Основные тренды технологии blockchain

Спикер: Максим Аверин

О себе

- Делаю коммиты в open-source проект Zulip (чат от Dropbox)
- Разработчик в EtherionLab

Проблемы централизации

- Один сервер - слишком много власти в руках одной организации
- Велик риск взлома и кражи данных
- Нужно доверять управляющей организации

Что сулит криптоэкономика?

- Уничтожение нотариата
- Отказ от использования бумаги при документообороте
- Адвокаты останутся, а юристы вымрут
- Нагрузка на судей сократится
- Все бизнес-процессы, не связанные с творчеством, станут автоматизированными

Что такое блокчеин?

Блокчейн – это, как понятно из названия, цепочка блоков.

Таким образом, большая бухгалтерская книга выглядит как цепочка блоков.

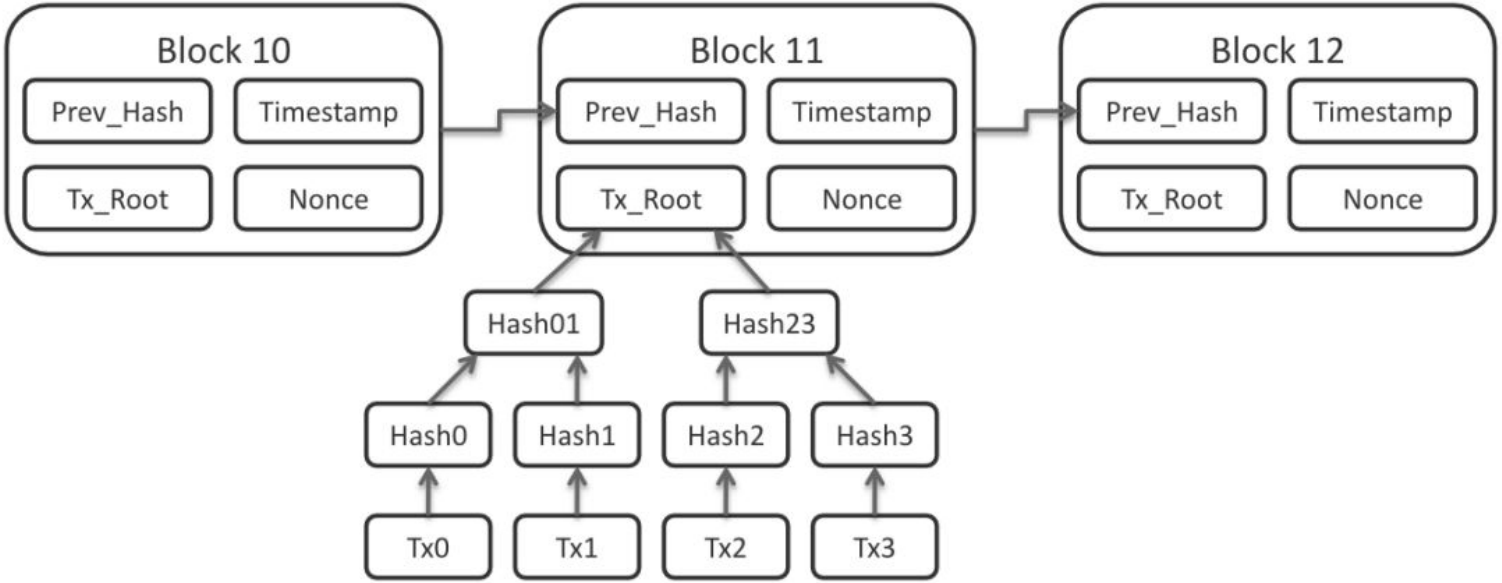
Принципы построения цепочки блоков

- Распределённость
- Открытость
- Защищенность

Децентрализованная книга учета

- Пусть теперь каждый хранит книгу балансов у себя
- Участники сети обмениваются данными о транзакциях
- Проверка корректности транзакций использует цифровую подпись

Blockchain


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Что такое биткоин?

