



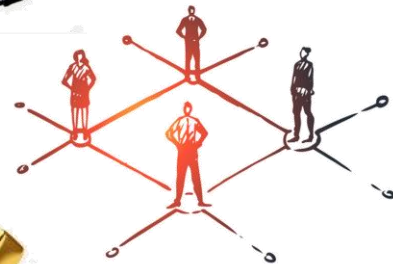
Архитектура блокчейн-систем

# Криптовалюты

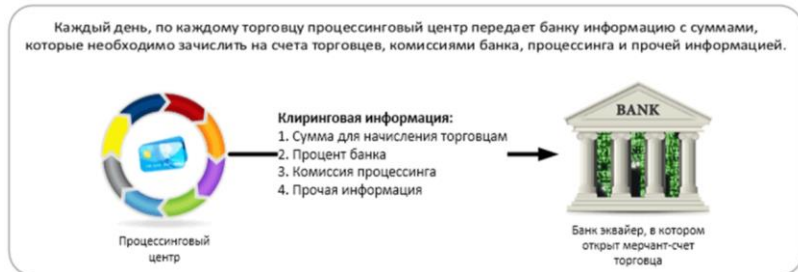
- Разновидность цифровой валюты, создание и учёт операций с которой обеспечивает децентрализованная платёжная система в автоматическом режиме
- Для защиты системы в неё интегрированы криптографические методы, используемые:
  - для подтверждения создания и переводов денежных единиц;
  - для генерации идентификаторов пользователей (адресов).

# Свойства криптовалют

- **Децентрализация.** Отсутствует орган администрирования, контролирующий эмиссию и перемещения криптовалюты. Эмиссия осуществляется всей сетью в соответствии с определёнными алгоритмами, платежи происходят непосредственно между участниками системы без посредников.
- **Открытость.** Возможность использования криптовалюты доступна любому пользователю, присоединившемуся к системе.
- **Не имеет внутренней стоимости.** Ценность криптовалюты определяется исключительно ожиданиями её пользователей.
- **Не имеет материального воплощения.** Хранится и перемещается только в электронном виде.
- **Псевдонимность.** Пользователи идентифицируются при помощи адресов, генерируемых криптографическим алгоритмом, информации о реальном субъекте в системе не хранится.



# Транзакция в обычной платежной системе









# Транзакция в криптовалюте



# Криптоэкономика

- В рейтинге [Coinmarketcap](https://coinmarketcap.com/) участвует около **10 тыс.** криптовалют.
- Суммарная капитализация рынка на конец 3 квартала 2024 г. – **2,3 трлн долл.**
- Доля Биткоина на рынке – около **56%**, Ethereum – **14%**.

	Name	Price	Market Cap 	Volume(24h) 
1	 <b>Bitcoin</b> BTC	\$65,562.37	\$1,295,519,971,984	\$17,687,431,985 269,720 BTC
2	 <b>Ethereum</b> ETH	\$2,666.60	\$320,963,879,237	\$11,599,371,284 4,349,677 ETH
3	 <b>Tether</b> USDT	\$1.00	\$119,431,014,222	\$42,317,502,559 42,312,616,620 USDT
4	 <b>BNB</b> BNB	\$600.58	\$87,643,988,576	\$1,953,866,011 3,253,861 BNB
5	 <b>Solana</b> SOL	\$156.81	\$73,535,607,599	\$1,526,745,776 9,739,056 SOL

# Криптокошелёк

- Средство для хранения закрытых ключей пользователя.
- Например, для алгоритма электронной подписи ECDSA
- **Закрытый ключ S**: случайное число между единицей и порядком подгруппы.
- **Открытый ключ O**:

$$O = SG$$

Пример:

- **закрытый ключ:**

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001

- **открытый ключ:**

0479be66 7ef9dcbb ac55a062 95ce870b 07029bfc db2dce28 d959f281 5b16f8179  
8483ada7 726a3c46 55da4fbf c0e1108a 8fd17b44 8a685541 99c47d08 ffb10d4b8

- **Bitcoin-адрес:**

**1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH**

# Криптокошелёк

- **Горячий** – кошелёк, средства с которого можно потратить в любое время. Приложение, веб-сайт или устройство, которое управляет закрытыми ключами.
- **Холодный** – кошелёк, не предназначенный для регулярного отправления криптовалюты, однако средства на него можно получить в любое время.  
Самый простой “холодный” кошелёк - лист бумаги, на котором записан закрытый ключ.
- **Кастодиальный** – кошелёк, который зарегистрирован на каком-либо сервисе-посреднике, например, на криптобирже. Управляется из веб-интерфейса, пароль можно быстро и легко восстановить, но при этом посредник знает вашу личность и имеет доступ к активам.
- **Некастодиальный** – предполагает, что все ключи и пароли находятся только у владельца. Если владелец что-то забудет/потеряет, восстановить доступ к кошельку будет невозможно.
- **Аппаратный** – устройства, подключаемые к ПК. Отличаются особо высокой степенью защиты.
- **Программный** – приложение на мобильном телефоне, ПК, интернет-сервере.





# Системы торговли криптовалютой

- **Централизованные криптобиржи (Centralized Exchange, CEX)** - платформы для торговли криптовалютами и производными инструментами, выступающие посредниками между продавцами и покупателями.
- **Децентрализованные криптобиржи (Decentralized Exchange, DEX)** – P2P-сервисы для обмена криптовалюты и производных инструментов между своими клиентами.
- **Криптовалютные обменные сервисы (криптообменники)** – сервисы, осуществляющие непосредственную торговлю криптовалютой с использованием собственных кошельков сервиса.

	Exchange	Trading volume(24h)	Weekly Visits	# Coins	Fiat Supported
1	 <b>Binance</b>	\$9,303,291,259	10,650,815	425	EUR, GBP, BRL and +8 more ⓘ
2	 <b>Coinbase Exchange</b>	\$1,132,370,148	33,921	258	USD, EUR, GBP
3	 <b>Bybit</b>	\$3,018,683,089	4,547,879	662	USD, EUR, GBP and +3 more ⓘ
4	 <b>OKX</b>	\$1,538,413,583	4,082,687	310	AED, ARS, AUD and +43 more ⓘ
5	 <b>Upbit</b>	\$2,010,386,002	1,032,611	215	KRW

# Bitcoin



**31 октября 2008 года**

Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System // <https://bitcoin.org/bitcoin.pdf>

Сатоши Накомото Биткоин: система цифровой пиринговой наличности // [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_ru.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf)

---

**3 января 2009 года**

Сгенерирован нулевой блок (блок генезиса) и получены первые 50 BTC

---

**12 января 2009 года**

Проведен первый перевод криптовалюты от одного пользователя другому

---

**22 мая 2010 года**  
**Bitcoin's Pizza Day**

Первая покупка реального товара за биткоины: американский разработчик Ласло Ханеч купил за 10 000 BTC две пиццы с доставкой.

---

**2011 год**

Основана компания BitPay - первый оператор по обработке платежей в биткоинах

---

**2012 год**

Создана некоммерческая организация Bitcoin Foundation, целью которой является стандартизация, защита и поощрение использования криптографических средств системы Биткоин на благо пользователей во всём мире.

