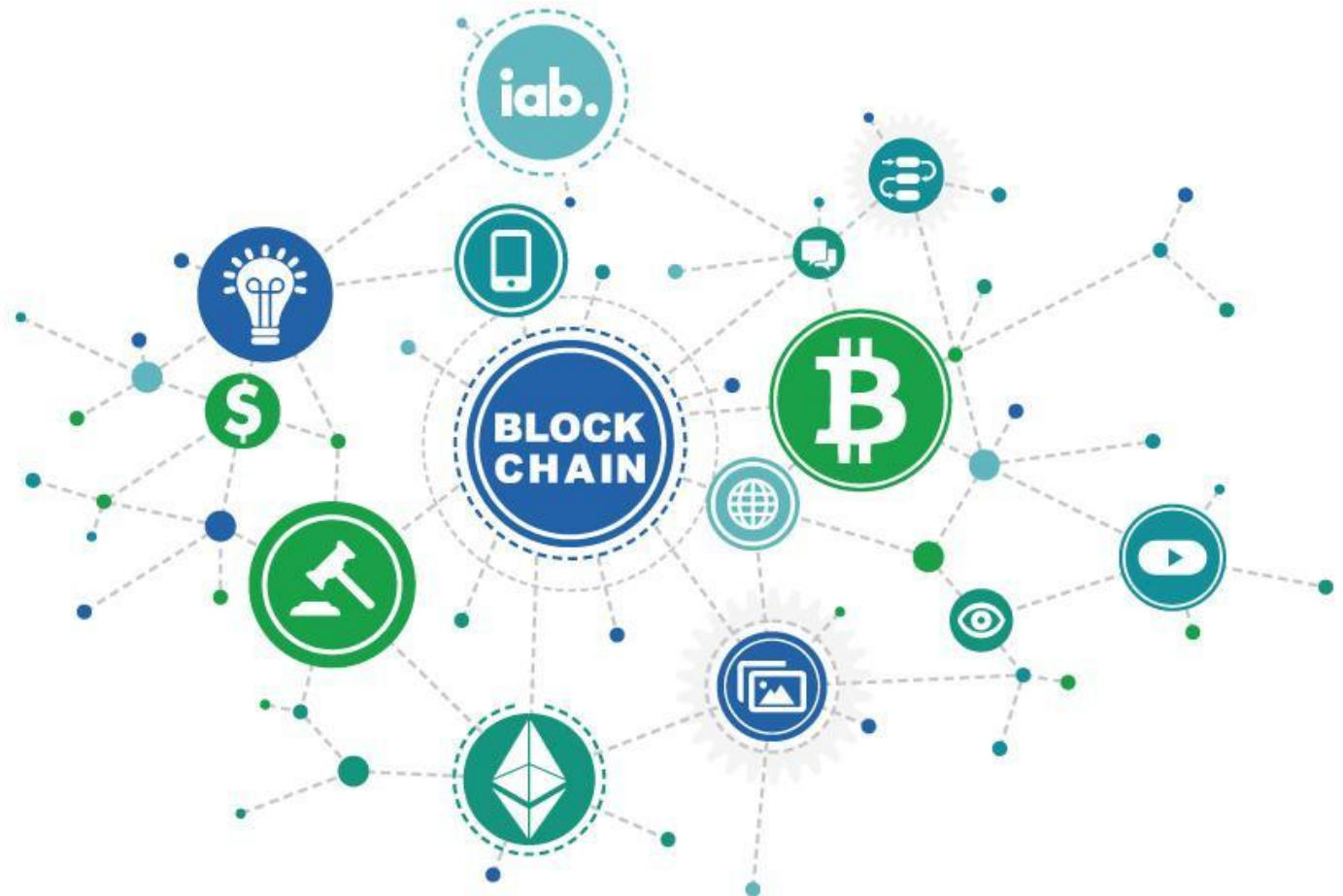


ТЕХНОЛОГИЯ БЛОКЧЕЙН

Блокчейн (цепочка блоков) — это распределённая база данных, у которой устройства хранения данных не подключены к общему серверу. Эта база данных хранит постоянно растущий список упорядоченных записей, называемых блоками. Каждый блок содержит метку времени и ссылку на предыдущий блок.