Биткойн – это первая в истории человечества децентрализованная платёжная система, созданная в 2009 г.

По совместительству – ещё и валюта. Но это скорее побочный эффект.

Чем биткоины удобнее обычных денег?

Вы много знаете способов перевести 160 миллионов долларов из произвольной точки Земли в произвольную точку Земли за 10 минут без комиссии?

Вы много знаете способов перевести друг другу средства, при которых вас не попросят предъявить паспорт? При которых об этом вообще никто не узнает, кроме вас двоих?

Об авторе

Автор системы Биткойн называл себя Satoshi Nakamoto.

Имя Satoshi переводится с японского как «мудрый».

Фамилия Nakamoto – как «находящийся внутри сложной (закрытой) системы».


HELLO?
YES, THIS IS SATOSHI
quickmeme.com

Получается, что печать биткоины можно бесконечно?

Почти.

Сейчас какой-то счастливчик раз в 10 минут добывает

12,5 BTC. Протокол устроен так, что «награда за нахождение блока» раз в 4 года уполовинивается.

Первые 4 года (янв. 2009 – янв. 2013) награда составляла 50 BTC.

Получается, что печать биткоины можно бесконечно?

В действительности всё не так, как на самом деле. Уполовинивание награды происходит не раз в 4 года, а спустя каждые 210 000 блоков.

Это, если мощность майнеров сильно не растёт, почти одно и то же (блоки добываются в среднем раз в 10 минут, а 4 года разделить на 10 минут равно 210384).

Кто умеет суммировать геометрическую прогрессию?

$$50 \cdot 210000 + 25 \cdot 210000 + 12{,}5 \cdot 210000 + \ldots$$

Да, детка!

S = 210000 * 100 = 21 000 000

Суммарно будет добыто 21 миллион биткойнов. Больше добыто не будет. Протокол неизменяем.

Дефляция и инфляция

- Количество биткоинов, как и золота ограничено
- Цена биткоина зависит только от внешних событий
- Сейчас доллар не подкреплён золотом
- Инфляция может привести к ситуации в Зимбабве

Как устроен обычныи платеж?

– Переводишь деньги с адреса 1KeatDCtrEnzaR42B2eUduYXmcM4U9jphB на адрес 1FTgzPJCbpCWYfF6VxPdmCMPUDBfygut2h

– Продавец спустя некоторое время соглашается с тем, что платёж произошёл, и предоставляет тебе услугу. Принято дожидаться **6** подтверждений.

Как устроен обычныи платеж?

Каждый конкретный продавец решает сам, какого количества подтверждений ему ждать. Некоторые биржи считают биткойны зачисленными после **трёх** подтверждений.

Сколько всего людеи держат полную ноду?

Веб-сайт bitnodes.21.co сообщает нам, что на момент написания этой презентации активных полных нод было 6153.

То есть полная копия всего блокчейна хранится как минимум в 6153 местах на планете Земля.

Чему равна комиссия в сети Биткоин?

Либо 0 BTC, либо 0.0001 BTC.

В переводе на российские реалии: либо 0 рублей, либо примерно 5 рублей.

Чем больше сумма перевода и чем более давно с этой суммой ничего не происходило, тем выше вероятность того, что комиссия составит 0 рублей.

Зачем нужна комиссия?

Комиссия нужна для того, чтобы мы с вами не хулиганили: чтобы, гоняя одни и те же монеты по кругу, не забивали сеть.

Достаётся она майнерам. Майнеры – это те, кто занимается майнингом. Каждый может стать майнером.

Истории

- Пицца стоимостью 12 миллионов долларов
- Писавший в 2009 курсач в универе по электронным валютам норвежский счастливчик
- Выброшенный на помойку жёсткий диск в Лондоне

Из чего состоит биткоин-кошелек?

