ДЕЦЕНТРАЛИЗОВАННЫЕ РЕЕСТРЫ В ТОРГОВЛЕ И ПРОМЫШЛЕННОСТИ: ПРОБЛЕМАТИКА

МИХАИЛ ЧЕКАНОВ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР КБ «КОНТРАКТ»

За последние пару лет мы реализовали несколько проектов для корпоративных и государственных заказчиков на базе блокчейн-технологий, и в этом курсе я постараюсь рассказать о возможностях и ограничениях применения этой технологии в бизнесе.

О ТЕКУЩЕЙ СИТУАЦИИ НА РЫНКЕ

Текущая ситуация на рынке прекрасно иллюстрируется кривой Гартнера — кривой зрелости любой новой технологии.

Сейчас все дружно и задорно летят с пика ожиданий в ущелье разочарования. Тому есть масса причин, но основной, на мой взгляд, является эта — первое поколение блокчейн-проектов оказалось неприменимым в бизнесе вследствие ряда принципиальных проблем, даже, можно сказать, барьеров для внедрения бизнеса.

ПОЧЕМУ ТАК ПРОИЗОШЛО?

Во-первых, речь идет о пресловутой анонимности, точнее — псевдонимности участников блокчейн-сети, которая ведет к разрушению существующей системы борьбы с отмыванием денег. Более того, если мы говорим о B2B-рынке, то, как правило, мы хотим точно знать, кто на самом деле является нашим контрагентом.

Как следствие, для того чтобы использовать технологию в бизнесе, нам необходимо иметь возможность достоверной аутентификации и авторизации контрагентов. Наиболее очевидным и логичным подходом выглядит использование уже существующей и хорошо знакомой бизнесу инфраструктуры электронной подписи, которая выдается удостоверяющими центрами.

Но есть одно но. Использование удостоверяющих центров закрывает возможность свободного подключения к сети. Поэтому, в принципе, все сети делятся на публичные, доступ к которым не контролируется, и частные (закрытые). Криптоанархисты и шифропанки считают последние ненастоящими блокчейнами. Эта дискуссия имеет идеологический характер, и мы не будем в нее углубляться.

Во вторых, данные о транзакциях в публичных блокчейнах по умолчанию общедоступны. Что, якобы, дает возможность аудита транзакций в любой момент времени каждому желающему.

Но хочет ли этого бизнес на самом деле? Чтобы, к примеру, информация о транзакциях компании была доступна конкурентам? Очевидно, что нет — бизнес, наоборот, заинтересован в сохранении коммерческой тайны.

Это означает что нам необходимы механизмы управления доступом к данным, желательно с использованием ролевой модели или хотя бы на уровне организации. Проще говоря, чтобы доступ к данным и аудит истории транзакций был возможен только в границах определенных полномочий, которые зависят от роли участника сети в том или ином бизнес-процессе.

РЕЗЮМЕ

1. Безопасность
2. Масштабируемость и производительность

Если все пользователи сети авторизованы и доступ к данным ограничен рамками бизнес-процессов, то сразу же теряют смысл как криптовалюты, так и их майнинг. Криптовалюты изначально являются средством мотивации участников к подключению и обработке транзакций других пользователей. Но если каждый участник хранит и обрабатывает только те данные, в которых он заинтересован, то это уже по определению является необходимой и достаточной для него мотивацией, чтобы инвестировать в развертывание и эксплуатацию блокчейн-сети.

Что касается проблемы производительности, то смартконтракты в Эфириуме, например, выполняются всеми узлами сети, и в итоге производительность сети равна производительности телефона начала века

3. Стоимость владения

В первом поколении публичных блокчейнов каждый участник, как правило, должен хранить данные о транзакциях всех участников сети. Как следствие, стоимость владения увеличивается в геометрической прогрессии по мере роста сети. Собственно, именно поэтому большинство обычных, казуальных пользователей популярных публичных блокчейнов пользуются веб-сервисами для доступа к сети

Немаловажным является готовность решения к эксплуатации в корпоративном ИТ-ландшафте, его зрелость с точки зрения документации, качества и безопасности кода. К сожалению, у большинства публичных проектов с этим есть определенная проблема. Наиболее популярные сети чаще всего хорошо документированы и написаны, но большинство проектов не могут этим похвастаться. Как следствие, мы имеем массу случаев, когда были взломы проектов.