Как это работает:



Хеш и нонс



Хэш - это результат работы хэш-функции. Ее можно себе представить неким черным ящиком — шифратором. Это сложный калькулятор, который вычисляет сумму всех входных данных, которые попадают в него. Или проще говоря абракадабра из 64-значных ключей в шестнадцатеричной системе исчисления, используется алгоритм шифрования SHA256

Нонс — это некое число, которое помогает майнерам добывать валюту, являясь тем самым предметом компьютерной "гонки"

Пример:

Dd679c0b9fd408a04148aa7d30c9df393f67b7227f65693fffe0ed6d0f0ade59 (0000) – привет

2502d4993c48d78e45bb3bd59ba24f5cefeaa7696b316cc4136f8b93b88b69b8 (0000)

группа менеджмента самая лучшая

КАК РАБОТАЕТ БЛОКЧЕЙН (НА ПРИМЕРЕ КРИПТОВАЛЮТЫ)

1

А хочет перевести деньги В



2

Транзакции передаются в сеть и собираются в «блоки», каждый «блок» имеет номер и хеш предыдущего «блока»



3

«Блоки» рассылаются всем участникам системы для проверки



4

Если ошибок нет, каждый участник записывает «блок» в свой экземпляр базы данных



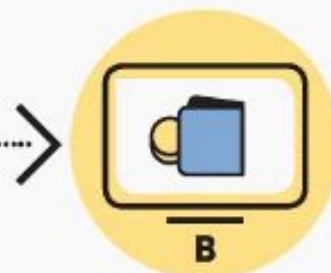
5

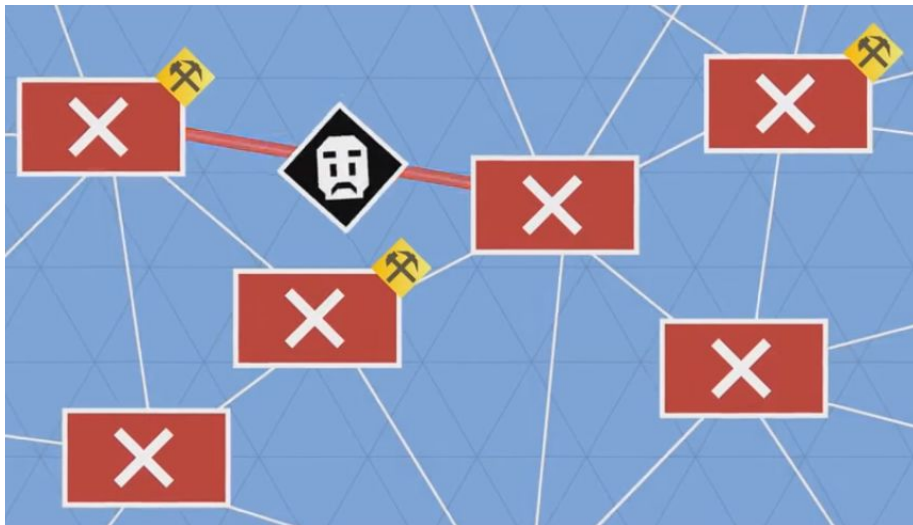
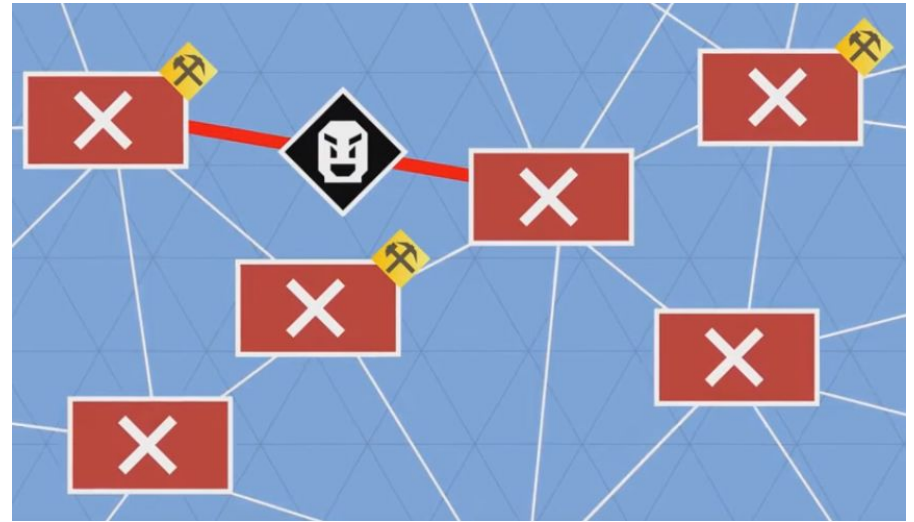
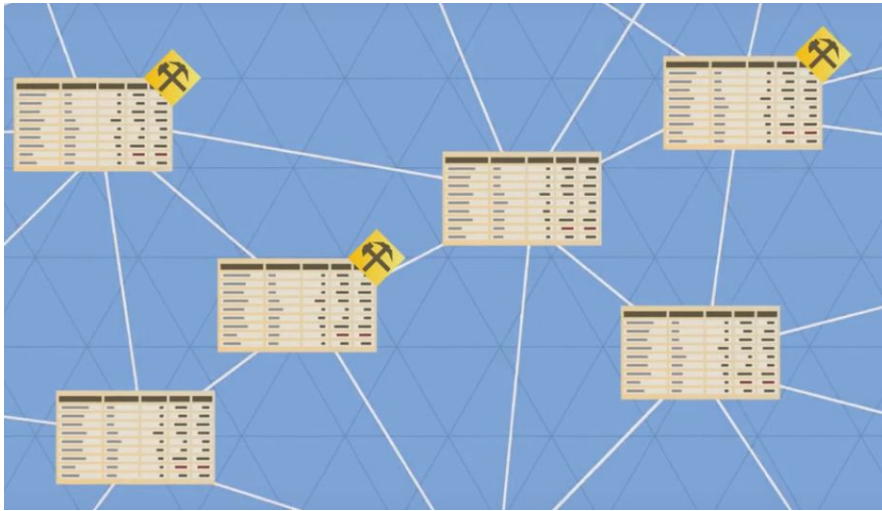
Теперь «блок» может быть добавлен к «цепочке блоков», которая содержит информацию обо всех предыдущих транзакциях



6

Деньги переведены от А к В





В чём важность технологии блокчейн?



В настоящее время уже существует ряд расширений для разработки бизнес-приложений на блокчейн, обеспечивающих:

