Правительство
Управление науки

Технология распределенного реестра: за рамками блокчейн

Отчет главного научного советника Правительства Великобритании

Содержание

Предисловие 4

Основные положения и рекомендации 5

Определения 17

Глава 1: Концепция 21

Глава 2: Технология 33

- **Практический пример - Исследования и обзор перспектив** 37

Глава 3: Управление и регулирование 41

Глава 4: Безопасность и конфиденциальность 47

Глава 5: Разрушительный потенциал 53

- **Практический пример - Бриллианты** 56
- **Практический пример - Корпоративные сделки** 58
- **Практический пример - SETL'ирование транзакций** 60

Глава 6: Применения в государственном управлении 65

Глава 7: Глобальные перспективы 73

- **Практический пример - Европейский энергетический рынок** 76
- **Практический пример - Блокчейны в Эстонии изменяют процессы оплаты, торговли и электронной подписи** 80

Ссылки 84

Благодарности 87

Короткое сопроводительное видео к настоящему отчету доступно по ссылке: https://youtu.be/4sm5LNqL5j0

Предисловие

Прогресс человечества характеризуется ростом новых технологий и человеческой изобретательностью, их открывшей.

В случае технологии распределенного реестра мы можем быть свидетелями одного из тех возможных взрывов творческого потенциала, который позволяет достичь выдающихся высот в инновациях.
Может оказаться, что эта технология способна предоставить новый уровень доверия широкому спектру услуг. Как политика открытых данных, и в этом мы уже убедились, коренным образом изменила взаимоотношения граждан и государства, так и прозрачность этих технологий может изменить к лучшему наши финансовые рынки, каналы поставок, клиентские и b2b сервисы, и публичные регистры.

Мы знаем, что нам придется столкнуться с испытаниями, так как Распределенные реестры разовьются и разрушат наше представление о данных и о способах их хранения. Великобритания имеет уникальную возможность изучить эти явления и позволить нашим государственным услугам и нашей экономике извлечь из данной технологии максимальную пользу. У нас уже есть цифровые мощности мирового класса, инновационные финансовые сервисы, сильное исследовательское сообщество и возрастающая компетентность частного сектора.
Жизненно необходимо, чтобы наши ключевые активы - включая Институт Алана Тьюринга (Alan Turing Institute), Институт Открытых Данных (Open Data Institute) и исследовательский центр Digital Catapult - работали вместе с частным сектором и международными партнерами, чтобы полностью раскрыть потенциал этой технологии.

Поэтому, мы оба испытываем огромную радость, совместно работая на ведущих позициях в этой области, и с нетерпением ждем возможности поработать с другими ведомствами по освоению этих возможностей. А также, поработать над пониманием того, как может быть применены данная технология, чтобы граждане Великобритании и ее экономика могли извлечь из этого значительную выгоду.

ДОСТОПОЧТЕННЫЙ ЧЛЕН ПАРЛАМЕНТА
МЭТТЬЮ ХЭНКОК
Министр по делам Администрации
Кабинета министров и Генеральный казначей

ДОСТОПОЧТЕННЫЙ ЧЛЕН ПАРЛАМЕНТА
ЭД ВЭЙЗИ
Государственный министр
по делам культуры и электронной экономики

Основные положения и рекомендации

Введение

Алгоритмы, позволяющие создать распределенные реестры, это мощные, разрушительные инновации, которые могут изменить способ предоставления государственных и частных услуг, а также увеличить продуктивность посредством широкого спектра применений.

Реестры были в основе коммерческой деятельности с древних времен и использовались для записи информации о многих вещах, но в основном о таких активах, как деньги или имущество. Сначала для записи использовались глиняные таблички, затем папирус, пергамент и бумага. Однако за все это время единственным примечательным нововведением было внедрение компьютерной техники, которое вначале использовалось просто для переноса информации с бумаги в цифровой код. На текущий момент алгоритмы впервые делают возможным совместное создание цифровых распределенных реестров, которые обладают свойствами и возможностями, идущими далеко за пределы традиционных бумажных реестров.

Распределенный реестр по сути это база данных активов, которая может быть распределена по сети разнообразных сайтов, в разных географических зонах или организациях. Все участники сети могут иметь свою собственную, идентичную копию реестра. Любые изменения в реестре отражаются во всех копиях в течение нескольких минут, а в некоторых случаях, секунд. Активы в реестре могут быть финансовыми, юридическими, физическими или электронными. Безопасность и достоверность хранимых в реестре активов осуществляется криптографически с помощью "ключей" и подписей, которые контролируют кто и какие действия может производить в общем реестре. Записи реестра также могут быть изменены одним, несколькими или всеми участниками сети, в зависимости от правил, принятых в сети.

В основе этой технологии лежит "блокчейн", технология изобретенная для создания пиринговой (децентрализованной) цифровой валюты Биткойн в 2008 году. Алгоритмы блокчейн позволяют объединять Биткойн-транзакции в "блоки" и добавлять их в "цепочку" существующих блоков, используя криптографическую подпись. Реестр Биткойн создан распределенным и "неконтролируемым", то есть любой может добавить блок транзакций, если он сможет собрать криптографический паззл для добавления каждого нового блока. Стимулом для этого служит награда в в виде двадцати пяти биткойнов, сложившему пазл, за каждый "блок". Любой, у кого есть доступ в интернет и вычислительные мощности для сборки криптографического пазла, может добавлять блоки в реестр. Таких людей называют "майнерами Биткойнов" (от английского "mine" добывать). Аналогия с "добычей" вполне уместна, так как процесс "майнинга" Биткойнов энергоемкий, поскольку требует больших вычислительных мощностей. Было рассчитано, что для генерации биткойнов требуется мощность свыше 1Гигаватта, что может быть сопоставимо с использованием электричества Ирландией.

Биткойн - это электронный эквивалент наличных денег. Подлинность наличных денег проверяется по их внешнему виду и определенным признакам, в случае с банкнотами это серийные номера и другие средства защиты. Но в случае использования наличных денег нет никакого реестра, в котором содержались бы записи о транзакциях, а также существует проблема подделки как монет, так и банкнот. В случае с биткойнами, реестр транзакций гарантирует их подлинность. И деньги и биткойны должны храниться в безопасном месте, в реальном или виртуальном кошельках соответственно - и если за ними не следить должным образом, то и деньги и биткойны могут быть украдены. Коренным отличием между обычными валютами и биткойнами является то, что первые выпускаются центральными банками, а последние выпускаются в согласованных количествах глобальным "совместным" усилием, что и является технологией Биткойн. Наличные деньги как способ обмена и торговли возникли тысячелетия назад, и их происхождение связано с раковинами каури, чеканными монетами и теперь с Биткойн.

Но данный отчет не о Биткойн. Он об алгоритмических технологиях, которые делают возможным существование Биткойн, и об их возможностях трансформировать реестры как инструменты, способные записывать, производить и обеспечивать защиту огромного количества транзакций. Так основной подход блокчейна может быть изменен, чтобы объединить в себе правила, смарт-контракты (также используется термин "умные контракты"), цифровые подписи и ряд других новых инструментов.

Технологии распределенного реестра могут помочь правительственным органам собирать налоги, выплачивать пенсии, выдавать паспорта, вносить записи в земельный кадастр, гарантировать каналы поставок товаров и в общем обеспечивать точность записей о государственной деятельности и услугах. В сфере Национальной службы здравоохранения Великобритании (National Health Service) эти технологии предоставляют возможность совершенствования здравоохранения путем улучшения и подтверждения качества услуг, а также безопасного совместного использования записей в соответствии со строгими правилами. В зависимости от обстоятельств, технология позволяет давать возможность отдельным получателям услуг контролировать доступ к персональным данным и узнавать, кто их использовал.

Существующие методы управления данными, особенно персональными данными, как правило используют крупные традиционные IT-системы, расположенные внутри отдельного учреждения. К ним добавляется ряд систем управления сетью и систем сообщений для связи с внешним миром, которые увеличивают стоимость использования IT-системы и ее сложность. Высоко централизованные системы демонстрируют высокие затраты при любом сбое. Они могут быть уязвимы для кибер¬атак, а данные часто несинхронизированы, неактуальны или попросту некорректны.

В отличие от них, распределенные реестры по своей сути гораздо лучше защищены от атак, потому что вместо одной базы данных они представляют собой множество копий одной и той же базы данных, и, таким образом, чтобы быть успешной, кибератака должна быть произведена на все копии одновременно. Технология также является устойчивой для несанкционированного изменения или взлома, так как участники сети сразу же обнаружат изменения в одной из частей реестра. Вдобавок к этому, методы, используемые для защиты и обновления информации, подразумевают, что участники могут делиться данными и быть уверенными, что все копии реестра совпадают друг с другом в любой момент времени.

Но это не значит, что распределенные реестры совершенно неуязвимы для кибератак, потому что, если кто-нибудь сможет найти способ "легально" изменить одну копию, то он изменит все копии реестра. Таким образом обеспечение безопасности распределенных реестров важная задача и часть общей проблемы обеспечения безопасности цифровой инфраструктуры, от которых зависит современное общество.

Правительства некоторых стран уже начинают использовать технологии распределенного реестра в своей работе. Например, правительство Эстонии в течение нескольких лет экспериментирует с технологией распределенного реестра, используя одну из реализаций технологии, известной как KSI (Keyless Signature Infrastructure - Инфраструктура подписи без кода), разработанной эстонской компанией Guardtime.

KSI позволяет гражданам проверять точность их записей в государственных базах данных. Также представляется невозможным выполнение незаконных действий инсайдерами с привилегированным доступом для работы с данными внутри правительственной сети. Способность гарантировать гражданам, что их данные корректны и хранятся в безопасном месте, позволило Эстонии запустить электронные услуги, такие как Электронный Бизнес Реестр (e-Business Register) и Электронные налоги (e-Tax). Эти услуги снизили

административную нагрузку на государство и граждан. Эстония - одна из группы государств "Digital 5", или D5, в которую также входят Великобритания, Израиль, Новая Зеландия и Южная Корея. У Великобритании есть возможность работать с этими и другими имеющими схожую позицию государствами и учиться у них, как внедрять технологию блокчейн и связанные с ней технологии.

Деловое сообщество быстро оценило открывшиеся возможности. Распределенные реестры могут предоставить новые способы обеспечения прав собственности и подтверждения происхождения товаров или интеллектуальной собственности. Например, Everledger (Вечный Реестр) предоставляет распределенный реестр, который гарантирует подлинность бриллиантов, начиная с их добычи и огранки до продажи и страхования. На рынке с относительно высоким уровнем подделки документов, эта технология делает установление подлинности более эффективным и дает возможность уменьшить количество фактов мошенничества и предотвратить поступление на рынок "кровавых бриллиантов".

Большая сложность состоит в коммуникации с высокопоставленными политиками и общественностью о важности этих новых технологий - и это одна из главных задач настоящего отчета.

Первая сложность при коммууникации - это стойкая ассоциация технологии блокчейн с системой Биткойн. Биткойн это криптовалюта, названная так, потому что криптография лежит в основе генерации и отслеживания валюты. Биткойн вызывает подозрение у граждан и государственных чиновников, потому что ассоциируется с преступными сделками и торговыми сайтами "темной сети", такими как интернет-портал Silk Road (Шелковый Путь), на данный момент неработающий. Но цифровые криптовалюты представляют интерес для центральных банков и государственных финансовых учреждений по всему миру, которые с большой заинтересованностью изучают их. Все потому, что электронное распространение цифровой валюты дает высокую отдачу. И в отличие от физической валюты, цифровая валюта сопровождается реестром транзакций, которые отсутствуют в случае физических наличных денег.

Вторую сложность для коммуникации представляет сбивающий с толку набор терминологии. Терминология разъясняется Саймоном Тейлором, который предоставил список определений в конце этого обзора. Одним из терминов, которые могут запутать пользователей - это "распределенный", который приводит к ошибочному представлению, что если что-то распределено, следовательно, не существует и полностью контролирующего это учреждения или владельца. Это может быть так, а может быть иначе - все зависит от выбранной модели реестра. На практике существует широкий спектр моделей распределенных реестров с различной степенью централизации и различными видами контроля доступа для удовлетворения различных нужд бизнеса. Это могут быть как "неконтролируемые" реестры, которые позволяют добавлять данные кому угодно и не могут принадлежать кому-либо; так и "контролируемые" реестры, которые могут иметь одного или несколько собственников, и только они могут добавлять записи в реестр и проверять его содержимое.

Ключевая идея в том, что, полностью понимая эту технологию, правительство и частный сектор могут выбрать модель, которая наилучшим образом соответствует определенной цели, балансируя между безопасностью и централизованным контролем для удобства и возможности делиться данными между учреждениями и физическими лицами.

Как и с большинством новых технологий, довольно сложно в полной мере оценить все будущие способы использования и угрозы. И в случае с каждой новой технологией вопрос не в том, хороша ли сама по себе технология или плоха. Вопросы в том: какое применение может найти технология? для какой цели? и в каком виде она может быть применена и как гарантирует безопасность?

Чтобы ответить на эти вопросы, Управление науки Правительства Великобритании создало группу экспертов от бизнеса, правительства и ученых с целью оценки возможностей распределенных реестров для использования правительством и частным сектором, и определения действий, которые потребуется выполнить правительству и другим заинтересованным лицам, чтобы способствовать использованию технологии распределенных реестров для получения пользы и избежать возможного вреда. Целью этого было расшифровать терминологию данной технологии для политической аудитории и предоставить правительственным чиновникам ее концепцию и основания для принятия ими решения, где ее необходимо применять и как ее лучше всего вводить в действие.

Подводя итог вышесказанному, технология распределенного реестра предоставляет правительству платформу для снижения объемов мошенничества, коррупции, ошибок и стоимости процессов, интенсивно работающих с бумажными документами. Она обладает потенциалом переопределить взаимоотношения между государством и гражданином по вопросам совместного использования данных, прозрачности и доверия. У нее есть схожие возможности и для частного сектора.

Этот краткий обзор описывает восемь основных рекомендаций из опыта нашей работы. Они представлены в виде сводного описания ключевых моментов из семи глав, которые описывают концепцию, технологию, государственное управление, конфиденциальность и безопасность, разрушительный потенциал, способы применения и глобальные перспективы. Главы были написаны экспертами в технологии распределенных реестров языком, который должен быть доступен людям, которые экспертами не являются. Я чрезвычайно благодарен этим экспертам за их наставления и содержательный вклад.

Марк Уолпорт, главный научный советник Правительства Ее Величества, Декабрь 2015

Концепция

Распределенные реестры дают ряд преимуществ правительству и другим организациям общественного и частного сектора. Как следует из их названия, они могут быть чрезвычайно широко распределены и при этом тщательно контролироваться. Они очень эффективны, потому что изменения, сделанные любым участником с необходимыми привилегиями на модификацию реестра, будут немедленно отражены во всех копиях реестра. Наравне с этим они надежно отклоняют несанкционированные изменения, таким образом исказить информацию в реестре чрезвычайно сложно. Однако распределенные реестры не должны рассматриваться как самоцель. Только в том случае, когда они для используются для других применений - таких как смарт-контракты (или "умные контракты") - они могут раскрыть весь свой потенциал.

Главная задача государства при поддержке развития технологии распределенных реестров заключается в разработке четкой концепции того, как эта технология может улучшить деловые процессы государственных органов и каким образом она может быть использована для оказания услуг гражданам. Вслед за этим государство должно выступить в роли продвинутого заказчика, внедряющего эту технологию - приобрести распределенные реестры для применения там, где это уместно. Поступая таким образом, государство может поддерживать и влиять на развитие экономической активности в соответствующем секторе, способствуя как возникновению новых растущих компаний, так и деятельности уже существующих более крупных предприятий.

Государство может способствовать наступлению будущего, в котором предоставление государственных услуг является более персональным, немедленным и эффективным. Там, где это уместно, у граждан должна быть возможность сигнализировать о своих индивидуальных предпочтениях и потребностях за счет участия в смарт-контрактах. Реализация распределенных реестров со встроенными в них смарт-контрактами должна привести к существенным улучшениям в соблюдении соответствий требованиям и нормам, в отчетности и экономической эффективности и надежности.

Служба электронных услуг Правительства (Government Digital Service, GDS) Великобритании разрабатывает электронную платформу, через которую государственные органы будут предоставлять свои услуги, и распределенные реестры могли бы стать ключевым элементом этой платформы.

Рекомендация 1: Мы рекомендуем правительству:

- *Назначить ответственных за данное направление на уровне министров, чтобы государство обеспечило разработку концепции, руководителей и платформу в рамках государственного управления. В частности, Служба электронных услуг должна возглавить работу в государственном секторе как пользователь распределенных реестров, а Управление электронной экономики (Digital Economy Unit) Министерства культуры, СМИ и спорта (Department for Culture, Media and Sport, DCMS) – сделать то же самое, создавая необходимые условия для внедрения распределенных реестров (взаимодействуя с Министерством по делам бизнеса, инноваций и компетенций и уполномоченным органом по инновациям – агентством Innovate UK).*

- *Службе электронных услуг и Управлению электронной экономики следует, на основе материалов отчета и уже проводимой сейчас министерствами работы, разработать высокоуровневый план создания необходимых возможностей и, поддерживающий его, более детальный план, и своевременно выполнить эти планы. Им также следует контролировать, как выполняются другие рекомендации данного отчета, поддерживая темпы и быстроту действий. При проведении этой работы перечисленные ведомства должны действовать в тесном контакте с другими государственными подразделениями, промышленностью и научными кругами. Стоит подумать также о создании на ограниченное время консультативной экспертной группы для поддержки этой работы.*

Технология

Технология распределенного реестра все еще находится на ранней стадии разработки. Разработка технологии блокчейн - это всего лишь первый, но очень важный шаг к революционному прорыву в технологии распределенного реестра, которая может изменить деятельность государственных и частных компаний. Технология может быть использована так, что «легальные» изменения в реестре могут быть сделаны, в принципе, кем угодно («неконтролируемый» реестр), или ограниченным числом пользователей, или даже единственным уполномоченным лицом (в «контролируемом» реестре). Для применения в сфере государственного управления «контролируемые» реестры выглядят более подходящими, чем неконтролируемая модель Биткойна, потому что они позволяют одному или нескольким владельцам данных определять, кому разрешено использовать систему, а кому нет. Распределенные реестры обладают дополнительным преимуществом, перенося сложность управления безопасностью на задний план, тем самым делая системы проще и дешевле в использовании.

Для реализации полного потенциала этой и связанных с ней технологий необходимо решить много проблем, включая проблемы конфиденциальности, безопасности, производительности и масштабируемости. Но также существует ряд возможностей для разработки алгоритмов, которые усовершенствуют реестры путем добавления поддержки "умных" контрактов (смарт-контрактов), цифровой подписи и других возможностей. Это повысит ценность и разнообразит способы использования реестров. Эта сфера деятельности быстро развивается и многие из указанных проблем уже исследованы, а в некоторых случаях, уже решены. Если правительство будет ждать появления "совершенных" решений, то оно упустит возможность сформировать и обеспечить различные внедрения технологии, которые принесут максимальную пользу государственному сектору, а также Великобритания может потерять возможности для получения экономической выгоды.

Наравне с обеспечением гарантий, что технология надежна и масштабируема, нам требуется понять этические и социальные последствия различных вариантов потенциального использования технологии, а также финансовые затраты и пользу от ее внедрения. Благодаря НИОКР, Великобритания находится в выгодном положении, однако мы не можем принимать это как должное, ввиду повышенного интереса и конкуренции в разработке технологии распределенного реестра по всему миру.

Научно-исследовательские советы, под руководством EPSRC (Engineering and Physical Sciences Research Council - Научно-исследовательский совет по инженерным и физическим наукам) и ESRC (Научно-исследовательский совет науки и инженерии), играют важную роль в поддержке исследований в университетах и недавно созданном Институте Алана Тьюринга. Также очень важная роль у бизнеса, которая заключается в инвестировании в НИОКР, использовании больших возможностей совместного государственного и частного инвестирования для решения типичных проблем, связанных с безопасностью, конфиденциальностью и разработкой стандартов - инвестировании во все области, где выигрыш в производстве будет получен скорее через сотрудничество, чем вследствие конкуренции.

Существующие инвестиционные проекты государства и частного сектора включают исследовательские центры Digital Catapult, Future Cities Catapult и Институт Открытых Данных. Вдобавок к ним, существуют структуры, такие как аналитический центр Уайтчепел (Whitechapel Think Tank), которые могут задавать точку фокуса для для дальнейшего обсуждения и обмена идеями. Это означает, что Великобритания находится в выгодном положении, благодаря которому она может выстроить фундаментальное исследование и тестирование технологии распределенного реестра. Но существует опасность, что мы не сможем получить максимальный результат вследствие потенциально разрозненной деятельности. Также существуют веские доводы, что научно-исследовательское сообщество в государственном и частном секторе должно "самоорганизоваться" таким образом, чтобы поощрять сотрудничество там, где это уместно, и конкуренцию там, где это будет стимулировать наиболее творческий подход к исследованиям.

Следующие две рекомендации направлены на поощрение дальнейшего исследования и создания в Великобритании возможности для проведения испытаний и экспериментов по решениям, с использованием распределенных реестров:

Рекомендация 2: *Британскому научному сообществу следует инвестировать в необходимые исследования, для проверки масштабируемости и защищенности распределенных реестров и получения доказательств корректности их содержания. Следует обеспечить высокую производительность операций и минимальное время отклика системы, соответствующие прикладной области, в которой внедряется данная технология. Также следует учесть необходимость эффективного использования энергии. Недавно созданный Институт Алана Тьюринга, во взаимодействии с такими структурами, как аналитический центр Уайтчепел, мог бы сыграть важную роль в координации и «самоорганизации» научно-исследовательских и опытно-конструкторских работ, проводимых в государственном и частном секторах, заинтересованных в работе с этой и связанным с нею технологиям. Частному сектору необходимо подумать об инвестировании в деятельность Института Алана Тьюринга с целью поддержки «доконкурентных» исследований, которые в конечном счете способствовали бы созданию новых надежных и защищенных коммерческих решений. Сюда входит как работа по таким очевидным направлениям, как криптография и кибербезопасность, так и расширение направления разработки новых типов алгоритма.*

Рекомендация 3: *Правительству рекомендуется поддержать создание пилотных распределенных реестров для муниципальных органов власти, объединяющих все элементы, которые необходимы для тестирования технологии и ее практической применимости. Пилотные проекты на уровне города могли бы предоставить ценные возможности для опробирования и внедрения технологий распределенного реестра. Британское агентство по инновациям Innovate UK могло бы использовать свое взаимодействие с городами в рамках проекта «специальных договоренностей с городами» (city deals) для реализации подобных пилотных проектов.*

Управление

Эффективное управление и регулирование - это ключ к успешному внедрению распределенных реестров. Управление включает в себя правила, установленные владельцами реестров и их партнерами, которые защищают их частные интересы. Они должны дополняться регламентами и/или законами, которые включают в себя рамочную систему правил, установленных внешними органами власти и направленных на защиту широкой общественности. Правительство издает законы и создает рамочные условия для регулирования, делая это единолично или в сотрудничестве с правительствами других стран. Также обычно создается, или привлекается со стороны, регулятор , подотчетный правительству и выполняющий эту работу.

В случае цифрового мира существует два набора правил или два кодекса, которые контролируют эксплуатацию цифровых технологий. Первый из них это классический набор правил законодательной системы, свод законов и нормативных актов. Второй кодекс - это набор правил, определяющих работу алгоритмов, закодированных в программном обеспечении. Это технический кодекс, и к строгому соблюдению технического кодекса требуется по крайней мере столько же внимания, сколько и к законодательному кодексу.

Успешное внедрение распределенных реестров потребует сочетания государственного управления, для защиты участников системы и заинтересованных сторон, и регулирования, чтобы гарантировать устойчивость системы к системным рискам или защищенность от использования в преступной деятельности. Трудность состоит в достижении баланса между защитой интересов участников системы и более широких интересов общества, избегая при этом нивелирования инноваций структурами с чрезмерно жесткой организацией.

Есть все возможности с выгодой использовать потенциальное взаимодействие между законодательным и техническим кодексами. Например, влияние государственных регуляторов может быть осуществлено через сочетание законодательного и технического кодексов, вместо

использования исключительно законодательного кодекса, как это происходит сейчас. В сущности, технический кодекс может быть использован для обеспечения соответствия законодательному кодексу и, тем самым, снизить затраты на достижение соответствия законодательно-нормативным требованиям. Для использования технологии в целях совершенствования регуляторной деятельности могут быть созданы "сценарии использования", так называемый РегТех, который сформировал ключевые рекомендации отчета ФинТех, опубликованного Управлением науки Правительства Великобритании1.

Установление оптимального баланса между управлением и регулированием, а также между законодательным и техническим кодексом, потребует необычного сочетания навыков и умений, включая необходимость совместной работы юристов, математиков и экспертов в компьютерных технологиях для решения многих ключевых вопросов, которые описаны в Главе 3.

Рекомендация 4: *Правительству требуется продумать как задействовать нормативно-правовую базу при использовании технологии распределенного реестра. Нормативно-правовому регулированию придется эволюционировать одновременно с развитием новых разработок и способов применения данной технологии. Как отдельную часть рассмотрения регулирования, правительство должно также рассмотреть вопрос о том, как возможно было бы достичь целей регулирования используя технический кодекс наряду с законодательным кодексом. Управление электронной экономики Министерства культуры, СМИ и спорта могло бы взять на себя выполнение этой рекомендации.*

Безопасность и конфиденциальность

Преступники давно отошли от вскрытия металлических сейфов и банковских хранилищ. Деньги сегодня существуют в их цифровом эквиваленте и они демонстрируют уязвимость для хакеров и взломщиков кодов цифрового мира. Криптографические коды в цифровом пространстве чрезвычайно сложно взломать. Однако как бы ни были они сложны для взлома, они могут содержать уязвимость для их обхода. Спектр механизмов обхода начинается с человека, который может выдать ключ случайно или намеренно, и заканчивается наличием "бэкдоров" из-за дефектов в программном коде. Сервера, на которых развернуты распределенные реестры могут иметь дополнительные уязвимости, поэтому равное внимание должно быть уделено устойчивости и безопасности аппаратных систем.

В случае с Биткойном, "кошельки", хранящие электронную валюту, имеют подтвержденную уязвимость для кражи - но сам по себе реестр остается устойчивым к внешним воздействиям. Хотя, в принципе, он был бы уязвим, если бы более 50% вычислительных мощностей, на которых расположен реестр Биткойна, оказались в руках одного злоумышленника или организации.

Несомненно, великая сила распределенных реестров заключается в их высокой устойчивости к взлому.

Однако значение имеет не только точность реестра. Важнейшими задачами также являются защита персональной информации и конфиденциальность. В зависимости от сферы применения реестра он может содержать личные конфиденциальные данные, начиная с финансовых данных и до информации о семье или состоянии здоровья. Еще одна возможность для использования технологии распределенных реестров, которая пока еще не реализована, это предоставление гораздо большей защищенности конфиденциальных данных, чем могут предоставить базы данных на текущий момент. Это еще одна область, в которой требуется провести много научно-исследовательской работы, и которая является частью развития технологии.

Правительство играет важную роль в обеспечении безопасности и конфиденциальности, поэтому наша пятая рекомендация состоит в следующем:

Рекомендация 5: *Правительству нужно работать вместе с учеными и представителями промышленности, чтобы обеспечить разработку стандартов по обеспечению целостности, безопасности и конфиденциальности распределенных реестров и их содержимого. Эти стандарты должны найти отражение и в нормативно-правовой области и в программном коде.*

Для каждого отдельного способа использования технологии пользователи государственного и, где это применимо, частного сектора должны провести предварительную оценку рисков, чтобы определить соответствующие угрозы. Центр защиты национальной инфраструктуры (CPNI - Centre for the Protection of National Infrastructure) и Группа Безопасности Коммуникаций и Электроники (CESG - Communications-Electronics Security Group) должны следить за развитием технологии распределенного реестра и играть роль главного эксперта по вопросам целостности, безопасности и конфиденциальности распределенных реестров, как внутри правительства, так и за его пределами. Как уже говорилось в рекомендации 2, недавно созданный Институт Алана Тьюринга, во взаимодействии с такими структурами, как аналитический центр Уайтчепел и Группа Безопасности Коммуникаций и Электроники (CESG), мог бы сыграть важную роль в координации и «самоорганизации» научно-исследовательских и опытно-конструкторских работ, проводимых в государственном и частном секторах.

Не следует игнорировать тот факт, что программное и аппаратное обеспечение со временем устаревает, в то время как появляются лучшие технологии, а злоумышленники учатся "новым трюкам". Таким образом для систем, которые планируется использовать в течение долгого времени, изначальный дизайн должен учитывать возможность безболезненного улучшения аппаратных и программных компонентов в течение срока службы системы. Вдобавок очень важно включать глубокое тестирование, как часть испытаний новых реализаций технологии, и делать это как на системном, так и на пользовательском уровне.

Доверие и совместимость

Как указано в главе 7, касающейся глобальных перспектив, доверие - это решение, касающееся рисков, между двумя или более людьми, организациями или государствами. В киберпространстве, доверие основано на двух требованиях: докажи мне, что ты тот, за кого себя выдаешь (аутентификация); и докажи мне, что у тебя есть необходимые полномочия, чтобы сделать то, о чем ты просишь (авторизация). В ответ я докажу, что я заслуживаю доверия, предоставляя тебе услуги или продукты безопасно, эффективно и надежно.

