

Блокчейн – технология будущего.



Технология Блокчейн
– это изобретение **Сатоши Накамото**,
создателя криптовалюты Биткоин
(2008 г)



Определение blockchain состоит из двух элементов:

- «Block» переводится, как блоки.
- «chain» — цепочка.



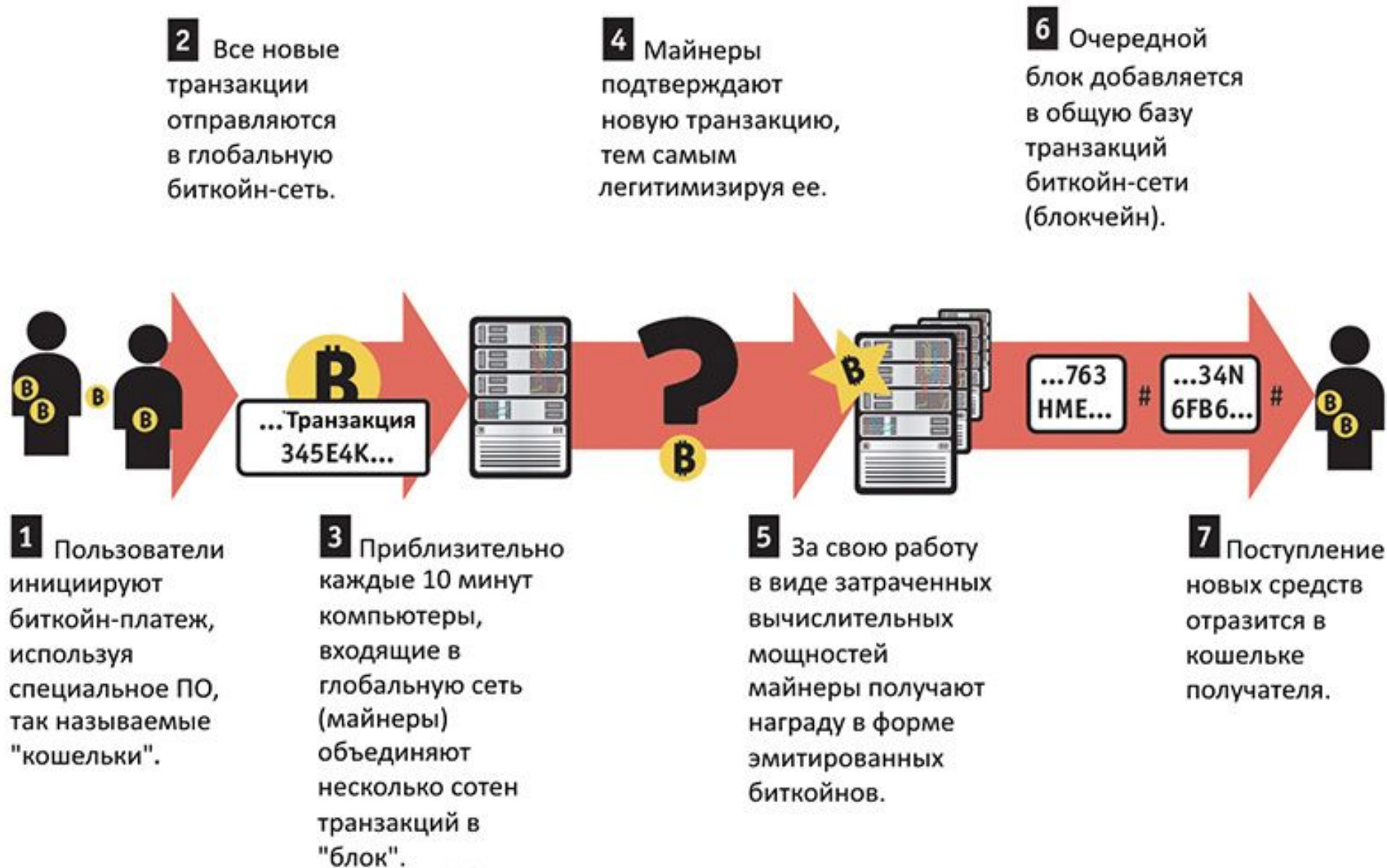
Что такое блокчейн Биткойна

Блокчейн Биткойна — это непрерывная цепочка блоков, которая построена с учётом конкретных правил и содержит информацию о проведённых транзакциях в сети.

