УДК 004

Система распространения полномочий и сертификатов открытых ключей на базе корпоративного блокчейна

Р. А. Шарапов
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская обл., Россия

Описывается решение задачи децентрализации доступа к централизованной иерархической PKI-системе на основе корпоративного блокчейна.

Ключевые слова: удостоверяющий центр, сертификат открытого ключа, иерархическая система PKI, корпоративный блокчейн, PBFT.

Классическая PKI-система, несмотря на надёжность и проверенность временем, имеет ряд недостатков, которые так и не были исправлены. Необходимость сверки своих данных с CRL на центральном сервере до принятия сертификата приводит к следующим проблемам:

- при задержках или проблемах с обновлением CRL на сервере клиент, обратившийся к этому серверу, может принять отозванный сертификат за действующий;
- если при обращении к серверу он не отвечает или если определить статус сертификата не удаётся (например, из-за технических неполадок или атаки отказа в обслуживании), то все дальнейшие операции клиента будут приостановлены, так как никакие операции, зависящие от этого сертификата, не будут разрешены, что может привести к остановке работы.

Простои в работе означают убытки. Поэтому возникла задача децентрализации доступа к PKI для повышения отказоустойчивости и доступности. При этом сама модель PKI должна в идеале остаться централизованной иерархической, так как в банковских и бизнес-структурах применяется иерархическая модель PKI с корневым управляющим центром (УЦ) в штаб-квартире и УЦ-наследниками в филиалах и внутри отделов каждого офиса [1].

Эту задачу можно решить с помощью системы распространения полномочий и сертификатов открытых ключей на базе приватного корпоративного блокчейна. При этом искомая система не должна быть анонимной, т. е. должна существовать возможность идентификации узла в блокчейне (это касается как обычных пользователей, так и фиксаторов транзакций). Также система должна иметь высокую пропускную способность для быстрого управления сертификатами. При этом она должна стабильно работать даже при выходе из строя или компрометации значительной части узлов.
Предложен концепт решения этой задачи, в рамках построения которого были рассмотрены ключевые аспекты системы, выбраны алгоритм консенсуса, фреймворк и анкоринг, предложен вариант имплементации блокчейна в иерархическую модель PKI и описан цикл работы системы на высоком (логическом) уровне.

Выбор алгоритма консенсуса

В блокчейн-системах одним из наиболее важных факторов является алгоритм консенсуса, который позволяет системе определить, какой блок и какая цепь должны считаться верными.

Рассмотрим, каким должен быть консенсус в данной системе.

Во-первых, он должен допускать определённую централизацию системы, т. е. поддерживать фиксированное количество заранее известных фиксаторов транзакций и при этом давать возможность идентифицировать каждого фиксатора по его электронной подписи. Во-вторых, алгоритм должен учитывать возможную компрометацию или выход из строя одного или нескольких узлов фиксаторов транзакций, т. е. он должен проверять содержимое транзакций и реагировать в случае обнаружения некорректной работы. Эти два условия дают возможность контролировать процесс производства блоков и обнаруживать все случаи некорректной работы узлов.

Также алгоритм в идеале не должен использовать майнинг, так как это довольно дорогостоящий

Шарапов Роман Андреевич, студент 4-го курса.
E-mail: sharapov.roman@gmail.com

Статья поступила в редакцию 13 июня 2018 г.

© Шарапов Р. А., 2018

и медленный процесс, но при этом должен обеспечивать невозможность переписать блокчейн с нуля при компрометации всех узлов фиксаторов сразу.

Алгоритмом консенсуса, удовлетворяющим всем обозначенным требованиям, является Practical Byzantine Fault Tolerance (PBFT), основанный на классической задаче византийских генералов.

Рассмотрим алгоритм PBFT подробнее.

