Bitcoin

математические основы криптовалют

Минко В.С.

2018

Что называют Bitcoin

- Электронная валюта.
- Одноранговая платёжная система.
- Протокол передачи данных.

Историческая справка

- 1983 – протокол «электронной наличности» от Чаума и Брэндса
- 1997 – Бак предложил систему Hashcash для борьбы со спамом и DoS-атаками. Финни реализовал связку цепочек хеш-блоков для Hashcash.
- 2008 – коллектив авторов опубликовал протокол Bitcoin.
- 2009 – создан первый блок, первые транзакции Bitcoin.
- 2010 – первый обмен Bitcoin на реальный товар.

Ключевое достоинство

Решение проблемы обеспечения доверия между сторонами к полученной информации, когда ни у одной из сторон нет доверия к действиям другой стороны.

Т.е. решение проблемы повторной траты денег (применительно к электронным платёжным системам).

Хеш-функция

Преобразует массив входных данных произвольной длины в битовую строку фиксированной длины.

Криптографические хеш-функции:

- Необратимы
- Стойки к коллизиям

MD5(«physics") = d65f2c2e29eec9b6516d99c2a148a5f9

MD5(“phyzics") = 68b00918046f9b218e4eb69318f3e011

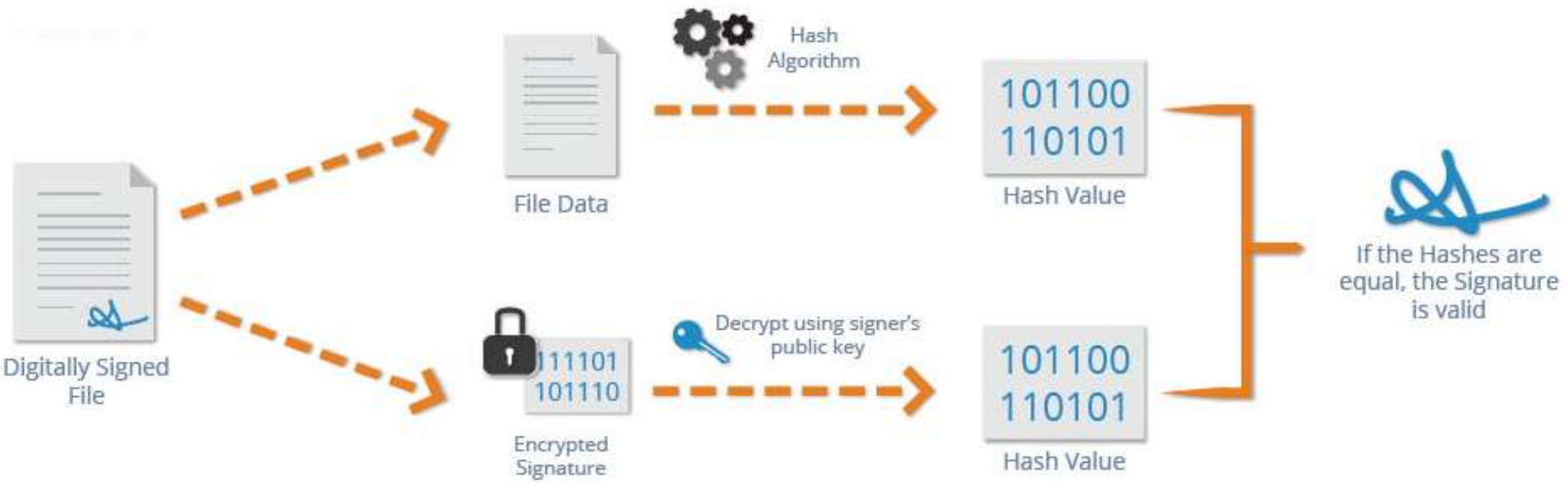
Симметричная криптография

Асимметричная криптография

Электронная Цифровая Подпись

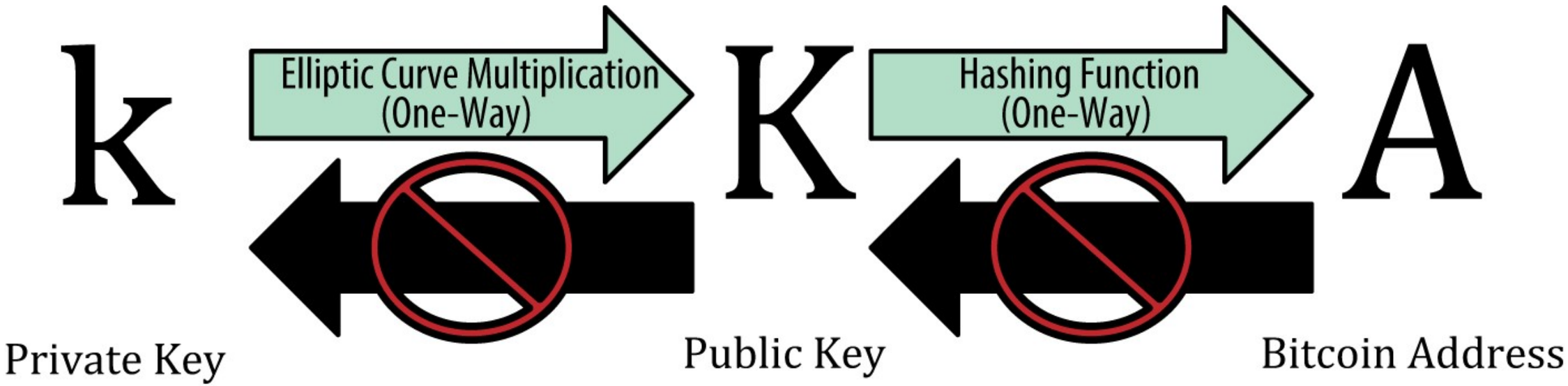
Подпись

Проверка

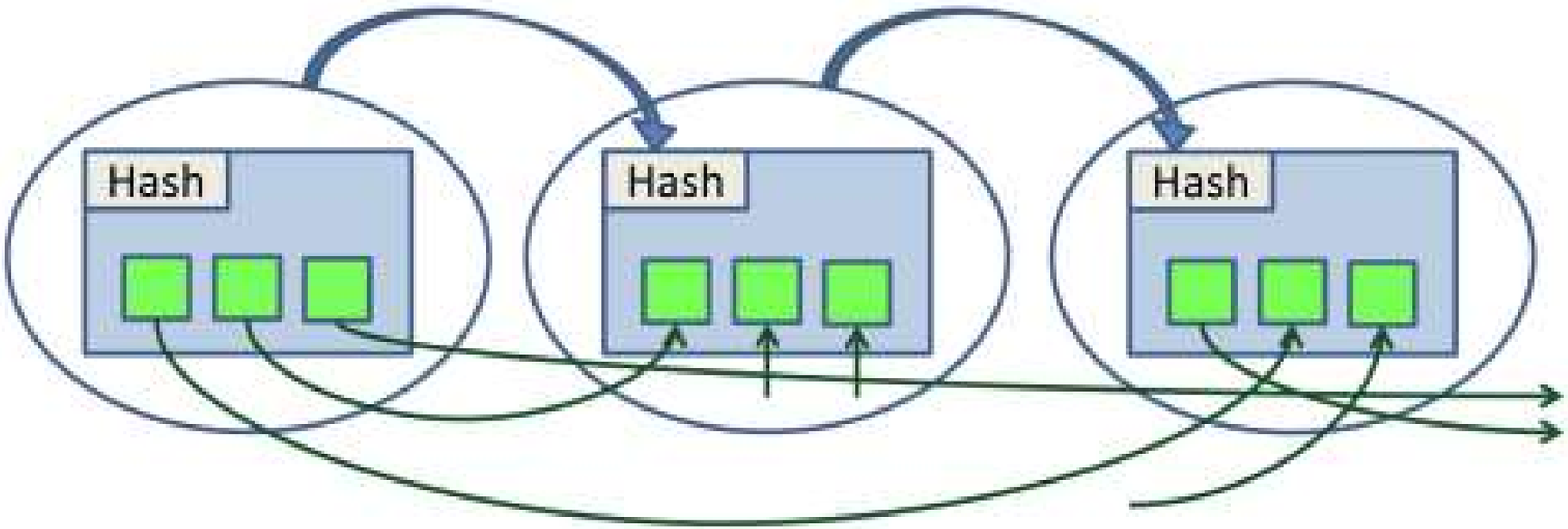


Адрес – хеш публичного ключа

```
{ "from" : 1FXySbm7jpJfHEJRjSNPPUqnpRTcSuS8aN,
  "to" : 1Eqm3z1yu6D4Y1c1LXKqReqo1gvZNrmfvN,
  "amount" : 1 }
```