Наивно, он состоит из двух строк:

публичного ключа и *приватного ключа* (public key, private key)

Богатые биткоин-адреса

	Address	Balance Δ1w	% of coins	First In	Last In
1	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v	128,440 BTC ($159,717,800 USD) +0.00018628 BTC	0.7894%	2015-10-16 17:43:06	2017-04-14 15:15:01
2	1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy	124,178 BTC ($154,418,115 USD) +0.0001 BTC	0.7632%	2016-08-23 11:09:04	2017-04-14 15:08:52
3	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	101,361 BTC ($126,044,423 USD) -16,377 BTC	0.6230%	2017-01-05 15:34:15	2017-04-18 09:49:51
4	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	79,957 BTC ($99,428,509 USD) +0.00876429 BTC	0.4914%	2011-03-01 13:26:19	2017-04-15 08:36:22
5	1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx	69,370 BTC ($86,263,274 USD)	0.4263%	2013-04-10 00:03:36	2016-11-12 06:16:46
6	16ZbpCEyVVdqu8VycWR8thUL2Rd9JnjzHt	66,651 BTC ($82,881,502 USD)	0.4096%	2013-11-26 07:06:12	2016-11-14 02:32:38
7	1KiVwxEuGBYavyKrxkLncJt2pQ5YUUQX7f	66,583 BTC ($82,797,723 USD)	0.4092%	2013-11-23 02:02:38	2016-02-13 09:40:01
8	1PnMfRF2enSZnR6JSexxBHuQnxG8Vo5FVK	66,452 BTC ($82,634,625 USD)	0.4084%	2013-11-22 22:06:31	2016-02-13 09:40:01

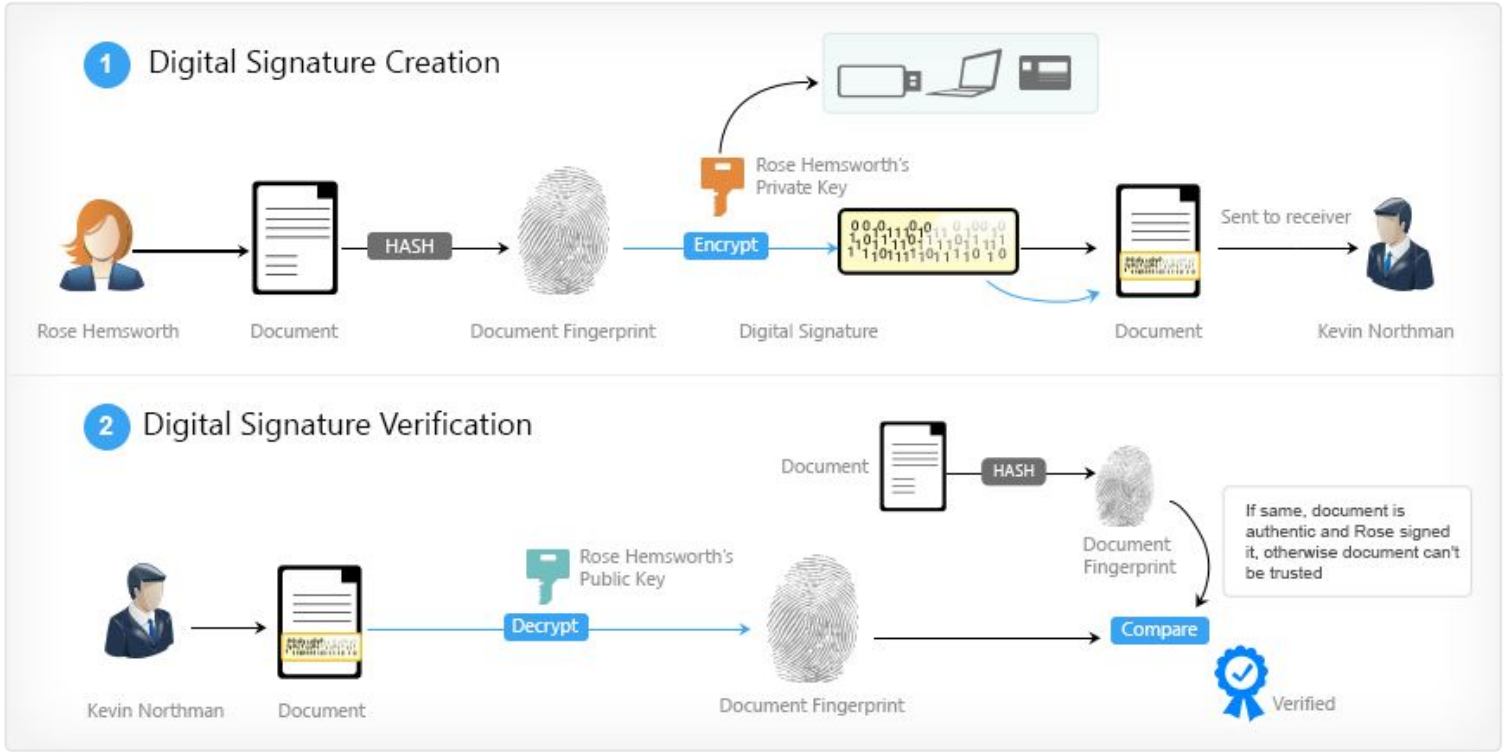
Как обзавестись биткоинами?