# Bitcoin сегодня

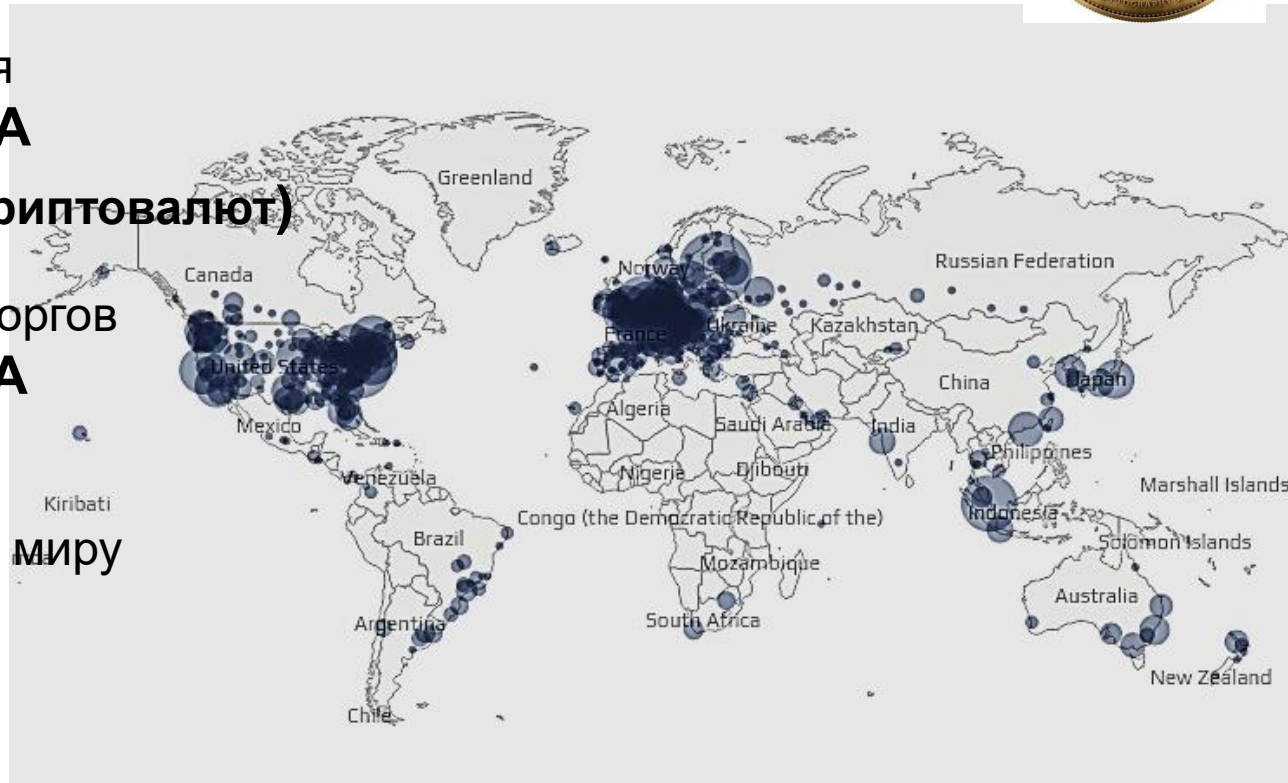
**1 BTC ~ 65 тыс. долл США**

Общая капитализация  
**1,3 трлн долл. США**

**(56 % всего рынка криптовалют)**

Ежесуточный объём торгов  
**14 млрд долл. США**

**Более 18 тыс.**  
узлов в сети по всему миру



# Bitcoin

- В блокчейне хранится информация о **транзакциях** – передаче цифровых денег между пользователями.
- Минимальная денежная единица **1 сатоши** =  $10^{-8}$  биткойна (BTC).
- Каждый пользователь в сети Биткойн имеет один или несколько **кошельков**, представляющих собой **пару ключей ECDSA**.
- Кошелёк идентифицируется **адресом**, получаемым хешированием открытого ключа, например:

[1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa](#)

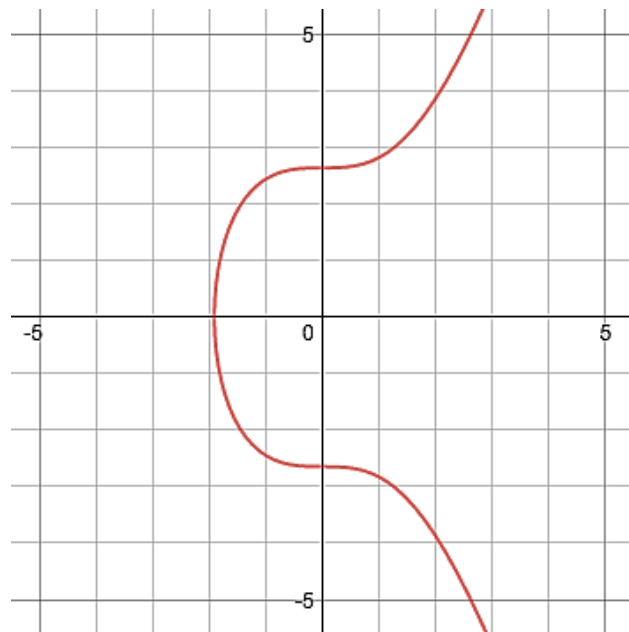
Первый адрес в сети Биткойн, принадлежащий Сатоши Накамото, на котором содержатся 50 замороженных биткойнов, полученных в качестве вознаграждения за генерацию нулевого блока.

# ECDSA в Bitcoin

- Уравнение эллиптической кривой:

$$y^2 = x^3 + 7$$

- Порядок поля =  $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 =$   
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF  
FFFFFFFF FFFFFFFE FFFFC2F
- Базовая точка **G**:  
 $x = 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB$   
 $2DCE28D9 59F2815B 16F81798,$   
 $y = 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448$   
 $A6855419 9C47D08F FB10D4B8$
- Порядок точки = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE  
BAAEDCE6 AF48A03B BFD25E8C D0364141
- Данная реализация известна как *secp256k1* и является частью семейства решений эллиптической кривой в области конечных полей, предложенных к использованию в криптографии.

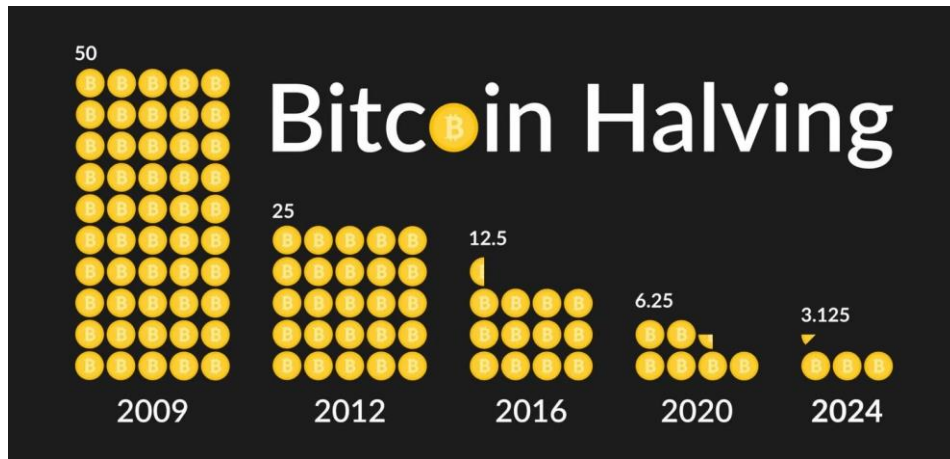


# Характеристики сети

- Сеть работает на консенсусе **Proof-of-Work**, узлы сети (майнеры) получают вознаграждение за создание блока, а также комиссию с транзакций, записанных в блок.
- Первоначальное вознаграждение за майнинг составляло 50 BTC. Оно уменьшается вдвое через каждые 210 тыс. блоков (примерно раз в 4 года) - **халвинг**. Последний халвинг произошёл в апреле 2024 года в блоке 840 000.

**3,125 биткоина** – текущее вознаграждение майнеров за блок

- Вознаграждение за блок станет менее 1 сатоши примерно в 2140 году. После этого выпуск новых биткоинов прекратится.
- Общее количество биткоинов в системе не может превысить **21 млн**
- К настоящему времени выпущено **19,76 млн BTC**, т.е. около **94%** всех монет в системе.



