

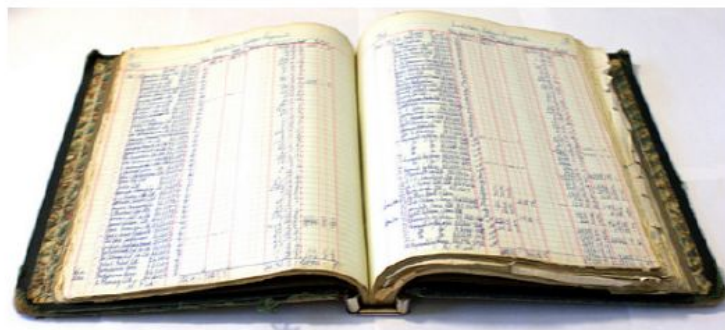
Технология «БЛОКЧЕЙН»

РАССКАЖУ ВСЁ О ЧЁМ ВЫ ХОТЕЛИ ЗНАТЬ, НО БОЯЛИСЬ СПРОСИТЬ ;)

Определение

Блокчейн

Технология создания распределенных реестров, позволяющая любому участнику коммерческой сети видеть всю систему учета



Реализация и преимущества

Закрытый (permissioned)

Выбранные участники

Несколько владельцев

Высокая скорость

Ориентирован на организации

Открытый (permissionless)

Доступ к системе разрешен любому

Отсутствие владельцев

Непредсказуемая скорость

Ориентирован на потребителей

Основные составляющие

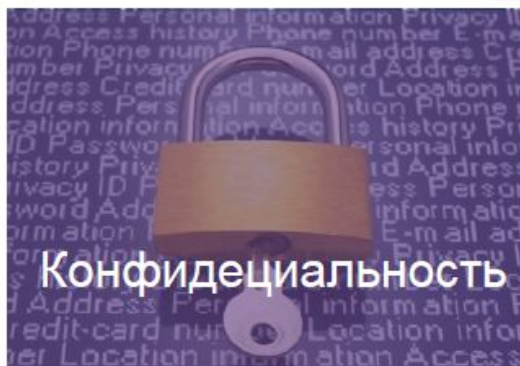
Добавление записи в
распределенную
бизнес-сеть

Общая книга
учета



Обеспечение
надлежащей видимости;
Безопасные,
аутентифицированные и
проверяемые

Конфиденциальность



Smart
контракт



Коммерческие
условия включены в
транзакции и
выполняются с
операциями

Консенсус



Все стороны сети
подтверждают
подлинность
транзакции

Темы для изучения

- Децентрализация (равноправные участники)
- Распределенная проверка (отсутствие доверия)
- Шифрование (использование маркеров безопасности)
- Bitcoin (*Blockchain 1.0*)
- Ethereum (*Blockchain 2.0*)
- Децентрализованные приложения

Принципы

Платформы

Индивидуальные
решения

Что такое децентрализация?



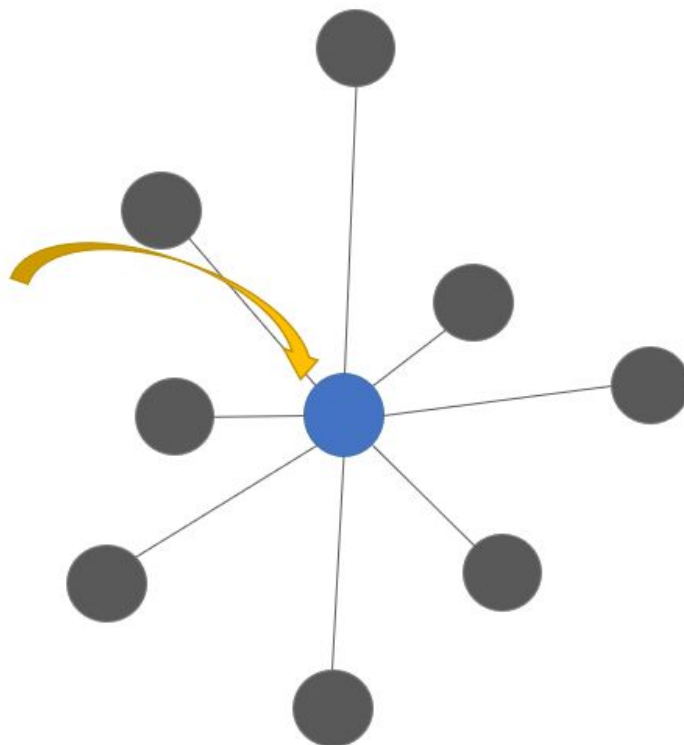
Распределенная
централизованная
структура



