УДК **681.3.067**

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ИСПОЛЬЗОВАНИЯ PKI С ТЕХНОЛОГИЕЙ BLOCKCHAIN

А.Колыбельников

Московский физико-технический институт(государственный университет)

Введение

В работе [1] представлен подход к построению инфраструктуры открытых ключей(PKI) с использованием технологии сцепления блоков (blockchain)[2], разработанная система была названа Certcoin. Система Certcoin интересна для исследования, потому что использование технологии сцепления блоков активно популяризируется в среде криптографов и она построена с использованием сетевой модели взаимодействия между участниками PKI.

Для создания системы Certcoin была выбрана сетевая модель PKI. Суть сетевой модели PKI сводится к следующему, каждый узел создает себе пару открытый/секретный ключ, сертификат открытого ключа подписывается всеми соседями и заносится в их базу данных, ранг узлов(УЦ) везде одинаковый, цепочка доверия строится исходя из поиска доверенного пути, когда от узла к узлу можно построить путь, за каждый этап которого поручится один из УЦ. Количество и направление связей между узлами ни чем не ограничено.

В Certcoin от классической схемы PKI есть одно важное отличие, список отозванных сертификатов (CRL) не ведется. Вместо него формируются отдельные записи об отзыве сертификатов, которые содержать идентификатор сертификата, слово revoke, отозванный открытый ключ и подпись. Такой подход приводит к росту базы данных отозванных сертификатов в 5-10 раз быстрее, нежели ведение списков CRL. Кроме того, Такой подход не дает возможности построить цепочку доверия между узлами до тех пор, пор пока не будут доступны все узлы, которые участвуют в организации цепочки доверия. Это означает следующее, если один из узлов получил когда-либо ранее сообщение от другого узла и хочет проверить подпись под этим сообщением, то должны быть доступны по сети все узлы, через которые строится цепочка доверия между отправителем и получателем, если же один из узлов был выключен или временно недоступен, цепочка доверия рвется и нет возможности проверить подпись. Так как не понятно отозваны сертификаты отправителя или нет. На рисунке ниже приведена процедура проверки подписи из [1].

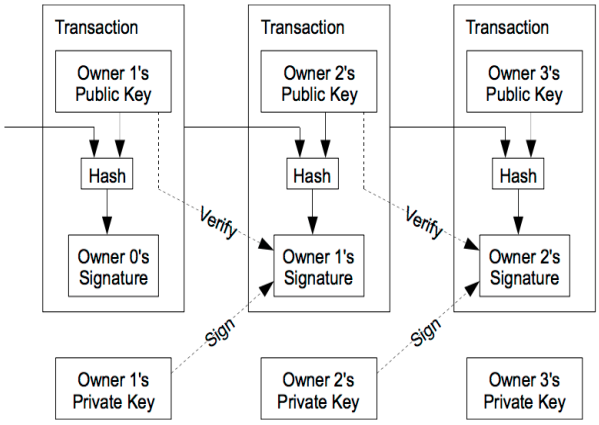

Рисунок 1 порядок проверки подписи в Certcoin

Кроме того, есть еще два нюанса. В реальной сети пользователи не располагают правами на удостоверения личности и принадлежности сертификата конкретной личности. Этой процедурой заведуют исключительно удостоверяющие центры, которые считаются источниками доверия. Исходя из этого, построить одноранговую сеть можно только на уровне УЦ. Второй нюанс заключается в том, что возможность доверять конкретному УЦ удостоверяет один или несколько государственных УЦ, то есть доверие делегируется сверху в низ, в случае же применения blockchain доверие выстраивается в обратном направлении, что может повлечь возникновение поддельных УЦ и утрате доверия к PKI в целом.

При построении PKI на базе сетевой модели, или с выделением главного УЦ следует учитывать те недостатки, которые уже найдены исследователями.

Для того, что бы система Certcoin была бы устойчива к известным атакам на PKI[3] и на системы с использованием blockchain необходимо систему Certcoin доработать или разработать альтернативную.

Для того, что бы система PKI на базе blockchain была бы устойчива к существующим атакам предлагается использовать доработанный протокол:

1. Генерация первого блока данных, который бы содержал информацию о всех сертификатах аккредитованных УЦ, должна быть осуществлена единым центром, которому все участники сети доверяют. Под аккредитацией должна пониматься процедура проверки безопасности УЦ и соблюдение ими правил выпуска сертификатов пользователей. В этом случае, УЦ берут на себя роль организаций ответственных за постоянную актуализацию базы данных, с точки зрения blockchain такие организации называются miner. Свой статус они должны будут поддерживать периодическим расчетом следующих блоков с данными действующих сертификатов.
2. В свою очередь УЦ обязаны требовать от пользователей прохождения аутентификации по паспорту или другим официальным документам при получении сертификата. В случае если пользователь отправляет УЦ информацию об отзыве сертификата он обязан выпустить новый блок без данных отозванного сертификата.
3. Пользователи сертификатов обязаны хранить у себя всю цепочку блоков для каждого сертификата.
4. Отсутствие цепочки блоков у пользователя является доказательством недействительности сертификата.

Список литературы

1. A Decentralized Public Key Infrastructure with Identity Retention C. Fromknecht D. Velicanu S. Yakoubov November 11, 2011 https://eprint.iacr.org/2014/803.pdf
2. Namecoin, https://www.namecoin.org/.
3. Tom Espiner. Trustwave sold root certi_cate for surveillance, 2012.