Аутентификация и идентификация взаимосвязаны, но это не одно и то же. Аутентификация не требует, чтобы я знал твою личность, но она требует, чтобы ты предоставил опознавательный знак (токен), который неразрывно связан с твоей личностью, например, пинкод от кредитной или дебетовой карты, отпечаток пальца, связанный с биометрическим паспортом или другим документом. В свою очередь, когда я предоставляю мой аутентификационный токен, то мне нужны гарантии, что я предоставляю его правильному человеку или организации, то есть гарантии того, что ты тот, за кого себя выдаешь. Таким образом так же важно, чтобы организации могли обеспечить своим пользователям аутентификацию, будь те физическими лицами, организациями или правительством.

В цифровом окружении есть возможность использовать и создавать более мощные и надежные инструменты для управления идентификацией, которые обеспечивают аутентификацию, в то же время защищая конфиденциальность. Одна из таких систем это инфраструктура открытых ключей (PKI - public key infrastructure), основанная на использовании крипографического стандарта X.509. Организации, использующие PKI, могут объединяться, чтобы предоставлять, разделять и потенциально упрощать безопасное предоставление услуг или продуктов. Другой важный международный стандарт разрабатывается для идентификации организаций. Он известен как Реестр Легальных Организаций (ROLO - Register of Legal Organisations) и может лечь в основу процесса аутентификации организаций, в отличие от аутентификации физических лиц.

Еще одним важным средством, позволяющим производить защищенное аутентифицированное взаимодействие между физическими лицами, является использование смартфонов, которые де факто являются доверенным устройством пользователя. Самые последние модели смартфонов содержат в себе важные средства обеспечения безопасности. Такие как криптопроцессор "Trusted Platform Module", безопасно хранящий цифровые сертификаты и криптографические ключи для аутентификации, шифрования и подписи, а также безопасную среду исполнения главного процессора "Trusted Execution Environment" (TEE)

и защищенный интерфейс пользователя "Trusted User Interface", каждое из которых обладает стойкостью к "вредоносному ПО" (malware).

Обсуждение аутентификации демонстрирует, что для максимального использования преимуществ распределенных реестров, они должны быть интероперабельными (совместимыми), способными взаимодействовать с другими реестрами. Однако максимизация возможности совместимости идет гораздо дальше совместимости аутентификации - это требует наличия соглашений о совместимости данных, совместимости политик и эффективного внедрения международных стандартов.

Рекомендация 6: Эта рекомендация связана с Рекомендацией 5. Правительству нужно работать вместе с учеными и представителями промышленности, чтобы убедиться, что наиболее эффективные и практичные протоколы идентификации и аутентификации используются как физическими, так и юридическими лицами. Эта работа должна быть неразрывно связана с развитием и внедрением международных стандартов.

Разрушительное будущее - некоторые потенциальные сценарии использования для правительства

Распределенные реестры потенциально могут быть совершенно разрушительными. Обработка операций ими производится в реальном времени, она практически полностью защищена от взлома и практически ничего не стоит. Они могут применяться в самых разных отраслях промышленности и услугах, таких как финансовые сервисы, операции с недвижимостью, здравоохранение и управление идентификацией. Они могут лежать и в основе других программных или аппаратных инноваций, таких как смарт-контракты или Интернет Вещей (система контроля промышленного оборудования или физических объектов через Интернет). Более того, лежащая в их основе философия распределенного согласования (или распределенного консенсуса), открытого исходного кода, прозрачности и наличия заинтересованного сообщества может быть чрезвычайно разрушительной для многих из указанных секторов экономики.

Как любое другое фундаментальное нововведение, распределенные реестры наряду с предоставлением новых возможностей создают угрозы для тех, кто им подвергся или не может таким угрозам противостоять. В особенности, в силу их природы согласованного распределения, они могут восприниматься как угрожающие занять роль доверенных посредников в контролирующих инстанциях с традиционной иерархической структурой, таких как банки или правительственные учреждения.

С таким большим количеством заинтересованных сторон, услуг и ролей, правительство выполняет великое множество различных действий. Некоторые из них скорее распространяют ценности, нежели создают их, а другие создают и поддерживают эффективные системы регулирования. Многие из этих видов деятельности будут усовершенствованы за счет инноваций, доступных благодаря распределенным реестрам, другие же окажутся под угрозой.

В конечном счете, лучший способ развивать технологию это использовать ее на практике. Экспертная группа, помогавшая готовить данный отчет, рассмотрела несколько конкретных примеров потенциального использования технологии правительством Великобритании, которые подробно описаны в Главе 6 в виде пяти практических примеров. Это:

- защита критически важной инфраструктуры от кибератак
- снижение операционных расходов и отслеживание прав на получение социальной поддержки с одновременным расширением объема финансовых услуг
- прозрачность учета и возможность отслеживания средств, выделяемых на помощь
- создание возможностей для экономического роста, развития мелкого и среднего предпринимательства и роста занятости
- сокращение налогового мошенничества

В каждом из этих случаев результатом исследования стали обзор использования распределенных реестров, их возможной полезности и оценка уровня зрелости технологии для эффективного использования.

В этом отчете была описана лишь малая часть всевозможных способов применения технологии, но мы уверены, что этого достаточно для начала работ по пилотному использованию технологии в работе подразделений правительства. Таким образом наши заключительные рекомендации нацелены на пробное внедрение технологии распределенного реестра и на развитие возможностей правительства в использовании этой технологии:

Рекомендация 7: Понимание истинных возможностей распределенных реестров требует не только исследования, но и применения технологии в реальной жизни. Правительство должно провести испытания распределенных реестров для оценки применимости технологии в государственном секторе.

Мы считаем, что эти испытания должны быть скоординированы таким же образом, как проводятся, документируются и оцениваются клинические испытания, чтобы обеспечить единообразие и максимальную точность выполнения процесса. Результаты этих испытаний и полученные знания должны быть отображены в поэтопном плане действий, создание которого предлагалось в Рекомендации 1.

Мы уверены, что в первую очередь работы должны быть проделаны в таких областях, как обеспечение защиты национальной инфраструктуры, снижение влияния рыночных колебаний на малые и средние предприятия, а также распределение фондов Министерства труда и пенсий Великобритании и других подразделений правительства. Во время подготовки данного отчета мы обнаружили не так много чиновников, которые уже серьезно думают о возможном использовании технологии распределенных реестров в работе правительства.

Мы рекомендуем оказывать этим людям большую поддержку и поощрять продолжение работы в этом направлении в сотрудничестве с министерствами и Службой Электронных Услуг (GDS).

Рекомендация 8: *Необходимо развивать способности и практические умения в правительстве, так же как иерархическое руководство и координацию. Мы рекомендуем учредить межправительственное сообщество, объединяющее аналитическое и политическое сообщества, для создания и разработки возможных "сценариев использования" и свода знаний и опыта для использования в государственной службе.*
Служба Электронных Услуг (GDS) и Партнерство в сфере наук о данных между GDS, Национальной статистической службой, Администрацией Кабинета министров и Управлением науки Правительства Великобритании могли бы действовать как координаторы этого сообщества. Правительства есть большие возможности для стимулирования бизнес-сектора, которые она может использовать, выступая в роли грамотного заказчика в процессе обеспечения использования распределенных реестров.

Заключение - принятие глобальной перспективы

Великобритания не одинока в осознании важности технологии распределенных реестров. Другие страны, маленькие и большие, также уже активно движутся в сторону принятия распределенных реестров - и практический пример Эстонии показывает как быстро может достигать прогресса маленькая страна с эффективным и осведомленным в цифровых технологиях руководством. Однако у Великобритании все еще есть время, чтобы позиционировать себя внутри этой лидирующей группы - конечно, это необходимо сделать, принимая во внимание важную роль финансового сектора и сектора услуг в экономике Великобритании.

Патрик Карри, Кристофер Сир и Майк Халсалл в Главе 7 рассмотрели отличительные особенности электронно-продвинутых наций, и утверждают, что ключевыми являются следующие характеристики:

- Высшее руководство, осведомленное о возможностях цифровых технологий.
- Обладающий полномочиями департамент правительства, , отвечающий в целом за переход страны на электронные технологии, который ориентирован на международное сотрудничество и тесно взаимодействует со всеми секторами экономики.
- «Живой», ориентированный на сотрудничество национальный план, выполняемый отраслями при поддержке государственных инвестиций.
- Наличие в каждом государственном органе и учреждении технически грамотных, квалифицированных и опытных руководителей высшего звена, отвечающих за разработку политик.
- • Активное участие инженеров и лидеров электронного бизнеса в выработке политики.

Мы все еще находимся на ранних стадиях необыкновенной постиндустриальной революции, движущей силой которой являются информационные технологии. Это революция, сулящая новые важные преимущества и риски. Уже понятно, что появление технологии распределенных реестров в рамках этой революции начинает разрушать многие из существующих способов ведения бизнеса.

Самые ранние записи расчетов между людьми появились в Вавилоне, Ассирии и Шумере около 5000 лет назад. Многие глиняные таблички уцелели, и представляют свидетельства о ранних технологических революциях в развитии письменности, счета и денег. Непонятно, будут ли цифровые записи такими же долговечными как глиняные таблички. Но, оставив эти размышления в стороне, совершенно ясно, что у Великобритании есть огромная возможность развить и использовать технологию распределенного реестра на благо граждан и экономики. Целые серии "великих вызовов" предстоит принять, чтобы максимизировать преимущества и минимизировать ущерб от выдающегося развития информационных технологий. Этот отчет описывает некоторые главные рекомендации для правительства, основанные на мнениях экспертов. Самая главная из них - это то, что требуется тесное сотрудничество между государственным и частным сектором, внутри Великобритании и между Великобританией и другими государствами.

Определения

Терминология этой новой области все еще развивается, и термины блокчейн, распределенный реестр и общий реестр часто трактуются по-разному. Формальные определения безусловно не будут соответствовать видению всех сторон, однако для целей данного отчета я хотел бы привести определения для следующих ключевых терминов:

- **Блокчейн** (block chain, букв. цепочка блоков) представляет собой тип базы данных, в которой записи группируются в блоки (очень похоже на то, как если бы несколько записей переписали на один лист бумаги). Каждый блок затем "связывается" со следующим блоком с использованием криптографической подписи. Благодаря этому блокчейн можно использовать как **реестр**, доступ к которому может быть представлен любому лицу с соответствующими полномочиями и может подтверждаться таким лицом.
  Существует много способов подтверждения точности реестра, и в целом они известны как **метод консенсуса** (для обозначения этого процесса для криптовалюты биткойн используется термин «майнинг» (mining – добыча)) -- см. ниже.
  Если участники этого процесса предварительно отбираются, то такой реестр является **контролируемым** . Если процесс открыт для всех, то реестр **неконтролируемый - см. ниже**.
  Реальная новизна технологии блокчейн состоит в том, что это больше, чем просто база данных - здесь есть возможность устанавливать правила транзакций (бизнес-логику), которые привязаны к самой транзакции. Это отличает данную технологию от традиционных баз данных, в которых правила часто устанавливаются на уровне всей базы данных или в программном приложении, но не на уровне отдельной транзакции.

- **Неконтролируемые реестры**, например, Биткойн, не имеют единственного владельца -- фактически, отсутствует возможность владения такими реестрами. Цель использования неконтролируемого реестра -- позволить любому лицу вносить данные в реестр и предоставлять возможность для любых лиц, в распоряжении которых находится реестр, получать его идентичные копии. Это предотвращает любые попытки контроля над содержанием и означает, что ни одни из игроков не имеет возможности препятствовать добавлению транзакции в реестр. Участники обеспечивают точность данных в реестре посредством достижения консенсуса в отношении его состояния.
  Неконтролируемые реестры могут использоваться для создания глобальной записи без возможности редактирования: например, для составления завещания или передачи прав владения объектом имущества. Однако использование реестров бросает вызов гегемонии институтов власти и существующих индустрий, в результате чего есть вероятность принятия политических решений против их использования.

- **Контролируемые реестры** могут иметь одного или нескольких владельцев. При добавлении новой записи целостность реестра проверяется при помощи ограниченного процесса достижения консенсуса.
  Такие действия выполняются доверенными участниками - например, государственными органами или банками - что существенно упрощает поддержку совместной записи в сравнении с процессом получения консенсуса, используемого для неконтролируемых реестров.
  Контролируемые блокчейны предоставляют данные, которые легко верифицировать, так как процесс получения консенсуса позволяет создавать цифровую подпись, которую могут проверить все стороны. Необходимость валидации записей несколькими государственными органами обеспечивает большую уверенность в ее безопасности, например, в отличие от текущей ситуации, когда департаменты зачастую обмениваются данными на бумажных носителях. Операции с использованием контролируемого реестра обычно выполняются быстрее, чем при использовании неконтролируемого.

- **Распределенные реестры** представляют собой тип базы данных, как правило, публичной, распределенной по многочисленным сайтам, странам или учреждениям. Записи хранятся одна за другой в непрерывной реестровой последовательности, а не группируются в блоки,

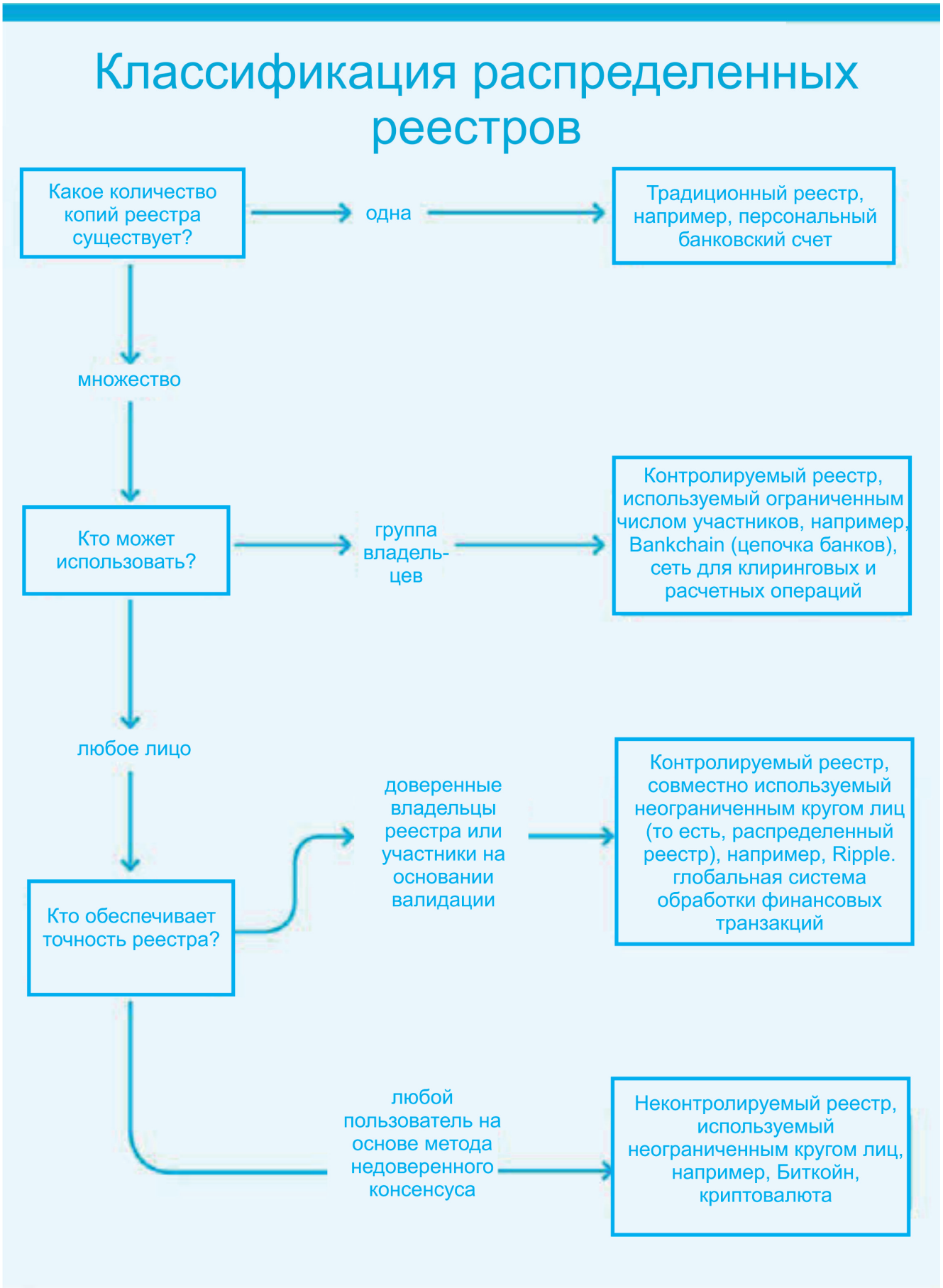
но добавлены они могут быть только тогда, когда собран кворум участников.

Использование распределенного реестра требует большего доверия к валидаторам или операторам реестра. Например, глобальная система финансовых операций Ripple выбирает группу валидаторов (известную как Unique Node Validators) из порядка 200 известных, неизвестных или частично известных валидаторов, про которых известно, что они не вступают в преступные сговоры с целью обмануть участников сделки. Этот процесс обеспечивает электронное подписание, которое считается менее устойчивым к контролю, чем схема биткойн, но работает значительно быстрее.

- **Общий реестр** - термин, который ввел Ричард Браун, Директор по технологиям компании Distributd Ledger Group, ранее занимавший такую же должность в IBM. Данный термин обычно обозначает любую базу данных или приложение, которое совместно используется отраслевыми участниками и частными консорциумами, либо находится в открытом доступе для широкой общественности. Данный термин является самым общим и популярным термином для данной группы технологий.

В общем реестре может использоваться распределенный реестр или блокчейн в качестве его основной базы данных, однако он зачастую настраивается для предоставления доступа для различных типов пользователей. Как таковой, "общий реестр" представляет собой широкий круг возможных архитектур реестров или баз данных, которые контролируется на каком-либо определенном уровне. При работе с общим реестром может привлекаться ограниченное количество валидаторов, которым доверяется ведение реестра, что предоставляет определенные существенные преимущества.

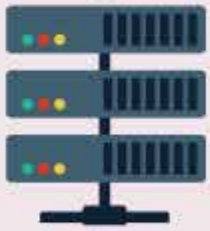
- **Смарт-контракты** представляют собой контракты, условия которых записаны на компьютерном, а не на юридическом языке. Смарт-контракты могут автоматически выполняться вычислительной системой, такой, как подходящая система распределенных реестров. Потенциальные выгоды от смарт-контрактов включают низкие затраты на процессы заключения и исполнения контрактов, а также на исполнение законодательно-нормативных требований; как следствие, становится экономически выгодным формировать контракты для многочисленных сделок на небольшие суммы. В число потенциальных рисков входит зависимость от вычислительной системы, которая исполняет контракт. На данной момент, эти риски и выгоды в основном теоретические, так как технология смарт-контрактов все еще находится в зачаточном состоянии, и ее широкомасштабное развертывание в кратковременной перспективе не ожидается.



Иллюстрации предоставлены Дейвом Бирчем (Consult Hyperion)

ГЛАВА 1

Видение



Цифровые валюты, включая Биткойн, основываются на технологическом решении, получившем название блокчейн (цепочка блоков). Данная система обеспечивает отражение всех транзакций в идентичных копиях цифрового реестра, совместно используемых пользователями. Метод "общего реестра" позволяет оптимизировать бизнес-процессы при предоставлении самых разных услуг, включая услуги госорганов и компаний.

Автор
Саймон Тейлор
Вице-президент по исследованиям блокчейн, Barclays

Глава 1: Видение

Введение

Цифровые валюты, такие как Биткойн, обеспечивают новые возможности по отслеживанию финансовых транзакций. Базисная технология -- известная под названием блокчейн -- обеспечивает отражение всех транзакций в идентичных копиях цифрового реестра, совместно используемых пользователями.

Сегодня финансовые институты, регуляторы, центробанки и правительства исследуют возможности по использованию данного подхода "общего реестра" для оптимизации бизнес-процессов при предоставлении самых разных услуг, включая услуги госорганов и компаний.

Многие из возможностей применения могут быть реализованы в среднесрочной перспективе, однако длительные циклы разработки для правительств и частного сектора, а также уже сейчас обнаруживающийся потенциал по существенному повышению эффективности, предполагают, что министры и государственные служащие должны уже сейчас начать рассматривать возможности получения преимуществ от их использования. В данной главе приводится общая информация о таких возможностях.

Что из себя представляет общий реестр?

Общий реестр -- это фактически база данных, в которой содержится актуальная информация о правах владения на финансовые, физические или электронные активы -- например, алмазы, суммы в валюте или грузы. Особенную важность представляет тот факт, что любой из участников может сохранять копию блокчейна, которая обновляется в автоматическом режиме при каждой новой транзакции. Безопасность и точность данных обеспечиваются с использованием математических методов -- в частности, с использованием криптографии -- для того гарантии, что все копии реестра соответствуют друг другу. Почти все данные, хранящиеся сегодня на бумажных носителях, могут храниться и в общем реестре (см. Главу 2 для получения более детальной информации в отношении технологии общего реестра).

В основе биткойн с момента запуска в 2008 году, лежит технология блокчейн. Существует большое количество заблуждений и стереотипов в отношении цифровой валюты и принципов ее использования. Ассоциирование системы Биткойн с интернет-порталом цифрового черного рынка Silk Road, оставляют у некоторых людей впечатление, что Биткойн действительно связан с отмыванием денег и террористами. Это заблуждение продолжает оказывать влияние на то, как люди воспринимают технологию блокчейн.

Фактически, общие реестры и базы данных могут предоставлять определенные существенные преимущества для государственных и финансовых институтов благодаря четырем важных характеристикам технологии блокчейн.

1) **Сверка данных с использованием методов криптографии.** Различные институты, такие как компании или госорганы, сегодня высылают друг другу сообщения для передачи детальных сведений о транзакциях. После получения соответствующего сообщения каждое учреждение обновляет свой собственный реестр. Однако сегодня не существует быстрого и эффективного способа для того, чтобы обеспечить соответствие таких копий. Технология блокчейн позволяет решить эту проблему при помощи различных методов: например, просто при обмене одними и теми же базовыми данными или при предоставлении "подтверждающих элементов" с целью верификации данных. Данный подход может также применяться и в отношении наборов данных, используемых правительствами. Различные участники (пользователи) реестра достигают консенсуса в отношении статуса базисных данных с использованием различных алгоритмов консенсуса (например, Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance).

2) **Распространение копий среди многочисленных получателей.** Копия всех или отдельной части данных

может направляться многочисленным сторонам, что снижает вероятность возникновения критической ошибки на единственном участке. Мультиплицирование сегодня составляет достаточно большую проблемы для существующих технологий организации баз данных, что приводит к появлению дополнительных затрат и сложностей при реализации IT проектов в частном и государственном секторах. Дополнительным преимуществом использования данной технологии является то, что в случае сбоев в одной из копий, остальные остаются целыми. Многочисленные стороны могут также подтверждать факты добавления определенных записей в ходе сверки собственными силами.

3) **Детализированный контроль доступа.** В распределенных реестрах используются "ключи" и подписи для того, что предоставлять определенным лицам права на выполнение определенных действий в общем реестре. Такие ключи могут получать определенные возможности, доступные только при соблюдении некоторых условий. Например, регулятор может иметь "ключ для просмотра", позволяющий ему просматривать все транзакции соответствующего учреждения, однако только в том случае, когда ключ, находящийся во владении суда, предоставляет регулятору разрешение (контроль) для осуществления таких действий.

4) **Детализированная прозрачность и конфиденциальность .** В связи с тем, что многочисленные стороны получают копию реестра (пункт 1) и многочисленные стороны могут выполнять верификацию каждой записи (пункт 2), общий реестр обеспечивает высокий уровень прозрачности. Это позволяет регулятору или независимому органу, например, судебному, убедиться, что содержание базы данных не редактировалось или изменялось мошенническим путем. При наступлении соответствующих условий, это также позволит им разблокировать записи, которые в противном случае остались бы полностью частными и недоступными для просмотра. Это может оказаться полезным для бизнеса (например, банков) при подготовке отчетности для регулятора, противодействии мошенничеству, и может наделять граждан полномочиями, необходимыми для эффективного контроля за деятельностью госорганов (см. Главу 5, в которой приводится более детальное описание). Добавление записей осуществляется с использованием уникальной криптографической подписи, подтверждающей тот факт, что соответствующий участник добавил запись в соответствии с применимыми правилами.

Совместно эти характеристики позволяют решать проблемы, которые ранее были слишком дороги для решения или сложны.

Что представляет собой смарт-контракт?

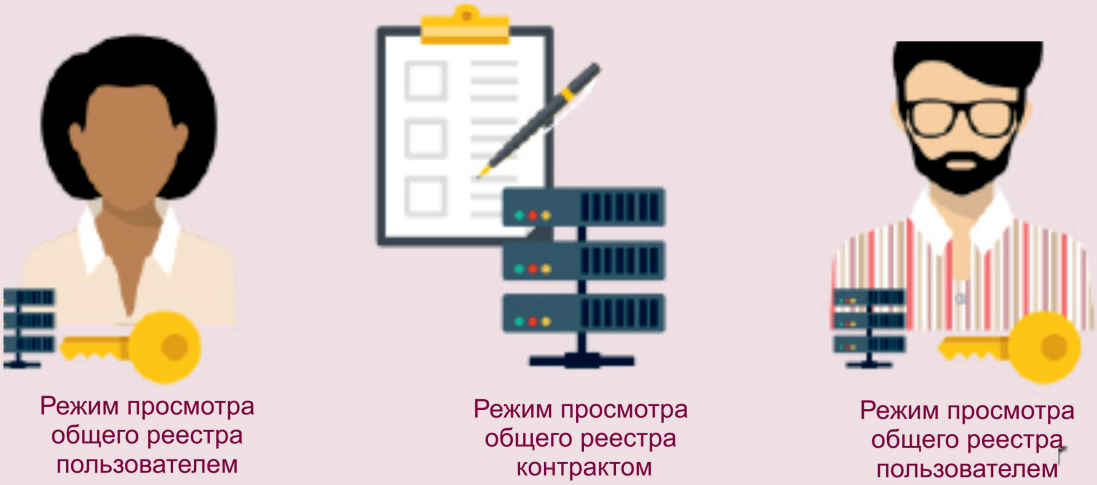
Технология блокчейн представляет собой по сути базу данных, а смарт-контракт - уровень применения данного решения, позволяющий реализовать потенциал данного решения. Большинство обычных договоров не имеют каких-либо прямых связей с компьютерным кодом, который бы создавал их (см. Главу 3). Во многих случаях подготовленный в бумажном формате договор архивируется и программное обеспечение используется для цифрового отражения его в компьютерном коде (см. Рис. 1).

Рисунок 1

Большинство обычных договоров не имеют каких-либо прямых связей с компьютерным кодом, который бы создавал их (см. Главу 3).

Рисунок 2

Смарт-контракты содержат компьютерный код, используемый для реализации контракта.



Данный подход обеспечивает высокую эффективность при получении подписки на услуг (например, видео по запросу), однако он представляет существенные сложности при предоставлении многочисленных сложных пакетов услуг для одного пользователя (например, обновление адреса в многочисленных базах данных государственного учреждения). Это привело к созданию еще более сложной системы защиты информации и регламентов по защите личной тайны для эффективного обеспечения конфиденциальности и защиты тайны личной жизни физических лиц. Кроме того, такие действия, как обмен данными или согласование условий договоров, все еще выполняются с использованием бумажных носителей вместо автоматизации в рамках всей экономики.

Сочетание ключевых свойств общего реестра (синхронизация через криптографию, воспроизведение для нескольких получателей, детализированный контроль доступа,

Рисунок 3

Смарт-контракты позволяют контролировать то, какие учреждения имеют доступ к закрытой информации

и прозрачности на высоком уровне гранулированности и защиты тайны личной жизни) совместно с использованием смарт-контрактов помогают преодолеть эти сложности, позволяя репликацию и обмен данными при определенных условиях. В случае, когда два пользователя подписывают смарт-контракт, такой договор устанавливает логику, применяемую в отношении всех частей общего реестра (см. Рис. 2). Это может стимулировать автоматизацию или ликвидацию ручных процессов в частном и государственном секторах, что позволит повысить производительность и темпы роста. Следует обратить внимание, что имеются и другие проблемы, например, управление устаревшими версиями баз данных и процессов, однако «доступ» в рамках многочисленных систем – это как раз та область, где смарт-контракты выходят на первый план.

В качестве альтернативного сценария (Рисунок 3), Пользователь 1 соглашается выступать в качестве одной из сторон смарт-контракта, созданного в рамках общего реестра, для того, чтобы направить свой адрес учреждению, имеющему "голубую копию" (может существовать большое количество других учреждений, обладающих большим количеством различных копий). Однако Пользователь 2 отказался от передачи своего адреса, поэтому учреждение может получить копию самого последнего адреса только от Пользователя 1. Данная функция может оказаться полезной в случае, когда физическое лицо изменяет свой адрес через местные службы, так как изменение может отражаться в паспорте, водительских правах и прочих ключевых базах данных департамента. Различные сервисы, например, Onename.io, используют сегодня данную концепцию при управлении социальными сетями и область ее применения можно расширить на все учреждения.

Смарт-контракты рассматриваются для разных видов использования, в частности, для соблюдения законодательных требований, возможности контроля товаров и менеджмента услуг, а также для борьбы с контрафактной продукцией и мошенническими действиями в следующих секторах:

- Продукты питания
- Финансовые Услуги
- Энергетика
- Фармацевтика
- Здравоохранение
- Аэрокосмическая область
- Авиация
- Телекоммуникации
- ИТ и коммуникации
- Транспорт
- Инфраструктура
- Сельское хозяйство
- Нефть и газ

Некоторые из этих пунктов будут рассмотрены далее в этой главе и в Главах 6 и 7.

