодательством.

---

[26] Сатоси добавил в первичный блок Bitcoin следующий заголовок из газеты The Times: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks (рус. "The Times, 3 января 2009 г.: Канцлер почти готов предоставить банкам помощь во второй раз")*

[27] Здесь читателю предлагается при желании ознакомиться с книгой Дэвида Вулмана The End of Money (рус. "Конец денег"). В ней рассказывается о международном движении против пропажи наличности.

Международная лицензия Creative Commons Attribution 4.0

В случае Cardano мы решили, что эти два варианта — ложная дихотомия, происходящая из недостатка воображения. На самом деле большинство пользователей даже не думают о том, какие законы действуют на рынках. Обычно их волнует только внезапное изменение этих законов в пользу одного или нескольких участников. Их волнует непрозрачность того, кто получает дополнительные привилегии.

Следует различать права физических лиц и права рынков. Учитывая глобальный характер криптовалют, права должны быть настолько ориентированы на пользователя, насколько это возможно.

Конфиденциальность должна быть разумной, и контролировать ее должен сам пользователь, а не какой-либо посредник. Движение стоимости не должно ничем ограничиваться. Стоимость не должна подвергаться отчуждению без согласия пользователя.

Если говорить о рынках — использование рынком данных и средств должно быть полностью прозрачно, и все участники рынка должны играть по одним и тем же правилам. Кроме того, если пользователь дал свое согласие, он не может внезапно передумать, потому что ему вдруг стало неудобно. Другой стороне тоже нужны гарантии.

Но как именно перейти от абстракции к реальной системе? Как выглядит "что-то практичное и разрешенное законодательством"? Мы разбили решение на три категории: метаданные, аутентификация и соответствие законам (а также DAO рынков).

Метаданные

Какое-либо действие зачастую может быть менее интересным, чем метаданные о нем. Например, "ехать из Денвера в Боулдер" — здесь речь идет о действии. А "ехать из Денвера в Боулдер на автомобиле Ferrari 488 со средней скоростью 190 км/ч" — это уже метаданные. И опыт этот будет разительно отличаться от поездки в автомобиле Toyota Prius со средней скоростью 50 км/ч.

С финансовыми транзакциями ситуация такая же. Окружающий их контекст очень важен для экономистов, налоговых органов, правоохранительных органов, предприятий и других структур. К сожалению, в нынешней системе, основанной на фидуциарных деньгах,

Международная лицензия Creative Commons Attribution 4.0

большинство пользователей не знает, какие метаданные у их транзакций и кто имеет к ним доступ[28].

В случае Cardano мы понимаем, что иногда пользователи могут или должны передавать метаданные транзакции определенным структурам — например, налоговым органам. Но мы убеждены, что пользователь должен дать свое согласие на передачу подобной информации.

Мы также считаем, что у блокчейн-систем есть огромный потенциал по устранению мошенничества, пустых трат и злоупотребления, поскольку они предлагают возможности аудита, метки времени и неизменяемость. Поэтому в блокчейне Cardano должны быть некоторые метаданные.

Сложность здесь в нахождении верного баланса, который не будет непомерно раздувать наш блокчейн. Учитывая это, мы избрали прагматичный подход.

Во-первых, в течение следующих 12 месяцев Daedalus начнет поддерживать огромный набор функций для маркировки транзакций и видов финансовой деятельности. Эти метаданные можно будет экспортировать и давать доступ к ним кому угодно по желанию пользователя. Кроме того, данными можно будет управлять из приложений, разработанных сторонними компаниями для узкоспециализированных целей (например, налогообложение).

Во-вторых, мы исследуем возможность добавления поддержки для специальных адресов, которые могут включать хеши и зашифрованные поля. Такая структура позволит пользователю делиться данными в рамках нашего блокчейна, не делая их публичными. Если пользователь захочет дать кому-либо доступ к своим данным, это можно будет сделать точно так же, как с транзакцией — с теми же возможностями для аудита, метками времени и неизменяемостью.

Мы уже сделали структуру адреса, в которой есть поле атрибута. Сейчас оно используется для хранения зашифрованной копии дерева иерархически детерминированного кошелька для быстрого восстановления кошелька (см. документацию по HD Wallets). В более поздних версиях мы обобщим эту конструкцию.

---

[28] Если рассматривать более глобальный уровень, то автор Juan Zarate в своей книге Treasury's War пишет о том, как эти данные использует Министерство финансов США для борьбы с терроризмом. Это дает подробное представление о том, как нынешняя структура мировых финансовых рынков может использоваться в геополитике.

Международная лицензия Creative Commons Attribution 4.0

Аутентификация и соответствие законодательству

С транзакциями тесно связаны темы прав на совершение транзакции и владение средствами. Например, даже если у пользователя достаточно средств на совершение какой-либо транзакции (например, покупку алкоголя), она все еще может подпадать под определенные ограничения (например, недостаточный возраст пользователя).