# Комиссия за транзакции

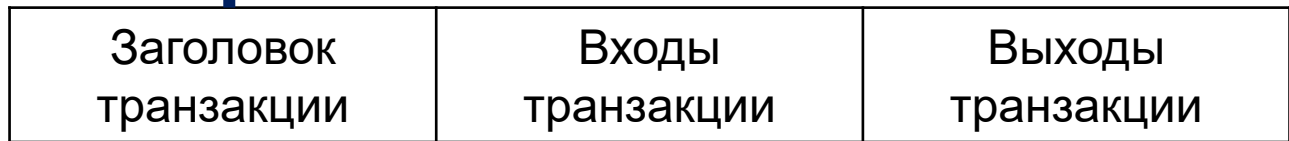
- Комиссия за транзакции определяется динамически в зависимости от загрузки сети.
- Размер комиссии зависит от размера транзакции и от приоритетности её обработки.
- Комиссия рассчитывается за 1 байт, поэтому чем больше входов и выходов содержит транзакция – тем комиссия выше.
- Максимальная комиссия берётся за включение транзакции в ближайший блок (10 мин.). Средний приоритет – включение в ближайшие 1 – 3 блока (ожидание до 30 мин.), низкий приоритет – ожидание до 6 блоков (до 1 часа).
- Текущую комиссию можно посмотреть на специальных ресурсах, например

<https://bits.media/fee/bitcoin/>

# Транзакции

## Служебная информация:

- версия;
- количество входов;
- количество выходов;
- время блокировки.



## Откуда получены деньги:

- идентификатор предыдущей транзакции;
- номер выхода предыдущей транзакции;
- скрипт подписи *scriptSig*.

## Куда направляются деньги:

- сумма (в сатоши);
- скрипт открытого ключа *scriptPubKey*.

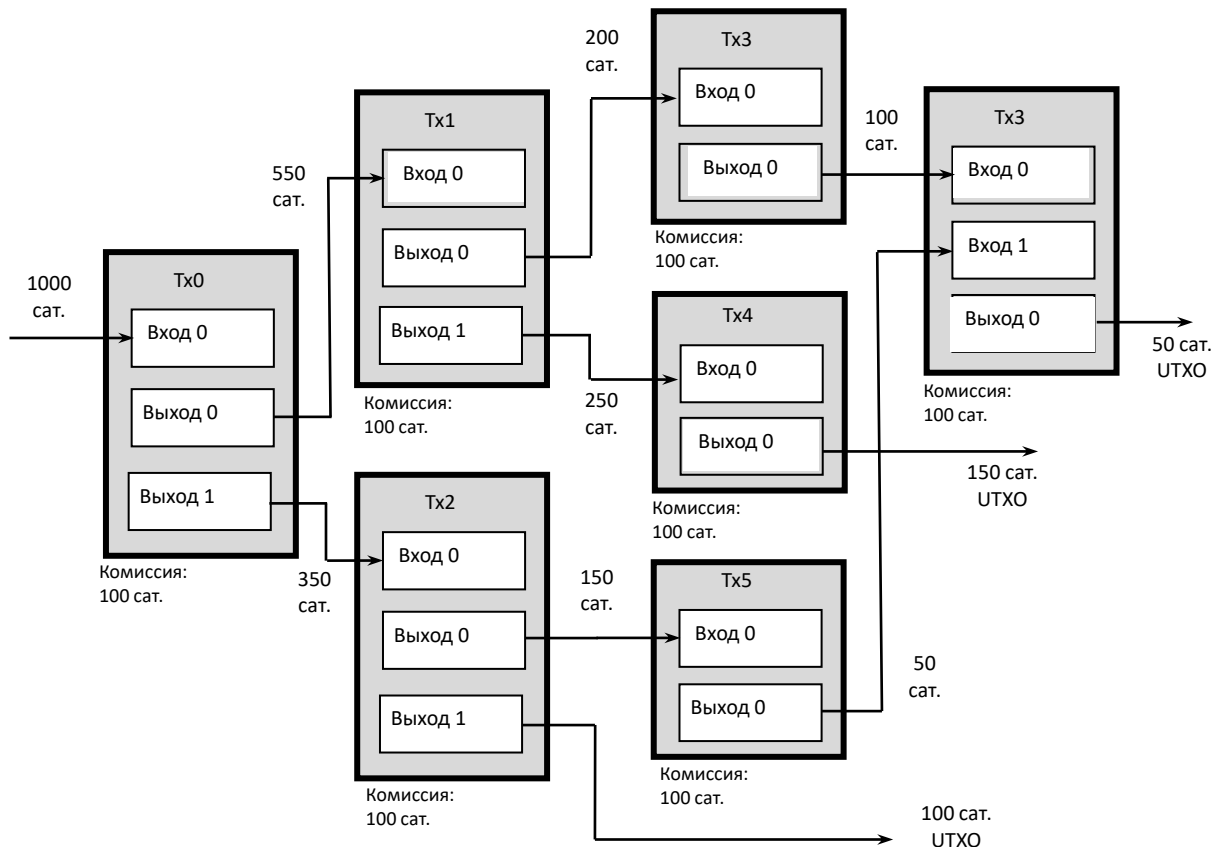


# Coinbase - транзакция

- Транзакция, перечисляющая вознаграждение узлу за добычу нового блока.
- Является первой по счёту транзакцией в блоке.
- Не содержит ссылок на предыдущие транзакции, так как распределяет вновь созданные системой деньги.

# Связь входов и выходов в транзакциях

- Все транзакции, кроме coinbase, тратят средства из непотраченных выходов предыдущих транзакций (UTXO, unspent transaction output).
- Разница между суммой входов и суммой выходов транзакции представляет комиссию узла за её включение в блок.



# Мемпул

- **Мемпул** – место, где все действительные транзакции ждут подтверждения сетью Bitcoin.
- Каждый узел в сети имеет свою версию мемпула, образуемого входящими в него транзакциями. Узлы распространяют подписанные транзакции по сети.
- Майнеры имеют возможность выбирать транзакции для включения в блок из мемпула. В первую очередь выбираются транзакции, имеющие наибольшую комиссию.
- Размер мемпула – это среднее количество транзакций в мемпулах отслеживаемых системой узлов.
- Большой размер мемпула указывает на большой сетевой трафик, что приведет к увеличению среднего времени подтверждения и более высокой платы за приоритет.
- При приближении размера пула к объему доступной памяти узел задает минимальную комиссию. Транзакции, в которых комиссия не достигает этого порога, удаляются из пула, после чего в пул допускаются только транзакции с достаточной комиссией.

<https://www.blockchain.com/ru/explorer/charts/mempool-size>

# Мемпул

Прежде чем поместить транзакцию в мемпул, узел должен выполнить следующие действия.

1. Проверить правильность синтаксиса транзакции.
2. Убедиться, что списки входов и выходов транзакции не пусты.
3. Убедиться, что размер транзакции в байтах меньше, чем максимальный размер блока.
4. Убедиться, что все выходы и их сумма являются допустимыми денежными значениями.
5. Убедиться, что транзакция не является coinbase-транзакцией.
6. Отклонить транзакцию, если транзакция уже есть в пуле или главной ветви блока.
7. Отклонить транзакцию, если какой-либо из ее входов ссылается на выход другой транзакции в пуле.

# Мемпул

8. Для каждого входа: если транзакция с соответствующим выходом является coinbase-транзакцией, убедиться, что она имеет как минимум 100 подтверждений (COINBASE\_MATURITY), в противном случае отклонить транзакцию.
9. Для каждого входа: если соответствующего входу выхода не существует, отклонить транзакцию.
10. Используя транзакции с соответствующими выходами, убедиться, что каждый вход и сумма являются допустимыми денежными значениями. Если сумма входов меньше, чем сумма выходов, отклонить транзакцию.
11. Если сумма входов меньше, чем сумма выходов, отклонить транзакцию.
12. Если комиссия за транзакцию (определяемая как разность между суммой входов и суммой выходов) слишком мала для включения транзакции в блок, отклонить транзакцию.

