СКОЛКОВО
Московская школа управления

ТЕХНОЛОГИИ В КРИПТОИНДУСТРИИ: СОСТОЯНИЕ, СТРАТЕГИИ И ЭФФЕКТЫ

Центр финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО

Оглавление

РЕЗЮМЕ

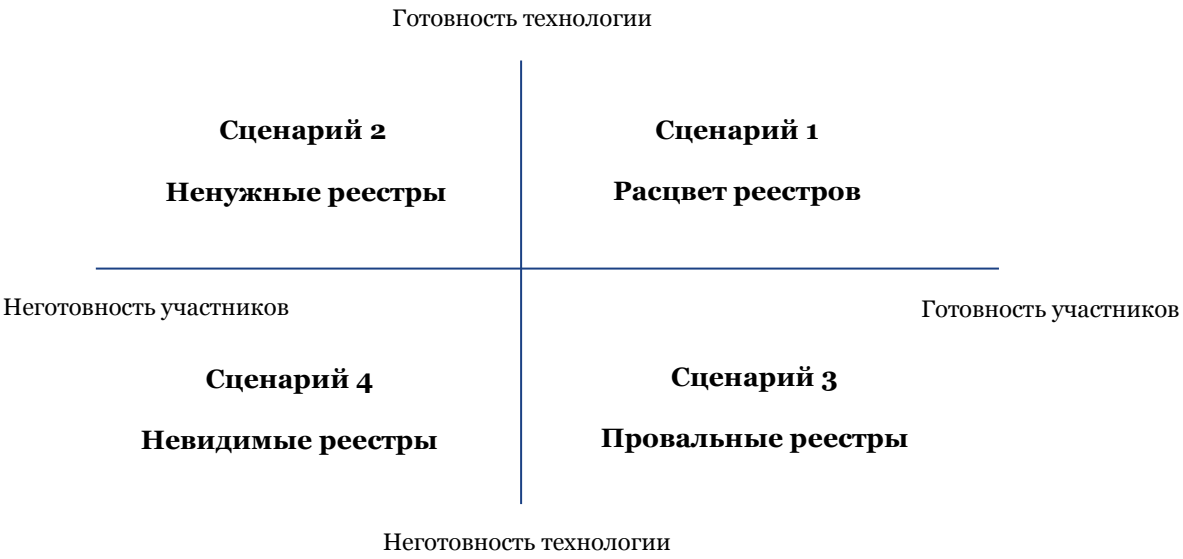
Криптоиндустрия стремительно набирает популярность. При этом все чаще как участники традиционных индустрий, так и специалисты криптоиндустрии отмечают особую роль технологий распределенных реестров (РР) в развитии фундаментальных инноваций, связанных с цифровой трансформацией как отдельных бизнесов, так и экономики в целом. 2018 год стал годом проектов, посвященных развитию инфраструктуры криптоиндустрии — с помощью как запуска новых РР, так и генерации инстанций уже существующих. При этом помимо уже известных крупнейших платформ, популярность стали набирать и нишевые проекты, полностью построенные с нуля. Так, на ICO стали все чаще выходить проекты, связанные больше с развитием инфраструктуры криптоиндустрии в целом, нежели с конкретными применениями РР, в том числе и в корпоративном сегменте. На данный момент у крупнейших корпораций из различных областей существует более 55 значимых проектов на стадии экспериментов или полноценного функционирования, связанных с развитием инфраструктуры криптоиндустрии.

Возрастающее число инфраструктурных предложений с одной стороны и увеличивающаяся неопределенность относительно технологической интеграции и уровня развития РР — с другой послужили мотивацией к созданию данного исследования. Данный отчет — второй в серии отчетов Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО, посвященных криптоиндустрии. Он систематизирует текущее состояние технологического развития в криптоиндустрии, предлагает новый метод классификации типов РР, а также предоставляет стратегический анализ настоящего и будущего криптоиндустрии в России и мире. Отчет будет полезен представителям частного и публичного секторов, которые планируют реализацию проектов, связанных с технологией РР, и другим участникам экосистемы криптоэкономики, заинтересованным в развитии криптоиндустрии.

Основные выводы:

1. **Для скачка в развитии криптоиндустрии необходимо создание РР разных типов. Исходя из технологических (архитектуры и структуры управления) и стратегических (универсальность и подрывной потенциал) классификаторов выделяется 24 типа РР.** Существующая инфраструктура криптоиндустрии в большей степени состоит из публичных неконтролируемых универсальных подрывных РР (21-й тип). Существует несколько примеров консорциумных и частных РР, большая часть которых — поддерживающие и контролируемые. Остальные типы РР не представлены.
2. **Исходя из типа РР меняются их технологические составляющие. Технологическая экосистема — компонент РР — состоит из двух кругов.** Внутренний круг — это основные элементы технологической архитектуры РР, которые определяются во время дизайна и запуска РР. Внешний круг — это различные особенности и базовые применения РР, которые чаще всего выходят за пределы внутреннего устройства РР и появляются при его функционировании как часть создающейся экосистемы.
3. **Текущие вызовы криптоиндустрии включают в себя регулирование, управление на РР, конфиденциальность данных, безопасность, масштабируемость и скорость изменений публичных РР.** Ключевые участники более широкой экосистемы, оказывающие влияние на формирование криптоиндустрии, включают в себя государство и регулятор, международные организации и регуляторы, экспертов, СМИ, индустриальные ассоциации, поставщиков ресурсов, инвесторов и новых игроков.

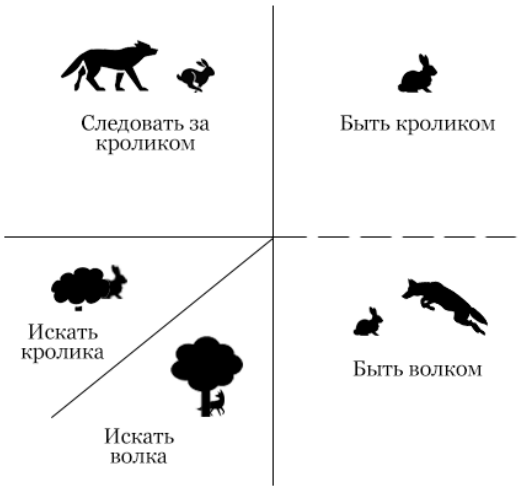
4. **Встраивание криптоиндустрии в контекст цифровой экономики возможно при готовности как технологий, так и участников экосистемы.** В разрезе осей поведения (готовности) участников и структуры внешней среды (готовности технологии) формируется четыре сценария будущего индустрии.



5. **Схема классификации и стратегический анализ профилей РР может помочь потенциальным участникам определить наиболее подходящий РР.** Первый вопрос, на который необходимо ответить при выборе, работать ли с РР, — это «Планируется ли в вашем применении работа с цифровыми записями?». Если ответ — «да», РР может являться опцией для рассмотрения среди других альтернатив, а следующим этапом является выбор архитектуры, структуры управления, степени универсальности и подрывного потенциала.
6. Всего существует **21 уникальный (первичный) распределенный реестр**. Большая часть из них (14 из 21, или 66,67%) являются **публичными, неконтролируемыми, универсальными и подрывными (21-й тип)**. Публичные РР 21-го типа можно считать универсальной инфраструктурой, которая управляется автоматически с помощью набора кодов и децентрализованных приложений. Этот вариант РР наиболее похож на интернет, который не имеет кнопки отключения и может быть адаптирован практически под любые нужды.
7. **Консорциумные РР в первую очередь создаются для автоматизации бизнес-логики между различными компаниями.** Консорциумных РР намного меньше; среди наиболее популярных всего 3 проекта: Corda, Hyperledger и Symbiont. Среди консорциумных РР, наоборот, чаще встречаются нишевые, а не универсальные РР.
8. **Ключевая ценность частных РР до сих пор не определена** и чаще всего сводится к возможности создания узлов для просмотра/аудита транзакций. Существует 3 уникальных частных РР, упоминаемых в публичных источниках (Chain, Openchain, Hydrachain).

9. **На текущий момент насчитывается более 50 уникальных областей применения РР.** В целом, на основании анализа применений, с точки зрения стратегии использования РР, можно выделить три основных типа идей, лежащих в основе применений РР: устранение доверия и массовая альтернатива, автоматизация бизнес-логики, верифицируемая база данных

10. **Формирование технологической инфраструктуры должно основываться на осознанной стратегии участников криптоиндустрии.** В разрезе отношения к другим предложениям и наличия собственного предложения формируется четыре основных стратегии поведения участников, в частности, создателей PP. Без осознанной стратегии невозможно эффективное формирование инфраструктуры.



Введение

За последние несколько лет криптоиндустрия из нишевой отрасли, о которой слышали только энтузиасты, связанные с технологиями или финансовыми услугами, превратилась в широко узнаваемую индустрию среди разных слоев населения как в России, так и в мире. Несмотря на то, что у рядового потребителя криптоиндустрия ассоциируется в первую очередь с криптовалютами, представители бизнеса и эксперты из различных отраслей все чаще обращаются непосредственно к технологии, породившей запуск и развитие всей криптоиндустрии, а именно технологии распределенных реестров (РР).

Несмотря на относительную молодость криптоиндустрии, она уже успела несколько раз кардинально измениться. Период 2017–2018 годов не стал исключением: на фоне осознания крупных проблем, связанных с лежащей в основе наиболее популярных криптовалют технологией, участники рынка переметнулись с поиска применения РР и попыток извлечь выгоду на быстрорастущем рынке с помощью разных инструментов (от трейдинга до привлечения средств) на формирование подходящей инфраструктуры для обеспечения эффективного функционирования индустрии. В результате среди 4576 ICO более половины (54,46%) составили проекты, связанные с платформами, а еще 39,4% — с привлечением средств на создание криптовалют. Отдельно 504 проекта было направлено на создание инфраструктуры. Все эти проекты приводят к появлению новых РР, новых инстанций РР или иных форм развития технологии. При этом активность ICO, по статистике на декабрь 2018 года, снижается: в ноябре 2018 года привлекли всего $65 млн. Помимо значительного снижения стоимости практически всех криптовалют, а также повышения осознанности инвестиций в криптоиндустрии, это может указывать на насыщение рынка.

Корректная инфраструктура РР может не только обеспечить качественный скачок в развитии криптоиндустрии за счет появления масштабных применений РР либо в рамках существующих процессов и бизнес-моделей, либо для создания подрывных решений, обеспечивающих фундаментально новые принципы функционирования экономики, но и заложить основу формирования криптоэкономики, в которой преимущества РР и их применений обеспечат новые правила и форматы взаимодействия различных участников. Такой потенциал технологии возводит РР в статус ключевых компонентов цифровой экономики и делает выбор подходящих платформ и технологий для своих целей одним из основных стратегических выборов как для государства и бизнеса, так и для других участников. Одновременно с этим растущее количество проектов, повышающаяся сложность технологической архитектуры, а также вероятность того, что, несмотря на растущее число предложений, подходящей инфраструктуры на рынке все еще может не существовать, делает работу с РР как никогда сложной.

В контексте возрастающих вызовов, связанных с криптоиндустрией, Центр финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО запустил серию комплексных исследований, посвященных наиболее актуальным темам, связанным с криптоиндустрией. Первый отчет «Регулирование в криптоиндустрии: состояние, стратегии, эффекты»[1] был посвящен анализу глобальных трендов крипторегулирования, стратегиям регуляторов и государственных органов различных стран и эффектам от вмешательства в криптоиндустрию. Данный отчет — второй в этой серии. Фокусом данного исследования является разработка схемы классификации РР, исходя как из технологических, так и из стратегических решений создателя системы, а также стратегический анализ текущих технологий и действий

[1] Здесь и далее «первый отчет серии исследований» означает данный отчет. Доступен онлайн: https://finance.skolkovo.ru/ru/sfice/research-reports/1797-2018-10-31/.

различных участников системы. Несмотря на растущее число отчетов и информации, появляющейся в отношении как технологии PP, так и криптоиндустрии в целом, до сих пор большая часть схем классификации ограничивалась лишь архитектурой PP, а описание технологических элементов инфраструктуры и текущих предложений никак не было связано со стратегическими решениями различных участников экосистемы. При этом анализ текущих предложений не учитывал гипотетические возможности и еще не реализованный потенциал PP, а большинство моделей выбора, нацеленных на облегчение принятия решений относительно использования технологии, не были независимыми и также не учитывали возможности создания собственной инфраструктуры различными участниками, а подразумевали использование уже имеющихся решений. Данный отчет решает эти проблемы и предлагает фундаментально новую схему классификации проектов, а также подходы к анализу принятия решений различными участниками и к стратегическому анализу текущего состояния, потенциала и тенденций развития технологической стороны криптоиндустрии.

Данное исследование будет полезно всем участникам, заинтересованным в развитии криптоиндустрии, а также изучении и понимании технологических аспектов ее функционирования. В частности, государство и бизнес могут использовать предложенную рамку для анализа и принятия решений относительно технологических выборов в криптоиндустрии и выработки конкретных решений относительно внедрения PP в свою деятельность. Новые участники экономики, предлагающие решения, связанные с криптоиндустрией, могут определить на базе данного анализа незакрытые ниши и возможности для развития собственных предложений и проектов. Регуляторы и институты поддержки, инвесторы и разработчики, используя результаты анализа из всех отчетов серии, могут определить разницу между применениями PP и лежащей в их основе технологией для формирования релевантных стратегий развития, инвестирования и поддержки проектов, а также защиты интересов участников индустрии.

Данный отчет состоит из шести ключевых разделов. 1-й раздел посвящен анализу ключевых моделей выбора PP и мотивации к внедрению PP. 2-й раздел предлагает новый взгляд на технологическую экосистему и технологические составляющие PP. Раздел 3 посвящен анализу текущего технологического состояния криптоиндустрии. 4-й раздел предоставляет основные результаты — схему классификации типов PP. 5-й раздел посвящен стратегиям поведения различных участников в криптоиндустрии. Раздел 6 — это взгляд на наиболее актуальные тренды, вызовы и будущее криптоиндустрии.

РАЗДЕЛ 1. МОТИВАЦИЯ К ВНЕДРЕНИЮ РР

Ключевые эффекты внедрения РР

Технология РР чаще всего ассоциируется с тремя основными эффектами на индустрию или проект, в который она внедряется.

1. Неизменность (immutability)

Дизайн РР создан таким образом, чтобы изменения записей происходили только по согласованию с создателем/управляющим лицом[2]. На данном этапе развития технологии существует значительное количество заблуждений вокруг неизменности записей в РР. Некоторые пользователи считают РР по определению полностью неизменным, однако это не так. Сродни другим программам и системам, РР является неизменным относительно тех правил, что прописаны в его программном коде и технической архитектуре системы. Поэтому записи в РР могут быть неизменными с точки зрения одних участников, но изменяемыми с точки зрения других. Возможность отдельных участников системы изменять записи в РР относится к структуре управления РР: контролируемые РР дают суперпользователям такую возможность, а неконтролируемые — нет.

В целом, практическая неизменность записей в РР обеспечивается:

- **Экономическими мотивами**, которые делают попытки поведения против правил системы (напр., взлома) дорогими относительно поведения согласно правилам системы.
- **Отсутствием API для изменения и удаления записей**, что требует более сложного проникновения в зачастую проприетарную или функционирующую систему.
- **Репликацией данных**, которая требует одновременного изменения записей не в одной базе данных, а во всех ее копиях.
- **Внешними и внутренними контролерами** (watchdogs). Внешние аудиторы могут проверить данные в РР с помощью анализа записей в открытых РР или с помощью специального узла в закрытых и консорциумных РР. Аудиторы могут инициировать проверки по своей воле, а также по инициативе управленцев/создателей РР и, в потенциале, по требованию со стороны регулятора. В качестве аудитора может выступать не только специализированная организация, но и публика. Внутренними контролерами обычно выступают держатели узлов системы или валидаторы транзакций.
- **Правилами и условиями хранения данных**. Некоторые виды правил и условий хранения данных (например коды с автоматическим удалением ошибок (error-correction codes)) делают несанкционированные изменения сложнее, а их идентификацию и отмену — проще.
- **Криптографическими подписями**, обеспечивающими возможность отслеживания попыток изменения записей. При этом записи и транзакции могут подписываться не одним, а несколькими участниками (multisignature). Криптографическая подпись уникальна для каждого участника системы и изменяется при взломе записей, при их передаче или хранении.
- **Периодическими** полными или частичными **резервными копиями.** Резервное

[2] Стоит отметить, что под неизменностью имеется в виду практическая неизменность (practical immutability) РР в силу того, что записи технически в теории могут быть изменены, в том числе благодаря использованию квантовых вычислений. Тем не менее на текущем этапе развития технологий сложность изменения записей в РР делает их практически неизменными.

копирование может производиться на другие РР, распечатки, жесткие диски или любые носители информации.

- **Самообеспечением безопасности узлов**. Владельцы/держатели узлов могут выработать собственные правила взаимодействия и хранения информации для себя и своих сотрудников (если масштабы узлов подразумевают хранение не одним лицом, а группой).
- **Разнообразием узлов**. При этом разнообразие может быть не только относительно географии, но и относительно любых других характеристик держателей узлов. Данная мера может также восприниматься как инструмент управления рисками (например, географическая диверсификация защищает от риска природных явлений, а юридическая — от геополитических и регуляторных рисков).

PoW (Proof of Work), наиболее распространенный протокол консенсуса, обеспечивает неизменность РР с помощью экономических стимулов. Технологически каждый блок в РР имеет запись о хэше. В ряде РР каждый блок также хранит хэш предыдущего блока, что делает попытку изменения записей в РР экономически дорогой, так как, чтобы взломать блок РР, необходимо потратить ресурсы, которые были потрачены на создание данного блока, а также всех блоков, созданных после данного блока. В силу того, что создание блока — динамический процесс, а блоки создаются лишь с определенной скоростью (например, в биткоине среднее время создания одного блока — около 10 минут, в litecoin — около 2 минут, в NEO — около 15 секунд, а в Ethereum — около 20 секунд), которая, помимо прочего, сопряжена с уровнем сложности в системе. По данной причине практически все существующее оборудование не способно достичь скорости создания блоков в крупнейших РР.

Во втором самом распространенном типе консенсусных протоколов (PoS, Proof of Stake) чаще всего используются внутренние контролеры, а экономические мотиваторы, при наличии, направлены в первую очередь на стимулирование их действий и стратегий поведения. Внутренние валидаторы проверяют состояние системы на каждой обозначенной отметке (checkpoint) — например, каждые 100 блоков, как в предлагаемой Ethereum системе перехода на PoS — Casper. После этого они ставят отметку о том, что нарушений не было, а верифицированные блоки считаются финальными и неизменными. Если до этого мошенник удачно взломает записи, а программа/валидаторы не заметят этого (например по изменению криптографической подписи), то изменения могут зафиксироваться как финальные, а взлом будет считаться успешным. По данной причине эти системы могут быть более уязвимы с точки зрения неизменности, но при этом иметь другие преимущества, в том числе с точки зрения скорости.
Тем не менее развитие которого достигли квантовые компьютеры, теоретически может обеспечить возможность совершать расчеты со скоростью, необходимой для успешного взлома записей в РР, однако наиболее мощные на данный момент квантовые компьютеры не способны взломать сеть, к примеру, биткоина[3]. Более того, при активном развитии квантовых технологий РР также могут создаваться с элементами данных технологий (например, квантовой криптографии), что обеспечит большую безопасность систем.

Помимо попытки взлома, изменение записей в РР может происходить по решению контролеров (в контролируемых РР) или участников системы (в неконтролируемых РР). В контролируемых РР это может происходить на основе решения управляющих лиц, а в неконтролируемых — посредством форка. Форк при этом может быть инициирован различными участниками системы, например, непосредственно группой разработчиков или пользователями, а режим принятия решений об

[3] См., например: https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/ или https://arxiv.org/pdf/1710.10377.pdf.

имплементации того или иного форка зависит от структуры управления РР (on-chain или off-chain управление). При этом форки могут быть мягкими (soft) или жесткими.

В любом случае, неизменность РР, во-первых, является относительным показателем и обеспечивается рядом факторов и характеристик системы, а во-вторых, является итеративной функцией, которая с развитием технологий может быть более или менее развитой.

2. Транспарентность

Транспарентность РР — это свойство записей, которое отвечает за возможность участников системы, а иногда и любых желающих внешних участников, просмотреть записи, хранящиеся в РР. Однако необходимо понимать, что транспарентность не эквивалентна полной прозрачности, поэтому РР не делает абсолютно всю информацию, связанную с РР, доступной всем желающим участникам.

В наиболее транспарентных на данный момент РР — например, публичных неконтролируемых РР, таких как Ethereum или блокчейн биткоина, — доступны полуанонимные записи о всех транзакциях. С помощью данных о публичном адресе кошелька (чаще) или различных идентификаторах транзакции/участника системы (в зависимости от конкретного РР) любой желающий может воспользоваться поисковым механизмом (explorer) для поиска информации о записях, хранящихся на РР и связанных с данным адресом/транзакцией/идентификатором/участником/кошельком. Однако это не означает, что без наличия информации о публичном адресе участник может узнать информацию о записях в РР. Чаще всего, даже при возможности скачать РР полностью или воспользоваться поисковым механизмом, доступна лишь обезличенная информация, которая имеет ограниченную ценность без дополнительной информации, которая хранится вне РР (например, о том, кому принадлежит публичный адрес или ключ).

Тем не менее, в силу того, что нынешние системы хранения и использования данных чаще всего централизованны и недоступны для просмотра, а записи хранятся в единой базе совместно с информацией о пользователях и связанных с ними действиях, любой РР предлагает некоторое улучшение транспарентности по сравнению с традиционной системой хранения данных. Однако и в классических системах хранения могут быть встроены различные технические свойства для различных целей (например, криптографическое шифрование для обеспечения безопасности хранения информации, распределенные базы данных и др.), что в результате может обеспечить большую транспарентность, чем у РР.

Среди РР также есть отличия в отношении транспарентности, подробнее о которых сказано в разделе 4. Публичные неконтролируемые РР, как наиболее распространенные и первыми набравшие популярность, характеризуются большей степенью транспарентности, чем, к примеру, частные контролируемые РР. Однако даже в частных РР возможна настройка узлов просмотра и других способов повышения транспарентности. В целом, несмотря на отличия между типами РР, чаще РР характеризуются более высоким уровнем транспарентности, что в контексте неизменности особенно важно для индустрий и процессов, требующих различных участников и имеющих вероятность компрометации данных. По этой причине ряд первых применений РР нацелен на создание приложений для цепочек поставок или индустрии здравоохранения.