- 1 Безопасное администрирование сетей, исключающее хакерские атаки MITM («человек посередине») и снимающее проблему «единого администратора»;
- 2 хранение цифровых сертификатов, делающее полностью защищенным доступ пользователей к сайтам (в частности, исключая перехват паролей);
- 3 безопасные двусторонние сделки без привлечения гарантирующей третьей стороны (юридической фирмы, нотариуса, банка и др.); фиксацию времени размещения документов, позволяющую решать вопросы патентования, авторского права и др.;
- 4 подтверждение подлинности продукта (товара) с помощью надежно защищенного сертификата
- 5 подтверждение прав на любую собственность;
- 6 создание общедоступных электронных визиток, информация на которых автоматически обновляется даже после «раздачи» по интернет-ресурсам;
- 7 систему DNS, неуязвимую для DDOS-атак,

Второй по капитализации проект среди всех публичных криптовалют. Основной идеей «Эфириума» является использование умных контрактов — записей, содержащих условия выполнения определенных действий.



Во многом похож на уже рассмотренный нами Ethereum и является платформой для разработки различных блокчейн-проектов. Однако, в отличие от Эфириума, данный стартап ставит во главу угла скорость обработки транзакций: подтверждение действия в системе занимает считанные секунды



nem

Японский Ripple — главный конкурент проекта NEM. Использование блокчейна Ripple позволяет банкам существенно снизить транзакционные издержки и сократить время прохождения денежных переводов по всему миру.