- В каждом раунде есть узел-лидер (или арбитр), который предлагает заготовку следующего блока и распространяет ее по сети. Этот лидер выбирается раз в цикл случайным образом.
- Узлы-валидаторы голосуют за предложенный блок, распространяя *prevote*-сообщение, которое обозначает, что узел смог распознать сообщение и подтверждает, что информация в сообщении корректна.
- После того как валидатор собрал достаточное количество *prevote*-сообщений с большинства узлов, он подтверждает транзакцию и распространяет *precommit*-сообщение, которое включает в себя содержимое блока и его хэш. Это сообщение означает, что узел готов поместить соответствующий блок в блокчейн, но ожидает одобрения других узлов-валидаторов.
- В конце раунда, если валидатор собрал превалирующее большинство *precommit*-сообщений с тем же хэшем состояния для того же предложения, то предложенная заготовка блока становится блоком и помещается в конец блокчейна [2, 3].

Лесли Лэмпорт доказал, что если злоумышленники не могут искажать информацию в узлах, то в системе с m скомпрометированными узлами можно достичь согласия при наличии $2m+1$ верно работающих узлов, т. е. двух третей от их общего количества [4]. При обмене информацией появляется возможность определить «предателя», который всем остальным участникам процесса сообщил разные данные. Этот вредоносный узел помещается в карантин и в дальнейшем не учитывается.

Набор, состоящий минимум из 2/3 *prevote*-сообщений от узлов за предложенный блок в текущем раунде при текущей высоте блокчейна (количество блоков в цепи), называется Proof-of-Lock (PoL) состоянием. Узлы хранят PoL-состояние как часть состояния узла. При этом один узел не может хранить более одного PoL-состояния.

Стоит отметить, что узлы фиксаторы могут выступать в роли УЦ, но эти сущности лучше разделить для диверсификации рисков (тогда при компрометации одного узла злоумышленнику достанется либо УЦ, либо узел-валидатор, а не обе сущности сразу). При этом УЦ будет выступать лишь в роли источника транзакций, а не в роли обработчика.

Так как подпись блоков считается тривиальной операцией с точки зрения вычислительных мощностей, существует возможность, хоть и маловероятная, уязвимости централизованного блокчейна с недоверенным центром, когда при компрометации или сговоре всех фиксирующих узлов возможна ситуация, в которой они могут переписать или создать с нуля несколько версий блокчейна, затем разослать их разным пользователям и держать каждого из них в своей версии цепи. В биткойне эту проблему решает майнинг (решение PoW-задачи).

PBFT подразумевает возможность интеграции PoW-консенсуса как дополнительного уровня защиты для замедления процесса создания блоков, однако, как уже было сказано, это слишком дорогой и энергозатратный вариант, что может отпугнуть ряд потенциальных фирм-клиентов. Рассмотрим альтернативное решение фиксации блокчейна.

Анкоринг

Анкоринг — это метод сохранения "слепка" последней рабочей нескомпрометированной версии блокчейна, т. е. создания последнего необратимого блока (Last Irreversible Block – LIB). Это блок, который был подтверждён двумя третями (или более) узлов-валидаторов и затем выслан в публичный блокчейн. Ни один узел не переключится на форк, который не был построен на основании последнего необратимого блока.

С определённой периодичностью администратор будет подписывать последний блок и посылать его хэш в виде транзакции в поддерживающий блокчейн, таким образом создавая чекпойнт системы.

Информация из эксклюзивного блокчейна остаётся нескомпрометированной, так как в общедоступную сеть посылаются только хэши. Для того чтобы совершить атаку, злоумышленнику придётся заполучить минимум 1/3 ключей фиксаторов транзакций, а также преодолеть механизмы защиты общедоступного блокчейна.

Схема анкоринга изображена на рис. 1.

Как только в публичной цепи блок с транзакцией будет подтверждён, любой желающий сможет проверить состояние корпоративной цепи на определённый момент времени [5].

В случае автоматизации процесса анкоринга необходимо учитывать, что блоки на публичной цепи чаще всего создаются с нерегулярными интервалами, значительно превышающими интервалы между блоками на эксклюзивном блокчейне. По этой причине протокол привязки может указывать, что заголовок блока в эксклюзивной цепи может

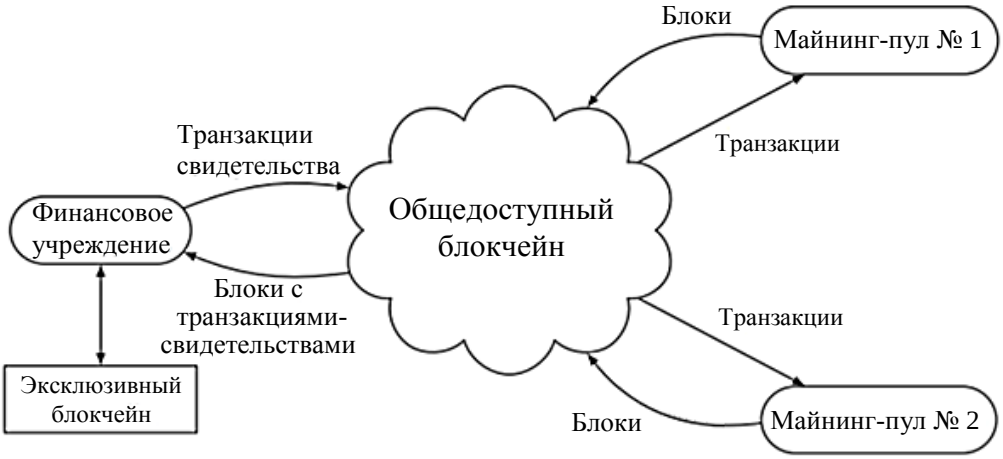

Рис. 1. Привязка эксклюзивного блокчейна при помощи поддерживающего общедоступного блокчейна

(но не обязан) включать SPV-доказательство транзакции-свидетельства одного из предыдущих блоков эксклюзивного блокчейна. Например, если блоки в эксклюзивной цепи создаются с интервалом в 10 с, то транзакцию-свидетельство можно отсылать для одного из 180 блоков (т. е. каждые полчаса). Транзакция-свидетельство должна приобрести необходимое количество подтверждений, чтобы реорганизация блокчейна, исключающая свидетельство из вспомогательного блокчейна, стала статистически маловероятным событием. После этого SPV-доказательство, соответствующее свидетельству, можно включить в заголовок блока эксклюзивной цепи.

PKI-составляющая системы

Рассмотрим имплементацию блокчейна в классическую иерархическую PKI-систему:

Доставка сертификата до конечного пользователя. У злоумышленника не должно быть возможности вмешательства в процесс распространения публичных ключей и отзыва сертификата. В классической централизованной системе доставка сертификата до пользователя является уязвимым моментом в случае, если генерация пары ключей идет на стороне УЦ и надо доставить закрытый ключ клиенту. При установке программного обеспечения на машину клиента ему генерируется пара ключей для его узла в блокчейне, а факт создания нового узла фиксируется в транзакции и заносится в блокчейн с указанием публичного ключа кошелька. При запросе сертификата и генерации приватного ключа на стороне УЦ последний шифрует приватный ключ сертификата на открытом ключе кошелька клиента и посылает полученное сообщение клиенту, который расшифровывает сообщение своим закрытым ключом кошелька. В транзакции фиксируется факт выдачи закрытого ключа сертификата, но выдается не сам ключ, а лишь его хэш.

Стандарт сертификата. В качестве сертификата должен использоваться стандарт X.509.

Доступность и отказоустойчивость. У любого клиента должна быть возможность в любой момент времени обратиться к списку отозванных сертификатов для проверки сертификата. CRL будет полностью храниться в УЦ, а его копии будут храниться на мастернодах, к которым лайтноды могут обратиться в любой момент для прочтения списка. Лайтнодам необходимо дать возможность скачать CRL целиком при запуске программного обеспечения. В небольших корпорациях этот список не должен быть слишком большим и тяжелым, так что объем информации, хранимый на лайтноде-клиенте, будет "по силам" даже для слабых машин. Этот список полностью скачивается и синхронизируется при запуске, затем он просто обновляется, считывая транзакции из поступающих в блокчейн блоков. Если УЦ, один или несколько мастернодов выйдут из строя, то у клиента все равно будет возможность обратиться к CRL либо на других узлах, либо прочитать его у себя на узле.

Неотказуемость. Все операции будут фиксироваться в блокчейне в виде транзакций (с указанием всех данных участников транзакций, включая публичный ключ блокчейн-узла); в результате в случае необходимости можно будет отследить всю историю операций в сети даже в случае компрометации УЦ и части мастернодов. Перечислим эти транзакции: запрос на выдачу сертификата/ на становление узлом-фиксатором/ на отзыв сертификата; отказ/выдача сертификата клиенту; генерация и выдача приватного ключа; добавление сертификата в CRL; добавление/ удаление нового узла.

Сформулируем протокол работы системы таким образом, чтобы она была устойчива к существующим атакам, а также сохраняла свойство доступности.

- Генерация первого блока данных, содержащего информацию обо всех сертификатах, аккредитованных УЦ, должна быть осуществлена единым центром, которому все участники сети доверяют. Под аккредитацией должны 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. Свой статус они должны поддерживать, периодически подписывая блоки с данными действующих сертификатов.
- УЦ обязаны требовать от пользователей прохождения аутентификации по паспорту или другим официальным документам при получении сертификата. Если пользователь отправляет УЦ информацию об отзыве сертификата, УЦ обязан выпустить новый блок без данных отозванного сертификата.
- Пользователи сертификатов обязаны хранить у себя всю цепочку блоков для каждого сертификата.
- Отсутствие цепочки блоков у пользователя является доказательством недействительности сертификата.

Во всем остальном (алгоритмы генерации, хранения, проверки и само содержимое сертификатов и CRL-листов) PKI-система остается без изменений.

Описание работы системы

Теперь перейдем к полному описанию цикла работы системы (рис. 2).

Генерация транзакции. Источниками транзакций являются клиенты и УЦ. Каждая операция запроса, выдачи, отказа, добавления в список и т. д. заносится в свою транзакцию.

Создание блока узлами-фиксаторами. Консорциум узлов производит блок по алгоритму PBFT. Затем арбитр раунда посылает этот блок в сеть.

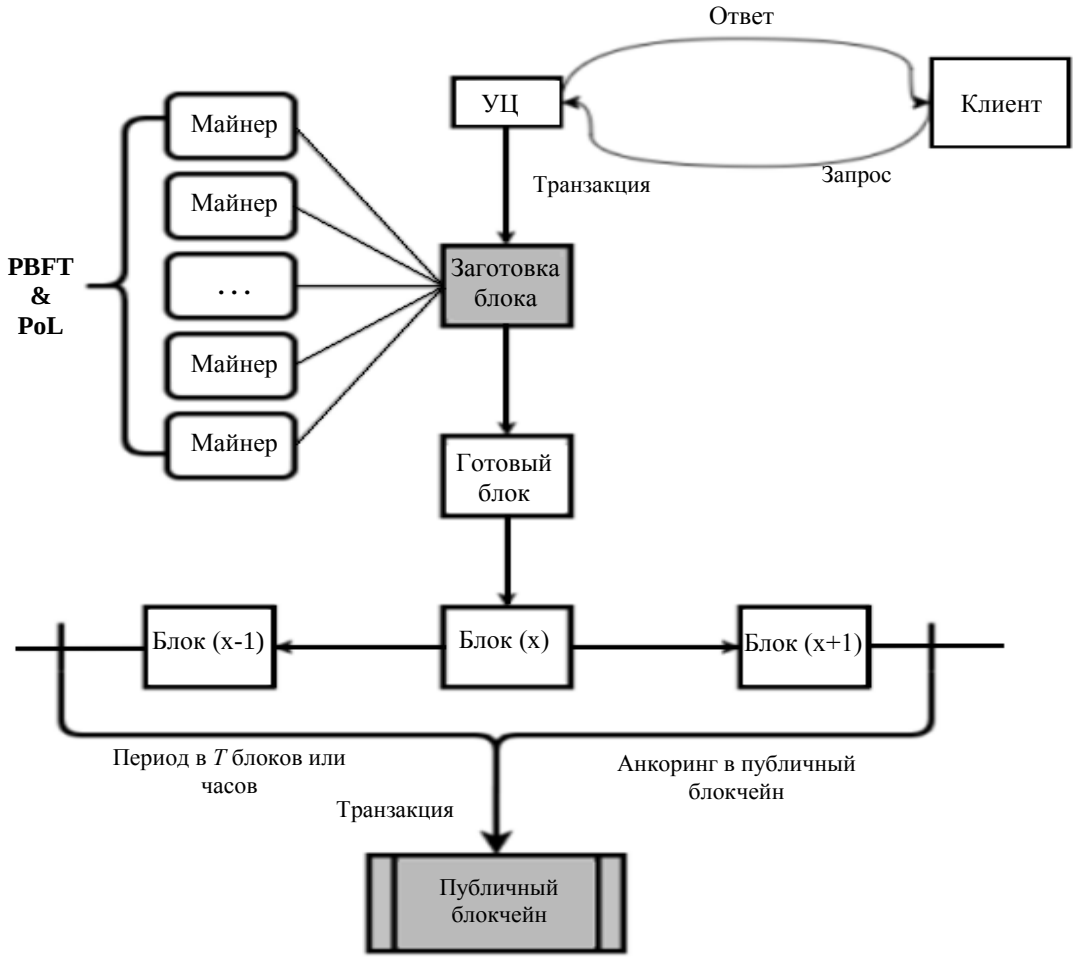

Рис. 2. Схема работы проектируемой системы

Обновление сети. Новый созданный блок попадает в сеть и рассылается по всем узлам.

Анкоринг. Раз в период на усмотрение администратора (обычно в зависимости от нагрузки в сети и ценности данных) делается транзакция, которая отсылается в публичный блокчейн (либо общекорпоративный, либо в биткойн). Предпочтительным вариантом является тот, в котором у фирмы есть возможность запустить публичный блокчейн для всех своих филиалов, а в каждом филиале запустить приватный блокчейн.

Заключение

Без углубления в код и машинно-математическую составляющую рассмотрено одно из возможных решений проблемы децентрализации доступа к классической централизованной иерархической PKI-системе с помощью корпоративного блокчейна.

Литература

1. Введение в криптографию и сертификаты [Электронный ресурс]. Режим доступа: http://www.autopark.ru/ASBProgrammerGuide/CRYPTO.HTM
2. Practical Byzantine Fault Tolerance [Электронный ресурс]. Режим доступа: http://www.pmg.lcs.mit.edu/papers/osdi99.pdf
3. Exonum [Электронный ресурс]. Режим доступа: https://exonum.com/doc/
4. Теорема о византийских генералах [Электронный ресурс]. Режим доступа: http://archive.is/iFLX
5. Открытые и закрытые блокчейны [Электронный ресурс]. Режим доступа: https://forklog.com/wp-content/uploads/public-vs-private-pt1-1.0-ru.pdf

The system of distribution of authority and public key certificates on the basis of corporate blockchain

R. A. Sharapov

Moscow Institute of Physics and Technology (State University), Dolgoprudny, Moscow region, Russia

The article describes the concept of solving the problem of decentralization of access to a centralized hierarchical PKI system based on the corporate blockchain.

Keywords: certification authority, public key certificate, hierarchical PKI system, corporate blockchain, PBFT.

Bibliography — 5 references. *Received June 13, 2018*