3. Автономность

Первый распространенный и наиболее популярный РР, блокчейн биткоина, не имеет единого органа управления/контролирующей организации. При этом подобная характеристика присуща большинству публичных РР, имеющих неконтролируемый характер (большинство существующих примеров РР). По этой причине РР чаще ассоциируются с неподконтрольной системой, консенсус в которой достигается непосредственно участниками РР, нежели создателем/контролером. Подобная характеристика РР является одной из характеристик их автономности.

С другой стороны, вторая характеристика автономности РР — это возможность настройки автоматизации процессов с помощью РР. Начиная со второго наиболее популярного РР, Ethereum, внедрение слоя автоматизации (умных контрактов) превратилось в индустриальный стандарт для РР. Большая часть существующих РР имеют ту или иную версию умных контрактов в своей технологической архитектуре. Умные контракты работают по логике IFTT (If this then that, или «Если это, то то») и помогают автоматизировать процессы, происходящие на РР. При этом подобная конструкция возможна практически в любой технологической архитектуре, однако благодаря неизменности и транспарентности записей в РР умные контракты обладают большей степенью влияния и могут применяться на более широком спектре задач, чем обычная автоматизация.

В отличие от первой характеристики РР, которая в большей степени присуща неконтролируемым РР, умные контракты могут быть внедрены и в контролируемую систему. Для обеспечения автономности РР с помощью отсутствия контроля чаще всего используют какой-либо протокол консенсуса. На данном этапе существует два наиболее популярных типа протокола консенсуса: Proof of Work (PoW), впервые примененный в контексте РР в блокчейне биткоина, и различные версии Proof of Stake (PoS) (например, классический PoS, delegated PoS, leased PoS). Более подробно протоколы консенсуса описаны в разделе 2.

Для обеспечения функциональности умных контрактов необходима интеграция информации из различных источников. Умный контракт подключает такую информацию с помощью оракулов. Оракул — это инструмент интеграции информации из различных источников в РР или в различные его элементы. Существуют различные способы классификации оракулов[4], однако наиболее полезным может быть разделение на внутренних оракулов, которые используют информацию, хранящуюся непосредственно в РР, и внешних оракулов, которые используют информацию из различных внешних по отношению к РР источников. Более подробно оракулы описаны в разделе 2.

В целом, необходимо понимать, что автономность РР — это не бинарный выбор. Существует несколько уровней автономности, а некоторые РР, которые не поддерживают автоматизацию и при этом являются контролируемыми, могут и вовсе полностью управляться вручную. Однако, при сравнении среднего РР и средней традиционной системы хранения данных, большая часть РР склонна иметь более высокую степень автономности. Автономность также часто ассоциируется с устранением необходимости доверия к создателю/управляющему РР, однако необходимо отметить, что данные два понятия не эквиваленты. О роли РР в устранении необходимости доверия будет сказано в разделе 4.

[4] См., например: https://blockchainhub.net/blockchain-oracles/.

Модели выбора PP (decision trees)

В последние годы многие криптоэнтузиасты и некоторые организации, выступающие в качестве экспертов в различных технологиях, в том числе PP, поставили перед собой задачу создания моделей выбора правильных PP[5]. Существует даже ряд шуточных моделей, которые отвечают «нет» на вопрос «необходим ли мне PP» при любом исходе, — тем не менее это может быть правдой, так как сам PP редко необходим различным участникам. PP стоит рассматривать в более широком контексте потенциальных решений задач участника, среди которых могут быть и другие технологии.

Одними из первых подходов к помощи выбора между различными типами PP являются модель от Consult Hyperion и модель Суичиса. Первая модель подразумевает, что пользователь уже пришел к выводу о том, что PP нужен, и позволяет выбрать более подходящий PP из четырех возможных (в зависимости от возможности ограничения участия (permission) и архитектуры PP (частные и публичные)), исходя из ответов на вопросы относительно ограничения прав участия и способа сохранения неизменности PP. Вторая модель более сложная и добавляет возможность получения отрицательного исхода относительно использования PP, основываясь на вопросах, касающихся целей и структуры участников, а также технических характеристик относительно публичности и контролируемости транзакций. Обе модели основаны на текущем состоянии развития криптоиндустрии и смешивают различные характеристики PP воедино. Так, например, в модели Суичиса, если участнику необходим контроль, то ему советуют выбрать частный или консорциумный (гибридный) PP, в то время как при необходимости существования доверительного третьего лица участнику вовсе не рекомендуется использовать PP. Подобный подход может быть корректен исходя из текущих трендов[6], однако он может ограничить инновации в области PP и исключить попытки создания новых типов PP, о которых (в том числе и об их целесообразности) подробно описано в разделе 4.

Последующие модели схожи с моделью Суичиса. Например, IBM предлагает подобную модель на основе ключевых эффектов от внедрения существующих PP. А модель Гарднера схожа с моделью Суичиса, но предлагает большую степень разделения между различными типами PP (исходя из архитектуры). Другие модели используют подобную логику, однако чаще ограничиваются либо применениями публичных PP, либо типичной логикой, стоящей за применениями PP, описанной в разделе 3. Интересной моделью является подход DHS, который предлагает различные альтернативы относительно PP с точки зрения хранения данных, исходя из текущих ограничений. Тем не менее критерии выбора PP также достаточно строги и основываются лишь на подтвержденных текущих, а не гипотетических применениях PP. Подобный подход изложен в модели Коэнса и Полла (2018), однако в их работе добавляются примеры PP и различных баз данных, которые могут быть использованы в качестве отправной точки для разработки собственных PP.

Один из наиболее фундаментальных подходов к PP изложен в работе WEF (2018), где, основываясь на исследовании PP в разных областях экономики, команда форума придумала рамку для анализа необходимости и применений с высоким потенциалом для PP. Данная модель — первая, которая основывается не только на уже существующих и разработанных PP, но и, потенциально, на применениях, которые находятся в стадии разработки. Первые три вопроса нацелены на понимание, необходим ли вообще PP компании/участнику. Первая причина использования PP подразумевает создание угрозы традиционным бизнес-моделям, в частности, направленность на

[5] Обширная коллекция большей части известных и популярных PP доступна в подборке Себастиена Мейниера: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1.
[6] Подробнее о текущих направлениях развития технологии и криптоиндустрии описано в Разделе 3.

устранение посредников. Два других вопроса касаются работы с цифровыми активами и возможности настройки постоянной записи о цифровом активе. После этого, в зависимости от необходимых технических характеристик, определяется, возможно ли применение РР на данном этапе, или проекты еще находятся в разработке. Затем, исходя из ответов на ряд вопросов относительно сущности проекта (необходимости возможности одновременного изменения записей, доверия участников друг к другу, возможности публикации транзакций и тд.) выбирается, нужно ли исследовать РР глубже или это один из подходящих кейсов под существующие примеры применений частных или публичных РР. Несмотря на относительную простоту, данный подход позволяет катализировать появление инноваций в области РР и направить исследования потенциальных пользователей в нужное русло. Тем не менее данный подход подразумевает, что РР обязательно подрывные (исходя из первого вопроса), что может дискредитировать потенциал поддерживающих РР.

В целом, текущие модели выбора РР чаще основываются на уже существующих успешных применениях РР, а также, в основном, на архитектурных различиях РР. Помимо этого, даже наиболее проработанные модели принятия решений относительно РР считают данную технологию подрывной, таким образом ассоциируя все применения с разрушением сложившихся процессов и традиционных бизнес-моделей. Ни одна из моделей не учитывает стратегические альтернативы РР (относительно подрывного потенциала и универсальности приложений), а большинство моделей ограничиваются исключительно архитектурными различиями между РР, не беря во внимание возможные различия в структуре управления. При этом ряд моделей предлагает выводы относительно применимости РР не в рекомендательной форме для дальнейшего изучения, а в более-менее однозначной — о необходимости/ненадобности РР определенных типов.

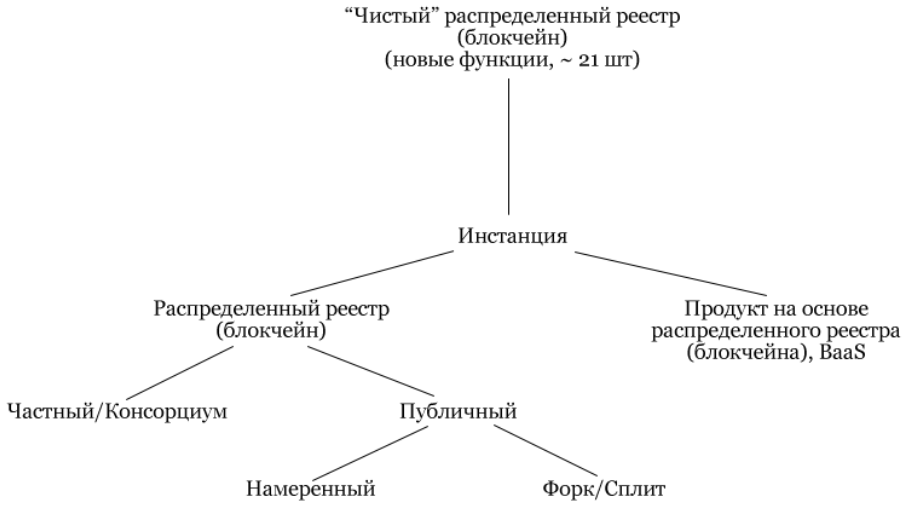
Чтобы решить образовавшиеся пробелы в моделях решений относительно РР, а также в подходах к классификации различных реестров, данный отчет предлагает новый подход к созданию типологии РР, изложенный в разделе 4. Исходя из этого подхода, в дальнейшем может быть выработана новая модель принятия решений относительного того, какой из РР необходим. Стратегический анализ, динамика изменения типов РР, а также предварительные рекомендации в области принятия решений относительно РР, учитывающих вышеуказанные недостатки, описаны в разделе 5. Тем не менее перед классификацией и построением модели выбора РР необходимо определить технологические характеристики и экосистему РР, а также описать их нынешнее состояние, чтобы задать верный контекст для принятия дальнейших решений.

РАЗДЕЛ 2. ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ СОЗДАНИЯ РР

Процесс создания распределенного реестра

Всего в мире, по состоянию на декабрь 2018 года, насчитывается до 100 известных уникальных распределенных реестров. 21 из них являются ключевыми и масштабными, а также имеют признание в криптоиндустрии, что позволяет использовать их в качестве отправной точки для изучения технологической стороны криптоиндустрии.

РИСУНОК 1. ТИПОЛОГИЯ СУЩЕСТВУЮЩИХ РР ПО ПРОИСХОЖДЕНИЮ



Источник: аналитика авторов

Исходя из сугубо технологических аспектов, РР бывают **первичными** (оригинальными или уникальными) и **вторичными**, иначе говоря, **инстанциями** уже существующего первичного РР. При этом инстанции можно разделить на **блокчейны** и на **продукты**. Продукты чаще всего представляют из себя какое-то решение, функционирующее по принципу **«блокчейн как услуга»** (BaaS, blockchain as a service), и предлагают клиентам использовать или адаптировать один из существующих РР под нужды и цели заказчика. Некоторые из проектов (например chain.com) являются универсальными, в то время как остальные (например Quorum) — нишевыми для определенной индустрии (например финансовых услуг).

Инстанции РР, в свою очередь, разделяются на частные и консорциумные, а также публичные. **Частные инстанции РР** невозможно технически отследить. В данном контексте создание частной инстанции распределенного реестра схоже с созданием сайта или внутренней сети (intranet) на локальном сервере компьютера: до тех пор, пока версия инстанции, созданная на локальном сервере, не загружена на веб-хостинг и недоступна для внешних пользователей, только те устройства, которые доверены/подключены к локальной внутренней сети, имеют доступ к инстанции блокчейна. **Консорциумные РР** подразумевают схожую структуру, но доступ к инстанциям не ограничен рамками одной компании, поэтому информация о них чаще становится известной. По аналогии с интернет-сайтами, консорциумные РР ближе всего к закрытым сайтам, весь контент которых доступен только с разрешения владельца сайта и/или существующих пользователей. **Открытые блокчейны**, в свою очередь, сродни большинству сайтов или интернету в целом: полностью открытая система, доступ к которой может получить любой желающий, иногда соответствующий определенным критериям, установленным дизайном протокола.

Открытые РР можно разделить на два типа, исходя из того, каким образом они появились. Первый тип РР появляется **преднамеренно**, когда частная инстанция блокчейна становится общедоступной на открытом веб-хосте. Чаще всего такие блокчейны близки по своим характеристикам к тому блокчейну, инстанция которого была изначально сделана. То есть отличия чаще всего касаются инкрементальных изменений (например, правила консенсуса, размер блока, ограниченность эмиссии и др.).

Второй тип открытых РР — результат форка, который привел к расколу сообщества какого-либо блокчейна. Форк — это предложение разработчиками изменений в существующий протокол РР. Форк бывает двух типов: **жесткий** (hard fork) и **мягкий** (soft fork). **Жесткий форк** — это предложение изменений, которые противоречат существующему протоколу РР и могут привести к конфликту, если сеть валидаторов не обновит ПО (например, если новый размер блока, предложенный разработчиками во время форка, больше старого, то такой форк является жестким, так как новые транзакции, которые должны быть валидированы по новым правилам, могут быть одобрены только узлами с обновленным ПО. Таким образом, все, кто не обновил ПО, не смогут подтвердить транзакцию, которая должна быть подтверждена). **Мягкий форк** — ситуация, когда изменения в правилах открытого кода, предложенные разработчиками, не противоречат существующим правилам, а следовательно, не могут привести к конфликту узлов со старой версией кода (например, если максимально допустимый размер блока уменьшается в обновлении, предложенном разработчиками, то все старые узлы смогут валидировать транзакции, проведенные по новым правилам, так как размер блока будет всегда не больше максимальной границы, установленной в старых правилах). Успешность форка зависит от того, сколько узлов приняли исправления, предложенные разработчиками (то есть обновили версию ПО).

В случае, если и для новой, и для старой версий ПО существует достаточно большая доля узлов, может произойти конфликт между частями одного и того же РР. Если в результате конфликта не обнаружен консенсус и две группы пользователей РР не могут договориться о корректной версии кода, происходит **раскол** (split) системы. Только жесткий форк может стать причиной раскола РР, так как мягкий форк не противоречит старым правилам, а лишь уточняет их. Раскол РР[7] приводит

[7] Стоит отметить, что раскол РР приводит к уменьшению вычислительной мощности сети, что особенно актуально в блокчейнах, основанных на PoW. Помимо этого, раскол приводит к уменьшению положительных экстерналий и распространению знаний (experience & knowledge spillovers) в связи с уменьшением количества единомышленников, работающих над улучшением протокола. По этой причине форки считаются неблагоприятным событием в криптоиндустрии, а их успешность становится менее вероятной в крупных сетях, где разнообразие участников сопряжено с разными взглядами на будущее РР. В связи с этим изменения в некоторых открытых (с открытым кодом) блокчейнах при достижении критической массы участников становятся трудновыполнимыми и могут привести к расколу РР.

к образованию двух копий РР, где отражена вся информация, но отличается технический код протокола (отличие заключается исключительно в изменениях, которые были выдвинуты в результате жесткого форка). Таким образом может появиться публичная инстанция существующего блокчейна.

В связи с относительной легкостью создания новых инстанций блокчейна с одной стороны и необходимостью иметь универсальную платформу для создания и обмена криптоактивами — с другой, в современной криптоиндустрии возникает дисбаланс: РР должны быть достаточно масштабными, чтобы в полной мере представить клиентам выгоды от эффекта масштаба, но при этом, при получении критической массы клиентов, РР становятся негибкими, а предложения изменений могут спровоцировать раскол системы в связи с неоднородными участниками. По этой причине лидирующими РР все еще остаются несколько ключевых протоколов, где раскол системы приводит к незначительным потерям выгод, а созданные инстанции РР могут сосуществовать, или где существует четкая структура управления развитием РР (то есть основные разработчики сосредоточены в рамках одной/нескольких компаний, а код не является открытым к изменениям любым программистом).

Технологическая экосистема РР

Ключевые технологические блоки РР можно условно разделить на три составляющие: слой интернета, слой реестра и слой приложений[8]. При этом слой реестра состоит из P2P-сети устройств, правил консенсуса и непосредственно базы записей данных. Слой приложений состоит в первую очередь из умных контрактов и в ряде РР первого поколения не выделяется отдельно. Представленная архитектура особенно популярна среди РР второго поколения, к примеру Ethereum и подобных. Однако РР могут отличаться по своему наполнению (примером могут служить некоторые РР третьего поколения — например, в white paper ArcBlock[9] показана технологическая архитектура системы, в которой присутствуют значительные отличия от РР Ethereum (к примеру, адаптеры)).

В силу появляющихся отличий, стирания границ между различными слоями и возможности кастомизации и изменения технологических компонентов (в том числе исключения части компонентов) в новых РР данное исследование предлагает новый взгляд на технологические составляющие РР. Они представлены в виде экосистемы, а не слоев. При этом в большинстве случаев чем ниже находится тот или иной элемент РР, тем более основным для технологической архитектуры он является, однако четкого разграничения нет и поэтому явные границы между различными элементами не обозначены. В данной экосистеме выделено два круга: внутренний круг — это основные элементы технологической архитектуры РР, которые определяются во время его дизайна и запуска, в то время как внешний круг — это различные особенности и базовые применения РР, которые чаще всего выходят за пределы внутреннего устройства РР и появляются при его функционировании как часть создающейся экосистемы. Данные элементы необходимы для определения подходов к классификации РР и понимания, какие из элементов технологической архитектуры могут измениться при изменении тех или иных классификаторов. Визуально данная экосистема может быть изображена следующим образом.

[8] Хорошее описание технологической архитектуры РР и ее составляющих элементов представлено на сайте https://blockchainhub.net/blockchain-intro/.
[9] Доступна онлайн: https://www.arcblock.io/whitepaper/latest/.

РИСУНОК 2. ТЕХНОЛОГИЧЕСКАЯ ЭКОСИСТЕМА РАСПРЕДЕЛЕННОГО РЕЕСТРА

Источник: аналитика авторов

Внутренний круг — основной набор элементов РР

Протокол (механизм) консенсуса

Простыми словами, протокол консенсуса — это способ достижения договоренности в системе. Формально протокол консенсуса — это набор правил, описывающий, как должны быть устроены коммуникация и процессы передачи данных между различными электронными устройствами, узлами, чтобы участники пришли к единому мнению[10]. Эти правила определяются до запуска РР и несут две функции: они гарантируют, во-первых, что РР будет обновлен и, во-вторых, что ни один участник, который не должен иметь прав контроля над РР, не получит их. Одна из ключевых целей РР — сделать такие условия, чтобы всеми участниками была использована единая цепь.

Большинство публичных РР используют автономные механизмы достижения консенсуса, при котором согласие о транзакциях происходит автоматически, без специального вмешательства валидаторов или других участников. Примером подобных механизмов являются PoW-механизмы, где для майнинга требуется подключение специального оборудования. Однако среди множества консенсусных механизмов существуют также ручные и полуручные механизмы достижения консенсуса, при которых необходимо вовлечение валидаторов, соответственно, на всех или на части шагов в процессе верификации транзакций. Последние чаще, но не обязательно всегда,

[10] См., например, https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/consensus-protocols или Олфати-Сабер и Мюррэй (2004)

используются в частных или консорциумных РР.

Согласно данным исследования Satis Group "Cryptoasset Market Coverage Initiation: Technical Underpinnings"[11], 61,3% сетей используют PoW, 9,4% — гибрид PoW и PoS, и еще по 6,6% каждый — PoS и DPoS. Подобная статистика и доминирование данных систем — результат большой экосистемы биткоина и Ethereum, которые в том числе привели к появлению большого количества инстанций РР на основе своих РР[12]. Тем не менее, в связи с ростом количества РР, а также популяризацией криптоиндустрии, количество различных механизмов консенсуса значительно возросло. Некоторые РР и криптоэнтузиасты ставят перед собой задачу разработки новых механизмов консенсуса. В криптоиндустрии появилось мнение, что механизмы консенсуса — центральная составляющая криптоэкономики, так как зачастую именно в них определяются механизмы обеспечения мотивации участников РР. Ряд данных механизмов уже продемонстрировали свою несостоятельность; тем не менее различные протоколы консенсуса формируют возможности выбора для создателей РР относительно способов обеспечения единства сети. Несмотря на то что большинство механизмов консенсуса — это какая-то модификация PoS- или BFT-систем (Byzantine Fault Tolerance), ряд механизмов консенсуса отличаются кардинально: к примеру, Proof of Burn (PoB, при котором консенсус гарантируется с помощью отправки участниками коинов на счет кошелька/умный контракт, с которого они не могут списать средства), DAG (Directed Acyclic Graphs, которые являются альтернативными блокчейну системами, основанными на графах, позволяющих обрабатывать транзакции асинхронно) или Proof of Importance (PoI, при котором участники, которые часто получают и отправляют транзакции на РР, получают награду)[13].

В частных и консорциумных РР чаще всего консенсус определяется индивидуально каждым узлом (N2N, node-to-node-консенсус) или правила консенсуса прописываются на уровне всей системы. В силу того, что большинство частных и консорциумных РР, примеры которых существуют сегодня, — это контролируемые РР, использование механизмов консенсуса, которые чаще всего нужны в системах, где нет суперпользователей и участники равного уровня должны прийти к общему мнению, не стоит так остро. Тем не менее в ряде частных и контролируемых РР используются модифицированные механизмы консенсуса, упомянутые выше: например, в Chain используется версия BFT, а в части консенсуса Openchain используется запись на PoW-системы[14].

P2P-сеть устройств

В силу того, что РР подразумевает использование данных и их хранение на различных устройствах, P2P-сеть устройств является ключевым элементом всей системы. Большинство проектов используют компьютеры в качестве ключевого устройства, на котором хранятся копии РР. Тем не менее появляется ряд проектов, которые пытаются перенести технологию на мобильные устройства, а также на любые устройства, поддерживающих подключение к интернету (интернет вещей). Помимо этого, в PoW-системах и в ряде других механизмов консенсуса необходимо специальное оборудование, чтобы участвовать в верификации и записи транзакций. Наиболее популярные РР, которые используют компьютеры как основу своей P2P-сети, также рассматривают возможность поддержки мобильных устройств, тем не менее на текущий момент это еще не перешло в практическое русло.

---

[11] Доступно онлайн: https://research.bloomberg.com/pub/res/d2246jsnqusjYSeacPbQc2IjVIw.
[12] Подробнее о статистике платформ описано в разделе 3.
[13] Хороший набор механизмов консенсуса и их описание представлены, к примеру, на сайтах https://101blockchains.com/consensus-algorithms-blockchain/, https://blockchain.intellectsoft.net/blog/consensus-protocols-that-meet-different-business-demands/, https://blockchain.intellectsoft.net/blog/consensus-protocols-that-serve-different-business-needs-part-2/ и в отчете KPMG "Consensus. Immutable agreement for the internet of value" (https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf).
[14] Подробнее о конкретных РР описано в разделе 3 и в приложении 1.