Таким образом, смарт-контракт удобен, когда технологии, организации или люди хотят создать цифровое соглашение с криптографическим подтверждением того, что данное соглашение отражено в реестрах, базах данных и аккаунтах всех сторон соглашения.

Видение будущего

Ключевая задача демократического правительства - оптимальное распределение ресурсов среди населения: физических и юридических лиц. Это касается не только денежных ресурсов, но и социальных нематериальных активов: безопасности, демократии, условий соблюдения законности; и экономической ситуации: поддержки свободного рынка, сохранения низкой и стабильной инфляции, защиты прав частной собственности и обеспечения договоров. Основа такой системы распределения - соглашение между населением и правительством о том, каким образом устанавливаются правила (посредством голосования и манифестов).

С распространением такой демократической модели, функционирование госаппарата (т.е. механизма, которым производится распределение ресурсов) стало шире, централизованнее и, дальше от физических лиц.

Накопление (денежных) ресурсов посредством установления различного рода налогов - огромный и затратный механизм из-за распределения на социальное обеспечение, гранты и пособия. Такая сложность может частично проистекать из централизованного характера системы.

Частный сектор начал осознавать, что такая централизованная модель дает низкий уровень обслуживания потребителей, более не является экономически выгодной и не в состоянии принимать во внимание все выгоды электронной коммерции и цифровых возможностей. Правительства начинают осознавать, что надежды населения должны быть оправданы аналогичным образом: с индивидуальными цифровыми услугами в реальном времени, применимыми ко всем государственным службам. Использование общих реестров и смарт-контрактов дает возможность поставить правительство во главе этого направления, гарантируя, что преимуществами технологий могут пользоваться те, кому они действительно нужны, а не те, кто может их себе позволить.

Эта тенденция также проявилась в свете роста менее-формальной "экономики совместного потребления", а также в феноменах, управляемых социальными сетями: таких как Арабская весна и движение "Захвати". Все это демонстрирует изменения в способах общения и самоорганизации общества. В настоящее время, тем не менее, не появилось безопасного способа применения этих идей, в условиях стимулирования свободного рынка и договоров поручительства. Существует мнение, что причина, почему мы так и не продвинули онлайн-демократию, в том, что без дорогостоящей и не-либертарианской централизованной системы идентификации невозможно быть уверенным в том, кто голосует за что. При условии, что такой исход неприемлем, возможности технологии блокчейн (криптографическая синхронизация, дублирование для различных учреждений, детализированный контроль доступа, и детализированная прозрачность и конфиденциальность) могут оказаться эффективными для населения.

Кроме того, раннее участие правительства в развитии и внедрении технологии блокчейн предоставляет возможность уменьшить сложность и высокую стоимость управления. Это приведет к более персонализированной, оперативной и потенциально более демократичной основе правительства, и, как результат, повышению степени соблюдения законодательных требований, экономической эффективности и надежности.

Шаги, направленные на внедрение технологии блокчейн

Технология общего реестра активно продвигается и развивается в главных мировых экономиках: Соединенных Штатах, Китае, Сингапуре и Латинской Америке. Великобритания имеет возможность составить конкуренцию в этой гонке, понимая и поддерживая рост этой зародившейся отрасли.

Возможное участие правительства в развитие технологий распределенного реестра просматривается через три аспекта:

- Правительство: государственная служба
- Правительство: законодательные органы
- Правительство: управляющие экономикой

Правительство: государственная служба

Органы государственной службы имеют ряд ключевых обязанностей, на которые может оказать влияние эта технология, в таком случае, сценарии применения направлены на связь конфиденциальности, переносимости данных и возможностей сенсорной системы мобильных технологий (см. Главу 6 для более подробного разбора практических примеров).

Правительство: законодательные органы

Технология распределенного реестра еще молода и, вероятно, пройдет еще через несколько циклов развития. В связи с этим, действия правительства могут быть сосредоточены на трех обособленных "направлениях" развития технологии.

Направление 1: Поддержка появившейся Экосистемы:

В экосистеме Биткойн и других системах общего реестра уже существует ряд сервисов по обмену электронных денег, обслуживанию "кошельков" и т.д. Учитывая, что технологии и бизнес будут продолжать развиваться, Направление 1 может включать в себя следующее:

- Требование от обменных сервисов удостоверять личность своих клиентов (правило, известное как "Знай Своего Клиента" (KYC).
- Выпустить руководство для банковского сектора, чтобы продемонстрировать различие между компаниями по следующим критериям: i) компании, которые переводят валюту по системе блокчейн; (ii) компании, которые предоставляют программное обеспечение предприятиям, которые используют блокчейн; (iii) компании, которые предоставляют программное обеспечение на базе системы блокчейн для решения задач традиционного бизнеса.
- Установить стандарты защиты для сервисов по обслуживанию кошельков.
- Поставить задачи перед научным сообществом и старт-ап экосистемой, чтобы проработать существующие недостатки в экосистеме блокчейн: (i) Создать надлежащую техническую архитектуру; (ii) определить, как технологии могут увеличить свою эффективность для усовершенствования процесса верификации личности пользователя, проведения борьбы с легализацией незаконных доходов и предотвращения преступлений; (iii) определить, как использование мульти-подписей для кошельков может создать новый опыт взаимодействия правительство-население и предоставить населению возможность контролировать и анализировать свои данные, которых хранит правительство.
- Привлечь партнеров для поддержания скоординированного разговора между правительством и промышленностью.

Направление 2: Предварительные испытания и Пилотные проекты

Как правило, в тех сферах, где правительство имеет определенные возможности, оно может начать осуществлять локальные испытания сценариев применения. Отдельные вопросы, которые могут интересовать правительство:

- Какие ключевые инфраструктуры получат выгоды от использования технологий общего реестра/базы данных?
- Где можно реализовать пробный период программы (к примеру, при проведении пенсионной реформы, реформы системы социального обеспечения)?
- Где пробный период программы может предоставить лучшую возможность для изучения?

Направление 3: Великобритания как лидер во Всемирной Гонке

Большая часть венчурных инвестиций в технологии распределенного реестра, в настоящее время направлена на систему Биткойн и западное побережье Соединенных Штатов. Но новые возможности для таких технологий лежат в других областях применения.

- Великобритания должна осознать этот фактор и, в этих целях, - установить руководство к действию для своих контролирующих органов (см. Главу 3 об управлении и регулировании).
- Великобритания может создать научно-инновационный центр для этих технологий и и добавить его в программу ФинТех /программу развития торговли и инвестиций Великобритании

Правительство: управляющие экономикой

Чтобы понять, каким образом правительство может максимально эффективно продвигать и реализовывать преимущества этой технологии, будет полезно рассмотреть сценарии применения в двух различных сферах: финансовые услуги; страхование и другие отрасли.

Финансовые услуги

Примеры, где может быть применена технология в сфере финансов:

- Повышение эффективности на рынке капиталов
- Снижение уровня мошенничества и повышение эффективности в сфере финансовых операций

1. Повышение эффективности на рынке капиталов

Рынок капиталов все еще полагается на бумажные записи при согласовании сделок между контрагентами. Несмотря на то, что основная инфраструктура уже создана, возможность сверить ("прояснить") транзакцию и иметь уверенность, что вторая сторона согласна, - имеет решающее значение, потому что в настоящее время этот процесс требует надежности. Большинство штрафов и большинство фиксированных комиссий банковских операций основаны как раз на концепции доверия. В сущности, один банк должен полагается на процедуры другого банка без контроля над его операциями. Здесь может оказаться полезной технология блокчейн, которая покажет всю цепочку транзакций (криптографически синхронизированных) и действующих лиц, вовлеченных в процесс, в понятном для регулятора виде. Кроме того, к, проверка таких данных, затратна и происходит после осуществления сделки. Крупные банки сейчас пытаются найти соответствующие механизмы для работы с этой технологией и эффективного использования ее преимуществ.

2. Снижение уровня мошенничества и повышение эффективности в сфере финансовых операций

Финансовые операции все еще осуществляются, практически таким же образом, как и на протяжении тычячелетий. В процесс продажи или покупки отдельного товара часто вовлечены не менее 5 или 6 сторон (к примеру, покупатель, банк покупателя, транспортная компания,

курьер, продавец, банк продавца). Уже предпринимались попытки стандартизировать и создать централизованную инфраструктуру в сфере финансовых операций. Общие реестры предлагают уникальные преимущества.

- "Частично контролируемая система" может предоставить возможность безопасного подписания бумажных документов (например, накладных, устанавливающих, какие товары были в контейнере, сколько, какого цвета и т.д.). Эти документы могут быть подписаны каждой стороной (в цифровой форме и доказуемо). (Ключевые характеристики: **Высокий уровень прозрачности; Сверка данных с использованием методов криптографии**)
- Вместо простого хранения документов, как это происходит сегодня, система общего реестра регистрировать изменения состояний этих документов. Более широкое применение позволит выдавать документы посредством общего реестра, вместо того, чтобы печатать и подписывать. (Ключевые характеристики: **Высокий уровень масштабируемости и воспроизводимости**)

Промышленность и государственные институты

1. Контроль активов и активов и подтверждение происхождения

Многие товары, такие как предметы искусства или электробытовая техника снабжены цифровыми метками. Однако, не существует глобального сервиса, для отслеживания и обнаружения этих товаров, который давал бы контроль прав доступа и определял, кто может следить за управлением этими активами. Многие организации доверяют бумажной документации при подтверждения происхождения продукции. Однако, невозможно подтвердить происхождение, если документация поддельная. Если бы стороны такой цепочки поставок использовали общий реестр и "подписывали" реестр в цифровом виде, для всех сторон было бы очевидно, что документы не были изменены или каким-то образом подделаны.

Например, Provenance.org - стратр-ап, через технологию блокчейн дает ритейлерам уверенность в происхождении и экологичности предметов одежды. В настоящее время, ритейлеры полагаются на бумажную документацию, чтобы подтвердить происхождение предметов одежды, однако невозможно быть уверенным, что эти документы были заполнены правильным человеком в правильное время. С помощью технологии блокчейн, соответствующий человек может подписать контракт методом электронной подписи с помощью своего приватного ключа, таким образом давая намного большую степень уверенности в том, что документ подписан правильным человеком в установленные день и время. Природа технологии блокчейн такова, что эта информация будет видна для всех ритейлеров, обладающих соответствующими правами.

2. Пользовательское управление для Конфиденциального Использования Данных

Точность данных и конфиденциальный совместный доступ к данным - ключевые задачи учреждений. Страховые компании могли бы создать более точные продукты, установить точные цены и премии, если бы обладали дополнительными данными, подтвержденными одним или несколькими надежными источниками (например, правительством или банками). Трудность состоит в том, чтобы сделать это безопасным образом и быть уверенным, что контроль личных данных остается у населения.

Технология блокчейн будет предоставлять подтверждение того, как получен каждый элемент данных, используя какую-то технологию, возможно, Guardtime. При использовании доверенной среды исполнения (TEEs) в мобильных телефонах, к примеру, чипов ARM's TrustZone, любые запросы на доступ к данным, которые хранятся в правительстве, будут зафиксированы в блокчейне. Если гражданин не давал разрешения страховой компании, данные не будут перемещены. В случае совершения любых попыток изменения или доступа к данным, гражданин или компетентные органы немедленно будут осведомлены.

Технология общего реестра в сочетании с удобным мобильным пользовательским интерфейсом, в состоянии отодвинуть в сторону сложности процесса управления безопасностью. Учреждения, которые примут решение применять такой способ, должны будут завоевать доверие пользователей, и предварительные испытания и внедрения будут полезны в достижении этой цели.

3. Промышленное Оборудование (связанное с "Интернетом Вещей")

Довольно сложно собрать точные данные в режиме реального времени о промышленном оборудовании по различным отраслям, в том числе транспортной, сфере коммунальных услуг, сельскому хозяйству. С появлением Интернета Вещей (Internet of Things, IoT) некоторые из сложностей были преодолены с помощью недорогого стандартного оборудования, которое, однако, уязвимо в случае атаки. Согласно недавнему отчету [2] института Коммерческих Ценностей IBM:

> "В результате: распространение сотен миллиардов устройств, которые будут стоить не дороже аналогов, и будут в состоянии функционировать как часть комплексной, интегрированной системы."
>
> "В сети масштаба Интернета Вещей, возможность доверия очень сложно спроектировать и очень дорого, если не невозможно, - гарантировать. Тем не менее, для масштабного внедрения постоянно расширяющегося Интернета Вещей, концепция конфиденциальности и анонимности должна быть интегрирована с интерфейсом, тем самым, предоставляя пользователям управление своей информацией. Современные модели обеспечения безопасности, основанные на методах закрытых источников (часто характеризуемых как "безопасность через неизвестность") устарели и должны быть заменены новым методом - "безопасность через прозрачность".
>
> "В нашей концепции децентрализованного Интернета Вещей, блокчейн - конструкция, облегчающая обработку транзакций и согласование взаимодействующих устройств. Каждый управляет своими функциями и действиями, что приводит к возникновению "Интернета Децентрализованных, Автономных Вещей" - и, соответственно, к демократизации цифрового мира"

Если каждое устройство одновременно функционирует как автономный участник и как часть целого, не может быть центральной точки отказа. При таком сценарии, учреждения будут применять устройства Интернета Вещей и получат множество преимуществ, связанных с цифровыми данными в реальном времени и взаимосвязанностью, которые были описаны в недавнем докладе Департамента по науке Правительства об Интернете Вещей3. Общий реестр и технология блокчейн обеспечивают новым технологическим и бизнес-моделям реализацию Интернета Вещей с высокой степенью безопасности.

Пример 1: Трактор, функционирующий как автономная единица, может давать доступ нескольким фермерам одного региона, предоставляя возможность оплаты мере пользования. Это дает возможность узнавать и платить в соответствии с погодными условиями, а также общаться с его производителем для технического обслуживания и ремонта.

Пример 2: Промышленное оборудование может получать возможность заказывать новые компоненты, в том случае, если есть уверенность, что это устройство подлинное и обладает соответствующими полномочиями. Это также может привести к появлению новых способов финансирования такого оборудования и рыночных ниш, основанных на эксплуатационных характеристиках и эффективности оборудования.

Заключение

Можно представить себе будущее, в котором эта технология создает форму "прозрачного правительства", более понятного для населения. Имеющееся количество вариантов использования, по мере развития технологии, конечно будет увеличиваться. Это также поможет достичь целей программы. Ключевые моменты для министров и государственной службы:

Технология находится на ранней стадии, но демонстрирует значительные перспективы. Чтобы раскрыть перспективы технологии блокчейн, очень важно понять, как следующие комбинации:

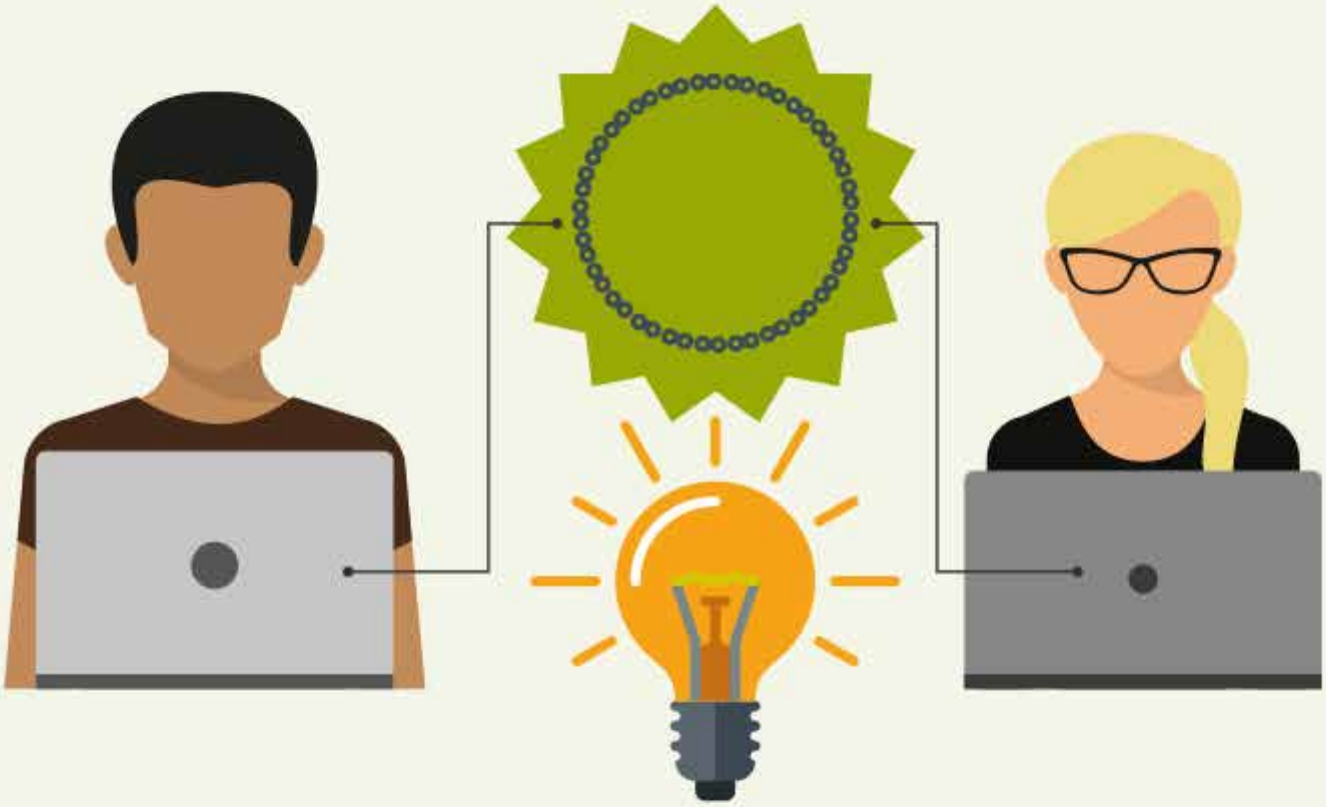
- Сверка данных с использованием методов криптографии
- Широкомасштабная, безопасная передача данных
- Подтверждаемая прозрачность

могут быть использованы с рамках трех направлений:

- Содействие появившейся экосистеме
- Предварительные испытания и пилотные проекты
- Позиция Великобритании в качестве мирового лидера

ГЛАВА 2

Технология



Наличные деньги отличаются от всех остальных форм денежных средств. Они могут передаваться между двумя людьми без вовлечения или разрешения третьих сторон, таких как банки или правительство. Биткойн и его блокчейн показали нам, как сделать то же самое в электронном виде. Однако сущность и возможности такой цифровой технологии намного шире.

Автор
Ричард Г. Браун
Технический директор, R3

Глава 2: Технология

Введение

Биткойн - это новая форма **цифровой валюты.** Вместо центральных банков, таких как Центральный Банк Великобритании, ее выпуск контролируется **децентрализованной** компьютерной сетью. Эта сеть основана на криптографических и других методах, которые позволяют регулировать запасы биткойнов и отслеживать их владельцев. Поэтому Биткойн также известен как **криптовалюта**.

Банки отслеживают балансы пользователей при помощи реестра. Биткойн тоже использует реестр, однако он эксплуатируется совместно децентрализованной сетью компьютеров, и называется **распределенным реестром**.

Когда новые группы данных добавляются в распределенный реестр, они включают в себя ссылки на предыдущие данные, таким образом все участники могут самостоятельно удостовериться в происхождении всех данных в реестре. Группы называются **блоками**, а вся совокупность - **блокчейн (цепочка блоков).**

В этой главе будет дано разъяснение этих принципов, почему они важны и каким образом они могут формировать основу для более широкого спектра применений.

Что такое деньги?

20-фунтовая купюра - необычное явление. Простая передача купюры кому-то означает мгновенную передачу ценности в 20 фунтов, не требующую заверения транзакции третьими сторонами. Если при этом присутствует только двое, никто в целом мире больше не знает об этом и никто не смог бы помешать передаче.

Но такая пиринговая передача работает только на близких расстояниях. Чтобы передать ценность в 20 фунтов кому-либо в другом городе или стране, мы должны довериться третьим сторонам и передать определенную степень контроля им: почтовому служащему, который держит в руках конверт с деньгами или банку, который осуществляет перевод электронных денег. Более того, если банк посчитает, что деньги связаны с преступной деятельностью, он может заморозить транзакцию или конфисковать электронные деньги.

Система мировых финансовых потоков - платежные системы, рабочие отношения между банками, сети электронных коммуникаций, такие как SWIFT (Общество всемирных межбанковских финансовых телекоммуникаций) - прямое следствие того факта, что наличные денежные средства фундаментально отличаются от всех остальных денежных форм. Только наличные денежные средства являются финансовым документом на предъявителя. И только наличные денежные средства могут быть переданы без разрешения третьих сторон - это "устойчивость к контролю".

Или мы так думали - до конца 2008 когда, когда была анонсирована система Биткойн. Ее создатели объявили ее "исключительно пиринговой (равный-к-равному) системой электронных денег", которые могут управляться напрямую держателем и отправляться без разрешения банка и риска быть конфискованными.

Каждый полноправный участник системы Биткойн имеет копии каждой транзакции, организованные в "блоки", восходящих вплоть до начала системы. Каждый блок криптографически соединен с предыдущим блоком, формируя блокчейн, которая хранит полную историю транзакций, и в следствие этого, выступает в роли распределенного реестра. Пользователи могут получить доступ к реестру с помощью различных приложений (к примеру,

Coinbase или Blockchain - не путать с лежащими в их основе технологиями). Каждая копия реестра синхронизируется алгоритмами, настроенными на достижение "консенсуса" в отношении состояния реестра.

Система Биткойн в 2008 году не появилась из ниоткуда. Исследования системы цифровой валюты проводились десятки лет, и каждый компонент системы уже существовал. Для создания прорывной системы Биткойн потребовалось лишь обобщить имеющиеся технологии с использованием инноваций, и сделать это в момент, когда идея разработки программного обеспечения с открытым исходным кодом уже созрела и люди стали открыты для идеи альтернативных денежных систем.

Система спроектирована таким образом, что чем дальше, тем сложнее - по сути, невозможно - изменить более ранние блоки. После того как транзакция подтверждена, она уже не может быть изменена, таким образом, демонстрируя свою устойчивость к контролю. Одним словом, то это действительно электронная наличность.

FAQ

Что такое "блокчейн"?

Блок - это простой список платежей. Блокчейн (цепочка блоков) - это список блоков, в которой каждый блок ссылается на предыдущий блок. Тем не менее, когда люди говорят о блокчейн, они обычно имеют в виду набор технологий и техник, которые легли в основу системы Биткойн, и которыми вдохновляются другие проекты, потому что они решают различные проблемы в финансовой и других сферах.

Неудивительно, что правительства и регулирующие органы во всем мире рассматривают это изобретение с такой осторожностью. Устойчивые к контролю активы на цифровых носителях выглядят идеальной валютой для преступного сообщества, и Биткойн стал основной денежной системой взаиморасчетов более несуществующего интернет-портала цифрового черного рынка Silk Road.
Тем не менее, большинство регулирующих органов, в том числе многочисленных учреждений в Великобритании, решили не запрещать Bitcoin, и многие уважаемые компании вносят значительные инвестиции в эту форму технологии. Почему?

Перспектива или угроза?

Во-первых, эти системы не настолько неуправляемые - или "неконтролируемые", как можно предположить. Вразрез с общественным мнением, базовая архитектура позволяет довольно просто отслеживать транзакции и устанавливать личность людей, которые злоупотребляют системой. Регуляторы также научились контролировать "входы" и "выходы", через которые денежные средства входят и выходят из системы.

Платформы типа Биткойн могут, поначалу, выглядеть настораживающе, но они не гарантируют анонимность пользователям, которые пожелают обменять биткойны на фунты, доллары или евро. В этом случае обменные системы должны будут применить соответствующие процедуры в отношении установления личности, предотвращения отмывания денег или финансирования терроризма. Кроме того, стоит отметить, что многие из наиболее интересных примеров применений этой технологии устанавливают правила относительно того, кто имеет право и кто не имеет права пользоваться системой.

Еще одно зарождающееся мнение относительно Биткойн, - то, что технологии, лежащие в ее основе, могут иметь значимые и полезные сценарии использования и создать условия для значительных инноваций в будущем.Устойчивость системы Биткойн к контролю проблематична с точки зрения правоохранительного регулирования, и поэтому маловероятно, что ключевые корпорации или банки начнут применять близкие к биткойн технологии в ближайшей или

среднесрочной перспективе.

Однако технология распределенного реестра, отдельно от криптовалюты предлагает

открытость, которая может оказаться очень ценной. Открытые платформы, управляемые не одной компанией, а активно расширяющимся сообществом разработчиков, демонстрируют своевременность и способность стать движущей силой инноваций. Они могут позволить аутсайдерам и новым участникам предлагать новые продукты и услуги ранее ограниченным в правах пользователям (см. Главу 5 о разрушительном потенциале технологии).

Не смотря на то, что технология распределенного реестра была изобретена с одной целью (электронной валюты), компании и различные учреждения сейчас активно исследуют, каким образом она может применяться для решения других насущных проблем. Например, бизнес-сектор часто находит "контролируемые" блокчейны гораздо более привлекательными, чем неконтролируемую модель Биткоин, потому что отдельные стороны должны авторизовываться для подтверждения транзакций. Это позволяет предприятиям создавать безопасные, частные сети компаний и индивидуальных пользователей, взаимно доверяющих друг другу (см. Главу 3 для более детального обзора контролируемых и неконтролируемых систем).

FAQ

Вопрос-ответ: В чем фундаментальное отличие Биткойн от предшествующих типов валют?

Любое частное лицо может владеть биткойнами, это не требует разрешения банков или правительства. Они могут быть отправлены кому угодно в мире, кто знает, как пользоваться "Биткойн-кошельком". Это и есть принцип "устойчивости к контролю", который определил существенный прорыв системы Биткойн - и который объясняет сомнения законодателей и регуляторов.

В целом, очевидно, что в этой сфере может существовать множество технологий, которые могут быть классифицированы по тому, насколько они "децентрализованы" (т.е. до какой степени они контролируемы) (см. рис. 1). Но централизация - всего лишь одна величина, по которой эту сферу можно анализировать. Другие активно изучаемые категории: степень, в которой использование средств может быть зарегламентировано (например, средства, которые могут быть потрачены ребенком, при условии совместного подписания родителями), а также возможность представления отличных от денег активов (например, ценных бумаг или даже права собственности на имущество).

Рисунок 1 Различные технологии реестров различаются по "степени централизации"

Возможности применения

Технология распределенного реестра может решить проблемы бизнеса, которые можно охарактеризовать как: затраты, копирование и согласование.

Возьмем банковское дело. Каждый банк создал или купил по крайней мере одну (обычно несколько) систему отслеживания и управления жизненными циклами финансовых транзакций. Каждая их этих систем требует затрат на создание и еще больших - на содержание. Они должны быть связаны друг с другом и синхронизированы, обычно посредством сверки данных. Эти процессы требуют присутствия целых команд людей в каждом банке и аналогичных команд в других банках, чтобы контролировать, что все совпадает и решать проблемы, если нет.

Стандартным решением является установление единого централизованного реестра, распределенного на всех участников. В Великобритании есть ряд удачных примеров использования такого подхода, в особенности - в Сервисе Ускоренных Платежей (Faster Payments Service). Но стоимость централизованной инфраструктуры, как правило высока, и, поскольку данные обрабатываются централизованно, такая система должна быть интегрирована с системой каждого участника. При другом подходе, многие децентрализованные базы данных, могут находиться в разных узлах сети во время перемещения сообщений между ними (см. рис. 2).

Рисунок 2

Распределенные сети могут работать без затратного по времени процесса заверения, который применяется централизованными и децентрализованными базами данных.

Тим Свинсон

Биткойн же синхронизирует тысячи компьютеров в распределенной сети через Интернет: если мой компьютер думает, что у меня есть Биткойн, то и любой другой компьютер в сети считает так же. Если использовать подобную методику в банковском секторе, то все системы банков могли бы идти в ногу друг с другом, не требуя армии людей для процесса согласования, а также для разрешения возникающих проблем. Важно то, что нам не нужен Биткойн для достижения этой цели, - технология распределенного реестра, которая лежит в основе Биткойна, дает возможное решение.