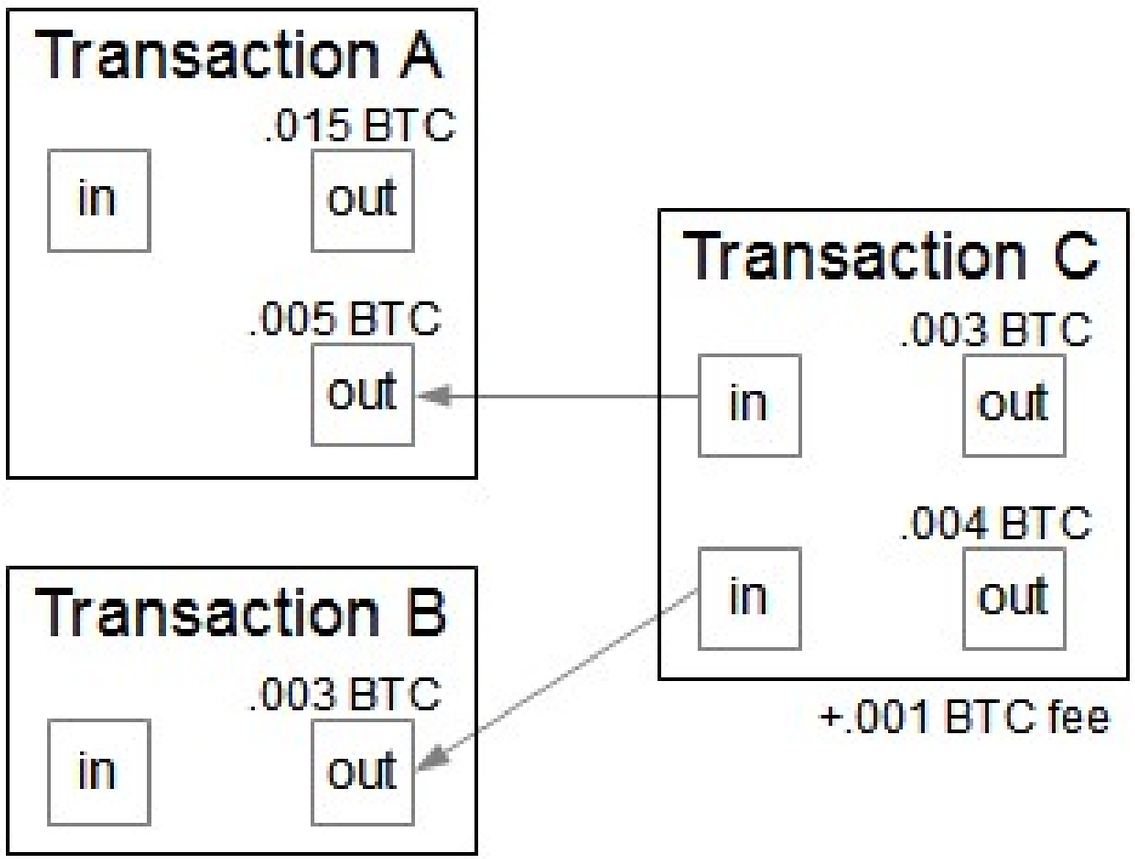


Транзакции



<address 1> sent <amount> BTC to <address 2>

Транзакции


Transaction A
.015 BTC
in
out
.005 BTC
out
Transaction C
.003 BTC
in
out
.004 BTC
in
out
Transaction B
.003 BTC
in
out
+.001 BTC fee

Структура транзакции

version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	
	scriptSig	script containing signature
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	
	scriptPubKey	script containing destination address
block lock time		00 00 00 00

Script

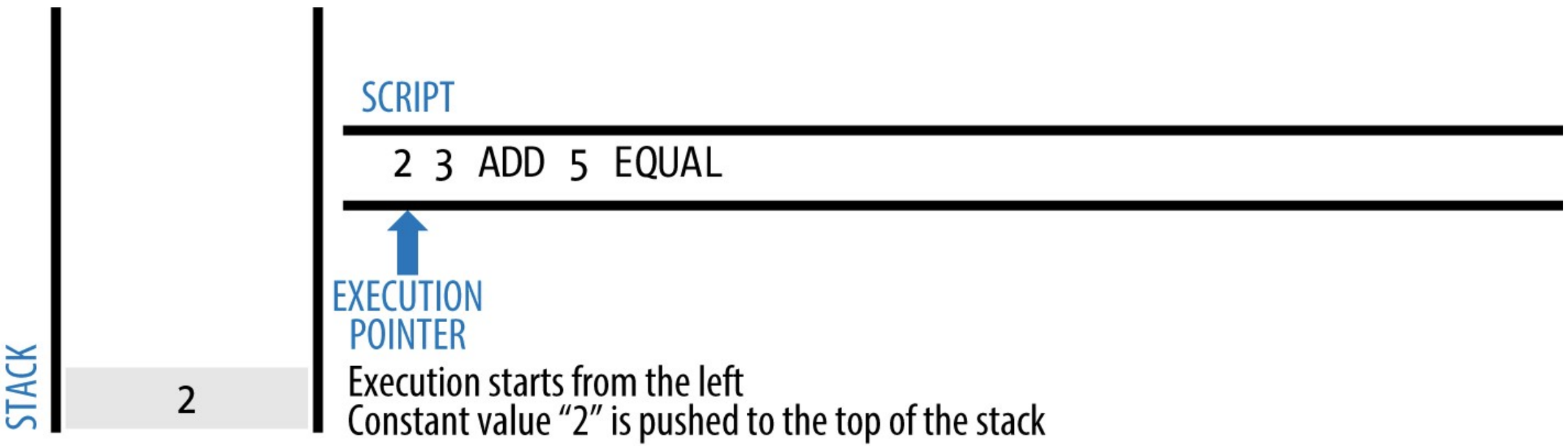
Собственный язык программирования:

- Stack-based:
- Неполный по Тьюрингу.

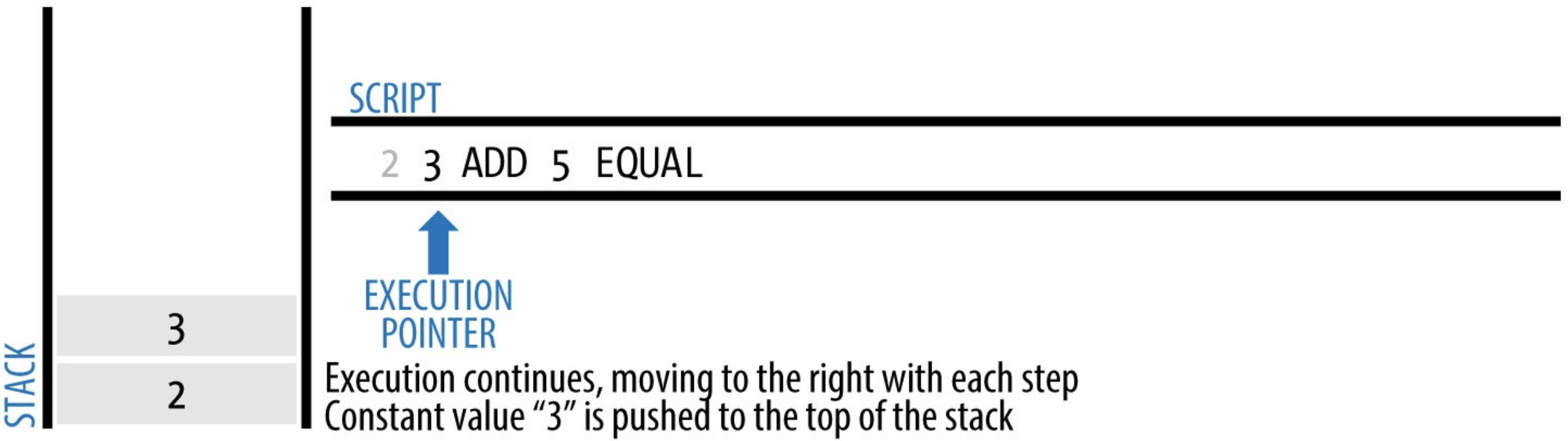
Типичной программы:

```
2 3 OP_ADD 5 OP_EQUAL
```

