Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт космических и информационных технологий
Кафедра вычислительной техники

РЕФЕРАТ

по Информатике

Блокчейн и криптовалюты

Преподаватель _____ Пушкарев К.В.
подпись, дата

Студент КИ18-09Б, 031831293 _____ Овсянников В.А.
подпись, дата

Студент КИ18-09Б, 031830645 _____ Котов С.А.
подпись, дата

Студент КИ18-09Б, 031830510 _____ Непомнящий Д.О.
подпись, дата

Красноярск 2019

Содержание

Введение

Впервые блокчейн стал использоваться как основа первой криптовалюты — биткоина, где он играл роль распределенного реестра для всех операций с цифровыми монетами (токенами). Благодаря блокчейну биткоин стал первой виртуальной валютой, которая способна решить проблему двойных расходов без использования авторитетного органа или центрального сервера (третьего лица). Блокчейн представляет собой единый защищенный реестр информации и данных, которая представлена в виде электронных файлов [1].

1 Определение блокчейна

Блокчейн [2] — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

Впервые термин появился как название полностью реплицированной (синхронизированный с несколькими копиями) распределённой базы данных, реализованной в системе «биткоин», из-за чего блокчейн часто относят к транзакциям (полностью совершенная операция) в различных криптовалютах, однако технология цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки. Биткойн стал первым применением технологии блокчейн в октябре 2008 года.

1.1 Суть работы блокчейна

При формировании цепи важным моментом считается создание и закрытии блока. Каждый элемент цепи содержит ключ, который требует расшифровки. До этого закрытие блока не происходит. Майнеры (добытчики цифровой криптовалюты), которые добывают виртуальные деньги, используют для этих целей процессоры, видеокарты и другое оборудование. Последнее берёт на себя опцию вычислений для поиска хеша (цифровая подпись). После её подбора происходит закрытие блока.

Цепочка блокчейн распределена и поддерживается миллионами компьютеров по всей планете. Работу цепи обеспечивают майнеры и другие участники — узлы сети [3].

Каждый новый блок содержит в себе (рис. 1): хеш предыдущего блока, некоторую информацию о блоке (для биткоина это сумма всех транзакций),

некоторое случайное число (нонс) с определёнными характеристиками, которое вычисляют майнеры.

