Масштабируемость блокчейн-систем: проблемы и решения

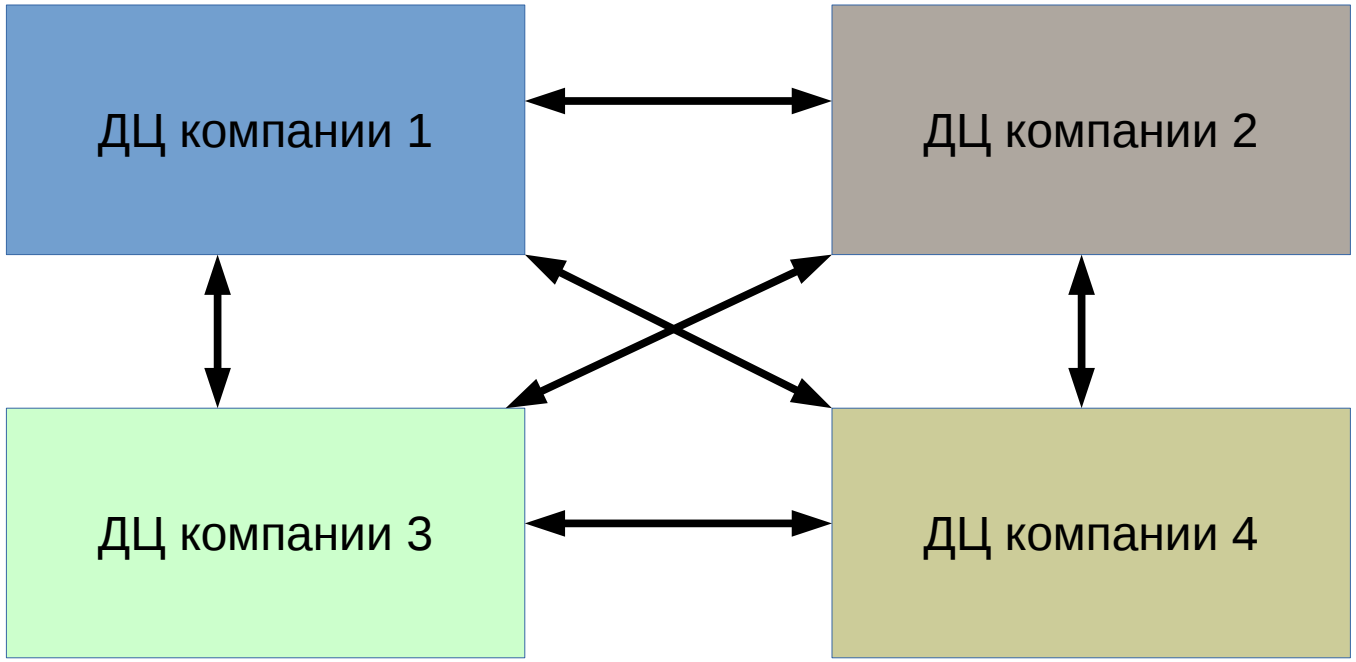
Александр Чепурной

IOHK Research

Этот разговор:

об открытых системах (Bitcoin, Ethereum Classic, etc)

