Криптографические основы цифровых денег

А. Н. Фионов

СибГУТИ ИВТ СО РАН Новосибирск

XVIII Всероссийская конференция молодых учёных по математическому моделированию и информационным технологиям
Иркутск, 21—25 августа 2017

Основные технологии цифровых денег

1. Слепая цифровая подпись
(David Chaum, 1983 // Ecash 1989—1998)

2. Блокчейн, цифровая подпись
(Satoshi Nakamoto, 2008 // Bitcoin 2009—)

Развитие Bitcoin

2009

10000 BTC за две пицы Papa John"s

Апрель 2010 1 BTC = $0.003

5000 транз / мес

2017

1 BTC = $4000.00

14 августа 2017 1 BTC = $4440.00

ок. 10 млн транз / мес

Рыночная капитализация $70 млрд

Криптографические средства

1. Хэш-функция

$y = h(x)$, $y \in \{0, 1, \ldots, 2^k - 1\}$, $k = 160, 256, 512, \ldots$ бит

Свойства:

- для заданного y трудоёмкость поиска x $O(2^k)$
- для заданного x_1 трудоёмкость поиска x_2 : $h(x_2) = h(x_1)$ $O(2^k)$
- трудоёмкость поиска x_1 , x_2 : $h(x_1) = h(x_2)$ $O(2^{k/2})$

Криптографические средства

1. Хэш-функция

ведёт себя как случайная функция:

- для случайно выбираемого x все значения $y = h(x)$ равновероятны
- даже если x_2 зависит от x_1, $h(x_2)$ и $h(x_1)$ выглядят как статистически независимые
- при изменении одного бита в x изменяется примерно половина бит в $h(x)$
- для произвольно выбираемого x вероятность того, что в $h(x)$ первые n бит будут нулевые, равна $1 / 2^n$

Криптографические средства

2. Цифровая подпись (ECDSA)

- ключи:

  S — секретный ключ (256 бит)

  P — открытый ключ (257 бит)

  $P = [S]G$ (S-кратная композиция точки G на эллиптической кривой)

  свойство: практически невозможно вычислить S из P

- вычисление подписи для x :

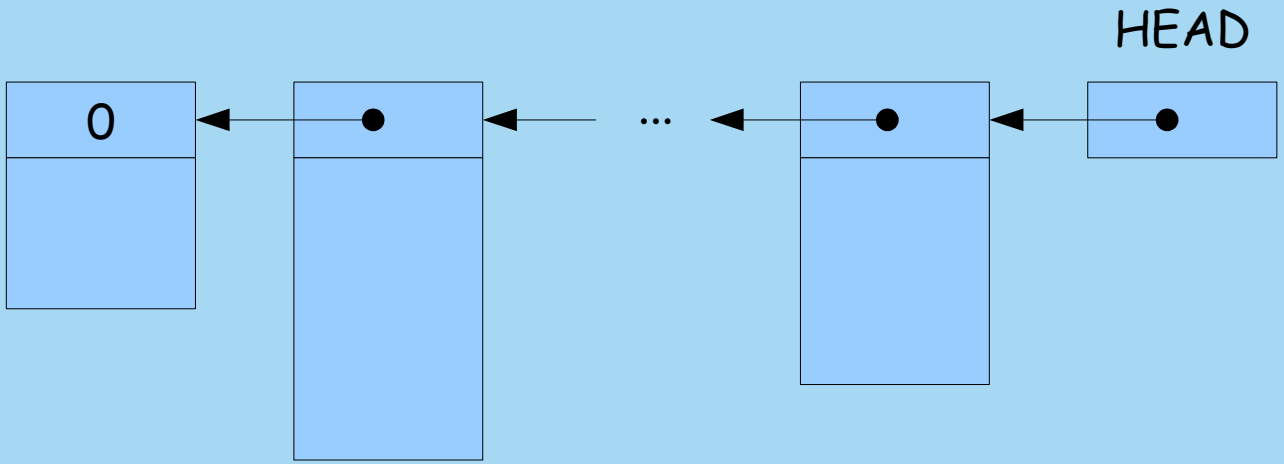
  $y = \mathrm{sign}(h(x), S)$ (512 бит)