# Мемпул

<https://www.blockchain.com/ru/charts/mempool-size?timespan=60days>

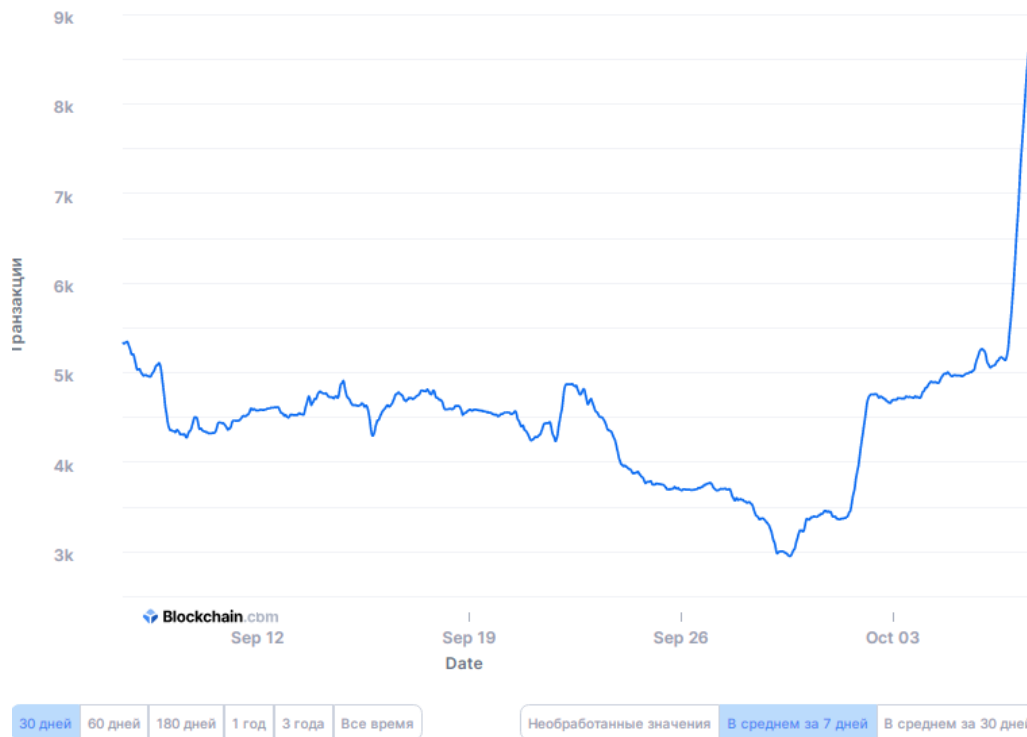


# Мемпул

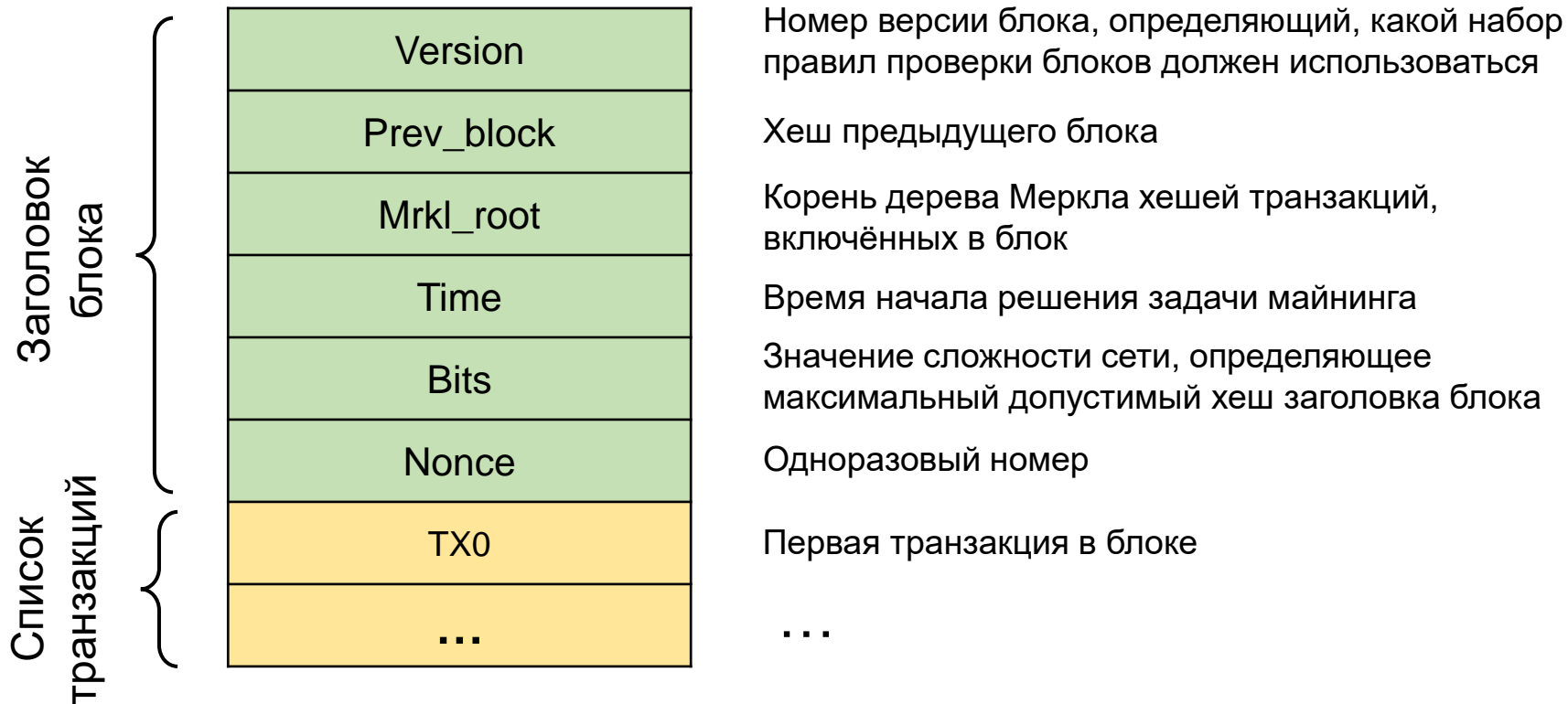
<https://www.blockchain.com/charts/mempool-count>

## Количество транзакций в мемпуле

Общее количество неподтвержденных транзакций в мемпуле.



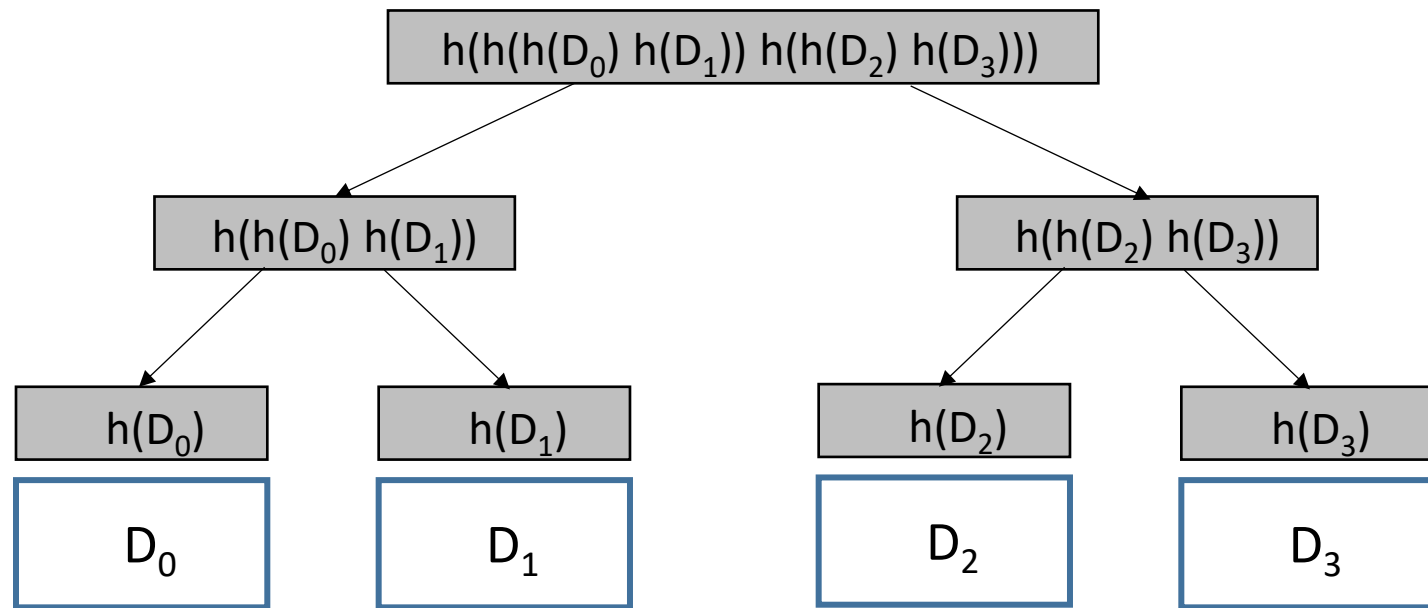
# Структура блока Биткоин





# Дерево Меркла

Бинарное дерево, каждая вершина которого содержит хеши следующих вершин. Используется для эффективного обобщения и проверки целостности больших наборов данных.