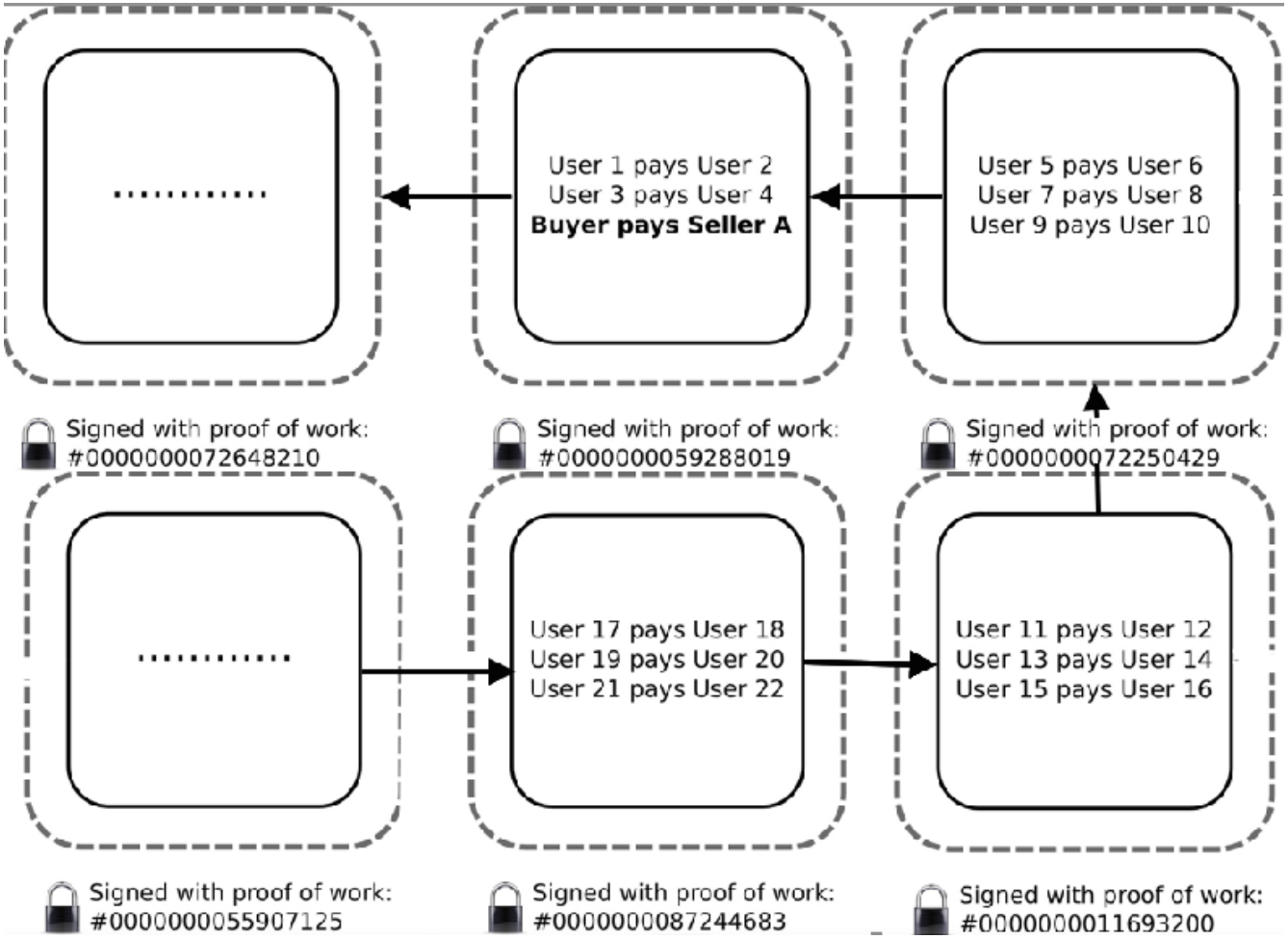
Закрытые – другой разговор:



Сложности в масштабировании открытых систем:

- среднестатистический современный компьютер должен иметь полные гарантии безопасности
- одноуровневая p2p-сеть, машин с широким каналом немного
- постоянные атаки (DoS итп)
- нетехнические способы решения проблем ограничены, обновления протокола затруднены
- сложной криптографии желательно избегать