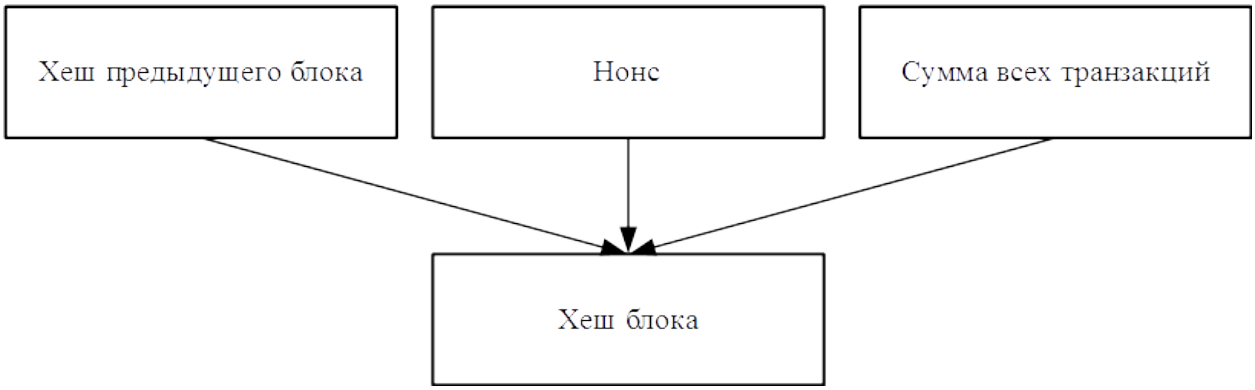

Рисунок 1 – Образование нового блока

1.2 Принцип работы блокчейна

Все данные в блокчейн накапливаются и формируют постоянно дополняемую базу данных. С этой базы данных невозможно ничего удалить или провести замену/подмену блока. Она «безгранична» - туда может быть записано бесконечное количество транзакций. Это одна из главных особенностей блокчейна. Работу блокчейн можно сравнить с сетью BitTorrent. Функционирование торрентов (файл данных) происходит в режиме P2P (peer to peer – компьютерная сеть, где все участники равноправны). Когда мы скачиваем какой-то файл с трекера (сервер, который хранит информацию о пользователях сети BitTorrent), то мы не используем центральный сервер или хранилище. Файл напрямую скачивается у такого же участника торрента, как и вы. Если в пиринговой сети (p2p сети) не будет участников, то и файлы скачивать вы не сможете. Аналогично и в блокчейне. Все операции проводятся между субъектами (участники перевода) напрямую. А осуществляются они за счет того, что все участники подключены к одной сети – блокчейну. Биткоин

или другая криптовалюта не хранятся в каком-то файле. Информация о транзакциях находится в глобальной, общедоступной базе данных – блокчейне. В ней происходит подтверждение и принятие операцией этой крупной P2P-сети. Вся цепь распределена: она поддерживается компьютерами по всему миру. Центрального сервера, который можно было бы сломать или взломать, не существует. Блокчейн публичный и очень надежный одновременно, так как использует зашифрованные данные [4].

2 Область применения

Несмотря на то, что интерес к блокчейн-технологии в большей степени связан скорее с областью финансов, сферы применения технологии распределенных реестров не ограничиваются только ей. Наряду с банками и физтех-стартапами (молодая небольшая техническая компания), игроки других, не связанных с финансовой отраслью рынков, также обратили внимание на технологию и ищут способы извлечения пользы из возможностей, которые она предоставляет [2].

Блокчейн может также найти своё применение в таких областях [5], как:

1. Авторство и право владения.
2. Операции с товарами и сырьем.
3. Управление данными.
4. Цифровая идентичность, проверка подлинности и подтверждение прав доступа.
5. Средства электронного голосования.
6. Организация частного и государственного управления.
7. Интернет вещей.

3 Определение криптовалюты

Криптовалюта [6] — разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах. Как правило, учёт криптовалют децентрализован. Функционирование данных систем основано на таких технологиях как блокчейн, направленный ациклический граф (рис. 2), консенсусный реестр (общий децентрализованный реестр, которым является распределённая база данных о всех счетах [7]). Информация о транзакциях обычно не шифруется и доступна в открытом виде. Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование).

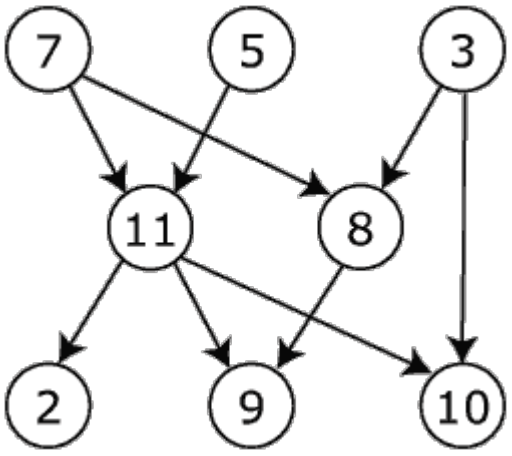

Рисунок 2 – Пример направленного ациклического графа

4 Децентрализация криптовалюты

Децентрализация криптовалюты – это рассредоточенность ее основных ресурсов (данных) по всему миру, с многократным дублированием для предотвращения их потери (рис. 3). Цепочка данных (Блокчейн) не хранится

на каком-то основном сервере, а находится одновременно на множестве компьютерах пользователей по всему миру.

Децентрализацию криптовалюты можно сравнить с файлообменом через торренты. Файл доступен для загрузки в случаях, если хоть один из компьютеров, на которых он скачан и раздается, включен и подключен к интернету. Точно так же и криптовалютная сеть функционирует, если хоть один из компьютеров, хранящих блокчейн, активен. Однако на практике обычно нужен не один компьютер, так как для подтверждения легитимности (согласия) транзакции ее должны подтвердить несколько участников сети.