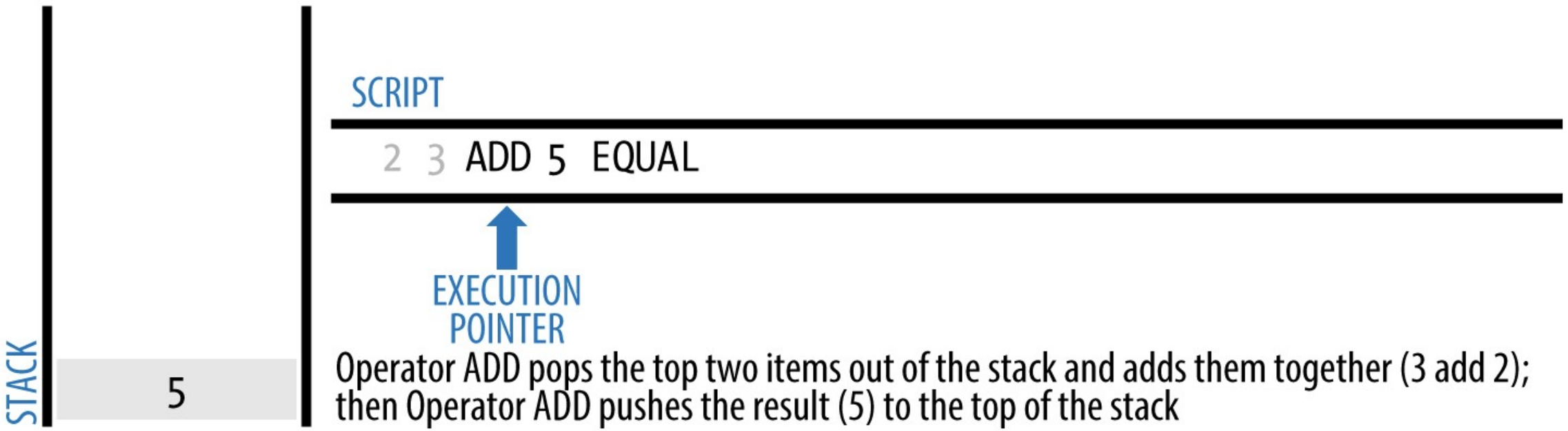
Процесс исполнения script



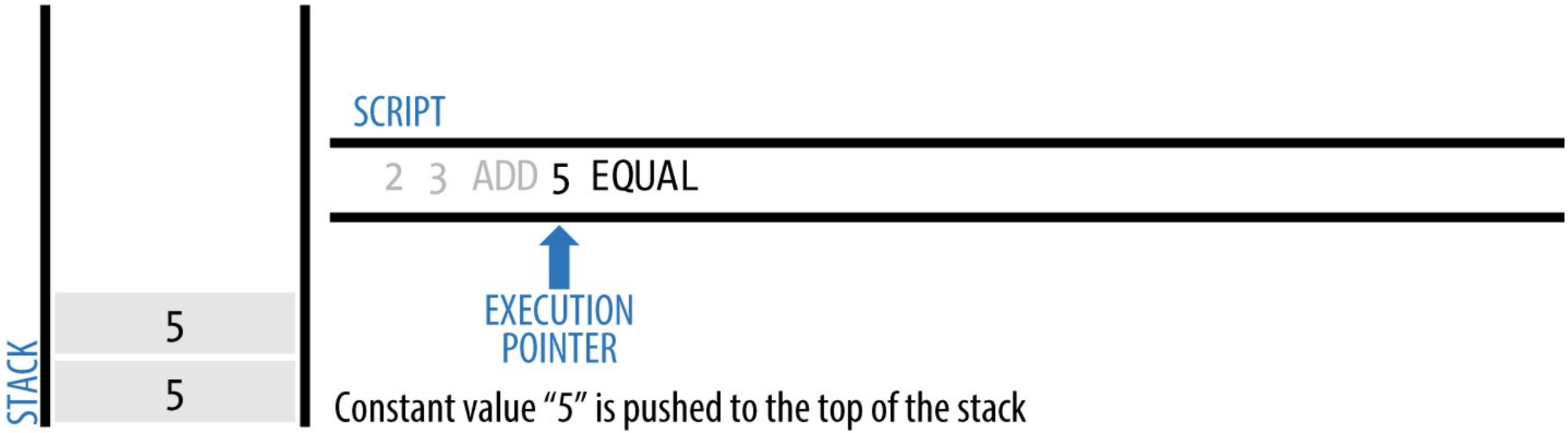
Процесс исполнения script



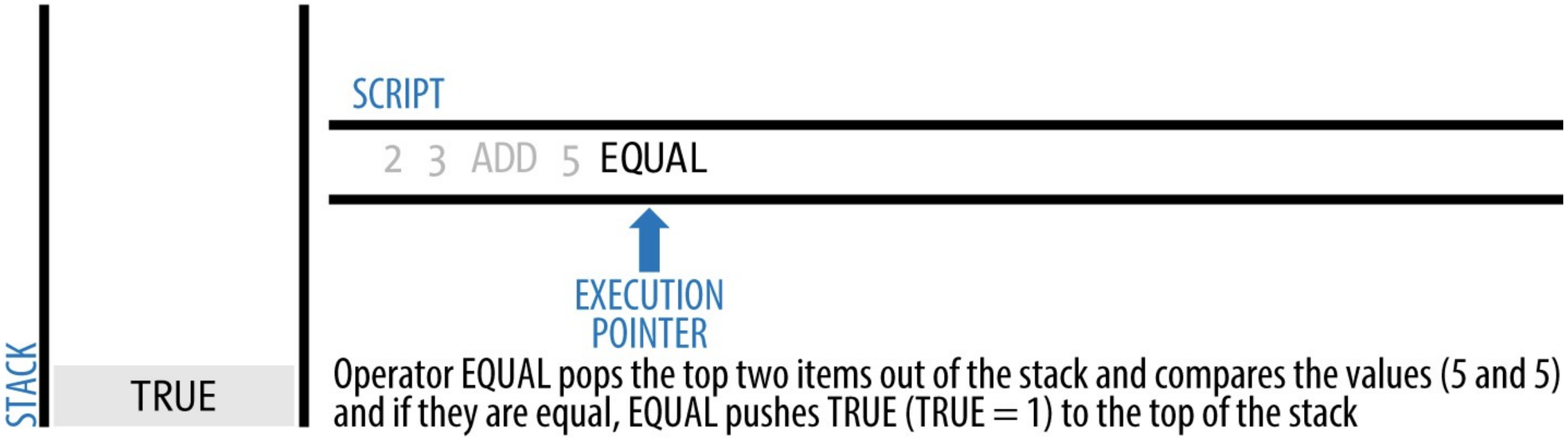
Процесс исполнения script



Процесс исполнения script



Процесс исполнения script



Условие траты выхода транзакции

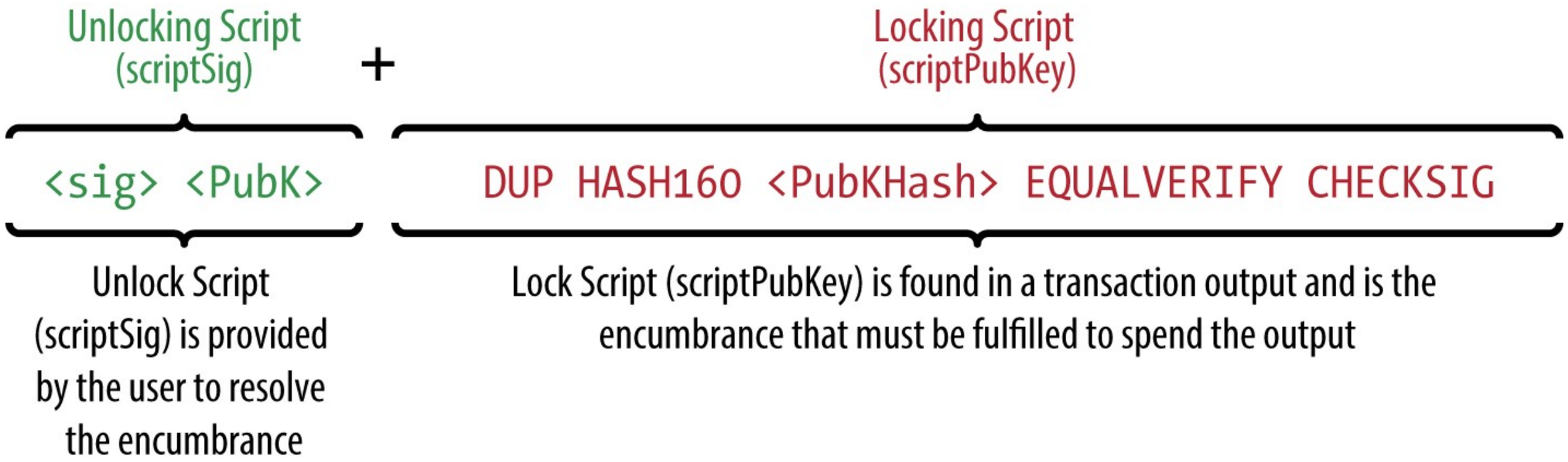
Условие: 1.000.000$ переходят к Алисе только после того, как ей исполнится 18 лет.

