БЛОКЧЕЙН

Николай ШАРАФУДИНОВ

Департамент Программная Инженерия и Автоматика, группа TI-196, Факультет Вычислительной Техники, Информатики и Микроэлектроники, Технический Университет Молдовы, Кишинев, Молдова

Автор Корреспондент: Николай ШАРАФУДИНОВ, e-mail: sarafudinov.nicolae@isa.utm.md

Научный руководитель: Дориан САРАНЧУК, DISA, FCIM, UTM

Аннотация: *цель статьи – определить, что такое блокчейн, из чего он состоит и где используется. Для этого в статье рассмотрены такие понятия как узел, хеширование и шифрование, технология DLT, консенсус и алгоритм консенсуса. А также в данной статье показано почему данная технология становится популярной в наше время.*

Ключевые слова: *блокчейн, хеш-дерево, хеширование, распределенный реестр, консенсус.*

Введение

Последние несколько лет технология распределенного реестра (distributed ledger technology, DLT), в частности блокчейн (blockchain), не только активно обсуждается, но и плотно внедряется в большинстве развитых стран во многих областях экономики. Многие организации ставят своей целью разобраться в возможном применении технологии. В данной статье будет описано что такое блокчейн, чем является алгоритм консенсуса, а также в каких сферах можно применить технологию блокчейн.

Что такое блокчейн?

Блокчейн — это система записи информации таким образом, чтобы ее было невозможно изменить, взломать или обмануть. Блокчейн, как следует из самого названия, представляет собой цепочку блоков. Каждый блок содержит в себе набор из совершенных в течение определенного периода времени (в биткоине это в среднем 10 минут) транзакций между пользователями.

Каждый последующий блок имеет временную метку и ссылку на предыдущий блок. Так же в блок заносится не сама транзакция, а 32-битное значение, обозначенное, как корень Меркла (merkle_root) рис. 1. Также блок содержит уникальный заголовок (block header) уникальность которого достигается за счет того, что каждый заголовок является значением хеш-функции SHA256, от информации, хранящейся в нем: список транзакций (корня Меркла), временная метка создания блока, версия текущего алгоритма, текущая сложности вычисления блока, nonce и заголовок предыдущего блока [1].

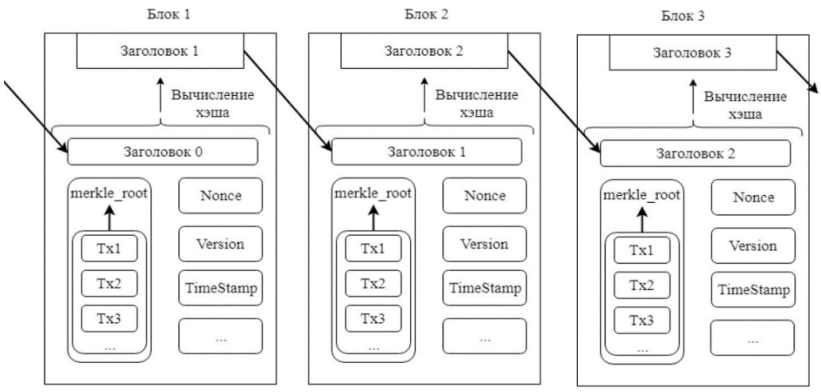

Рисунок 1. Blockchain

Узел в блокчейне

Узел — это любой компьютер, который подключен к блокчейну, проверяющий и подтверждающий транзакции, а также хранит копию блокчейна. Узлы обеспечивают безопасность блокчейна, даже при условии, когда узел отключен от сети «offline node», или же подключена к сети непостоянно то при подключении, данные узлы должны загрузить обновлённые копии реестра для синхронизации с сетью. Синхронизируя свои хранилища с данными о последних транзакциях, большее количество узлов делает внесение изменений невозможным, а также не оставляет хакеру шансов остаться незамеченным. Хакер не сможет удалить данные с множества различных узлов, что значит — вся информация в безопасности. Более того, узлы сортируются по их доступности и в соответствии с их состоянием, в сети или же нет, принимается решение непрерывно отправляет данные в сеть или же игнорировать узлы, не подключенные к сети.

Хеширование и Шифрование

Шифрование и временные метки в совокупности позволяют технологии блокчейн автоматически проверять неизменность этой постоянно увеличивающейся последовательности хеш-кодов. Эта операция не позволяет вставлять новые блоки не по порядку, делая невозможными изменение или фальсификацию данных транзакций.