Распределенная
децентрализованная
структура

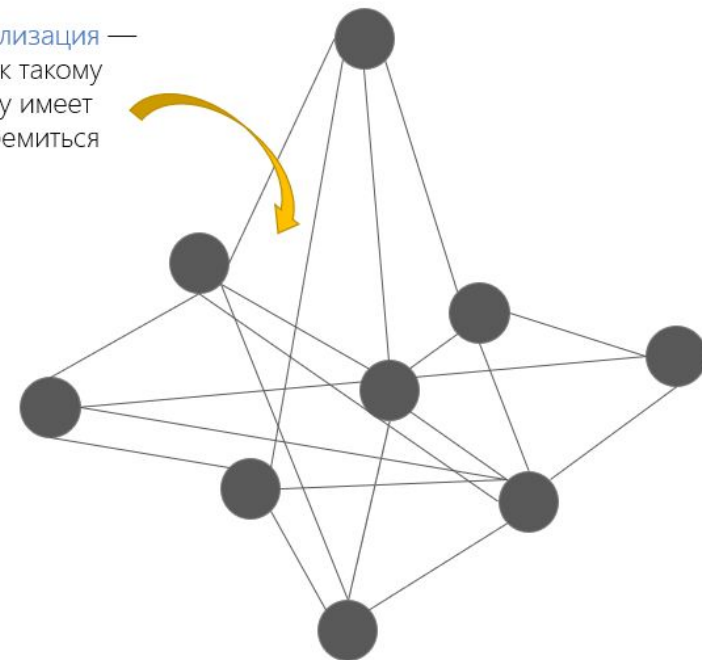
Выбираем?

- Одна точка управления
- Одна точка отказа
- Одна точка доверия
- Одна точка атаки
- Система с одним узким местом



- Не используется центр управления
- Используется согласие равноправных участников

Децентрализация —
пожалуй, к такому
устройству имеет
смысл стремиться



* Decentralized
* Peer-to-peer technology

Децентрализация – это ещё не всё

Отсутствие доверия означает,
что стороны, не доверяющие
друг другу, могут сотрудничать,
не привлекая при этом
доверенную третью сторону
или центр

Заменить доверие на шифрование

Нужна электронная платежная система, основанная на криптографическом подтверждении вместо доверия. Это даст возможность любым двум желающим сторонам проводить между собой прямые транзакции без необходимости привлекать третью сторону.

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System | Oct 31, 2008



Основы криптографии

Как отправлять секретные сообщения по проводной сети, если за тобой следит старуха Шапокляк?

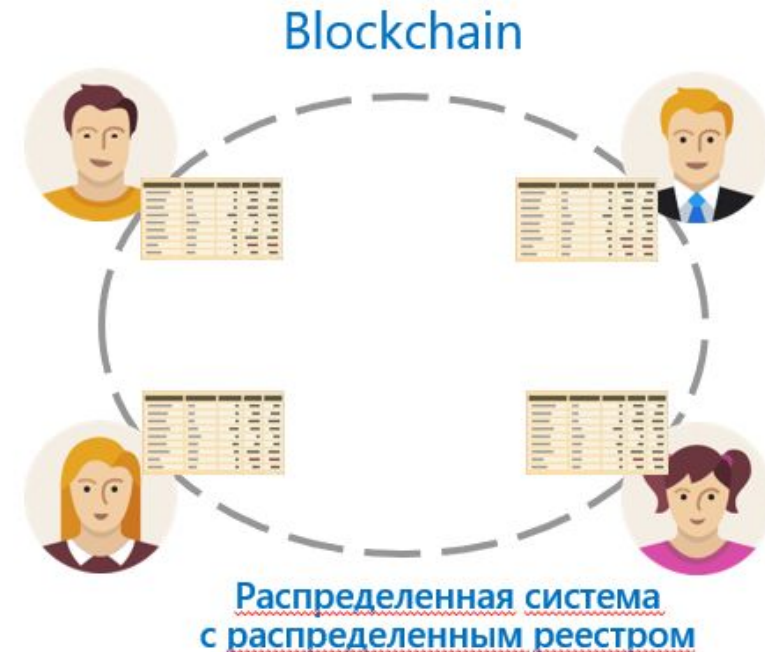


Электронная подпись

- Объединение алгоритмов хеширования и шифрования с использованием открытого ключа.
- Подтвердить, что содержание полученного сообщения не изменилось с момента его отправки.
- Подтвердить, что полученное якобы от Гены сообщение действительно было отправлено Геной, а не другим крокодилом.

Blockchain децентрализует данные в ненадежной среде

- Традиционная модель взаимодействия между контрагентами предполагает использование централизованного реестра и помощь посредников для подтверждения и регистрации транзакций.
- Blockchain обеспечивает безопасное распределение реестра по всей сети и позволяет обойтись без посредников.
- Технология поддерживает создание множества копий данных о транзакциях по принципу технологии p2p файлообмена.
- Технология Blockchain заменила **ДОВЕРИЕ** на **КРИПТОГРАФИЮ**, убрав посредников в ненадежной среде.



Консенсус используется для добавления блоков в блокчейн

- Транзакции, еще не размещенные в блоке, называются «неподтвержденными» (или «неупорядоченными») транзакциями.
- Чтобы определить следующий блок, Blockchain использует механизм консенсуса. Он позволяет заменить посредников для гарантии подлинности и надежности транзакции.
- Существует несколько типов механизма консенсуса, например «доказательство выполнения работы» (Proof of Work, POW) и «подтверждение доли» (Proof of Stake, POS).
 - Процесс предоставления доказательства называется «майнинг».
- В Blockchain 1.0 используется POW. В его основе лежит решение сложной математической задачи. Предоставление доказательства выполнения работы может быть случайным процессом с низкой вероятностью, для получения нужного результата в котором требуется много проб и ошибок.
- В Blockchain 2.0 используется POS (альтернатива POW). В основе POS — не сложные вычислительные задачи, а права владения цифровыми активами. Другими словами, узел, владеющий 1 % цифрового актива, обеспечивает майнинг 1 % блоков.
- Как только транзакции подтверждены с помощью механизмов консенсуса, информация сохраняется в новый блок.