# Эффективность дерева Меркла

Количество транзакций	Прибл. размер блока	Размер пути (в хэшах)	Размер пути (в байтах)
16 транзакций	4 килобайта	4 хэшей	128 байт
512 транзакций	128 килобайт	9 хэшей	288 байт
2048 транзакций	512 килобайт	11 хэшей	352 байт
65535 транзакций	16 мегабайт	16 хэшей	512 байт

# Типы транзакций Bitcoin

- Начиная с версии ядра Bitcoin Core 0.9, можно выделить следующие стандартные типы транзакций:
  - Плата на открытый ключ (P2PK)
  - Плата на хэш открытого ключа (P2PKH)
  - Плата на скрипт (P2SH)
  - Коллективная подпись (Multisig)
  - Нулевые данные
- Основная часть транзакций в блокчейне – P2PKH. Небольшую часть занимают P2SH и Multisig.
- С версии Bitcoin Core 0.16 начали использоваться транзакции Segregated Witness (SegWit), позволяющие хранить электронные подписи в отдельной структуре данных вне основной цепочки.

# Язык Script для Bitcoin

- Транзакции в Bitcoin включают в себя скрипты для исполнения.
- Язык программирования скриптов так и называется "Script"
  - разработан специально для использования в сети Bitcoin;
  - очень узкая функциональность;
  - стеково-ориентированный;
  - ограничения по времени выполнения/памяти;
  - не имеет циклов.
- Программы на языке "Script" состоят из двух частей: **скрипта открытого ключа** (scriptPubKey), записанного в выход предыдущей транзакции и **скрипта подписи** (scriptSig), записанного во вход текущей транзакции.
- Транзакция считается корректной, если входной скрипт подписи проверяемой транзакции объединенный со скриптом открытого ключа предыдущей транзакции, отработывает без ошибок и по окончании работы в стеке находится значение **True**.

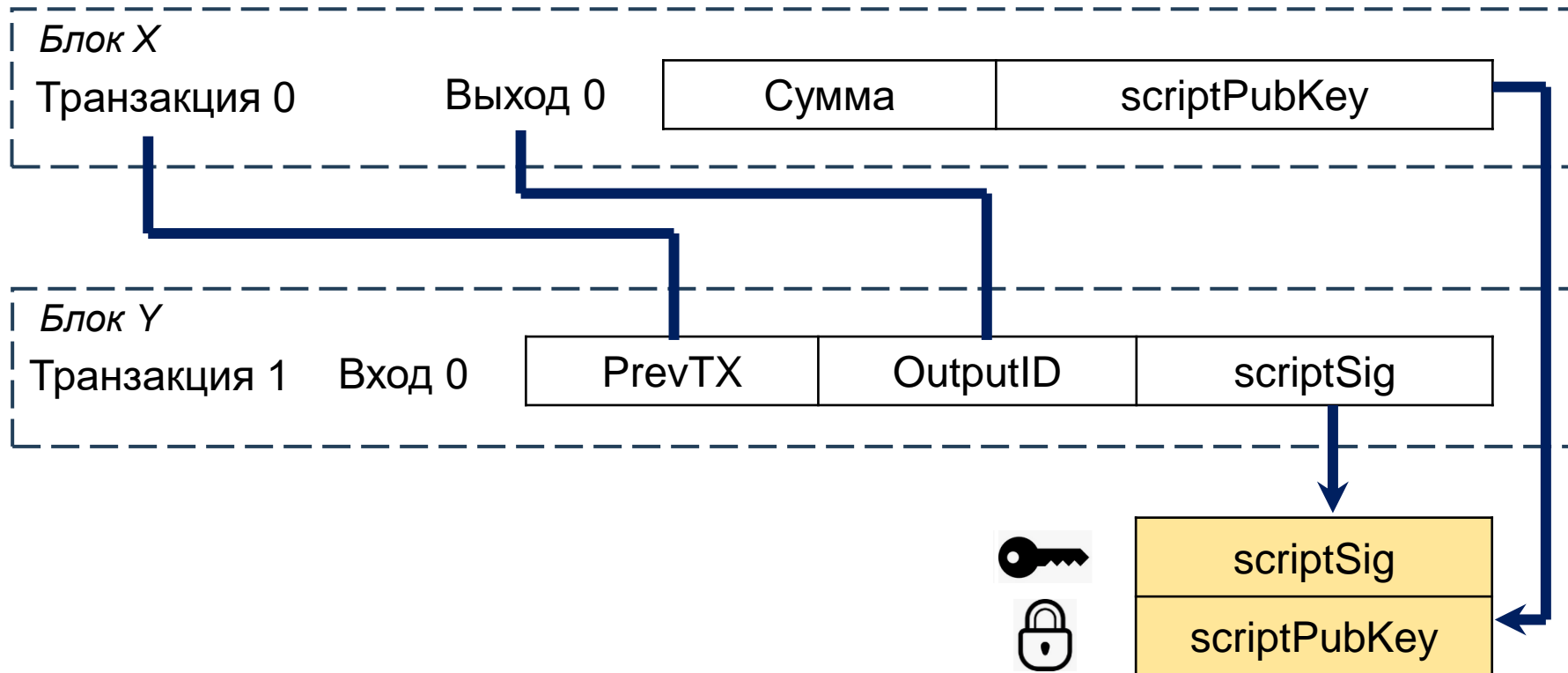
# Язык Script для Bitcoin

- Всего 256 кодов операций (15 не работают, 75 – в резерве):
  - Работа со стеком (загрузка/выгрузка данных)
  - Арифметические
  - Условные (if/then)
  - Криптографические (хэши, проверка подписи, проверка множественных подписей)
- Длина каждой операции (без обрабатываемых данных) – 1 байт.
- Примеры команд:

Word	Opcode	Hex	Input	Output	Description
OP_0, OP_FALSE	0	0x00	Nothing.	(empty value)	An empty array of bytes is pushed onto the stack. (This is not a no-op: an item is added to the stack.)
N/A	1-75	0x01-0x4b	(special)	data	The next <i>opcode</i> bytes is data to be pushed onto the stack
OP_PUSHDAT1	76	0x4c	(special)	data	The next byte contains the number of bytes to be pushed onto the stack.
OP_PUSHDAT2	77	0x4d	(special)	data	The next two bytes contain the number of bytes to be pushed onto the stack in little endian order.
OP_PUSHDAT4	78	0x4e	(special)	data	The next four bytes contain the number of bytes to be pushed onto the stack in little endian order.
OP_1NEGATE	79	0x4f	Nothing.	-1	The number -1 is pushed onto the stack.
OP_1, OP_TRUE	81	0x51	Nothing.	1	The number 1 is pushed onto the stack.
OP_2-OP_16	82-96	0x52-0x60	Nothing.	2-16	The number in the word name (2-16) is pushed onto the stack.