Отличительной чертой распределенного реестра является активное использование криптографических методов. В первую очередь, речь идет о криптографически стойкой хеш-функции (hash-function SHA-256). Если процесс хеширования повторяется с точно такими же транзакциями, будут созданы точно такие же хеши. Это позволяет любому, кто использует блокчейн, проверить, что данные не были подделаны, потому что любое изменение в любой части данных приведет к совершенно другому хешу, влияющему на каждую итерацию хешей вплоть до корня в Merkle tree рис. 2.

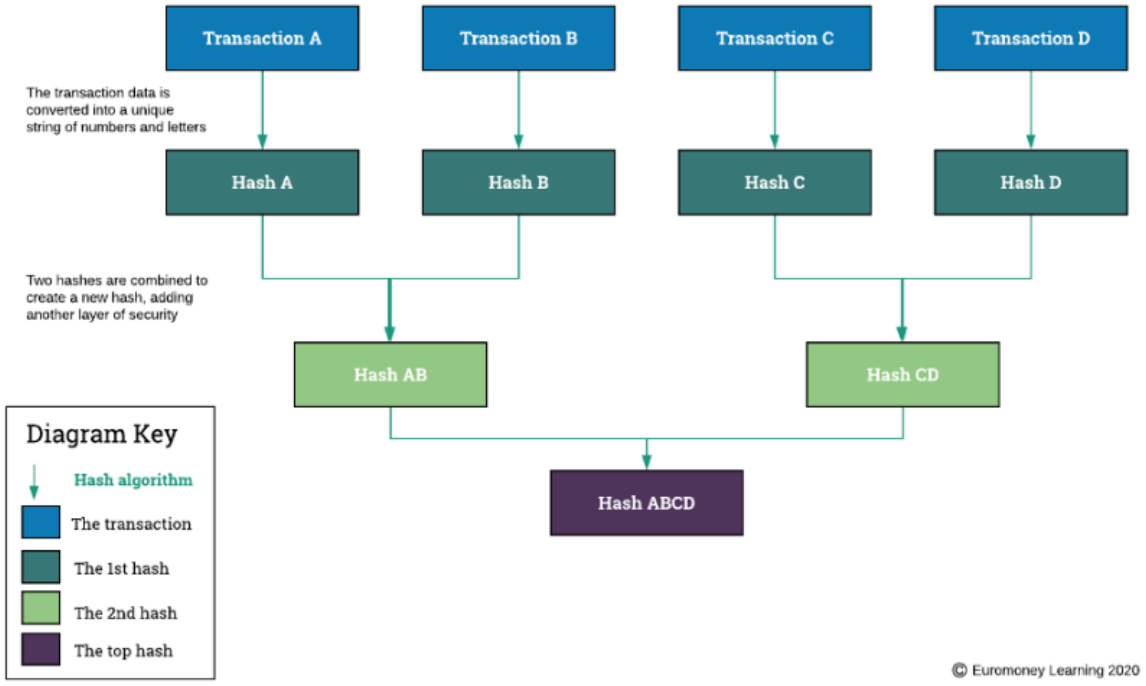

Рисунок 2. Хеш-дерево, Merkle tree

Merkle tree служат для значительного сокращения объема данных, необходимых для хранения, передачи по сети, путем объединения наборов хешированных транзакций в один корневой хеш. Поскольку каждая транзакция хешируется, затем объединяется и снова хешируется, окончательный корневой хеш по-прежнему будет иметь стандартный размер.

Технология распределенного реестра DLT (distributed ledger technology)

Несмотря на то, что на рынке существует большое количество DLT, все они состоят из одних и тех же строительных блоков: распределенного реестра, алгоритма консенсуса (для обеспечения идентичности всех копий реестра) и вознаграждения за участие в сети. DLT — это протокол, который обеспечивает безопасное функционирование децентрализованной цифровой базы данных [2]. DLT позволяет безопасно и точно хранить всю информацию с помощью криптографии. Как только информация сохраняется, она становится неизменной в базе данных и регулируется правилами блокчейна. Главными особенностями DLT являются:

- Хранение данных в одноранговой сети — у каждого узла равные права.
- Удаленность узлов — узлы с копиями баз данных удалены друг от друга географически и связаны друг с другом через интернет.
- Механизм синхронизации — узлы сообщают друг другу о любых изменениях, внесенных в реестр, проверяют эти изменения и вносят их в свою копию реестра.