- проверка подписи для x :

  $\mathrm{verify}(h(x), y, P)$ (true, false)

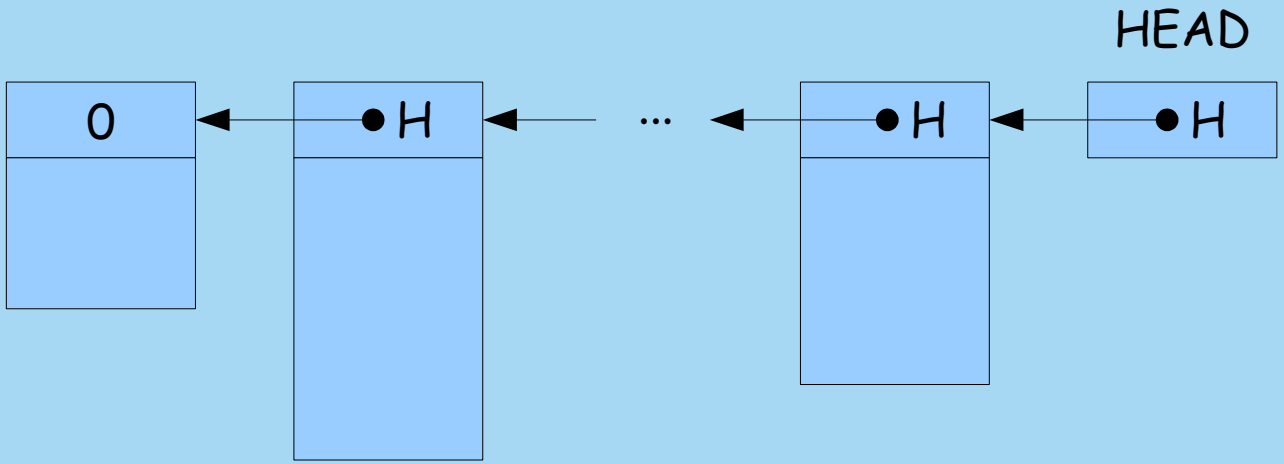
Bitcoin: основные идеи

1. Блокчейн



Bitcoin: основные идеи

1. Блокчейн

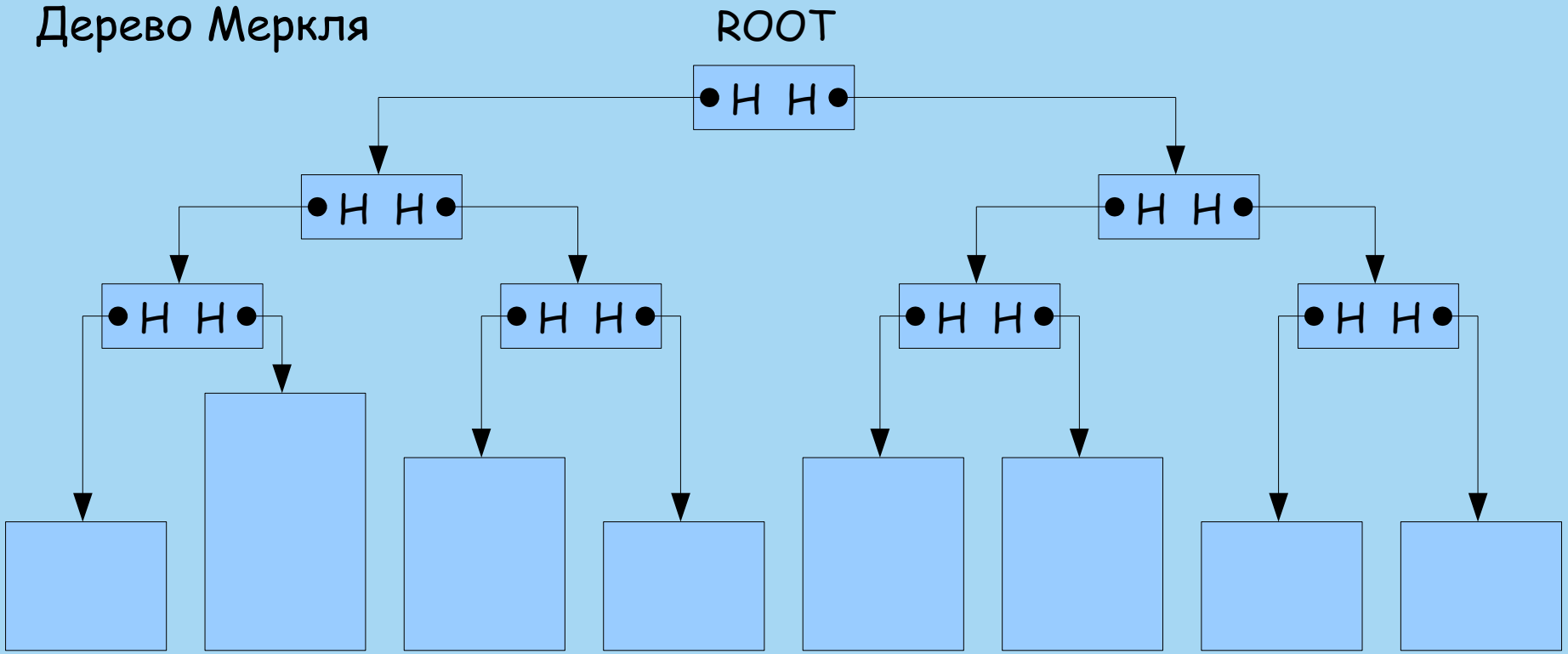


H-указатель — значение хэш-функции предыдущего элемента

Bitcoin: основные идеи

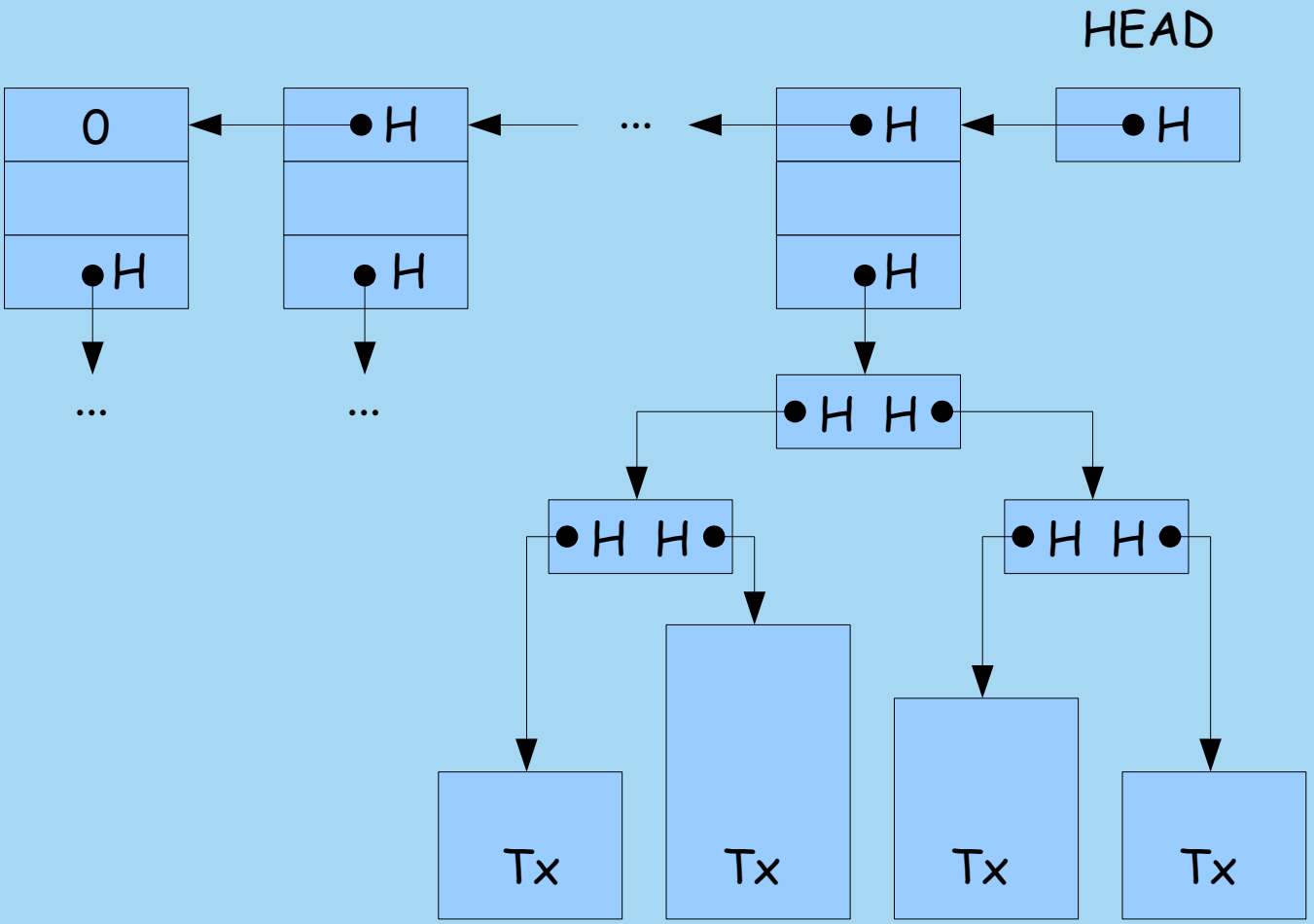
1. Блокчейн

Дерево Меркля



Bitcoin: основные идеи

1. Блокчейн



Bitcoin: основные идеи

2. Идентификация через открытые ключи

	секретный ключ	открытый ключ