Умные контракты

Простыми словами, умный контракт — это часть кода на РР, записанная в логике IFTT (if this, then that). Умные контракты — основной источник автоматизации на РР. Умные контракты должны обладать тремя основными свойствами: быть самоверифицируемыми, самоисполняющимися и защищенными от (несанкционированных) изменений. При этом для использования информации как с РР, так и извне реестра умному контракту необходимы оракулы. Умные контракты могут быть связаны с одним или несколькими (multi-signature) участниками. Помимо этого, ряд РР, в первую очередь те, которые позиционируются как платформы, используют виртуальные машины, в которых хранятся, исполняются и верифицируются (тестируются) умные контракты. Иногда виртуальную машину выделяют отдельным техническим элементом, однако почти всегда в текущих РР она играет одну из составляющих ролей в умных контрактах. В силу того, что умные контракты — основной источник автоматизации, они являются базой для более сложных применений автоматизации на РР (к примеру, децентрализованных автономных организаций (ДАО) и других).

Записи данных

Записи данных — это непосредственно формат и структура информации, хранящейся на РР. Исходя из потенциальных целей РР, формат и структура данных могут различаться. При этом информация не обязательно должна формировать блоки с течением времени: ряд РР не использует блочную структуру, поэтому их принято называть РР, а не блокчейнами. Обычно публичные РР более строги к структуре, чем частные и консорциумные, в силу того, что информация должна проходить через автоматизированный/стандартизированный механизм консенсуса. Более того, часть РР, которые поддерживают кастомизацию, могут содержать опциональные части в структуре своей информации или позволять участникам добавлять разделы. Часть РР фокусируется на возможности использования не только фактической информации, занесенной в РР, но и метаданных, связанных с различными записями и транзакциями (например Cardano). Записи данных в РР изменяются с помощью транзакций. Сами данные о записях могут быть представлены в финальном (текущем) состоянии записей, в виде списка примененных изменений или в виде изменений и предыдущего состояния.

Записи данных можно просмотреть с помощью поискового механизма (explorer), который можно как выделить в отдельный технологический элемент, так и записать в рамках данного элемента. Поисковый механизм позволяет просмотреть записи в РР любому участнику. Как было отмечено ранее, в большинстве случаев доступен просмотр полуанонимных или полностью анонимных данных о транзакциях, по причине чего без дополнительной информации об идентификаторах эти данные могут не дать всей полезной информации.

Транзакции

Транзакции на РР не обязательно относятся исключительно к передаче ценности от одного участника к другому. В контексте РР транзакция — это любой запрос участника на изменение записи в РР, который в дальнейшем проходит верификацию у других участников, оперирующих им согласно протоколу консенсуса. Существуют различные способы инициализации транзакций, однако практически все из них включают использование какого-то рода интерфейса (например криптокошельков[15]) для взаимодействия с РР. В зависимости от протокола консенсуса и структуры

[15] В данном контексте криптокошельки могли бы попасть во внутренний круг технологической экосистемы РР, однако в силу того, что большинство из них создается не при дизайне РР, а после его запуска и обычно другой группой разработчиков, нежели сам РР, криптокошельки вынесены во внешний круг.

записи данных ПО или другие участники проверяют валидность транзакций и, применяя их, изменяют записи в РР. Скорость проведения транзакций — один из ключевых параметров РР. В неконтролируемых РР обычно скорость проведения транзакций (время от момента инициации до изменения соответствующих записей в РР) значительно ниже, чем в контролируемых, однако ряд протоколов консенсуса, особенно в РР третьего поколения, предлагают решения, позволяющие достичь более высокой скорости транзакций, чем в традиционных системах. При этом зачастую подобные механизмы подразумевают компромисс в ряде других характеристик РР.

Токены (нативные)

Определение и классификация токенов были представлены в первой части данной серии отчетов[16]. Токен — это взаимозаменяемая (fungible) цифровая единица, представляющая ценность базового актива в цифровом пространстве и позволяющая при передаче через интернет (с записью на блокчейне) передать право контроля над активом/сущностью другому лицу. В большинстве своем нативные токены — это криптовалюты, так как большая часть инфраструктуры появилась в результате краудфандинга и создания именно криптовалют. Более подробная классификация и разделение токенов на четыре типа согласно швейцарскому регулятору FINMA (платежные токены, токены услуг, токены активов и гибридные токены) представлены в первой части серии отчетов.

Исследование Satis Group “Crypto Asset Market Coverage Initiation: Market Composition”[17] в рамках разделения на коины и токены предлагает более подробную классификацию токенов. Так, выделяя две основные группы — инвестиционные/секьюрити-токены и токены услуг/использования, — авторы предлагают разделять инвестиционные токены на те, что приносят доходность, и те, что основаны на ценности реальных активов, а токены услуг — на шесть категорий: сеть валют, частные сети (privacy networks), сети платформ, стейблкоины, сети криптобирж и мастерноды.

С технологической точки зрения токены могут лежать в основе обеспечения консенсуса как механизм мотивации участников. Помимо этого, ряд токенов (например gas в Ethereum) выполняют функцию защиты от спама и других видов атак, делая ряд базовых операций (например, написание умных контрактов или размещение ненативных токенов) небесплатными. Так как только нативные токены появляются в системе в момент ее создания и запуска, все ненативные токены можно считать частью внешнего круга технологической экосистемы РР.

Оракулы

Как и в контексте любых баз данных, оракул — это инструмент, позволяющий найти, верифицировать и интегрировать информацию из различных источников. Оракулы особенно важны в контексте умных контрактов, особенно вовлекающих нескольких/многих участников, как инструмент обогащения контракта данными и канал определения действий и момента его исполнения. Самое простое разделение оракулов — это внутренние оракулы, которые интегрируют информацию в различные части РР (например умные контракты) непосредственно из самого РР, и внешние оракулы, которые интегрируют информацию в элементы РР извне.

Blockchainhub[18] выделяет 5 основных типов оракулов:

[16] Исследование «Регулирование в криптоиндустрии: состояние, стратегии и эффекты», доступно онлайн: https://finance.skolkovo.ru/ru/sfice/research-reports/1797-2018-10-31/.
[17] Доступно онлайн: https://research.bloomberg.com/pub/res/d2gg3p_HTg39HRCuzQjIyy8NVZQ.
[18] Доступно онлайн: https://blockchainhub.net/blockchain-oracles/

I. По источнику информации:

1. Программные оракулы.

Данные оракулы собирают информацию из онлайн-источников (например, сайтов компаний/новостей и др.)

2. Оракулы с использованием оборудования.

Данные оракулы собирают информацию из офлайн-источников из физического мира (например сенсоров).

II. По направлению информации:

1. Внутринаправленные (Inbound) оракулы.

Данные оракулы интегрируют информацию из внешних источников в РР.

2. Внешненаправленные (Outbound) оракулы.

Данные оракулы позволяют умным контрактам отправлять информацию в источники вне РР (например разблокировать замок на хранилище при получении платежа).

III. По количеству источников информации:

1. Оракулы, основанные на одном источнике информации.

Данные оракулы интегрируют информацию только из одного источника. Подходят для рынков, где есть единственно верный источник информации.

2. Консенсусные оракулы.

Данные оракулы интегрируют информацию более чем из одного источника. Чаще всего при этом оракулам присваивается рейтинг, позволяющий оценить достоверность и ценность представленной информации. Особенно актуальными данные оракулы стали при развитии рынков предсказаний (например Augur) в силу работы с будущими периодами и большой степенью неопределенности.

Счета и идентификаторы пользователей

Отдельным элементом данных, хранящихся в РР, можно выделить идентификаторы и счета пользователей. Важно отметить, что РР не хранит счета пользователей, РР хранит записи информации, которые могут быть присвоены какому-то идентификатору. Ряд РР делает записи полуанонимными (например используя публичный ключ участника в качестве идентификатора). Отдельный сегмент РР посвящен анонимизации транзакций и информации. Один из наиболее популярных способов анонимизации транзакций — использование не одного, а нескольких случайно сгенерированных публичных ключей, которые выбираются случайным образом для

транзакций и заменяются с течением времени. Информация о частных ключах и зачастую персональная информация о владельцах ключей нередко хранится в кошельках и на криптобиржах, но не на PP.

Другие элементы внутреннего круга

К другим элементам внутреннего круга можно отнести, например, криптографию и шифрование. Подробная информация про подходы к хешированию доступна в исследовании Satis Group "Cryptoasset Market Coverage Initiation: Technical Underpinnings"[19]. Несмотря на то, что они не являются самостоятельными элементами, без данных функций не обходится практически ни один PP.

Внешний круг — технологическая экосистема PP

Инстанции

Простыми словами, инстанции — это использование кода оригинального PP для создания нового продукта. Новым продуктом может быть модифицированный PP или какой-либо продукт на основе PP, в том числе блокчейн как услуга (BaaS), который в данной экосистеме выделен отдельно в силу растущей популярности данной инстанции. Анализ инстанций от текущих наиболее популярных PP представлен в разделе 3. Стоит отметить, что в случае неконтролируемых PP, так как изменения в коде происходят с помощью форков, возможен раскол PP на два реестра, что тоже приведет к созданию инстанции, как было отмечено ранее. Различные инстанции PP обычно являются более совместимыми, чем реестры с различными происхождениями.

Совместимость и интеграция PP

Одной из наиболее актуальных проблем на текущий момент является проблема интеграции и совместимости различных PP, особенно имеющих разные первоисточники. Наиболее заметные проекты и разработки, связанные с решением данной проблемы, включают в себя системы для интеграции сайдчейнов, а также адаптеры для записи данных с одних PP на другие.

Так как Ethereum является одним из наиболее активных проектов с одной из наиболее развитых экосистем девелоперов и инстанций, одни из первых предложений по решению данных проблем были представлены для данного PP. Так, к примеру, Plasma, которая планируется к запуску в 2020 году, предлагает способ интеграции различных сайдчейнов и основного PP Ethereum. Помимо возможности интеграции сайдчейнов воедино, данное решение также может позволить разгрузить основную сеть и ускорить проведение транзакций[20]. Существует также ряд стартапов, которые предлагают схожие решения и интегрируют различные PP в один, однако большинство из них нацелены на PP, написанные на одном или нескольких похожих языках программирования.

Альтернативный блок решений проблем совместимости — это адаптеры PP. Адаптеры позволяют перевести записи и транзакции с одного PP на другой, тем самым обеспечив возможность перевода информации. Данное решение подробно описано, к примеру, в PP ArcBlock. Однако в целом стоит отметить, что, несмотря на появляющиеся решения относительно совместимости и ряд предложений как от стартапов, так и от разработчиков уже относительно развитых PP, проблемы совместимости все еще остаются актуальными для криптоиндустрии.

[19] Доступно онлайн: https://research.bloomberg.com/pub/res/d2246jsnqusjYSeacPbQc2IjVIw.
[20] Подробнее о Plasma: http://plasma.io.

Автоматизация и ее применение

Как было отмечено ранее, умные контракты — основной источник автоматизации на РР. Несмотря на то, что сама технология РР, а тем более умные контракты на ней, появилась сравнительно недавно, ряд простых умных контрактов уже нашли практические применения, поэтому криптоиндустрия начала задумываться о более сложных конструкциях, состоящих из более чем одного участника или более чем одного умного контракта. PwC структурировал данные попытки и положил на ось, отображающую сложность приложений автоматизации.

РИСУНОК 3. СХЕМА ПРИМЕНИМОСТИ УМНЫХ КОНТРАКТОВ ОТ САМОГО ПРОСТОГО ДО САМОГО СЛОЖНОГО

Источник: адаптировано из статьи Алана Моррисона (2016)[21]

В целом, текущие усилия в рамках автоматизации выходят за пределы исключительно умных контрактов и начинают расширяться вплоть до децентрализованной автономной экономики (ДАЭ). Сюда же включается тенденция стартапов, связанных с криптоиндустрией, предлагать децентрализованные версии существующих приложений и предложений. Однако здесь стоит отметить неудачный опыт создания децентрализованных автономных организаций и проблемы с управлением на неконтролируемых РР, что приводит к замедлению развития подобных инициатив[22]. При этом, благодаря тому что большая часть умных контрактов пишется для открытых РР, экосистема криптоиндустрии сложилась таким образом, что умные контракты появляются в открытом доступе, что стимулирует инновации в данной области. Часть частных и консорциумных РР также выбрали стратегию использования открытых разработок в области умных контрактов и создали агрегаторы наработок, а также платформу запросов для разработчиков, на которой любой участник может написать/выбрать, какие умные контракты ему нужны. Подобные инициативы также появляются не только со стороны РР, но и независимо, как отдельные компании/организации.

Блокчейн как услуга (BaaS)

Блокчейн как услуга — это предложение от облачных и инфраструктурных провайдеров, которое позволяет строить, хранить (host) и использовать приложения для РР, созданные клиентом, а

[21] Доступно по ссылке: https://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digital-business/.
[22] Подробнее о текущих проблемах, связанных с автоматизацией и развитием РР в целом, написано в разделе 6.

также умные контракты и другие элементы РР в их инфраструктуре[23]. Подобные решения особенно популярны среди бизнес-применений РР, так как зачастую BaaS-предложения предоставляются крупными технологическими компаниями, работающими в B2B-сегменте по принципу Software as a Service (SaaS), например, AWS, Microsoft Azure, IBM и другими, а также нишевыми стартапами. Данное предложение включает в себя сложную настройку и создание узлов, необходимых для работы с РР. С точки зрения развития экосистемы данные приложения выделяются отдельно, так как все инфраструктурные и технологические разработки, а также связанные с ними настройка и поддержка, передаются провайдеру услуг, в то время как клиент получает возможность внедрить РР в свой привычный бизнес. Большинство бизнес-применений РР сегодня работает по принципу BaaS[24].

Криптокошельки и другие пользовательские интерфейсы

Криптокошельки выполняют функцию платежного интерфейса для участников РР. На данный момент криптокошельки являются наиболее популярным и, по сути, единственным работающим интерфейсом взаимодействия участников с РР. Как было отмечено в первой части серии отчетов, посвященной криптоиндустрии, кошельки совместно с криптобиржами начинают внедрять процедуры KYC и системы соответствия правилам/законам о CFT и AML. Помимо этого, в ряде государств необходимо получение лицензии как для операторов криптокошельков, так и для операторов криптобирж.

Подробное описание и анализ криптокошельков в контексте более широкого рынка цифровых кошельков представлены в исследовании Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО «Классификация цифровых кошельков»[25]. На основе проведенного анализа существующих кошельков можно выделить горячие (всегда подключенные к интернету) и холодные (работающие офлайн) кошельки, мультивалютные и одновалютные кошельки, кошельки, поддерживающие один ключ или несколько, а также по интерфейсу: онлайн-, мобильные и десктопные кошельки.

Криптобиржи

Криптобиржи выполняют функцию обмена разных токенов, в том числе с разных реестров. По этой причине криптобиржи можно считать еще одним инструментом обеспечения совместимости и интеграции РР с точки зрения использования различных токенов. В целом можно выделить две основные группы бирж: централизованные и децентрализованные. Централизованные биржи отличаются высокой скоростью и низкой стоимостью процессинга транзакций и поддержкой обмена на фиатные валюты, а также токены с разных РР. Децентрализованные биржи реже позволяют обменивать разные токены (только те, что размещены в рамках одного РР), медленнее и дороже обрабатывают транзакции, но при этом отдают право ведения счета клиенту, хранят данные о владении токенах только на РР, что может быть более безопасным с точки зрения взломов, и более дешевы в создании.

Централизованные криптобиржи подключаются к различным РР и позволяют совершать транзакции с помощью токенов, размещенных на разных РР. Помимо этого, так же как и криптокошельки, криптобиржи являются местом хранения информации о клиенте, а также соединения информации с РР и из реального мира. Также биржи являются источником информации о курсе обмена токенов, что может быть важно для оракулов. Как и в случае

[23] Введение в рынок BaaS и анализ тенденций провайдеров данных услуг представлен в работе Синга и Майкелса (2017). Доступна онлайн: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091223.
[24] Обзор бизнес-применений и тенденций разных РР представлен в разделе 3.
[25] Более подробная информация о цифровых кошельках и исследование доступны онлайн: https://finance.skolkovo.ru/ru/sfice/research-reports/1836-2018-11-29/.

криптокошельков, криптобиржи начинают внедрять процедуры KYC и системы соответствия правилам/законам о CFT и AML. Помимо этого, в ряде государств необходимо получение лицензии для криптобирж — это требование появилось вследствие серии взломов ряда централизованных бирж (например Mt. Gox).

В серии исследований Satis Group "Crypto asset market coverage initiation" есть несколько отчетов, включающих информацию о криптобиржах[26]. Согласно исследованиям, 99,8% объема торгов происходит через централизованные биржи. Среди децентрализованных бирж ярче всего выделяются iDex, ForkDelta и Waves DEX, однако по объему торгов ни одна из них не генерирует даже 0,1% транзакций в силу того, что ни одна децентрализованная биржа не поддерживает фиатные валюты. Тем не менее внедрение стейблкоинов сделало децентрализованные биржи более популярными. Среди централизованных бирж лидерами являются Bitmex, Binance, OKEx, Huobi, Bitfinex, Bithumb и HitBTC. Топ-20 бирж генерируют более 75% всего объема криптотранзакций. Обмен биткоина — на первом месте, на втором — стейблкоин USDT, а на третьем — Ethereum. При этом обмен на доллары США составляет почти 50% всего объема обмена биткоинов, а на японскую йену — около трети, несмотря на специфику крипторегулирования в США и Я понии. В 2019 году прогнозируется рост объема торгов более чем на 50%. При этом, помимо традиционных бирж, на рынке также появились институциональные провайдеры услуг по торговле.

ICO, STO и др. методы предложения токенов

Один из наиболее популярных рынков, связанных с криптоиндустрией[27], — рынок размещения токенов (ICO и появляющееся направление STO). Аналитика по данному рынку представлена в первой части серии отчетов, посвященных криптоиндустрии. Помимо этого, существует ряд отдельных направлений аналитики, посвященных исключительно ICO и предложению токенов. К примеру, ресурсы ICO rating, ICO Bench и другие сайты-агрегаторы ICO выпускают периодические исследования рынка. Ключевыми тенденциями здесь можно отметить выбор платформы: несмотря на доминирующую позицию Ethereum, альтернативные площадки также начинают набирать обороты. Помимо этого, как было отмечено в первом отчете, большинство проектов являются обманными или провальными, однако на рынке существует тенденция к выравниванию количества проектов в силу повышения грамотности инвесторов и появления регулирования.

С технологической точки зрения размещение ненативных токенов — одна из наиболее стандартизированных областей криптоиндустрии. Начиная с Ethereum сложился индустриальный стандарт размещения ненативных токенов (сначала ERC 20, затем он дополнился, к примеру, ERC 223, ERC 721 и ERC 777). Однако данный стандарт лишь предлагает несколько строчек кода, которые используются для программирования параметров токенов таким образом, чтобы они подходили PP Ethereum. Подобной стандартизацией занялись и другие PP. Различие между ICO и STO носит не технологический, а скорее регуляторный или маркетинговый характер. ICO изначально задумывалось как инструмент размещения токенов услуг, в то время как STO задумывается как инструмент краудфандинга и, возможно, обеспечения долевого участия в проектах. С технологической точки зрения второе, возможно, будет вовлекать больше умных контрактов, однако в остальном данные методы предложения токенов схожи.

[26] См., например: https://research.bloomberg.com/pub/res/d2gg3p_HTg39HRCuzQjIyy8NVZQ и https://research.bloomberg.com/pub/res/d3h2iTlKWIa4FTLKGJsUn3mis5g.

[27] Стоит отметить, что на момент написания отчета (декабрь 2018 года) объем привлеченных средств на ICO и количество проектов снижаются. Так, по статистике на ноябрь 2018 года, рынок ICO достиг годового минимума в $65 млн, что почти в 4 раза меньше февральского значения.

Токенизация

Токенизация является близким к ICO применением PP, однако вместо размещения токена услуги, как в случае ICO, она подразумевает создание токена, подвязанного к какой-либо ценности, т.е. чаще токена активов или гибридного токена. Существует ряд платформ токенизации, которые предоставляют возможность размещения ненативных токенов на разных блокчейнах и предлагают услуги по программированию характеристик токенов исходя из желаний и указанной клиентом специфики. Токенизация может предоставить основу для формирования нового метода обмена и учета ценности с точки зрения экономики, однако с технической точки зрения токенизация — это запись информации о какой-либо ценности на PP. При этом выбор PP, на который возможна запись, ограничивается лишь желанием и целями токенизатора, а также возможностью размещения ненативных токенов. Так, к примеру, блокчейн биткоина не поддерживает размещение подобных токенов в силу соединения слоя приложений и реестра, однако несколько проектов, включая закрывшийся CoinPrism, работают над рядом решений, к примеру, colored coins или сайдчейн Roostock, которые позволяют использовать умные контракты для размещения ненативных токенов на PP биткоина. Как было отмечено ранее, именно характеристики PP (неизменность, транспарентность, автономность, верифицируемость и т.д.) сделали токенизацию более привлекательной для участников экономики по сравнению с токенизацией с помощью других технологий хранения данных.

Шардинг и управление хранением данных

Одно из технологических решений, позволяющих обеспечить достаточный объем памяти для PP, — это шардинг. Простыми словами, шардинг — это горизонтальное разделение записей в базе данных на несколько и последующее хранение различных частей данной базы на разных серверах/дисках. В контексте PP это означает, что часть узлов будет иметь один блок информации, в то время как другая часть — другой. Шардинг не может быть использован в ряде протоколов консенсуса (например PoW), а также может вызвать проблемы с точки зрения исполнения умных контрактов и связанных с ними решений, однако в целом на данном этапе шардинг рассматривается в качестве одного из возможных решений для обеспечения масштабируемости и повышения скорости проведения транзакций на PP. Тем не менее существуют и группы критиков, предлагающие альтернативные масштабированию решения. Подробнее о тенденциях PP сказано в разделе 3.

РАЗДЕЛ 3. ТЕКУЩЕЕ ТЕХНОЛОГИЧЕСКОЕ СОСТОЯНИЕ КРИПТОИНДУСТРИИ

21 основной РР

В данной секции представлен анализ 21 основного уникального РР, существующего сегодня в криптоиндустрии. Подробный анализ каждого из данных РР, включая стратегический анализ профиля РР, представлен в приложении 2.

