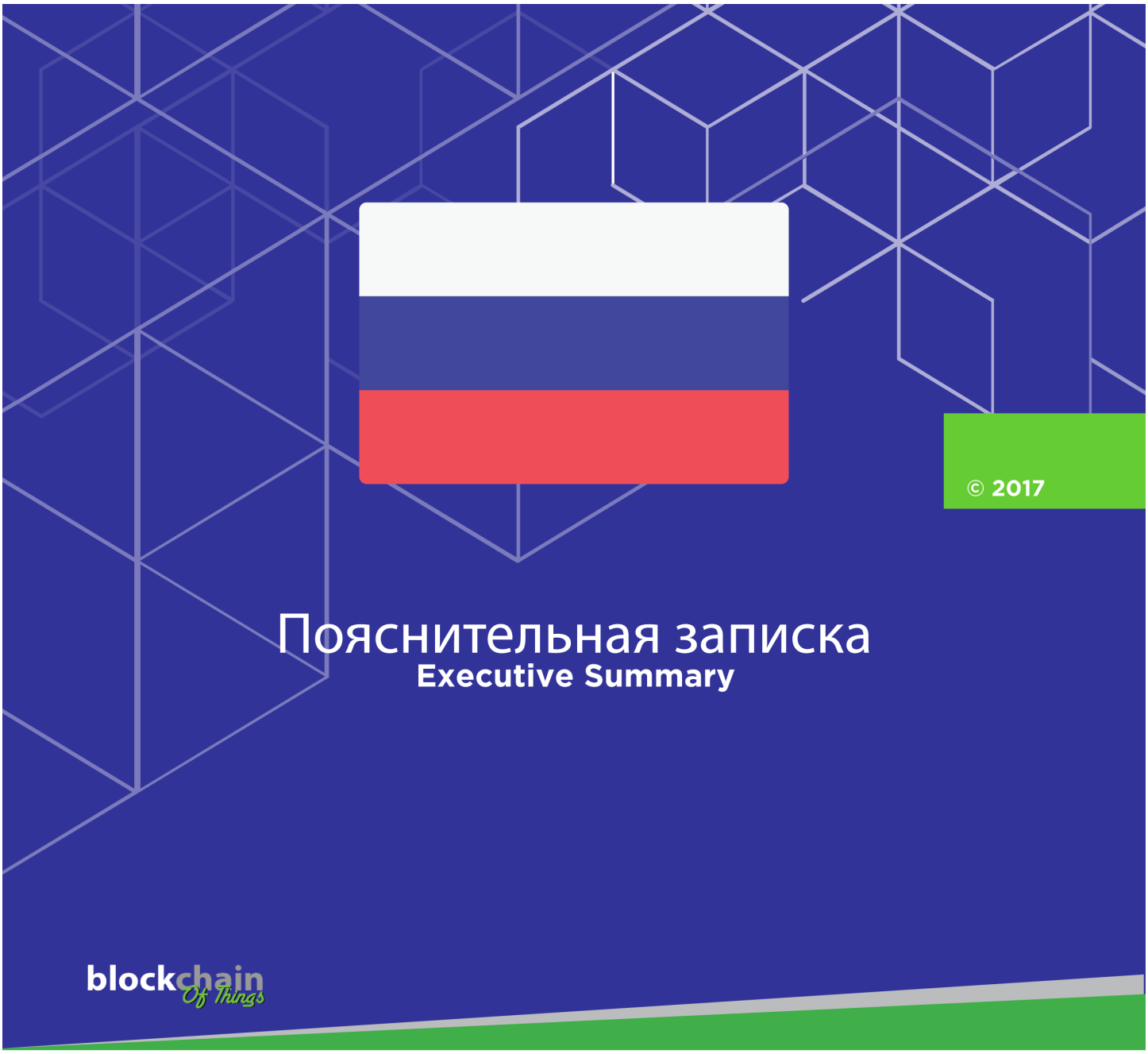

BCOT Global Holdings

Аннотация

Технология Интернета вещей (IoT) небезопасна, и мы планируем это исправить.

Компания Blockchain of Things ставит своей целью решить проблему безопасности технологии Интернета вещей при помощи простого в использовании сервиса Catenis Enterprise, встроенного в блокчейн Bitcoin. Используя подход, основанный на уровне веб-служб, Catenis легко адаптировать для поддержки Ethereum, Hyperledger, и многих других блокчейнов. Catenis (в экспериментальной версии) представляет собой активную сеть с несколькими действующими корпоративными клиентами.

В этом документе мы вначале опишем природу угроз для безопасности IoT и те препятствия, которые они создают для внедрения IoT на предприятии. Затем мы сосредоточимся на тех преимуществах с точки зрения безопасности, которые технология блокчейна имеет перед традиционными инфраструктурами IoT. Далее мы обрисуем препятствия, мешающие организациям использовать сеть Bitcoin для осуществления безопасной связи между устройствами IoT. Мы опишем, как Catenis Enterprise преодолевает эти препятствия, эффективно используя безопасность и надежность блокчейна Bitcoin. Наконец, мы представим концепции надежного подтверждения и интеллектуальных средств, как ключевых атрибутов, которые распространяют функциональность Catenis Enterprise на применения, выходящие за пределы традиционной сферы IoT.