Доказательство: паспорт Алисы.

scriptPubKey – скрипт условия, обычно содержит публичный ключ получателя.

scriptSig – скрипт доказательства, обычно содержит подпись получателя.

Условие траты выхода транзакции



Протокол – поиск нод

DSN seeding:

- seed.bitcoin.sipa.be
- dnsseed.bluematt.me
- dnsseed.bitcoin.dashjr.org
- seed.bitcoinstats.com
- seed.bitcoin.jonasschnelli.ch
- seed.btc.petertodd.org

```
$ nslookup seed.bitcoin.sipa.be
Non-authoritative answer:
Name: seed.bitcoin.sipa.be
Address: 76.111.96.126
Name: seed.bitcoin.sipa.be
Address: 85.214.90.1
Name: seed.bitcoin.sipa.be
Address: 94.226.111.26
Name: seed.bitcoin.sipa.be
Address: 96.2.103.25
```

Протокол – рукопожатие

When the local peer **L** connects to a remote peer **R**, the remote peer will not send any data until it receives a version message.

- **L -> R** Send version message with the local peer's version
- **R -> L** Send version message back
- **R** Sets version to the minimum of the 2 versions
- **R -> L** Send verack message
- **L** Sets version to the minimum of the 2 versions

Протокол - структура сообщения

Field Size	Description	Data type	Comments
4	magic	uint32_t	Magic value indicating message origin network
12	command	char[12]	ASCII string identifying the packet content, NULL padded
4	length	uint32_t	Length of payload in number of bytes
4	checksum	uint32_t	First 4 bytes of sha256(sha256(payload))
?	payload	uchar[]	The actual data

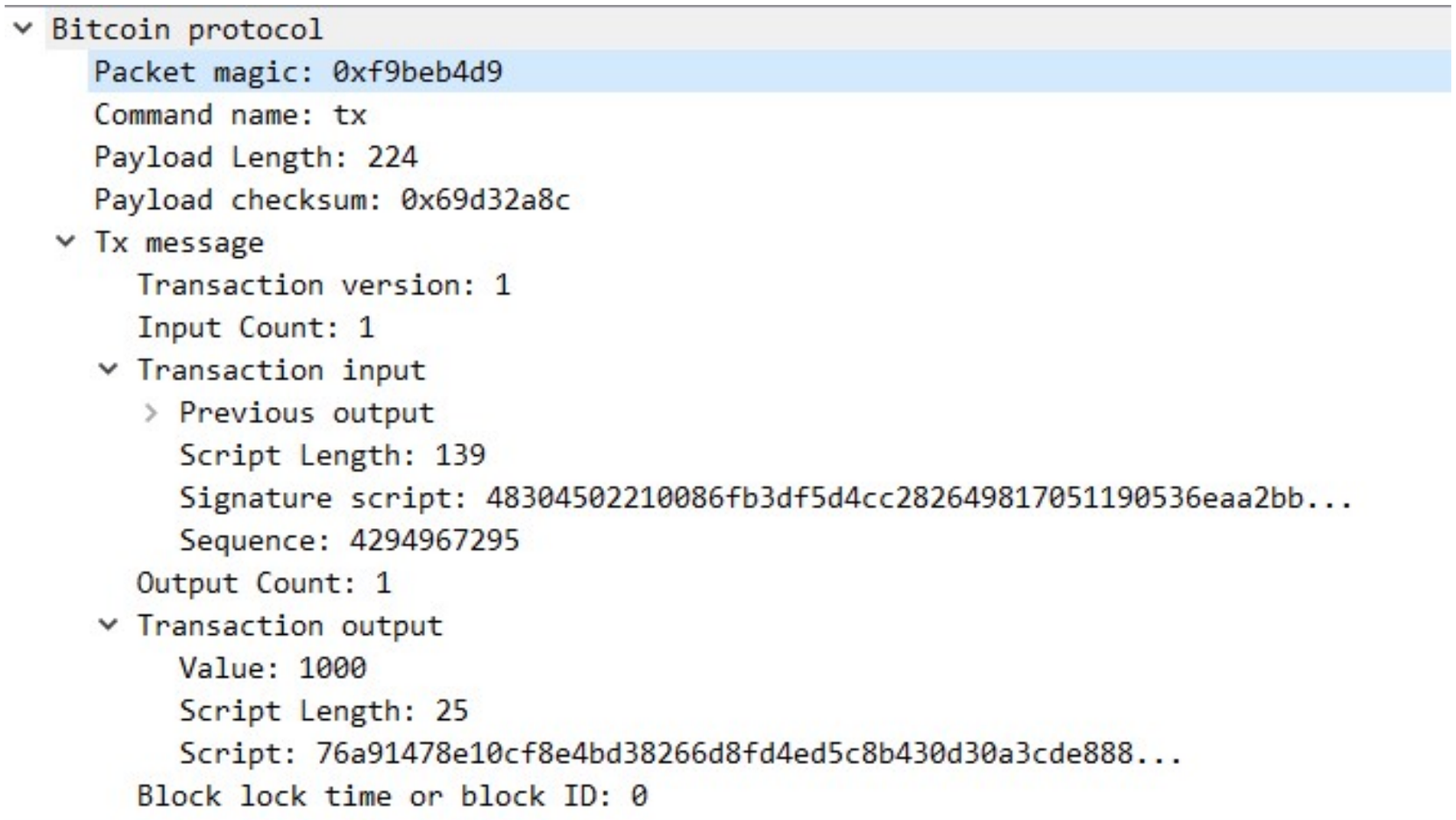
Протокол – подпись транзакции

version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	
	scriptSig	script containing signature
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	
	scriptPubKey	script containing destination address
block lock time		00 00 00 00

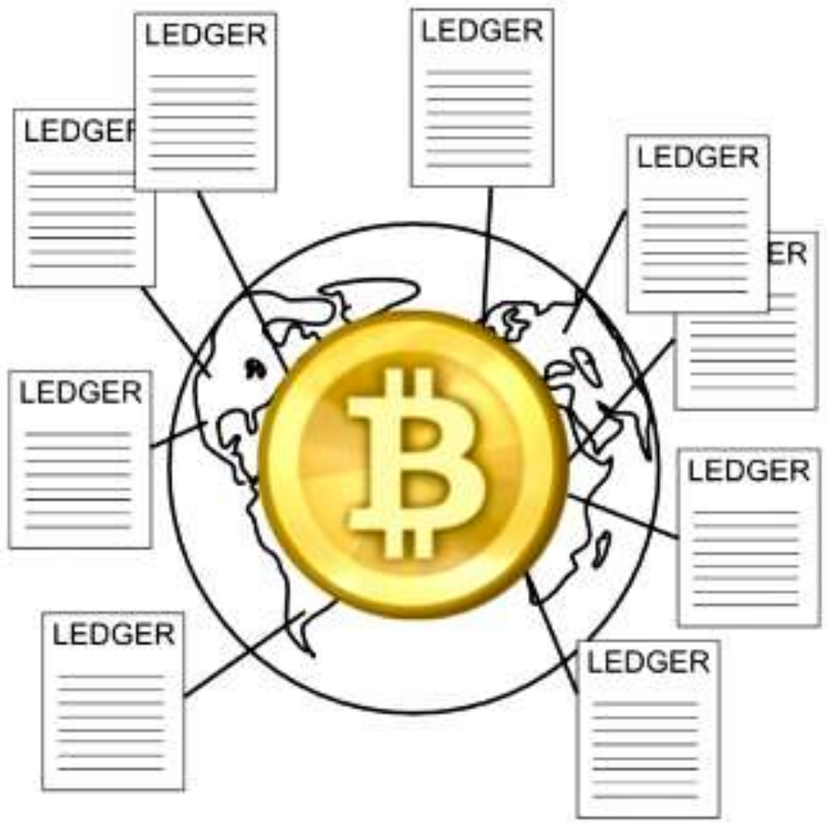
Протокол – подпись транзакции

Подписывается ненастоящая транзакция, которая будет отправлена другим нодам, а ее модификация, где в unlocking script указан locking script из выхода.