Обычно право на владение средствами и происхождение средств реализуется принципом "знай своего покупателя". Когда предприятия, предоставляющие финансовые услуги — например, банк или обменник — открывают учетную запись для нового клиента, они, как правило, должны собрать базовые факты о личности клиента и происхождении его средств.

Техническая сложность здесь в том, что в процессе подачи этой обязательной по закону информации пользователь, пересылающий информацию, не получает гарантий относительного того, как она будет использоваться, храниться и будет ли она когда-либо уничтожена. Персональные данные имеют коммерческую ценность. Их можно похитить для того, чтобы притвориться кем-то другим или перепродать — там, где это позволяют законы.

В случае с Cardano мы хотим изменить это положение вещей настолько, насколько сможем. С точки зрения программного обеспечения и протоколов почти нет способов гарантировать, что получатель данных будет действовать только в рамках дозволенного. Но вот с точки зрения аппаратного обеспечения протоколов можно использовать Intel SGX и другие аппаратные модули безопасности (HSM) для претворения в жизнь определенных принципов.

Поэтому мы исследуем возможность использовать технологию Sealed Glass Proofs вместе с определенной политикой доступа к данным, чтобы обеспечить безопасную передачу персональных данных контролеру. Контролер, в свою очередь, обязан соответствовать определенной политике доступа к данным. Мы считаем, что могут появиться два унифицированных стандарта, и что такой метод уменьшит риск потери контролером персональных данных пользователя в результате атаки хакеров.

Уровневая модель для Cardano, разделяющая передачу стоимости и вычисления, также может использовать этот подход. Если CCL запускают предприятия, ограниченные законодательством (например, обменники или казино), им придется проверять

Международная лицензия Creative Commons Attribution 4.0

персональные данные пользователей и, возможно, применять к ним политики налогообложения.

Используя технологию SGP, пользователи могут посылать средства вместе с данными, идентифицирующими личность, не опасаясь при этом, что данные попадут в общий доступ или будут навсегда сохранены узлами консенсуса в CCL. Таким образом CCL получит уверенность в том, что все транзакции пользователей аутентифицированы и легальны.

Подобный подход также дает возможность переноса учетной записи клиента между регулируемыми предприятиями. Биржи могут мгновенно переносить балансы и учетные записи клиентов, используя эти безопасные каналы, а также передавать данные регулирующим органам там, где это разрешено законом.

Мы надеемся провести первый бета-тест этой технологии в середине 2018 года и интегрировать ее в Cardano в конце 2018 или начале 2019 года в зависимости от результатов исследования. Это расписание верно в случае, если нам дадут возможность сотрудничать с ARM и Intel, чтобы наш код можно было запускать на их оборудовании[29].

Рыночные DAO

В двух предыдущих главах речь шла о генерации и движении информации, если предположить, что существует некая внешняя система. Чтобы обеспечить совместимость с традиционными финансовыми системами, всегда будет нужна такая функциональность — но она не касается регулирования на базе блокчейна.

Умные контракты предлагают совершенно новую финансовую систему, в которой отношения между сторонами детерминированы и не могут быть неправильно поняты. Их, в свою очередь, можно использовать для создания правил рынков, включая структуры произвольной сложности — например, арбитраж, возмещение средств или обнародование фактов при определенных условиях.

Мы называем такие структуры на основе умных контрактов "рыночные DAO" (англ. "Marketplace DAO"). Для них не нужна ни поддержка в протоколе, ни изменяемое состояние. Они могут быть полностью сконструированы из взаимозависимых умных контрактов.

[29] См. Intel SGX Commercial License Policy

Международная лицензия Creative Commons Attribution 4.0

Архитектурная концепция состоит в том, чтобы создать коллекцию коммерческих шаблонов на основе контрактного права и передовых бизнес-практик. Эти шаблоны можно встроить в умный контракт какого-либо разработчика, чтобы получившийся рынок соответствовал заданным условиям.

Пусть, например, разработчик хочет создать токен ERC20 на базе CCL, чтобы провести краудсейл (англ. "crowdsale" — эмиссию и продажу по фиксированной цене внутренней валюты организации). Можно создать рыночное DAO специально для краудсейл-продаж с условиями, выбранными самим разработчиком или продиктованными требованиями закона. Компенсации, перераспределение средств или заморозка платежей — все это можно взять из ERC20-контракта разработчика.

Такая инициатива позволяет нам начать масштабное обсуждение того, как следует контролировать рынок, чтобы обеспечить должную защиту прав потребителей.
Во-вторых, мы можем обсудить, как моделировать транзакции таким образом, чтобы автоматически обеспечивать правовую защиту, полагающуюся в определенной юрисдикции — например, штата Нью-Гэмпшир.