Word	Opcode	Hex	Input	Output	Description
OP_TOALTSTACK	107	0x6b	x1	(alt)x1	Puts the input onto the top of the alt stack. Removes it from the main stack.
OP_FROMALTSTACK	108	0x6c	(alt)x1	x1	Puts the input onto the top of the main stack. Removes it from the alt stack.
OP_IFDUP	115	0x73	x	x / x x	If the top stack value is not 0, duplicate it.
OP_DEPTH	116	0x74	Nothing	<Stack size>	Puts the number of stack items onto the stack.
OP_DROP	117	0x75	x	Nothing	Removes the top stack item.
OP_DUP	118	0x76	x	x x	Duplicates the top stack item.
OP_NIP	119	0x77	x1 x2	x2	Removes the second-to-top stack item.
OP_OVER	120	0x78	x1 x2	x1 x2 x1	Copies the second-to-top stack item to the top.
OP_PICK	121	0x79	xn ... x2 x1 x0 <n>	xn ... x2 x1 x0 xn	The item <i>n</i> back in the stack is copied to the top.
OP_ROLL	122	0x7a	xn ... x2 x1 x0 <n>	... x2 x1 x0 xn	The item <i>n</i> back in the stack is moved to the top.
OP_ROT	123	0x7b	x1 x2 x3	x2 x3 x1	The 3rd item down the stack is moved to the top.
OP_SWAP	124	0x7c	x1 x2	x2 x1	The top two items on the stack are swapped.
OP_TUCK	125	0x7d	x1 x2	x2 x1 x2	The item at the top of the stack is copied and inserted before the second-to-top item.
OP_2DROP	109	0x6d	x1 x2	Nothing	Removes the top two stack items.
OP_2DUP	110	0x6e	x1 x2	x1 x2 x1 x2	Duplicates the top two stack items.
OP_3DUP	111	0x6f	x1 x2 x3	x1 x2 x3 x1 x2 x3	Duplicates the top three stack items.
OP_2OVER	112	0x70	x1 x2 x3 x4	x1 x2 x3 x4 x1 x2	Copies the pair of items two spaces back in the stack to the front.
OP_2ROT	113	0x71	x1 x2 x3 x4 x5 x6	x3 x4 x5 x6 x1 x2	The fifth and sixth items back are moved to the top of the stack.
OP_2SWAP	114	0x72	x1 x2 x3 x4	x3 x4 x1 x2	Swaps the top two pairs of items.

# Связь входов и выходов в транзакциях



# Транзакция P2PK

- Самая первая транзакция в сети Биткоин между Сатоши Накамото и Хэлом Финни в 2009 году записана в блоке **170**.

- Выход транзакции содержит **скрипт открытого ключа**:

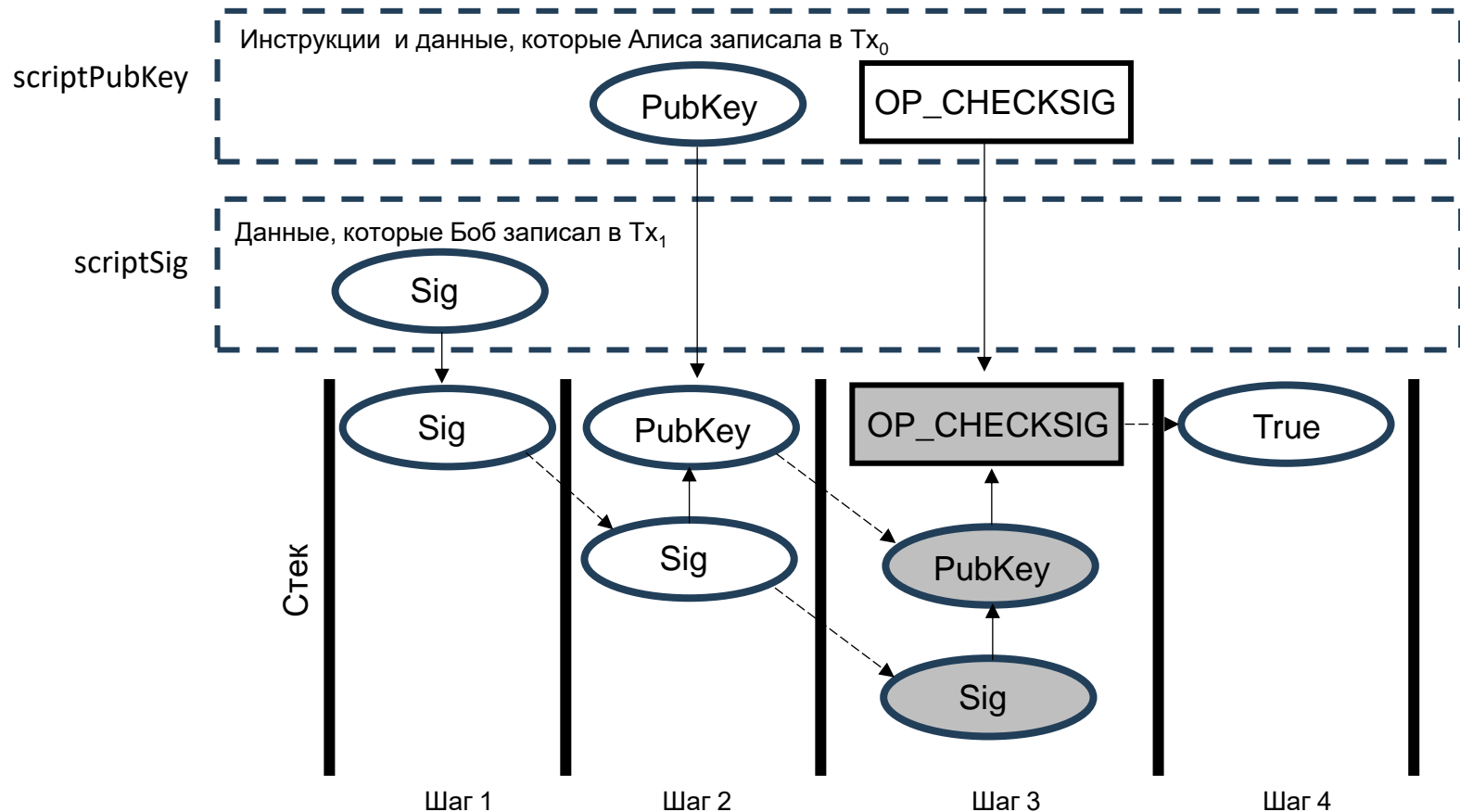
<b>4104ae1a62...</b>	# открытый ключ Хэла Финни
<b>OP_CHECKSIG</b>	# проверка подписи

- Переведённые средства были потрачены в блоке **92 240**. Вход соответствующей транзакции содержал скрипт подписи:

<b>47304402205...</b>	# подпись Хэла Финни
-----------------------	----------------------



# Транзакция P2PK



# Транзакция P2PKH

- В транзакции P2PK открытый ключ виден всем уже на выходе транзакции – снижает безопасность. Кроме того его надо передавать между пользователями для включения в scriptPubKey.

