

Лушников Никита Дмитриевич,

*студент 4 курса, специальность «Безопасность информационных технологий
в правоохранительной сфере»;*

Альтерман Анна Дмитриевна,

*студентка 4 курса, специальность «Безопасность информационных технологий
в правоохранительной сфере»,*

ФГБОУ ВО «Башкирский государственный университет»,

г. Уфа, Республика Башкортостан, Россия

BLOCKCHAIN КАК НОВАЯ ЕДИНИЦА В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В данной статье рассказывается о современной технологии, которая работает через транзакцию, так же как работает Blockchain, и об особенностях этой технологии.

Ключевые слова: Blockchain, технология, транзакция, операция, сеть, данные.

Blockchain – это технология, на базе которой построен Bitcoin. Но есть, пожалуй, десятки других способов использования блокчейна в отрыве от криптовалют.

Многие считают, что Blockchain – это главный технологический прорыв со времен изобретения интернета. Такое внимание к нему связано с революционностью, которую он привнес. Сам термин Blockchain частично характеризует его задачи и назначение. Часть «Block» – это блоки, «chain» – это «цепочка». Получается, что Blockchain – это цепочка блоков. Причем, не просто цепочка. В ней выдерживается строгая последовательность.

Если говорить более подробно, то блоки – это данные о транзакциях, сделках и контрактах внутри системы, представленные в криптографической форме. Изначально блокчейн был (и остается до сих пор) основой криптовалюты Bitcoin. Все блоки выстроены в цепочку, то есть, связаны между собой. Для записи нового блока, необходимо последовательное считывание информации о старых блоках.

Все данные в Blockchain накапливаются и формируют постоянно дополняемую базу данных. С этой базы данных невозможно ничего удалить

или провести замену или подмену блока. И она «безгранична», то есть туда может быть записано бесконечное количество транзакций. Это – одна из главных особенностей Blockchain [1].

Работу блокчейн можно сравнить с Torrent. Функционирование торрентов происходит в режиме P2P (peer to peer – компьютерная сеть, где все участники равноправны). Когда скачиваем какой-то файл с трекера, то не используем центральный сервер или хранилище. Файл напрямую скачивается у такого же участника торрента. Если в пиринговой сети не будет участников, то и файлы скачивать будет не возможно. Аналогично и в блокчейн – все операции проводятся между субъектами напрямую, то есть, все участники подключены к одной сети – Blockchain. Существует два вида цепочки [3]:

1. Публичный Blockchain – открытая, дополняемая база данных. Такой вид блокчейна используется в криптовалюте Bitcoin. Каждый участник может записывать и читать данные.

2. Приватный или частный блокчейн имеет ограничения по записи или чтению данных. Могут устанавливаться приоритетные узлы. Подвид Private Blockchain – эксклюзивный блокчейн. В такой цепочке устанавливается группа лиц, занимающаяся обработкой транзакций.

Ключевыми особенностями Blockchain являются [1]:

- децентрализация – в цепочке нет сервера. Каждый участник – это и есть сервер. Он поддерживает работу всего блокчейна;
- прозрачность – информация о транзакциях, контрактах и так далее хранится в открытом доступе. При этом эти данные невозможно изменить;
- теоретическая неограниченность – теоретически блокчейн можно дополнять записями до бесконечности;
- надежность – для записи новых данных необходим консенсус узлов блокчейна. Это позволяет фильтровать операции и записывать только легитимные транзакции. Осуществить подмену хэша нереально.

На примере денежной транзакции рассмотрим работу Blockchain. Это последовательность блоков – цепочка, а не замкнутый круг или что-то еще.

Каждый из блоков содержит массив определенных данных. И все блоки связаны между собой. То есть, новый «массив» может быть создан только после того, как закрыт старый массив.

Основной технический момент – формирование и закрытие блоков. Каждое звено цепочки содержит определенный ключ. Пока он не будет расшифрован, блок (звено) не закроется. Сама расшифровка происходит через майнинг. Майнеры, занимающиеся добычей криптовалюты, делают это с помощью мощностей видеокарт и процессоров. Те, в свою очередь, выполняют вычислительные операции, главная цель которых – поиск криптографической подписи к блоку в виде хеша. Как только она подобрана – блок закрывается. А майнер за это получает вознаграждение в виде криптовалюты. Функционирование блокчейна и его безопасность обеспечивается майнерами и другими участниками блокчейна. Их еще называют нодами или узлами. Есть полные ноды. Под ними подразумеваются майнеры и простые пользователи полновесных кошельков. Это значит, что они на своем компьютере или другом устройстве имеют полную версию блокчейна [3].

Его объем постоянно растет. Если в 2015-м году он занимал 35 гигабайт памяти, то в 2018-м – уже более 100. Из-за этого количество полноценных узлов начало сокращаться. Пример полновесного кошелька – Bitcoin-Core. Сущность «цепи блоков» как общедоступной, распределенной и 100% достоверной базы данных, делает применение блокчейн весьма привлекательным для компаний, работающих в разных областях.

Как видим, блокчейн – универсальная технология, применимая в разных сферах жизни, что однозначно является ее плюсом. Также Blockchain уменьшает транзакционные издержки, сокращает время проведения сделок с нескольких дней, а то и недели, необходимых для проверки данных и обмена документами, до нескольких часов; кроме того, позволяет организациям, учреждениям избавиться от лишних статей расходов [2].

Однако есть и минусы. Это – масштабируемость, так как сегодня блокчейн не способен обеспечивать огромное количество транзакций за

короткое время. Также ежедневно растет и вес базы, которая хранится на компьютерах сети. Все эти сложные вычисления заставляют компьютеры потреблять большое количество энергии.

Говоря о неустойчивости блокчейна, эксперты указывают также на вероятность так называемой «атаки 51%». Иными словами, если группа участников сети сконцентрирует в своих руках 51% вычислительных мощностей, она может начать действовать в своих интересах, подтверждая только выгодные для себя транзакции. Однако для этого потребуются настолько мощные ресурсы, что осуществить на практике эту идею чрезвычайно сложно.

СПИСОК ЛИТЕРАТУРЫ

- 1. Что такое блокчейн и зачем он нужен [Электронный ресурс]. – URL: <https://habr.com/ru/company/bitfury/blog/321474/> (дата обращения 20.01.2019).*
- 2. Что такое блокчейн, и как это работает [Электронный ресурс]. – URL: <https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc> (дата обращения 20.01.2019).*
- 3. Что такое блокчейн простыми словами [Электронный ресурс]. – URL: <https://prostocoin.com/blog/blockchain-guide> (дата обращения 20.01.2019).*