Общие тенденции развития РР

Большая часть распределенных реестров (14 из 21, или 66,67%) являются публичными, неконтролируемыми, универсальными и подрывными (21-й тип[28], 15-й из 21 представленного). Blockchain DB поддерживает существующую IT-инфраструктуру, и только Hydrachain, который по факту является дополнением к сети Ethereum, Openchain, который предлагал симбиоз с существующими публичными РР и больше не оперирует в силу банкротства/закрытия компании CoinPrism, занимавшейся разработкой системы, и Chain, предлагающий настройку РР под нужды клиента, являются частными РР. Еще три — консорциумные варианты РР, нацеленные так или иначе на модернизацию существующих IT-инфраструктур в корпорациях.

Публичные РР 21-го типа можно считать универсальной инфраструктурой, которая управляется автоматически с помощью набора кодов и децентрализованных приложений. Этот вариант РР наиболее похож на интернет, который не имеет кнопки отключения и может быть адаптирован практически под любые нужды. Вследствие наличия подобной амбициозной цели программисты уделяют наибольшее внимание именно этому типу РР. Особенный всплеск активности наблюдается в конце 2017–2018 годов. При этом стратегия вывода новых РР отличается и может быть атакующей, когда разработчики предлагают альтернативу существующим РР, или независимой, когда создатели РР пытаются завоевать еще не вовлеченную в криптоиндустрию аудиторию.

Существующие консорциумные РР в большинстве своем создаются крупными ассоциациями (например R3 CEV) или компаниями, представляющими технологическую архитектуру (например, Linux, IBM). При этом РР воспринимаются этими организациями как очередной этап модернизации существующих процессов, а не как прорывная платформа для предложения абсолютно новых продуктов и услуг. Как следствие, консорциумные РР, создаваемые самими же компаниями-потребителями или компаниями, чьи прибыли зависят от взносов клиентов, выглядят как излишне безопасная система, не позволяющая создать прорывные решения.

В последний год (с конца 2017 года), в связи с развитием ICO и предложений по альтернативным криптовалютам, появилось большое количество новых распределенных реестров. В целом, выделяют три поколения реестров. Первое поколение (к нему относят блокчейн биткоина) — это реестры, позволившие обменивать нативные токены (то есть использовать криптовалюты). Ко второму поколению реестров относят реестры, которые позволили прописывать умные контракты или иным образом автоматизировать процессы и размещать ненативные токены. Начало РР

[28] Типология РР доступна в разделе 4.

второго поколения относят к появлению Ethereum. Третье поколение PP призвано устранить проблемы масштабируемости, управления, энергозатратности, совместимости, приватности и устойчивости реестров и нативных для реестров токенов. Формализованных критериев, должны ли реестры решать все из вышеперечисленных проблем или лишь часть их, не существует.

Активный рост количества PP приходится именно на реестры **третьего поколения**. 10 проектов из 21 (47,62%) — это PP третьего поколения, а еще девять — второго поколения. Всего два проекта — это PP первого поколения. Вызван данный рост в первую очередь тем, что изменения в существующие реестры требуют жесткого форка, который, в свою очередь, может спровоцировать раскол системы. Чем больше изменений предлагает форк, тем больше вероятность появления группы несогласных с ними участников, которые вызовут раскол системы. Раскол системы приведет к потери вычислительных мощностей и дроблению экосистемы проекта, поэтому разработчики и участники пытаются его избежать. Как следствие, группы разработчиков, несогласные с направлением развития существующих PP, начали инициировать PP третьего поколения как попытку предложить альтернативу существующим реестрам вместо использования форков, однако подобное развитие PP может быть неустойчивым, так как требует перехода участников с одной системы на другую. Предлагаемые изменения при этом, как видно из новейших PP, представленных в конце таблицы, большинство которых еще находится в стадии разработки, скорее инкрементальны, нежели фундаментальны. Во многом, помимо прочего, это происходит благодаря отсутствию исследования рынка (большинство проектов не имеют признаков глубокого анализа конкурентов и текущего состояния криптоиндустрии в своих документах (например white paper), блогах, высказываниях в открытых источниках или на сайтах, а те проекты, которые имеют хотя бы некоторые признаки аналитики существующих решений, в большинстве своем ограничиваются сравнением с несколькими крупнейшими проектами и в большей части не столь актуальными проблемами существующих PP).

Что касается инстанций PP, то большая часть PP, упоминания о которых встречаются в открытых источниках, — это модификация публичных PP. Ряд наиболее популярных PP, лежащих в основе токенов и криптовалют, являются форками (результатами сплита) какого-либо PP: например, из 10 наиболее популярных криптовалют по состоянию на 2018 год[29], помимо пяти уникальных PP, которые уже были упомянуты (Ethereum, биткоин, Ripple, NEO и Cardano), три проекта — результаты форков биткоина, а еще два — проект на Ethereum и инстанция Ripple. Из топ-100 криптовалют по рыночной капитализации, по данным Coinmarketcap по состоянию на начало декабря 2018 года, помимо 14 нативных токенов уже упомянутых оригинальных PP, 19 работают на инстанциях биткоина (большинство — результаты форков, а часть — форков более чем первой степени (созданных от криптовалют, которые являются результатом форка или инстанцией блокчейна биткоина)), 44 работают на PP, который образовался как какая-либо инстанция Ethereum, или непосредственно на Ethereum, а еще восемь, хоть и утверждают, что создали собственные PP, на самом деле также связаны или схожи с PP Ethereum. Оставшиеся PP являются инстанциями или связаны с другими платформами.

В целом, что касается инстанций, существует отдельная активность в криптоиндустрии, посвященная отслеживанию форков и — реже — инстанций различных PP. Так, например, к данному моменту существует 101 проект в результате форков биткоина, 72 из которых активны, а 21 считаются историческими и нерелевантными[30]. 43 проекта уже имеют систему, позволяющую совершать транзакции, а еще 29 — в процессе ее разработки. При этом семь форков Litecoin, а также форки Dogecoin и Dash можно также отнести к форкам биткоина, так как данные проекты

[29] См., к примеру: https://www.telegraph.co.uk/technology/digital-money/top-10-popular-cryptocurrencies-2018/.
[30] Более подробная информация об анализе форков биткоина и других популярных PP доступна онлайн: https://forkdrop.io/how-many-bitcoin-forks-are-there или https://list.wiki/Ethereum_Forks.

сами являются инстанциями блокчейна биткоина. Количество форков у альткоинов значительно меньше — из-за разницы, во-первых, возраста проектов, а во-вторых, размера сети. При прочих равных, чем больше участников в РР, тем более вероятен раскол системы в результате форка в силу появления несогласных групп участников РР.

Существуют также попытки отразить всю историю появления различных криптовалют и токенов. Так, по статистике проекта Map of Coins[31], на основе инстанций РР биткоина действуют 436 токенов (около 20,83% всех криптовалют согласно статистике Coinmarketcap), в то время как у других проанализированных альткоинов — от 5 до 16 валют. Проект не включает попытку отразить токены и коины на основе платформы Ethereum, однако список ERC20- и ERC223-токенов, автоматически собранный с Coinmarketcap компанией Eidoo[32], насчитывает 1039 токенов (49,64%). Основываясь на данной статистике, можно отметить четкое доминирование инстанций блокчейна биткоина и Ethereum над другими проектами. Среди подобных проектов можно также отметить намеренные инстанции публичных РР — к примеру, Stellar, созданный на основе Ripple одним из бывших создателей Ripple и направленный на изменение как технологических (например подход к консенсусу), так и идейных (например, целевая аудитория и направленность РР) составляющих.

Что касается размера систем, блокчейн биткоина занимает лидирующие позиции с точки зрения сетей, нацеленных на предоставление валют. Согласно исследованию Satis group[33], биткоин составляет 76% рынка сетей РР, направленных на предоставление валют. С точки зрения сетей, предоставляющих платформенные решения, однако, Ethereum лидирует с 86,5% рынка, хотя альтернативные системы начинают появляться и составлять ему конкуренцию. Исследование Satis Group также выделяет другие сети, предоставляющие токены услуг, а также токены для приватности, криптобиржи и стейблкоины. Однако с технологической точки зрения их структура схожа с РР или лежит вне фокуса данного исследования. Тем не менее появляется тенденция создания собственных РР либо с нуля (даже если подобный РР похож на один из существующих РР), либо после использования одной из существующих платформ для размещения собственных токенов. Так, Tron изначально использовал Ethereum, а затем перевел токены и связанные операции на собственный РР, а Binance coin, размещенный сейчас на платформе Ethereum, планирует создание собственного РР, в том числе нацеленного на распределенные приложения (dApps).

Что касается предложений BaaS, то, как отмечалось ранее, практически все крупнейшие технологические компании предлагают подобные решения — к примеру, Microsoft, SAP, AWS. Среди данных компаний также есть консультанты, к примеру, Deloitte, и ряд стартапов в данной области — например, Peer Ledger, PayStand, Blockstream, Blocko, BitSE. Все их предложения довольно схожи. Среди применений и интеграции различных технологий РР набирают популярность фасилитаторы интеграции РР, особенно в области соответствия требованиям регулирования и стандартам. Так, можно выделить ряд платформ токенизации, где размещение токенов сопровождается автоматическим соответствием регулированию, — к примеру, Harbor, Securitize, Securrency и др.

Среди инстанций отдельно можно выделить Quorum, который является частотным РР от J.P. Morgan, разработанным специально для финансового сектора на основе инстанции Ethereum. Система использует умные контракты и систему транзакций для автоматизации бизнес-логики в рамках финансового сектора и по факту является конкурентом для Chain. Консенсус в данной системе достигается посредством голосования на QuorumChain, что позволяет достичь большей

[31] https://mapofcoins.com.
[32] https://eidoo.io/erc20-tokens-list/.
[33] Исследование “Crypto asset market coverage initiation: market composition” доступно онлайн: https://research.bloomberg.com/pub/res/d2gg3p_HTg39HRCuzQjIyy8NVZQ.

скорости транзакций.

Тенденции публичных РР

На текущем этапе развития РР существует двойственная проблема открытых РР. С одной стороны, открытые РР, появившиеся некоторое время назад (2016 год и ранее), уже успели набрать критическую массу пользователей (например, Ripple, Blockchain, Ethereum). С другой — данные РР часто критикуют за их **проблемы с масштабируемостью, энергоэффективностью, совместимостью, приватностью и системой управления**, которые не могут быть решены форками из-за высокой вероятности раскола разрозненной базы пользователей. Новые РР, однако, еще не представили решений, которые бы были приоритетны с точки зрения пользователей: в большинстве РР третьего поколения отсутствуют основные сети и рабочие версии системы, а в некоторых — даже описание критических элементов системы, несмотря на то, что по плану-графику проекта срок уже истек.

Большая часть уникальных публичных РР использует PoS или какую-либо его вариацию (DPoS, Provably securic PoS). Тем не менее, в силу бурного роста количества инстанций (и публичных, и частных) блокчейнов биткоина и Ethereum, PoW чаще ассоциируется с криптоиндустрией и встречается в транзакциях на РР. Несколько проектов существенно выделяются: Tangle от IOTA, использующий DAG, Ripple, Solana (Proof of History), — однако в полной мере данные подходы к консенсусу до сих пор не изучены, поэтому вызывают резонанс в криптоиндустрии.
Довольно большая доля проектов предлагает шардинг как решение для масштабируемости, однако эффективность шардинга и вероятность потери части данных при разделении цепи также не изучены до конца.

Большая часть публичных РР поддерживает умные контракты. Те РР, которые не поддерживают умные контракты в своей базовой версии, имеют расширения или инстанции, позволяющие прописать умные контракты в системе. Существует тенденция к упрощению процесса создания умных контрактов и поддержки различных языков для их программирования. Тенденция к упрощению работы с РР есть и в других областях: кошельках, запуске узлов, установке программ для верификации и процессинга транзакций, поиска блоков (block explorer) и др.

Часть предложений не предлагают полное инфраструктурное решение, а пытаются вписаться в архитектуру существующих проектов. Отдельно стоит выделить BigChainDB, который предлагает распределенную базу данных, встраиваемую в любую технологическую архитектуру, а также Hydrachain, который является расширением для Ethereum, позволяющим создавать частные инстанции данного РР.

В отличие от консорциумных РР, нишевые РР, нацеленные на одну или несколько областей или индустрий, отсутствуют. Даже Tangle, позиционирующийся как РР для интернета вещей, имеет преломления во всех областях и может считаться универсальным. Разделение на ттри поколения РР наиболее заметно именно в публичных РР. В целом публичные РР пытаются предложить в первую очередь именно инфраструктурные решения, поэтому их часто сравнивают с интернетом

или операционными сетями и пророчат лидерство одного или нескольких предложений (тем не менее относительно токенов тенденция такова, что многие эксперты говорят о сосуществовании большого количества токенов и, возможно, криптовалют[34]).

Всплеск количества уникальных публичных PP приходится на 2017–2018 годы, когда разработчики стали массово выводить на ICO не проекты и децентрализованные приложения, а протоколы PP, размещая собственные токены на других PP (например Ethereum), обещая затем перевести их на токены внутри разработанного PP по курсу 1:1. Большая часть предлагаемых PP, однако, повторяют историю проектов/компаний, выходящих на ICO, и являются неудачами или обманом. Есть несколько объяснений подобному тренду, например:

- **слабое исследование существующих реестров и рынка в целом**. В открытых источниках до сих пор нет полноценного анализа существующих PP и их технических составляющих. Большая часть описанных проблем PP — результат анализа лишь наиболее популярных PP (Blockchain, Ethereum, Ripple и производных) или гипотез авторов без какой-либо аналитики. В большинстве описаний проектов (white papers и сайты) не представлено сравнений с существующими PP, а решаемые проблемы и уникальность описаны абстрактно;
- **провалы большинства проектов и неудачные эксперименты с существующими PP**. 81% существующих ICO-проектов признаны мошенническими, а еще 15,3% — провальными, исчезающими или умершими, как было отмечено в первом отчете. Среди предложенных проектов на существующих PP есть громкие провалы, например, неудачные попытки создать децентрализованные компании (например, см. кейс 3. The DAO) или проблемы с управлением в рамках PP (например вероятность голосования за неэффективные и деструктивные решения участниками PP и держателями токенов (см. случай заморозки 27 транзакций в сети EOS));
- **готовность людей рисковать и инвестировать в высокорисковые проекты**. Благодаря этому собрать инвестиции стало возможным даже под описание проекта без наличия реальных разработок;
- **отсутствие высококвалифицированных специалистов в области PP.** Большинство блокчейн-специалистов — это специалисты общих компьютерных наук или экономики, но специалистов в PP до сих пор не существует в необходимых масштабах. Большая часть наиболее популярных PP создана узким кругом людей, часто переходящих из проекта в проект.

В приложении 1 не представлены некоторые PP без значительных отличительных особенностей, такие как Tron или Qtum, даже несмотря на то, что они привлекли достаточно большое внимание со стороны криптосообщества. Это сделано по причине того, что их технические характеристики близки к уже описанным в таблице PP. Помимо этого, существует PP Multiversum, который утверждает о создании PP четвертого поколения, однако детального конкретного описания технологической составляющей не предоставляет. Основным тезисом отличия его от PP третьего поколения является поддержка многомерной структуры данных, однако некоторые PP третьего поколения (например Cardano) также могут поддерживать данные такого вида. Также пути решения обозначенных проблем не были протестированы на практике. Сайт проекта не обновлялся со второго квартала 2018 года, а основная сеть пока что отсутствует. По данным причинам описание проекта не включено в таблицу из приложения 1. В общей сложности, большая часть уникальных и видоизмененных PP попадают в категорию публичных, но не могут предложить критических и фундаментальных изменений.

[34] https://steemit.com/steemit/@etcmike/multiple-crypto-currencies-can-coexist-just-like-multiple-national-currencies-coexist-today https://venturebeat.com/2017/09/20/how-many-cryptocurrencies-does-the-world-need/.

Тенденции консорциумных РР

Среди консорциумных РР, наоборот, чаще встречаются нишевые, а не универсальные. В целом, консорциумных РР намного меньше; среди наиболее популярных — всего три проекта: Corda, Hyperledger и Symbiont. Corda и Hyperledger созданы крупными компаниями (R3 CEV и Linux Foundation). Corda и Symbiont разработаны в основном для применений в индустрии финансовых услуг. Все консорциумные РР поддерживают умные контракты.

Консорциумные РР в первую очередь создаются для автоматизации бизнес-логики между различными компаниями. В них не существует проблем публичных РР, так как консенсус определяется правилами валидации, которые разработаны участниками или дизайнерами системы. **Ни один из публичных РР, как и частных, не является подрывным или неконтролируемым**. Потенциал прорывного развития финансовых или других продуктов под сомнением благодаря поддержке текущих бизнес-моделей архитектурой консорциумных РР.

Все три представленные консорциумные РР требуют вовлеченности в разработку узла и активного технического участия от клиентов, что в контексте небольшого количества специалистов в области РР вызывает замедление распространения успешных и новаторских решений, основанных на подобных РР. В связи с этим появляется ряд посредников, например Digital Asset Holdings, которые предлагают настройку РР и разработку приложений, необходимых клиентам.

РР от Digital Asset Holdings не включен в таблицу, так как описания в открытых источниках недостаточно для полноценного понимания технологической составляющей и вывода о том, что РР вообще был запущен. Помимо этого, Digital Asset Holdings купила Hyperledger в 2015 году, что может означать, что используемый РР — это Hyperledger. Основная инновация РР от Digital Asset Holdings — это разделение частного, где происходят транзакции, и публичного РР, куда записываются шифрованные записи, наподобие системы Openchain, о которой будет сказано далее.

В связи с тем, что данные РР запущены и контролируются компаниями, возникают вопросы касательно прав администратора данных РР, возможности просмотра и степени влияния на информацию, занесенную в РР. По этой причине, а также по причине использования прописанных правил валидации вместо BFT-подходов к консенсусу консорциумные РР в криптоиндустрии зачастую критикуют.

Тенденции частных РР

Большая часть инстанций РР являются изначально частными, поэтому точное их количество обозначить невозможно. Однако существует три уникальных частных РР, упоминаемых в публичных источниках. Ключевая ценность частных РР до сих пор не определена и чаще всего сводится к возможности создания узлов для просмотра/аудита транзакций. Тем не менее представленные РР имеют четкое позиционирование и преимущества. Критика частных РР чаще всего сводится к тому, что базы данных являются более эффективным инструментом, однако в силу изменяемости записей в базах данных внешний аудит может не принести достоверного результата или быть сложнее.

Как и в консорциумных РР, в частных РР чаще консенсус определяется дизайнером или участниками системы, однако в РР, основанных на Hydrachain, консенсус в базовой версии определяется по принципам сети Ethereum. Openchain и Hydrachain являются универсальными РР, в то время как Chain в первую очередь нацелен на индустрию финансовых услуг.

Openchain не функционирует с середины 2018 года в силу закрытия компании CoinPrism, управлявшей проектом. Chain предлагает широкую бизнес-линейку решений, которая включает консалтинг и разработку РР под определенные нужды клиентов. Непонятны права Chain и CoinPrism в своих системах: частные данные клиентов могут быть доступны провайдерам РР. В целом, архитектура частных РР наиболее разрознена/наименее стандартизована: у Chain каждая инстанция создается под нужды клиента, у Openchain происходит запись о совокупности транзакций на публичный РР, а Hydrachain оставляет часть архитектурных решений на выбор создателя инстанции.

Текущие применения РР

На настоящий момент насчитывается около 50 уникальных областей применения РР. Статья Зиле и Страздины (2018) классифицировала данные применения в четыре категории: управление данными, верификация данных, финансовые применения и другие. При этом в ряде областей насчитывается более одного, а иногда и более пяти конкретных применений[35]. Несмотря на то, что в упомянутой работе не хватает ряда примеров, не попадающих ни в одну из категорий (например токенизации), данная классификация позволяет сделать выводы о том, что применение РР в разных областях становится более распространенным с каждым годом. Вероятно, что при добавлении новых и менее популярных идей и проектов список применений РР может составить более 100 проектов.

Помимо данной классификации, существует ряд других инициатив, посвященных поиску и агрегации проектов, связанных с использованием РР. Особенно часто в данном контексте появляются применения в искусстве и других отраслях, связанных с креативными профессиями, здравоохранении и цепочках поставок в силу высокой асимметрии информации и высоких потенциальных выгод создания единого РР, содержащего информацию об участниках индустрии[36].

Исследование McKinsey “Blockchain beyond the hype: What is the strategic business value” предлагает анализ потенциальных применений РР в различных индустриях, а также их доступности исходя из текущего состояния отраслей и технологии и потенциального влияния. Согласно данному исследованию, наибольший эффект РР имеют в публичном секторе, индустрии технологий, медиа и телекоммуникаций и в финансовых услугах. При этом авторы исследования выделяют шесть основных категорий потенциальных применений РР: статичная запись, идентичность/личность, умные контракты, динамическая запись данных, платежная инфраструктура и другие.

[35] Конкретный список применений РР и различных проектов указан в таблице 1 в работе Зиле и Страздины (2018). Доступно онлайн: https://content.sciendo.com/view/journals/acss/23/1/article-p12.xml.

[36] Полезными в данном контексте могут быть, к примеру, следующие источники информации, предлагающие агрегацию проектов, связанных с РР: https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99, https://www.coindesk.com/information/applications-use-cases-blockchains, https://www.ibm.com/blockchain/use-cases/, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value, https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b, https://www.cbinsights.com/research/industries-disrupted-blockchain/.

Крупные корпорации также ищут применения РР в различных ситуациях. На данный момент насчитывается больше 55 корпоративных проектов, связанных с РР[37]. При этом, помимо компаний из индустрии финансовых услуг, которые начали экспериментировать с технологией РР еще 4–5 лет назад, в последние годы все чаще встречаются проекты в компаниях вне финансового сектора. Подобные проекты чаще всего направлены на автоматизацию бизнес-логики между различными участниками для устранения асимметрии информации или гармонизации отношений. Также существует тенденция к открытию своих РР — так, проект Tracr по отслеживанию бриллиантов, инициированный компанией DeBeers, стал индустриальным и теперь вовлекает различные компании из отраслей, связанных с добычей, обработкой и реализацией бриллиантов.

КЕЙС 1. De Beers

В 2016–2017 году компания De Beers, занимающаяся добычей, продажей и производством бриллиантов, которая была практически монополистом в добыче бриллиантов до XXI века, предложила использовать технологию РР в контексте цепочки поставок для отслеживания контрафактных бриллиантов. Вплоть до 2018 года компания занималась экспериментами с РР и была одной из первых, предложивших нефинансовое применение технологии. В начале 2018 года компания De Beers заявила о запуске системы Tracr, построенной на основе Ethereum, совместно с пятью другими лидирующими производителями бриллиантов: Diacore, Diarough, KGK Group, Rosy Blue NV и Venus Jewel. Несмотря на то, что в первоначальных заявлениях рассматривался вариант частного РР, компания в итоге перешла к идее консорциумного РР для поиска синергии и укрепления собственного конкурентного преимущества в индустрии как на локальных, так и на глобальном рынке. В мае 2018 года компания впервые отследила поставку 100 высокоценных бриллиантов от добычи до ритейла. Tracr присваивает каждому бриллианту идентификационный номер и делает записи о его характеристиках (например, карате, чистоте и цвете). Затем с помощью этого в РР отслеживается каждое действие, предпринятое с бриллиантом на каждом из этапов цепочки поставок.