Чаще всего копии цепей блоков, которые не зависят друг от друга находятся параллельно, а их обработка производится с различных ПК.



Как работают транзакции в blockchain на примере биткоина



Блокчейн по сути состоит только из истории транзакций. Он не хранит баланс каждого кошелька, иначе бы нам пришлось изобретать дополнительные способы защиты



Биткойн кошелек

1. Интерфейс
2. Файл с ключами
3. База данных всех блоков за все время

Одноранговая p2p сеть



Любой блокчейн существует только пока существуют его **майнеры**, которые решают вычислительные задачи.

Эти задачи должны быть достаточно простыми, чтобы у участников сети была стабильная вероятность найти ответ — иначе транзакции будут подтверждаться вечно.



Майнинг — это когда тысячи компьютеров по всему миру гудят по подвалам, перебирая миллионы чисел в секунду, пытаясь подобрать хеш, начинающийся на 10 нулей

За нахождение ответа компьютер (по данным на 2017 год) получает **12.5 BTC** — это сумма вознаграждения, которая генерируется системой биткоин «из воздуха» и уменьшается каждые четыре года.



Майнеры, которые добывают виртуальные деньги, используют для этих целей **процессоры, видеокарты и другое оборудование**. Последнее берёт на себя опцию вычислений для поиска хеша. После её подбора происходит закрытие блока.

Цепочка блокчейн распределена и поддерживается миллионами компьютеров по всей планете.



Надёжность работы цепочки блокчейн обеспечивают специальные алгоритмы:

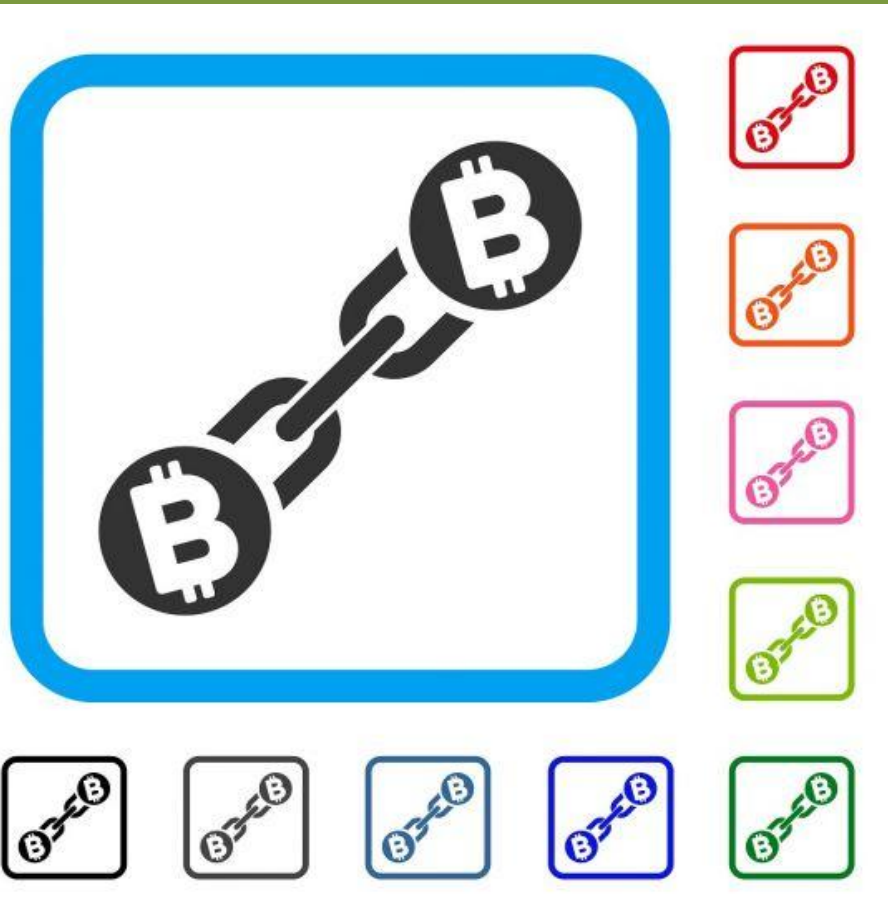
Proof-of-Work

Proof-of-Stake

В блокчейне Биткойна применяется первый вариант. Принцип его действия схож с процессами, которые происходят в офисе. Если сотрудник организации не выполнил поставленную работу, ему не выдадут заработную плату. Алгоритм PoW выполняет проверку расчётов, которые делаются при создании элементов цепи. Система признаёт блок в случае, если параметр его хеша ниже подписи, поиском которой занимались майнеры. Иными словами, правильность блока вычисляется по специальному шифру, а контроль работы возлагается на полные узлы. На формирование блока в цепи блокчейн уходит 10 минут. За это время майнеры, участвующие в добыче криптовалюты, находят подпись, а проверка выполняется без задержек по времени. Недостаток алгоритма в том, что для обеспечения его функционирования требуются огромные мощности. Как результат, за проведение транзакций взимаются комиссии. Что касается Proof-of-Stake — это обновлённый алгоритм, но применяется он в блокчейне Эфириума.



Виды блокчейна



Публичный — цепочка блоков, которая доступна другим пользователям. Этот тип цепи применяется в Биткоине

Сервисный — цепочка блоков доступна всем пользователям, но их количество ограничено.

Приватный — цепочка, где доступ к чтению и записи ограничен. Здесь доступна установка приоритетных узлов. В таком блокчейне участвует ограниченная группа лиц, которые занимаются обработкой операций.



Плюсы блокчейна

Децентрализация. Участники сети имеют равные права и способны обмениваться сведениями непосредственно друг с другом, без участия посредников.

Надёжность. Вероятность взлома злоумышленниками или замена информации в блоках исключена, что обусловлено применением шифрованных ключей.

Прозрачность. Блоки цепочки блокчейн открыты для пользователей, а транзакции легко проверить.

Универсальность. Блокчейн — уникальная технология, которая может применяться не только в финансовой сфере, но и в других областях.

Высокая скорость. Возможности блокчейн-технологии позволяют снизить время транзакций до одной минуты.

Низкие комиссии. Благодаря отсутствию комиссионных платежей, транзакционные сборы минимальны.



Минусы блокчейна

Невозвратность. Отменить операцию, если она проведена по ошибке, не получится.

Риск атаки. Если 51 процентом цепи Биткойна будет владеть один пользователь, целостность сети может быть нарушена.

Масштабируемость. При текущем размере блока система обрабатывает до семи операций за 1 секунду. С ростом числа пользователей этого показателя становится мало.

Неопределенность статуса. Многие страны никак не определятся с применением технологии, а вопрос регулирования криптовалюты открыт до сегодняшнего дня.



Сферы применения

Технология блокчейн может использоваться не только в финансовом мире, но и ряде других сфер жизни:

- Для защиты авторства и идентификации личности.
- При голосовании.
- В юриспруденции и управленческой деятельности
- В секторе недвижимости
- На бирже и в сфере услуг и др.



Итак, **Блокчейн** — одна из самых важных инноваций со времен создания Интернета.

Возможности технологии Блокчейн обширны и могут навсегда изменить мир к лучшему, затрагивая **все сферы жизни.**



СПАСИБО !