Консенсус

Механизм консенсуса представляет собой некий компьютерный алгоритм, который лежит в основе распределенного реестра. Благодаря данному алгоритму децентрализованные узлы сети достигают согласия о текущем состоянии данных во всех блоках [3]. Алгоритм консенсуса необходим для проверки корректна ли транзакция. Другой важной задачей механизма консенсуса является разрешение конфликтов между некоторыми противоречащими транзакциями, проводимыми одновременно. Ситуация, когда два майнера одновременно сгенерировали подходящие блоки, вызывает раздвоение цепи блоков. Тогда главной цепочкой будет считаться та, ответвление которой будет быстрее продолжено. Множество алгоритмов консенсуса находятся еще в процессе создания. Наибольшую популярность приобрел механизм консенсуса Proof-of-Work (доказательство выполнения работы).

Механизм консенсуса Proof-of-Work (PoW)

Чтобы участвовать в проверке транзакции, участникам необходимо публично доказать проведенную работу. А именно решение криптографической задачи [4]. Решение криптографической задачи сводится к простейшему перебору миллионов комбинаций кода путем изменения динамического числа nonce, создающих доказательство «работы». В момент, когда майнер находит хеш, он отправляет хеш другим компьютерам сети на проверку. Другие участники не могут использовать его для создания блока так как ключ разгадки хеша принадлежит майнеру, что решил криптографическую задачу первым. Считается, что транзакция является окончательно проведенной, если от блока, в котором она учтена, цепь блоков продлена хотя бы на 6 блоков. В противном случае, если транзакция по передаче некоторого количества биткоинов оказалась в отвергнутой цепочке, она становится недействительной и автоматически вновь становится в очередь на подтверждение при генерации текущего блока. Особенность полученного хеша в его асимметрии — он достаточно сложен для нахождения майнеру, но при этом данный хеш легко проверить [5].

Формирование цены

Криптовалюты имеют ценность, потому что, они являются уникальными цифровыми активами, которые могут быть использованы для проведения безопасных, быстрых и анонимных транзакций без участия посредников.

Для сдерживания инфляции и для регулирования сложности работы по генерированию новых блоков, система автоматически анализируется время, затраченное на нахождения хеш кода, и раз в две недели настраивает сложность для обеспечения среднего показателя 6 блоков в час. Кроме того примерно раз в четыре года уменьшается в два раза вознаграждение за нахождение нового блока что приводит к росту цены криптовалюты.

Сферы применения блокчейн

На сегодняшний день экосистема, складывающаяся вокруг блокчейна, увеличивается в геометрической прогрессии и становится все более сложной. Одной из сфер использования децентрализованного распределенного реестра является криптовалюта которая позволяет быстро и безопасно осуществлять платежи.

Помимо финансовой сферы блокчейн используется там, где каждый блок представляет собой токен. Токен — это единица учёта, не являющаяся криптовалютой, выполняющая функцию «заменителя ценных бумаг» в цифровом мире. Токены представляют собой запись в регистре, распределенную в блокчейн-цепочке.

В медицине технологию блокчейн можно использовать для картотеки с медицинскими данными пациентов. В сфере сделок по купле-продаже и передача прав на собственность. Также Блокчейн может использоваться в регистрации транспортных средств и проверке истории владения ими. А также Блокчейн избавит производителей и потребителей от подделок и облегчит сертификацию отслеживаемой продукции.

Не меньше востребована и технология NFT – невзаимозаменяемых токенов. Она позволяет закрепить и передавать право собственности на цифровые произведения искусства. Развитие блокчейн-экосистемы не ограничивается этими технологиями, и в будущем мы увидим новые решения.

Заключение

Данная технология все еще развивается и в скором будущем вытеснит устоявшиеся порядки изменив вид отношений между поставщиком и получателем. Система прозрачна так как ничего не скрывается, возможность защиты и неизменности данных на сегодняшний день очень важны, именно поэтому технология в ближайшем будущем не утратит, а на оборот приобретёт еще большую популярность и востребованность.

Библиография

1. К. Д. ШИЛОВ, А. В. ЗУБАРЕВ. Блокчейн и распределенные реестры как виды баз данных [online]. [20.12.2022]. Доступно: https://cyberleninka.ru/article/n/blokcheyn-i-raspredelennye-reestry-kak-vidy-baz-dannyh
2. ДАРЬЯ КЛЕЙН. Технология распределенного реестра DLT за рамками блокчейна. [online]. [25.12.2022]. Доступно: https://crypto-fox.ru/faq/distributed-ledger-technology/
3. ЕВГЕНИЙ ХАТА. Что Блокчейн для бабушки за 60 минут. [online]. [30.12.2022]. Доступно: http://loveread.ec/read_book.php?id=72457&p=1
4. Euromoney. How does a transaction get into the blockchain? [online]. [05.01.2022]. Доступно: https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain
5. ForkLog. Что такое алгоритм Proof-of-Work (PoW)?. [online]. [10.01.2022]. Доступно: https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake