Знакомство с блокчейн

Блокчейн – это распределённая база данных, которая содержит информацию обо всех транзакциях, проведенными участниками системы.



Блокчейн представляет собой последовательность блоков транзакций, связанных между собой криптографической хэш-функцией, где корректность каждого блока проверяется и подтверждается всеми участниками сети.

Банковская транзакция – это операция с денежными средствами: перевод вывод зачисление и т.д. т.е. любой процесс, связанный с использованием банковских счетов.

Транзакция блокчейна – это операция сохранения данных в блокчейне, в ходе которой происходит передача крипто активов или другой информации между адресами кошельков получателя и отправителя.

Отправка транзакции происходит после её создания и подписания цифровой подписью на основе закрытого ключа.

Крупные компании осваивают блокчейн для того чтобы снизить транзакционные издержки, ускорить прохождение транзакций, снизить риск мошенничества и устранить посредников.

Некоторые фирмы с его помощью пытаются перестроить устаревшие системные сервисы чтобы вывести их на следующий уровень.

Криптовалюта – это разновидность цифровой валюты. Базовый принцип криптовалюты заключается в том, что контроль над созданием каких-то новых транзакций или контроль над перемещением базируется на элементах криптографии.

Криптовалюты децентрализовано учитываются в противовес обычным цифровым. Все функционирование криптовалют основано на технологии блокчейн, которое использует криптографию.

Криптография в криптовалютах используется в основном для обеспечения неизменяемости базы самого блокчейна.

Происхождение блокчейна

Блокчейн впервые появился в криптовалюте в виде BTC в основу которой заложен блокчейн и тем самым представил.

Концепция децентрализованной цифровой валюты витала в воздухе десятилетиями.

Сатоши Накамото в 2009 году представил первую криптовалюту биткоин и тем самым представил практическую реализацию блокчейна.

Он объединил в себе уже известные на тот момент понятия:

1. Криптографическая система с открытым ключем
2. Алгоритм консенсуса Proof of work – данный алгоритм появился впервые как решение проблемы на электронной почте. Блокчейн стал той недостающей частью интернет революции, которая превращает уязвимую систему обмена ценностями в криптографический защищенную

Банковская система отстала от технологической революции. Банки создали централизованные организации, которые хранят транзакционные записи, контролируют взаимодействие, обеспечивают доверия и безопасность и регулируют всю систему. Вся коммерция опирается на эти финансовые учреждения, которые служат доверенными посредниками при обмене.

Что такое блокчейн?

Блокчейн – система записей о переносе любой ценности. Это означает что нет необходимости в посреднике, который служит доверенной третьей стороной при обмене ценностей.

Транзакции с использованием посредника

Транзакции с использованием блокчейна



Блокчейн – одноранговая система передачи ценностей без участия третьей доверенной стороны. Это общий децентрализованный и открытый реестр транзакций.

База данных реестра работает только в режиме добавления записей, и не может быть изменена или исправлена. Это означает, что каждая запись является постоянной и неизменяемой. Любая новая запись появляется во всех копиях базы данных, размещённых на разных узлах.

Нет необходимости, чтобы доверенные третьи стороны выступали в качестве посредников для проверки обеспечения безопасности и подтверждения транзакций.



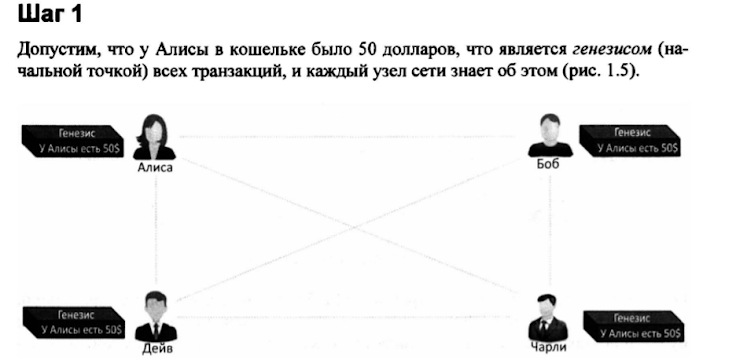
Первый блок цепочки – Генезис. Генезис-блок – самый первый блок распределительного реестра, который является основой и прототипом для создания всех остальных блоков.