Это могло бы способствовать решению одной из самых больших проблем, связанных с финансовыми услугами: проблемы расходов на использование бумаги. В последние годы было предпринято много различных инициатив, направленных на исключение бумажных документов из экономики. Тем не менее, во многих случаях новая технология просто воспроизводила старые процессы по-новому, или сохраняла использование бумаги в других стадиях операций. Например, предоставление финансовых ресурсов для экспортеров остается чрезвычайно ручной процедурой: банк импортер выдает письменный аккредитив, по которому банк экспортера будет авансировать средства. Хотя этот процесс, как правило, электронный, последующие заверения опираются на стопки бумажных документов, которые обрабатываются вручную по всему миру. Технология распределенного реестра может, в отличие от этого, заменить некоторые аспекты "бумажных" банковских услуг, процессами, которые работают гораздо быстрее и без-

ПРАКТИЧЕСКИЙ ПРИМЕР

Исследования и обзор перспектив

Джон Г. Бэйрд, Глава Научного Совета по вопросам Цифровой Экономики, Совета по инженерным и физическим научным исследованиям (RCUK Digital Economy Theme, EPSRC)

Совет по инженерным и физическим научным исследованиям руководит вопросами Цифровой Экономики по поручению Научного Совета Великобритании. С 2008 года Совет по вопросам Цифровой Экономики инвестировал более £170 млн в прикладные междисциплинарные исследования, с особым акцентом на социально-культурные проблемы при электронизации экономики и ее влиянии на социальную интеграцию, сельское хозяйство, персональные данные, безопасность, установление личности, надежность и конфиденциальность. Совет по вопросам Цифровой Экономики продвигает сферу и Цифровой Валюты, и Интернета Вещей, анонсированных в Бюджете на март 2015. На сегодняшний день мы инвестировали в следующие виды деятельности в области технологий распределенных реестров:

1. CREDIT (Влияние криптовалюты на Цифровые Преобразования) 1, - 18-месячный научно-исследовательский проект стоимостью £0,4 миллиона, который направлен на изучение феномена криптовалюты и связанных, лежащих в его основе технологий, блокчейн, объединенных по 4 главным тематикам: цифровые преобразования, конфиденциальность, сообщества и учреждения. Основным результатами исследования станут:

- Пошаговое руководство, направленное на оказание помощи стартап¬ам и действующим игрокам в понимании различных вопросов для включения технологии блокчейн в свои продукты и услуги.
- Ряд небольших пилотных исследований совместно с компаниями, изучающими потенциальные воздействия криптовалют.
- Сообщество ученых-исследователей и специалистов, готовых к дальнейшему развитию этой зарождающейся области

2.Проект CREDIT основывается на двух предыдущих исследованиях, которые мы поддержали: "Революционная роль криптовалюты" 2 и "ИКТ и Будущее Финансовых Услуг" 3. Оба исследования пересмотрели текущее понимание криптовалют и выявили пробелы в понимании социальных, этических, правовых, регулирующих воздействий крипто-валют. В результате, мы недавно опубликовали запрос на исследование стоимостью £10 млн миллионов фунтов стерлингов по теме: 'Доверие, Идентичность, Конфиденциальность и Безопасность в Цифровой Экономике' 4, которое демонстрирует "Широкое применение технологий распределенного реестра" в качестве одной из шести ключевых областей. Это направление ориентировано на поддержку исследований, которые интегрируют и уравновешивают технический прогресс в системах распределенных реестров с пониманием того, что социальные, этические, правовые и бизнес-структуры, должны создавать условия для уверенности, доверия и принятия таких систем отдельными лицами, сообществами, организациями и государствами. В конечном счете, мы надеемся, что это исследование проложит путь к "умной" экономике, которая может поддерживать различные сценарии монетарного и неденежного обмена ценностями между отдельными лицами и организациями, а в будущем и к "умным" объектам.

3.И, наконец, мы вложили £260 000 в исследовательский проект Сторонней дематериализации и рематериализации капитала (3DaRoC) 5, который изучает, как разработать эффективные цифровые торговые финансовые сервисы на основе практических примеров с двумя типами торговых финансовых организаций: Zopa Limited, пиринговая кредитная организация; и Bristol Pound, - социальная валюта. В ходе проекта был подготовлен онлайн инструментарий, призванный помочь пользователям и бизнесу, которые хотят повлиять на ключевые вопросы разработки и использования цифровых финансовых продуктов6.

lбумажным способом. Совет по инженерным и физическим научным исследованиям (EPSRC) поддерживает исследования для таких финансовых применений (см. практический пример научных исследований и обзора перспектив).

Однако возможности не ограничены банковской сферой. Применение технологии в настоящее время тестируется в медицинских учреждениях (записи историй болезни), правительстве (земельные реестры и выплаты пособий - смотрите Главу 6), электронике (в том числе "Интернете вещей" -

см. Главу 1) и даже мире искусства и ювелирных изделий (отслеживание происхождение алмазов - смотрите Главу 5).

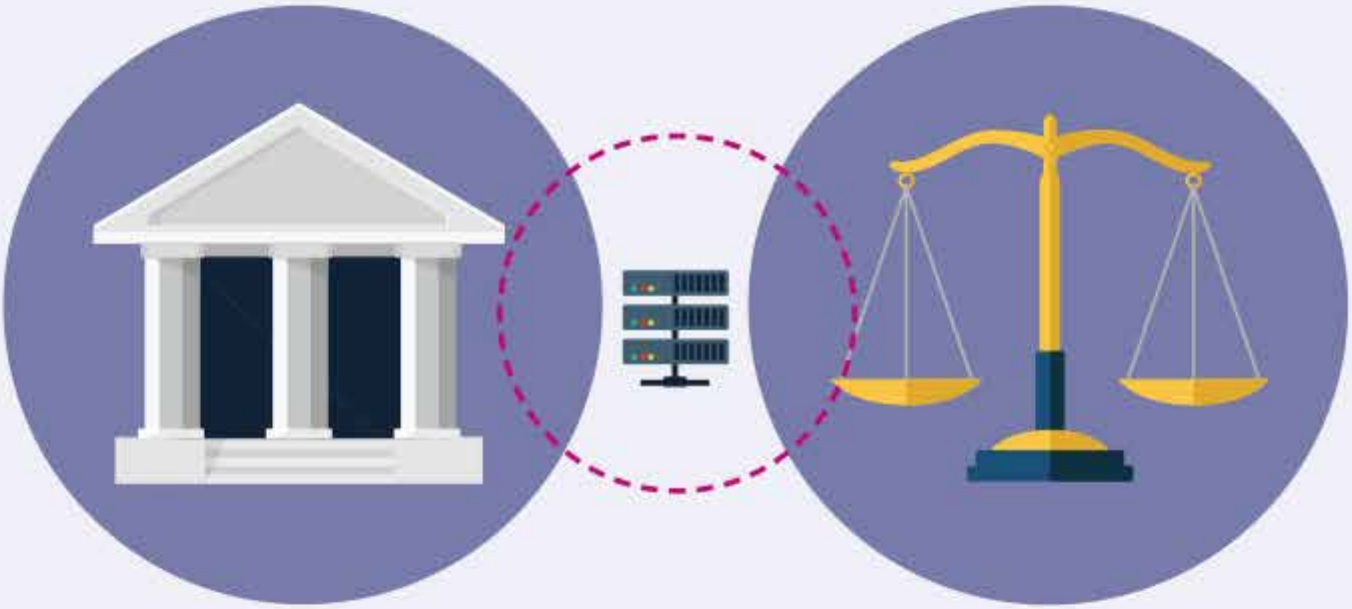
Важно подчеркнуть, что эти технологии находятся на очень ранней стадии своего развития, и есть много нерешенных проблем, за которые нужно взяться, прежде чем эти сценарии применений могут быть реализованы, а именно: вопросы конфиденциальности, производительности и масштабируемости. Достаточно ли хорошо работает технология, чтобы банки могли ей доверять? Кто будет создавать такие платформы, если за них нельзя взимать плату, так как они распределенные и объединенные?

Однако сфера быстро развивается, и многие из этих проблем уже решаются. Теперь становится возможным провести различие между теми аспектами технологии, которые будут изменяться со временем, и теми, которые являются врожденными и вряд ли изменятся. Уже сейчас мы видим, что технология распределенных реестров могла бы позволить компаниям и правительствам более эффективно работать, без дорогостоящих процессов заверения и согласования. И это могло бы позволить действующим и новыми участниками конкурировать на равных условиях, предлагая новые продукты и услуги потребителям на основе открытого доступа к защищенным общим данным.

Это может привести к мировой революции, выходящей за пределы цифровой валюты, устойчивой к контролю.

ГЛАВА 3

Управление и регулирование



И правовая и цифровая сферы регулируются определенными правилами, но характер этих правил отличается. В цифровой среде, деятельность регулируют и законы (юридический кодекс) и программное обеспечение (технический кодекс) . Влияние обоих факторов должно учитываться при разработке нормативных требований к системам распределенного реестра.

Автор
Вили Лехдонвирта, Оксфордский Институт Интернета, Оксфордский университет;
Робли Али, Менеджер - Департамент цифровых валют, Центральный Банк Великобритании

Глава 3: Управление и регулирование

Введение

В этой главе рассматриваются правила и правила их разработки в системах распределенного реестра.

Мы проведем различие между **правовым кодексом** (правила, состоящие из юридических обязательств) и т**ехническим кодексом** (программное обеспечение и протоколы). Мы также проведем различие между **руководством** (разработка правил владельцами или участниками системы с целью защиты своих частных интересов) и **регулированием** (разработка правил по поручению высших органов власти, в интересах общественности).

Правовой кодекс против технического кодекса: два типа правил

Финансовая система - одновременно совокупность юридических обязательств между учреждениями и совокупность электронных записей этих обязательств. И правовая и цифровая сферы регулируются определенными правилами, но характер этих правил отличается. В фундаментальной работе на эту тему 1, Лоуренс Лессиг из Гарвардского университета рассмотрел, как эти правовые и цифровые правила взаимодействуют в целях управления деятельностью. Лессиг утверждает, что в цифровой среде и закон (правовой кодекс) и программное обеспечение (машинный кодекс) регулируют деятельность, и что влияние обоих необходимо учитывать при построении теории управления. В этой главе мы коснемся технического кодекса, а не машинного. Это определение включает в себя программное обеспечение и протоколы, которые нужны для функционирования распределенных реестров.

Одно из фундаментальных различий между правовым и техническим кодексом - механизм, посредством которого каждый из них воздействует на деятельность. Правовой кодекс - 'внешний': правила могут быть нарушены, но последствия этого нарушения возникают с целью обеспечения соблюдения правил. Технический код, напротив, является «внутренним»: если его правила нарушены, то возвращается ошибка, и никакой деятельности не происходит, поэтому соответствие обеспечивается за счет работы самого кода. Еще одной особенностью программного обеспечения является то, что машина будет жестко следовать правилам даже в тех случаях, когда соблюдение приведет к непредвиденным и нежелательным результатам. Это приводит к некоторым разительным отличиям в работе систем распределенного реестра по сравнению с современной финансовой системой.

1. Современная финансовая система: управление с помощью правового кодекса

Современная финансовая система уже в значительной степени цифровая и сильно зависит от технического кода. Этот технический код регулирует создание и изменение цифровых записей юридических обязательств между учреждениями. Финансовое регулирование направлено на последствия, к которым эти юридические обязательства производят: например, имеет ли банк достаточный капитал или ликвидность. Финансовая система регулируется сочетанием технического и правового кодексов, но финансовое управление и регулирование традиционно сосредоточены на последнем.

Исполнение публичной части правового кодекса контролируется специализированной группой финансовых регуляторов, в обязанности которых входит обеспечение соблюдения согласованности между участниками системы. Участники должны предоставить информацию, с помощью которой их регулирующий орган оценивает их соответствие правилам системы. Если учреждение не соответствует требованиям, то регулирующий орган может принять меры, чтобы привести их в соответствие. Это не значит, что технический кодекс не оказывает никакого влияния на существующий процесс регулирования - вся информация, предоставленная регуляторам является цифровой, и продуктом технического кода - но управление и регулирование производятся путем применения правового кодекса, а не изменения технического.

2. Системы распределенных реестров: управление с помощью технического кодекса.

Системы распределенного реестра, такие как Биткойн продемонстрировали, что они могут функционировать без правовых норм. Вместо этого, правила, которым каждый участник должен следовать, определены и применяются только при помощи технического кода. Каждый участник в сети применяет одно и то же или схожее программное обеспечение, которое определяет, какие виды операций допустимы. Например, программное обеспечение Биткойн позволяет участникам расходовать только те средства, в отношении которых участники могут доказать свое право владения, применив криптографический ключ. Программное обеспечение Биткойн также регулирует выпуск новой валюты и устанавливает абсолютный лимит на размер денежного пула. Не существует никаких постановлений или иных правовых документов, подтверждающих эти правила, и людей, которые бы обеспечивали их соблюдение - системы распределенного реестра регулируется исключительно их собственным техническим кодом.

Для того, чтобы не допустить изменения копий кода участниками и выпуска транзакций не по правилам, каждая транзакция должна быть подтверждена перед включением в реестр. В "неконтролируемой" системе распределенного реестра, такой как Биткойн, те, кто подтверждает транзакции (майнеры) выбираются методом лотереи. Система направлена на поддержание чистоты транзакций через систему экономических стимулов в процессе, управляемом программным обеспечением. В системе "контролируемого распределенного реестра", контролеры назначаются владельцем системы, и их честность обеспечивается с помощью традиционных средств, таких, как юридический договор.

Таким образом, системы распределенного реестра отличаются от традиционной финансовой системы тем, что они управляются техническими, а не юридическим кодексом. Одним из их преимуществ являются низкие затраты на соблюдение требований: участники всего-лишь должны использовать совместимый комплекс программного обеспечения для проведения транзакции. Может показаться, что затраты на исполнение тоже ниже, но это не обязательно так, потому что майнинговая система, используемая для верификации транзакций во всех наиболее популярных системах распределенного реестра требует значительных вычислительных ресурсов. Эти расходы в конечном итоге должны нести пользователи системы.

Руководство против регулирования: два типа разработки правил

Поскольку в настоящее время финансовая система и распределенные реестры в основном регулируются различными типами правил, мы должны задать вопрос: кто устанавливает правила?

1. Текущая финансовая система: смесь частного и государственного нормотворчества.

Существует много примеров, когда правовой кодекс разрабатывается текущей финансовой системой, но все они могут быть разделены на две категории: частное нормотворчество (управление) и государственное нормотворчество (регулирование). Примером частного нормо¬творчества являются Основные Правила Visa, обнародованные финансовой компанией Visa Inc., чтобы управлять действиями всех участников системы Visa. Такое частное нормотворчество осуществляется собственниками частных финансовых сетей, таких как Visa, а также частными ассоциациями финансовых учреждений, желающих координировать деятельность друг друга для общей выгоды. Примером государственного нормотворчества является установленный законом надзор за платежной системой Visa Europe Центральным Банком Великобритании.

Разработка государственного правового кодекса в существующей финансовой системе - компетенция политических деятелей, которые должны учитывать влияние нормативных требований на различные учреждения финансовой системы ('микропруденциальный' подход) и влияние на систему в целом ('макропруденциальный' подход). Так как финансовая система глобальна, международные организации, такие как Базельский Комитет по Банковскому Надзору, созывает политиков со всего мира, для достижения добровольных

договоренностей, которые затем могут быть переведены в законодательство в конкретной юрисдикции.

2. Системы распределенного реестра: ситуативное частное нормотворчество

Иногда считается, что неконтролируемые системы распределенного реестра существуют независимо от человеческого нормотворчества, и управляются только с помощью математических алгоритмов. Это заблуждение. Так же, как правовой кодекс, технический код должен быть создан и поддерживаться людьми, которые определяют правила, которые воплощает в себе код. Если взять систему Биткойн в качестве примера, первоначальная версия программного обеспечения была опубликована Сатоши Накамото (псевдоним). В 2010 году Накамото передал контроль над проектом Гэвину Андресену, программисту австралийского происхождения, проживающему в Соединенных Штатах. Как и любое программное обеспечение, Биткойн необходимо регулярно обновлять, чтобы устранять баги, решать вопросы безопасности и изменений в операционной среде. Такое обновление может в принципе изменить все аспекты программного обеспечения, в том числе идентификации пользователей и правил собственности. Поэтому критически важно для всех участников системы распределенного реестра: кто пишет программное обеспечение и как этот процесс регулируется.

В случае с Биткойн, программное обеспечение регулируется с помощью специального процесса с участием группы неформальных институтов и держателей власти. На рисунке 1 показано, кто написал большую часть текущего кода Биткойн. Программное обеспечение представляет собой открытый исходный код, и любой может предложить изменения к нему, но техническое право признать изменения в официальной версии программного обеспечения принадлежит группе из пяти основных разработчиков, утвержденных Андресеном. Власть основных разработчиков ограниченна неофициальным уставом, который утверждает, что значительные изменения правил требуют консенсуса сообщества. Более того, любое обновление программного обеспечения должно быть установлено большинством майнеров (что определяется вычислительной мощностью компьютера, которую они отдают) для того, чтобы изменения вступили в силу. Группа лиц, которая управляет так называемыми майнинговыми пулами, имеют очень большое влияние на то, ратифицируют или нет майнеры подобное обновление программного обеспечения.

Этот процесс управления работал хорошо, пока изменения в коде были однозначными исправлениями ошибок, но в последнее время он начал давать сбои, потому что некоторые решения требуют выбора, интересы какой из заинтересованных сторон одержат верх. Андресен и другие заявили, что этот процесс должен стать более формальным. Сообщество спорит по поводу того, как должна выглядеть такая система управления, но это осложняется тем фактом, что

Рисунок 1
Разработчики главных частей кода Bitcoin Core, 14 мая 2015 (источник: исследование автора)

Система Биткойн была основана на идеалах анти-институционализма. Этот парадокс демонстрирует ценность правового кодекса и показывает, что технический код сам по себе не дает оптимального результата.

В системах контролируемого распределенного реестра, управление программным обеспечением становится проще благодаря тому, что, как правило, существует владелец системы, обладающий четкой правовой и технической властью над кодом. Владелец системы определяет, как изменяется код, пользователи (часто клиенты службы), - решают, комфортно ли им с наличием собственника, который обладает властью над программным обеспечением. Соглашения об уровне обслуживания и другие стандартные средства могут устанавливать сферы ответственности и обеспечивать их соблюдение. Системы контролируемых распределенных реестров в этом отношении не очень отличаются от обычных частных финансовых сетей, таких как Visa или "систем программного обеспечения как услуг" (SaaS).

Как мы должны контролировать системы распределенных реестров?

Управление в системе распределенного реестра, как описано выше, затрагивает интересы участников, однако могут существовать более широкие общественные интересы, влияющие на функционирование распределенного реестра. Например, регуляторы могут пожелать собирать налоги, привлекать к ответственности за преступления, а также ограничить использование распределенного реестра в преступных целях. Если система настолько адаптировалась, что потенциально может воздействовать на другие сферы общества, то регуляторы также могут захотеть получить гарантии, что система будет устойчивой к системным рискам и провалам рынка. Такое регулирование может применяться посредством правового или технического кода.

1. Регулирование распределенного реестра посредством правового кодекса

Регулирование в системе контролируемого распределенного реестра - просто вопрос наложения юридических обязательств на его собственника. Регулирование неконтролируемой системы, такой, как Биткойн с помощью правового кодекса - более сложный процесс, так как в управляющем сообществе системы нет ни одного юридического лица . Это затрудняет контроль над тем, какое программное обеспечение людям разрешено устанавливать на своих компьютерах. Попытки регулировать Биткойн посредством правового кодекса, вместо этого сосредоточились на регулировании тех видов бизнеса, которые имеют дело с Биткойн, например, сервисы обмена валют и обслуживания кошельков. Такие организации могут контролироваться сами по себе (например, предотвращение попыток исчезновения с деньгами пользователей владельцев сервисов по обслуживанию кошельков) или как средство непрямого контроля деятельности реестра (например, для соблюдения правил по борьбе с отмыванием денег).

Хорошо известный пример регулирования Биткойн с помощью правового кодекса - это BitLicense, которую разработал Департамент финансовых услуг штата Нью-Йорк для компаний, которые предоставляют услуги цифровых операций жителям Нью-Йорка.2. Для организаций был установлен дэдлайн - 8 августа 2015 года - для приобретения этой лицензии, а нелицензированные поставщики услуг могли быть оштрафованы.

2. Регулирование распредленного реестра посредством технического кодекса

Технический код для систем распределенного реестра, таких как Биткойн в настоящее время разрабатывается частными лицами в ходе специального процесса. Но технический код, включающий в себя программное обеспечение и протоколы, также может быть выпущен и государственным сектором. Например, протоколы TCP/IP и некоторые другие базовые интернет-протоколы стали результатом финансируемых правительством исследовательских проектов и в настоящее время эксплуатируются при содействии Общества Интернета, международной некоммерческой организации с открытой структурой, основанной на принципах географического положения и специальных интересов. Другие стороны Интернет-инфраструктуры поддерживаются международными многосторонними процессами, и некоторые из них остаются под контролем американских государственных регуляторов.

Хотя эта путаница далека от идеального решения, она указывает на возможность участия общественности и демократического представительства в производстве технического кода - государственного регулирования через технический, а не юридический кодекс.

Таблица 1
Примеры частного и государственного правового кодекса и компьютерного кода

	Правовой кодекс	Протокол
Закрытая разработка	Ключевые правила Visa Правила сервиса ускоренных платежей	Протокол обмена финансовой информацией (FIX) Биткойн
Публичная разработка	Инфраструктурное регулирование Европейского РынкаBitLicense	Интернет (TCP/IP) Всемирная паутина (http)

Применительно к системам распределенного реестра, это может означать что угодно, - от создания формальных многосторонних процессов для управления техническим кодом, до разработки государственных стандартов для кода. Если это позволит правительству или общественности напрямую достичь цели законного регулирования путем влияния на правила, встроенных в компьютерный код, то это может уменьшить потребность в новом правовом кодексе для регулирования этих систем.

С другой стороны, государственный сектор мог бы разработать контролируемую систему, которая позволит влиять на государственное регулирование за счет сочетания правового и технического кодексов, а не только через правовой кодекс, как это происходит в настоящее время. Некоторые из ключевых интернет-технологий, показали, что правительство может успешно стимулировать создание технического кодекса, который стал основополагающим для деятельности частного сектора.

Заключение

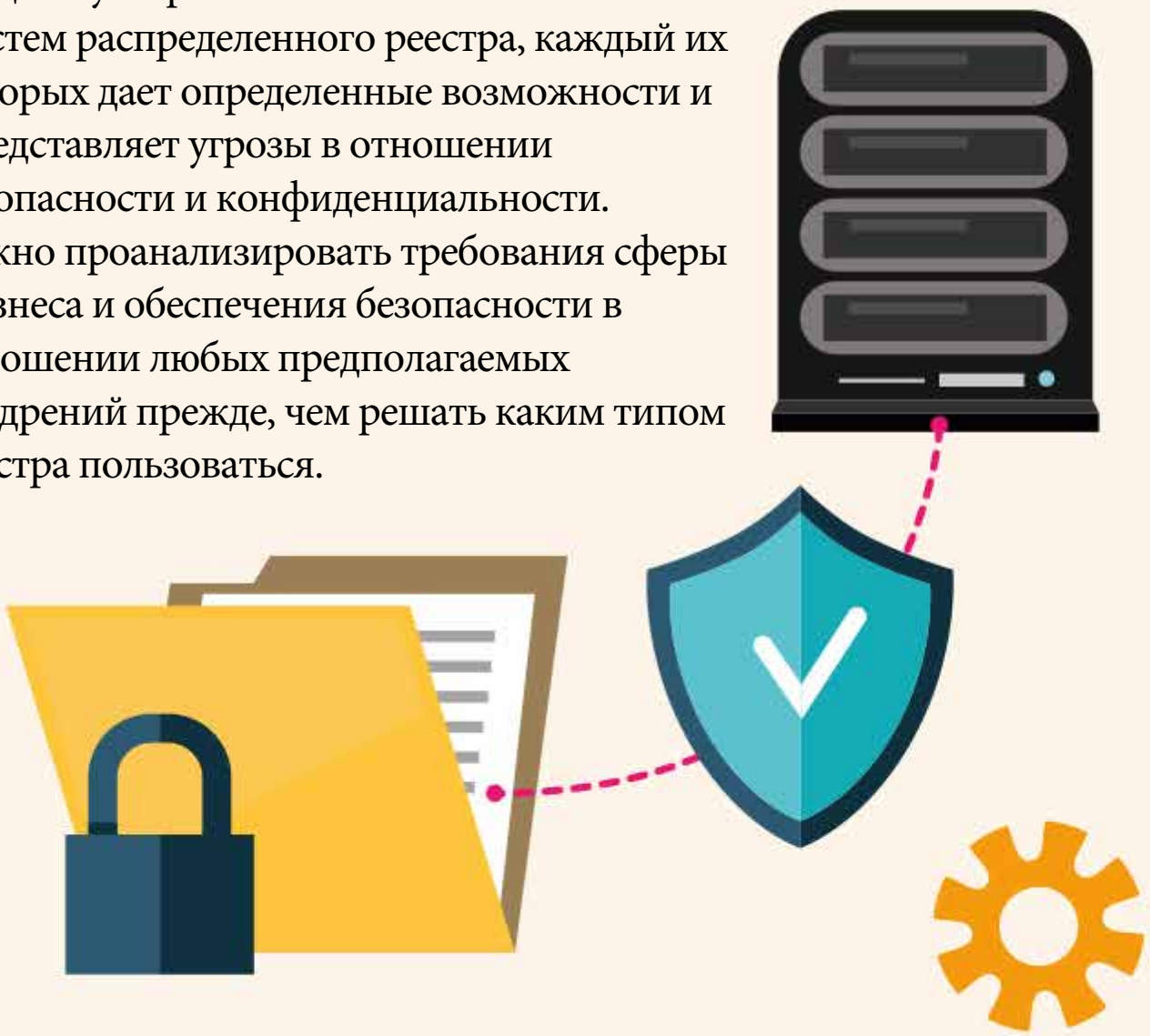
lВ отличие от обычных частных финансовых сетей, таких как Visa, в системах неконтролируемого распределенного реестра, таких как Биткойн, отсутствует центральное юридическое лицо с формальной ответственностью за систему. Вместо этого, они регулируются специальными процессами, как правило, сконцентрированными в руках группы разработчиков программного обеспечения, которые создают программный код системы. Если эти системы будут расти в цене и степени влияния, они, скорее всего, потребуют разработки более надежных процессов внутреннего управления. Отсутствие центрального юридического лица также делает более сложным для государственных регуляторов процесс контроля за системой распределенного реестра посредством правового кодекса. Поэтому, правительствам следует также рассмотреть способы регулирования систем распределенного реестра путем воздействия на технический код, который определяет правила системы. При нахождении правильного сочетания, правительство должно учитывать сильные и слабые стороны как технического кода, так и правового кодекса, признавая, что они взаимодействуют между собой и должны быть разработаны во взаимосвязи.

Появление Биткойн и систем распределенного реестра вынесло вопрос технического кодекса на первый план в контексте нынешней финансовой системы. Распределенные реестры демонстрируют, что финансовые системы могут управляться и регулироваться техническим кодексом, также, как и правовым. Политикам следует признать влияние технического кодекса на финансовую систему и рассмотреть возможность сделать его частью системы регулирования с потенциальными преимуществами, такими как более низкие затраты на соблюдение правил.

ГЛАВА 4

Безопасность и Конфиденциальность

Существуют различные типы систем распределенного реестра, каждый их которых дает определенные возможности и представляет угрозы в отношении безопасности и конфиденциальности. Важно проанализировать требования сферы бизнеса и обеспечения безопасности в отношении любых предполагаемых внедрений прежде, чем решать каким типом реестра пользоваться.



Автор

М. Анжела Саас, Университетский колледж Лондона, при участии: Джорджа Данезиса и Сары Майклджон, Университетский колледж Лондона; Даниеля Шиу, Центр правительственной связи; Филипа Годсиффа, Университет Суррея

Глава 4: Безопасность и конфиденциальность

Введение

Простое определение безопасности: "Делать то, что можно делать; и не делать того, чего делать нельзя." В каждом случае реализации распределенного реестра и блокчейн, риски желательных и нежелательных последствий зависят от того, как технология разработана, внедрена и управляется.

Разные игроки сталкиваются с разными рисками.

Среди угроз для системы, - не только атаки со стороны внешних сообществ, но и действия внутренних участников и отказы компонентов (например, программного обеспечения). Подробные модели угроз должны быть разработаны до начала любого внедрения, а также определены конкретные требования к безопасности, для того, чтобы справиться с последствиями.

Эффективная безопасность предоставляет необходимую, но недостаточную базу для обеспечения конфиденциальности индивидуальных лиц и организаций-участниц. Мы должны также продумать, как информация, раскрываемая в конкретной разработке, может быть объединена с другой доступной информацией в целях определения личности конкретного лица или группы людей, и установления их деятельности.

Преимущества инноваций

Ключевой составляющей безопасности Биткойн и других криптовалют является децентрализованный контроль сети. Система управляется глобальным сообществом узлов, которые работают на основе распределенного консенсуса (см. Определения, стр. 17), поэтому не существует центральной точки доверия или ошибки. Это означает, что любой агрессор должен предпринять значительные усилия, чтобы атаковать систему. Система тоже может обеспечить высокую степень безопасности индивидуальных пользователей - для того, чтобы переместить биткойны, которые хранятся к кошельке, злоумышленник должен знать закрытый ключ, привязанный к открытому ключу (который находится там, где хранятся биткойны). Таким образом, злоумышленник должен быть в состоянии взломать защиту установленного криптографического стандарта (Алгоритм с открытым ключом для создания электронной подписи (ECDSA), чтобы украсть чужие биткойны.

Биткойны и ассоциированные "альткойны" (альтернативные монеты) применяют гораздо более широкую инфраструктуру компьютерной безопасности, а именно - распределенные реестры - что обеспечивает высокую целостность и логичность визуализации. Поскольку такие реестры обладают небольшим количеством критически важной информации, они используют криптографические методы, чтобы гарантировать, что любой человек может проверить, находится ли конкретная запись в пределах реестра. В то же время, комплексные протоколы консенсуса обеспечивают возможность для каждого пользователя в системе получать полное представление о реестре. Это дает ключ к пониманию способности Биткойн предотвращать двойное расходование, но может быть также важно и при использовании распределенных реестров в других целях, таких как регистрация контрактов или договоров. Распределенные реестры, естественно, годятся для реализации услуг высокого уровня, связанных с нотариусами, фиксацией времени и архивированием с высокими требованиями безопасности, и позволяют снизить расходы на эти действия за счет увеличения автоматизации, возможности легкой смены провайдеров, а также пиринговых транзакций.