- Принимать в дар (обнародовать свой публичный ключ и сказать людям «пересылайте деньги по этому адресу»)
- Принимать в качестве оплаты за услуги
- Заняться майнингом (нереально в 2017 году)
- Открыть сайт любой биржи и купить

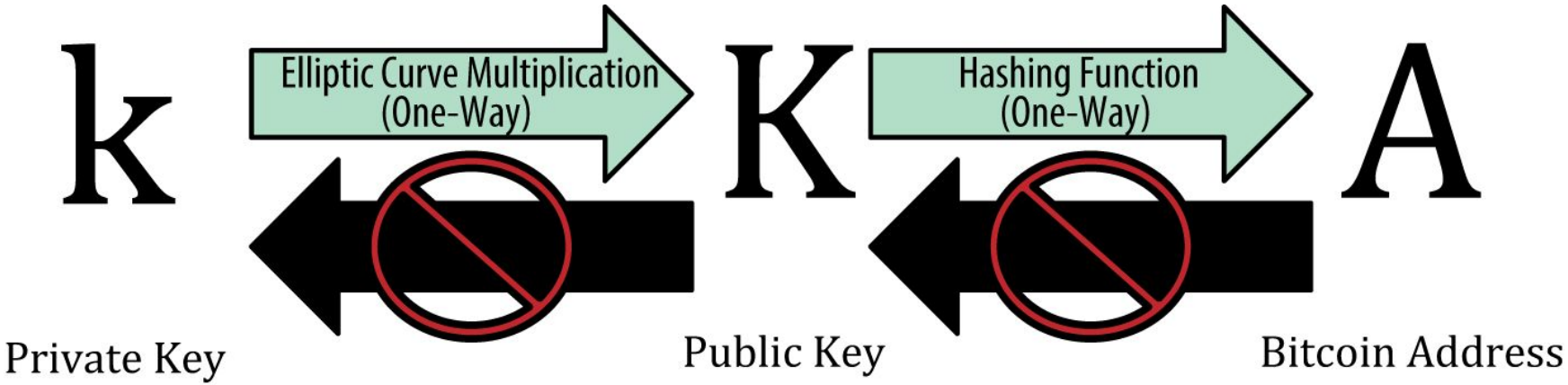
Как оповестить сеть о новои транзакции?

- Децентрализованного способа нет
- Есть доверенные адреса:
  - bitseed.xf2.org
  - dnsseed.bluematt.me
  - seed.bitcoin.sipa.be
  - dnsseed.bitcoin.dashjr.org
  - seed.bitcoinstats.com

Электронная подпись



О шифровании



Немного про хэш-функции

Хэш-функцией называется функция, берущая на вход строку произвольной длины и возвращающая строку фиксированной длины, удовлетворяющая трём свойствам:

- Невозможность восстановить input (исходную строку, исходный файл) по output’у
- При незначительно отличающемся input’е совершенно разный output
- Отсутствие коллизий

Немного про хэш-функции

К примеру, SHA3-хэш от "Saturday" даёт c38bbc8e93c09f6ed3fe39b5135da91ad1a99d397ef1694860 6cdcbd14929f9d.