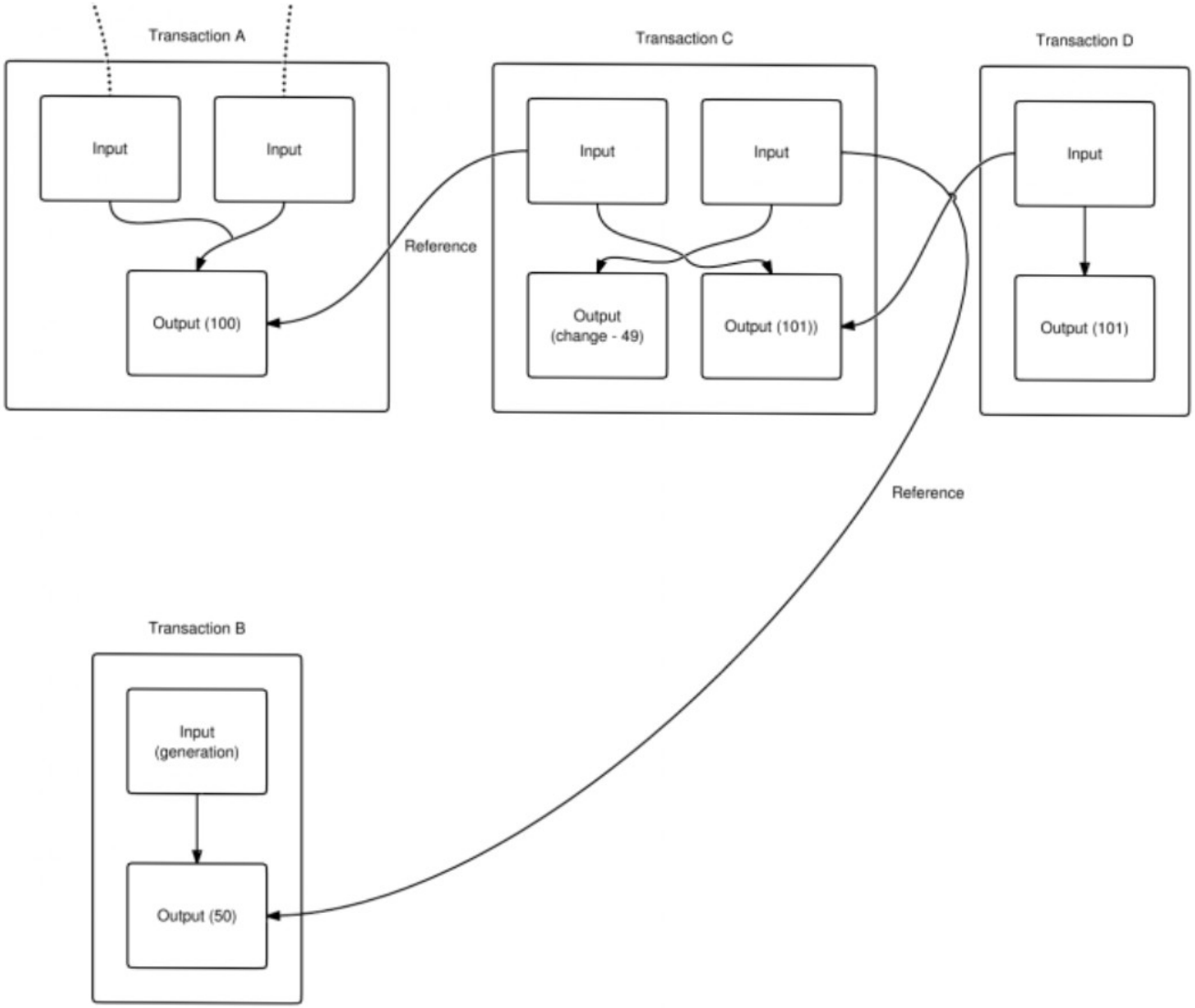
Блокчейн


.....
User 1 pays User 2
User 3 pays User 4
Buyer pays Seller A
User 5 pays User 6
User 7 pays User 8
User 9 pays User 10
Signed with proof of work:
#0000000072648210
Signed with proof of work:
#0000000059288019
Signed with proof of work:
#0000000072250429
.....
User 17 pays User 18
User 19 pays User 20
User 21 pays User 22
User 11 pays User 12
User 13 pays User 14
User 15 pays User 16
Signed with proof of work:
#0000000055907125
Signed with proof of work:
#0000000087244683
Signed with proof of work:
#0000000011693200

Состояние

- Извлекать данные из блокчейна непрактично
- Текущее минимальное состояние позволяет проверить валидность любой транзакции
- В случае биткойна – набор UTXO
- Ethereum – “world state” (задан протоколом)