Одна из главных проблем безопасности онлайн коммуникаций заключается в том, что открытый ключ принадлежит сервису, к которому пользователь хочет получить доступ. Наиболее часто используемый с 1990-х годов механизм известен как Инфраструктура открытых ключей, (PKI) - это набор доверенных третьих сторон, которые предоставляют сертификаты, подтверждающие связь между ключами и сервисами. Но такая система сертификатов продемонстрировала

несовершенство; при сбоях, они могут выпускать неверные сертификаты незаметно.

Система Прозрачности Сертификатов 1 (CT) (недавно предложенная компанией Google, в настоящий момент курируемая рабочей группой) использует технологию распределенного реестра для устранения этой проблемы. Все сертификаты добавляются к распределенному реестру, и любой пользователь или сервис может убедиться, что сертификат, который они собираются использовать находится в реестре. Следовательно, мошеннические сертификаты могут быть обнаружены быстро. Это - существенное препятствие для злоумышленников, желающих злоупотребить или взломать систему PKI.

Проблема установления надежной связи между ключом и субъектом также существует, когда пользователи хотят защитить личную коммуникацию. Но существующие решения (такие, как Сеть Доверия PGP или централизованные решения) являются либо непригодными для использования, либо имеют ненадежные характеристики безопасности. Перспективной альтернативой является технология CONIKS2, которая основана на специально разработанном распределенном реестре, предназначенном для хранения и поиска открытых ключей, которые можно использовать для шифрования или подписи электронных почтовых сообщений. В отличие от концепции прозрачности сертификатов (CT),

— которая при хранении и проверке распределенного реестра опирается на сеть третьих сторон, в технологии CONIKS для формирования реестра с высоким уровнем интеграции используются провайдеры связи и имеющиеся у них базы данных пользователей.

Угрозы безопасности

Связанные с безопасностью преимущества децентрализованных систем, указанные выше, в частности, устойчивость и защищенность, в полной мере применимы только к неконтролируемым реестрам, которые формируются в соответствии с глобальной теорией доверия. Для контролируемых реестров или примеров с другими централизованными функциями устойчивость и защищенность характерны в меньшей степени, однако они обладают лучшей способностью обеспечивать центральный уровень доверия и (или) функции.

В действительности между полностью децентрализованными системами (как Биткойн) и полностью контролируемыми системами (частная выделенная сеть) существует множество вариантов (см. главу 2). Примером оптимального решения, в котором используются сильные стороны обеих систем, является предложение Джорджа Дэнезиса и Сары Мейклджон из Университетского колледжа Лондона по криптовалютам с централизованной регуляцией3, которые используют сервер с централизованным контролем при формировании блокчейна, применяя распределенную сеть «mintettes» для совершения транзакций.

Учитывая весь спектр решений, важно проанализировать деловые требования и требования к безопасности всех предлагаемых вариантов до принятия решения о том, какой тип реестра следует использовать.

Например, ключевые приоритеты системы, управляющей платежами соцобеспечения для Министерства труда и пенсионного обеспечения, включают в себя гарантию как доступности сервиса, так и его устойчивости к отказам сети (см. главу 6). Источником наибольших угроз, вероятно, станет оппортунистический кибер¬криминалитет, нацеленный на индивидуальных пользователей с целью хищения денег. Следовательно:

- Система должна быть спроектирована так, чтобы от индивидуальных пользователей требовался минимальный объем знаний и усилий, т. е. должно быть доступно лишь некоторое число вариантов выбора и конфигураций, и при этом должна обеспечиваться четкая реакция в виде результата.
- Если используются однофункциональные устройства, такие как смартфоны, необходимо обеспечить безопасный доступ к регистрационным данным и ключам и их недоступность для других приложений.
- Чтобы обеспечить устойчивость реестра к отказам сети, его следует эксплуатировать в широкой сети серверов.

- Для более масштабных задач сервис авторизации платежей должен быть централизован на выделенном оборудовании и защищен от атак.

В качестве альтернативы, для системы, которая может использоваться для распределения помощи иностранного государства, потребуется обеспечить целостность транзакций (чтобы предотвратить несанкционированное использование финансовых ресурсов на другие цели) и обеспечить доступность системы, например, во время оказания помощи при стихийных бедствиях. Источниками угроз могут становиться государства, которые могут получить геополитические преимущества от срыва транзакций, или непорядочные агенты внутри государств, принимающих помощь. Следовательно:

- Система должна работать на базе небольшой защищенной выделенной сети серверов, которая синхронизирует правительственные копии реестра с автономными резервными копиями.
- Следует призывать клиентов создавать свои собственные сети реестров, предоставляя консультации по разработке безопасного проекта системы, которая позволяет выполнять регулярные обновления или получать корректировки от правительственных серверов.

- Необходимо предусмотреть перевод системы в автономный режим в случае возможной сетевой атаки.

Тем не менее, пожалуй, самая серьезная угроза для любой поддерживаемой государством системы заключается в ее моральном устаревании. Если система слишком сложна в эксплуатации или не обладает необходимой функциональностью, она не будет внедрена в практику.

Еще одна из новых угроз — хайджекинг (от англ. hijack - захватывать, угонять), так как внедрение различного программного обеспечения создает «дыры» в существующей системе. Криптоаналитик Николя Куртуа из UCL, который тщательно следил за историей развития Биткойна, в августе 2015 г. отметил следующее:

«Будет возможность осуществлять майнинг блоков с новой версией и новыми правилами. Это необходимо для того, чтобы сделать систему Биткойн более демократичной — больше блоков, больше транзакций в секунду, меньше комиссий, более широкий охват. В последние месяцы текущая версия Биткойн достигла своей максимальной емкости (немногим более 3 транзакций в секунду), и сообществу разработчиков Биткойн НЕ УДАЛОСЬ разрешить эту проблему».

Этот факт показывает, что управление любой поддерживаемой государством системой потребует серьезного предварительного анализа возможных технических решений, а также решения вопроса о защите системы от перехвата контроля другими субъектами - враждебными или нет.

Рекомендации по обеспечению безопасности

В каждом конкретном случае применения технологии правительство должно тщательно идентифицировать существенные угрозы. Хотя ни одно государство не заинтересовано в разрушении системы Биткойн, оно может быть заинтересовано в атаке на национальную цифровую валюту Великобритании, и если в результате действий с мошенническими данными в реестре можно получить какую-либо финансовую выгоду, то существует вероятность, что организованная преступность будет атаковать пользователей с низким уровнем знаний и понимания мер безопасности.

С учетом выявленных угроз правительство должно принять решение о надлежащем уровне безопасности в отношении злоумышленника и времени предполагаемого использования.

Если ожидаются кибератаки, то системы с самого начала должны проектироваться с учетом фактора безопасности эксплуатации. Например, неконтролируемые сети реестров позволяют злоумышленникам угрожать целостности сети путем добавления своих собственных серверов или путем реализации DoS-атаки на легитимных серверах. С целью противодействия атакам для долгосрочного реестра, представляющего интерес для государства, может потребоваться множество устойчивых схем получения подписей.

Проще построить новую безопасную инфраструктуру, чем адаптировать уже существующую к новому безопасному приложению. По этой причине проще конфигурировать и сертифицировать новый выделенный комплекс контролируемых серверов, чем использовать уже существующие интернет-серверы. Консультации по созданию безопасных систем должно предоставлять Управление правительственной связи Великобритании (GCHQ) или надежные поставщики услуг в этой отрасли.

Для систем, эксплуатация которых будет осуществляться в течение длительного периода времени, первоначальный проект должен позволять непосредственно обновлять компоненты в течение указанного срока эксплуатации (например, иметь возможность переключения на узлы сети с более современным оборудованием, обновлять криптографические алгоритмы, которые более нельзя использовать безопасно).

При любом испытании технологии также важно финансировать тесты на проникновение как на уровне системы, так и на уровне пользователя. Реальные хакеры не заинтересованы в экспериментальных концепциях небольшого масштаба, находящихся на уровне тестирования, но при выходе приложений на более крупные масштабы они могут становиться источником угрозы.

Проблемы конфиденциальности

Система криптовалюты Биткойн с самого начала была разработана с возможностью использования псевдонимов5 (разработчик системы Сатоши Накамото назвал это свойство «анонимностью», однако этот термин неверен).

Пользователи могут создавать несколько кошельков для хранения биткойнов, и не существует ни ограничения на число кошельков, которыми они могут владеть, ни требований к процедуре идентификации для входа в кошелек. Биткойны могут переводиться из одного кошелька в другой, а скрытые взаимосвязи между кошельками и реальными людьми обеспечивают некоторую степень конфиденциальности.

Решение о возможности использовать псевдонимы и не привязывать кошельки к реальным людям является практичным для системы Биткойн, и именно оно привело к ее широкому охвату. В большинстве стран отсутствуют надежные способы привязки онлайн-транзакций к реальным людям, следовательно, при наличии такого механизма систему Биткойн не удалось бы развернуть в то время, и сейчас. Более того, с учетом международного характера операций в сети Биткойн непонятно, какая страна могла бы реализовать процесс подтверждения идентификационной информации, и как определить, какая страна имеет право идентифицировать конкретного пользователя с юридической точки зрения.

Наконец, необходимость в идентификации при входе в кошелек может повлиять на свободу обращения биткойнов как валюты: если поставщик идентификационной информации должен участвовать в авторизации транзакций, то он может иметь возможность блокировать их, таким образом избирательно снижая стоимость биткойнов какого-либо пользователя. Другие стороны не могут быть уверены в том, что стоимость биткойнов была бы в безусловном порядке доступна в будущем. Таким образом, «псевдонимность» системы Биткойн обеспечила быстрое распространение (путем ухода от зависимости от существующей инфраструктуры или инфраструктуры фрагментированной идентификации) и сохранила важные аспекты биткойнов как валюты (т. е. статус безусловного средства хранения стоимости).

Однако эти «псевдонимные» отношения между пользователями и кошельками не характеризуются полной или идеальной анонимностью. Входящие и исходящие цепочки транзакций в кошельках и от одного кошелька к другому доступны всем и могут открыто прослеживаться. Сара Мейклджон и ее коллеги из UCL показали, что цепочки транзакций можно проследить по блокчейну Биткойн, например, чтобы связать

случаи воровства биткойнов с конкретными попытками изъять биткойны за счет обменных операций[6].

Этот подход можно использовать для выполнения некоторых правил идентификации пользователей, так как после идентификации адреса конкретного кошелька и его привязки к физическому лицу можно раскрыть все его транзакции.

Эта редуцированная форма псевдонимности в сочетании с прозрачностью транзакций в блокчейне Биткойна действительно представляет собой угрозу конфиденциальности. В отличие от традиционных онлайн-платежей, которые могут видеть только участники транзакции и финансовые учреждения, биткойн-платежи, в том числе участвующие в них кошельки, приблизительное время транзакции и стоимость транзакции, регистрируются в открытом блокчейне. Любой человек может открыть блокчейн и сделать выводы, например, об обороте онлайн-продавца, покупках конкретного пользователя или даже о многих переводах между частными лицами, тогда как ранее эта возможность была доступна лишь финансовыми учреждениями и правоохранительными органами.

Рекомендации по обеспечению конфиденциальности

Для решения проблем конфиденциальности полностью прозрачного блокчейна был предложен ряд методик и альтернативных криптовалют.

Первый комплекс методик включает «смешивание» систем. Оно заключаются в следующем: у нескольких пользователей берутся биткойны и передаются по разным адресам, не связанным с первоначальными пользователями. Это обеспечивает некоторую анонимность за счет разрыва связи между кошельками плательщика и получателя. Тем не менее существуют две основные проблемы с разработкой таких систем. Во-первых, обеспечиваемая ими анонимность не идеальна: несмотря на то что биткойн можно отследить лишь до одного из нескольких адресов, он не скрыт идеально среди всех возможных кошельков в системе Биткойн. Такая частичная утечка информации позволяет приложению для статистических атак де-анонимизировать повторные транзакции посредством там называемых атак статистического раскрытия 7. Степень эффективности этих атак остается под вопросом. Во-вторых, при мошеннических смешиваниях существует возможность принимать биткойны, не выплачивая их, то есть по сути воровать. В ряде проектов по смешиванию биткойнов (например, Mixcoin8) сделана попытка решить эту проблему за счет того, что часть операции по смешиванию становится достаточно прозрачной с целью обеспечить целостность операции, не ставя под угрозу ее конфиденциальность.

Второе семейство систем радикально меняет способ осуществления платежей биткойнами, а также изменяет информацию, фиксируемую в блокчейне, чтобы обеспечить более высокий уровень конфиденциальности. Например, Zerocoin9, Zerocash10, Pinocchio Coin3 или некоторые протоколы Sigma12 для оформления транзакций с криптовалютой используют алгоритмы групповых подписей.

Плательщик предоставляет доказательство с нулевым разглашением о том, что у него есть какие-либо биткойны из списка, но не показывает, какие именно, в то же время раскрывая достаточный объем информации для предотвращения двойных расходов. Это позволяет ему осуществлять оплату биткойнами, не сохраняя полную связь с предшествующими транзакциями. Как и в случае со смешивающими системами («миксерами»), эти методики позволяют лишь прятать получателей платежа в ограниченном списке потенциальных, но не всех, пользователей, что позволяет деанонимизировать множественные транзакции. Тем не менее они надежны с точки зрения целостности и позволяют избегать смешивания как операции с привлечением третьей стороны, которая может стать источником проблем с эффективностью или доверием.

ГЛАВА 5

Разрушающий потенциал

Технологии распределенного реестра (DLT) представляют серьезную проблему для существующих бизнес-моделей и моделей управления. Технические инновации, такие как, технологии DLT, могут открывать возможности для революционных изменений в этих бизнес-структурах, что в конечном итоге приведет к серьезным изменениям принципа организации и управления экономикой и обществом в целом. Такие изменения гораздо более масштабны, чем простые инновации в сфере продуктов, услуг и операционных систем.

Автор
Фил Годсиф, старший научный сотрудник, Суррейский центр цифровой экономики, Суррейская школа бизнеса, Университет Суррея

Глава 5: Разрушающий потенциал

Введение

Технологические инновации могут колоссально повлиять на способы ведения бизнеса. Возможно, новая технология позволит компаниям предлагать новые продукты и услуги, осваивать новые потоки поступления дохода, внедрять более низкозатратные операции и оптимизировать организационные структуры в соответствии с современными требованиями. Если существующие компании адаптируются медленно или пытаются создавать входные барьеры, то новые участники могут использовать инновации, чтобы заменить действующих игроков.

Достаточно радикальные технические инновации могут приводить к революционным изменениям не только в бизнес-моделях или отраслях, но, в конечном итоге, и в принципах организации и управления обществом. Например, изобретение парового двигателя повлекло за собой развитие железной дороги и позволило населению мигрировать в городские центры.

Технологии распределенного реестра (DLT) имеют разрушительный потенциал, не связанный с инновациями в сфере продуктов, услуг, денежных потоков и операционных систем в рамках существующих отраслевых структур. Они могут разрушить экономику и общество в целом. Понимание этого факта поможет нам сформулировать возможности и угрозы, связанные с технологиями

Роль инноваций

Организации постоянно внедряют инновации, чтобы повысить свою конкурентоспособность. Когда мы думаем об инновациях, то, как правило, представляем себе новые продукты и процессы, при этом производственная индустрия фокусируется на инновации по продуктам, а сфера услуг развивается за счет инноваций по процессам. Даже небольшие изменения могут повлиять на структуру отрасли — например, многие производители дисковых приводов не смогли адаптироваться к появлению более легких и меньших по размеру [1]. Инновации также могут быть реализованы в пределах бизнес-моделей. Зачастую они «узаконивают» новые отношения в отрасли с целью формирования кооперативной конкуренции, в рамках которой фирмы одновременно взаимодействуют и конкурируют[2].

Цифровая революция привела к все большему пониманию: инновации могут быть реализованы на уровне бизнес-модели3 и даже на уровне целых отраслей. Вспомните, как приложение Uber, благодаря которому пользователи получили возможность нанимать находящихся поблизости от них водителей, уничтожило таксопарки. Смена ориентации организации с нацеленности на получение краткосрочной прибыли к долгосрочному¬ накоплению капитала может привести к радикальному изменению функций и взглядов на будущее, например, за счет применения программного обеспечения с открытым исходным кодом для создания платформы, которую другие пользователи могут использовать и модифицировать[4].

Такие технологические инновации, как приложения, не позволяют клиентам выступать в качестве ресурса.

FAQ

Каков разрушающий потенциал DLT?

Технологии DLT могут быть весьма разрушительными. Отчасти это связано с разработками, которые они уже позволили реализовать (например, в сфере криптографии и разработки программного обеспечения), отраслями и услугами, в которые они могут привнести инновации (например, финансовые услуги, недвижимость, здравоохранение, управление идентификационной информацией), а также их технологическими свойствами (например, низкой стоимостью, возможностью реализации в реальном времени, неизменяемостью). Но их разрушительный потенциал заключается также и в базовой концепции распределенного согласования, открытом исходном коде, прозрачности и сообществах.

ресурсов, предлагающих решения, а не использующих решения, продвигаемые поставщиками.

Этот факт может поставить под сомнение существующие предположения о создании дополнительной стоимости, например, за счет модели проактивного потребления (в которой одни и те же стороны участвуют в производстве и потреблении; реализуется сервисом совместного использования транспортных средств BlaBlaCar и сервисом аренды жилья Airbnb), социальной ссуды (между физическими лицами) и краудсорсинга. Эта форма инноваций влияет на структуру отрасли и может создавать новые. Она изменяет объекта операции и получателей выгоды4.

Разработки в сфере мобильных платежных систем, которые внедряют новые участники рынка, создают новые клиентские базы (например, позволяя мелким продавцам использовать свой телефон как устройство для считывания банковских карт). Ранее неиспользуемые данные направляются новым участникам для формирования новых потоков получения дохода с целью фиксации ценности. Кроме того, растет использование цифровых кошельков и отправка денежных переводов через различные операционные системы, таких как мобильные операторы (например, M-Pesa), вместо банков. Но во многих из этих случаев лежащие в их основе транзакции все еще обрабатываются традиционными участниками с использованием устаревших систем (например, клиринговыми банками и конкурирующими карточными системами, такими как Visa и Mastercard). Компания M-Pesa поставила под сомнение идею о том, что денежные переводы во время обменных транзакций должен осуществляться через банки, и перепрыгнула несколько стадий развития. Однако эти инновации все же опираются на существующую иерархическую структуру, использование проприетарной (собственнической) технологии и доверенных посредников. Несмотря на то что изменения повышают уровень удобства для клиента и значительно снижают стоимость для пользователей и клиентов, все же это эволюция, а не революция.

Технологические революции

Как правило, инновации выходят на арену постепенно, при этом их оттеняют радикальные эпизоды, которые экономист Йозеф Шумпетер назвал «творческим разрушением», а Карлота Перез — «технологическими революциями»5. Такие инновации существуют в динамичном комплексе с технологией, экономикой и обществом, а порой инновация может принципиально изменять уклад конкретного общества или способ организации экономики.

За несколько прошедших веков мы видели множество технологических революций — например, первая промышленная революция, железнодорожная революция и нефтяная революция. Каждая из них изменила отраслевую структуру, способствовала появлению новых форм энергии и повлияла на уклад общества (см. таблицу 1). В настоящее время мы являемся свидетелями информационно-телекоммуникационной революции, для которой характерна информационная интенсивность, взаимосвязанность, специализация и глобализация.

Как правило, такие революции основаны на трех «китах» — существенно более низкая стоимость, новые способы коммуникации и изменение инфраструктуры и логистики.

Снижение затрат на получение входных данных приводит к созданию напряжения на рынках и — зачастую — к формированию финансовых пузырей и кризисов, что, в конечном итоге, требует капитальной перестройки существующих институтов. По мнению Перез, революционные инновации характеризуются «комплексом взаимосвязанных фундаментальных "прорывов", формирующих группу взаимозависимых технологий» и «сильной взаимосвязанностью участвующих систем в соответствующих технологиях и рынках, а также способностью в корне преобразовать остальную экономику (и, в конечном итоге, общество)»[5].

	Описание	Год ((прибли-зительно)	Новые технологии и отрасли	Новые инфраструктуры	Принципы "здравого смысла"
1й	Промышленная революция	**1770**	Механизация промышленности	Каналы и водная энергия	**Фабричное производство, продуктивность, локальные сети**
2й	Пар и железные дороги	**1830**	Паровые двигатели, железные механизмы	Железные дороги, телеграф, порты	**Экономика агломерации, стандартизованные запчасти, урбанизация**
3й	Сталь, электричество, тяжелое машиностроение	**1875**	Дешевая сталь, химия тяжелых элементов	Электрические сети, глобальные перевозки	**Экономика масштаба и вертикальной интеграции, наука как двигатель производства, эффективность**
4й	Нефть, автомобиль, массовое производство	**1910**	Автомобили, дешевая нефть, нефтехимический синтез, бытовые приборы	Автодорожные сети, всеобщая электрификация	**Массовое производство, горизонтальная интеграция, стандартизованные продукты, энергоемкость, субурбанизация**
5й	Информация и телекоммуникации	**1970**	Дешевая микроэлектроника, компьютеры, мобильная телефония	Всемирные цифровые коммуникации	**Информационная интенсивность, децентрализованные сети, знание как капитал, экономика специализации, глобализация**

Таблица 1. Пять технологических революций (по материалам Перез[5])

Каждая технологическая революция приносит с собой разные системы «принципов здравого смысла», которые изменяют способ ведения бизнеса и функционирования общества. Мы перешли от механизации на фабриках, через экономику масштаба и вертикальную интеграцию, массовое производство и стандартизацию, к функциональной специализации, иерархическим пирамидам и бюрократии, а затем к сегодняшней информационной интенсивности и децентрализованным сетям, для которых типична «гетерогенность, разнообразие, возможность адаптации и взаимодействие»5. В конечном итоге эти революции ведут к созданию новой технико-экономической парадигмы с разными структурами стоимости, разными возможностями для проведения инноваций и организациями, построенными по существенно отличающимся принципам. В рамках каждой парадигмы организации развиваются в соответствии с S-образной кривой от разрушительных инноваций через применение и эксплуатацию (и сопротивление) к зрелости и, в конце концов, замещению5. Изменение такого образа мышления и его замещение на новый требует трансформационного сдвига, для которого необходимы новые навыки, способности и знания, которые принципиально изменяют способ ведения бизнеса.

Технологические революции прошлого влияли в малой степени или вовсе не влияли на пирамидальные иерархические системы организации и управления. Однако некоторые предполагают, что в теории наша новая технологическая эра допускает появление принципов коллективного использования общих ресурсов, в соответствии с которыми общество руководствуется коллективными интересами, а не индивидуальной выгодой6. Они могут иметь ввиду распределенные согласованные структуры сообществ, которые не зависят от иерархически организованных посредников (таких как банки или правительства). Технологии DLT представляют собой именно такую проблему.

Технология распределенных реестров

Технологии DLT являются частью потенциально революционных инноваций в ряде смежных областей — виртуальных валют, распределенного открытого и прозрачного делопроизводства, неиерархических сетевых систем, криптографии и разработки программного обеспечения. DLT — это инновация со стороны «радикального конца» спектра изменений, так как они способны повлиять на множество сфер в бизнес-модели — от новых продуктов и услуг через операционные системы и организационные структуры, до огромного множества потенциальных отраслей. Таким образом, они являются компонентом взаимосвязанных и взаимозависимых «прорывов», которые и составляют технологическую революцию.

Технологии DLT предлагают значительные преимущества с точки зрения операционных затрат. Они не просто низкозатратны по своей сути, но еще и позволяют избегать дублирования и неэффективности при контроле и координации, предоставляя общий открытый реестр, который может функционировать на уровне отрасли,

ПРАКТИЧЕСКИЙ ПРИМЕР 1

АЛМАЗЫ

Лиэнн Кемп, основатель и генеральный директор Everledger

В алмазной индустрии широко распространена криминальная деятельность. Камни имеют небольшой размер, поэтому их легко секретно перевозить, транзакции, как правило, проводятся конфиденциально, а алмазы сохраняют свою стоимость в течение многих лет. По этой причине алмазы используются в отмывании денег и финансировании терроризма во всем мире.

Попытки нейтрализовать противоправную деятельность включали отслеживание алмазов по бумажным документам, подтверждающим их происхождение. Но подделка документов очень распространена. Действительно, иногда для прикрытия нелегальных транзакций документы фабрикуются, а в ряде стран, являющихся крупными участниками алмазной индустрии, действующее законодательство в достаточной степени не защищает от такого рода преступлений.

Для борьбы с преступностью в алмазной индустрии начинается развертывание системы Everledger, основанной на технологии блокчейна, которая создает цифровой «паспорт» для каждого алмаза. Система регистрирует его происхождение, перемещения и транзакции с помощью уникального криптографического «отпечатка пальца».

Система включает три стадии:

- Установление e-ID (электронной идентификационной информации) для каждого алмаза посредством оцифровки его характеристик и выгравированного лазером серийного номера в блокчейне авторизованного реестра.
- Присвоение алмазу цифрового паспорта для регистрации его перемещений, истории транзакций и происхождения.
- Обнаружение и защита от нелегальных или мошеннических действий.

Используя неизменяемый блокчейн для хранения этих данных, реестр может обеспечивать прозрачность информации обо всех алмазах, раскрывая их происхождение, историю владения и виды выполненной обработки. Этот реестр может быть единственным способом получить подтверждаемые сведения об алмазах для индустрии, правительственных учреждений, потребительских рынков, пограничного контроля и правоохранительных органов.

Эта система также позволяет использовать смарт-контракты — положения и условия, связанные с продажей и транспортировкой алмазов, которые могут приводиться в исполнение автоматически. При использовании блокчейна для создания распределенного реестра можно прослеживать и использовать смарт-контракты для подтверждения деловых отношений и соглашений. Прозрачность блокчейна — это один из способов принудительного исполнения контракта независимо от причины (смена владельца алмаза, приобретение алмаза, реализация его страхового полиса, регистрация титула и т. д.). Авторизация транзакции вместе с документальным подтверждением подлинности позволяет оставить актуальный доказательный «шлейф» для правительства и правоохранительных органов.

уровень, тем самым снижая системные затраты, связанные с такими процессами, как перекрестная проверка в отдельных реестрах и базах данных. Возможность оцифровывать и надежно хранить информацию практически о любом активе — от алмазов до мешков с рисом — позволяет организациям идентифицировать и отслеживать их владельцев и местоположение (см. практический пример по подтверждению подлинности алмазов, с. 56). На основе DLT разрабатываются новые способы фиксации обязательств и перевода стоимости с использованием программируемых контрактов, например, Ethereum — децентрализованная платформа для смарт-контрактов (см. главу 1). Их разрушительный потенциал может даже простираться на новый ландшафт, в котором доверенные или обязательные посредники, действующие в условиях иерархической монополии (модель веерной структуры), объединяются или заменяются на более открытую и плоскую согласованную структуру, основанную на сообществах (см. практический пример по корпоративным сделкам, с. 58).

Разработка DLT и сопутствующих технологий также позволяет регистрировать транзакции и обеспечивать доступ в реальном времени, что делает транзакции более быстрыми и дешевыми (см. практический пример по SETL, с. 60). Например, автотранспортная страховка может быть основана на состоянии как автомобиля, так и его водителя, при этом условия страховки у разных поставщиков меняются в зависимости от поведения, цены и склонности к риску. Такая возможность может привести к созданию «программируемой экономики», включающей смарт-контракты, которые базируются на децентрализованных сетях и агентах, требующих меньшего внимания людей, и функционируют как распределенные автономные организации, предлагающие широкий ассортимент продуктов и услуг.

FAQ

Какие угрозы возможны в связи с использованием технологий DLT?

Как и любые радикальные инновации, технологии DLT открывают возможности действующим игроками, и создают угрозы для тех, кто неспособен или не сможет совладать с ними. В силу их природы распределенного согласования, они также угрожают занять роль доверенного посредника внутри иерархических контролирующих структур. Блокчейны, непосредственно создающие новую валюту, такую как Биткойн, ставят под сомнение текущее верховенство правительств в сфере управления национальной и международной экономикой и валютной системой.

Лучшим примером использования технологии DLT является криптовалюта биткойн, а самой очевидной областью для проведения инноваций в виде появления новой валюты является сфера финансовых услуг. Технологии DLT обеспечивают более низкую стоимость эксплуатации в рамках существующих структур и моделей управления, а также позволяют снижать затраты и уровень сложности в масштабе всей системы. Этого можно достичь за счет устранения дублирования и затрат на множество отдельных проприетарных систем, а также за счет кардинального изменения централизованных архитектур этих систем. Например, выпуск денег перестал быть единоличной ответственностью или прерогативой национальных правительств. Наоборот, там, где идентификационная информация и связи между людьми становятся средством подтверждения и подписания транзакций в пределах сообщества[7], могут появляться новые виды валюты.

Дальнейшая разработка, которая стала возможной благодаря технологическим достижениям, позволяет добавлять конкретную атрибутивную информацию (например, о физических активах или контрактах) к базовым биткойнам, получая в итоге «маркированные биткойны». Это открывает возможность существования денег, которые имеют больше характеристик, нежели просто стоимость: они могут иметь такие атрибуты, как обязательная цель, срок действия или место допустимого использования. Например, на деньги могут быть наложены ограничения по типу продуктов и услуг, на приобретение которых они могут быть направлены (см.главу 6), или же у человека, арендующего квартиру через сервис Airbnb, можно отозвать ключ электронного доступа, если он опоздал с оплатой или если завершился срок действия контракта.

