УДК 004.65
DOI 10.21685/2587-7704-2018-3-2-12

Open Access | RESEARCH ARTICLE

Технология распределенных реестров как способ защиты данных от подмены

С. Н. Борисова
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Статья посвящена исследованию надежности и защищенности технологии распределенных реестров. Распределенный реестр – это реплицированная база данных, работающая на основе децентрализованных сетей. Ярким примером использования технологии распределенных реестров является технология блокчейн. Защита данных от подмены при использовании распределенных реестров обеспечивается использованием последовательного хеширования, асимметричной криптографии, децентрализованной сети.

Ключевые слова: распределенный реестр, база данных, блокчейн, криптография, электронная подпись, защита информации от подмены, хеш-функция, децентрализованная сеть.

Distributed ledger technology as a way of data protection against spoofing

S. N. Borisova
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article is devoted to research of reliability and security of distributed ledger technology. A distributed ledger is a replicated database operating on the basis of decentralized networks. A vivid example of using distributed ledger technology is blockchain technology. Data protection against spoofing in using distributed ledgers is ensured by sequential hashing, asymmetric cryptography, and a decentralized network.

Keywords: distributed ledger, database, blockchain, cryptography, electronic signature, information protection against spoofing, hash function, decentralized network.

При простейшем подходе распределенный реестр (РР) – это база данных, которая хранится у каждого участника большой распределенной сети и обновляется независимо каждым участником (узлом) данной сети. Узлами называются устройства, на которых установлено соответствующее программное обеспечение и которые совместно ведут распределенные базы данных. Важной особенностью является то, что записи в этой базе данных не передаются в каждый узел из одного управляющего центра, а формируются и хранятся ими на месте независимо. Каждый узел сети обрабатывает каждую транзакцию, принимая свое решение, которое впоследствии согласовывается коллективно всеми узлами сети. При подобной схеме узлы участников сети подключаются друг к другу для обмена и подтверждения информации, что существенно отличается от традиционной архитектуры централизованных систем, в которых присутствует единственный источник достоверных данных (рис. 1). Распределенные реестры позволяют вести актуальные копии базы данных на нескольких узлах, тем самым обеспечивая повышенную операционную устойчивость.

Таким образом, при использовании технологии распределенных реестров соблюдаются следующие принципы (рис. 2):

– каждый участник может обладать полноценной копией реестра;

– соглашения между участниками на добавление новой информации (синхронизация копий реестра) осуществляются на основе протокола достижения распределенного консенсуса;

– участники общаются через децентрализованную сеть;
– для каждого участника взаимодействия имеется доступ к истории транзакций.