Протокол – отправка транзакции



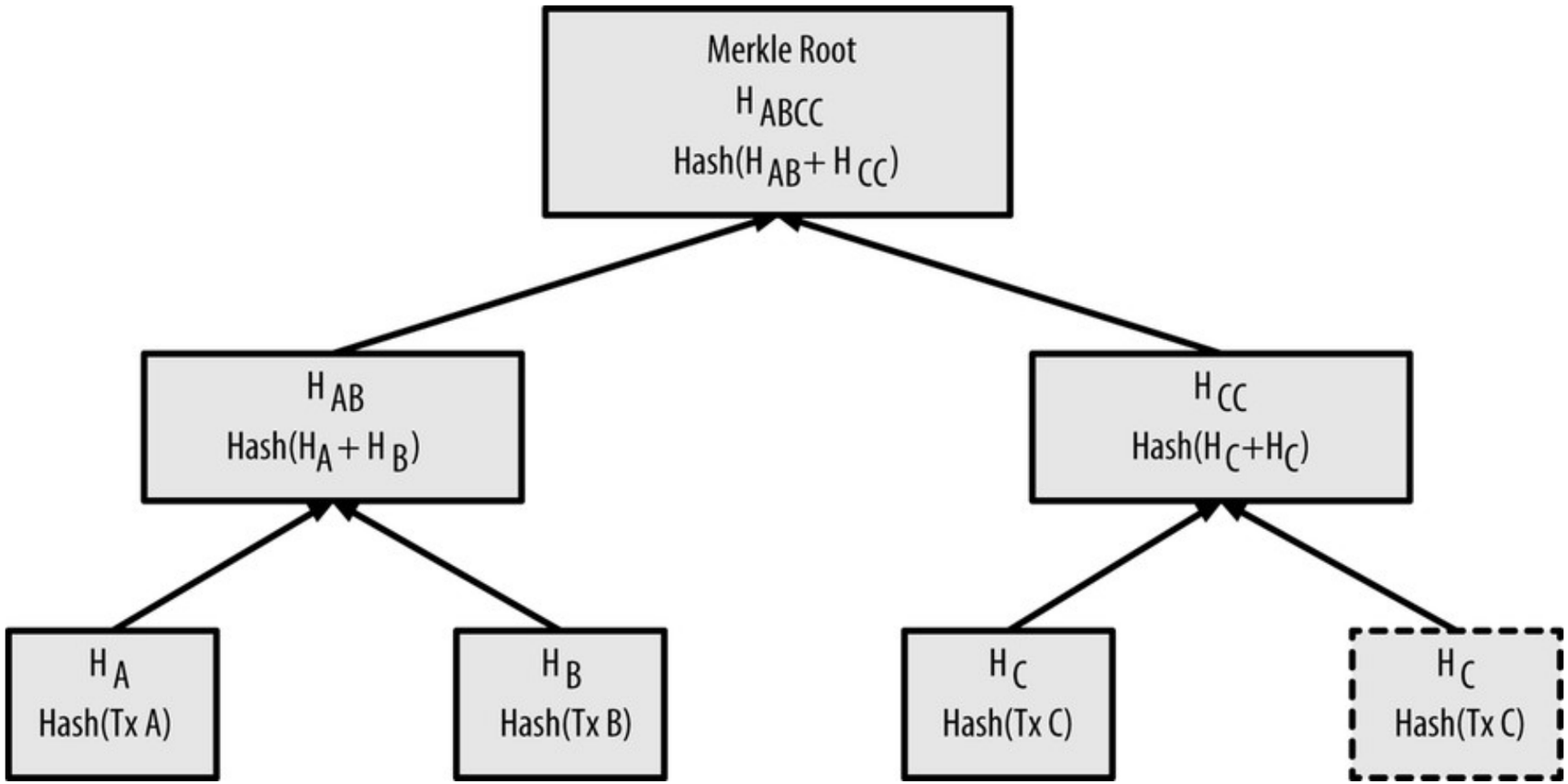
Блокчейн



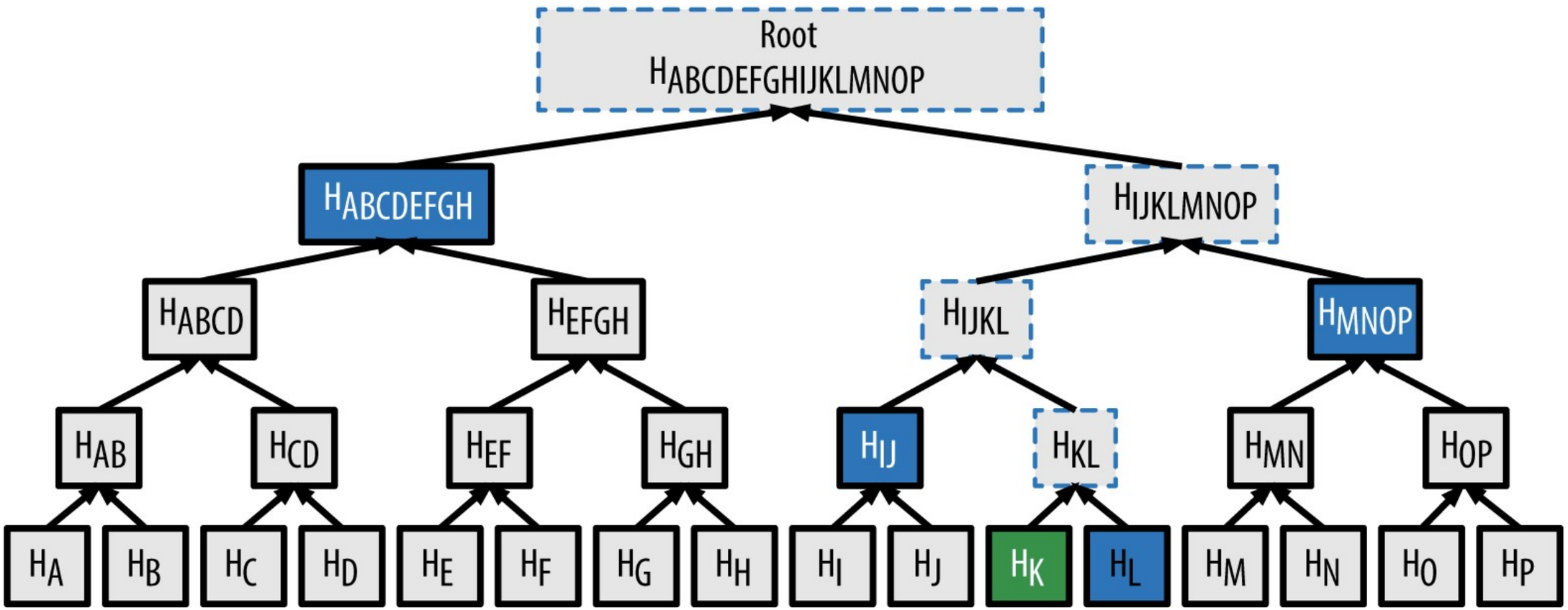
Структура блока

Field Size	Description	Data type	Comments
4	version	int32_t	Block version information (note, this is signed)
32	prev_block	char[32]	The hash value of the previous block this particular block references
32	merkle_root	char[32]	The reference to a Merkle tree collection which is a hash of all transactions related to this block
4	timestamp	uint32_t	A Unix timestamp recording when this block was created (Currently limited to dates before the year 2106!)
4	bits	uint32_t	The calculated difficulty target being used for this block
4	nonce	uint32_t	The nonce used to generate this block… to allow variations of the header and compute different hashes
?	txn_count	var_int	Number of transaction entries
?	txns	tx[]	Block transactions, in format of "tx" command

Дерево Меркла



Дерево Меркла



Майнинг

Деятельность по поддержанию распределенной платформы и созданию новых блоков с возможностью получить вознаграждение в форме эмитированной валюты и комиссионных сборов.

Цели:

- Производство денежной массы.
- Обеспечение работы сети.

Ограниченная эмиссия.