Транзакция Bitcoin



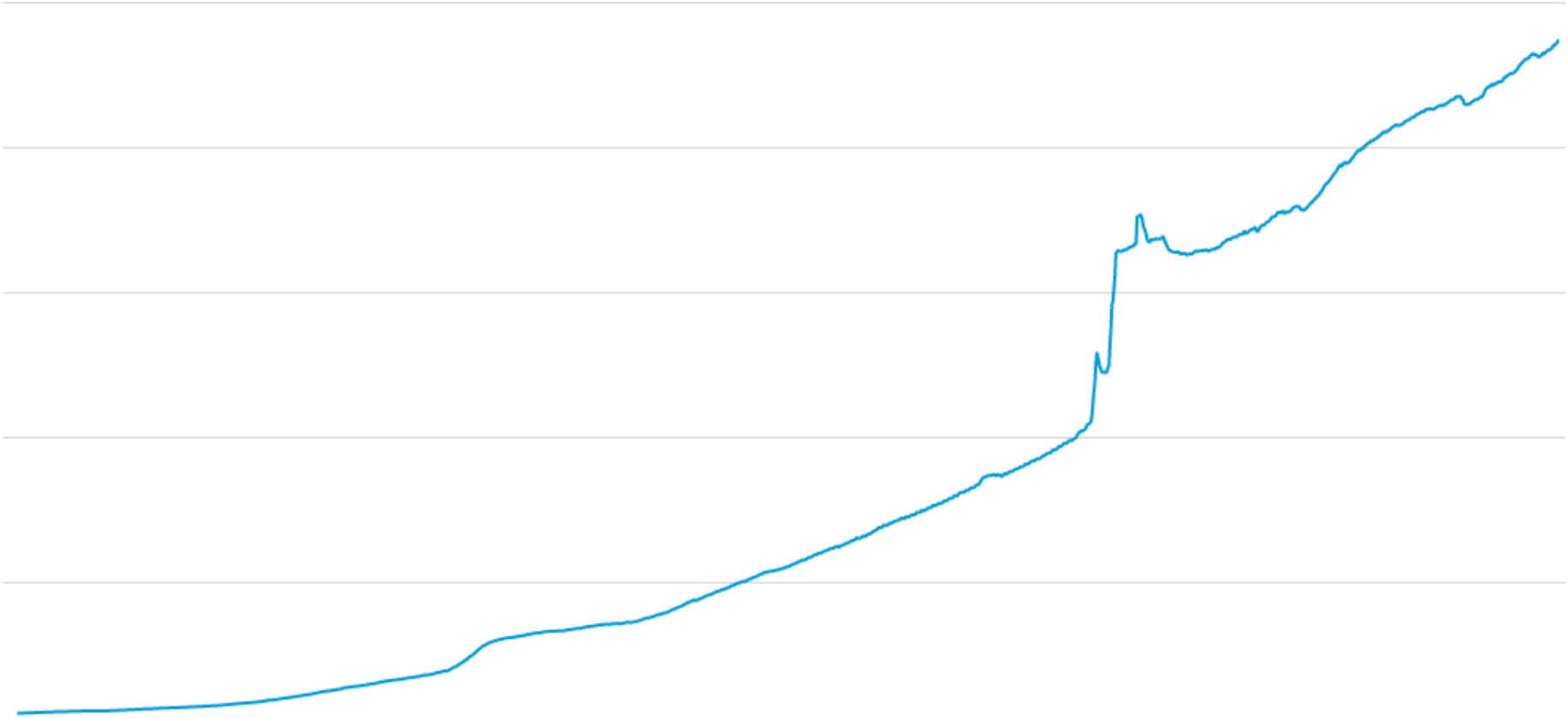
Bitcoin: что измерять?

Число неподтвержденных транзакций – как сильно система перегружена в данный момент?

Bitcoin: что измерять?