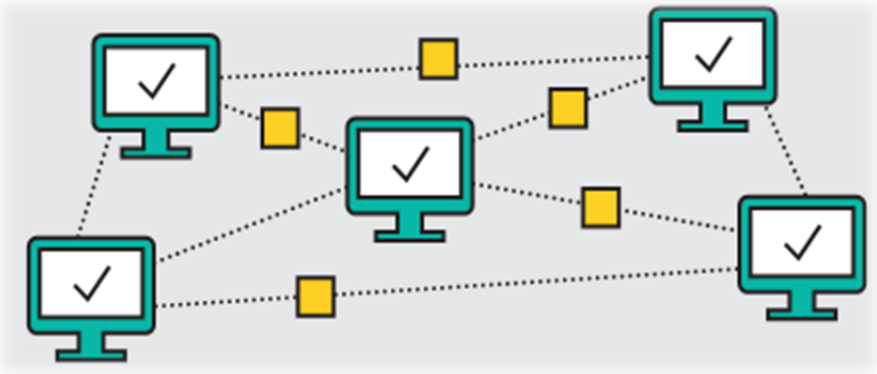

Рис. 1. Пример децентрализованной сети

Рис. 2. Принципы технологии распределенных реестров

Ярким примером использования технологии PP является блокчейн-технология, в которой данные о совершенных транзакциях структурируются в виде цепочки (последовательности) связанных блоков транзакций. Но не стоит отождествлять распределенные реестры и блокчейн. В источнике указано: «Распределенный реестр и блокчейн на самом деле находятся не в синонимичных, а родовидовых отношениях» [1]. То есть блокчейн является видом распределенного реестра, но не каждый распределенный реестр является блокчейном. В случае использования блокчейн-технологии каждый новый блок транзакций подтверждается как валидный всеми участниками сети, только после этого он встраивается в цепочку со всеми предыдущими операциями в распределенном реестре (рис. 3). Блокчейн-технология основана на криптографических протоколах цифровой подписи и хеширования.

Биткойн, являющийся наиболее распространенной и в наибольшей степени исследованной технологией блокчейн, использует очень сложный механизм консенсуса – майнинг. Майнинг заключается в получении хеш-кода блока. Этот процесс является доказательством работы майнера (proof-of-work), доказательством того, что он затратил на вычисление определенные вычислительные мощности [2]. Доказательство проведенной работы требует наличия значительных компьютерных мощно-

стей и является энергоемким. Наряду с этим в PP в качестве алгоритма достижения консенсуса используется «доказательство доли» (proof-of-stake), являющейся капиталоемким.

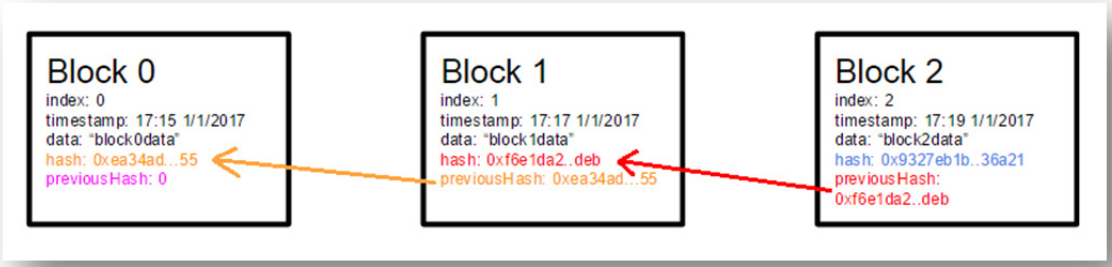

Рис. 3. Цепочка блоков

Таким образом, биткойн является разновидностью блокчейн-технологии, а блокчейн, в свою очередь, разновидностью распределенного реестра. Биткойн является примером открытого распределенного реестра, блокчейн же может быть как открытым, так и закрытым реестром. Разновидности реестров представлены на рис. 4.

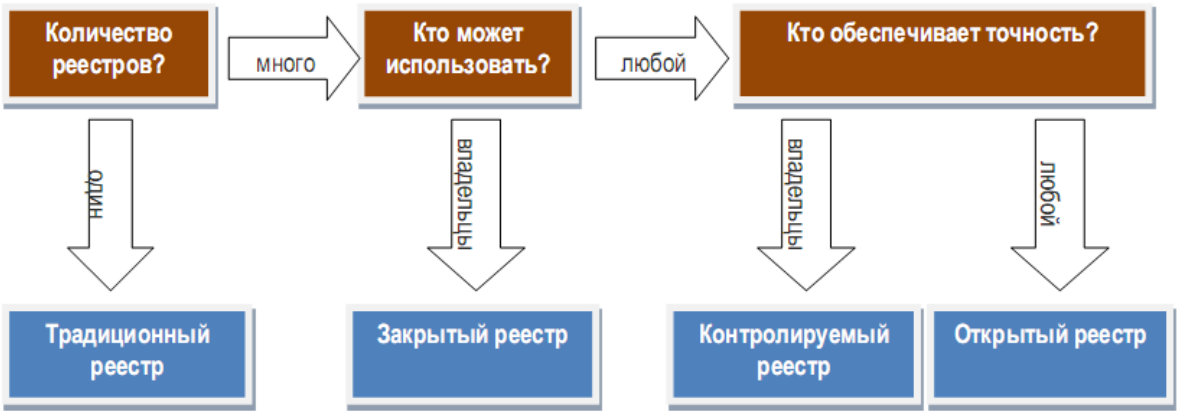

Рис. 4. Классификация сетей распределенных реестров

Открытые сети распределенных реестров – это сети, в которых участники не проходят полноценной идентификации (анонимность или псевдоанонимность), допуск к участию в которой не ограничен для широкого круга пользователей, статус не закреплен за определенными участниками, а также отсутствуют централизованные инстанции, управляющие правилами сети, ее конфигурацией и выпуском криптографических ключей.