В целом, на основании анализа применений, с точки зрения стратегии использования РР, можно выделить три основных типа идей, лежащих в основе применения РР.

1) Устранение доверия и массовая альтернатива.

Суть: создание альтернативной инфраструктуры и, в частности, системы «без необходимости доверия» другим участникам.
Используемые РР: публичные, неконтролируемые, универсальные (чаще — 21-й тип).
Зачем используется: предоставление альтернативы традиционной централизованной инфраструктуре (чаще всего инфраструктуре финансовых услуг). Нацелено в первую очередь на участников, которые не доверяют традиционным посредникам.
Примеры РР и проектов: биткоин, Ethereum, Cardano, IOTA и другие РР в основе публичных криптовалют; децентрализованные приложения и компании.

2) Автоматизация бизнес-логики.

Суть: гармонизация отношений между различными участниками какого-либо процесса, особенно

[37] Хорошая подборка и описание проектов представлены, к примеру, в исследованиях CB Insights: https://www.cbinsights.com/research/organizations-corporates-test-blockchains-distributed-ledgers/ и https://www.cbinsights.com/research/financial-services-corporate-blockchain-investments/. Также существует статистика Forbes, где описаны эксперименты крупнейших компаний, связанные с РР: https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain/#549af5cd2b5b.

между теми, которые часто не доверяют друг другу.
Используемые РР: консорциумные, контролируемые (чаще — 10-й или 12-й тип).
Зачем: чтобы перевести инновации и части бизнес-моделей/процессов изнутри компаний в рамки межкомпанейских отношений и интегрировать бизнес-процессы между различными участниками. Особенно подходит для систем, где высоки транзакционные издержки (например на проверку информации).
Примеры РР и проектов: Hyperledger, Corda, Symbiont, Quorum и проекты, предлагаемые на них.

3) Верифицируемая база данных.

Суть: инкорпорация аспектов неизменности и других преимуществ РР во внутренние базы данных и процессы компаний/юридических лиц.
Используемые РР: частные, контролируемые (чаще —2-й или 4-й тип).
Зачем: данные в базах могут быть изменены, а аудит обычно сопровождается высокими издержками и не является гарантированным инструментом выявления ошибок/махинаций. РР может позволить проще отследить изменения состояний записей во внутренних процессах.
Примеры РР и проектов: BigChainDB, Hydrachain, Chain, Openchain (больше не функционирует) и связанные с ними проекты.

Стоит отметить, что данные категории применений не являются взаимоисключающими и не формируют исчерпывающий список, а лишь предлагают взгляд на то, что уже существует в криптоиндустрии с точки зрения использования РР. В частности, к примеру, упомянутая выше токенизация, ключевая идея которой заключается в предоставлении цифрового эквивалента какой-либо ценности, с точки зрения категорий применений, описанных выше, может содержать элементы или быть на РР, нацеленных на все три категории, исходя из контекста проекта. К слову, сама идея цифрового предоставления ценности не уникальна для РР, ее имплементация возможна и с помощью других технологий, в том числе классических баз данных. Однако именно из-за возможности верификации, автоматизации или устранения доверия в частях данного процесса, а также возможности обеспечения более простого обмена ценностью благодаря данным категориям применений РР, токенизация получила активное развитие именно на базе РР, а не на базе других технологий. Помимо этого, РР может быть использован как инструмент интеграции с существующей криптоиндустрией (в том числе, например, криптобиржами для обеспечения торговли токенами) для получения дополнительных преимуществ от операций в ней. При этом, к примеру, платежная инфраструктура также может быть создана как на основе, к примеру, устранения необходимости доверия, так и на основе автоматизации бизнес-логики.

В силу важности данных применений стратегический анализ типов РР включает в себя оценку РР относительно устранения необходимости доверия и автономности[38]. Ряд гипотетических применений РР описан в профилях РР в приложении 1 исходя из классификации РР, представленной в разделе 4.

[38] Подробнее методология изложена в методологическом комментарии в конце данного документа.

РАЗДЕЛ 4. КЛАССИФИКАЦИЯ РР

Ключевые классификаторы РР

Основываясь на анализе существующих РР, а также на существующих подходах к классификации типов РР, в данном отчете выделено четыре ключевых классификатора РР, которые фундаментально влияют на последующий дизайн и функционирование РР. Несмотря на то что все четыре классификатора предопределяют технологическую архитектуру РР, первые два (архитектура и структура управления/контроля) в большей степени относятся к центральным технологическим элементам РР (например, относительно структуры и дизайна слоя хранения данных или слоя автоматизации), в то время как следующие два критерия (универсальность и подрывной потенциал) влияют в большей степени на стратегию развития и позиционирование РР, нежели исключительно на технологические особенности. По этой причине можно сказать, что первые два выбора относятся к технологическим, в то время как последние два — к стратегическим, — однако подобное разделение не столь четкое, должно использоваться с оговорками и представлено исключительно для удобства.

Технические классификаторы

1. Архитектура

Наиболее популярное разделение РР в открытых источниках происходит по технологической архитектуре. Выделяют три типа РР: **частные, консорциумные и публичные**. Визуально данные три типа можно положить на шкалу открытости.

Архитектура РР определяет **технические ограничения**, так как в закрытых РР, как и в других системах хранения данных, необходимо обеспечить безопасность и недоступность данных, в то время как в открытых РР, наоборот, записи должны быть возможны для просмотра (например через поисковый механизм) и, возможно, изменения (или взаимодействия с помощью транзакций) различными, зачастую не предопределенными заранее участниками. Помимо этого, публичные РР чаще имеют открытый исходный код (open source), который может быть изменен группой разработчиков как минимум с помощью форков, в то время как исходный код в частных РР доступен только закрытому сообществу разработчиков.
Консорциумные РР, в отличие от частных, управляются не одним юридическим лицом, а

группой. При этом условно можно выделить две ключевые группы консорциумных РР: с несколькими участниками и с большим количеством участников. В дальнейшем анализе данные группы не выделяются отдельно, кроме нескольких частей анализа, однако необходимо отметить, что консорциумные РР с несколькими участниками ближе по своей архитектуре и, соответственно, характеристикам и эффектам к частным РР, в то время как консорциумные РР с большим количеством участников ближе к публичным РР. Количество участников, которое считается большим и разделяет эти два типа консорциумных РР, при этом определяется не абсолютными значениями, а скорее относительной вовлеченностью различных участников экосистемы (например, потребителей, компаний, регулятора и др.) в дизайн, создание, запуск и возможное управление РР.

В целом, отличия архитектуры РР можно выделить относительно:

- открытости/доступности для публичного просмотра и изменения кода РР;
- возможности различных участников просматривать записи на РР;
- возможности отправлять транзакции (взаимодействовать с записями на РР).

Архитектура РР определяет то, какие элементы существуют в РР и каким образом они запрограммированы. Особенно это касается непосредственно слоя реестра. Например, существует ли поисковый механизм, какова структура консенсуса, какова структура сети девайсов, имеющих копию протокола РР, как записываются транзакции и т.д. В силу того, что слой реестра архитектурно находится ниже, чем остальные слои (например слой приложений/автоматизации), он влияет на все остальные технологические особенности РР. Решение по поводу архитектуры в том числе отвечает за уровень распределенности РР. При прочих равных, в среднем публичный РР обладает более высоким уровнем распределенности, чем частные РР, которые могут быть централизованы (как минимум на уровне юридического лица).

2. Структура управления/контроля

Структура управления РР может быть условно разделена по наличию прав контроля у различных участников. При наличии прав контроля участник может самостоятельно инициировать транзакции, в том числе изменять записи на РР. Помимо этого, в ряде случаев права контроля могут также позволить данному участнику изменять технический код РР. Зачастую структура управления и контроля также ассоциируется с разрешением/запретом на вход участникам (permissioned/permissionless). Однако это лишь один из аспектов управления РР.

Со структурой управления в первую очередь связан **слой приложений/автоматизации**. В неконтролируемом РР слой автоматизации развит на более высоком уровне, так как неуправляемая сущность РР требует большего уровня планирования и сценирования различных ситуаций заранее, а это происходит с помощью умных контрактов и других инструментов автоматизации. Выбор относительно структуры управления во многом определяет уровень автономности РР. Неконтролируемые РР чаще в большей степени подходят для применений умных контрактов (например, децентрализованных автономных бизнес-юнитов/компаний/обществ и т.д.), в то время как контролируемые РР могут предложить решения для децентрализованных, но не автономных приложений (децентрализованных компаний/обществ/бизнес-юнитов), сохраняя при этом возможность изменения записей в РР по решению управляющих.

В управляемых РР решения принимаются произвольно теми, кто управляет РР. При этом структура управления может быть различной: решения могут приниматься **единолично** или **рядом участников**, в рамках установленных правил или нет, автоматизированно или вручную и т.д. Однако обязательно существуют участники с правами администратора (superusers), которые позволяют им принимать решения относительно участников и записей в РР произвольно. **В неконтролируемых РР не существует участников с правами администратора**. Тем не менее в неконтролируемых РР возможна некоторая дифференциация ролей участников, например, на разработчиков, майнеров/валидаторов, держателей токенов или голосующих, — однако все разделения и ограничения автоматизированы. Все участники (в рамках любых автоматизированных ограничений) могут занять любую роль (например, стать валидатором, скачав ПО, или голосующим, получив/купив специальные токены). Это не означает, что у всех участников есть одинаковые шансы занять любую роль (например, в ряде PoS-систем валидаторами становятся те, кто имеет большее количество токенов), но означает, что **правила**, по которым определяются те или иные роли и функции участников, **стандартизованы**, а участники с ними **согласились, участвуя в системе.**

Отдельное внимание на текущий момент уделяется системам управления на РР (**on-chain governance**). Однако необходимо отметить, что большая часть предложений пытается встроить систему управления в инфраструктуру неконтролируемых РР, что противоречит их технологической составляющей и вызывает ряд проблем[39]. Системы управления РР на данный момент основываются на разделении типов токенов и введении токена с правом голоса (напр., Dai и MKR в системе MAKERDAO, см. кейс 2). Участники — держатели специальных токенов имеют право голоса для выбора определенных решений (например, стратегических приоритетов в системе или распределения пула ресурсов). В подобных системах существует риск ухода в хаос (например ситуации, когда ресурсы бесконечно собираются и хранятся на неактивном умном контракте), поэтому их применимость пока что остается под сомнением. Однако даже в подобных системах, благодаря тому что различные участники имеют право по определенным заранее правилам стать владельцем токена с правом голоса, подобная система может считаться неконтролируемой. В контролируемых системах управление на РР может осуществляться с помощью произвольных решений отдельных участников. Данная проблема может частично решиться с помощью систем искусственного интеллекта, однако скорее подобные системы можно будет классифицировать как контролируемые, где права контроля будут принадлежать искусственному интеллекту.

Стратегические классификаторы

3. Универсальность

С точки зрения применимости и потенциальных вариантов использования РР могут разделяться на нишевые и универсальные. **Нишевые** РР:

- нацелены на определенные группы/индустрии/рынки, учитывая их специфику и конъюнктуру;
- имеют ограниченный спектр применений с точки зрения действий и функционала.

Универсальные РР, наоборот, не имеют ограничений с точки зрения применимости и могут быть использованы для любых целей любыми участниками. По данной причине универсальные РР чаще создаются для государства или для нескольких/всех государств, нежели для

[39] Подробнее в разделах 3 и 6.

определенных групп/компаний/индустрий, а также являются инфраструктурой для **сквозных применений** (например, платеж или хранение информации любого вида), не зависящих от конкретного примера. Тем не менее универсальные РР могут быть кастомизируемыми под нужды различных участников, особенно если РР подразумевает создание инстанций.

Нишевые РР чаще, чем универсальные, создаются по инициативе самих участников и имеют четко обозначенные области применения. Однако экономически выгоднее может быть создание именно универсальных, нежели нишевых РР. Тем не менее, несмотря на то, что РР считается инфраструктурой, издержки на его создание относительно невысоки (основные издержки связаны с написанием программного кода РР, а не с созданием и строительством физической инфраструктуры, как происходит в случае классических инфраструктурных проектов). Но с точки зрения стратегии монетизации (если, к примеру, выбрана стратегия заработка на капитализации токена) и обогащения программ и слоя автоматизации данными, универсальные РР могут предоставить создателям и участникам РР больше выгод.

С точки зрения технологического строения РР, универсальность влияет не на фундаментальные элементы РР, а на второстепенные решения (например, необходимый размер блоков/поддерживаемой информации, структура записи данных на РР, правила консенсуса, направленность умных контрактов, поддержка открытых кодов и т.д.). Тем не менее подобные нефундаментальные элементы, несмотря на то, что могут быть изменены после запуска РР, могут вызвать резонанс у участников системы (см. кейс 5).

4. Подрывной потенциал

С точки зрения своего отношения к традиционным участникам РР могут быть **подрывными** или **поддерживающими**. **Поддерживающие** РР нацелены на **оптимизацию** операций/процессов у уже существующих участников рынка/экономики и т.д., в то время как подрывные РР пытаются предоставить инфраструктуру для альтернативных процессов, которые могут заменить традиционных участников.

Подрывной потенциал РР может возвести его в статус угрозы для существующих процессов/участников, что может вызвать сопротивление как со стороны непосредственно существующих участников, так и со стороны регулятора[40]. В силу того, что большая часть предложений РР, существующих сегодня на рынке, носит именно подрывной характер, реакции участников и регулятора были скорее протекционными, а криптоиндустрия получила своеобразный имидж. Тем не менее ряд критиков частных и консорциумных РР, большая часть которых носит поддерживающий характер, отмечает, что фокус на сохранении и поддержании текущих процессов и моделей может привести к развитию инкрементальных, а не фундаментальных инноваций.

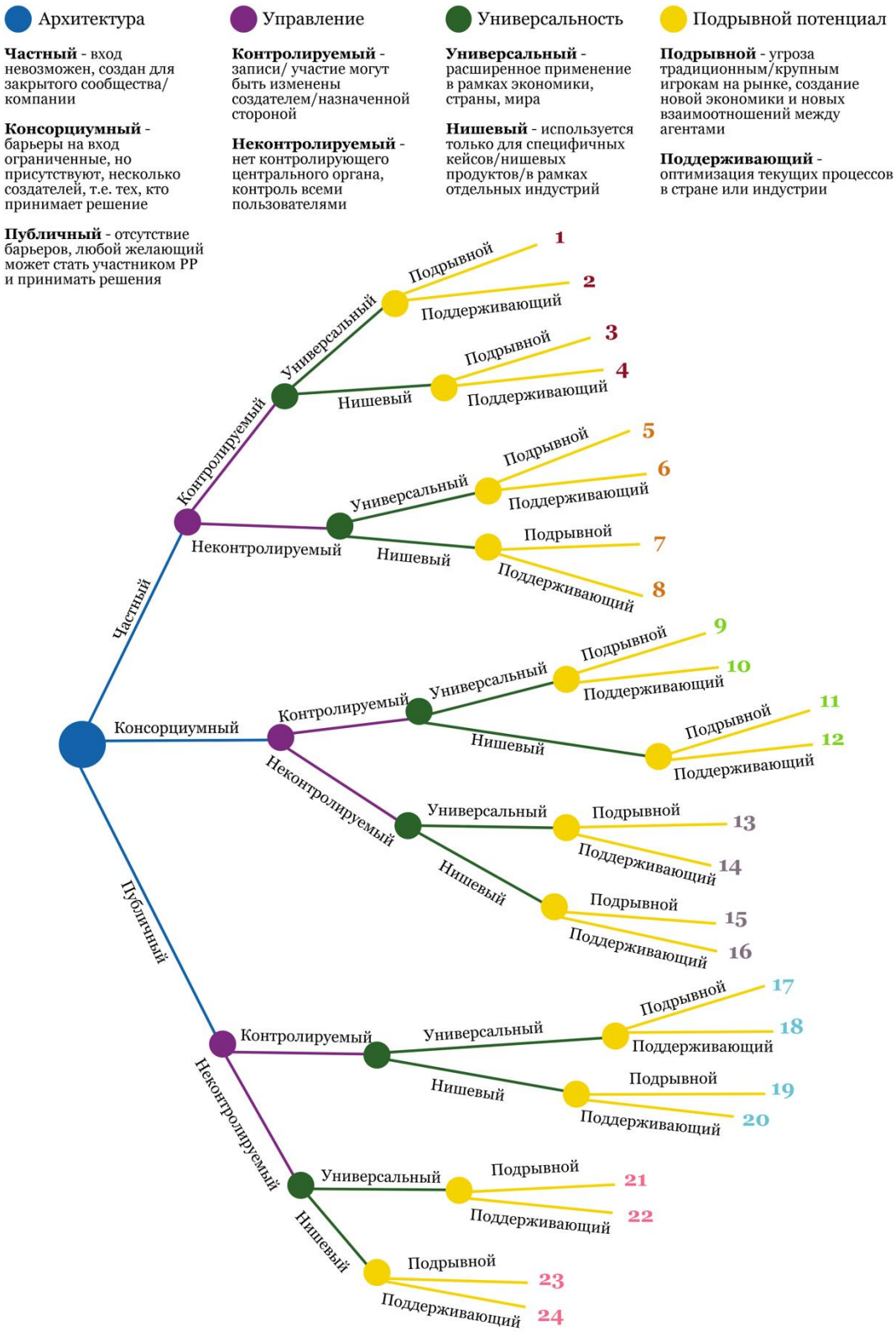
Как и в случае универсальности, отношение к традиционным участникам влияет скорее на содержание и направленность РР, нежели на его технологические составляющие, однако подрывной потенциал может также изменить содержание умных контрактов, структуру записи информации на РР, правила участия в РР и т.д., что в дальнейшем может быть сложно изменено, особенно для универсальный публичных неконтролируемых РР, где любое изменение требует консенсуса со стороны всех участников и может привести к расколу системы (см. кейс 5).

[40] Более подробно — в отчете «Регулирование в криптоиндустрии: состояние, стратегии и эффекты» Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО для обзора текущего состояния и трендов в регулировании криптоиндустрии: https://finance.skolkovo.ru/ru/sfice/research-reports/1797-2018-10-31/.

24 типа РР

В результате объединения данных четырех ключевых классификаторов получается карта 24 ключевых типов РР.

РИСУНОК 4. КАРТА КЛЮЧЕВЫХ ТИПОВ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ



Подробный анализ (профиль) каждого из типов РР представлен в приложении 2, а также в сводной таблице всех типов РР в приложении 3.
Отдельно можно выделить анализ характеристик РР разного типа и появляющиеся на его фоне тренды касательно эффектов использования РР разного вида[41].

ТАБЛИЦА 1. Ключевые характеристики 24 типов РР

Тип	Автономность	Транспарентность	Неизменность	Скорость	Кастомизация	Устранение необходимости доверия
1 (ЧКУР[42])	-1	-2	0	1	1	-1
2 (ЧКУП)	-1	-2	1	2	1	-2
3 (ЧКНР)	0	-1	-1	3	3	-1
4 (ЧКНП)	0	-1	0	4	3	-2
5 (ЧНУР)	0	0	2	-1	-1	1
6 (ЧНУП)	0	0	3	0	-1	0
7 (ЧННР)	1	1	1	1	1	1
8 (ЧННП)	1	1	2	2	1	0
9 (ККУР)	-1	-1	1	0	0	0
10 (ККУП)	-1	-1	2	1	0	-1
11 (ККНР)	0	0	0	2	2	0
12 (ККНП)	0	0	1	3	2	-1
13 (КНУР)	0	1	3	-2	-2	2
14 (КНУП)	0	1	4	-1	-2	1
15 (КННР)	1	2	2	0	0	2
16 (КННП)	1	2	3	1	0	1
17 (ПКУР)	-1	0	1	-1	-1	1
18 (ПКУП)	-1	0	2	0	-1	0
19 (ПКНР)	0	1	0	1	1	1
20 (ПКНП)	0	1	1	2	1	0
21 (ПНУР)	0	2	3	-3	-3	3
22 (ПНУП)	0	2	4	-2	-3	2
23 (ПННР)	1	3	2	-1	-1	3
24 (ПННП)	1	3	3	0	-1	2

Наибольшим уровнем автономности обладают неконтролируемые нишевые РР. Происходит это во многом по причине того, что данные РР требуют автоматизации, которая более вероятно может быть прописана заранее в силу нишевого характера РР. По этой же логике, наименьшим уровнем

[41] Методология выставления баллов описана в методологическом комментарии в конце данного документа.
[42] Номера и аббревиатуры типов РР в таблице соответствуют номерам типов РР из картинки выше. Первая буква — характеристика архитектуры (Ч — частный, К — консорциумный и П — публичный РР). Вторая — структуры управления (К — контролируемый, Н — неконтролируемый). Третья — универсальности (У — универсальный, Н — нишевый). Четвертая — подрывного потенциала (Р — подрывной (разрушительный), П — поддерживающий).

автономности обладают контролируемые универсальные РР. Что касается транспарентности, то здесь лидером являются публичные РР, при этом нишевые и неконтролируемые РР обладают большим уровнем транспарентности в силу четко обозначенной и более однородной группы участников и отсутствия участников с правами администратора. Схожая ситуация у параметра неизменности, однако здесь универсальные неконтролируемые РР имеют преимущество в силу отсутствия участников с правами администратора и более строгого контроля со стороны всех участников в силу большей базы пользователей.

В скорости лидируют частные и контролируемые РР, при этом наиболее популярные сегодня РР (21-го типа) — наименее быстрые с точки зрения скорости совершения транзакций в силу необходимости достижения консенсуса между большим количеством разнородных участников. Подобная тенденция наблюдается и в кастомизации: нишевые и контролируемые РР легче настроить под нужды отдельных участников, по причине чего РР данного типа легли в основу проектов блокчейна как услуги (BaaS).

В силу доминирования публичных РР в криптоиндустрии на текущий момент одним из наиболее часто упоминаемых свойств РР является **устранение необходимости доверия участников ко всем, кроме технологии**. Однако подобное свойство присуще в большинстве своем лишь РР данного типа. В контролируемых РР необходимо доверие к создателю/контролеру, а в частных и консорциумных РР часто требуется некоторое доверие участников друг к другу, особенно при наличии отдельных участников — валидаторов транзакций или иного распределения ролей в системе.