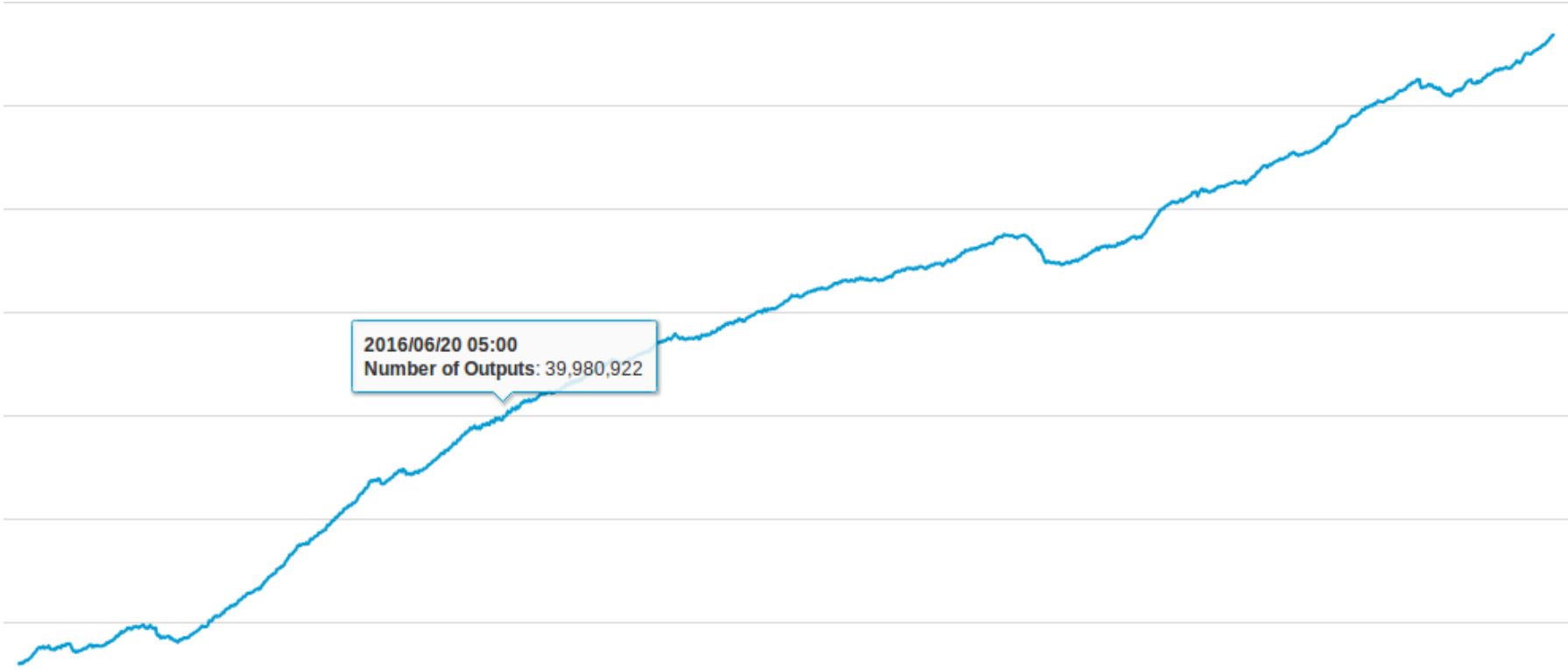
Количество UTXO (непотраченных выходов транзакций) – как тяжело выжить в сети среднему компьютеру.

За все время жизни Биткойна:



Набор UTXO – постоянный размер блоков

За последний год



Пропускная способность

- Чем больше пропускная способность, тем больше транзакций может принять блокчейн
- Обратная сторона: и тем быстрее растет блокчейн и состояние

Как увеличить?

Решение №1: изменить константу!

- Размер блока
- Среднее время между блоками

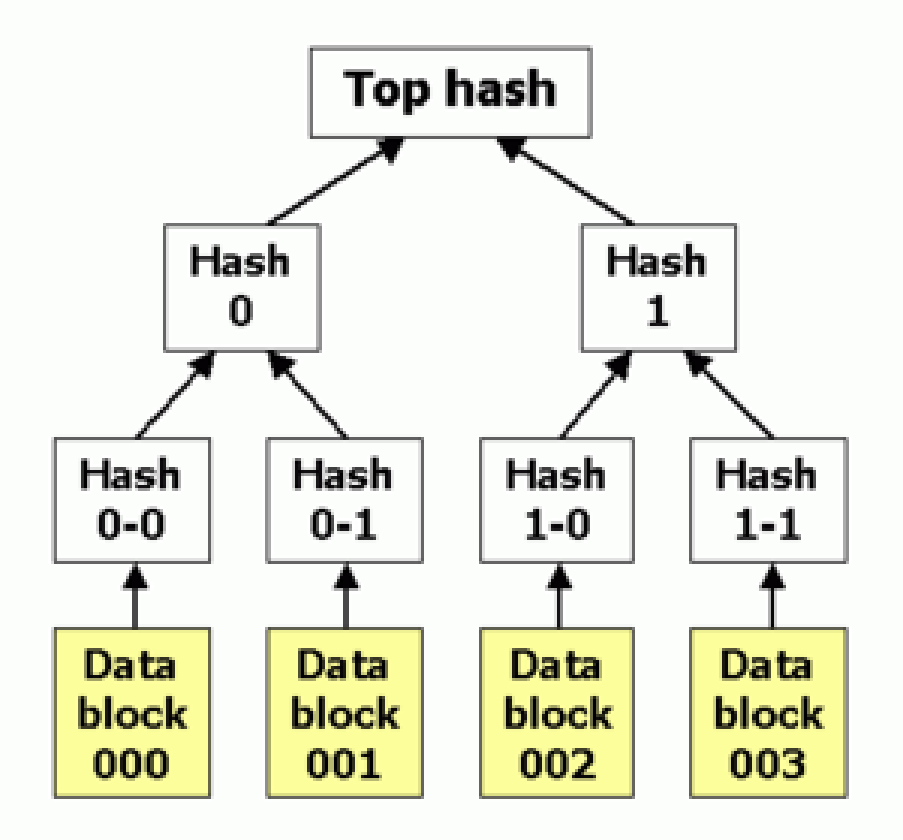
- Настройки Биткойна очень консервативны, увеличить размер блока или уменьшить время между блоками в 2-4 раза не представляет проблем **для консенсуса**