Сущность A:	S_A	P_A
Сущность B:	S_B	P_B
Сущность C:	S_C	P_C

. . .

открытый ключ — приём платежей
секретный ключ — отправление платежей

отсутствуют счета пользователей
в блокчейн заносятся только подписанные транзакции
(информация об отправлении платежей)

Bitcoin: основные идеи

3. Отсутствие счетов пользователей

в блокчейн заносятся только подписанные транзакции
(информация об отправлении платежей)

Примеры транзакций

Tx1 in 0: 0
out 0: 50.0 → P_A

Tx2 in 0: Tx1 out 0
out 0: 20.0 → P_B
1: 30.0 → P_C (sign A)

Tx13 in 0: Tx2 out 0
out 0: 10.0 → P_C
1: 10.0 → P_B (sign B)

Tx14 in 0: Tx2 out 1
1: Tx13 out 0
out 0: 40.0 → P_D (sign C)

Bitcoin: основные идеи

4. Эмиссия путём создания блока (mining)

Задачи майнера:

- получение и проверка транзакций
- поддержка блокчейна, получение и проверка новых блоков
- построение блока-кандидата
- подбор переменных полей для получения хэш-функции блока $H < T$
- представление блока-кандидата в сеть

Bitcoin: основные идеи

4. Эмиссия путём создания блока (mining)