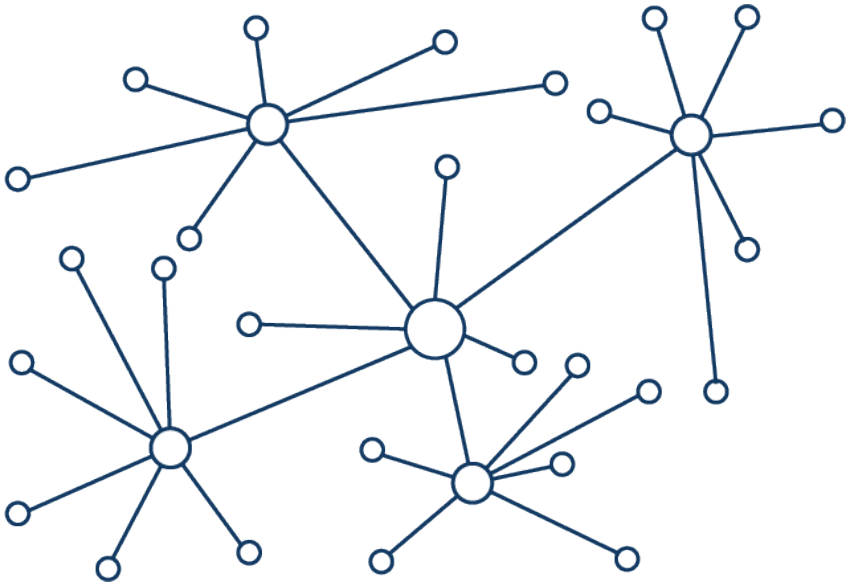

Рисунок 3 – Схема децентрализации криптовалют

5 Метод защиты Proof-of-Work

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса (согласия) в блокчейне; он используется для подтверждения транзакций и создания новых блоков. С помощью PoW майнеры конкурируют друг с другом за завершение транзакций в сети и за

вознаграждение. Его основная цель — это защита сервера от постоянных запросов (DDos-атак, спама) через добавление специальной задачи, на решение которой необходимо потратить определенное количество времени и ресурсов. При этом сервер (или просто валидатор) на проверку будет тратить намного меньше времени. Механизм PoW предназначен именно для вычислительной техники. От него зависит точность и скорость блокчейна. При этом проблема не должна быть слишком сложной — в этом случае генерация блока займет много времени, а значит, в сети «зависнет» много незавершенных транзакций. Если проблема не может быть решена за предсказуемое время, создание блоков станет счастливой случайностью. Майнеры решают задачу, формируют новый блок и подтверждают транзакции. Сложность задачи зависит от количества пользователей, текущей мощности и нагрузки на сеть. Кроме того, хэш каждого блока содержит в том числе хэш предыдущего блока, что повышает безопасность и делает невозможным нарушение порядка созданных блоков. Если майнер сумел решить задачу, формируется новый блок — в нем размещается очередной комплект транзакций, и они считаются подтвержденными [8].

Именно принцип PoW лежит в основе валидации транзакций в блокчейне Bitcoin. Также этот алгоритм консенсуса используется в десятках других криптовалют, в которых есть возможность майнинга, например: Ethereum (ETH), Bitcoin Cash (BCH), Litecoin (LTC), Monero (XMR) и т.д.

6 Метод защиты Proof-of-Stake

Proof-of-Stake, или PoS (Доказательство доли владения) — это альтернативный алгоритм достижения консенсуса, который был разработан сугубо для использования в криптовалютах. Вместо решения криптографической задачи транзакции валидируются (подтверждаются) путем «заморозки» некоторого количества монет майнеров в качестве

обеспечения. Монеты заморожены до тех пор, пока не будет достигнута «договоренность» валидности транзакций. После достижения консенсуса в сети транзакции добавляются в блокчейн, а монеты держатся замороженными еще некоторое время с целью защиты от атаки на сеть и избегания «двойной траты». Когда монеты майнеров разморожены, они получают свои монеты обратно плюс небольшую комиссию за запись транзакций в блокчейн. Такой алгоритм предназначен для того, чтобы отбить охоту у злоумышленников валидировать поддельные транзакции из-за риска потерять «залог». Таким образом, больше шансов сгенерировать следующий блок имеет узел с большим балансом. Схема выглядит достаточно привлекательно прежде всего из-за небольших требований к вычислительным ресурсам, а также потому, что не стоит вопрос «потраченных впустую» мощностей [9].