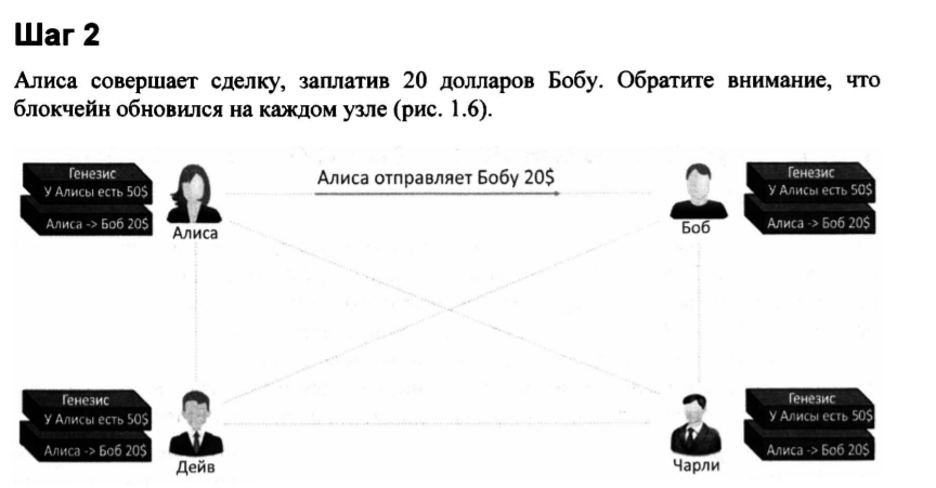
Блокчейн-сеть состоит из большого количества узлов. Каждый узел в сети имеет идентичную копию блокчейна. Каждый блок – совокупность транзакций и связь с предыдущим блоком.

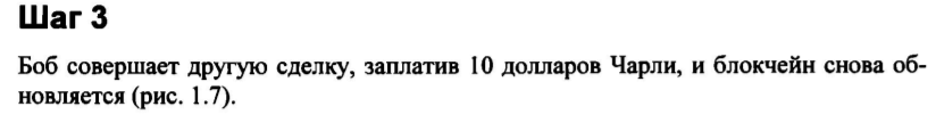
Каждый блок состоит из двух частей: заголовка и тела блока. Заголовок ссылается на предыдущий блок в цепочке. Каждый заголовок содержит хэш предыдущего блока. Поэтому никто не может скрытно изменить транзакцию в предыдущем блоке. Тело блока содержит список проведенных транзакций.

Пример:

Есть 4 участника, которые проводят транзакцию между собой в сети блокчейна.





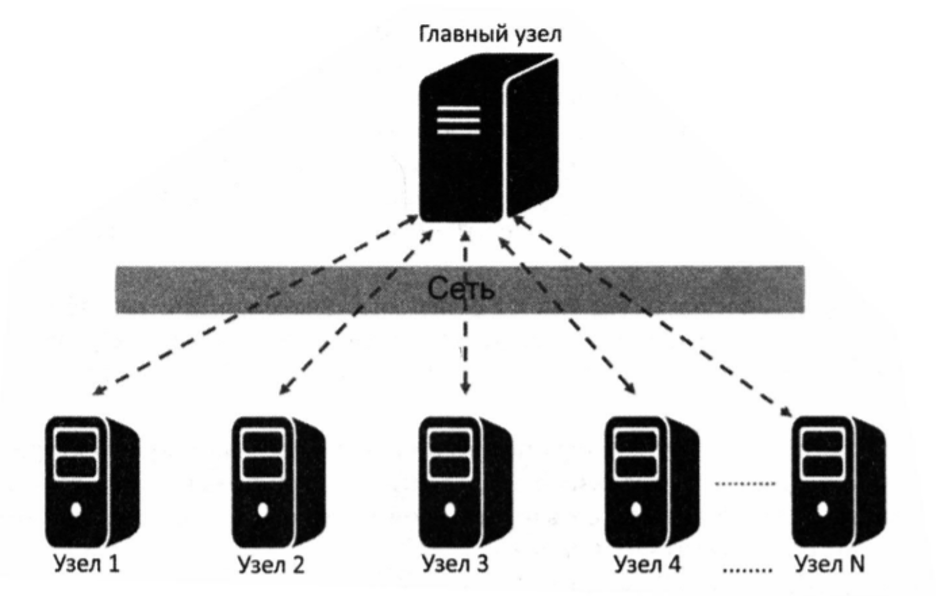


Данные транзакции в блоках неизменяемы. Все транзакции полностью необратимы. Любое изменение создаст новую транзакцию, которая будет подтверждена всеми участниками сети, а старая просто остается на месте. У каждого участника сети есть своя копия блокчейна.