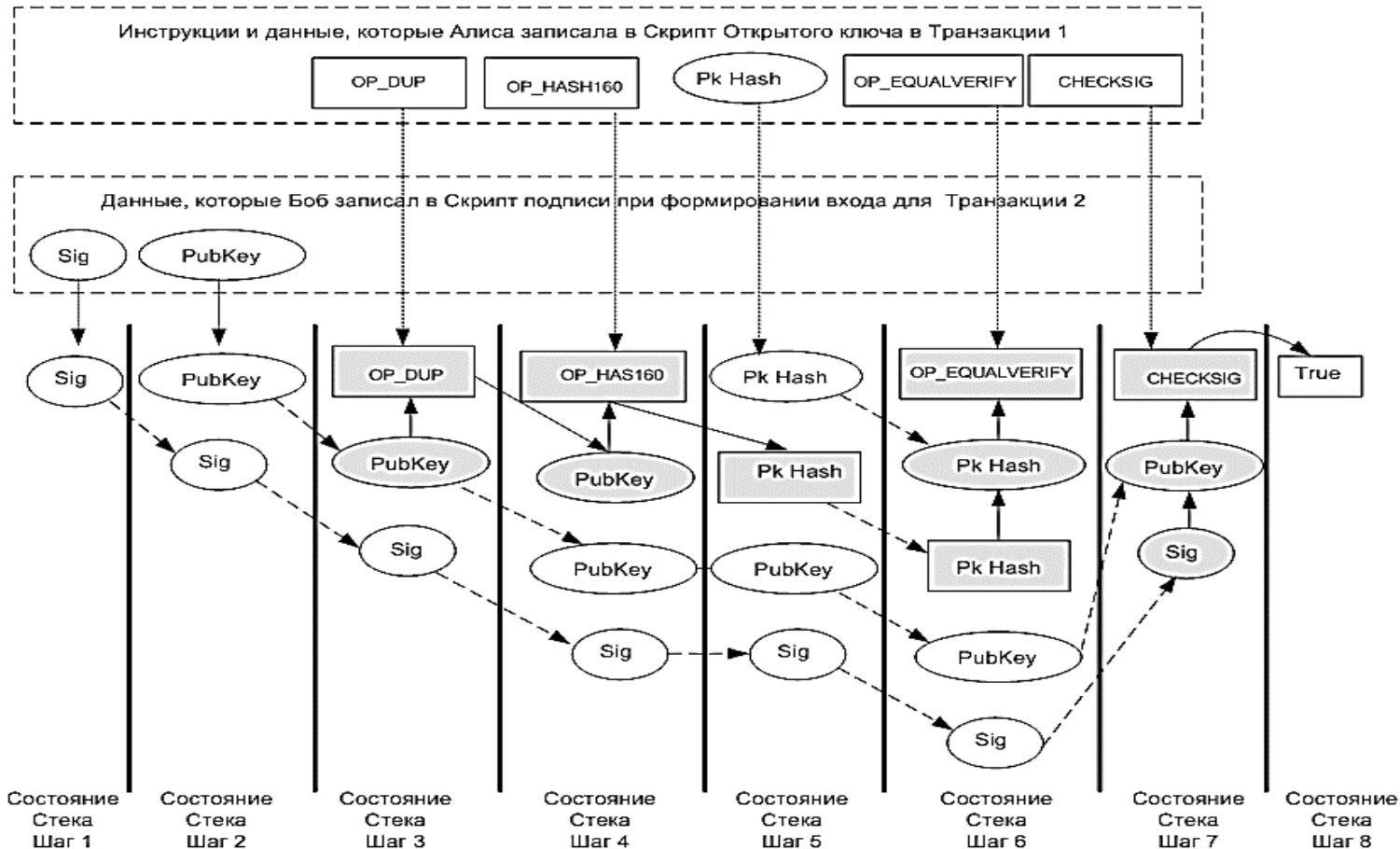
- **Скрипт открытого ключа scriptPubKey:**

<b>OP_DUP</b>	# копирование предыдущего значения в стеке
<b>OP_HASH160</b>	# хэширование предыдущего значения
<b>69e02f19...</b>	# хэш открытого ключа
<b>OP_EQUALVERIFY</b>	# проверка равенства
<b>OP_CHECKSIG</b>	# проверка подписи

- **Скрипт подписи scriptSig:**

<b>47304402203...</b>	# подпись
<b>0d40be0d3c...</b>	# открытый ключ

# Проверка скрипта Р2РКН

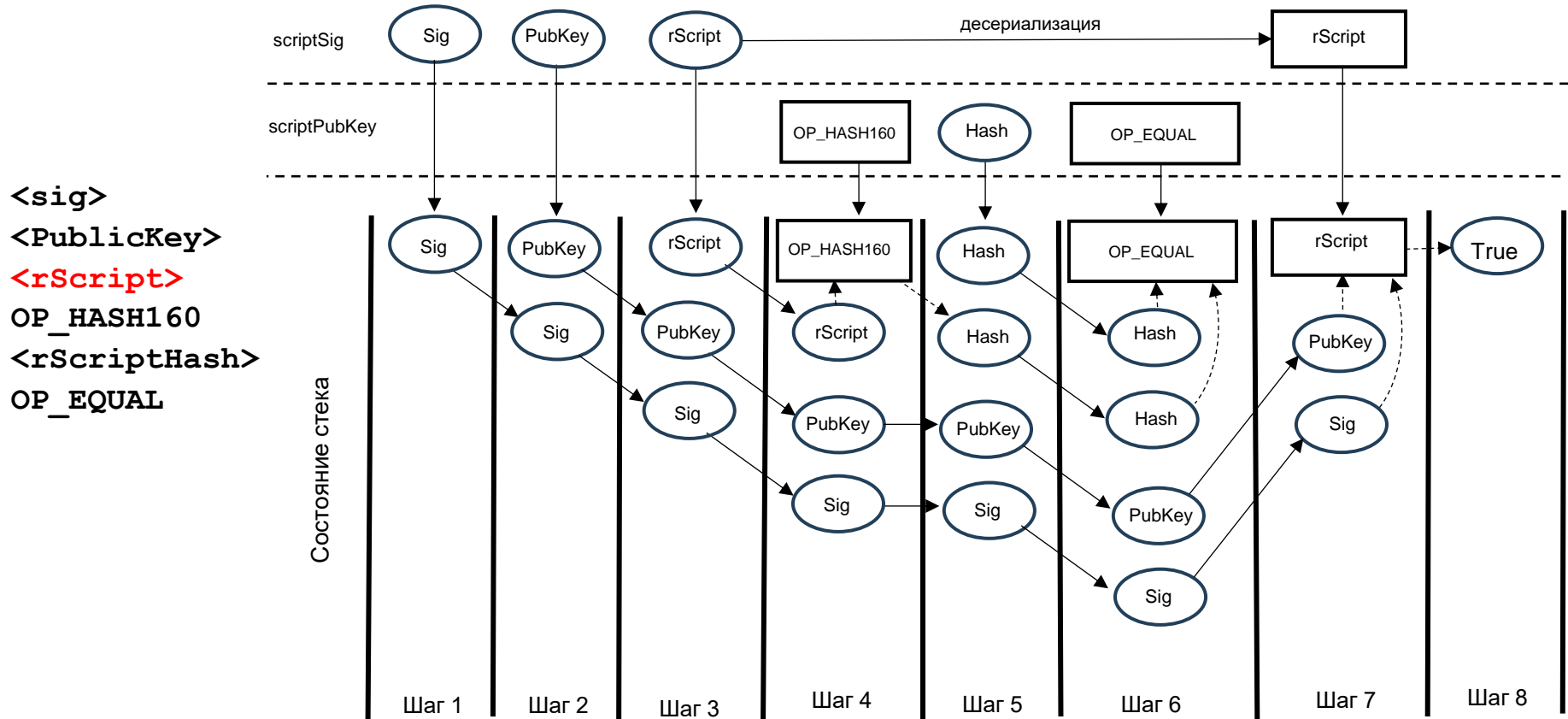


# Плата на скрипт (P2SH)

- Используется для перечисления средств на адрес смарт-контракта.
- Отправитель может не знать код скрипта, но получатель должен предоставить его хэш.
- При попытке потратить транзакцию скрипт выполняется в два этапа:
  1. *Выполняется проверка хеша скрипта*
  2. *В случае успеха выполняется сам скрипт.*
- Затраты на запись в транзакцию скрипта несёт получатель средств при их последующей трате.

Скрипт Открытого ключа	OP_HASH160 <Hash160 (redeemScript)> OP_EQUAL
Скрипт подписи	<sig> [sig] [sig ...] <PublicKey> [PublicKey ...] <redeemScript>

# Выполнение транзакции P2SH



# Коллективная подпись (Multisig)

- Используется если потратить полученные средства можно только с согласия  $M$  из  $N$  участников.
- Скрипт открытого ключа содержит ключи всех  $N$  участников.
- В скрипте подписи должно находиться  $M$  подписей для разблокировки транзакции.

Скрипт Открытого ключа	<code>&lt;m&gt; &lt;A pubkey&gt; [B pubkey] [C pubkey ...] &lt;n&gt; OP_CHECKMULTISIG</code>
Скрипт подписи	<code>OP_0 &lt;Asig&gt; [Bsig] [Csig ...]</code>

# Multisig 2/3



# Multisig 2/3

- Если Алиса и Боб удовлетворены исполнением контракта – они подписывают транзакцию средства переводятся.
- Если возникли разногласия – они обращаются к Виктору.
- Виктор и одна из сторон подписывают транзакцию и деньги либо возвращаются к Алисе, либо переводятся Бобу.