Решение №2: изменить протокол консенсуса!

- Bitcoin-NG
- GHOST / SPECTRE (?)
- ByzCoin (collective signing)
- Proof-of-Stake (?)

Дерево Меркла

Один хэш (32 байта) определяет целостность потенциально очень большого массива данных (гигабайты!)



Блокчейн

- Хранить блоки все накладнее

- В Биткойне, приходится обрабатывать целиком
- Но потом можно не хранить (рационально!)
- Но откуда брать тогда блоки новым узлам?

- В Эфириуме можно сгрузить только заголовки блоков, затем состояние некоторое количество блоков назад, и блоки
- Гарантии безопасности?

Решение: Rollerchain

- Статья https://arxiv.org/abs/1603.07926 (Chepurnoy, Larangeira, Ozhiganov)

- Новый алгоритм майнинга
- Заставляет майнера сохранять несколько старых версий состояния
- Все майнеры хранят “n” последних состояний и блоков

Table 1. Bootstapping Methods

	Full Blocks Stored	Rational	Full State
Bitcoin Fullnode	All	No	Yes
SPV	None	Yes	No
Headers Then State	None	Yes	Yes
Rollerchain	last n blocks	Yes	Yes

Состояние

Должно храниться в памяти (RAM)
Текущий размер в Биткойне: 1.5 GB (47.5M выходов)

Если не помещается в памяти, серьезные проблемы!

Источник проблем

Пример проблем:

- Bitcoin: CVE-2013-2293 (DoS через чтение выходов с диска)
- Ethereum: часть атак осенью 2016 была направлена сначала на резкое увеличение размера состояние(чтобы вытолкнуть его на жесткий диск на большинстве узлов сети), а затем DoS атаки через запрос состояние элементов, хранящихся на диске