Централизованные и децентрализованные системы

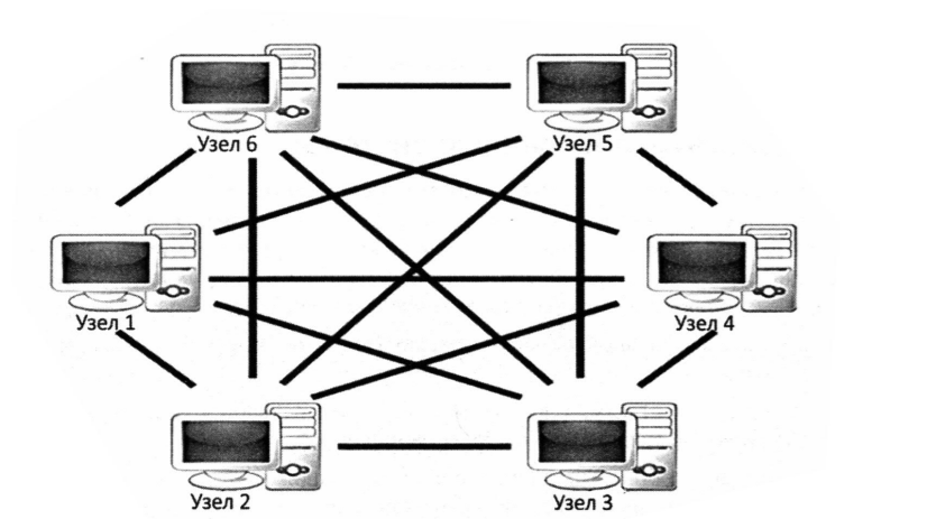
Независимо от того, централизована или децентрализована система – её все равно можно распределить.

Централизованная распределенная система – это такая система, в которой есть главный узел, ответственный за дробление задач и данных, а также распределение нагрузки между узлами.



Децентрализованная распределенная система – система, где нет главного узла как такового, но все же, вычисления могут быть распределены.

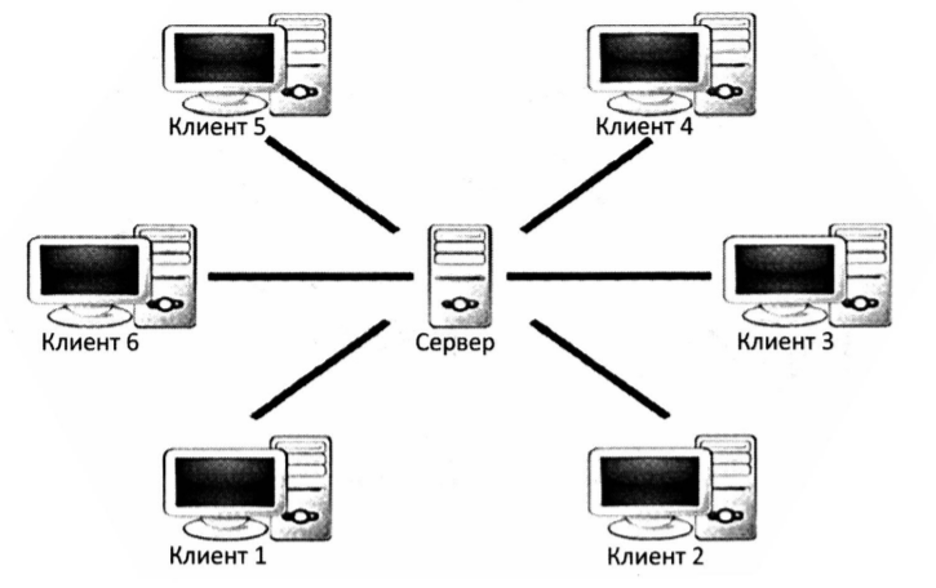
Децентрализованная система каждый с каждым



Централизованные системы

Централизованная система имеет централизованное управление со всеми административными полномочиями. Такие системы легко разрабатывать, поддерживать, навязывать им доверие и управлять ими. Но, они страдают от многих неотъемлемых ограничений. А именно:

1. У них есть центральная точка отказа, поэтому они менее стабильны.
2. Они более уязвимы для атаки, следовательно, менее защищены.
3. Централизация власти может привести к неэтичным действиям.



Децентрализованные системы

Децентрализованные системы не имеют центрального органа управления и каждый её узел равноправен. Такие системы сложно разрабатывать, поддерживать, управлять, или навязывать им доверие. Они не страдают от ограничений от ограничений обычных централизованных систем.

Преимущества децентрализованных систем:

1. Нет центральной точки отказа, поэтому они более стабильные и отказоустойчивы.
2. Устойчивость к атакам, так как они не имеют центральной точки, доступной для легкой атаки, следовательно, более защищены
3. Симметричная система с равными полномочиями

Ограничения централизованных:

1. Проблема доверия
2. Проблема безопасности
3. Проблема кофиденциальности

Преимущества децентрализованных систем:

1. Устранение посредников
2. Прозрачность
3. Проверка транзакций
4. Меньшие затраты и большая безопасность
5. Отсутствие уязвимого центра