Сотрудничая с Cardano Foundation, IOHK и другими предприятиями, проект Cardano предоставит референс-библиотеку различных рыночных DAO, чтобы их могли использовать разработчики умных контрактов. Мы надеемся, что с помощью рыночных DAO будут формироваться рынки страхования и регулирования, которые будут самостоятельно развиваться на основе происходящих событий.

5. Самодостаточность

В области криптовалют существует много концептуальных противоречий. Криптовалюты создаются так, чтобы их было сложно изменить, но при этом, как любые технологии, их нужно постоянно улучшать — а значит, изменять. Блокчейны должны препятствовать сосредоточению управления в одних руках, но при этом для проведения перемен или поддержки кода нужны влиятельные структуры.

Самые неприятные случаи — это когда есть явные недочеты, и большинство стейкхолдеров согласны, что их надо исправить, но не могут прийти к консенсусу относительно дальнейших шагов.

Международная лицензия Creative Commons Attribution 4.0

Размер блоков в Bitcoin активно обсуждается уже более двух лет. Каждый день транзакции общей стоимостью более миллиарда долларов стоят в очереди на выполнение, потому что сеть достигла максимальной пропускной способности.

Если невозможно согласовать изменение всего одного параметра, и это при том, что существуют временные решения — как предприятия и правительства могут со спокойным сердцем инвестировать миллиарды долларов в построение инфраструктуры на основе таких систем? Как может предприятие идти на стратегические риски, делая ставку на протоколы, которые не могут провести разумные улучшения проекта?

Если мы обратимся к истории, то развитие интернета шло по тому же пути: даже простые изменения, например, переход от IPv4 к IPv6 занял десятилетия. С другой стороны, технология блокчейн и интернет очень различаются тем, что у них совершенно разные стили кураторства.

Интернет начался как военный проект, который перешел из-под опеки DARPA (Управление перспективных исследовательских проектов Министерства обороны США) в академические круги с мощной правительственной поддержкой и хорошо известным набором кураторов. Интернет развивался в некоммерческих условиях без корпоративных махинаций в попытках монополизировать всю сеть. На самом деле интернет-коммерция была нарушением Приемлемой политики использования интернета Государственного научного фонда США (NSF AUP),пока ее в 1992 году не отменили.

К моменту, когда интернет стал коммерческой площадкой, уже существовал понятный набор стандартов и принципов, были активисты, продвигающие те или иные принципы. Это не помешало некоторым компаниям, например, AOL и Microsoft, создавать закрытые экосистемы и разрабатывать проприетарные технологии, например, ActiveX. Это не помешало таким структурам, как Google, воплощать собственные программы, учитывая их огромные базы пользователей и суммы капитала.

Учитывая огромное количество участников с рентоориентированным поведением[30] — от трейдеров до майнеров — криптовалюты по своей сути являются коммерчески мотивированными экосистемами. И поэтому кураторство в сфере криптовалют развивалось таким образом, что произошла оптимизация в соответствии с личными интересами.

Например, сейчас все чаще происходит выпуск пустых блоков, так как это увеличивает прибыль майнера, но это полностью противоречит смыслу и предназначению процесса

[30] По ссылке больше информации

Международная лицензия Creative Commons Attribution 4.0

майнинга. Уже произошла централизация майнинга, поскольку небольшое количество структур контролирует большую часть мощностей Bitcoin.

Как и в случае с интернетом, чтобы изменить криптовалюту, нужно прийти к консенсусу. Но если происходит такое быстрое сосредоточение власти в руках небольшого количества брокеров, что случится, если какое-либо изменение будет им невыгодно?

Здесь ситуация уже не такая: криптовалюты, в отличие от интернета, появляются не в результате альтруистического некоммерческого или научного процесса. С самого начала какая-то группа ищет прибыли, и есть какие-то влиятельные деятели, которые помогут эту прибыль получить.

В своем развитии каждая криптовалюта должна пройти через этап централизации. Мы не можем полностью этого избежать, однако должны хотя бы ориентироваться на постепенную децентрализацию.

В случае Cardano мы тщательно продумали, какие факторы поддерживают централизацию и какие техники можно применить, чтобы наш протокол постепенно стал общественной инфраструктурой — как интернет.

Мы признаем, что полная децентрализация невозможна и, наверное, даже антипродуктивна. Но некоторые факторы можно усилить, чтобы получилась более сбалансированная система.

Во-первых, хотя централизованный контроль за фондами первичной распродажи токенов обеспечивает гибкое и быстрое развитие протокола на начальном этапе, постепенно финансирование нужно диверсифицировать, а темпы разработки — снижать до более спокойных, позволяющих систематический подход. В соответствии с этим пунктом на финансирование не должны влиять никакие культурные, лингвистические и географические предрассудки.