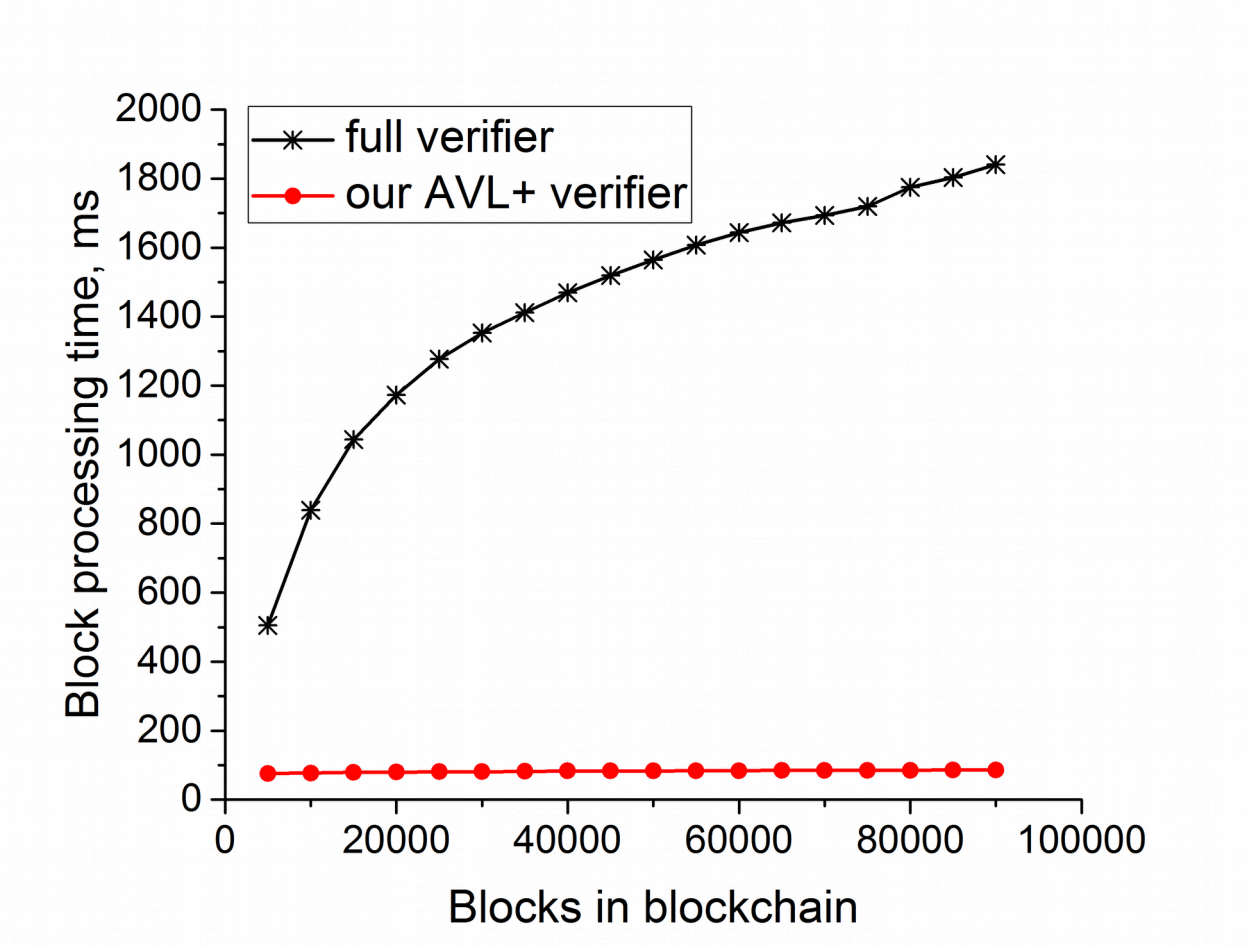
Решение:

- Не хранить узлу состояния совсем!
- Его хранят только майнеры, которые могут потратиться на RAM
- Майнер включает в блок доказательства правильности трансформации состояний

- Статья: https://eprint.iacr.org/2016/994
  (Reyzin, Meshkov, Chepurnoy, Ivanov – Financial Cryptography'17)

- Видео: https://www.youtube.com/watch?v=PHY7JnLrK5o
  (Leonid Reyzin @ RealWorldCrypto'17)

Решение:


full verifier
our AVL+ verifier
Block processing time, ms
Blocks in blockchain
0
200
400
600
800
1000
1200
1400
1600
1800
2000
0
20000
40000
60000
80000
100000

Экономические механизмы:

Блокчейн-системы – красивое пересечение технических и экономических моделей

Пример, модель “газа” в Ethereum: майнеры могут регулировать доступную пользователям сложность вычислений

Проблема:

- Непотраченный выход в Bitcoin живет вечно!
- Контракты в Ethereum тоже!
- Сжимать состояние никому не выгодно
- Состояние растет даже в отсутствие роста пользовательской базы
- Особенно проблематично в случае хранения данных о голосованиях, аудите, протоколах итп.

Решение:

- Сейчас комиссия берется только за размер транзакции (+ за сложность вычислений в Ethereum)
- Предполагается брать комиссию и за время жизни объекта и его размер
- Аналог “газа” за хранение – стоимость байто-блока
- Майнеры собирают просроченные объекты за вознаграждение
- Токены могут стать подобными “свободным деньгам” Гезелля (открытый вопрос!)

- “On Space-scarce Economy in Blockchain Systems” (Meshkov, Chepurnoy) – пока нет в публичном доступе!

И нечего сюда писать всякое!

- Lightning network / Sprites
- Sidechains
- Aspnes / Ardor
- Sharding

Некоторые выводы:

- Можно поднять на порядок-другой пропускную способность сети без компрометации базовых принципов и безопасности, и без сложной криптографии
- Все предложения (кроме изменения констант) по изменению дизайна блокчейна неприменимы для Биткойна (скорее всего, и для Ethereum)

Вопросы?