

ЭЛЕМЕНТЫ БЛОКЧЕЙН ТЕХНОЛОГИЙ И АНАЛИЗ УГРОЗ

¹Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, профессор

²Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, магистрант

Блокчейн – распределенный реестр, состоящий из взаимосвязанных блоков транзакций. Блоки транзакций, которые регистрируют пользователи, называются узлами реестра, или нодами (nodes). Соответственно, технически блокчейн представляет собой децентрализованную базу данных, предназначенную для хранения и подтверждения достоверности информации. Все размещаемые в блокчейн сведения сохраняются пользователями на своих компьютерах, а достоверность регистрируемых данных обеспечивается криптографическими алгоритмами [1].

Технология блокчейн не представляет собой совершенно нового парадигма. Функционирование технологии основано на старом шаблоне бухгалтерской книги: что-то, что используется для регистрации транзакций за определенный период времени [2].

Блокчейн предлагает те же функции ведения учета, но без централизованной архитектуры. Напротив, блокчейн – это общий децентрализованный распределенный реестр среди сети заинтересованных сторон, которые не могут быть обновлены

любим администратором. Его обновить можно только с согласия участников сети и всех изменений в распределенный регистр подлежат аудиту. Эта проверка выполняется надежно и автоматически от имени каждого пользователя, создавая очень быструю и безопасную систему с исключительной защитой от несанкционированного доступа [2, 4-5].

Существует несколько протоколов организации работы технологии блокчейна, но все они в значительной степени делают одно и то же, и каждый имеет четыре основных элемента: транзакцию, блок, цепочку и процесс консенсуса [2]. Блок – это просто подборка логически организованных транзакций, объединенных в пакет. Транзакция – это регистрация события, например события пересылки денег со счета отправителя на счет бенефициара. Блок состоит из транзакций, а размер его может варьироваться в зависимости от типа и структуры используемого блокчейна [3].

Блок создается путем группирования похожих транзакций вместе. Эти блоки добавляются в хронологическом порядке, напоминая цепочку, отсюда и название цепочка. Затем узлы сохраняют эти новые блоки в локальной базе данных цепочки блоков на своем компьютере или сервере. Сеть узлов управляет базой данных, также известной как блокчейн. Узлы являются точками входа для новых данных, а также для проверки и распространения новых данных, которые были отправлены в цепочку блоков [2].

Добавление нового блока в цепочку означает обновление реестра, который ведется всеми пользователями. Пользователи принимают новый блок только тогда, когда будет подтверждено, что все его транзакции действительны. Если неточность найдена – блок отклоняется. В противном случае блок будет добавлен и останется там как постоянный – публичный отчет. Запись транзакции в один из взаимосвязанных блоков позволяет установить дату ее совершения с точностью до минуты. Алгоритм шифрования данных и присвоение каждому блоку уникального кода сокращают вероятность подлога. Ни один пользователь не может самостоятельно внести в него какие-либо изменения или удалить [1, 4].

Для большей надежности каждое последующее звено цепочки содержит информацию о предыдущем звене или блоке. Увеличение количества проверенных блоков повышает достоверность всех предыдущих транзакций, ведь каждый раз при создании нового блока пользователи проверяют действительность полной цепочки транзакций: от начала и до конца. Чем длиннее цепочка взаимосвязанных блоков, тем меньше вероятность фальсификации [1].

В системе блокчейн между узлами устанавливается протокол, то есть заранее согласованные правила технической и деловой достоверности записываемых данных, а также правило, определяющее, как достигается консенсус.

Технология блокчейн имеет довольно широкий спектр возможного применения и очень большие перспективы развития как в финансовом секторе, транспорте, так и в других отраслях. В ряде стран уже активно внедряются блокчейн-технологии в таких сферах как регистрация различных движимых и недвижимых активов и данных, интеллектуальная собственность, завещания, социальное обеспечение, данные о здоровье в системе здравоохранения и в пенсионной системе. Имеются опробованные блокчейн-решения для проведения аукционов и повышения прозрачности государственного и местных бюджетов, обеспечения честного подсчета голосов на выборах, создания краудфандинговых площадок, позволяющих инвесторам отслеживать, как и на что тратятся средства [6-8].

В докладе представлен анализ угроз в технологии блокчейн. Угрозы технологии блокчейн условно подразделяются на три уровня: угрозы на уровне майнера, угрозы на уровне сети и на уровне пользователя. Рассмотрена модель противодействия таким угрозам и атакам, обеспечивающая информационную безопасность в технологии блокчейн. Суть модели заключается в установлении объекта блокчейн сети, который может быть подвержен возможным атакам и угрозам; определения потенциально уязвимых мест, наиболее подверженных различного рода угрозам безопасности; разработка комплекса мероприятий по обеспечению информационной безопасности сети.

ЛИТЕРАТУРА

1. Блокчейн на пике хайпа: правовые риски и возможности / А. Ю. Иванов [и др.] ; под ред. А. Ю. Иванова. – 2-е изд. – М. : Изд. дом Высшей школы экономики, 2018. – 237 с.
2. Boucher, Ph. How blockchain technology could change our lives: In-depth Analysis / Ph. Boucher, S. Nascimento, M. Kritikos. – Brussels : STOA, 2017. – 26 s.
3. Имран, Б. Блокчейн: архитектура, криптовалюта, инструменты разработки, смарт-контракты / Б. Имран. – М. : ДМК-Пресс, 2019 – 538 с.
4. Blockchain for the Humanitarian Sector: Future Opportunities [Electronic resource] // *ReliefWeb – Informing humanitarians worldwide.* – Mode of access : <https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20%20November%202016.pdf>. – Date of access : 11.10.2020.
5. Blockchain: A catalyst for new approaches in insurance [Electronic resource] // *PwC Schweiz.* – Mode of access : https://www.pwc.ch/en/publications/2017/Xlos_Etude_Blockchain_UK_2017_Web.pdf. – Date of access : 11.10.2020.
6. Технология Blockchain. Принципы работы и перспективы применения [Электронный ресурс] / Ю. Штольц [и др]. // Научная электронная библиотека «КиберЛенинка». – Режим доступа : <https://cyberleninka.ru/article/n/tehnologiya-blockchain-printsipy-raboty-i-perspektivy-primeneniya/viewer>. – Дата доступа : 02.12.2020.
7. Блокчейн – новые возможности для производителей и потребителей электроэнергии. Обзор мировой электроэнергетики [Электронный ресурс] // *PwC в России.* – Режим доступа : https://www.pwc.ru/ru/publications/blockchain/blockchain_opportunity-for-energy-producers%20and-consumers_RUS.pdf. – Дата доступа : 25.11.2020.
8. Маркушевский, Д. Технологии блокчейн для электронного правительства. Краткий аналитический обзор [Электронный ресурс] / Д. Маркушевский, Н. Рябова, В. Кухарчик // Школа молодых менеджеров публичного администрирования. – Режим доступа : http://sympa-by.eu/sites/default/files/library/brif_issledovaniya_vozmozhnostey_primeneniya_tehnologii_blockchain_v_gosupravlenii.pdf. – Дата доступа : 01.12.2020.