Информация к размышлению для правительства

В связи с огромным спектром участников, услуг и ролей, правительства, несомненно, ведут целый ряд различных видов деятельности. Некоторые из них скорее распространяют ценности, нежели создают их, а другие создают и поддерживают эффективные системы регулирования. Многие из этих видов деятельности будут усовершенствованы за счет инноваций, доступных благодаря технологиям DLT, другие окажутся под угрозой. Изменения возможны на уровне продуктов и услуг, а также на операционном и организационном уровнях.

ПРАКТИЧЕСКИЙ ПРИМЕР 2

Корпоративные сделки

Доминик Хобсон, основатель COOConnect

Публичные компании обязаны предоставлять годовые отчеты в структурированном формате, однако сообщения компаний, которые могут потребовать действий со стороны инвесторов или их представителей - известные как корпоративные сделки - обычно публикуются как неструктурированный текст, или в формате PDF. Они основываются на информации и перед проведением действий им приходится читать и интерпретировать данные вручную.

Более 90% корпоративных сделок распределяются поставщиками информации (вендорами), а затем проводятся от имени инвесторов агентами, такими как финансовая организация или фондовый менеджер. Информация вручную извлекается из оригинала, интерпретируется и расшифровывается вендорами. Уровень автоматизации низок, ошибки происходят часто, и весь процесс является крайне неэффективным. По одной из оценок глобальные затраты на проведение корпоративных сделок составляют до $10 млрд. в год. Финансовые институты часто возмещают расходы клиентов в связи с отсутствием или некорректным следованием инструкциям.

Технология "блокчейн" может сделать этот процесс более эффективным. Корпоративные сделки являются разновидностью договорной информации или ценности, которые в принципе могут проводиться напрямую между плательщиком и получателем платежа без необходимости в посредниках, при условии, что стороны могут доверять исходным данным и имеют необходимый опыт проведения действий по полученной информации.

Если бы блокчейн была объединена с приложением, которое собирает и хранит объявления о корпоративных действиях в структурированном формате, ее можно было бы использовать для подтверждения того, что данные получены из проверенного источника, а также чтобы убедиться за счет наличия временных меток, что они были опубликованы. Также это может быть сделано и в обратном порядке для выпуска инструкций. Распределенные реестры, построенные на таких блокчейнах будут гарантировать сторонам по всем вопросам в ходе процесса, что их информация точна, актуальна и неизменна с тех пор, как была опубликована эмитентом.

Теоретически, они могут исключить всех посредников между эмитентом и фондовыми менеджерами, гарантируя точность и актуальность информации.

Важный вопрос: может ли это быть организовано полностью децентрализованно. Данные о корпоративных сделках отличаются от более простых договорных данных (таких как о переходе денежных потоков), так как инвесторы и акционеры зачастую нуждаются в посредниках со специальными знаниями, чтобы совершать действия от их имени.

Посредникам может понадобиться изменить или дополнить данные перед совершением действий, и исходные корпоративные сделки могут измениться за счет последующих уведомлений, которые заменяют собой более ранние. Эти видоизмененные данные могут быстро терять связь с источником происхождения, так как вендоры делятся ими с клиентами и объединяют их с другими данными, затрудняя процесс автоматизации.

Сама по себе технология блокчейн в настоящий момент слишком медленная, чтобы справиться с этими постоянно перемещающимся пакетами данных. Блокчен Биткойна может выдержать около 20 000 транзакций в час, с периодом ожидания одобрения транзакции до 1 часа. Это неудобно для процесса корпоративных сделок, у которого есть определенный дэдлайн, который фондовый менеджер предпочитает держать открытым как можно дольше.

К примеру, процесс обеспечения того, что финансовые перечисления, такие как платежи в рамках социального обеспечения, "уйдут" правильному человеку в правильное время, может быть улучшен несколькими путями (смотри Главу 6). Единый реестр, содержащий идентификационные данные и данные о выплатах потенциальным заявителям, обновляемый в режиме реального времени, может стать кардинальной инновацией, более эффективной и уменьшающей одновременно и операционные расходы, и расходы на модернизацию. Добавление атрибутов к определенному платежу может означать, что также как и сумма, могут быть определены и отслежены и цели, и график расходования. Это, конечно, потребует широкомасштабных переговоров с участниками рынка, и, возможно потребует некоторого управления данным видом валюты для обеспечения желаемого паритета с фунтом стерлинга.

Компания Codel с штаб-квартирой в Монмут, которая работает с данными о корпоративных сделках, обошла эти ограничения за счет комбинирования системы блокчейн с программным обеспечением "цифровой нотариус". Эта система создает непрерывно обновляемый журнал регистрации событий, на который стороны по всей цепочке могут ссылаться, чтобы установить подлинность, что дает ценное подтверждение источника происхождения данных.

Наряду с Мгновенными Действиями, это создает новый удобный для поиска централизованный реестр данных о корпоративных сделках, который является совместным проектом участников рынка и Codel. Данные реестров хранятся в форматах ISO 15022 и ISO 20022, которые обеспечивают методологию перевода финансовой информации в машинно-считываемый формат. Это означает, что реестры могут быть обновлены по мере изменения или удаления данных о корпоративных сделках. Это гарантирует целостность и точность информации, которую можно затем сделать доступной всем сторонам цепочки корпоративных сделок через защищенную сеть SWIFT. Это решает вопрос задержки верификации, который существует при использовании блокчейн самой по себе. Также становится возможным обновление, распространение и изменение информации - эффективно передаваемой как распределенный реестр - в режиме реального времени с гарантией точности и актуальности.

Правительство могло бы помочь подобной системе "расцвести" за счет законодательно закрепленного требования для компаний выпускать информацию о корпоративных сделках с использованием принципа распределенного реестра.

Существуют инновационные возможности замещения иерархических организаций более распределенными системами. Правительства и их учреждения как правило имеют уровни власти, как внутренние, так и в пределах соответствующих систем: например, граждан представляют представляют выборные должностные лица, как в местных, так и национальных и надгосударственных институтах; финансовая деятельность вовлекает клиринговые банки, клиринговые организации, центральные банки и правительства. Вместо того, чтобы зависеть от периодически повторяющегося процесса голосования, в основе которого чаще всего лежат бумажные записи, демократия могла бы опираться на блокчейны для голосования, для чего электорат получил бы электронный кошелек и "голосовую монету".

Это потенциально может уменьшить подтасовки (так как каждый избиратель может проверить, был ли засчитан его голос), а также положить начало демократии в режиме реального времени, с возможность устроить голосование по любому вопросу. Это поднимает важные вопросы социальной ответственности и готовности принимать участие, но может создать более распространенные формы демократии.

Угрозы

Инновации, доступные, благодаря технологиям DLT, могут быть очень привлекательными, но это не значит, что они не создают серьезных угроз, в том числе связанных с природой денег, ролью иерархий и доверием.

ПРАКТИЧЕСКИЙ ПРИМЕР 3

SETL'ирование транзакций

Доминик Хобсон, основатель COOConnect

Услуги клиринга, заключения сделок, депозита или регистрации - создают существенное дополнительное бермя расходов при выпуске, торговле и владении ценными бумагами. Существует огромное множество специализированных агентов и контрагентов, задействованных при движении ценных бумаг и денежных потоков между инвесторами. За эти услуги берутся существенные комиссии, но также дополнительные издержки возникают в связи с необходимостью взаимодействия с мириадами различных систем, которые должны быть связаны и интегрированы с бизнес-процессами. В общей сложности, мировая финансовая индустрия тратит от $65 до $80 миллиардов в год на расчетно-клиринговые операции.

Технология блокчейн позволяет значительно снижать степень сложности и стоимость таких расчетно-клиринговых услуг за счет того, что участники используют общий реестр, который хранится на множестве серверов, выступающих в роли узлов. Полномочия для совершения транзакции предоставляются посредством криптографии открытых/личных ключей.

Транзакции добавляются в базу данных блоками, и каждый блок анализируется узлами. Блок добавляется в базу данных только если узел находит подтверждение, что блок содержит только корректные транзакции. За исключением настройки и администрирования узлов, такая сеть блокчейна должна быть полностью автономной и не требует наличия контролирующего или регулирующего участника.

Решение SETL

Целью венчурного проекта с частным финансированием SETL является разработка и реализация специализированного блокчейна, который позволит участникам финансового рынка совершать одноранговые транзакции с ценными бумагами и использовать распределенный «золотой» реестр ценных бумаг и денежных средств. В частности,
целью SETL является обеспечение доступности денежных средств центрального банка в блокчейне. Блокчейн проекта будет функционировать автономно и интегрироваться с текущими финансовыми рынками, платежами и биржевой нфраструктурой.

Проект SETL сможет работать как с ценными бумагами, так и с денежными средствами во время каждой транзакции и будет также разрешать односторонние переводы ценных бумаг и денежных средств в виде простых платежей или в целях заключения индивидуальных контрактов, проведения корпоративных сделок, начисления дивидендов и выдачи купонов.

Проект SETL будет разработан так, чтобы «ужать» дорогостоящий и рискованный процесса клиринга и заключения сделок до ¬процесса заключения сделок между участниками в реальном времени. Кроме того, за счет формирования «золотого» реестра владельцев SETL позволит существенно снизить накладные расходы на регистрацию и хранение ценных бумаг.

Блокчейн SETL будет иметь следующие характеристики:

- Используемые в блокчейне SETL открытые ключи потребуется подписывать в центре сертификации, чтобы пользователи блокчейна могли видеть, кто сертифицировал каждый ключ. Центры сертификации будут хранить подробные реальные идентификационные данные пользователей открытых ключей и проводить проверки на предмет отмывания денег и соблюдения процедуры идентификации. В проекте SETL предполагается, что центр сертификации будет при необходимости раскрывать эту информацию в случаях, предусмотренных законодательством.
- Проект будет обладать возможностями, достаточными для обработки тысяч транзакций в секунду, что сопоставимо с обычными объемами сделок на финансовых рынках.
- Он будет иметь возможность обрабатывать множество классов активов, в том числе денежные средства и ценные бумаги любых типов.
- Проект позволит осуществлять транзакции с подписями нескольких лиц, допуская авторизацию указанным подмножеством пользователей.
- Он позволит осуществлять «атомарные транзакции» (т. е. когда осуществляются либо все транзакции, либо ни одна из них), так что

Технологии DLT могут разрушить традиционные финансовые институты, основная сфера деятельности которых связана с денежными средствами и переводами. Однако деньги сами по себе подвергаются разрушительному воздействию во всех своих формах и видах благодаря использованию криптовалют, такик как биткойны, выдуманные деньги, не поддерживаемые правительством, и «маркированные монеты», которые позволяют денежным единицам проводить различные виды применения.

транзакций и будут обработаны только в том случае, если все стадии были подтверждены и надлежащим образом авторизованы.

- Проект будет обладать специализированной функциональностью, цель которой — упростить для участников управление ликвидностью.
- Он будет осуществлять полную регистрацию транзакций и балансов в исторической последовательности в для упрощения ведения нормативного делопроизводства, отчетности о транзакциях и проведения аудита.

Больше преимуществ

В настоящее время денежные средства и другие активы, как правило, хранятся в специальных системах и могут использоваться только для определенных целей. Иными словами, они зависят от системы. В противоположность этому, деньги и активы, хранящиеся в блокчейнах, можно использовать для любых целей. Эта особенность позволит снизить объем средств, которые банки должны размещать в резервах ликвидных активов, и упростить для них управление ликвидностью.
Предполагается, что проект SETL сможет предложить решение, которое будет работать наравне с уже существующей системой валовых расчетов в реальном времени (RTGS)Центрального Банка Великобритании, обеспечивая безопасную и жизнеспособную альтернативу в те моменты, когда RTGS недоступна. Проект SETL будет доступен всегда, что снижает межбанковские¬ риски, аккумулируемые в периоды, когда RTGS не работает, например, ночью и по выходным.
Система платежей и совершения сделок SETL будет простой, унифицированной и оперативной. Если Великобритания будет первой страной, развернувшей такую систему, то это позволит Лондону и фунту стерлингов стать местом и валютой выбора при оказании финансовых услуг. Существует вероятность, что после развертывания в Лондоне система будет использоваться более активно, еще больше укрепляя положение Лондона как мирового лидера в сфере международных финансов.

Управление денежными средствами средствами, а через них и экономикой, рассматривается многими как основная роль правительства, поэтому альтернативные валютные системы могут представлять угрозу.

Технологии DLT представляют угрозу для любой иерархической структуры, так как они позволяют соединяться и работать в распределенной сети без доверенных или обязательных посредников, замещая нисходящий контроль согласием. Иерархии могут обладать серьезными недостатками: дублирование, дополнительные расходы, возможности потенциального злоупотребления властью и финансовых манипуляций. Тем не менее у иерархий есть и преимущества, когда необходима помощь нейтрального брокера и, например, в представительской демократии.

Представительская демократия обеспечивает стабильность и поступательный процесс гражданской власти, но более масштабное использование технологий DLT может ставить ее под угрозу. Страны уже столкнулись с угрозами, вызванными глобализацией и размыванием границ, а между тем некоторые из первых разработчиков и сторонников системы Биткойн поддерживают крайне антиправительственные взгляды. Сложно будет обеспечить, чтобы технологии DLT и сопутствующие инновации были направлены на объединенное продуктивное общество на базе благоприятной инфраструктуры.

Заключение

Сплав творчества и технологий может привести к радикальным изменениям существующих бизнес-моделей и организационных структур, в рамках которых они функционируют. В настоящее время технология DLT поднимает столько же проблем и вопросов к существующим структурам, сколько предлагает ответов и практических возможностей. Но, похоже, она обладает по меньшей мере некоторыми свойствами, которые в надлежащем контексте вызовут волну изменений в более революционном конце спектра.

Технологии DLT несут существенные проблемы для традиционных организаций и предлагают такие условия передовой практики, которые выходят далеко за пределы области регистрации транзакций и реестров. Такие потенциально революционные организационные структуры и практики должны быть экспериментально апробированы, возможно, в форме технических и нетехнических демонстрационных проектов, чтобы мы могли изучить практические, юридические и политические последствия.

Радикальные инновации в бизнес-моделях, в особенности в структурах и операционных системах, могут происходить за счет экспериментирования в расслабленной, но эффективной нормативно-регулирующей обстановке. Правительство должно продумать, как нормативная база может наилучшим образом стимулировать и извлекать преимущества в ситуации, позволяющей изучать такие низкозатратные операционные модели и организационные структуры, при этом обеспечивая свободное участие новых игроков.

Необходимы дополнительные исследования на уровне системы по финансовым затратам и преимуществам внедрения технологии распределенного реестра. Они позволили бы правительству определить, каких имеющихся временных затрат можно избежать и где искать остальные возможности и способы экономии.

ГЛАВА 6

Применения в государственном управлении

Технология распределенного реестра уже основательно повлияла на управление данными и взаимодействие с клиентами и поставщиками в частных компаниях. Применение технологии в правительстве позволит снизить затраты, повысить прозрачность, улучшить финансовую вовлеченность граждан и стимулировать проведение инноваций и экономический рост. В данной главе представлены пять практических примеров, иллюстрирующих эти преимущества.

Автор

***Кэтрин Маллиган**, научный сотрудник, Имперский колледж Лондона, и руководитель подразделения цифровой стратегии и экономики в компании Future Cities Catapult. Также принимали участие Саймон Тейлор, вице-президент по НИР по технологии блокчейн, Barclays, и Майк Халсалл, группа по изучению глобальных проблем, Университет сингулярности, научно-исследовательский парк NASA, штат Калифорния, США.*

Глава 6:
Применения в государственном управлении

Введение

Технологии распределенного реестра (DLT) способны гораздо на большее, нежели простое управление цифровыми валютами, такими как Биткойны. Идеи и структуры, созданные для распределенных реестров, а также используемые ими блокчейны очень мобильны и могут распространяться на другие сферы экономики и социальной деятельности. По этой причине существует возможность их использования в работе правительства. Действительно, потенциальное воздействие технологий DLT на британское общество может быть столь же значимо, как воздействие фундаментальных событий — например, подписание Великой хартии вольностей[1].

При надлежащем использовании и принятии мер по вопросам конфиденциальности, безопасности, идентификации и доверия распределенные реестры создают интересные возможности для правительства и других локальных и региональных органов власти следующим образом:

- Снижение стоимости операций, в том числе уменьшение мошенничества и количества ошибок при платежах.
- Более высокая прозрачность транзакций между правительственными учреждениями и гражданами.
- Более высокая финансовая вовлеченность людей, которые сейчас находятся на периферии финансовой системы.
- Снижение расходов на защиту данных граждан за счет обеспечения возможности совместного использования данных с разными субъектами, что позволяет создавать информационные биржи.
- Защита критически важной инфраструктуры — мостов, туннелей и т. д.
- Снижение «рыночного трения», что облегчает взаимодействие малого и среднего бизнеса (SME) с местными и национальными органами власти.
- Стимулирование инноваций и экономического роста для среднего и малого бизнеса.

Такой весьма широкий диапазон потенциальных преимуществ реализуется за счет применения технологии DLT тремя способами:

- В приложениях, работающих с валютами.
- Для управления контрактами и создания новых типов контрактов.
- Для содействия разработке новых приложений третьими сторонами и предоставления более эффективных способов структурирования и осуществления деятельности.

В пяти практических примерах, представленных в настоящей главе, будет проиллюстрирована каждая из этих возможностей и варианты их применения в виде разных технических решений:

- Защита критически важной инфраструктуры от кибератак.
- Снижение операционных расходов и отслеживание прав на получение социальной поддержки с одновременным расширением объема финансовых услуг.
- Прозрачность учета и возможность отслеживания средств, выделяемых на помощь.
- Создание возможностей для экономического роста, развития мелкого и среднего предпринимательства и роста занятости.
- Сокращение налогового мошенничества

Пример 1: Защита критически важной инфраструктуры

Обзор

Технологии распределенного реестра (DLT) позволят Великобритании и правительству страны обеспечить более надежную защиту критически важной гражданской инфраструктуры от кибератак.

Освещение проблемы

Цифровые технологии все шире внедряются в критически важные инфраструктуры разных стран, и доступ ко многим из этих систем осуществляется через Интернет. Это подвергает их риску возможных атак со стороны хакеров или других государств, которые могут остаться не идентифицированными за счет использования существующих ресурсов кибербезопасности. Например, возможен злонамеренный перехват управления критически важными сетевыми маршрутизаторами с целью получения полного контроля и возможности манипуляций. Это позволило бы перехватывать данные всех компаний и правительственных организаций, защищенных межсетевыми экранами маршрутизаторов. Более того, по мере внедрения различных встраиваемых технологий в гражданскую инфраструктуру, - в том числе, мосты, железные дороги, туннели, дамбы для защиты от наводнений и энергетические установки - шансы нанесения значительного материального ущерба и повышения рисков для жизни людей существенно возрастают.

Возможности технологий DLT

Применение технологий DLT позволит исключить внесение несанкционированных изменений в операционную систему и встроенные микропрограммы. Распределенный реестр позволяет отслеживать состояние и целостность программного обеспечения и выявлять несанкционированные изменения, а также блокировать несанкционированный доступ к данным, передаваемым в системах, где применяются технологии "Интернет Вещей" (IoT).

Результаты

- Повышение эффективности и результативности крупномасштабной инфраструктуры, снижение рисков для жизни человека.
- Обеспечение целостности данных, передаваемых и принимаемых критически важной инфраструктурой.

Уровень зрелости

Готовность

Пример 2: Министерство труда и пенсионного обеспечения

Обзор

Применение новейших моделей оплаты позволит Казначейству Ее Величества и Министерству труда и пенсионного обеспечения более эффективно распределять средства социальной поддержки и улучшить ситуацию со страховыми полисами. Применение технологий DLT в процессах регистрации и оплаты при распределении государственных субсидий и льгот позволит Министерству труда и пенсионного обеспечения более эффективно:

- Предотвращать финансовые потери из-за мошенничества и ошибок.
- Оказывать поддержку наиболее социально незащищенным гражданам, предлагая полный спектр финансовых услуг.
- Содействовать правительству в реализации более масштабных планов развития, в частности, оказывая непрерывную поддержку малоимущим в целях улучшения их уровня благосостояния.
- Наиболее выгодно вкладывать инвестиции и добиваться стабильности управления государственными расходами.

Освещение проблемы

Ежегодно Министерство труда и пенсий Великобритании выплачивает на социальную поддержку около 166 млрд. фунтов стерлингов из налоговых поступлений. Из этой суммы около £3,5 млрд переплачивается из-за мошенничества (£1,2 млрд), ошибок заявителей (£1,5 млрд) и ошибок со стороны официальных органов (£0,7 млрд)[2], из которых вернуть удается только £930 млн. С учетом мошенничества и ошибок, имеющих место в текущей налоговой кредитной системе, которая в течение ближайших нескольких лет станет элементом нового режима Универсального кредитования Министерства труда и пенсий, ежегодный валовой объем переплат только по основным показателям превышает £5 млрд.

Помимо прямых финансовых затрат в связи с переплатой средств лицам, не имеющим на то прав, налогоплательщик также несет затраты и после выплат (взимание задолженностей, расследование и судебное преследование, урегулирование споров и запросов заявителей).

Кроме этого, не представляется возможным отследить движение части средств на социальную поддержку, пока что не поддающихся количественному учету, в рамках реализации запланированных программ. Например, возможно эффективное финансирование затрат заявителями, аналогичному тому, как распределяются средства на социальную поддержку. В конечном итоге это позволит обслуживать небанковские долговые обязательства и выплачивать ‘пособия для малоимущих’[3].

Возможности технологий DLT

Значительное число заявителей на получение пособий не пользуются банковскими услугами, или пользуются ими в недостаточном объеме4, либо сталкиваются с барьерами в получении дополнительных финансовых услуг, такими как проверки кредитоспособности, доступность традиционных финансовых продуктов, и стоимость несанкционированных транзакций. Технологии DLT предлагают недорогое и удобное средство вовлечения таких заявителей в систему социальных льгот.

Цифровая идентификация может проходить в распределенных реестрах, работающих на устройствах с безопасным шифрованием- либо даже в программе на мобильном устройстве. Это позволит конечным пользователям получать пособия напрямую при меньших транзакционных издержках в пользу банков или местных органов власти. Это позволило бы им стать более вовлеченными в систему финансовых операций, совершаемых через безопасный распределительный узел, более надежный, чем банковский счет. Такое решение можно было бы привязать к другими системам в целях снижения уровня мошенничества или ошибок официальных органов в процессе перечисления пособий, так как подделка цифровых идентичностей намного сложнее.

Такие операции могли бы помочь Министерству труда и пенсий Великобритании в достижении одной из важнейших целей: неуклонно выводить людей из цикла бедности и снижать зависимость от государства. Такие инновационные технологии позволили бы - с согласия конкретного заявителя - задавать правила совершения транзакций в рамках социального обеспечения как на уровне получателя, так и на уровне отправителя. Это дает возможность министрам рассматривать различные стратегии более эффективного распределения средств на на социальную поддержку за счет согласования или выработки правил использования социальных выплат.

Результаты

- Сокращение потерь от мошенничества и ошибок со стороны официальных органов.
- Возможности для министров более эффективно распределять государственные средства, поступающие от налогоплательщиков, в пользу действительно нуждающихся.

Уровень зрелости

- Требуется высокий уровень образования получателей.
- Требуется некоторая интеграция фунта стерлингов в систему распределенного реестра социальных выплат.
- Может привести к образованию отдельной экономики с сомнительной репутацией "экономики льготных купонов".

Пример 3: Укрепление системы международной помощи

Обзор

Технология DLT позволит правительству более четко управлять распределением международной помощи и гарантировать получение средств законными получателями. Это также позволит министрам улучшить прозрачность и обеспечить эффективное финансовое управление. Применение технологии DLT таким образом позволило бы популяризировать международный вклад Великобритании в достижение поставленных глобальных целей.

Освещение проблемы

Для выполнения глобальных обязательств страны должны поддержать планы действий по реализации Глобальной Цели, включающие в себя меры по обеспечению прозрачности, финансовой ответственности и целостности информации5. Международные доноры уделяют особое внимание обеспечению большей прозрачности и стабильности систем оказания помощи. Мероприятия по борьбе с мошенничеством, кражами и незаконным¬ присвоением средств могут оказаться дорогостоящими. Внедрение технологических новшеств может значительно усилить превентивные меры и расширить масштабы помощи.

Мошенничество и коррупция не способствуют снижению уровня бедности, приводят к сокращению притока иностранных инвестиций, и в значительной мере вызваны низким уровнем академической успеваемости. Это в свою очередь открывает отличные возможности для применения технологий DLT в целях обеспечения прозрачности и возможности отслеживания финансовых потоков в рамках оказания международной помощи. Гарантия добросовестного расходования средств могла бы подтолкнуть целые страны жертвовать больше, а всех финансовых доноров к более активному участию в достижении поставленных ключевых целей.

Возможности технологий DLT

Главное преимущество технологий DLT заключается в трех основных аспектах. Во-первых, эти технологии позволяют донорам международной финансовой помощи выпускать монеты, привязанные в денежном выражении к фунту стерлингов, минуя многочисленные бюрократические препятствия традиционной банковской сферы. В среде распределенных реестров эта цель достигается благодаря отсутствию географических границ — реестры работают одинаково в любой юрисдикции по всему миру.

Таким образом открывается возможность значительно снизить размеры комиссий за обмен валют при оказании международной финансовой помощи до уровня ниже стандартных операционных издержек. Более того, возможность составлять смарт-контракты может использоваться для “заключения самопринудительных соглашений между незнакомыми лицами, которые обеспечат гражданам основу для совершения операций независимо от законодательной и исполнительной власти в своей стране”6.

Во-вторых, доноры международной финансовой помощи смогли бы, используя преимущества технологий DLT уменьшить взаимозаменяемость наличных денег за счет надежности и безотзывности перемещения цифровой продукции — в данном случае, предоставления финансовой помощи. Кроме того, с помощью цифровых реестров можно решить проблему двойного расходования средств: если в цифровых валютах конечные пользователи могут тратить одну и ту же валютную единицу дважды, то в цифровых реестрах такая возможность блокируется, поскольку каждая "монета" уникальна. Благодаря этому становится возможной оплата без посредников6. В тех случаях, когда финансовая помощь адресована конечным получателям, можно обойти ограничения и лимиты на некоторые валюты и банковские услуги в отдельных странах за счет одноранговой (пиринговой) передачи финансовых средств.

В-третьих, использование уникальных монет, привязанных к фунту стерлингов, позволило бы исключить их расходование на оплату товаров и услуг, не разрешенных в контексте международной финансовой помощи. Например, денежные средства, направленные на создание инфраструктуры для снижения уровня бедности, не могут быть потрачены на другие цели. Это возможно за счет способности технологий DLT точно отслеживать место расходования валюты и ее отправителя.

Результаты

Большая прозрачность расходования международной финансовой помощи, направляемой на реализацию Глобальных Целей с целью снижения уровня коррупции и достижения поставленных задач.

Уровень зрелости

- Из-за непредсказуемости требований со стороны финансовых доноров могут возникать более серьезные проблемы, чем мошенничество и коррупция, поэтому в целях обеспечения эффективности эти требования необходимо согласовывать с ожидаемыми результатами проекта.
- В каждом отдельном случае оказания международной помощи, финансовый должен должен поддерживать доверительные отношения с правительством страны-получателя. Там, где отмечаются факты коррупции среди отдельных лиц в некоторых министерствах, либо если коррупционные схемы встроены в системы правительств страны-получателя, то на использование такого рода систем важно получить поддержку от государств-получателей.
- Для преобразования распределенных реестров в набор полезных услуг данного рода требуется создать целую сеть дополнительной функциональности.

Пример 4:
Снижение влияния рыночных колебаний и продвижение инноваций

Обзор

Одним из важнейших потенциальных преимуществ технологий DLT является возможность устранения барьеров и колебаний на рынке и ускорение процессов создания новых форм информационных рынков7. Как уже отмечалось в Главе 1, обмен информацией между субъектами хозяйственной деятельности через распределенные реестры будет способствовать активизации новых видов инноваций. Это облегчит министерствам достижение поставленных целей, ориентированных в основном на создании возможностей для экономического роста мелкого и среднего предпринимательства за счет эффективного использования технологических инноваций.

Освещение проблемы

Сокращение транзакционных издержек при взаимодействии с местными и центральными органами власти позволит этим предприятиям действовать на рынке более свободно и добиваться существенного снижения суммарных операционных затрат. В то же время, возможность для этих компаний регистрировать свою интеллектуальную собственность (IP) в распределенном реестре, а не посредством традиционной процедуры подачи заявки на выдачу патента позволила бы сократить общее число споров по контрактам. Доля споров по контрактам является самой многочисленной и составляет порядка 57% от общего числа судебных исков в Великобритании.

Возможности технологий DLT

Технологии DLT могли бы найти применение в самых различных областях, в частности, для ведения смарт-контрактов и регистрации активов. После регистрации активов в распределенном реестре все объекты недвижимости могли бы перейти в разряд "интеллектуальных активов", что позволило бы создать надежную и достоверную базу прав по самым различным услугам. Сегодня малому и среднему предпринимательству приходится тратить на это немало времени и денег. К подобным примерам следует отнести регистрацию прав интеллектуальной собственности и патентов, составление завещаний, нотариальные услуги, данные историй болезни в Национальной службе здравоохранения, а также пенсионное обслуживание и персональные пенсии из собственных доходов (SIPP). С помощью распределенных реестров можно по-новому ко¬ординировать данного рода услуги, в по-настоящему цифровом формате, масштабно и эффективно.