В целом, с точки зрения выбранных характеристик, одними из наиболее сильных профилей являются неконтролируемые нишевые РР, что может привести к тому, что криптоиндустрия будет построена на большом количестве нишевых РР, направленных на нужды отдельных участников. Эта тенденция укрепляется относительно низкими издержками на создание инстанций и дальнейшую кастомизацию РР. Однако в силу наличия РР, выделяющихся рядом других характеристик, как было указано выше, развитие инфраструктуры РР зависит скорее от стратегических решений, а также их конкретных применений.

Второстепенные классификаторы

Исходя из анализа технологических составляющих, тенденций, потенциальных эффектов, а также гипотетических и реальных применений РР, можно выделить ряд второстепенных классификаторов, которые не меняют вид РР значительно, однако могут оказать некоторое влияние на вид отдельных технологических компонентов. Хороший набор характеристик РР представлен в отчете Deloitte “Bitcoin, Blockchain & distributed ledgers: Caught between promise & reality”[43]. Классификация ниже частично основана на информации из данного отчета. Как и прежде, второстепенные классификаторы разделены на технологические и стратегические, однако данное разделение условно, так как выбор по каждому из критериев может повлиять на технологические компоненты РР. С точки зрения классификации, представленной выше, второстепенные классификаторы ниже гипотетически могут подходить для любого из РР. Однако в ряде случаев указаны наиболее вероятные типы РР, где данный классификатор может быть применим.

I. Технологические классификаторы

[43] Доступен онлайн: https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf.

1. Возможность аутсорсинга валидации

Выбор: валидация может быть отдана на аутсорс vs. валидация не может быть отдана на аутсорс.

Описание: данный классификатор посвящен возможности вовлечения валидаторов, которые являются внешними по отношению к РР. Наиболее ярким примером подобной валидации является аудит. Частный РР может иметь специальный узел просмотра, настроенный, к примеру, для регулятора и/или специальных участников, которые верифицируют, что в транзакции не было внесено никаких несанкционированных изменений. В зависимости от протокола консенсуса, подобная схема валидации, вовлекающая внешних, к примеру, независимых участников, может быть внедрена в любой тип РР.

2. Поддержка логики

Выбор: текстовые записи без автоматизации vs. логика в рамках РР vs. логика, включая элементы вне РР

Описание: данный классификатор относится к уровню развития умных контрактов на РР. Первый случай (текстовые записи) подразумевает, что никакой автоматизации, т.е. умных контрактов, нет. Второй выбор (логика в рамках РР) подразумевает, что настроенные умные контракты используют только внутренние оракулы. Третий выбор касается использования хотя бы одного из внешних оракулов и возможности интеграции информации/отправки информации вне РР. Выбор для данного классификатора зависит от выбора и настройки умных контрактов и оракулов, а также отделения слоя реестра от слоя автоматизации.

3. Основа консенсуса

Выбор: весь РР vs. чистое состояние (net state) vs. индивидуальные записи vs. обновления РР

Описание: данный классификатор в большей степени относится к структуре данных и протоколу консенсуса. Первый выбор подразумевает, что протокол консенсуса (например ПО верификации) использует информацию из всего реестра для принятия решения о валидации транзакций. Второй выбор касается консенсуса по отношению к набору транзакций, а не реестра. Участники/ПО проверяют набор транзакций, накопившихся с момента последней верификации (current net state). В результате образуется цепочка реестров, где каждый реестр хранит информацию о текущем состоянии, ссылку к прошлому состоянию и набор транзакций, подлежащих верификации. Подобный подход используется в Ripple и схожих РР. Третий выбор (записи) — это консенсус на уровне отдельных записей в РР, что позволяет им существовать в изоляции. Для использования данного подхода необходимо введение собственного определения консенсуса. Четвертый выбор (обновления РР) относится к согласию участников на уровне каждой отдельной транзакции. Транзакции могут быть собраны в блоки, в результате чего образуется блокчейн, как, к примеру, в сети биткоина.

4. Энергоэффективность

Выбор: РР требует меньше энергии, чем традиционные участники для подобных задач vs. РР

требует больше энергии, чем традиционные участники для подобных задач

Описание: данный PP относится в первую очередь к протоколу консенсуса, а также энергоэффективности и устойчивости выборов каждой из технологических компонент PP. К примеру, при использовании компьютеров или специального оборудования, скорее всего, потребление энергии будет выше, чем у традиционных участников, предлагающих подобные услуги в централизованном виде. В случае использования интернета вещей или мобильных устройств обратное, скорее всего, будет правдой, однако необходимо сравнение конкретных показателей деятельности проектов и PP.

5. Наличие нативного токена

Выбор: с нативным токеном vs. без нативного токена

Описание: данный выбор относится к выбору создателя внедрять или не внедрять нативный токен в соответствии с одной из целей их внедрения. Может быть использован на любом из PP, однако при текущей специфике PP чаще выбор стоит на контролируемых PP, так как валидаторами могут быть только выбранные пользователи, а не любые, поэтому нативный токен может быть не необходим для обеспечения мотивации участников.

II. Стратегические классификаторы

1. Оригинальность записей

Выбор: оригинальные записи vs. отсылки

Описание: выбор относится к тому, какой тип информации записывается на PP. Первый выбор (оригинальные записи) касается новой информации, которая не хранится нигде, кроме PP. Это касается в том числе информации, которая появляется в результате операций PP (например эмиссии и обмена токенов и др. транзакций). Второй выбор (отсылки) касается информации, которая уже существует где-то помимо PP (например, физические активы или информация на частных базах данных).

2. Сокращение издержек

Выбор: PP создает решение, направленное на сокращение издержек для пользователя vs. PP не создает решение, направленное на сокращение издержек для пользователя

Описание: данный выбор относится в первую очередь к применениям PP. В первом случае PP создает инфраструктуру, подходящую для решений, нацеленных на сокращение издержек. С технологической точки зрения это может отражаться в усиленной базе умных контрактов (для автоматизации) и каких-либо искусственных ограничениях и других составляющих архитектуры PP.

3. Альтруистический реестр

Выбор: PP устраняет набор посредников или иным образом снижает комиссии для финальных

пользователей vs. PP не снижает комиссии пользователям

Описание: данный выбор относится в первую очередь к применениям PP. В первом случае PP создает инфраструктуру, подходящую для устранения посредников и/или сокращения издержек для финального потребителя. С технологической точки зрения это может отражаться в усиленной базе умных контрактов (для автоматизации) и каких-либо искусственных ограничениях и других составляющих архитектуры PP.

4. Борец с неэффективностью

Выбор: PP устраняет неэффективности рынка (например асимметрию информации) vs. PP не устраняет неэффективности рынка

Описание: данный выбор относится в первую очередь к применениям PP. В первом случае PP создает инфраструктуру, подходящую для решений, нацеленных на устранение неэффективностей рынка. С технологической точки зрения это может отражаться в усиленной базе оракулов, и специальной структуре данных, а также настройки узлов просмотра, например, для обеспечения повышенного уровня транспарентности, и каких-либо искусственных ограничениях и других составляющих архитектуры PP.

5. Фундаментальные инновации

Выбор: PP способствует развитию фундаментальных инноваций vs. PP не способствует развитию фундаментальных инноваций

Описание: данный выбор относится в первую очередь к применениям PP. В первом случае PP создает инфраструктуру, подходящую для решений, нацеленных на развитие фундаментальных (в том числе подрывных) инноваций. С технологической точки зрения это может отражаться в усиленной базе умных контрактов (для автоматизации), а также наборе оракулов и решений по интеграции различных PP и других составляющих архитектуры PP.

6. Структура доверия

Выбор: доверие одному участнику vs. доверие всем участникам vs. доверие некоторым участникам vs. доверие никому

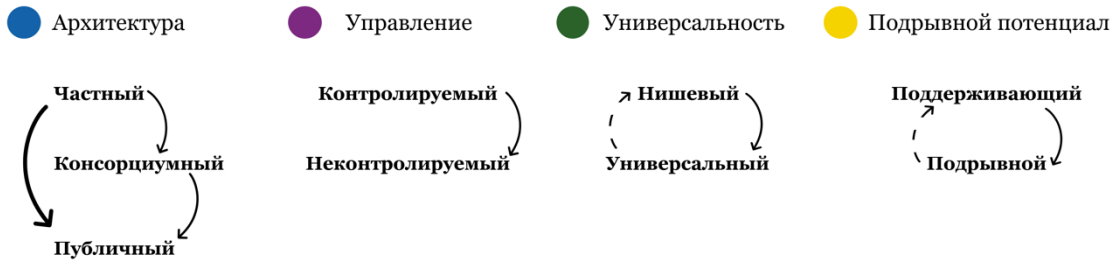
Описание: данный выбор относится к структуре контроля, протоколу консенсуса, а также обеспечению транспарентности транзакций. В первом случае (доверие одному участнику) существует один валидатор/контролер, ответственный за изменения в системе. Во втором случае (доверие всем участникам) все участники равны и могут изменять PP, поэтому необходимо доверять всем, что не будет несанкционированных изменений. Третий случай (доверие некоторым участникам) схож с первым и отличается лишь тем, что контролеров/валидаторов больше одного. Четвертый выбор (доверие никому) подразумевает доверие технологии или другому механизму определения консенсуса. Подобная ситуация может быть достигнута автономным механизмом верификации транзакций и отсутствием участников с правами администратора.

РАЗДЕЛ 5. СТРАТЕГИИ ВЫБОРА РР

Динамика перехода и трансформация РР

Указанные выше классификаторы предлагают статичную картину РР. Тем не менее, с технологической и стратегической точек зрения, возможен переход различных РР из одной категории в другую. Однако стоит отметить, что любой переход может быть сложно имплементируем в силу сопротивления участников к изменениям (см. кейс 5), тем более таким масштабным. Ниже представлены возможные переходы классификаторов РР из одного состояния в другое.

РИСУНОК 5. ПЕРЕХОДЫ КЛАССИФИКАТОРОВ РР



Источник: аналитика авторов

С точки зрения архитектуры частные РР являются наиболее гибкими. Если в ряд участников частного РР (например участников фирмы/государства) добавить участников из других подобных юридических лиц (например другой фирмы/государства), то есть распространить РР из рамок одного юридического лица на несколько, то частный РР станет консорциумным. В то же время, если снять любые ограничения на участие в РР, то частный и консорциумный РР могут стать публичными. Однако обратный переход невозможен. При попытке закрытия публичного РР (ограничения доступа к РР) те участники, у которых уже есть копия РР, могут получить доступ к записям до момента закрытия РР. Гипотетически возможно закрытие РР среди тех участников, что уже им пользуются, однако в силу того, что база пользователей публичных РР обычно разнородна по различным характеристикам (например, география, возраст, индустрия и т.д.), закрытие может быть практически невозможным. Более того, даже если дальнейший вход в РР станет закрытым, код и ранние версии РР могут храниться у неизвестных сторон и быть реплицированы далее. Помимо этого, наличие поискового механизма (explorer) усложняет возможность ограничения доступа к данным, так как, даже не имея копии РР, часть данных может быть сохранена различными участниками. Консорциумный РР также не может быть закрыт в силу того, что копии реестра будут храниться у бывших участников до закрытия РР.

С точки зрения структуры управления контролеры РР могут отпустить контроль и сделать РР

неконтролируемым. В данном случае решения, принимавшиеся до решения об отпущении РР произвольно, автоматизируются и РР становится более автономным, а права контроля над РР уничтожаются и участники становятся равноправными. Обратное невозможно. Однако существует ситуация, при которой у одного или нескольких участников искусственно аккумулируются права контроля (например, более 50% мощности в PoW-системах или большая часть токенов для голосования). В данном случае права подобных участников несколько выше, чем у других. Однако в отличие от контролируемых РР, где права контроля защищены от внешнего воздействия, данные права контроля можно разрушить (например, аккумулировав большую сумму токенов, обесценив их или использовав один из механизмов защиты от 50%+1 атаки, которые уже предложены в криптоиндустрии). По этой причине неконтролируемый РР невозможно сделать по-настоящему контролируемым ни при каких условиях. Точно так же возможно усиление и ослабление ограничений на вход и участие в РР, однако в силу того, что это лишь один из аспектов управления РР, сделать любое решение подконтрольным после уничтожения прав администратора, заложенных при дизайне РР, невозможно.

Что касается стратегических классификаторов, то переход из одного состояния в другое здесь проще, чем в технологических классификаторах, однако переход из некоторых состояний в другие затруднительнее. Так, из нишевого РР возможно сделать универсальный РР, изменив спектр возможных применений и задач, на которые рассчитан РР. Так произошло с рядом нишевых РР, например Corda и Symbiont, где изначальный фокус на применение исключительно в финансовой индустрии сменился более широким подходом для любых заинтересованных услуг. Стоит отметить, что в силу возможных технологических ограничений (например, размер блока, структура записи информации и т.д.) данный переход может сопровождаться рядом барьеров, однако при изначальном проектировании дизайнеры РР чаще закладывают некоторый запас на универсальность и делают параметры несколько больше, чем необходимо только в рамках определенных применений. Помимо этого, расширение и устранение отдельных ограничений обычно проще, нежели их установка, особенно в контексте управляемых и/или частных РР, где для изменений необходим консенсус меньшего количества участников. При попытке сделать из универсального РР нишевый ограничения, наоборот, необходимо устанавливать, что может быть сложно как с точки зрения принятия изменений (особенно если необходим консенсус большого количества участников), так и с технологической, так как, если в ряде настроек РР запрограммирован таким образом, что ограничения отсутствуют, их внедрение может быть затруднительно. Тем не менее РР может стать естественно нишевизированным, если область применения будет ограничена самими пользователями РР исходя из специфики и характеристик данного РР. Более того, при возможности кастомизации универсального РР и соединения отдельных инстанций (или сайдчейнов) в единую сеть (см. раздел 5) настроенные и более нишевые инстанции РР могут формировать единую универсальную инфраструктуру. Однако подобные варианты развития РР более трудоемкие и менее вероятные, нежели переход от нишевых РР к универсальным, по причине чего подобный переход обозначен пунктирной линией на схеме.

Наконец, с точки зрения отношения к традиционным участникам изначально поддерживающий РР может стать подрывным в зависимости от конкретных применений, предложенных на инфраструктуре. Руководствуясь той же логикой, что и в случае универсальных и нишевых РР, в силу того, что поддерживающие РР в своем дизайне уже могут иметь ряд ограничений, устранение данных ограничений может быть проще, чем их установка на оперирующем РР. По данной причине, как и в случае универсальности, переход из поддерживающего в подрывной РР проще, нежели наоборот. Более того, с точки зрения дальнейшего продвижения и стратегии применения

инфраструктуры, если на РР предложены подрывные проекты, традиционные участники, операции которых подрываются благодаря данному РР, вряд ли согласятся использовать РР с целью поддержания своего бизнеса. По данным причинам переход из подрывного в поддерживающее состояние обозначен пунктирной линией.

Комбинируя данные возможные переходы, можно получить динамичную версию классификации РР, которая показывает, каким из оставшихся типов РР может стать каждый отдельно взятый тип РР. Возможные варианты перехода из одного типа РР в другой представлены в таблице ниже. Номер и цвет соотносятся с номером и цветом РР из рисунка 4 и таблицы 1 из раздела 4. Первая строка каждого столбца соотносится с отправной точкой (первоначальным состоянием РР). Значения в строках ниже — возможные типы РР, которыми может стать данный тип РР, исходя из возможной трансформации классификаторов, представленной выше (рисунок 5).

ТАБЛИЦА 2. ВАРИАНТЫ ПЕРЕХОДА РР ИЗ ОДНОГО ТИПА В ДРУГОЙ

Тип блокчейна																			
1 2 3 4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
любой	6	5	5	5	10	9	9	9	14	13	13	13	18	17	17	17	22	21	21	21
	7	7	6	6	11	11	10	10	15	15	14	14	19	19	18	18	23	23	22	22
	8	8	8	7	12	12	12	11	16	16	16	15	20	20	20	19	24	24	24	23
	13	13	13	13	13	13	13	13	21	21	21	21	21	21	21	21				
	14	14	14	14	14	14	14	14	22	22	22	22	22	22	22	22				
	15	15	15	15	15	15	15	15	23	23	23	23	23	23	23	23				
	16	16	16	16	16	16	16	16	24	24	24	24	24	24	24	24				
	21	21	21	21	17	17	17	17												
	22	22	22	22	18	18	18	18												
	23	23	23	23	19	19	19	19												
	24	24	24	24	20	20	20	20												
					21	21	21	21												
					22	22	22	22												
					23	23	23	23												
					24	24	24	24												

Источник: аналитика авторов

Новый подход к выбору РР

Выбор наиболее подходящего типа РР позволяет создать или использовать корректную инфраструктуру для участия в криптоиндустрии или ее развития. Как отмечалось ранее, возможный провал применений автоматизации, в частности ДАО, а также ICO связан не только с мошенническими действиями разных участников, но и с отсутствием подходящей инфраструктуры. В данном контексте профили РР из приложения 2 — это своеобразный каталог возможных РР, прочитав который, можно выбрать наиболее подходящий для конкретных целей и применений реестр. Стоит отметить, что, согласно текущим тенденциям, в ряде случаев гонка за

попыткой внедрения РР может привести к созданию неэффективных решений (т.е. выбору, когда компания решает внедрить РР несмотря на то, что обычная централизованная база данных или другие альтернативы эффективнее). По этой причине, даже рассматривая РР в качестве возможного выбора, необходимо учитывать и сравнивать существующие решения с альтернативами, в том числе среди других технологий хранения и управления данными. Несмотря на то, что для получения более точных рекомендаций относительно использования того или иного реестра необходимо проведение дополнительного исследования, исходя из конкретных характеристик различных потенциальных применений, данный стратегический анализ может быть полезным для получения первого понимания о том, какой РР можно рассмотреть.

Суммируя результаты моделей, упомянутых в разделе 1, перед определением типа РР необходимо определиться, нужен ли РР в целом. В контексте данной классификации, учитывающей гипотетические возможности развития РР, более точно сформулированный вопрос, на который необходимо ответить при выборе, работать ли с РР, — это «Планируется ли в вашем применении работа с цифровыми записями?». Если ответ — «да», РР может являться опцией для рассмотрения среди других альтернатив, однако, как отмечалось в других моделях, решения с помощью РР могут быть неэффективными по сравнению с альтернативами. Есть ответ — «нет», то РР может не подходить для данных применений.

Выбор архитектуры

Для выбора архитектуры РР необходимо ответить на вопрос: «Есть ли ограничения по правам просмотра записей в данном РР?»

Если ответ — «нет», то наиболее подходящий вариант — это публичный РР. Если — «да, просмотр ограничен рамками одного юридического лица», то наиболее подходящий вариант — частные РР. Если — «да, просмотр ограничен рамками нескольких юридических лиц», то наиболее подходящий вариант — консорциумные РР.

Выбор структуры управления

Для выбора структуры управления РР необходимо ответить на вопрос: «Есть ли необходимость в выделении прав изменения записей на РР?» Помогающим вопросом также может быть: «Есть ли необходимость ручного контроля за изменениями данных?» Данная необходимость может появиться в результате минимизации рисков изменения записей или при других причинах необходимости сохранения прав администратора у одного или более участников[44].

Если ответ — «нет», то наиболее подходящий вариант — это неконтролируемый РР, однако при нем необходим более высокий уровень автоматизации, что может быть барьером для создания и внедрения подобных РР. Если — «да», то наиболее подходящий вариант — контролируемые РР.

Выбор универсальности

Для выбора универсальности РР необходимо ответить на вопрос: «Есть ли четко обозначенная индустрия или бизнес-процесс, на который направлено применение РР?»

Если ответ — «нет, применения должны быть не ограничены», то наиболее подходящий вариант —

[44] Потенциальные причины такого решения описаны в разделах 1 и 3

это универсальный PP, однако при нем возможен более низкий уровень кастомизации решений. Если — «да», то наиболее подходящий вариант — нишевые PP.

Выбор подрывного потенциала

Для выбора подрывного потенциала PP необходимо ответить на вопрос: «Устраняет ли/уничтожает ли данное применение какие-либо существующие процессы/участников?» Данными участниками могут быть, к примеру, централизованные посредники.

Если ответ — «нет», то наиболее подходящий вариант — это поддерживающий PP. Если — «да», то наиболее подходящий вариант — подрывной PP.

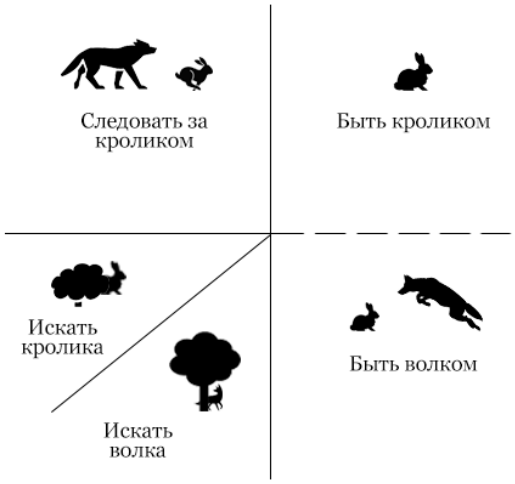
Совместив результаты ответов на данные вопросы, можно получить один из 24 PP, который, вероятно, наиболее подходит для конкретного применения. Если на какой-то из вопросов ответ неоднозначен, то полезно может быть изучить все категории PP по одному из/нескольким параметрам. Однако общая рекомендация заключается в просмотре всех типов PP независимо от ответов на вопросы и проведении дополнительных исследований, исходя из информации и специфики проекта, при желании использовать PP.

Стратегии создания и продвижения PP

Исходя из позиционирования и истории появления новых PP, можно выделить четыре основные стратегии создателей PP. Данный подход вдохновлен аналитической рамкой Cynefin и предлагает динамический инструмент принятия решений, а не статическую классификацию существующих стратегий участников криптоиндустрии. McKinsey также предлагают классификацию стратегий, однако не относительно создания различных PP, а относительно их применений[45]. Данные два подхода можно считать комплементарными.

[45] В исследовании McKinsey “Blockchain beyond the hype: What is the strategic business value” предлагаются четыре стратегии применения PP исходя из стандартов и регуляторных барьеров (высокие и низкие) и доминирования на рынке (высокое и низкое). В результате соединения данных растяжек появляются четыре стратегии применения PP: лидер, аттакующий, последователь и организатор. Лидер действует сейчас, чтобы создать индустриальный стандарт, и фокусируется на проектах с наибольшим потенциальным эффектом. Аттакующий фокусируется на подрывных P2P-кейсах. Последователь готовится к принятию появляющихся стандартов и тестирует технологию PP. Организатор строит альянсы с другими организациями, чтобы найти проекты с высоким потенциальным эффектом. Данные стратегии схожи со стратегиями, представленными в данном исследовании, однако фокусируются только на применении PP, в то время как рамка, представленная в данном анализе, описывает стратегии создания и взаимодействия с различными PP и предлагает более широкий взгляд на стратегический выбор участников криптоиндустрии.