Количество биткойнов с течением времени

Свойства алгоритма майнинга

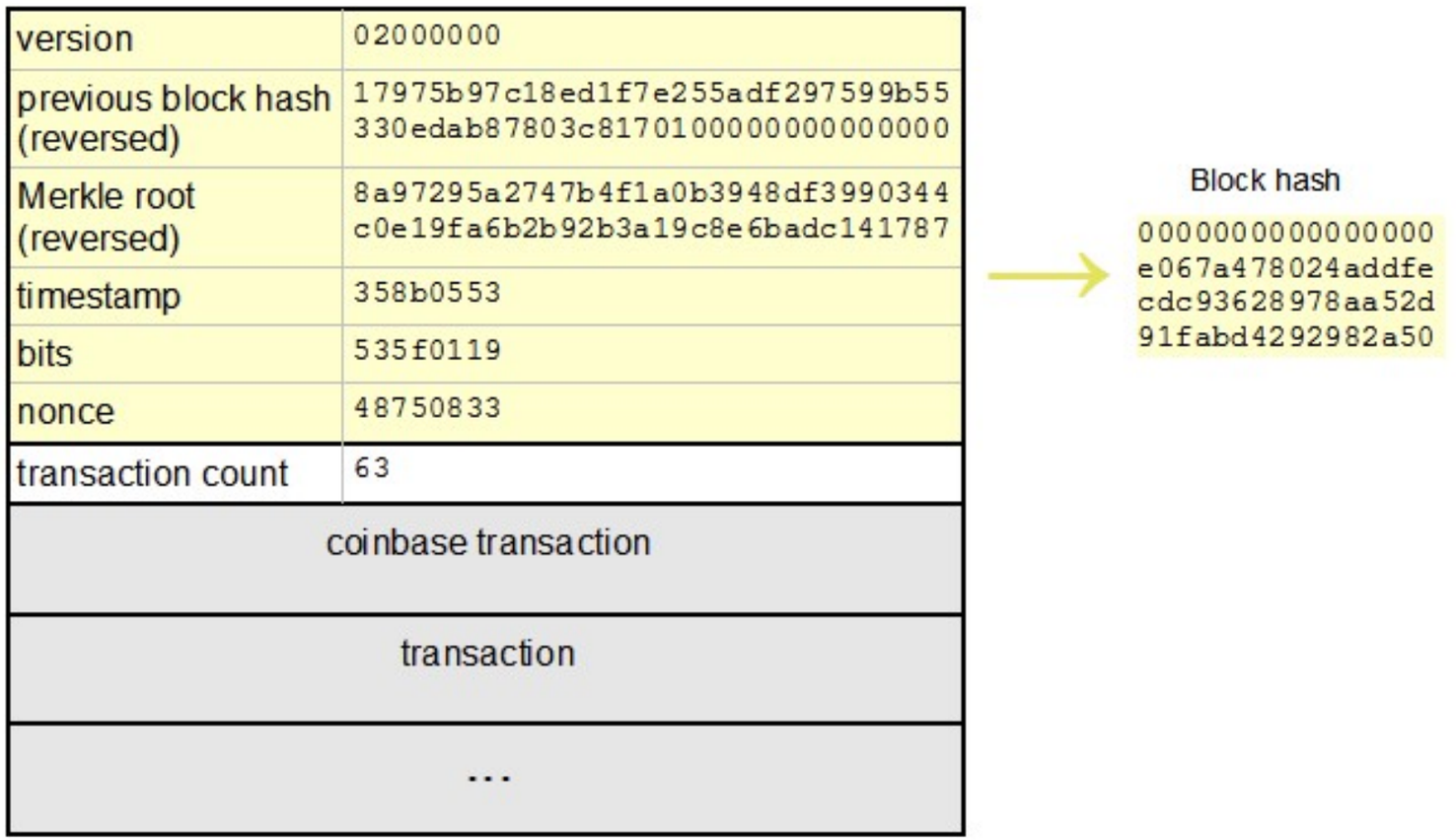
- Создание нового блока — вычислительно сложная задача.
- На вычисление нового блока у всей сети уходит 10 минут (в среднем).
- Это время не зависит от числа участников сети.
- Проверка блока на "корректность" должна быть простой.

Proof-of-Work

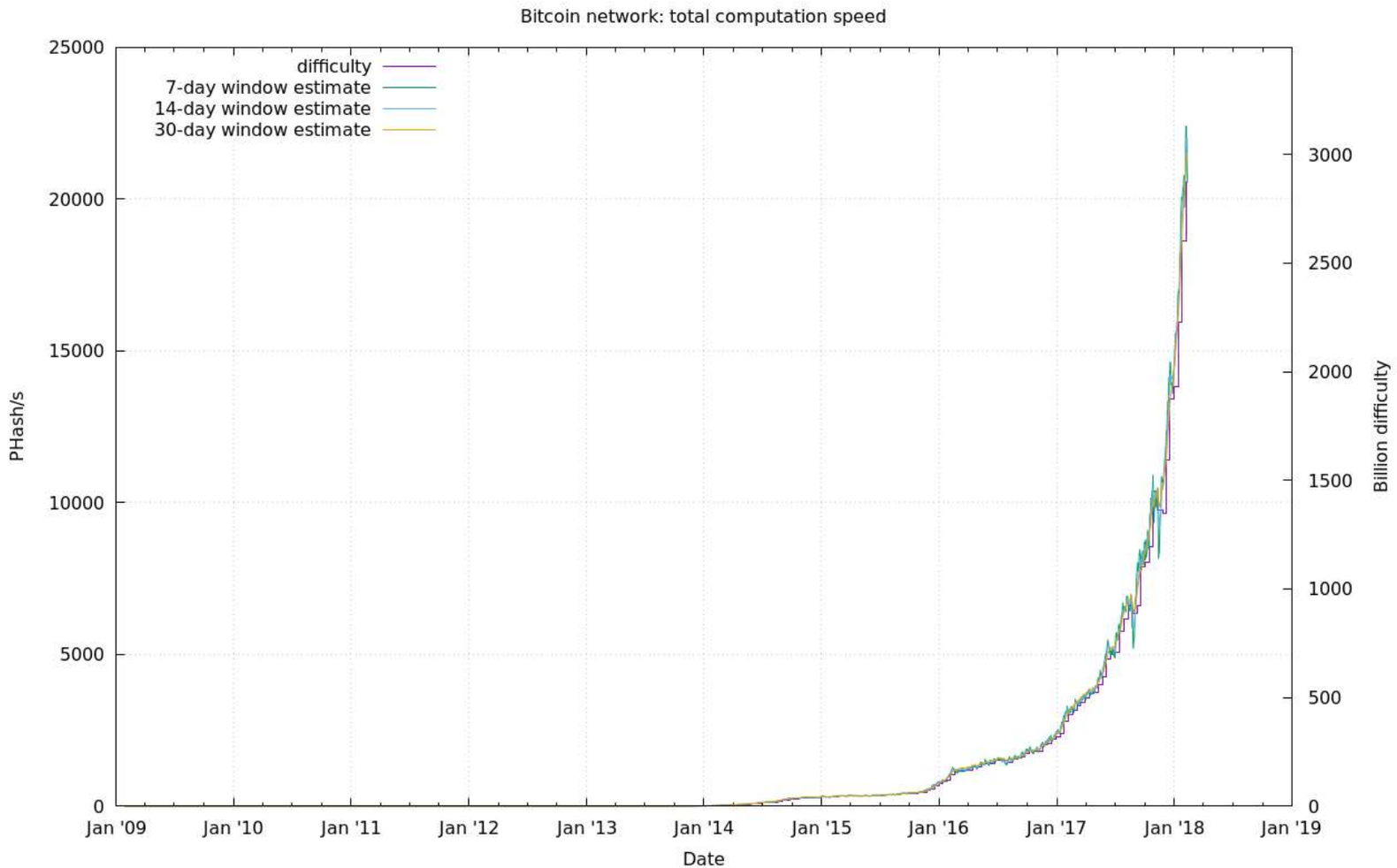
- Формируется блок из транзакций, *nonce* = 0
- Пока хеш блока > N:
  - *nonce*++
  - Пересчитать хеш блока

Число N — именно тот параметр, который сеть настраивает в зависимости от суммарной мощности майнеров.