Пояснительная записка

Технология Интернета вещей (IoT) небезопасна, и мы планируем это исправить.

Технология IoT НЕ является безопасной. Спонсированный Bain обзор более чем 500 корпоративных покупателей технологии IoT показывает, что главным препятствием на пути ускорения промышленного внедрения IoT является недостаточная безопасность.[1] Проблемы с безопасностью — традиционный бич для рынка IoT в основном потому, что в настоящее время при организации связи между устройствами IoT упор делается на централизованные серверы. Если говорить конкретнее, то уязвимости IoT делятся на три категории:

- **Атаки с целью вызова отказа в обслуживании (DoS-атаки).** DoS-атака на неопределенный срок прерывает работу критически важных IoT-служб.
- **Хакерский взлом.** К краже данных или к захвату контроля над устройством могут привести разнообразные методы взлома, такие как имитация соединения, «незаконный посредник» или захват устройства.
- **Недостаточная контролируемость.** Недостаточная контролируемость означает, что администраторы сети могут не знать о произошедшем вторжении в течение месяцев и даже лет.

Безопасность Bitcoin. Блокчейн Bitcoin, старейшая и наиболее испытанная технология, безоговорочно решает эти проблемы безопасности за счет того, что не имеет никаких уязвимых центральных точек. Сеть Bitcoin доказала свою устойчивость к различным методам взлома и DoS-атакам, демонстрируя в то же время контролируемость, вытекающую из невозможности изменить однажды созданные записи. Таким образом, администратор может надежно контролировать IoT-устройство, привязав его к адресу Bitcoin и используя его блокчейн для пересылки сообщений (например, командных сигналов) по этому адресу.

Catenis преодолевает ограничения блокчейна Bitcoin при использовании Интернета вещей. Несмотря на все преимущества блокчейна Bitcoin в смысле безопасности, у него есть ряд ограничений, не позволяющих использовать его в IoT. Catenis Enterprise преодолевает эти преграды и делает это таким образом, что все преимущества Bitcoin при этом сохраняются. Это становится возможным благодаря встраиванию web-служб Catenis в блокчейн Bitcoin. Для промышленных IoT-приложений ограничения блокчейна Bitcoin и соответствующие функциональности Catenis можно разбить на шесть категорий.

- **Ограничение в 80 байтов.** Поле сообщения в блокчейне Bitcoin ограничено 80 байтами, что не дает возможности отправлять IoT-устройствам большие объемы необходимых данных. Catenis решает эту проблему, снимая ограничение на объем передаваемых данных — программного кода или файлов данных любого типа и размера.

- **Нехватка управления доступом.** Если IoT-устройство подключено к адресу Bitcoin, неавторизованные узлы сети могут активировать устройство, поскольку сообщения на его адрес может посылать кто угодно. Catenis решает эту проблему путем создания сети с контролем доступа, встроенной в публичный блокчейн Bitcoin.
- **Нехватка шифрования.** Сообщения, пересылаемые через блокчейн Bitcoin, полностью открыты, поскольку не зашифрованы. Catenis решает эту проблему реализацией сквозного шифрования. Но на этом меры по обеспечению безопасности не кончаются. Catenis автоматически использует новый Bitcoin-адрес для IoT-устройства всякий раз, когда система отправляет сообщение этому устройству. Таким образом, любое сообщение, отправленное по прежнему адресу, не дойдет до устройства. Это обеспечивает так называемую «совершенную прямую секретность» (Perfect Forward Secrecy)[2], поскольку сообщения передаются по одноразовым туннелям, которые существуют лишь мгновение. Это не позволяет неавторизованным узлам выявлять путем анализа связанные сообщения.
- **Проблемы скорости и масштабирования.** Время подтверждения в Bitcoin велико, а проблемы с масштабированием хорошо известны. Catenis решает эту проблему, работая в качестве надстройки над сетью Lightning Network[3], которая позволяет выполнять быстрые и масштабируемые транзакции. Однако в отличие от Lightning Network мы можем работать без «контрагентского риска», поскольку Catenis является доверенной сетью.
- **Трудности при использовании техническими руководителями.** Блокчейн Bitcoin труден в использовании, поскольку большинство ИТ-персонала не знакомо с протоколами блокчейна. Catenis решает эту проблему созданием надстройки из web-служб и простого в использовании API.
- **Трудности при использовании финансовыми руководителями.** Блокчейн Bitcoin труден в использовании для многих финансовых директоров, поскольку не все из них имеют опыт работы с криптовалютами. Catenis решает эту проблему путем выполнения действий, присущих операциям с криптовалютой, в фоновом режиме, благодаря чему операции приобретают привычный для корпоративных клиентов вид валютных операций.

Catens реализует доказательную проверку подлинности. Расширенная функциональность Catenis позволяет использовать приложения, которые находятся вне традиционной сферы IoT, что создает возможность «надежного подтверждения» или «доказательства подлинности». Catenis позволяет проследить подлинность реальных продуктов, что снижает возможность мошенничества в розничных сетях и цепочках поставок на сумму в 1,9 трлн долларов в год.[4] Процесс подтверждения включает следующие два ключевых шага.