С помощью распределенных реестров можно управлять микроплатежами, выполнять децентрализованные обменные операции, вести учет заработанных и потраченных опознавательны знаков (токенов), а также переводить средства, что современные веб-приложения не позволяют[8]. В конечном итоге технологии DLT могут привести к радикальному пересмотру операционных издержек в местных юрисдикциях и на предприятиях в следующих направлениях[9]:

- Лицензирование коммерческой деятельности
- Регистрация
- Страхование
- Налоговый учет на многих муниципальных и нормативно-правовых уровнях
- Данные пенсионного учета

Возможно, что технологии DLT полностью заменят собой некоторые функции, поскольку компании смогут регистрировать цифровые идентичности не только своей коммерческой деятельности, но и своих активов. Что более важно, граждане также смогут получить больший контроль над своими персональными данными (например, данные об истории болезней), которые традиционно находятся в ведении правительства. Это позволит гражданам отслеживать факты обращения к своим данным со стороны третьих лиц, а также оценивать правомерность и корректность использования этой информации.

Использование распределенных реестров позволит обмениваться данными в новых формах информационных рынков — возможно даже в системах данных общего пользования, что обеспечило бы обмен данными пенсионного учета.

Результаты

- Сокращение транзакционных издержек для малого и среднего предпринимательства и оптимизация операционных затрат для местных и центральных органов власти. Кроме того, наличие достоверного подтверждения права собственности на цифровые активы, такого как право интеллектуальной собственности, приведет к снижению числа судебных исков, что в целом принесет значительную общественную выгоду Великобритании.

Уровень зрелости

- Требуется признание технологий DLT местными и центральными органами власти

Пример 5: Европейский НДС

Обзор

Экономику можно разделить на категории по многим признакам, например (i) экономика с соблюдением налоговых норм, (ii) квази-налоговая экономика и (iii) экономика с нарушениями налоговых норм (или "черный рынок"). Недопоступления НДС имеют место в экономиках всех трех категорий в силу самых разных причин, например, неплатежеспособность предприятия; творческий подход к применению международного законодательства с целью формирования структуры компаний, позволяющей уходить от уплаты налогов; либо оплата наличными "в черную" без каких-либо документов. Ежегодный объем недопоступлений НДС в странах ЕС колеблется в пределах от €151 млрд до €193 млрд10.

Темпы внедрения технологии DLT постоянно растут, поскольку она позволяет добиться большей прозрачности совершаемых операций. Великобритания может сыграть ключевую роль в поддержке дальнейшего развития этой технологии, разработке протоколов и внедрении решений для DLT в целях снижения объемов недопоступлений НДС в странах ЕС.

Освещение проблемы

Экспоненциальный рост плотности ресурсов вычислительной обработки был точно спрогнозирован по закону Мура еще несколько десятилетий назад. По сути, с конца 19 века и по настоящее время наблюдается экспоненциальный рост информационных технологий, и как показывают текущие прогнозы, эта тенденция сохранится до конца 21 века.

Информационные технологии являются самовоспроизводящимися и помогают человечеству изучать неизвестные явления природы через научные открытия. Это, в свою очередь, способствует созданию более быстрых и экономичных технологий, позволяющих раскрыть

новые загадки природы, что в конечном итоге приводит к преумножению технических возможностей.

В настоящее время известны многочисленные информационные технологии, позволяющие значительно сократить недопоступления НДС, среди которых следует отметить технологии машинного обучения, цифровые суперкомпьютеры, квантовые аналоговые вычисления, а также технологию распределенного реестра. Перед правительствами стоит ключевая проблема - внедрить эти технологии и получить ожидаемый результат раньше, чем это успеют сделать организованные преступные сообщества.

Возможности технологий DLT

Разработка единых для всех стран ЕС стандартов и протоколов НДС позволила бы быстрее внедрить технологии распределенного реестра во всей Европе, унифицировать все бухгалтерские операции по НДС - от счетов-фактур до банковских квитанций. Такая система может включать в себя смарт-контракты, позволяющие блокировать лазейки, имеющиеся в квази-налоговых экономиках, позволяющих уходить от уплаты НДС за счет разницы в пороговых значениях, принятых в разных странах - членах ЕС.

Устройства машинного осмысления, считывающие транзакции по перечислению НДС в странах ЕС в реальном времени, позволяют быстрее отслеживать ошибочные транзакции (в том числе так называемое карусельное мошенничество), чем это возможно при использовании текущих методик аудита. Более прозрачное и простое отслеживание операций, - в том числе совершаемых провайдерами платежного сервиса, банками и прочими финансовыми учреждениями - значительно ослабит возможности черного рынка.

Результаты

- Снижение административной нагрузки на компании и прочие организации при взимании и уплате НДС.
- Улучшение прозрачности операций в реальном времени во всем экономическом пространстве.
- Создание возможностей для более точной оценки кредитных рисков, сокращение возможных потерь вследствие неплатежеспособности.
  Предоставление данных кредиторам, финансирующим малое и среднее предпринимательство, включая оказание услуг кредитного факторинга.
- Заключение смарт-контрактов между казначейскими организациями и коммерческими структурами.

Уровень зрелости

- Технологическая готовность
- Важно установить диалог с платежными организациями уже на ранних стадиях, поскольку их входные данные также должны гарантировать прозрачность в процессе урегулирования платежей.
- Правительственные организации должны научиться использовать технологии DLT для налоговых расчетов.
- Конечные пользователи и собственники малых предприятий должны понимать механизм использования технологий DLT для целей эффективного налогового управления.

Заключение

Распределенные реестры несомненно представляют ценность для государственных организаций как более прогрессивный инструмент взаимодействия, позволяющий снизить масштабы мошенничества, ошибок, а также сократить затраты на оказание услуг пользователям, не получающим их в полном объеме. В то же время, эти технологии несут в себе новые формы инноваций и позволят сократить транзакционные издержки малого и среднего предпринимательства в Великобритании. В этой главе были рассмотрены некоторые из сценариев применения. По мере широкого внедрения распределенных реестров вполне возможно, что появится новая форма предоставления государственных услуг.

ГЛАВА 7

Глобальные перспективы

Организации, занятые в сфере цифрового бизнеса в киберпространстве, должны быть уверены в своих партнерах и пользоваться таким же доверием со стороны партнеров. Они также должны иметь возможность взаимодействия с большим и постоянно увеличивающимся числом сообществ других организаций по всему миру. Добиться этого можно с помощью технологии блокчейнов.

Автор
***Патрик Карри**, директор Управления федерации бизнеса Великобритании; **Кристофер Сир**, директор, компания FiNexus; а также **Майк Халсалл**, группа по изучению глобальных вызовов, университет Сингулярити, научно-исследовательский парк NASA, штат Калифорния*

Глава 7: Глобальные перспективы

Введение

Глобальные изменения — как положительные, так и отрицательные — происходят постоянно возрастающими темпами. Этому способствуют глобализация, ускоряющаяся благодаря Интернет-технологиям, социальные ожидания, а также обостряющаяся конкуренция за ресурсы. Граждане развитых стран отличаются от представителей стран "третьего мира" обостренным духом потребительства и ожиданиями неприкосновенности частной жизни, что может вступать в противоречие с традиционными, устоявшимися общественными ценностями и нормами поведения индивидуума. Поэтому именно государство, а не общество, ответственно за оказание поддержки нуждающимся и оказавшимся в тяжелом положении. Правительствам приходится балансировать между постоянно растущими потребительскими ожиданиями и кажущейся бездонной социальной поддержкой. Высказывание президента США Джона Ф. Кеннеди "Не спрашивай, что твоя страна может сделать для тебя, но спрашивай, что ты сможешь сделать для своей страны" сегодня становится все более актуальным: большинство граждан стремятся помочь своей стране, но не находят способов это сделать в эпоху цифровых технологий. Они стремятся быть частью целого, а не уязвимыми одиночками.

Одним из следствий такого недостаточного общественно-ориентированного поведения является поляризация жизненных позиций, возникновение противоположных ценностных ориентиров и тенденция к излишнему упрощению сложных изменений в последовательности простых несвязанных сущностей.

Реальный мир в глобальном масштабе представляет собой сложную сеть физических, виртуальных, законодательных, исторических, географических, общественных, поведенческих, экономических, информационных и технологических факторов. Дополнительные сложности возникают из-за скорости изменений и темпов внедрения новейших, прорывных технологий. Масштабы, скорость и сложность происходящих перемен должны рассматривать в комплексе. Отраслевым лидерам и национальным правительствам становится все труднее разобраться в этой сети и соответственно планировать, внедрять и реализовывать преимущества новых технологий в рамках традиционных, разрозненных организационных структур. Инициатива находится в руках наиболее расторопных - это финансовые рынки и организованная преступность. Развивающиеся страны, такие как Кения и Руанда, свободные от законодательного бремени, все активнее внедряют эти технологии. Среди промышленно развитых стран некоторые небольшие по численности и более однородные по составу государства добиваются значительного прогресса на пути внедрения новейших технологий, что в итоге идет на пользу другим странам, в частности, в Европе (см. практические примеры по европейским энергетическим рынкам, стр. 76, и пример с Эстонией, стр.80).

Среди признаков продвинутых в сфере цифровых технологий наций можно назвать:

- Высшее руководство, осведомленное о возможностях цифровых технологий.
- Обладающий достаточными полномочиями уполномоченный орган государственной власти, отвечающий в целом за переход страны на цифровые технологии, который ориентирован на международное сотрудничество и тесно взаимодействует со всеми секторами экономики.
- «Живой», ориентированный на сотрудничество национальный план, выполняемый отраслями при поддержке государственных инвестиций.
- Наличие в каждом государственном органе и учреждении технически грамотных, квалифицированных и опытных чиновников.
- Присутствие инженеров и лидеров цифрового бизнеса на выборных должностях.

Великобритании предстоит многое сделать по каждому из этих направлений, если она намерена стать одной из ведущих наций в сфере цифровых технологий. При этом в мире все активнее развиваются цифровые экономики. Для этого от нас требуется не только применять компьютерные технологии в существующих экономических

моделях - мы должны пересмотреть свое представление о том, в каком направлении движется цифровая экономика, а также о ее основных участниках и выполняемых операциях. Это можно сравнить с переходом от наличного бухгалтерского учета к бухгалтерскому учету на основе активов. Для этого каждая организация должна иметь более широкое представление о комплексной цепочке поставок, услугах и рынках, а также стремиться изменить свой подход к коллаборативному управлению рисками, принятию решений, участию в доходах и общей ответственности. Чтобы вести электронный бизнес в киберпространстве, организация должна быть уверена в своих партнерах и в свою очередь заслуживать доверие. Она также должна иметь возможность взаимодействия с большим и постоянно увеличивающимся числом сообществ других организаций. В киберпространстве доверие и взаимодействие более важны, чем в мире физическом. Добиться этого можно с помощью технологии блокчейнов, но гарантия успеха не в самой технологии, а в том, как она используется в масштабах страны.

Доверие и совместимость

Доверие это оценка рисков между двумя людьми, организациями или странами.

В киберпространстве для построения доверия должны выполняться два основных требования:

- Докажи мне, что ты являешься именно тем, за кого себя выдаешь (**аутентификация**).
- Докажи мне, что ты обладаешь разрешениями, необходимыми для выполнения того, что ты просишь (**авторизация**).

Если меня не устроит ответ, я могу позволить тебе продолжить, но при этом принимаю на себя риск. При этом, если другие мне тоже не доверяют, не будут выстроены устойчивые отношения. В этом смысле быть заслуживающим доверия аналогично статусу кредитоспособности.

Взаимодействие включает в себя несколько факторов:

- Совместимость данных. Для успешной совместной работы мы должны понимать друг друга, поэтому наши данные должны быть построены на основе одинаковых синтаксических и семантических правил.
- Совместимость политик. Наши политики должны быть согласованными или построенными на основе общей согласованной политики. В этом случае я буду уверен в том, что моя информация будет обрабатываться ожидаемым образом (и наоборот).
- Эффективная совместная реализация и применение международных стандартов.

Защита информации подразумевает организацию управления доступом, для чего требуются механизмы аутентификации, авторизации и многое другое. Для аутентификации требуется управление идентификационной информацией всех участвующих субъектов (обычно это люди, организации, устройства и программы) на определенном, международно признанном уровне доверия (LoA). Для аутентификации сообществ нескольких компетентных органов или организаций требуется управление федеративной идентификационной информацией (FIM).

В международном масштабе механизм FIM существует только на низком уровне доверия LoA 1, представленном в международных стандартах1. Он применяется главным образом в социальных сетях, где множественность юрисдикций не имеет большого значения. Это Google,

GakuNin (социальная сеть университетов Японии), Microsoft, Ping Identity, газета Nikkei, Корпорация Tokyu, mixi, Yahoo! Япония и SoftBank развернули у себя FIM-системы; на подходе - системы более высокого уровня зрелости, запланированные к внедрению такими организациями, как Deutsche Telecom, AOL и Salesforce.com.

Для среднего доверительного уровня (LoA 2) личная встреча с клиентом при регистрации (правило, известное как - "Знай Своего Клиента"), является обязательным требованием со стороны бизнеса для

проведения финансовых операций. Объединение на доверительном уровне LoA 2 представлено в основном банковскими системами.

В ряде отраслей применяются системы ограничения доступа, построенные на основе объединений инфраструктуры открытых ключей (PKI), основанной на использовании криптографического стандарта X.509. В таких системах для удостоверения подлинности сотрудника действует высокий и очень высокий доверительные уровни (LoA 3 и 4). Системы такого уровня применяются главным образом в авиации, фармацевтической отрасли, обороне, банковской сфере и все чаще в электронной системе здравоохранения. Больше всего систем, построенных по принципу объединения инфраструктуры открытых ключей (PKI), развернуто в США и Китае. За ними по численности следуют Южная Корея (где все компании обязаны по закону внедрять такие системы), а также Эстония, Нидерланды и ряд других. На доверительном уровне LoA 3+ используется возможность привязки идентификатора пользователя к другим проверенным функциям, таким как, законодательно-защищенные цифровые подписям, шифрование с привязкой к идентификатору пользователя и управление физическим доступом в здания. Объединение систем PKI не является единственным инструментом взаимодействия между цепочками поставок на высоком доверительном уровне и масштабного обмена конфиденциальной информацией. Сегодня это фактически стало нормой. Технология блокчейнов является перспективной альтернативой, а ее сочетание с PKI открывает еще более широкие возможности на пути к более высокой надежности цифровых операций, гарантий и доверия к бизнес-процессам в рамках развития новых технологий.

В Великобритании только в полиции применяется система PKI, построенная в соответствии с требованиями международных стандартов, пусть даже и в исходной форме. Внедрение передовых методик совместного управления позволит подключить к системе многие государственные службы Великобритании, в том числе экстренные службы. Совместное управление на международном уровне в таких сферах, как торговля, пограничный контроль, учет мигрантов и беженцев, позволило бы объединить ресурсы других систем, построенных по аналогичному принципу PKI. При этом, стратегия применения системы PKI государственными сетями общего пользования для аутентификации личности сотрудников пока еще не реализована, поэтому отсутствует высокий уровень доверия в управлении пользовательскими идентификаторами сотрудников или отношения взаимного доверия между правительственными организациями на основе международных стандартов, что позволило бы объединить ресурсы партнеров в отрасли с международными альянсами таких стран, как США, Франция и Нидерланды. Объединение инфраструктуры PKI в сочетании с технологией блокчейнов позволит увеличить производительность обработки идентификационных с сохранением конфиденциальности, а также эффективность отслеживания платежей.

В Национальной службе здравоохранения Великобритании внедрена развернутая инфраструктура на основе открытых ключей, но она не отвечает требованиям международных стандартов и пока еще не может быть объединена с другими системами. Министерства обороны взялло на себя международные обязательства внедрить PKI в цепочки поставок военного назначения, привязанные к структурам США, а также аналогичные обязательства в рамках Программы НАТО по борьбе с киберугрозами. Однако планы реализации мероприятий пока что не опубликованы. Возможны и другие области применения объединений PKI в промышленности, например, для борьбы с подделками в пищевой отрасли, описанными в Отчете Элиотт Ревью за 2014 год, посвященном проблеме доверия сети поставок продуктов питания. В разработке находится меморандум о взаимопонимании с правительственным учреждением Южной Кореи, которое позволит британским компаниям получить ключи доступа к PKI корейских предприятия для участия в цепочке поставок корейских компаний, таких как Samsung, Kia, Hyundai и Daewoo (производителем самых больших в мире контейнерных судов). Международная Морская Организация при ООН в настоящее время разрабатывает международные правила обеспечения кибербезопасности на морских судах и в перспективе может использовать преимущества от объединения инфраструктур открытых ключей Великобритании и Кореи. Можно привести еще множество примеров применения в других областях, и совместное обсуждение актуальных проблем лишь пойдет на пользу всем участникам дискуссий.

В сентябре 2014 года Европейский парламент утвердил нормативные акты в сфере Цифровой идентификации, аутентификации и трастовых услуг (eIDAS), обязав стран-участниц за 3 года

обеспечить его выполнение. Согласно eIDAS, если какая-либо из стран-участниц "уведомляет" своих граждан о схеме электронной идентификации (e-ID), то используемые в ней идентификаторы в обязательном порядке должны приниматься всеми другими странами-участницами при совершении открытых электронных операций. Предстоит еще большая работа, но уже сейчас законодательство elDAS заставляет правительства и отрасли составлять глобальные планы использования FIM-систем на пользу обществу и коммерческим структурам. В Великобритании правительство ввело объединенный стандартизированный подход для идентификации личности: GOV.UK Verify. GOV.UK Verify спроектирован в соответствии с последними требованиями рынка: иметь возможность выбора между несколькими конкурирующими провайдерами услуг идентификации. Привязка системы Verify к блокчейнам и объединенным инфрастуктурам открытых ключей (PKI) лишь повышает привлекательность самой системы Verify. Комплексные решения на базе блокчейнов и объединения PKI с высоким уровнем доверия в свою очередь выиграют от возможностей обеспечения конфиденциальности личных данных, доступных в системе Verify. Совместными усилиями, но в разных направлениях, они внесут существенный вклад в развитие цифровой экономики Великобритании, сферы пограничного контроля и борьбы с киберпреступностью.

ПРАКТИЧЕСКИЙ ПРИМЕР 1

Розничный рынок энергетики Европы

Игорь Най Фовино и Жан-Пьер Нордвик, Объединенный исследовательский центр при Европейской Комиссии

В рамочной стратегии Энергетического союза, принятой Европейской Комиссией, 1) изложена концепция "Энергетического союза", "где центральное место отведено гражданам (они берут под свой контроль переход к энергетической безопасности, используют возможности новых технологий для уменьшения своих платежей, активно ведут себя на рынке), а незащищенным потребителям обеспечивается поддержка". Несмотря на устойчивое развитие интеллектуальных сетей (smart-grid) в сфере энергетики, розничный рынок электросбытовых услуг все еще ожидает модернизации. Для реализации Инициативы Еврокомиссии 'Проект новых энергетических рынков" необходимо решить ряд ключевых проблем:

- каким образом предоставлять клиентам достоверную информацию по расходам и потреблению, чтобы они смогли оценить новые возможности полностью интегрированного континентального энергетического рынка
- как стимулировать активное участие, упростить процесс перехода на новые контракты и управлять категорией "спросом-предложение" в условиях меняющихся цен
- как обеспечить интеграцию на рынке услуг жилого энергоснабжения, расширить рамки потребительского выбора, продемонстрировать преимущества самостоятельной выработки электроэнергии и энергопотребления, а также местной микрогенерации.

В этом контексте распределенные реестры могут выступать в качестве катализаторов перехода на новый уровень интеграции и развития розничного энергетического рынка. Центр совместных исследований[2] при Европейской Комиссии в настоящее время изучает следующие практические примеры применения.

1. Рынок микрогенерирующих энергоустановок. Микро-генерация предполагает возможность самостоятельной выработки электроэнергии для потребителей в пределах одного дома или местного сообщества. Понятие "рынок" указывает на возможность продажи энергии, выработанной в условиях микро-генерации потребителям и "протребителям" (прим. переводчика: от англ. prosumer = producer - consumer, т.е. производящий потребитель). Традиционно этот рынок работал на основе предварительно ¬составленных двусторонних соглашений между "протребителями" и розничными поставщиками энергии. До настоящего времени "протребители" не имели полноценного доступа на энергетический рынок, который остается привилегированной площадкой для институционализированных поставщиков энергии. Это существенно ограничивает экономические преимущества микрогенерации для конечных пользователей. Распределенные реестры, в сочетании с системами и интеллектуального учета и аккумуляторами нового поколения (для местного накопления энергии), в перспективе могут открыть доступ "протребителям" на энергетический рынок. Интеллектуальные счетчики можно использовать для учета и регистрации самостоятельно сгенерированной энергии в распределенном реестре (тем самым формируя эквивалент системы "энерго-монет").

Самостоятельно сгенерированное электричество может быть либо использовано на бытовые нужды, накоплено в аккумуляторах нового поколения для последующего применения, либо передано в сеть. Либо, используя распределенную и вездесущую природу реестра,

привязывать каждый субъект и транзакцию в киберпространстве к какой-либо организации. Фундаментальным требованием цифровой среды является установление подлинности организации до желаемого доверительного уровня (LoA) и получение необходимой информации в реальном или почти реальном времени. Выполнению этого требования будет способствовать более активное применение блокчейнов во избежание нарушения целостности записей. В настоящее время разрабатывается новый международный стандарт идентификации организаций? известный как Реестр правовых Организаций (ROLO). Уже несколько стран, в том числе США, изучают возможности адаптировать спецификацию ROLO под свои требования. Глобализация и отсутствие адаптированных к цифровой среде реестров предприятий приводят к ситуациям, особенно в ЕС, когда большинство финансово активных организаций не зарегистрированы совсем, либо в определенной стране, при этом сложно определить эту разницу. Промышленные и правительственные организации Великобритании, включая правоохранительные органы и организации по борьбе с киберугрозами, остро нуждаются в ROLO-реестре Великобритании в качестве цифрового, заслуживающего доверия источника информации. Промышленность уже приступила к разработке ROLO-реестра Великобритании при активном содействии правительственных организаций потребителей.

произведенную энергию можно также обменять как товар в другом месте, например, во время зарядки электромобиля за рубежом; либо продать ее через реестр наиболее выгодному покупателю, используя механизм, аналогичный механизму биржевого рынка.

2. Реестр энергетических контрактов. Потребитель, планирующий перейти на обслуживание к другому поставщику энергии, должен закрыть действующий контракт с текущим поставщиком и заключить контракт с новым поставщиком и изучить условия контракта по всем дополнительным услугам энергоснабжения, предоставляемым третьими сторонами. Управление множеством процессов администрирования при выполнении таких операций является реальным препятствием для дальнейшего развития конкурентного розничного рынка услуг энергоснабжения и источником затрат для поставщиков и дистрибьюторов энергии. Применение распределенных реестров для онлайн-регистрации энергетических контрактов позволило бы значительно упростить эти операции. Потребители смогли бы оформить переход от одного поставщика к другому всего за несколько кликов на компьютере или мобильном устройстве. Аналогично поставщики энергии и поставщики услуг энергоснабжения смогли бы сэкономить значительные ресурсы для выполнения этих операций.

Пока еще не решены вопросы масштабируемости, безопасности и стабильности таких приложений. Тем не менее, преимущества оказываются такими многообещающими, что дальнейшие исследования в этом направлении стоят того.

Электронные экономики

Электронным экономикам свойственны скорость распространения, охват и эффективность. Объединение доверенных ресурсов позволяет снизить риски по повысить общий доверительный уровень. Совместимость данных способствует повышению эффективности и открывает новые возможности ¬для повторного использования. В цепочках поставок с высоким уровнем зрелости всякий раз, когда компаниям приходится конкурировать в новой программе или в секторе, повторное использование дает определенную свободу действий и конкурентные преимущества: эту точку зрения поддерживают компании аэрокосмической и оборонной отраслей, что нашло подтверждение в публичных докладах компаний Airbus, Boeing, BAE Systems, Lockheed Martin, Northrop Grumman, Raytheon2 и других.

В феврале 2014 года Ниле Крёс (Neelie Kroes), в то время занимавшая пост вице--президента Европейской Комиссии и курировавшая вопросы электронной экономики, отметила: “демократия должна найти общий язык с технологией[3]”. Она аргументировала необходимость перехода к

среде, управляемой данными, где ключевым фактором является уровень доверия, и то, что "без безопасности нет конфиденциальности". Она отметила, что для Единого Электронного Рынка Европы важно обеспечить надежную защиту от киберугроз, и что Стратегия кибербезопасности Евросоюза развивается в правильном направлении. В заключение она отметила, что без такой инициативы "демократия не сможет управлять технологией".

Диалоги на эти темы с участием представителей банковской сферы, электронной промышленности, фармацевтики, пищевой промышленности, морских перевозок, аэрокосмической отрасли, структур по борьбе с киберугрозами и правоохранительных органов стран ЕС, США и стран региона ASEAN все больше проходят в режиме совместных конструктивных дискуссий. На уровне ООН и таких организаций, как Совет Европы, в адрес промышленно развитых стран все настойчивее звучит призыв помочь странам "третьего мира", поскольку они становятся частью глобальной электронной экономики. Но недостаток ресурсов цифрового управления сдерживает движение развитых стран в этом направлении, открывая широкие возможности для киберпреступности и терроризма, нацеленные в конечном счете на промышленно развитые страны. Содружество могло бы сыграть значительную роль в разрешении этой ситуации. Взаимодействие - ключ к успеху.

Возможности децентрализованных реестров и блокчейнов

Национальные экономики полагаются на совместное управление для завоевания доверия на финансовых рынках, добиваясь, чтобы все играли по согласованным правилам. В электронных экономиках действуют те же принципы. Главной причиной того, что блокчейны ассоциируются с киберпреступностью, является отсутствие стратегического управления с целью установления согласованных правил и контроля за выполнением требований. Как только станет возможным такое управление (с помощью политик, процедур и механизмов) и контроль за исполнением требований, общество оценит преимущества блокчейнов. Обеспокоенность правительств в связи с неустойчивостью и уязвимостью криптовалют и операций их обмена привела к настороженному использованию блокчейнов. И в целом правительства склоняются к тому, чтобы промышленность развивалась в этом направлении в более благоприятной ситуации.

На текущий момент можно отметить следующие направления развития:

- Неконтролируемые блокчейны применяются для совершения нерегулируемых и преступных операций, в частности, когда стороны предпочитают оставаться анонимными и не нести никакой ответственности.
- Начинающие компании, работая с ведущими банками, стремятся заработать авторизованные криптовалюты и блокчейны, например "доверительные биткойны". Это могло бы дать значительные преимущества ведущим Интернет-компаниям потребительского сектора.
- В закрытых коммерческих сообществах для поддержания цифровых механизмов доверия используются закрытые блокчейны, работающие по собственным правилам. Такие блокчейны не являются совместимыми и не могут распространяться на более масштабные цепочки поставок.

И лишь недавно правительства начали сотрудничать с отраслью с целью изучения стратегического потенциала блокчейнов. Реализация продолжается ускоренными темпами благодаря следующим четырем факторам:

Создание основы доверия к криптографической системе, аналогичного инфраструктуре открытых ключей PKI. Это означает, что блокчейны могут объединяться между собой, а также с существующими

- объединениями инфраструктуры открытых ключей (PKI). Блокчейны могут использовать распределенный масштаб и управление инфраструктуры открытых ключей (PKI), в то время как системы PKI могут использовать функции платежа и функции реестра блокчейнов. Такая синергия открывает новые возможности, которые могут быть усилены еще больше умным, основанным на сотрудничестве управлением.
- Контролируемые реестры создают поле данных неограниченного размера. Они могут содержать информацию о транзакции, включая контракт, лицензию или авторское право,

тем самым обеспечивая мощный дополнительный фактор доверия. Это обеспечивается "смарт-контрактами" (т.е. связыванием контракта с транзакцией - см. главу 1), что обеспечивает эффективность и отсутствие отказоустойчивость.

- Использование новых протоколов, таких как новый Единый экономический коммуникационный протокол (UETP) соединяет поставщика с носителем, клиентом, продуктом, платежами и банками, а также со смарт-контрактом. В этой сфере лидером являются Нидерланды, при участии в отрасли Великобритании и возможном привлечении полиции. США только присоединяется, но ее роль будет усиливаться по мере введения законодательного регулирования киберстрахования по всем цепочкам поставок. Как ожидается, вскоре к этим странам присоединятся и другие государства, такие как Южная Корея и Япония.

- Фактически, смартфоны становятся доверенным устройством пользователя. Смартфоны нового поколения оснащены новыми важными элементами безопасности, включая Доверенный платформенный модуль (TMP) обеспечивает защиту цифровых сертификатов и криптографических ключей для аутентификации, шифрования и подписи. Защищенные процессы проходят в доверенной среде исполнения (TEE) без использования операционной системы, которая может быть уязвимой для вредоносного программного обеспечения. Доверенный пользовательский интерфейс (TUI) защищает от хакерских аттак на уровне пользователь-устройство. Используя беспроводную связь ближнего радиуса действия, смартфон может безопасно вступать в контакт с некоторыми национальными картами электронной идентификации (e-ID) и электронными паспортами, предоставляя пользователю возможность безопасно взаимодействовать с органами власти (например на границе или при контактах с полицией) в режиме онлайн. Пользователи и сотрудники, таким образом, впервые получают безопасное защищенное устройство, позволяющее подписывать транзакции (например, используя блокчейн) и платежи (например используя "доверительные биткойны"). Samsung, HTC и LG продают десятки миллионов таких совершенных смартфонов, оснащенных дополнительными функциями защиты, готовых к установке программного обеспечения, которое появится в начале-середине 2016 г. Как ожидается, Apple и другие компании последуют за ними.