РИСУНОК 6. СТРАТЕГИИ В ОТНОШЕНИИ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ УЧАСТНИКОВ КРИПТОИНДУСТРИИ



Источник: аналитика авторов

Стратегия «Следовать за кроликом»

Найти лидера — обосновать действия лидера — следовать за ним

Описание: участники/создатели РР выбирают один из существующих РР и идеализируют его. Новые РР создаются по образу существующих с инкрементальными изменениями или же вовсе не создаются, так как предпочтение отдается «идеальному» РР, а применения или улучшения предлагаются на базе существующей инфраструктуры. В результате могут провоцироваться инкрементальные инновации, поддерживающие уже существующие РР. С другой стороны, проработанная идея, которая постоянно дополняется предложениями последователей, может привести к значительному развитию инфраструктуры.

Существующие примеры: инстанции существующих РР (например блокчейна биткоина), экосистема Ethereum.

Стратегия «Быть кроликом»

Обосновать свои действия — быть лидером/найти последователей — (со)существовать

Описание: участник создает РР, предлагая решение, которое должно подходить для решений проблем на различных рынках/приносить выгоды различным участникам. Предложение и позиционирование предложения опирается не на существующие РР и их (не)успешность, а на гипотетические преимущества непосредственно создаваемого РР. Независимость РР от существующих решений может, с одной стороны, привести к фундаментальным инновациям, однако, с другой стороны, — к отсутствию рыночного исследования и повторению уже

существующих идей, а также допущению уже существующих ошибок.

Существующие примеры: NEO и Waves — два практически одинаковых PP, схожих с Ethereum. Хакатоны и девелоперские сообщества Ethereum, где Ethereum Foundation выступает в роли лидера, который краудсорсит идеи от участников подобных мероприятий.

Стратегия «Быть волком (съесть/гнаться за кроликом)»

Найти проблемы в существующих решениях/PP — разрушить престиж существующих решений/PP — создать свое решение

Описание: после исследования рынка участник выявляет проблемы существующих PP, объясняет их публике и предлагает решение, учитывающее и решающее данные проблемы. Изучение криптоиндустрии позволяет учесть сложившийся уровень развития технологий, а также проблемы, которые уже наличествуют в результате использования существующих подходов к созданию PP. Это не означает, что исследование рынка окажется всеобъемлющим и будет учитывать как негативный, так и позитивный опыт, что могло бы привести к фундаментальным инновациям и прорывным предложениям на рынке, однако предложения по улучшению существующих PP приводят к постоянному развитию технологии, ее применений, а также экспериментов с PP.

Существующие примеры: Cardano — решение предлагается частью команды создателей/разработчиков Ethereum для того, чтобы предложить решение, устраняющее проблемы PP второго поколения и особенно Ethereum; Stellar — криптовалюта и инстанция PP, созданная бывшими разработчиками Ripple, в том числе для решения проблем Ripple; большинство PP третьго поколения позиционируются как решения проблем PP второго поколения. Особенно часто критике и атаке подвергается PP Ethereum и биткоина.

Стратегии поиска

Данные стратегии не предлагают альтернативных/новых действующих PP, однако могут предложить новые концепции или объяснить, почему ряд предложений не работает, что позволит разработчикам затем учесть эти проблемы или создать новые PP.

Вариант 1. «Искать кролика»

Придумать идею — обосновать ее необходимость — ждать решения

Описание: участник придумывает идею для криптоиндустрии и объясняет ее полезность другим участникам. Тем не менее по различным причинам (например у предлагающего участника отсутствуют необходимые ресурсы/навыки) решение ожидается от других участников. Подобный подход позволяет придумать инновации для криптоиндустрии, в том числе фундаментальные, во многом благодаря краудсорсингу и обсуждению идей до их имплементации, однако предложенные идеи могут быть нереалистичными и нереализуемыми как благодаря сопротивлению сообщества или отсутствию свободных разработчиков, заинтересованных в выполнении предложения, так и благодаря отсутствию необходимых технологий на должном уровне.

Существующие примеры: Bitcointalk и предложения там; форумы, посвященные криптовалютам (например ветки Reddit), особенно посты держателей криптовалют на своих ветках.

Вариант 2. «Искать волка»

Найти проблемы в существующих решениях/PP — разрушить престиж существующих решений/PP — ждать решения

Описание: участник находит ограничения, проблемы и недостатки существующих PP и объясняет их другим участникам, что подрывает доверие к данным PP. Тем не менее по различным причинам (напр., у предлагающего участника отсутствуют необходимые ресурсы/навыки) альтернативное решение или улучшение не предлагаются и ожидаются от других участников. Подобный подход позволяет улучшить существующие решения и привести к инновациям, в том числе фундаментальным, во многом благодаря краудсорсингу и обсуждению идей до их имплементации, однако предложенные идеи могут быть нереалистичными и нереализуемыми как благодаря сопротивлению сообщества или отсутствию свободных разработчиков, заинтересованных в выполнении предложения, так и благодаря отсутствию необходимых технологий на должном уровне. Помимо этого, даже необоснованные и непроверенные решения могут подорвать доверие других участников к существующим PP и ограничить развитие/применение существующей инфраструктуры.

Существующие примеры: Bitcointalk и предложения там; форумы, посвященные криптовалютам (например ветки Reddit), особенно посты держателей криптовалют на ветках других криптовалют; колонки и посты на medium и в СМИ; ответы на Quora. Особенно заметны в данном контексте критики EOS и IOTA, которые привели к существенному обвалу нативных токенов данных PP.

Состояние криптоосознанности

Наподобие аналитической рамки Cynefin, которая предлагает учитывать, что посредине, между стратегиями, находится состояние беспорядка (Disorder), в котором принимаются решения и находятся различные участники большую часть времени, данный инструмент тоже предлагает своё видение состояния между всеми стратегиями и подходами участников криптоиндустрии. В середине между стратегиями находится состояние криптоневедения (cryptoignorance), в котором участники не обладают никакой позицией и знаниями относительно существующих процессов в криптоиндустрии. Данное состояние — это противоположность криптоосознанности, состоянию, при котором решения в криптоиндустрии принимаются исходя из полного понимания существующей ситуации и процессов. Криптоосознанность — одна из составляющих концепции финансовой осознанности, при которой решения на рынке финансовых услуг принимаются без воздействия поведенческих и когнитивных смещений[46].

Благодаря тому что большая часть решений принимается в состоянии криптоневедения, часть решений, предлагаемых в криптоиндустрии, полностью игнорирует существующие решения, а количество PP растет в темпе, опережающем спрос на использование подобной инфраструктуры. Изобилие PP, с одной стороны, может привести к появлению большего числа применений, особенно если предложения направлены на решения нишевых проблем и задач. С другой стороны, большая часть существующих предложений — это универсальные PP 21-го типа, которые ставят

[46] См. отчет «Финансовая инклюзивность за пределами доступности» Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО для деталей относительно финансовой осознанности, стратегии ее повышения, а также описания поведенческих и когнитивных смещений на рынке финансовых услуг и путей уменьшения их влияния: https://finance.skolkovo.ru/ru/sfice/research-reports/1810-2018-11-15/.

перед собой задачу создания универсальной новой инфраструктуры. Широкий спектр предложений обосновывается тем, что для различных применений могут использоваться различные PP, однако ряд предложений дублируют друг друга или предлагают лишь инкрементальные инновации, а универсальный характер изначально подразумевает использование PP в различных целях. По данной причине зачастую подобные доводы и объяснения несостоятельны, а криптоиндустрия требует переформатирования с точки зрения предложений и стратегии их выработки. Помочь подобному реформатированию может стратегия продвижения и повышения криптоосознанности, в том числе благодаря площадкам и платформам образования различных участников относительно криптоиндустрии (в том числе со стороны разработчиков — например, Lisk Academy, Blockchain Hub и др., — государства и других заинтересованных участников).

Переход из кролика в волка

Переход между стратегиями «быть кроликом» и «быть волком» обозначен пунктирной линией, так как переход между ними намного проще, чем между другими стратегиями. Это происходит в силу того, что при обосновании своих предложений создатели PP иногда прибегают к критике существующих предложений. Помимо этого, после запуска решения, основанного на критике существующих предложений, создатели нового PP могут выбрать стратегию «быть кроликом» и начать развивать и продвигать свой продукт в отрыве от предложений, появляющихся и существующих в криптоиндустрии.

Переход между другими стратегиями относительно сложнее и обозначен сплошной, а не пунктирной линией. Обычно для смены стратегии требуется значительное усилие и признание изменения позиции со стороны разработчиков/создателей/контролеров PP. Помимо прочего, по данной причине в контексте публичных неконтролируемых PP, где для любых изменений требуется консенсус большого числа участников PP, предложения по изменениям и форки могут привести к расколу системы и появлению новых PP.

Особые стратегии

«Атака на слона»

Данная стратегия — подвид стратегии «быть волком» или «искать волка», где объектом критики является один из крупнейших существующих PP (обычно блокчейн биткоина или Ethereum). Отличительной особенностью данной стратегии является то, что эффекты критики на данные PP минимальны, а сама критика зачастую неактуальна в силу быстрого развития сети и экосистемы подобных проектов или появления альтернативных PP, в которых данные проблемы уже были решены (например, частая критика — это отсутствие возможности интеграции с другими PP, хотя в Ethereum уже есть ряд подобных предложений, включая Plasma, или критика скорости проведения транзакций/создания блоков, хотя данная проблема уже решена рядом PP (например, Solana, Tangle, EOS) и некоторые решения предложены и для Ethereum). Тем не менее благодаря низкому уровню исследования рынка и осознания процессов в криптоиндустрии у различных участников подобная стратегия может быть успешной для привлечения клиентов, особенно на стадии ICO и предпродажи.

«Кроборотень», или «кролик-оборотень», или «хищный кролик»

Данная стратегия основывается на простом переходе из стратегии «быть кроликом» в стратегию «быть волком» и наоборот. В отличие от случайного перехода, данная стратегия подразумевает осознанный выбор создателя РР сначала создать продукт, а затем критиковать решения или, наоборот, обосновывать свое решение исходя из критики, но затем не следить за рыночными предложениями или, наоборот, следить и объяснять свои отличия/изменять собственный продукт. Данная стратегия может быть как более эффективной, чем отдельно взятые стратегии «быть кроликом» и «быть волком», так и менее, в зависимости от конкретных действий управляющих/создателей РР.

РАЗДЕЛ 6. БУДУЩЕЕ КРИПТОИНДУСТРИИ

Экосистема криптоиндустрии

Чтобы определить релевантные вызовы и тенденции в развитии криптоиндустрии, необходимо сначала обозначить ключевые элементы ее экосистемы. Данные элементы не являются непосредственными участниками криптоиндустрии, однако оказывают на нее влияние, формируя направления развития, устанавливая драйверы и барьеры. На основе анализа информации по криптоиндустрии было выделено девять основных групп участников, которые визуально можно представить следующим образом.

РИСУНОК 7. ЭКОСИСТЕМА КРИПТОИНДУСТРИИ

Источник: аналитика авторов

Данная экосистема является расширением технологической экосистемы, представленной в разделе 2, и предлагает стратегический взгляд на индустрию и ее развитие. В частности, государство и регулятор устанавливают национальные приоритеты, могут сами являться потребителями услуг криптоиндустрии и определяют регуляторную рамку. Международные организации и регуляторы при этом могут помочь локальным регуляторам сформировать единые глобальные стандарты в отношении криптоиндустрии. Эксперты и СМИ формируют общественное мнение относительно ключевых элементов криптоиндустрии и также могут быть потребителями предложений. Индустриальные ассоциации могут быть катализатором или, наоборот, источником сопротивления для коммерческих применений PP и создания альтернативных бизнес-моделей.

Новые игроки в этом контексте могут предложить подрывные инновации, которые приведут к качественному скачку всей цифровой экономики. Наконец, поставщики ресурсов и инвесторы предоставляют необходимые финансовые и другие ресурсы (к примеру электроэнергию) для функционирования и развития индустрии. В целом, экосистемный взгляд на криптоиндустрию позволяет задать рамку для дальнейшего анализа как технологического, так и общего развития как применений, так и индустрии и, возможно, криптоэкономики в широком смысле данного понятия.

Текущие вызовы криптоиндустрии

Среди вызовов, существующих на данный момент в криптоиндустрии, можно выделить пять основных: регулирование, управление, конфиденциальность данных, безопасность и масштабируемость. При этом данные проблемы и болевые точки выделяются практически во всех отчетах, посвященных криптоиндустрии[47]. Дополнительно можно выделить вопрос скорости изменения публичных РР. Несмотря на то, что это не универсальная индустриальная проблема, так как публичные неконтролируемые РР — наиболее популярный тип РР, данный вызов можно отнести к уровню индустриальных. Нарастающую важность также набирают этические и политические вопросы использования РР, однако пока что они не выделяются в качестве ключевых вызовов. Ниже описаны основные проблемы, связанные с этими областями, и кейсы, демонстрирующие их важность.

1. Регулирование

Ключевые вызовы касательно регулирования, а также стратегии и пути их ослабления были описаны в первом отчете данной серии. Среди ключевых вызовов криптоиндустрии можно отметить неясность эффектов внедрения технологии РР на страну на макро- и микроуровнях, повышение активности регулятора в области лицензирования, налогообложения, а также процедур KYC и правил CFT и AML. С точки зрения технологий дополнительным вызовом является необходимость настройки возможности просмотра и верификации транзакций регулятором и государством, что особенно важно в контексте частных, консорциумных и контролируемых РР, где данные могут быть недоступны для просмотра любым участникам.

2. Управление на РР

Одним из наиболее сложных и открытых вопросов является вопрос управления. Основной причиной этому, как показал анализ выше, служит тот факт, что попытки создания системы управления происходят на контролируемых РР (чаще всего 21-го типа), что противоречит их технологической архитектуре. Ключевые вопросы управления включают в себя определение критериев/решение о предоставлении доступа в сеть потенциальным участникам, определение политик и администрирования, создание стандартов, особенно управления данными и совместимостью различных РР, решение конфликтов и контроль за изменениями в РР.

Одним из наиболее эффективных решений для устранения данного вызова является использование контролируемых версий РР под цели, где необходимо обеспечение системы управления. Другим примером попытки устранения проблем управления может служить попытка внедрения систем искусственного интеллекта в системы на основе РР. Подобные предложения пока находятся в стадии разработки в силу уровня развития технологии искусственного

[47] См., например: https://blocksdecoded.com/blockchain-issues-security-privacy-legal-regulatory-ethical/ или https://www.hpe.com/emea_europe/en/solutions/blockchain.html.

интеллекта, однако гипотетически, в будущем, это может быть решением и ряд стартапов начинают двигаться в этом направлении[48]. Альтернативным решением, которое существует уже сейчас, является разделение токенов в PP на два вида: одни — как инструмент мотивации участников (сродни нативным токенам), а другие — токены для голосования и управления. Одним из наиболее ярких кейсов здесь является проект MAKERDAO.

КЕЙС 2. Управление в MAKERDAO

MAKERDAO — это децентрализованная автономная организация на базе PP Ethereum, созданная в 2017 году. У MAKERDAO есть два ключевых токена: DAI и MKR. DAI — это стейблкоин, привязанный по курсу 1:1 к доллару США. DAI эмитируется по правилам, установленным MAKERDAO, с помощью отправки токенов ETH или других поддерживаемых токенов на специальный умный контракт. DAI также можно купить извне через криптобиржи. DAI использует залоговые средства, чтобы держать курс с долларом стабильным, а также позволяет пользователям использовать торговлю с помощью финансового рычага/плеча. MAKERDAO собирает периодические комиссии с пользователей DAI, чтобы наполнять пул залоговых средств, а также действует как покупатель последней инстанции, если нет других покупателей для каких-либо сделок. MAKERDAO состоит из набора умных контрактов на сети Ethereum и управляется полностью на PP.

Управление происходит с помощью токена MKR, который невозможно купить на криптобиржах. Изначально MKR был распределен по определенному списку держателей, которые затем могут изменять правила покупки/продажи данного токена. Токены MKR используются для отправки на специальные умные контракты, учрежденные для голосования о ключевых стратегических решениях касательно управления MAKERDAO, включая вопросы распределения пула залоговых средств, риск-менеджмента и правил внутри системы.

Одна из ключевых проблем для MAKERDAO — эффективное голосование. В истории голосования MAKERDAO были случаи, когда участники либо не голосовали, либо голосовали неэффективно. Один из центральных рисков — это вероятность голосования участников таким образом, что пул резервных средств будет навсегда заблокирован на умном контракте и их невозможно будет оттуда достать, что может привести к появлению «черной дыры», которая разрушит всю систему. До сих пор способов борьбы с подобными рисками не нашли, однако инцидентов, когда неэффективность достигала таких масштабов, тоже пока не было.

3. Конфиденциальность данных

С одной стороны, PP используют полуанонимные или полностью анонимные записи о данных, которые дополнительно шифруются криптографией. С другой стороны, нарастающее давление со стороны регуляторов и повышающаяся частота взлома криптобирж и криптокошельков приводят к тому, что часть участников криптоиндустрии выбирают для хранения личных данных хранилища вне PP. Помимо этого, возникает вопрос баланса между транспарентностью и приватностью. Остро встает вопрос выбора правильной модели хэширования и криптографической защиты. В ряде применений выбор правильных технологических компонент PP становится вопросом национальной безопасности. Так, к примеру, в российском «Мастерчейне», несмотря на то, что он является инстанцией Ethereum, используются национальные разработки в области криптографии. При этом интересным наблюдением здесь является то, что ряд компаний, наоборот, открывает свои наработки PP, к примеру, используя открытые коды для умных контрактов и других частей PP, а также расширяя сеть с одной

[48] См., к примеру: https://hackernoon.com/artificial-intelligence-blockchain-passive-income-forever-edad8c27844e или https://www.nytimes.com/2018/10/20/technology/how-the-blockchain-could-break-big-techs-hold-on-ai.html.

компании на всю индустрию. Хорошим кейсом здесь может быть DeBeers и Tracr, упомянутые ранее в данном отчете.

4. Безопасность

В связи с участившимся количеством взломов и утечек данных с PP и из компаний внутри экосистемы криптоиндустрии (например, Mt. Gox и ряд взломов других криптобирж) остро встает вопрос безопасности. При этом, в связи со спецификой пользовательского интерфейса, отдельным блоком стоят вопросы, связанные с выпуском, отзывом и восстановлением ключей, в том числе утерянных или попавших в публичное пространство.
Другим отдельным блоком стоят вопросы, связанные с безопасностью PP и проектов на их основе. Так, достаточно часто даже в крупнейших PP находят ошибки в коде. В 2018 году в PP биткоина была найдена опечатка, позволявшая участникам эмитировать более 21 млн биткоинов. Помимо этого, показательным здесь может быть пример The DAO Ethereum, взлом которого привел к расколу системы на два PP: Ethereum и Ethereum Classic.

КЕЙС 3. The DAO

The DAO была автономной децентрализованной организацией, запущенной на сети Ethereum в 2016 году. ДАО представляла собой форму венчурного капитала, где инвестиции приходили от пользователей системы. Целью DAO было предоставить новый способ организации децентрализованных бизнес-моделей для коммерческих и некоммерческих организаций. ICO организации был одним из самых масштабных и успешных: объем привлеченных средств составил более $100 млн в терминах ETH. При этом структура контрольных пакетов была высоко диверсифицирована: крупнейший инвестор имел менее 4% всех токенов DAO, а топ-100 — чуть более 46%. К 21 мая 2016 года под управлением DAO находилось около 14% всех эмитированных к тому моменту токенов ETH общей стоимостью более $150 млн от более чем 11 тыс. инвесторов.

В мае 2016 года вышла статья, упоминающая ряд технических проблем в коде организации, однако разработчики оперативно исправляли данные проблемы, включая рекурсивные вызовы — ситуацию, когда одна и та же команда исполняется большое количество раз. 17 июня 2016 года The DAO был атакован по ряду проблем, включая рекурсивные вызовы. Пользователь, совершивший атаку, получил доступ почти к трети всех токенов, находящихся во владении организации к тому моменту, однако данные средства были заморожены на счете по правилам Ethereum. Чтобы решить данную проблему и вернуть средства изначальным владельцам, сообщество пользователей решило совершить жесткий форк сети, в результате которого произошел сплит системы и образовался Ethereum Classic. В конце 2016 года токены The DAO были делистены со всех бирж. 25 июля 2017 года американский регулятор SEC выпустил отчет, в котором пришел к выводу, что токены DAO, размещенные с помощью ICO на Ethereum, считались ценными бумагами. Это породило глобальную волну регулирования криптоиндустрии.

5. Масштабируемость

Как было упомянуто выше, скорость проведения транзакций в публичных неконтролируемых PP намного ниже, чем в частных, консорциумных и контролируемых, в силу специфики механизмов консенсуса. Несмотря на то, что был предложен ряд альтернативных механизмов и подходов (в том числе шардинг и сайдчейны), их применимость на практике остается под вопросом в силу того, что они еще не внедрены в существующие PP. При этом текущие системы стремятся к централизации (например, в системе биткоина большая часть вычислительных мощностей

контролируется двумя людьми) в силу требований к техническим характеристикам. Хорошим примером здесь является кейс проекта криптокотиков на Ethereum, которые привели к потреблению более 20% вычислительных мощностей сети и значительным задержкам транзакций.

КЕЙС 4. Криптокотики и Ethereum

В октябре 2017 года Axiom Zen продемонстрировал тестовую версию децентрализованного приложения для Ethereum, которое было игрой и называлось CryptoKitties на хакатоне ETH Waterloo. Пользователи получали возможность купить виртуального кота, которого они могли продать другим пользователям, скрестить за плату с другим криптокотом и получить новых котят или скрестить за вознаграждение с другим криптокотом и отдать котят. Генетический код (256-битный геном) каждого криптокотика уникален и определяет внешние черты, которые передавались котятам, включая окрас, форму рта, шерсть, цвет и форму глаз, цвет заливки фона и акцентов, цвет обводок и случайные характеристики.

К декабрю 2017 года игра стала вирусной. 2 декабря 2017 года первый криптокотик, Genesis, стоил 246,9255 ETH, или по курсу того времени около $117 712. Пользователи игры активно торговали и повышали количество газа, который они были готовы отдать за процессинг связанных транзакций, до таких значений, что около 20% транзакций сети Ethereum приходилось исключительно на игру. В результате сеть Ethereum начала значительно замедляться и появились первые вопросы относительно масштабируемости данного PP.