- **Подтверждение того, что производитель продукта имеет сертификат подлинности.** Производитель заносит в блокчейн уникальный криптографический идентификатор сертификата подлинности и передает дилеру или покупателю ссылку, которая позволяет при помощи независимого криптографического

подтверждения убедиться в том, что производитель является владельцем сертификата подлинности.

- **Подтверждение подлинности сертификата.** Catenis позволяет продемонстрировать независимую криптографическую верификацию удостоверения. Владелец данной конечной точки может подтвердить свою личность, продемонстрировав доступ или права собственности в отношении соответствующего веб-домена, государственной регистрации или стороннего сертификата. Сочетание этих двух шагов дает возможность доказать подлинность в условиях отсутствия доверия, а это ограничивает возможности мошенничества как в цепочке поставок, так и в розничной сети.

Catenis реализует настраиваемые «интеллектуальные активы». Далее возможности Catenis выходят за пределы традиционной сферы Интернета вещей и позволяют клиентам перевести больше вещей в цифровое поле. Эта цель достигается путем предоставления клиентам возможности создавать «интеллектуальные активы» и передавать их от одного пользователя другому. Интеллектуальные активы Catenis (smart-assets) обладают всеми основными возможностями «протокола цветных монет» (Colored Coin Protocol)[5], но обладают также и другими возможностями в четырех основных аспектах:

- **Возможность доставлять фактическое полезное цифровое содержимое.** Интеллектуальные активы Catenis вкупе с его функциями доставки сообщений позволяют передавать полезную цифровую информацию, чем отличаются от многих других криптопроектов, в которых цифровой актив — просто ссылка на информацию, подкрепленная обещанием третьей стороны передать ее по требованию через стороннюю внешнюю систему. Интеллектуальные активы Catenis могут содержать реальные сертификаты акций, акты передачи прав на недвижимость или MP3-файлы, так, что полезная информация передается напрямую от одного пользователя к другому.
- **Возможность шифрования цифрового содержимого.** Цифровое содержимое, которое переносится интеллектуальными активами Catenis, может быть зашифровано открытым ключом получателя так, что только получатель сможет иметь к ней доступ. Это прямая противоположность другим криптопроектам, где передаваемая информация не шифруется и полностью открыта.
- **Возможность реагировать на сообщения.** Интеллектуальные активы Catenis можно настроить для реагирования на сообщения от других конечных устройств, что отличает их от других криптопроектов, где цифровые активы не вступают во взаимодействия. Например, пользователь Catenis может запрограммировать автоматическое создание и рассылку интеллектуальных активов при получения определенного сообщения. Это позволяет сделать Catenis платформой для эффективного распространения цифровых активов, включая первичное размещение токенов.

- **Контролируемая сеть.** Поскольку Catenis является контролируемой сетью, интеллектуальные активы не реагируют на сообщения от неутвержденных узлов. Это отличается от других криптопроектов, в которых не реализованы функции контроля.

Catenis как платформа для сторонних приложений. Catenis в основе своей — это платформа, на которой сторонние разработчики могут строить свои приложения, пользуясь в качестве строительных блоков базовой функциональностью Catenis (например, безопасная передача сообщений, интеллектуальные активы и т. д.). Рассмотрим четыре направления, в которых сторонний программист может сосредоточить усилия по разработке.

- **Отраслевые приложения для обеспечения безопасности IoT.** В различных отраслях промышленности и сферах деятельности функциональность Catenis в контексте защиты IoT окажется полезной. Так, сторонний разработчик может создать специальное приложение, которое использует возможности Catenis для внедрения специфических решений для разных сегментов рынка IoT.
- **Аппаратное обеспечение как услуга.** Catenis позволяет использовать услугу аппаратного обеспечения на основе технологии блокчейна, поскольку цифровые ключи в форме интеллектуального актива могут включать функциональность удаленного оборудования, подключенного к конечным точкам Catenis. Сторонние разработчики могут создавать отраслевые приложения, использующие эту функциональность различными способами.
- **Рынок билетов.** Catenis позволяет исходному эмитенту интеллектуальных активов взимать комиссию за перепродажу активов (возмездные интеллектуальные активы). Например, эмитент билетов на концерт может получать комиссию, если билеты перепродаются на вторичном рынке. Сторонние разработчики могут коммерциализировать такую возможность, создав площадку для торговли билетами с учетом особенностей интеллектуальных активов на основе служб Catenis.
- **Рынок акций.** Закон штата Делавэр разрешает корпорациям США торговать акциями с использованием блокчейна при расчетах за акции. Catenis уже обладает функциональностью, позволяющей кодировать интеллектуальные активы для передачи фактических сертификатов акций. У Catenis также есть функциональность для операций с криптовалютами, поэтому традиционные инвесторы могут покупать акции через своих брокеров, не имея напрямую дела с криптовалютами. Сторонний разработчик мог бы построить торговую площадку, которая реализовала бы процесс расчетов за акции.