



Нравится

Зарегистрируйтесь, чтобы посмотреть, что нравится друзьям.

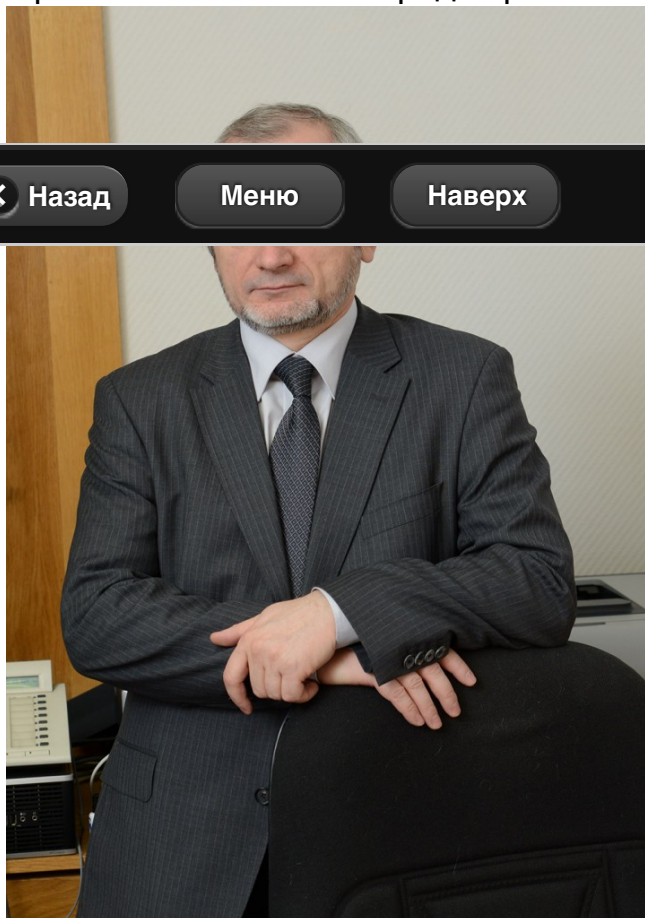


Твитнуть

17.02.2016

Корпоративный блокчейн: за и против. Взгляд эксперта

Сегодня технология блокчейнов (blockchain), изначально реализованная в системе Bitcoin, вызывает все больший интерес участников банковского и платежного рынка с точки зрения использования ее в других проектах, не связанных напрямую с криптовалютами. Портал PLUSworld.ru предложил Валерию Лопатину, к.э.н., старшему научному сотруднику Центра ДКП Института ФЭИ Финансового университета при Правительстве РФ, советнику председателя НП «Национальный совет финансового рынка», оценить перспективность такого рода проектов.



«Технология блокчейнов находит все больше и больше приверженцев.

Появляются и каждый день нам приходят предложения по новым блокчейн – проектам в области регистрации и подтверждения прав, заключения «умных» контрактов, хранения информации и т. д., которые обещают совершить переворот в бизнесе.

Далеко не всегда участники стартапов раскрывают детали проектов, но в некоторых случаях ясно, что с большой вероятностью речь идет о корпоративных блокчейнах, централизованное сопровождение которых будет осуществлять та или иная компания. В частности, это касается банковских стартапов, которые надеются с помощью блокчейнов сократить транзакционные

издержки и повысить эффективность банковского бизнеса.

В то же время корпоративный блокчейн несет в себе больше вопросов, чем ответов, так как источник повышения эффективности бизнеса за счет его использования на настоящий момент не вполне ясен.

Как известно, блокчейн представляет собой последовательность блоков, содержащих транзакции участников системы, в которой каждый последующий блок содержит в себе хэш (результат вычисления хэш-функции) предыдущего блока. Это позволяет легко проверить всю цепочку блоков путем последовательного пересчета хэшей.

Изначально блокчейн создавался как один из элементов системы защиты и подтверждения транзакций в пиринговой сети, когда каждый узел сети имеет доступ ко всем транзакциям, но при этом обеспечивается псевдоанонимность участников транзакций и блокируется возможность узлов вносить изменения в совершенные транзакции. Это достигается криптографической защитой адресов участников транзакций и защитой всего блокчейна сложностью вычисления хэшей блоков транзакций.

Например, в системе Bitcoin получатель включает в состав своего адреса хэш своего открытого ключа, что позволяет ему подтверждать свое право использования средств (на этапе, когда он становится плательщиком) путем включения своего открытого ключа в тело транзакции.

Одновременно для каждого блока транзакций в процессе майнинга осуществляется поиск сложного хэша (имеющего в первых разрядах заданное количество нулей), что практически до нуля снижает возможность перехвата управления блокчейном злоумышленниками. Последнее обстоятельство связано с тем, что поиск сложного хэша осуществляет большое количество майнеров с использованием большого объема вычислительных средств, что ставит перед злоумышленниками неразрешимую задачу концентрации в своих руках вычислительной мощности, сопоставимой с вычислительной мощностью майнеров.

В случае использования корпоративного блокчейна (последовательной цепочки блоков транзакций) вместо классической СУБД (реляционной базы данных с записями о транзакциях), совершенно очевидно следующее.

Во-первых, корпорация не сможет обеспечить защиту блокчейна путем вычисления сложных хэшей, так как не сможет сконцентрировать в своих руках вычислительную мощность, сопоставимую с вычислительной мощностью потенциальных злоумышленников.

Во-вторых, большинство корпораций не заинтересованы в раскрытии информации о транзакциях, в том числе, в случае шифрования адресов

участников транзакций.

Таким образом, для защиты корпоративного блокчейна в любом случае должны использоваться средства безопасности, аналогичные средствам защиты СУБД (включая средства ограничения доступа), в том числе, в случае применения защиты с помощью вычисления сложных хэшей.

При этом использование блокчейна может несколько повысить расходы на обработку транзакций, так как поиск и сортировку транзакций в условиях блокчейна (например, для подготовки отчетов по счетам клиентов) осуществить может оказаться сложнее, чем в случае реляционной СУБД.

Таким образом, на вопрос «можно ли повысить эффективность бизнеса за счет использования корпоративного блокчейна» можно ответить, что вероятность такого эффекта сомнительна.

Совсем другой ответ будет в случае использования корпоративного сайдчейна (sidechain) к хорошо защищенному публичному блокчейну. В этом случае преимущества сайдчейна вполне могут повлиять на эффективность бизнеса. Но об этом я предлагаю поговорить в следующий раз».

По материалам PLUSworld.ru