Во-вторых, поскольку сообщество все больше понимает в технологии, лежащей в основе криптовалют, решения о плане развития не могут принимать только ключевые разработчики. Должен быть основанный на блокчейне метод голосования, проверок и внесения изменений в протокол.

В-третьих, все инициативы по поддержке блокчейна Cardano SL должны быть напрямую связаны с общими пожеланиями всех пользователей. Нельзя допустить доминирования избранных деятелей, которые не зависят от воли остальных участников сообщества.

Международная лицензия Creative Commons Attribution 4.0

Для выполнения первого принципа мы решили интегрировать в Cardano систему казначейства (treasury system). Для выполнения второго принципа мы запустим формальный процесс, который позволит вносить предложения по улучшению Cardano (Cardano Improvement Proposals), используя систему, которую координирует CSL. А что касается третьего принципа — мы считаем, что Ouroboros может предложить элегантное решение.

По вышеуказанным темам есть и более детальная информация, однако она уже выходит за рамки обзорного доклада. Проектирование механизмов распределения (mechanism design) — одна из самых сложных научных областей со множеством взаимосвязей, пока еще неполной теорией и отсутствием стабильной классической модели, от которой можно отталкиваться.

Наш наукоориентированный подход, описанный во второй главе, здесь очень помогает. Команда IOHK Veritas совместно с группой исследователей Ланкастерского университета под руководством профессора Bingsheng Zhang разрабатывает эталонную модель казначейства Cardano. Мы надеемся на интеграцию в 2018 году и ожидаем рецензированную публикацию по этой теме к концу 2017 года.

В сфере формальных описаний и предварительного анализа изменений эта тема наименее понятна — здесь и онтологические концепции, и механизм для поощрения всеобщего участия. Возможно, здесь получится применить какой-то типичный демократический процесс или использовать Liquid Feedback для обеспечения более рационального голосования.

Мы предполагаем, что участие IOHK в разработке Cardano будет заключаться в проведении исследований в этом направлении[31]. Для начала параллельно с эталонной моделью казначейства мы запустим несколько механизмов для фиксирования согласия. Для того, чтобы уверенно выбрать решение, необходимы дальнейшие исследования.

И наконец, работа по улучшению премиальных схем в протоколе Ouroboros проходит под наблюдением профессора Elias Koutsoupias из Оксфордского университета. После того, как основные криптографические принципы Ouroboros закрепятся и будут проведены все необходимые работы по масштабируемости, мы добавим в эталонный протокол более широкий анализ облигаций, штрафов и премиальных схем.

[31] IOHK будет заниматься разработкой Cardano до конца 2020 года.

Международная лицензия Creative Commons Attribution 4.0

6. Заключение

Криптовалюта — это больше, чем просто сумма протоколов, исходного кода и выполняемых им функций. Это общественная система, которая вдохновляет и объединяет людей и помогает им. Разочаровавшись в полумерах, провалах и нарушенных обещаниях протоколов прошлого, мы хотим построить нечто лучшее.

Этот процесс непростой — и мы никогда не считали, что его можно довести до конца. Социальные протоколы продолжают изменяться вместе с людьми и обществом. Мы хотим, чтобы проект Cardano приносил пользу, и для этого придется поймать саму концепцию эволюции и заключить ее в наш проект.

Эволюцией не может управлять только одна рука или только один великий замысел. Ею правят счастливые случаи, происходящие в результате бесконечных ошибок и проблем. Проект Cardano — это попытка цифрового воплощения эволюции, способная выжить на современных рынках и приспособиться к требованиям будущего.

Предыдущие главы дают краткое описание того, какими путями мы идем к этой цели. Мы стараемся замечать собственные когнитивные искажения, учиться на ошибках истории и придерживаться научного подхода. Мы пытаемся удержать баланс между необходимостью быстрой разработки и формальными методами, которые обычно неторопливы.

Для нас большая честь стоять у истоков этого пути. За прошлые два года мы разработали протокол с защитой по методу proof of stake с доказанной эффективностью, наняли небольшую армию разработчиков на Haskell, а также привлекли к работе по Cardano множество талантливых ученых.

На пути от лабораторного образца к полностью запущенной системе проблем будет все больше и больше. Но мы надеемся, что будущее криптовалюты Cardano можно выразить в одной очеловечивающей ее фразе. Cardano — прагматичная мечтательница, которая учится у старших, законопослушная гражданка в своем сообществе, и она всегда платит по счетам.

Международная лицензия Creative Commons Attribution 4.0

Мы не знаем, каким окажется будущее, но стараемся сделать его лучше для всех.
Спасибо за внимание.

Международная лицензия Creative Commons Attribution 4.0