В то время как та же хэш-функция SHA3, взятая от "Caturday", приводит к результату b4013c0eed56d5a0b448b02ec1d10dd18c1b3832068fbbdc65b98fa9b14b6dbf.

Маининг

Майнер перебором ищет такое число nonce (от английского «number used once»), что

hash(nonce) < target

nonce – случайное число

target – 256-битное число, начинающееся с очень большого количества нулей, прямо связанное со сложностью майнинга (target = const/difficulty)

Маининг (на самом деле)

Майнер перебором ищет такое число nonce (от английского «number used once»), что

sha256(sha256(version|hash_prev|merkle_root_hash|timestamp|bits|nonce)) < target

где | обозначает оператор конкатенации

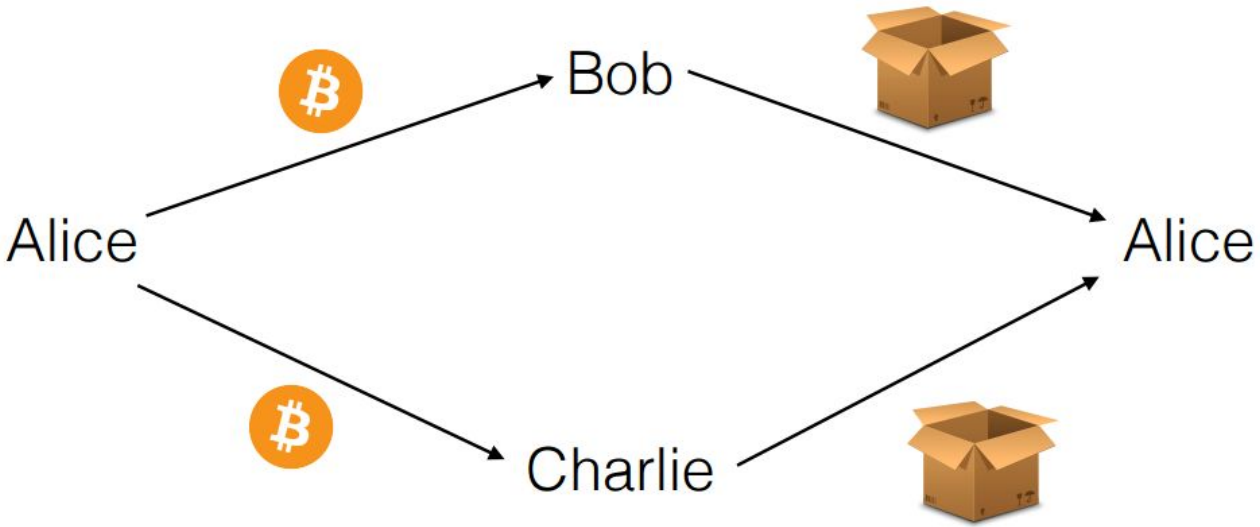
Сложность

Самое главное, что нужно знать – что сложность вычислений подстраивается так, чтобы какой-то счастливчик «находил блок» раз в 10 минут.

Заработок маинера

- Вознаграждение за блок
- Комиссии

Атака «двоиная трата»

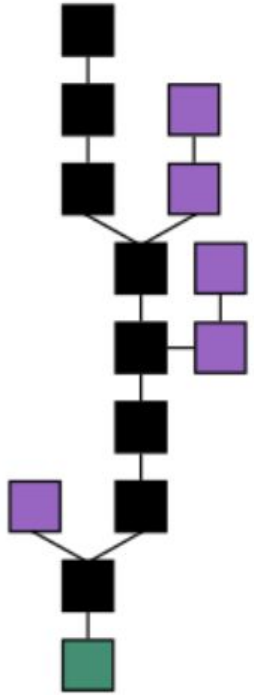


Атака «двоиная трата»

- Изменить размер вознаграждения за генерацию блока
- Получить неограниченное количество биткойнов
- Уничтожить сеть
- Потратить биткойны, которые ранее не принадлежали злоумышленнику.