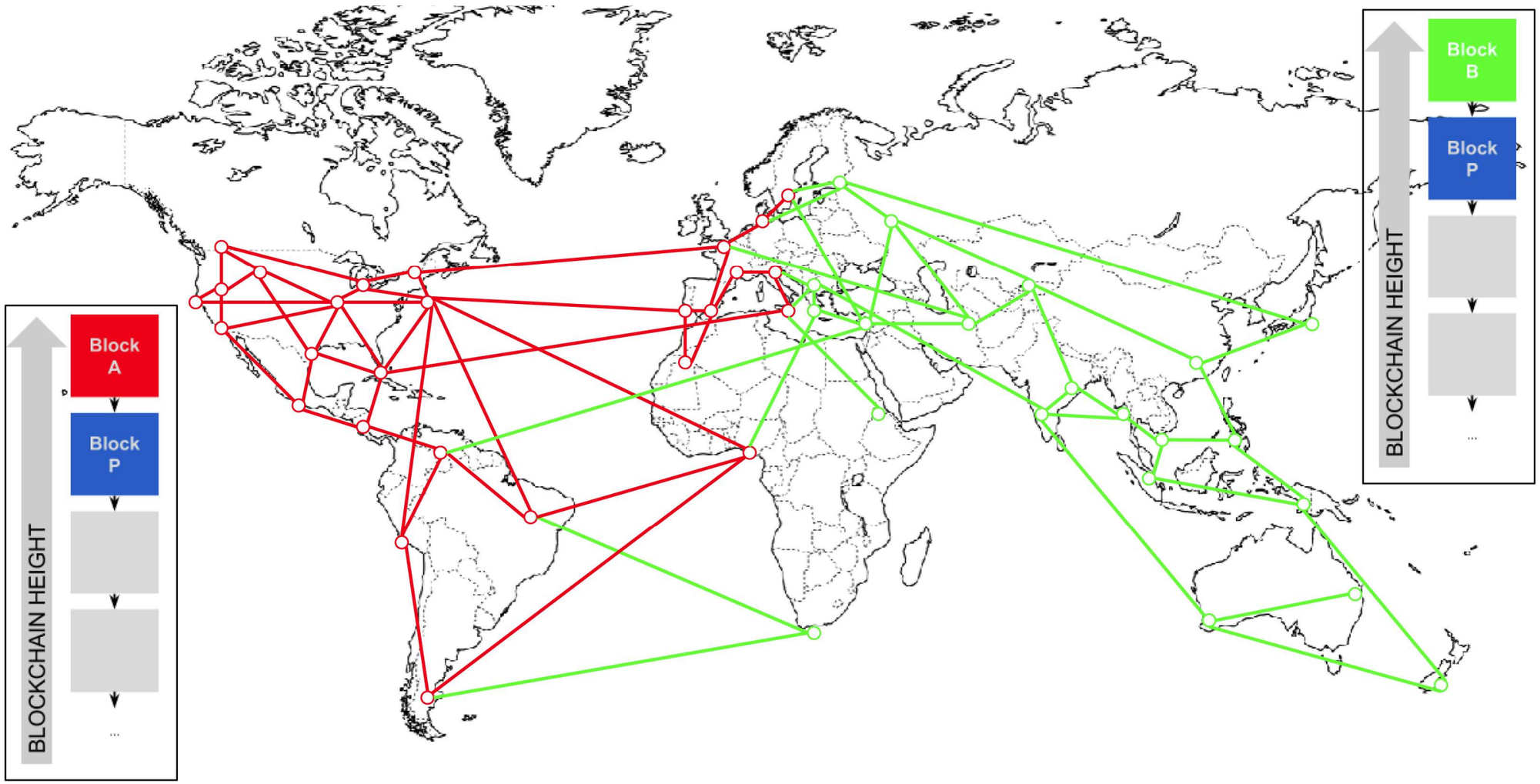
Proof-of-Work



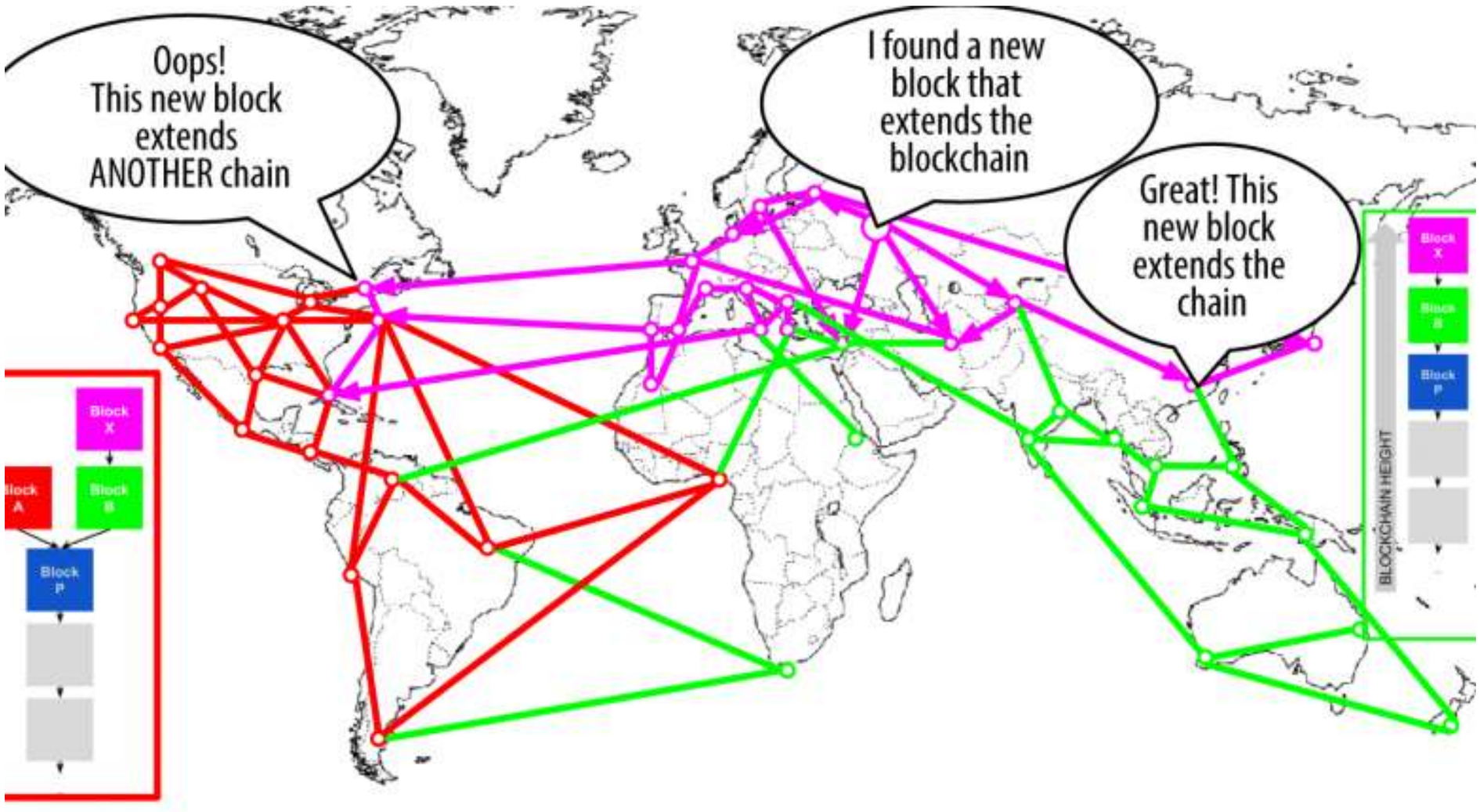
Hash rate


Bitcoin network: total computation speed
difficulty
7-day window estimate
14-day window estimate
30-day window estimate
PHash/s
Billion difficulty
Date
0
5000
10000
15000
20000
25000
0
500
1000
1500
2000
2500
3000
Jan '09
Jan '10
Jan '11
Jan '12
Jan '13
Jan '14
Jan '15
Jan '16
Jan '17
Jan '18
Jan '19

Разветвление блокчейна



Разветвление блокчейна



Атака 51%

- Мошенник покупает товар на 1000 BTC в каком-нибудь магазине.
- Продавец проверяет блокчейн, видит, что транзакция была, прошла ве проверки и попала в какой-нибудь блок, например #123.
- Продавец идет на почту и отправляет вам товар.
- Мошенник включает свою майнинг-ферму и начинает майнить, **начиная с блока #122**. Если у него достаточно мощностей, то он может обогнать всю остальную сеть и быстрее всех досчитать до блока #124. При этом транзакцию на 1000 BTC, он будет включать ни в один из блоков.

В результате продавец лишится товара и не получит своих денег.