Алгоритм PoS используется в таких криптовалютах, как: Ripple(XRP), EOS(EOS), NEO(NEO), Stellar(XLM) и т.д.

7 Сравнение Proof-of-Work и Proof-of-Stake

Споры между сторонниками Pow и PoS длятся уже долгое время, но природа этих споров больше теоретическая. Практика показывает, что роль разработчика в вопросах обеспечения безопасности по-прежнему очень высока [10].

В то же время многие считают наиболее безопасным решением гибридный вариант PoS- и PoW-систем. Такой подход уже активно практикуется — у многих криптовалют существует этап PoW, когда валюта выпускается через классический майнинг, и этап PoS, наступающий после завершения эмиссии [10]

У обоих протоколов есть свои преимущества и недостатки. Вроде бы Proof-of-Stake экономически выгоднее и рациональнее с технической точки

зрения, но в таких глобальных платформах как блокчейн Bitcoin или других криптовалютах с миллиардной капитализацией, PoW кажется более надежным вариантом. Еще в 2012-2013 годах на рынке начали появляться монеты с гибридным PoS/PoW протоколом. Среди них Peercoin, Emerecoin, Novacoin и другие [9].

Заключение

Резюмируя всё вышесказанное, можно сделать вывод, что блокчейн со своей децентрализацией позволяет исключить третьи лица из денежных сделок и других областей применения. Что сделает процесс более прозрачным и безопасным.

Но не всё так однозначно. У блокчейна есть и ряд проблем, которые придётся решать:

1. Для полноценного внедрения блокчейна необходимо перестраивать множество отраслей экономики.
2. Чтобы блокчейн и криптовалюты приобрели всеобщее доверие необходима хотя бы какая-то законодательная база.
3. Для поддержки блокчейна, если брать во внимание PoW, необходимо большое количество энергии и вычислительных мощностей.

Но в целом у блокчейна перспективное будущее, так как именного на его технологии планируется развитие цифровой экономики.

Список использованных источников

1. Blockchain для чайников. Технология блокчейн простыми словами — URL: https://cryptonisation.ru/chto-takoye-blokcheyn-prostymi-slovami/ (Дата обращения: 17.05.2019)

2. Блокчейн — URL: https://ru.wikipedia.org/wiki/Блокчейн (Дата обращения: 17.05.2019)

3. Блокчейн биткоина — что это такое, принцип работы — URL:https://tehnoobzor.com/cryptolife/bitcoin/1995-blokcheyn-bitkoina-chto-eto-takoe-princip-raboty.html#sut-tehnologii (Дата обращения: 17.05.2019)

4. Что такое блокчейн простыми словами — URL:https://prostocoin.com/blog/blockchain-guide (Дата обращения: 17.05.2019)

5. 20 областей применения Блокчейн вне финансовых сервисов, ч. 1 — URL: https://habr.com/ru/company/wirex/blog/397999/ (Дата обращения: 17.05.2019)

6. Криптовалюта — URL: https://ru.wikipedia.org/wiki/Криптовалюта (Дата обращения: 17.05.2019)

7. Ripple — URL: https://ru.wikipedia.org/wiki/Ripple#Консенсусный_реестр (Дата обращения: 17.05.2019)

8. Proof-of-Work: Как это работает — URL: https://ru.ihodl.com/tutorials/2018-01-23/proof-work-kak-eto-rabotaet/ (Дата обращения: 17.05.2019)

9. PoW vs PoS – описание терминов, сравнение и отличия — URL: https://prostocoin.com/blog/pos-pow (Дата обращения: 17.05.2019)

10. Что такое Proof-of-Work и Proof-of-Stake? — URL: https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/ (Дата обращения: 17.05.2019)