Закрытые сети распределенных реестров устанавливают критерии членства, в соответствии с которыми участники допускаются к управлению узлами и получают доступ к сервисам сети. Эти критерии могут включать финансовые требования (например, платежеспособность участника или возможность получения доступа к ликвидным ресурсам), а также юридические требования (способность участника выполнять договорные обязательства перед системой или наличие соответствующих лицензий на осуществление деятельности). В такой сети участники идентифицируемы, допуск ограничен и регламентирован согласно правилам сети, статус участников, ответственных за валидацию, закреплен за определенными контрагентами, и в большинстве случаев существует некоторая инстанция, управляющая правилами сети.

Защита данных от подмены при использовании технологии PP (на примере блокчейн-технологии) осуществляется за счет того, что распределенная база данных формируется как цепочка блоков независимо каждым участником сети, поэтому подмена информации на этапе формирования блока невозможна. Подменить уже сформированный блок цепочки также невозможно, так как новая информация записывается в конец цепочки поверх уже проверенной и частично основывается на ней (каждый последующий блок содержит хеш-код предыдущего блока). При изменении информации в одном блоке путем взлома необходимо изменить информацию во всей цепочке на всех узлах, что

в реальности неосуществимо. Блокчейн-технология использует криптографически стойкую хеш-функцию SHA-256.

Существующие методы управления данными предполагают, что данные расположены в периметре отдельного учреждения, в отдельном хранилище данных. Увеличение стоимости использования системы хранения данных и ее сложность обусловливается использованием ряда систем управления сетью и систем сообщений для связи с внешним миром. Высокоцентрализованные системы демонстрируют большие затраты при любом сбое. Они могут быть уязвимы для атак, а сами данные могут быть несинхронизированны, некорректны или попросту неактуальны.

Распределенные реестры, в отличие от них, по своей сути гораздо лучше защищены от атак, так как вместо одной базы данных они представляют репликацию одной и той же базы данных. Для успешности атаки подмены данных она должна быть произведена на все копии одновременно. Технология также является устойчивой для несанкционированного изменения или взлома, так как участники сети сразу же обнаружат изменения в одной из частей реестра. Кроме того, методы, используемые для защиты и обновления информации, подразумевают, что участники могут делиться данными и быть уверенными, что все копии реестра совпадают друг с другом в любой момент времени. Проблема обеспечения конфиденциальности данных может быть обеспечена использованием закрытых сетей распределенных реестров.

Библиографический список

1. Технология распределенного реестра DLT за рамками блокчейна. – URL: https://crypto-fox.ru/faq/distributed-ledger-technology/ (дата обращения: 18.10.2018).
2. Борисова, С. Н. Исследование защищенности технологии блокчейн и возможностей ее применения / С. Н. Борисова // XXI век: итоги прошлого и проблемы настоящего плюс. Серия: Технические науки. Информационные технологии. – 2017. – № 05 (39) / 06 (40). – С. 148–154.
3. Bitcoin: A Peer-to-Peer Electronic Cash System. – URL: https://bitcoin.org/bitcoin.pdf/ (дата обращения: 18.10.2018).
4. Bitcoin (Биткоин) алгоритм. – URL: https://crypto-wallet.ru/bitcoin-algoritm/ (дата обращения: 18.10.2018).

Борисова, С. Н.

Технология распределенных реестров как способ защиты данных от подмены / С. Н. Борисова // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-12.