Скрипт Открытого ключа	OP_2 04a882d414e... 046ce31db9b... 0411ffd36c7... OP_3 OP_CHECKMULTISIG
Скрипт подписи	OP_0 30440220762... 3045022100a...



# Транзакции с нулевыми данными

Скрипт Открытого ключа	OP_RETURN <от 0 до 40 байт данных>
Скрипт подписи	Отсутствует, т.к. транзакции с нулевыми данными не могут быть потрачены

# Стандартные транзакции

Начиная с версии ядра Bitcoin Core 0.9.3, стандартные транзакции должны соответствовать следующим условиям:

- Транзакция должна быть завершена: ее время блокировки должно быть в прошлом либо меньше или равно текущей высоте блока.
- Размер транзакции должен быть меньше 100 000 байт. Это примерно в 200 раз больше, чем типичная транзакция P2PKH с одним входом и одним выходом.
- Каждый из скриптов подписи транзакции должен быть меньше 1650 байт. Этого достаточно, чтобы выполнить проверку 15 транзакций с несколькими подписями вида P2SH с использованием сжатых открытых ключей.
- Открытые транзакции с несколькими подписями, которые не являются транзакциями типа P2SH и для которых требуется более 3 открытых ключей, в настоящее время являются нестандартными.
- Задача скрипта подписи заключается в том, чтобы поместить данные в стек для выполнения проверки. Он не может использовать коды операций, за исключением тех, которые помещают данные в стек.
- Выход транзакции не может быть меньше, чем  $1/3$  от того количества сатоши, которое необходимо потратить в качестве комиссии за транзакцию. Исключение составляют стандартные транзакции с нулевыми данными, у которых выход должен содержать нулевую сумму.

# Развитие сети Биткоин

- **Bitcoin Improvement Proposal (BIP)** - документ, предоставляющий информацию сообществу биткоина, в основном разработчикам, о предлагаемых улучшениях в сети.
- Выкладываются на GitHub для обсуждения сообществом:

<https://github.com/bitcoin/bips>

- Если предложение поддерживается разработчиками, в ПО вносятся соответствующие изменения.
- Однако, каждый узел **самостоятельно** решает, устанавливать ли новую версию ПО или нет. В результате работы на разных узлах разных версий ПО блоки могут формироваться по разным алгоритмам – в блокчейне возникают форки.

# Софтфорки и хардфорки

- **Софтфорк** – обновление с обратной совместимостью, то есть обновленные узлы могут взаимодействовать с узлами со старой версией ПО. Обычно софтфорк происходит при добавлении новых правил, которые не противоречат старым.

## Пример: софтфорк SegWit

- Изменил формат блоков и транзакций, цифровые подписи были вынесены в отдельное хранилище.
- Старые узлы все еще могли проверять блоки и транзакции (изменение формата не противоречило правилам), но просто не понимали их. Для прочтения определенных полей и анализа дополнительных данных необходимо переключение на новое программное обеспечение.
- Даже через несколько лет после активации SegWit ещё не все узлы в сети были обновлены.

# Софтфорки и хардфорки

- **Хардфорк** – обновление программного обеспечения, несовместимое с предыдущими версиями. Обычно это происходит, когда изменения ПО приводят к противоречию с существующим правилам работы сети.
- Узлы, использующие новую версию ПО, не могут взаимодействовать со старыми.
- В результате блокчейн разделяется на две отдельные сети: одну со старыми правилами и другую — с новыми.

## Пример: хардфорк BCH

- Изменил максимальный размер блока, увеличив его до 8 Мб.
- Старые узлы не принимали блоки, генерируемые новым ПО.
- В результате с блока № 478 559 (1 августа 2017) сеть разделилась на классический Bitcoin (BTC) и Bitcoin Cash (BCH).
- Так как все блоки до этого у сетей одинаковы, каждый адрес BTC получил то же самое количество монет в сети BCH.

# Блокчейн-эксплореры

- Информация, хранящаяся в публичных блокчейнах, является общедоступной.
- Она может быть получена непосредственно из цепочки – для этого нужно установить себе на компьютер программное обеспечение узла блокчейна и скачать её копию.
- Доступ к информации из цепочки также предоставляют сторонние сервисы, например при криптобиржах и т.д. – блокчейн-эксплореры.
- Доступ возможен из обычного браузера:

<https://www.blockchain.com/explorer/>

<https://blockchair.com/>

<https://etherscan.io/>

# Blockchain.com

Возможности поиска:

- По номеру блока в цепочке
- По адресу пользователя
- По хешу блока/транзакции

# Генезис-блок

- Изучить содержимое генезис-блока Биткойна
  - Когда он добыт?
  - Кто его добыл?
  - Сколько транзакций он содержит?
  - Были ли потрачены средства, полученные в coinbase-транзакции?
  - Каков текущий баланс адреса, на который были переведены средства в coinbase-транзакции?
  - Сколько транзакций было совершено с участием этого адреса?
  - Когда была совершена последняя транзакция с этого адреса? Сколько средств было переведено в этой транзакции?



# Первая транзакция между пользователями

- Перевод 10 BTC от Сатоши Накамото Хэлу Финни
- Хеш транзакции:

[f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16](#)

# Bitcoin Pizza Day

- 22 мая 2010 года американский криптоэнтузиаст Ласло Ханеч заплатил своему коллеге Джереми Стердиванту 10 000 BTC за 2 пиццы Papa John's.
- Это событие вошло в историю развития криптовалют как Bitcoin Pizza Day и считается первой покупкой реального товара за биткоины.
- Транзакция по переводу средств записана в блоке Биткойна № 57 043

## Задание:

1. Сколько входов использовано в данной транзакции?
2. Какую комиссию уплатил Ханеч за эту транзакцию?
3. Потратил ли Стердивант полученные средства?
4. Сколько средств сейчас находится на счетах Ханеча и Стердиванта, которые участвовали в транзакции?



# Хардфорк BCH

- Хардфорк, который привёл к появлению Bitcoin Cash (BCH), произошёл 1 августа 2017 года в блоке № 478 559.
- Сравните предыдущие и данные блоки в цепочках BTC и BCH.
- Адреса, существовавшие в сети Биткоин до хардфорка, продублировались в BCH.
- Сравните транзакции и балансы адреса Сатоши Накамото, существующего в цепочках BTC и BCH.

[1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa](#)

# API сервиса Blockchain.info

[https://www.blockchain.com/ru/explorer/api/blockchain\\_api](https://www.blockchain.com/ru/explorer/api/blockchain_api)

- Блок по хешу:

[https://blockchain.info/rawblock/<block\\_hash>](https://blockchain.info/rawblock/<block_hash>)

- Транзакция по хешу:

[https://blockchain.info/rawtx/<tx\\_hash>](https://blockchain.info/rawtx/<tx_hash>)

- Блок по порядковому номеру (высоте):

[https://blockchain.info/block-height/<block\\_height>?format=json](https://blockchain.info/block-height/<block_height>?format=json)

- Блоки по времени (за 24 часа):

[https://blockchain.info/blocks/<time\\_in\\_ms>?format=json](https://blockchain.info/blocks/<time_in_ms>?format=json)

# API сервиса Blockchain.info

- Один адрес:

[https://blockchain.info/rawaddr/<bitcoin\\_address>](https://blockchain.info/rawaddr/<bitcoin_address>)

- Несколько адресов:

<https://blockchain.info/multiaddr?active=<address>|<address>>

- Непотраченные транзакции (UTXO):

<https://blockchain.info/unspent?active=<address>>

- Баланс адреса:

<https://blockchain.info/balance?active=<address>>

# Домашнее задание

Изучить самостоятельно API сервиса blockchain.info

[https://www.blockchain.com/ru/explorer/api/blockchain\\_api](https://www.blockchain.com/ru/explorer/api/blockchain_api)