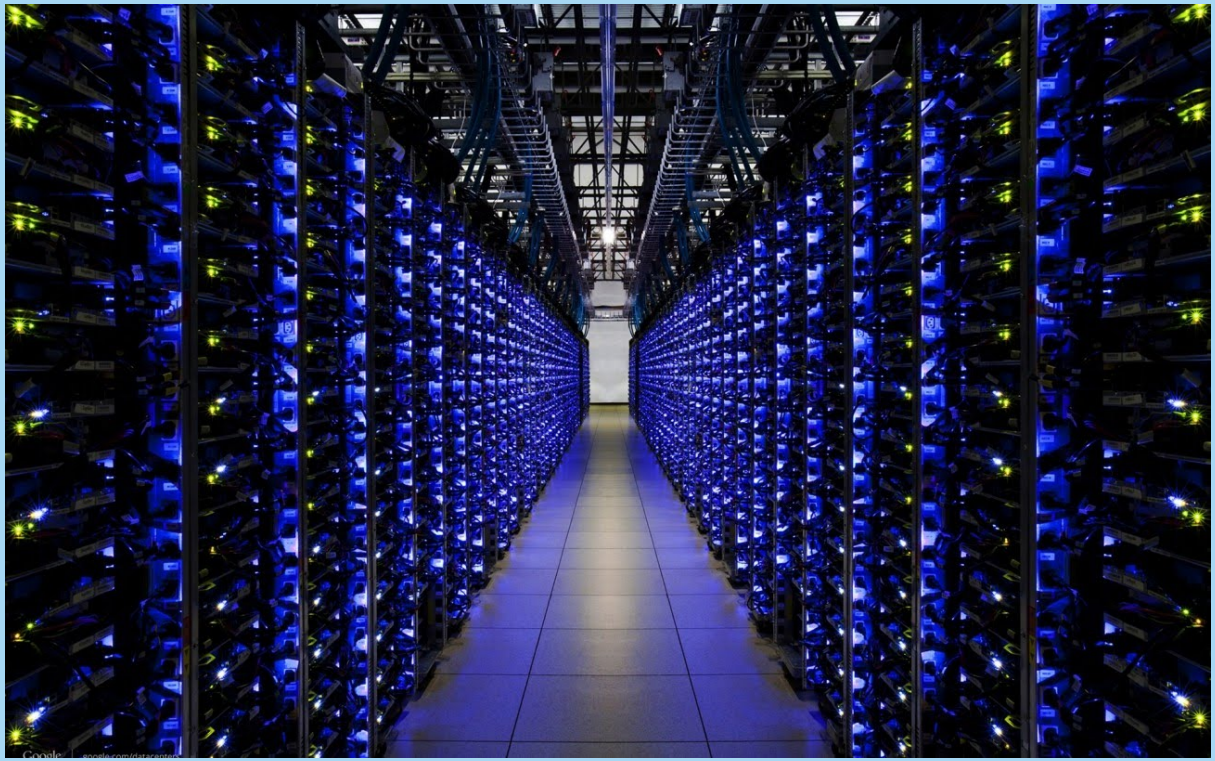
Некоторая статистика:

- текущий размер блокчейна ≈ 128 Гб
- один блок может содержать до 4000 транзакций (≤ 1 Мб)
- среднее время порождения блока 10 мин
- пересчёт порога T происходит через каждые 2016 блоков
- в настоящее время T содержит ≈ 70 старших нулевых бит
- вознаграждение за создание блока:
  изначально 50 BTC
  / 2 через каждые 210000 блоков
  в настоящее время 12.5 BTC
  эмиссия полностью прекратится в 2140 г., предел 21 млн BTC

Bitcoin: основные идеи

4. Эмиссия путём создания блока (mining)

Mining Farms



Bitcoin: основные идеи

4. Эмиссия путём создания блока (mining)

Плата майнеру за транзакции

Tx14 in 0: Tx2 out 1
1: Tx13 out 0
out 0: 40.0 → P_D (sign C)

бесплатная транзакция

Tx14 in 0: Tx2 out 1
1: Tx13 out 0
out 0: 39.0 → P_D (sign C)

майнер получает 1.0 BTC

Bitcoin: основные идеи

5. Децентрализация

P2P сеть, все узлы равноценны,
узлы могут добавляться и удаляться в любой момент,
каждый узел взаимодействует со случайным подмножеством узлов

Алгоритм наводнения (flooding algorithm)

Два типа узлов: FV (Fully Validating)
SPV (Simple Payment Verification)

Размер сети: ~ 10000 FV, 1000000 SPV

Изучение блокчейна

https://blockchain.info

и др.

Вопросы для анализа

- Анонимность биткоина
- Атаки на биткоин
- Экономические аспекты биткоина