Аппаратура для майнинга

	Miner	Hash Power	Price
	Antminer S5	1.16 TH/s	$139.99
	Antminer S7	4.73 TH/s	$489.99
	Antminer S9	14.0 TH/s	$3,000
	Avalon 6	3.50 TH/s	$559.95
	SP20 Jackson	1.3-1.7 TH/s	$90.00

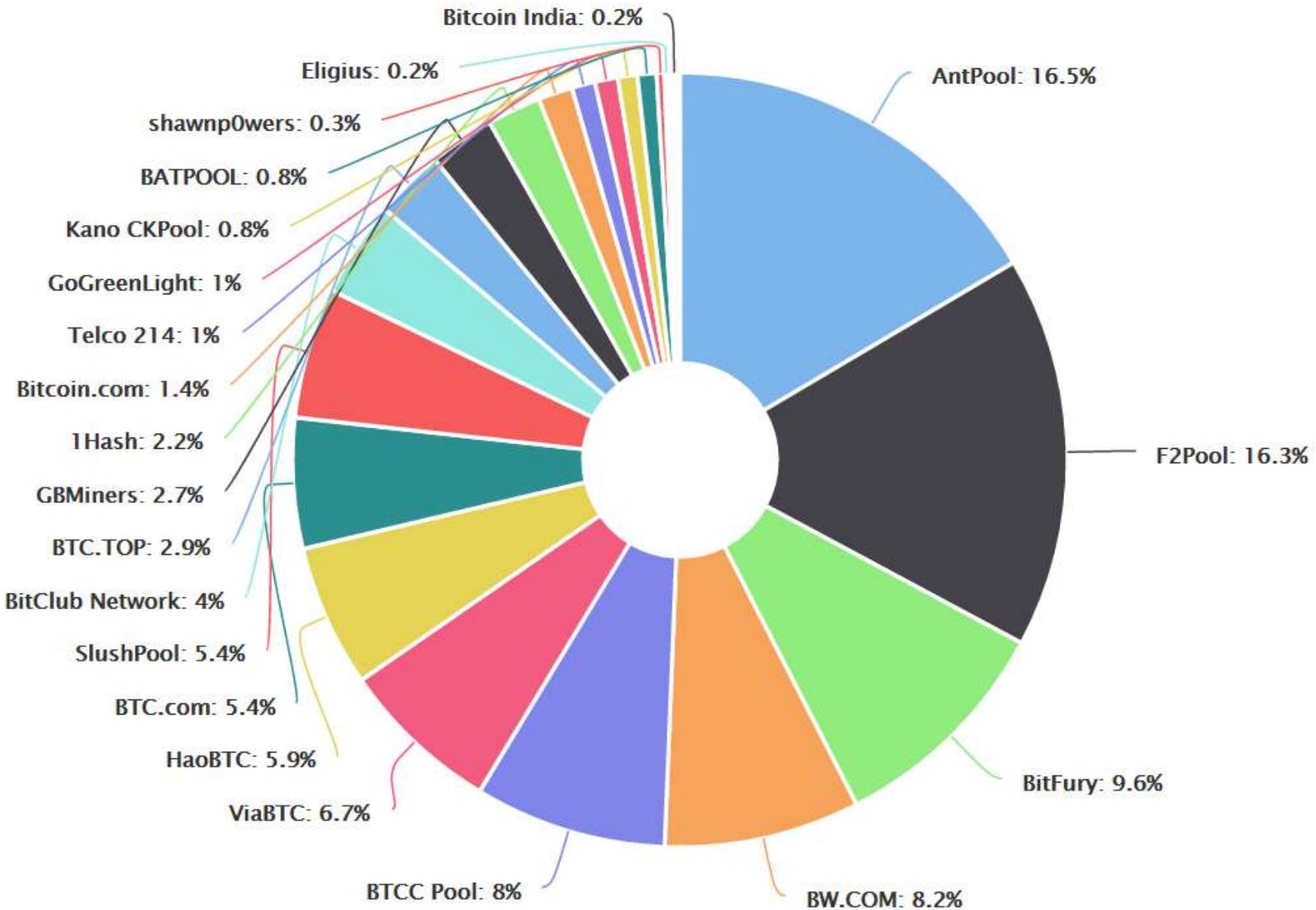
СМИ: физики-ядерщики задержаны за попытку майнить биткоины на суперкомпьютере

Как сообщает Telegram-канал Mash, в Сарове (Нижегородская область) задержаны сотрудники закрытого ядерного объекта — Федерального ядерного центра, которые попытались воспользоваться имеющимся у организации суперкомпьютером для майнинга биткоинов.

Сверхмощные суперкомпьютеры используются для выполнения сложнейших расчётов в научных и производственных целях. Однако у двух физиков-ядерщиков была задача попроще: намайнить с помощью имеющихся компьютерных мощностей побольше биткоинов, благо что по долгу службы они имели доступ к суперкомпьютеру. Реализовать план будущим крипто-предпринимателям не позволяла лишь одна проблема — суперкомпьютер не был подключён к Интернету. Однако, как оказалось, и это препятствие можно преодолеть.

Однако развернуться «на полную» им так и не удалось. После подключения суперкомпьютера к Сети работники центра попали в поле зрения Управления собственной безопасности, следившего за тем, чтобы на объекте не было дополнительных подключений к Сети. Далее предприимчивыми физиками занялись

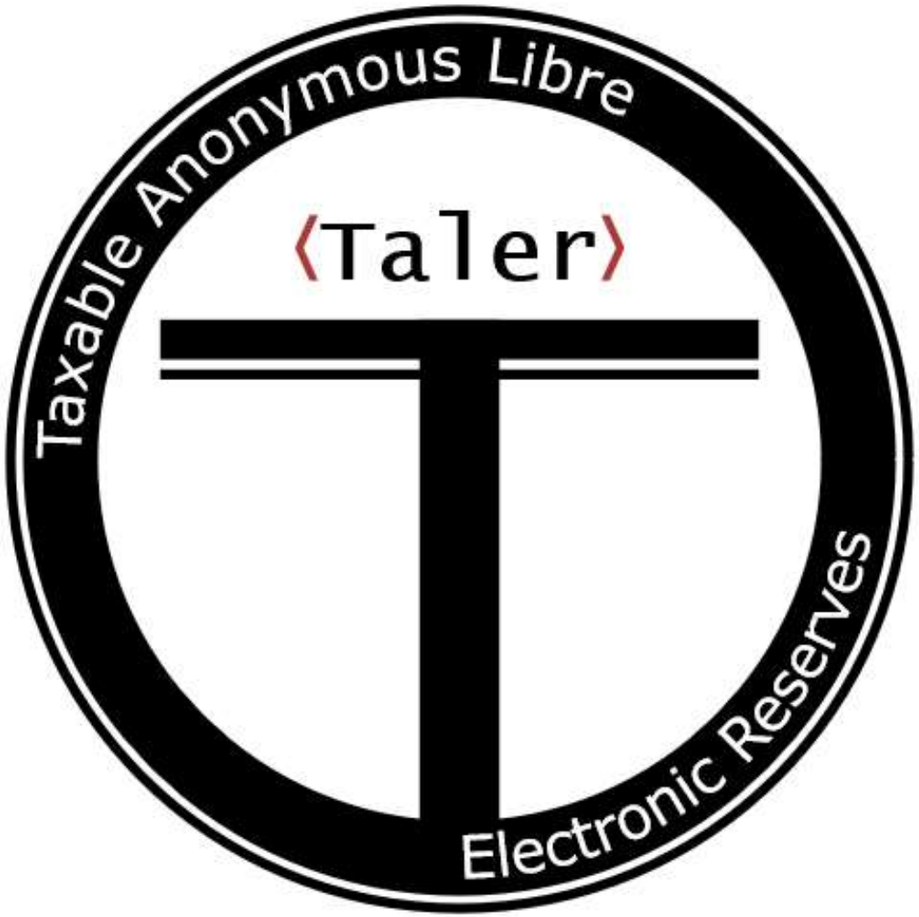
Пулы


Bitcoin India: 0.2%
Eligius: 0.2%
shawnp0wers: 0.3%
BATPOOL: 0.8%
Kano CKPool: 0.8%
GoGreenLight: 1%
Telco 214: 1%
Bitcoin.com: 1.4%
1Hash: 2.2%
GBMiners: 2.7%
BTC.TOP: 2.9%
BitClub Network: 4%
SlushPool: 5.4%
BTC.com: 5.4%
HaoBTC: 5.9%
ViaBTC: 6.7%
BTCC Pool: 8%
BW.COM: 8.2%
BitFury: 9.6%
F2Pool: 16.3%
AntPool: 16.5%

Критика

- Неэффективное использование ресурсов.
- Плохая масштабируемость блокчейна.
- Низкая пропускная способность (в транзакциях).
- Высокая латентность транзакций.
- Уязвимость к атаке 51%.
- Открытая доступность финансов.
- Невозможность обложения налогами.

GNU Taler



https://taler.net/videos/grothoff2014fossa.webm

?

vitaly.minko@gmail.com