Однако, потребуется повсеместное строгое совместное управление для того, чтобы обезопасить эти возможности от злоупотреблений и нецелевого использования. Эти четыре фактора способствуют более широкому использованию блокчейнов и распределенных реестров для финансовых целей, а все увеличивающегося числа новых целей, связанных с цифровыми технологиями и данными, по всем цепочкам поставок и при участии государств. По мере совершенствования этих систем и расширения их возможностей, эти четыре фактора могли бы способствовать решению целого ряда сложных социальных и глобальных проблем. Например:

- **Прозрачное и честное правительство.** Доверие среди граждан в развивающихся странах ниже, чем в странах со стабильными и понятными нормативно-правовыми структурами, обеспечивающими условия для лучшего общества и социального поведения. Для людей, живущих в регионах, опустошенных войнами и автократическими режимами, потребуется больше времени, чтобы вновь начать доверять своим правительствам и, насколько это возможно, избавиться от коррупции. Внедрение в бизнес-процессы механизмов обеспечения прозрачности и доверия (реализуемых с использованием блокейчнов, FIM-систем и соответствующих возможностей), является жизненно необходимыми для обеспечения эффективного использования и применения законов, политик и организационных структур.

- **Уклонение от уплаты налогов и отмывание денег.** По мере роста кривой распределения богатств страны вверх, владельцы денежных средств и активов стремятся уйти в оффшоры и спрятать состояния, тем самым уменьшая финансовую ликвидность отечественных рынков и еще более сокращая экономические возможности тех, кто и так находится внизу кривой распределения богатств. В конечном счете, дефицит капитала может привести к расшатыванию экономик, за которыми последует масштабная безработица среди молодежи, что чревато серьезными последствиями для "потерянных"

поколений и вызовет глубокое недоверие к их лидирующей роли. Это подрывает основы демократии, приводит к расколу в обществе, образованию "несостоявшихся" государств, усугубляет угрозы терроризма и бедности. И опять, для решения этих проблем необходимы прозрачность и доверие.

- **Незаконная торговля и вандализм в отношении окружающей среды.** Около 50% видов морских обитателей истреблено за последние 30 лет. Аналогичная ситуация и на суше. Несмотря на усилия международного сообщества согласно Конвенции о международной торговле исчезающими видами дикой фауны и флоры (CITES), данные свидетельствуют о тенденции к шестому массовому истреблению видов. Если мы хотим решить эту глобальную проблему, нам следует использовать более мощные механизмы определения и отслеживания активов, с аналогичными характеристиками прозрачности и доверия.
- **Мошенничество в сфере пищевых продуктов и разрыв цепочек поставок.** Великобритания в гораздо большей степени зависит от импорта продуктов питания, чем когда-либо ранее и гораздо в большей степени чувствительна к отказам отказу от отечественных продуктов питания, чем в 1917 или 1942 гг. Цепочку поставок продуктов питания бывает сложно отследить - о чем свидетельствует история с фальсификацией мяса в 2013 г. (широко известная как "скандал вокруг конины"),

ПРАКТИЧЕСКИЙ ПРИМЕР 2

Эстонские блокчейны трансформируют систему оплаты, торговли и подписи

Алестер Брокбанк, посольство Великобритании, Таллинн

Эксперименты с технологией блокчейнов были логическим шагом для Эстонии. Они обладают идеальными качествами для хранения открытых ключей и управления ими за счет использования распределенных и неизменных реестров информации. Они имеют форму криптоключа, предоставленного уполномоченным органом, который может сочетаться с приватным ключом для эффективного шифрования сообщений и аутентификации цифровых подписей. Страной, наиболее регулярно использующей национальную инфраструктуру открытых ключей (PKI), сегодня является Эстония.

Более того, в качестве децентрализованного решения, блокчейны по своей сути являются более портативыми и масштабируемыми.

Они способны считывать большие объем данных каждую секунду и бесперебойно работать в разных странах. Для компаний, работающих в стране с населением всего лишь 1.3 млн человек, блокчейны предоставляют возможность простого преобразования национальных решений в глобальные. Их вычислительная мощность также ускоряет их работу. А разрушительная сила заключается в том, что в некоторых случаях они делают ненужными существующих посредников.

Три практических примера, приведенных ниже - анализ банка, стартапа и поставщика услуг кибербезопасности, - демонстрируют революционные возможности блокчейнов для широкого спектра транзакций. Все эти три примера подчеркивают, что блокчейны должны создаваться удобными для пользователей. Клиентам не обязательно знать, что они совершают сделки маркированными монетами, или что их идентификационная карта-логин использует криптографическую функцию хеширования информации. В этом смысле блокчейн работает как молчаливый и эффективный инструмент, стоящий за решением, которое кажется знакомым: мобильные платежные приложения, онлайн краудфандинговая и торговая платформа или портал для аутентификации.

Как и для Великобритании, необходимость в регулировании и его степень являются ключевыми вопросами для эстонских властей. Они понимают, что сомнения и неуверенность могут быть так же разрушительны для инноваций, как и строгость. Среди очевидных рисков инноваторов, попадающих в новые менее жестко регулируемые юрисдикции, - потеря прибыли из-за невозможности капитализации коммерческих возможностей, и криминальная угроза.

например - и здесь имеется немало возможностей для мошенничества. Международные и британские цепочки поставок продуктов питания не имеют других вариантов, кроме как копировать лучшие в своем классе цепочки в других секторах для гарантии прозрачности и детализированной прослеживаемости.

- **Угрозы цепочек поставок.** По мере роста киберпреступности и фактов хищения интеллектуальной собственности (на суммы более 7 трлн долларов по всему миру) увеличивается законодательное, рыночное и общественное давление на цепочки поставок, с целью получения более надежных гарантий безопасности, основанных на совместном управлении рисками, в том числе прозрачности и управлении федеративной идентификационной информацией (FIM).

Наряду с другими развитыми странами и международными экспертами, Великобритания может оказать влияние на Совет Европы, Всемирный Банк, Большую двадцатку и ООН для перехода к осуществлению блокчейнов со строгой аутентификацией, что позволит обеспечить прозрачность и доверие к операциям. Правительство Великобритании не может достичь этой цели в одиночку. Для целей развития промышленности правительство должно принять активное участие в реализации национального энергетического подхода, начать развитие потенциала страны и использовать преимущества первопроходца, чтобы в итоге вывести (в сотрудничестве с промышленностью) Великобританию в мировые лидеры.

Первый выпуск банком ценных бумаг в криптовалюте

Ранее в этом году LHV Pank - крупнейший независимый банк Эстонии - стал первым в мире банком, который в качестве эксперимента с аппаратно-управляемым валютами, выпустил криптографически-защищенные депозитные сертификаты на сумму €100 000 . Эксперимент состоялся сразу после регистрации нового филиала LHV - Cuber Technology - который специализируется исключительно на ценных бумагах на основе биткойнов. Работа Cuber включает два направления: Ценные бумаги CUBER и Cuber-кошелек.

CUBER (аббревиатура от англ. "Криптографические Универсальные Блокчейны, Подтвержденные к Принятию). Ценные бумаги CUBER - банковские депозитные сертификаты, зарегистрированные в блокчейне биткойн. Их номинальная стоимость установлена в евро. Они способны приносить процентный доход и могут использоваться для разных целей - для хранения ценных бумаг, как средство расчетов, для предоставления трастовых и депозитарных услуг и даже для межмашинных транзакций, что делает их потенциально применимыми в Интернете вещей (IoT). LHV рассматривает ценные бумаги CUBER как строительные кирпичики Lego для своих будущих финансовых инноваций.

Кошелек Cuber - первая демонстрация возможностей CUBER. Он представляет собой программный объект для мобильных телефонов, позволяющий проводить мгновенные бесплатные одноранговые (пиринговые) транзакции в евро, а также недорогие мгновенные платежи для продавцов и потребителей с использованием внутренних ценных бумаг CUBER.

Для большей безопасности и мобильности пользователи хранят приватные ключи на своих смартфонах. Для защиты системы от сбоев на сервере, кошелек Cuber снимает функции доверия с сервера и превращает самих пользователей в клиентов системы Биткойн. Приложение использует упрощенную верификацию платежей (SPV) - тип безопасности "тонкого клиента", при которой пользователь не получает копии всех блоков в цепочке. Вместо этого они загружают меньшее количество данных, "заголовки блоков", которые связывают транзакции с определенным местом в цепочке. Это позволяет им видеть, что сетевой узел принял транзакцию, а блоки, добавленные после этого подтверждают, что ее приняла сеть.

Кошелек использует биткойны как носитель данных, который они "окрашивают", добавляя к ним уникальные маркеры. После этого делается запрос на официальную валюту в Банк LHV, поскольку вход в базу данных представляет собой запрос к традиционной банковской системе. За счет привязки к официальной валюте, кошелек можно использовать не только для личных переводов, но и для розничных платежей - как и в случае с кредитной картой, продавец должен одобрить этот метод платежа. LHV в настоящее время тестирует систему в нескольких физических точках, но, как ожидается, эти функции получат большее распространение для онлайн-операций, в частности для проведения небольших платежей.

Использование официальной валюты несомненно делает приложение более дружественным для пользователя. LHV считает, что лежащая в основе технология - это забота банка: пользователю и продавцу нет необходимости

ПРАКТИЧЕСКИЙ ПРИМЕР 2 (продолжение)

видеть или знать, что Cuber использует биткойны.

Открытый исходный код Cuber и интерфейс программного приложения доступны третьим лицам онлайн, что позволяет обменивать другие криптовалюты, а также дает доступ к технологии разработчикам. Как LHV, так и его партнер по развитию, ChromaWay, предпочитают внедрять полезные инновации с менее крупными разработчиками программного обеспечения и старт-апами, нежели с крупными банками.

Испытывая давление вызовов времени, LHV однозначно считает, что неопределенность в сфере нормативного регулирования рискует свести на нет преобразовательный потенциал технологии Cuber, существенно ограничивая ее распространение. Банки призывают регуляторов принять и адаптировать технологию блокчейн, а не испуганно "бежать" от нее.

В свете этого, банковская поддержка дает Cuber огромные преимущества, поскольку перечисление средств с обычного банковского счета на электронный кошелек (и обратно) проходит по упрощенной схеме. Технически, CUBER относится к ценным бумагам - основе банковской системы - хоть и с децентрализованным делопроизводством. Но в реальности, быть банком означает сталкиваться с препятствиями нормативно-правового характера, что связано с тем что банки чаще молодых инноваторов имеют дело с законодательно регулируемыми арбитражными сделками. Так же и правило, известное как "Знай Своего Клиента" (KYC) в ЕС , требующее для открытия банковского счета встречи с клиентом лицом к лицу, ставит Cuber в более невыгодное положение по сравнению с другими сервисами онлайн-платежей, такими как TransferWise и Holvi, которые требуют лишь быструю онлайн-регистрацию. Чтобы помочь банкам эффективно конкурировать на этом рынке, регуляторы не должны создавать дополнительных барьеров или препятствовать их усилиям по охвату или привлечению новых пользователей.

По общему мнению, LHV находится в необычном положении, будучи банком, открытым к инновациями и внедряющим их самостоятельно, однако, дальнейший прогресс которого ограничивается законодательной неустойчивостью. В случае, если позитивных сдвигов в будущем не произойдет, Cuber либо придется дистанцироваться от лицензии LHV и тех преимуществ, которые приносит связь с банком, либо рассматривать возможность выбора какой-либо другой юрисдикции за пределами Европы.

Развитие простого, безопасного и соответствующего юридическим требованиям связующего звена между криптографической системой и традиционной банковской системой продолжает оставаться трудноразрешимой задачей для всех игроков. Но пока ни один из них не подошел к решению проблемы ближе, чем LHV.

Гибкий вторичный рынок для инвестиций в стартапы

Неликвидность инвестиций в стартапы - претензия, одинаково озвучиваемая и бизнес-ангелами, и основателями. Кредиторам, как правило, приходится вложить не менее €10 000 евро, и ждать возврата 5 или более лет.

Funderbeam - авторитетная коммерческая интеллектуальная платформа для инвесторов - возможно нашла решение этой проблемы: инвестиционный рынок, основанный на блокчейнах позволяет покупать и продавать инвестиционные пакеты маркированных монет в объединениях стартапов.

Инвесторы вскоре смогут использовать онлайн платформу Funderbeam для создания инвестиционного объединения одного или нескольких стартапов. Инвестиции могут осуществляться в любой конфигурации. Не существует и ограничений по размерам объединений. Инвестиционный пакет в £100 000 может состоять из одного лид-инвестора и 99 дополнительных кредиторов, инвестирующих по £1000 фунтов; либо из одного лид-инвестора с £75 000 инвестиций и 5 дополнительных, инвестирующих по £5000. Возможны и любые другие комбинации. Аналогично краудфандингу, это снижает порог входа для инвесторов стартапов.

Что отличает Funderbeam от других краудфандинговых альтернатив, так это выпуск маркированных монет, отражающих пакеты участников объединений, которые могут быть мгновенно куплены, проданы или переданы для участия в торговых операциях с другими инвесторами. Это позволяет более гибко управлять инвестиционным портфолио и упрощает получение финансирования старт-апами. Блокчейны биткойнов поддерживают вторичный рынок, позволяя отслеживать права собственности на активы быстро, эффективно и прозрачно.

Каждое объединение работает в паре с микрофондом. Как только объединение завершено и стартап получил финансирование, на вторичный рынок Funderbeam выпускаются маркированные монеты, электронно отражающие долю участников объединения в микрофонде, которые к тому же могут сразу же участвовать в торговых операциях. Кредиторы могут таким образом полностью продать свою долю или часть доли, как только они получили достаточную прибыль или если они хотят сократить свои убытки.

Гибкость для инвесторов - не единственное преимущество, которое предлагают блокчейны. Кайди Руусалепп, генеральный директор Funderbeam, также указывает на выгоды, которые предлагают распределенные реестры

за счет обхода бюрократических препятствий. "Мы не нуждаемся в коммерческом реестре, центральном депозитарии или другом формальном органе для подтверждения чистоты транзакции", - утверждает он. Благодаря технологии блокчейн, каждая инвестиция или изменение собственности имеет свой защищенный, распределенный отслеживаемый след".

Джин Таллинн, со-основатель Skype и инвестор в Funderbeam, оценил дополнительный слой безопасности и верификации, который она предлагает для онлайн операций. Будучи децентрализованными и неизменными, блокчейны обеспечивают большую прозрачность на фондовом рынке без ущерба чьей-либо конфиденциальности.

Предложение Funderbeam - обеспечивающее гибкость, скорость, безопасность и прозрачность, - показывает каким образом распределенные реестры могут обеспечить альтернативную, но в то же время жизнеспособную основу для увеличения финансирования малых и средних предприятий в 21 веке.

Следующее поколение инфраструктуры открытых ключей (PKI)

С 2013 г. реестры эстонского правительства, включая те, в которых хранится вся информация о гражданах и бизнесе, используют Guardtime для аутентификации данных в своих базах данных. Инфраструктура подписи без кода (KSI), сочетает криптографические функции хэширования (см. ниже) с распределенным реестром, позволяя эстонскому правительству гарантировать наличие сведений о состоянии каждого компонента в рамках сети и хранение данных.

Это важная инициатива. В Эстонии находится наиболее часто используемая национальная система PKI в мире. Используя идентификационную карту, граждане заказывают рецепты, голосуют, используют системы банк-онлайн, просматривают электронные школьные дневники своих детей, подают заявки на государственные пособия, регистрируют налоговые декларации, подают заявления о планировании, загружают свои завещания, регистрируют заявление на службу в вооруженных силах и выполняют еще около 3000 функций. Предприниматели используют идентификационные карточки для подачи годовых отчетов, выпуска документов акционеров, отправки заявок на лицензию и т.п. Государственные чиновники используют идентификационную карту для шифрования документов в целях безопасной коммуникации, ознакомления и утверждения разрешений, контрактов и заявлений, а также отправки информационных запросов в правоохранительные органы. Министры используют идентификационные карты для подготовки и проведения совещаний, что также позволяет им знакомиться с повесткой дня, высказывать свои позиции и возражения и просматривать протоколы.

Таким образом электронная аутентификация приобретает особое значение для оказания правительственных, коммерческих и социальных услуг, начиная с разработки политик и законодательных актов и заканчивая подачей финансовых деклараций, регистрацией собственности и прав наследования. Уже было сделано свыше 200 млн цифровых подписей с использованием идентификационной карты: около 39 на одного человека в год. И их число продолжает расти. Для правительства важно понимать, что эти записи являются верными, и что они не были изменены извне или в результате кибератаки.

Как же в этом случае может помочь технология блокчейн? Она позволяет записывать каждое изменение единицы данных. Подтверждая время, идентичность и аутентичность, инфраструктура KSI обеспечивает целостность данных, защиту от датировки задним числом и подтверждаемые гарантии того, что данные не стали объектом манипуляций. Также она прозрачна и работает также в интересах пользователя: граждане могут видеть, кто просматривал их данные, почему и когда, а любые изменения их персональных данных должны быть авторизованы. Более того, используемая функция хэширования, в отличие от асимметрической криптографии, используемой в большинстве инфраструктур PKI, KSI, не может быть взломана при помощи квантовых алгоритмов. Она также масштабируема, поскольку способна подписывать эксабайт данных в секунду с использованием пренебрежимо малых переменных издержек на вычисления и сетевые ресурсы. Тем самым снимается необходимость наличия центра доверия. Подписанные данные могут быть верифицированы в любой точке земного шара, и не нарушат конфиденциальности, поскольку система не хранит клиентские данные. Очевидно, что система представляет значительные успехи в создании инфраструктуры открытых ключей (PKI).

В конечном счете, блокчейн KSI гарантирует устойчивость эстонских идентификационных карт к взломам (хотя их пока еще не было), а правительство получает полную (100%-ю) гарантию, что мошеннические операции с открытыми данными будут отслежены.

Ссылки

Основные положения и рекомендации

1. Государственное управление науки, Будущее финансовых технологий Великобритания как мировой лидер в области финансовых технологий, 2015 г. Доступно на сайте https://www.gov.uk/government/uploads/ system/ uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

Глава 1

1. Государственное управление науки, Будущее финансовых технологий Великобритания как мировой лидер в сфере финансовых технологий, 2015 г. Доступно на сайте https://www.gov.uk/government/uploads/ system/ uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf
2. Институт Коммерческих Ценностей IBM, "Демократия устройств": Сохранение будущего Интернета вещей, 2015 г. Доступно на сайте http://www-01.ibm.com/common/ ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF
3. Правительственное управление науки: Интернет вещей: максимальное использование преимуществ Второй цифровой революции, 2014 г. Доступно на сайте https://www.gov.uk/government/ uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things- review.pdf

Глава 2 Практический пример: Исследования и обзор перспектив

1. Благодарности: Влияние криптовалют на трансформацию цифровых технологий: Справочник EPSRC EP/ N015525/1 (2015). Доступно на сайте http://gow.epsrc.ac.uk/NGBOViewGrant. aspx?GrantRef=EP/N015525/1
2. Общественная конференция ITaaU 2015 г. Доступно на сайте http://www.itutility.ac.uk/ event/2015-itaau-community-conference/
3. Networked Society Lab, Ericsson, ICT и Будущее финансовых услуг (2014 г.) Доступно на сайте http://www.slideshare.net/Ericsson/horizon-scan-ict-and- the-future-of-financial-services
4. EPSRC 'Доверие, идентичность, конфиденциальность и безопасность в цифровой экономике ' (2015). Доступно на сайте https://www.epsrc.ac.uk/funding/calls/trustidentityprivacysecurity/
5. Перри М, и др. "Валюта электронных денег" (2015 г.) Доступно на сайте https://www.youtube.com/watch?v=PCa3pTCegE8
6. 3DaRoC 'Инструментарий электронных обменных операций с участием посредников" (2015). Доступно на сайте https://digitalintermediaries.wordpress.com/toolkit/

Глава 3

1. Лессиг Л. Кодекс и прочие законы киберпространства, Версия 2.0 , Нью-Йорк: Базовые книги 2006.
2. Департамент финансовых услуг Нью-Йорка "Нормативные рамки лицензирования биткойнов" Доступно на сайте http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework. htm

Глава 4

1. Оперативная рабочая группа по интернет-инжинирингу "Прозрачность сертификата" 2013 г. Доступно на сайте: https://tools.ietf.org/html/rfc6962. Также см. : http://www.certificate-transparency.org/
2. Мелара М.С, и др. "CONIKS: Обеспечение ключевой открытости для конечных пользователей: электронный криптологический архив: Отчет 2014/ 1004 Доступно на сайте http://eprint.iacr.org/2014/1004.pdf
3. Данезиз и Майклджон С. Криптовалюты, которые поддерживаются центральным банком ' Архив электронных публикаций по криптологии: Отчет 2015/ 502. Доступно на сайте https://eprint.iacr.org/2015/502.pdf
4. Н. Куртуа "Разделится ли Биткойн на две криптовалюты? 2015 г. Доступно на сайте http://blog.bettercrypto.com/?p=1811

5. С. Накамото " Описание равноправной пиринговой системы электронных денег Биткойн" 2008. Доступно на сайте: http://satoshi.nakamotoinstitute.org/emails/cryptography/1/
6. Майклджон С, и др. : "Полный карман биткойнов - характеристика платежей среди анонимных пользователей", Конференция по параметрам Интернета, 2013, страницы 127-140.
7. Данезис Дж. и др. "Статистические данные и перекрестные атаки на анонимные системы", - Information Hiding 2004, стр. 293-308.
8. Бонно Дж. и др." Микскоин: Анонимность биткойнов в проверенных структурах", Финансовая криптография, 2014 г. , страницы 486-504.
9. Гарман Дж. и др" Рациональный ноль: Экономическая безопасность нулевой валюты с вечной анонимностью", Семинары по финансовой криптографии, 2014, стр. 140-155.
10. Мирс И. и др. "Нулевая валюта: Анонимные распределенные электронные деньги от Биткойн" Симпозиум по безопасности и приватности IEEE, 2013, страницы 397-411.
11. Данезис и др. "Монета "Пиннокио" - создание нулевой криптовалюты в результате системы подтверждения на основе существующей непродолжительное время пары валют", PETShopCCCS, стр. 27-30
12. Грот Дж. и Кольвайс М. Одно из множества доказательств: Или как допустить утечку секретной информации и израсходовать валюту" - EUROCRYPT 2015, стр. 253-280.

Глава 5

1. Кристенсен С.М, и др. "Стратегии выживания в быстро меняющихся отраслях", Наука об управлении, 1998, том 44, страницы S207-S220.
2. Джейкобайдс М.Дж. и др. "Получение преимуществ от инноваций: Создание ценностей, присвоение ценностей и роль отраслевой инфраструктуры, Политики исследования, 2006, том 35, страницы 1200-1221
3. Баден-Фюллер К. и другие "Бизнес-модели и технологические инновации", Долгосрочное планирование 2013: том 46, страницы 419-426.
4. Джейкобайдс М Дж. и др. "Кто что делает и кто что получает: извлечение ценностей из инноваций: Краткий отчет Института современных исследований в области управления, 2006 г. Доступно на сайте http:// faculty.london.edu/mjacobides/assets/documents/whodoeswhat. pdf
5. Перез С. Технологические революции и техно-экономические парадигмы, Рабочие тетради в области технологического управления и экономической динамики, 2009 г. Таллинский технологический университет, Таллинн, Норвегия
6. Рифкин Дж. "Общество с нулевыми маржинальными затратами: Интернет вещей, сообщество, действующее на принципе сотрудничества и закат капитализма, 2014 г. Нью-Йорк, Пелгрейв Макмиллан
7. Берч Д. Идентичность - новая валюта, 2014 г. Лондон Паблишинг Партнершип

Глава 5 Практический пример: Корпоративные сделки

1. Оксера " Обработка корпоративных сделок: каковы риски? май 2014 г. http://www.oxera.com/Oxera/media/Oxera/downloads/reports/Corporate-action-processing.pdf?ext=.pdf

Глава 6

1. Сван М. "Блокчейн: Проект новой экономики" О' Рейли Медиа Инк, 2015 г.
2. Департамент труда и пенсий: мошенничество и ошибки в системе пенсионного обеспечения 2013/14, 2014 Доступно на сайте https://www.gov.uk/government/collections/fraud-and-error-in- the-benefit-system
3. Комиссия по финансовому участию "Расширение доступа к финансовым услугам: Улучшение финансового здоровья нации , 2015 г. Доступно на сайте http://www.financialinclusioncommission.org.uk/ report
4. Роулингсон К. и МакКей С. "Расширение доступа к финансовым услугам: Отчет по результатам годового мониторинга , 2014 г. Доступно на сайте http://www.birmingham.ac.uk/Documents/college-social-sciences/social-policy/CHASM/annual-reports/chasm-annual-monitoring-report-2014.pdf

5. ООН "Отчет о целях развития тысячелетия, 2010 г. Доступно на сайте: http://www.un.org/millenniumgoals/pdf/MDG%20Report%202010%20En%20 r15%20-low%20res%2020100615%20-.pdf
6. Амму С. Экономики за пределами финансового посредничества: кибервалюты", возможность роста, снижения уровня бедности и международное развитие", Рабочая тетрать Колумбийского Университета, No 82, ноябрь 2013 г.
7. Маллиган СЕА "Коммуникационные отрасли в эпоху конвергенции, Рутледж, 2011 г.
8. Сван М. "Блокчейн: Проект новой экономики" О' Рейли Медиа Инк, 2015 г.
9. Более подробный список литературы доступен "Bitcoin Series 24: Список основных публикаций по теме Блокчейн" Доступно на http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the- mega-master-blockchain-list (доступ 13 августа 2015 г.)
10. Комиссар ЕС по налогообложению Альгирдас Шемета, процитирован в 2013 г на сайте http://www.eureporter.co/economy/2013/09/20/fight-against-fraud-study-confirms- billions-lost-in-vat-gap/ (по состоянию на 18 Сентября 2015)

Глава 7

1. ISO/IEC 29115 - Основы безопасности аутентификации объектов
2. Включая совместное видео Boeing, Northrop Grumman и Raytheon.
3. Укрупненный анализ стратегии кибербезопасности ЕС , 28 февраля 2014 г.

Глава 7. Практический пример: Розничный рынок энергетики Европы

1. Европейская комиссия "Рамочная стратегия гибкого энергетического союза с долгосрочной политикой изменения климата", 25 февраля 2015г. COM(2015) 80 final. Доступно на сайте http://eur-lex.europa.eu/resource. html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0001.03/DOC_1&format=PDF
2. Центр совместных исследований Доступно на сайте https://ec.europa.eu/jrc/

Благодарности

Я хотел бы поблагодарить многих коллег за поддержку, которую они оказали при составлении этого обзора - сэр Марк Уолпорт, главный научный советник Правительства.

Комиссию экспертов за руководство и составление обосновывающих документов:

Ричарда Брауна	R3
Патрика Карри	Управление федерации бизнеса Великобритании
Ричарда Копленда	Группу CGI
Доктора Фила Годсиффа	Университет Суррея
Майка Холсалла	Университет Сингулярити/ Олманис
Дервена Хиндса	CESG
Мэтью Джонсона	Guardtime
Доминика Хобсона	COOConnect
Доктора Вили Ледонвирта	Оксфордский университет
Джонатана Левина	Chainalysis
Доктора Кэтрин Маллиган	Империал Колледж Лондон / Катапульта будущих городов
Профессора М. Энджелу Сасс	Университетский колледж Лондона
Доктора Криса Сира	FiNexus
Дэниэла Шиу	GCHQ
Саймона Тэйлора	Barclays

Дополнительно хотелось бы поблагодарить за консультации:

Хэдли Биман	GDS
Д-ра Джона Бэрда	EPSRC
Алестера Брокбанда	Британское посольство, Таллинн, Эстония
Д-ра Джорджа Данези	Университетский колледжа Лондон
Шоль Дэвида	UKTI
Ника Дэвиса	DWP
Игоря Наи Фовино	Совместный исследовательский центр, Европейская комиссия
Лин Кемп	Everledger
Д-ра Сару Майклджон	Университетский колледж Лондона
Жан-Пьера Нордвика	Совместный исследовательский центр, Европейская комиссия
Тома Прайса	BIS
Томаса Уилкинсона	МВД Великобритании
Наоми Райт	Министерство Ее Величества по налоговым и таможенным сборам

Команду экспертов за поддержку и обобщение обосновывающих документов:

Д-ра Клэр Крейг	GO-Science
Мартина Гласспул	GO-Science
Эмму Гриффит	GO-Science
Элизабет Сурковиц	GO-Science

Редактор
Д-р Марк Пеплоу

Данная публикация доступна на сайте www.gov.uk/go-science
Свяжитесь с нами, если у вас возникли какие-либо вопросы об этой публикации, включая запросы на получение альтернативных форматов, по адресу:
Государственное Управление науки
1 Виктория стрит
Лондон SW1H 0ET
Телефон: 020 7215 5000
E-mail: contact@go-science.gsi.gov.uk
GS/16/1
Дизайн и производство: WordLink