6. Скорость изменений публичных PP

Отдельным вызовом является повышающийся риск раскола систем в связи с увеличением количества и неоднородности участников. При этом, чем дальше идет развитие технологий в криптоиндустрии и чем больше упрощается процесс создания инстанций/чем больше экспертов в данной области появляется, тем более мелкие нужны изменения, чтобы вызвать раскол системы. Как упоминалось ранее, у блокчейна биткоина более 100 форков. У более молодых, но тоже популярных PP также присутствуют как минимум десятки, а то и больше форков. Показательным кейсом здесь может быть первый сплит в результате жесткого форка биткоина, приведший к появлению Bitcoin Cash.

КЕЙС 5. Размер блока и Bitcoin Cash

В середине 2017 года группа разработчиков и пользователей биткоина предложила увеличить размер блока как ответ на увеличение комиссий за проведение транзакций. 1 августа 2017 года был предложен жесткий форк системы, внедряющий данные изменения. В результате форка система раскололась на две и привела к созданию Bitcoin Cash.

Тренды развития криптоиндустрии на 2019 год и далее

На текущий момент можно выделить три группы трендов[49], связанных с развитием технологии PP и криптоиндустрией в целом.

1. *Предложения токенов (ICO, STO и др.)*

Разделение между ICO и предложением акций становится менее явным. Все больше проектов воспринимают ICO не как инструмент размещения токенов услуг, а как инструмент финансирования собственной деятельности, связанной с криптоиндустрией. Одновременный рост количества мошеннических проектов вызывает ответную реакцию регулятора и ведет к ужесточению его позиции относительно ICO и предложений токенов.
Усиление активности регуляторов. Как было проанализировано и отмечено в первой части серии исследований, глобальная активность регуляторов повышается. При этом инициативы рознятся от внедрения базовых правил AML, CFT и KYC до лицензирования и внедрения государственных криптоинициатив.

2. *Активность фондов*

Ключевые фонды VC переходят из фондирования проектов, связанных с PP, на инвестиции в токены. Данный тренд увеличивает количество доступных средств в криптоиндустрии, а также уверенность неинституциональных участников, что ведет к росту активности.
STO предоставляют интерес для инвесторов, в том числе институциональных. STO, предлагающее долевое участие в компании, ближе к стандартным методам институционального финансирования компаний, поэтому предоставляет новую бизнес-возможность для фондов.
Перефинансирование компаний. Компании, проведшие ICO, оказались на раннем этапе своего развития с несопоставимо большим количеством средств. Несмотря на то что большая часть проектов оказалась мошенническими и закрылась, подобные ресурсы могут позволить добросовестным проектам совершить фундаментальный скачок в развитии инноваций.

3. *Активность бизнеса*

Упоминание PP увеличивает финансовые показатели. Даже без реальных действий PP увеличивает финансовые показатели торгуемых компаний, что обращает их интерес к инициативам, связанным с технологией.
Увеличение корпоративных инвестиций и партнерств. Количество новых применений PP растет ежегодно. Часть из этих применений вышли из стадии тестирования и уже приносят первые результаты (например Tracr).
Несмотря на развитие применений PP, остаются вопросы к готовности самой технологии. Как было отмечено ранее, технологические элементы PP не все готовы к полномасштабному использованию в криптоиндустрии. Несмотря на то, что количество их применений растет, вопрос о готовности технологии будет становиться с каждым годом все острее, если доминирование первых систем продолжится (например криптокотики и Ethereum).

[49] Данные тренды основаны на исследовании CB Insights и адаптированы под данный анализ. Доступно онлайн: https://www.cbinsights.com/research/blockchain-future-trends/.

Сценарии технологического развития криптоиндустрии

Исходя из ключевых неопределенностей в криптоиндустрии и трендов развития, можно выявить ключевые сценарии технологического развития криптоиндустрии на ближайшие годы. Данный подход основан на исследовании «Безналичная экономика в России — 2030: сценарии для рынка и отрасли» Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО[50] и использует результаты, полученные в рамках более широкого анализа для криптоиндустрии. Сценарии безналичной экономики основаны на двух ключевых неопределенностях относительно структуры внешней среды и поведения участников. Адаптируя данные неопределенности для криптоиндустрии, можно получить следующую рамку для сценарного планирования на горизонте до 2030 года.

Ось «Структура внешней среды»

Неготовность технологии — Готовность технологии

Исходя из ключевых технологических вызовов и трендов в криптоиндустрии, основной неопределенностью является готовность технологий для масштабного коммерческого и некоммерческого использования PP. С одной стороны, появляются реальные примеры использования PP с осязаемыми выгодами для разных участников экосистем проектов, а также растет активность и размер инфраструктуры, связанной с криптоиндустрией. С другой стороны, масштабные применения сопровождались рядом проблем, начиная от снижения скорости транзакций, заканчивая вопросами безопасности, совместимости различных PP и т.д.

Ось «Поведение участников»

Неготовность участников — Готовность участников

Текущие тренды в криптоиндустрии указывают на двойственную позицию различных участников. С одной стороны, ряд бизнесов и даже государств выражают готовность создавать проекты на основе PP. С другой, регулирование и крупные коммерческие компании, в том числе большие технологические компании, пока не готовы к использованию децентрализованных механизмов для обновления бизнес-моделей и создания инноваций. При этом данная тенденция отмечается как в России, где, к примеру, крупнейшие банки заявляют о том, что не планируют использовать технологию PP в ближайшие годы, так и в мире, где американские GAFA и китайские BAT до сих пор остаются в стороне.

В результате соединения данных осей получается четыре ключевых сценария развития

[50] Доступно онлайн: https://finance.skolkovo.ru/ru/sfice/research-reports/1208-2017-06-05/.

криптоиндустрии.

Сценарий 1. Расцвет реестров. Готовность технологии — готовность участников

В данном сценарии и участники, и технологии готовы к полномасштабному полноценному запуску проектов, связанных с криптоиндустрией. Основные проблемы, связанные с технологической составляющей, быстро решаются сообществом разработчиков. В данном сценарии могут преобладать как децентрализованные, так и централизованные структуры, однако благодаря выгодам PP их работа более эффективна, чем у традиционных участников экономики. PP становятся ключевой инфраструктурой и, возможно, постепенно заменяют традиционную инфраструктуру.

Сценарий 2. Ненужные реестры. Готовность технологии — неготовность участников

В данном сценарии технологии готовы, однако участники не хотят полномасштабного полноценного запуска проектов, связанных с криптоиндустрией. В результате создается масштабная инфраструктура, которая в потенциале могла бы быть использована для трансформации индустрий, однако она не востребована и не используется участниками экономики в полной мере. В данном сценарии возможны только инкрементальные инновации.

Сценарий 3. Провальные реестры. Неготовность технологии — готовность участников

Данный сценарий подразумевает использование участниками неготовых технологий, что приводит к применению технологий, которые в задумке и проекте выглядят воодушевляющими и инновационными, однако на деле их выполнение не представляется возможным. В результате большое количество проектов и инициатив, связанных с PP, проваливается и криптоиндустрия приобретает негативный имидж.

Сценарий 4. Невидимые реестры. Неготовность технологии — неготовность участников

В данном сценарии ни участники, ни реестры не готовы к развитию криптоиндустрии, по причине чего распределенные реестры даже если и развиваются, то только в ограниченных нишевых сообществах, которые не видны основным участникам экономики. РР не становятся ключевым элементом инфраструктуры.

Заключение

Первые применения PP в области криптовалют, децентрализованных приложений и организаций не только привлекли обширное внимание как со стороны сторонников криптоиндустрии, так и со стороны критиков, но и продемонстрировали ряд проблем, связанных с нынешней инфраструктурой. Использование PP мотивируется набором выгод, особенно в области транспарентности, автономности и неизменности хранящихся данных и записей, однако получение данных выгод критическим образом зависит от корректного применения PP под контекст конкретных задач пользователя. Существующие подходы к выбору PP в большинстве отталкиваются лишь от наиболее популярных и уже предложенных PP, игнорируя потенциал развития PP и возможности создания собственных инфраструктурных проектов с нуля. При подобном подходе может падать мотивация создавать новые PP, а доминирование существующих предложений, которые часто бывают не готовы к полномасштабному использованию, будет лишь укрепляться.

Осознавая необходимость комплексного подхода к ответу на возрастающие технологические вызовы в криптоиндустрии и основываясь на фундаментальном исследовании как существующих предложений PP, так и находящихся в разработке или гипотетических применений, исходя из технологических элементов PP, Центр финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО создал данное исследование. Отчет предлагает новую модель классификации типов PP исходя из технологических и стратегических характеристик, выбор которых может повлиять на состав технологических элементов разрабатываемого распределенного реестра. Данная классификация основана как на технологической экосистеме и составляющих PP, так и на текущих технологических тенденциях и гипотетических эффектах от развития криптоиндустрии. Стратегический анализ каждого из типов PP, а также текущих предложений PP на рынке может позволить участникам, рассматривающим создание новых или использование существующих технологий, принимать более осознанные решения, тем самым развивая криптоиндустрию и максимизируя собственные выгоды от участия в ней. Более того, отталкиваясь от разработанной типологии PP, исследование предлагает взгляд на стратегии участников криптоиндустрии, в том числе создателей реестров, а также взгляд на будущее данной индустрии. Данный отчет является частью инициативы Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО в области финансовых инноваций и в частности криптоиндустрии.

Одна из ключевых неопределенностей в криптоиндустрии касается готовности технологий. Более 2/3 уникальных PP — это PP 21-го типа (публичные, неконтролируемые, универсальные и подрывные), а сети биткоина и Ethereum насчитывают абсолютное большинство инстанций и связанных с ними применений. При этом данные PP не являются наиболее подходящими для всех применений, которые внедряются с их помощью. К примеру, для децентрализованных приложений и ICO более подходящим инфраструктурным решением может быть использование нишевых неконтролируемых публичных PP 23-го или 24-го типа, а для ДАО полезным может также оказаться частный PP 7-го типа, примеров которых до сих пор не существует. Для ЦВЦБ, потенциал и текущее состояние которых подробно проанализированы в прошлом отчете данной

серии, одним из наиболее подходящих РР может быть частный РР 1-го типа, пример которого существует, хоть и не используется так же часто, как РР 21-го типа. При этом РР не обязательно должны иметь подрывной характер: ряд применений и инфраструктурных решений могут быть поддерживающими по отношению к существующим процессам и бизнес-моделям. В целом, потенциальные применения РР не ограничены лишь существующим спектром инфраструктурных решений, однако для качественного рывка в развитии участникам криптоэкономики необходимо изменить стратегию следования за лидерами во всех потенциальных использованиях РР и рассмотреть возможные альтернативы.

У технологии РР есть перспектива стать основой для фундаментального скачка в развитии цифровой экономики как в России, так и в мире, но для этого необходимо, чтобы и технология, и участники экосистемы были готовы к ее полномасштабному использованию. В данном случае может наступить «расцвет реестров», когда данная технология станет сквозной и будет использоваться либо вместе, либо иногда даже вместо существующих инфраструктурных предложений. В контексте программы «Цифровая экономика Российской Федерации», где технология РР является одной из девяти сквозных, необходимых для внедрения во все сферы экономики, а также текущих трендов цифровизации[51] это подразумевает использование корректных типов РР и развития технологии до необходимого уровня. В противном случае при неготовности технологий есть вероятность, что большая часть инициатив, посвященных применению РР, будут провальными. Однако необходимо отметить, что готовой должна быть не только технология, но и участники экосистемы криптоиндустрии. Без их готовности внедрение РР может быть просто формальностью, а потенциал технологии не будет раскрыт в полной мере.

Для качественной подготовки участников экосистемы криптоиндустрии важную роль играют не только самостоятельные исследования в данной области, но также и образовательные программы, посвященные отдельным направлениям цифровой трансформации как бизнеса, так и экономики в целом, а также более узконаправленным программам, связанным с РР и криптоиндустрией. Роль подобных инициатив важна и в повышении осознанности создания и использования РР. Как было описано в разделе 5, без осознанного взгляда на процесс создания новых инфраструктурных проектов в криптоиндустрии есть вероятность попадания в одно из наиболее распространенных когнитивных и поведенческих смещений. Для выбора корректных стратегий необходимо учитывать подобные риски и пытаться их минимизировать, стремясь к финансовой и, в частности, криптоосознанности.

Несмотря на то, что серия отчетов Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО, посвященная криптоиндустрии, покрывает ряд ключевых вызовов криптоиндустрии, в том числе регуляторные и технологические, такие как риски конфиденциальности данных, управления на РР, безопасности, масштабируемости и скорости изменений отдельных РР, необходимо понимать, что диалог о развитии криптоиндустрии — это динамичный процесс, который требует постоянной переоценки собственных стратегий, позиций и подходов. Для того чтобы криптоиндустрия стала одним из ключевых элементов цифровой экономики и, возможно, основой более широкой концепции криптоэкономики, участникам экосистемы необходимо ответить на вопросы касательно как технологической готовности, так и стратегических приоритетов. Помимо прочего, необходимо определить мотивацию и собственную позицию относительно криптоиндустрии, а также возможности для обеспечения интеграции между существующей экономикой и криптоиндустрией. Несмотря на то, что ряд первоначальных выгод развития технологий РР и их

[51] См. исследование «Индекс Цифровая Россия» Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО, представляющее результаты количественной оценки прогресса цифровой трансформации российских субъектов федерации и анализа основных трендов, связанных с развитием цифровой экономики. Доступно онлайн: https://finance.skolkovo.ru/ru/sfice/research-reports/1779-2018-10-15/.

применений уже описан, потенциал развития криптоиндустрии может быть намного больше. В том числе интересными могут быть вопросы изменения принципов экономического взаимодействия между участниками, а также эффект внедрения технологии на бизнес-модели и процессы в различных индустриях. Несмотря на то, что первые попытки подобной аналитики уже предпринимаются, необходимо переосмыслить потенциал технологии, в том числе исходя не из текущих предложений, а из возможных тенденций и новых инфраструктурных проектов. Предложенная типология может быть первым шагом к созданию фундамента для рывка в развитии как криптоиндустрии, так и экономики в целом.

Методологический комментарий

Стратегия выбора РР

РР считались уникальными и оригинальными и попадали в список из 21 основных РР, если:

1) в открытых источниках было упоминание о данном РР;
2) из описания проекта (например, white paper, сайт проекта, информация из открытых источников) достаточно информации о технологической составляющей для формирования стратегического профиля РР;
3) РР не является инстанцией (производной) от другого существующего РР, а построен с нуля.

Приоритетной информацией считалась информация из официальных источников проекта (white paper и сайт проекта). Открытые источники использовались в качестве дополнительных материалов.

В список РР не включен ряд упомянутых в основном тексте исследования РР по причине того, что они не отличаются значительным образом от других, уже проанализированных ранее в данном исследовании РР. Этот критерий не является оценкой проектов и не предлагает рекомендации об инвестировании или ином взаимодействии с данными проектами.

Ключевые и второстепенные идентификаторы

Ключевые идентификаторы — это те критерии выбора РР, что в большей степени влияют на технологическую архитектуру РР. Второстепенные классификаторы влияют лишь на некоторые элементы технологических составляющих РР и по данной причине не вошли в ранг ключевых. Также ключевые идентификаторы — это те критерии, о которых чаще всего упоминается в аналитике, посвященной криптоиндустрии.

Профили 24 типов РР

В профиль 24 ключевых типов РР включена следующая информация:

1. Словесное описание характеристик РР .
1. Количественная оценка ключевых характеристик РР.
2. Наиболее подходящее применение.
3. Наименее подходящее применение.
4. Примеры РР (при наличии).
5. SWOT-анализ.
6. Потенциальные пользователи РР.
7. Основные проблемы и рекомендации к их устранению.
8. Наиболее подходящие сценарии безналичной экономики — 2030.

Данный набор информации позволяет комплексно оценить профиль РР для принятия первоначального решения относительно потенциала его использования. В приложениях

последняя Р в аббревиатурах обозначает подрывной (разрушающий) характер РР.

Количественная оценка ключевых характеристик РР

Количественная оценка выставлялась исходя из гипотетического анализа набора технологических элементов, включенных в РР, из выбора по четырем основным классификаторам типов РР. Каждый из классификаторов мог увеличить (+1), не повлиять (0) или уменьшить/ухудшить (-1) характеристику. Результирующее значение в таблице — это сумма баллов по всем критериям РР. Набор характеристик сформирован исходя из ключевых эффектов и текущих вызовов РР.

Автономность определяется наличием и составом умных контрактов. Набор умных контрактов в большей степени определяется структурой управления РР. Нишевый характер может облегчить написание умных контрактов, так как на моменте дизайна проекта понятны потенциальные применения РР.

Транспарентность — это возможность для внешних участников системы просматривать записи в РР хотя бы в анонимном или полуанонимном формате. Частные РР — наиболее закрытые системы, в то время как консорциумные РР чаще публикуют о себе информацию, а открытые и вовсе обладают механизмами просмотра записей на РР. Неконтролируемые РР подразумевают равнозначных участников и невозможность несанкционированного изменения записей, что повышает прозрачность процессов в РР. Нишевые РР обычно вовлекают меньшее количество участников, в силу чего просмотр их активности может быть проще.

Неизменность отражает сложность несанкционированного изменения данных. Благодаря большему количеству участников в консорциумных и публичных РР несанкционированное изменение данных может быть сложнее. Контролируемый характер напрямую подразумевает возможность самовольного изменения данных контролером/управляющим. В универсальных РР благодаря большему количеству участников одному участнику сложнее изменить данные. Применение поддерживающих РР реже подразумевает необходимость махинаций с данными.

Скорость — это скорость проведения транзакций в РР при учете стандартных существующих характеристик РР. Чем больше размер сети, тем ниже скорость. В неконтролируемых РР есть необходимость внедрения более сложного протокола консенсуса, требующего времени на верификацию транзакций. Нишевые РР имеют конкретные применения и поэтому могут быть быстрее. Универсальные РР менее кастомизированы под определенные цели проектов. Применение поддерживающих РР часто подразумевает эффективность с точки зрения скорости.

Кастомизация — это возможность настройки характеристик РР под нужды проекта. Чем больше размер сети, тем ниже возможность учета индивидуальных необходимостей проектов. В неконтролируемых РР есть необходимость внедрения более сложного протокола консенсуса, требующего стандартизации процессов. Нишевые РР имеют конкретные применения и поэтому могут быть легче кастомизированы. Универсальные РР менее кастомизированы под определенные цели проектов. Применение поддерживающих РР часто подразумевает эффективность с точки зрения кастомизации.

Устранение необходимости доверия — это уровень доверия, который участникам необходимо возлагать на других участников РР. Частные РР — наиболее закрытые системы, в то время как консорциумные РР чаще публикуют о себе информацию, а открытые и вовсе обладают механизмами просмотра записей на РР. Неконтролируемые РР подразумевают равнозначных участников и невозможность несанкционированного изменения записей, а также автоматизацию процессов. Исходя из применений, подрывные РР пользуются большим уровнем доверия в современной криптоиндустрии.

Классификатор	Автономность	Транспарентность	Неизменность	Скорость	Кастомизация	Устранение необходимости доверия
Архитектура						
Частный	0	-1	0	1	1	-1
Консорциумный	0	0	1	0	0	0
Публичный	0	1	1	-1	-1	1
Управление						
Контролируемый	-1	-1	-1	1	1	-1
Неконтролируемый	1	1	1	-1	-1	1
Универсальность						
Нишевый	1	1	0	1	1	0
Универсальный	0	0	1	-1	-1	0
Подрывной потенциал						
Подрывной	0	0	0	0	0	1
Поддерживающий	0	0	1	1	0	0

Наиболее и наименее подходящие применения

Наиболее подходящие применения — это гипотетические и/или реальные применения конкретных типов РР, где по информации из открытых источников и результатам анализа авторов эффект может быть наибольшим, исходя из набора технологических характеристик и элементов, которые содержатся в среднем РР данной категории. Наименее подходящие применения выбраны из списка наиболее подходящих применений РР с наименее похожим (максимально противоположным) набором технологических характеристик.

Соответствие сценариям безналичной экономики — 2030

Соответствие сценариям безналичной экономики — 2030 — это соответствие наиболее подходящих применений РР трендам и характеристикам сценариев безналичной экономики — 2030 из проекта «Безналичная экономика в России — 2030: сценарии для рынка и отрасли» Центра финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО[52]. Подробное описание сценариев представлено в исследовании.

В целом, данный анализ призван дать начальное представление об эффектах среднего РР каждой из групп. Финальная оценка РР должна строиться на основе информации о конкретных проектах.

[52] Доступны онлайн: https://finance.skolkovo.ru/ru/sfice/research-reports/1208-2017-06-05/.

ПРИЛОЖЕНИЯ

Приложение 1. Анализ 21 уникального PP

Отдельная таблица, доступна онлайн:
https://finance.skolkovo.ru/downloads/documents/FinChair/Research_Reports/SKOLKOVO_2018_12_Cripto-annex_001.pdf

Приложение 2. Профили 24 типов PP

Отдельный документ, доступен онлайн:
https://finance.skolkovo.ru/downloads/documents/FinChair/Research_Reports/SKOLKOVO_2018_12_Cripto-annex_002.pdf

Приложение 3. Сводная таблица анализа 24 типов PP

Отдельная таблица, доступна онлайн:
https://finance.skolkovo.ru/downloads/documents/FinChair/Research_Reports/SKOLKOVO_2018_12_Cripto-annex_003.pdf

SKOLKOVO
Moscow School of Management

Московская школа управления СКОЛКОВО — одна из ведущих частных бизнес-школ России и СНГ, основанная в 2006 году по инициативе делового сообщества.

Образовательные программы Московской школы управления СКОЛКОВО ориентированы на все стадии развития бизнеса — от стартапа до крупной корпорации, выходящей на международные рынки. Программы построены по принципу «обучение через действие» и включают в себя теоретические блоки, практические задания, проектную работу и международные модули.

Московская школа управления СКОЛКОВО также является центром экспертизы и притяжения для тех, кто делает ставку на Россию и работу на рынках с быстро меняющейся экономикой.

Центр финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО создан с целью построения независимого российского центра компетенции в вопросах финансовых инноваций и безналичной экономики.

Повестка работы Центра определена в трех областях: проведение профильных исследований, разработка образовательных программ и создание институциональных партнерств. Результаты исследований публикуются в академических источниках, а также используются в национальных программах развития.

Московская школа управления СКОЛКОВО 143025,
Россия, Московская область Одинцовский район
дер. Сколково, ул. Новая, 100
тел.: +7 495 539 30 03
факс: +7 495 994 46 68
E-mail: info@skolkovo.ru
Website: www.skolkovo.ru