Раздвоение цепи

- Сеть выбирает самую длинную цепочку
- Можно считать транзакцию окончательной после 6 подтверждений (6 блоков над блоком с транзакцией)
- Майнеры “голосуют” за правильный блок своей вычислительной мощностью



Как бросить учебу и начать маининг?

В 2017 году **никак**, этим надо было заниматься раньше.

Сейчас майнинг конкурентный бизнес. Люди, которые начинают заниматься майнингом, закупают огромное количество специализированного оборудования, арендуют склад, следят за тем, чтобы не было перегрузки сети.

Китаиская биткоин-ферма в Changchen


BitNovosti
bitnovosti.com
MOTHERBOARD
At the beginning,
I wasn't very optimistic.


BitNovosti
bitnovosti.com
MOTHERBOARD
But now I think it's great.

А если ну очень хочется?

Что еще за ASIC?

Application-specific integrating circuit (ASIC).

CPU → GPU → FPGA → ASIC

Маининг пул

- Распределение награды за блок.
- PROP (Proportional).
- PPS (Pay Per Share).

Правовои аспект

- Правовое поле не создано
- К оплате биткоины принимать **нельзя**
  - статья 27 ФЗ «О Центральном банке РФ» (выпуск запрещён)
  - статья 140 ГК РФ (официальная валюта – рубль)
- Верить можно только законам
- Герман Греф хранит деньги в биткоинах

Альтернативы Bitcoin

- Zcash
- **Ethereum**
- Dogecoin
- NXT (“окрашенные” монеты и децентрализованный обмен)
- Litecoin (block time = 2.5 minutes; 84 миллиона монет; хэш-функция не sha256, а scrypt)

Ethereum (Виталик Бутерин)

- “World Computer”, тьюринг-полный язык
- EVM - виртуальная машина ethereum
- Распределенное исполнение кода
- Распределенное хранение данных
- Ether - криптовалюта, “топливо” для оплаты “строк кода”

Адреса и контракты

- Адреса контролируются пользователями
- Контракты обладают своим кодом и памятью
- С адреса можно послать транзакцию на контракт для вызова функции
- Каждая операция стоит gas

```
contract Token {
    mapping (address => uint) balances;
    uint256 public totalSupply;

    function Token(uint initialAmount) {
        balances[msg.sender] = initialAmount;
        totalSupply = initialAmount;
    }

    function transfer(address to, uint value) returns (bool success) {
        if (balances[msg.sender] >= value && value > 0) {
            balances[msg.sender] -= value;
            balances[to] += value;
            return true;
        } else { return false; }
    }

    function balanceOf(address owner) constant returns (uint balance) {
        return balances[owner];
    }
}
```

Вендинговыи аппарат

Купля-продажа

Приватныи blockchain

- Hyperledger от IBM
- Приватный реестр от Сбербанка

HYPERLEDGER

SBERBANK

By your side

Gambling

Договора

- S7 и Альфа банк
- Barclays

Blockchain – не философскии камень

- Не подходит, когда много транзакций
- Плохая масштабируемость
- Высокая волатильность валюты
- Прозрачность транзакций
- Риск плохого кода

Существующие проекты на Ethereum

- Slock.it и Golos
- TheDAO
- Edgeless.io
- MediaChain

Как бросить учебу и провести ICO?

- Сделать лендинг за 10 тысяч рублей
- Посадить одногруппницу, знающую английский, писать whitepaper
- Скопировать код успешного ICO с github
- Заказать статью в CoinTelegraph
- Собрать 2-3 миллиона $ за несколько дней
- Вынуть все деньги из контракта и убежать в неизвестном направлении

Какие задачи есть сеичас в криптомире?

- Research
- Developing core features
- Smart-contracts

Спасибо!

email: amax0703@gmail.com
github: misteraverin
telegram: misteraverin

Ссылка на эту лекцию:
https://github.com/misteraverin/blockchain-materials