Феномен криптовалюты «Биткоин». Построение математических моделей децентрализованных информационных систем, реализующих функции платежных систем криптовалют. Подходы к комплексной оценке безопасности, в том числе оценке криптографической стойкости

Директор по развитию ЗАО «БЕЛТИМ СБ»,
директор ассоциации «РусКрипто»
Комисаренко Владимир Владимирович
229@tut.by,
специалист отдела информационной безопасности ОАО «Банк Москва-Минск»
Роговой Александр Сергеевич

Про Биткоин говорят:

На фундаментальном уровне Bitcoin является прорывом в области компьютерных наук — тех, что опираются на 20 лет исследований криптографических валют и 40 лет работы в области криптографии тысяч исследователей по всему миру.

— Марк Андрессен

Про Биткоин говорят:

Криптовалюты — это очень интересный международный эксперимент, который ломает парадигму валютной эмиссии. И их определено не стоит запрещать, но следует попытаться понять, изучить и, возможно, начать правильно регулировать.

— Герман Греф

Оценка ситуации с Биткоин (США)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Federal Bureau of Investigation

Intelligence Assessment

Intelligence Assessment

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

24 April 2012

UNCLASSIFIED

(U) A Bitcoin logo from https://en.bitcoin.it.

Prepared by

FBI

Directorate of Intelligence

Cyber Intelligence Section and Criminal Intelligence Section

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Оценка ситуации с Биткоин (Россия)

Весь сайт → Пресс-центр

Пресс-центр

Центральный банк Российской Федерации (Банк России)
Пресс-служба

107016, Москва, ул. Неглинная, 12
тел.: +7 495 771-44-17, +7 495 771-46-69; факс: +7 495 771-49-32;
www.cbr.ru

Информация

Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн

Банк России отмечает, что в последнее время в мире получили определенное распространение так называемые «виртуальные валюты», в частности, Биткойн. По «виртуальным валютам» отсутствует обеспечение и юридически обязанные по ним субъекты. Операции по ним носят спекулятивный характер, осуществляются на так называемых «виртуальных биржах» и несут высокий риск потери стоимости.

Банк России предостерегает граждан и юридических лиц, прежде всего кредитные организации и некредитные финансовые организации, от использования «виртуальных валют» для их обмена на товары (работы, услуги) или на денежные средства в рублях и в иностранной валюте.

Согласно статье 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» выпуск на территории Российской Федерации денежных суррогатов запрещается.

В связи с анонимным характером деятельности по выпуску «виртуальных валют» неограниченным кругом субъектов и по их использованию для совершения операций граждане и юридические лица могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.

Банк России предупреждает, что предоставление российскими юридическими лицами услуг по обмену «виртуальных валют» на рубли и иностранную валюту, а также на товары (работы, услуги) будет рассматриваться как потенциальная вовлеченность в осуществление сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

27 января 2014 года

При использовании материала ссылка на Пресс-службу Банка России обязательна.

Основная идея, Wei Dai:

I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender and encrypted to its receiver.

1. The creation of money.
The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities
2. The transfer of money. If Alice (owner of pseudonym K_A) wishes to transfer X units of money to Bob (owner of pseudonym K_B), she broadcasts the message "I give X units of money to K_B" signed by K_A.
3. The effecting of contracts.
4. The conclusion of contracts.
5. The enforcement of contracts.

Базовая статья:

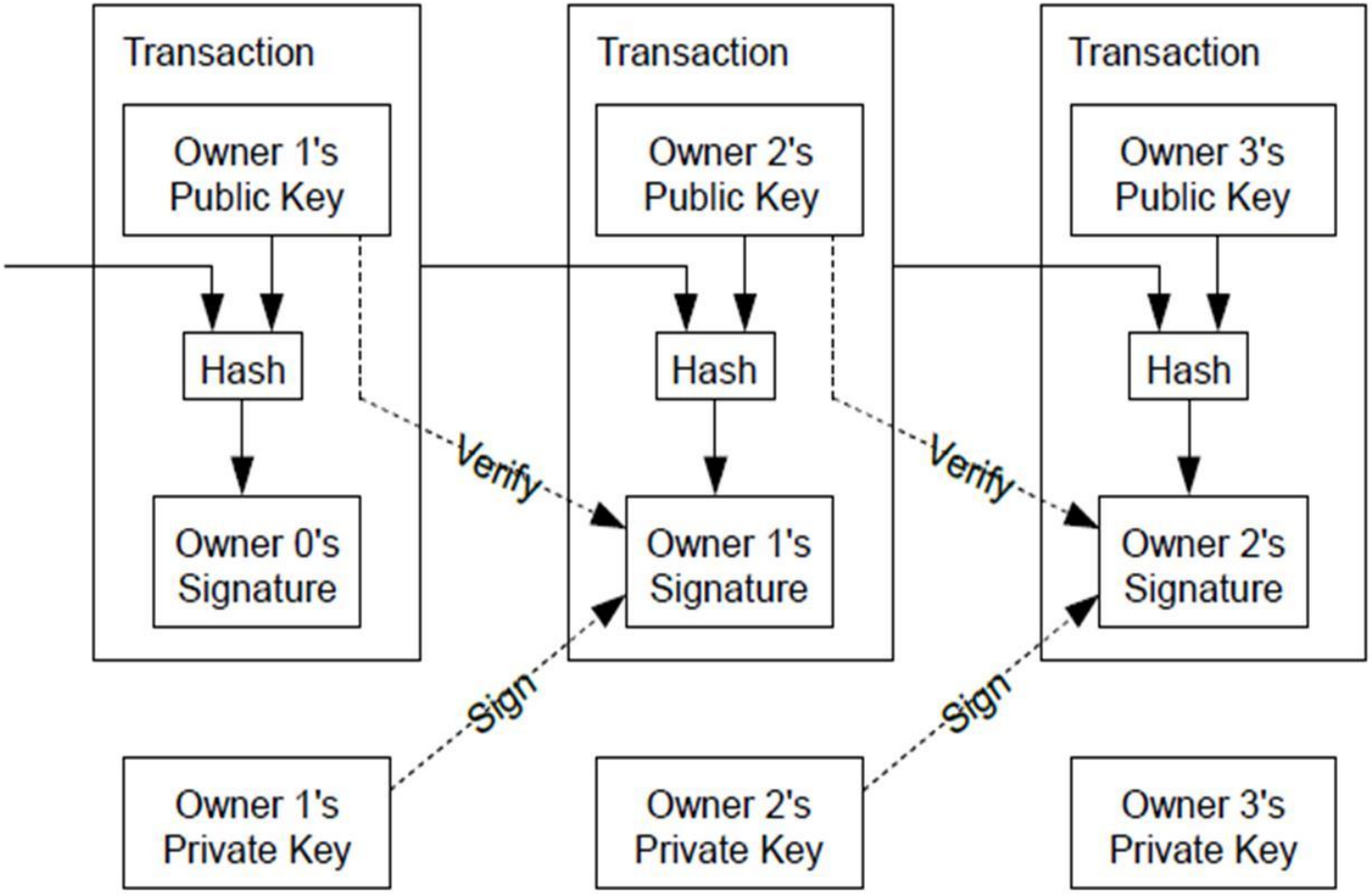
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

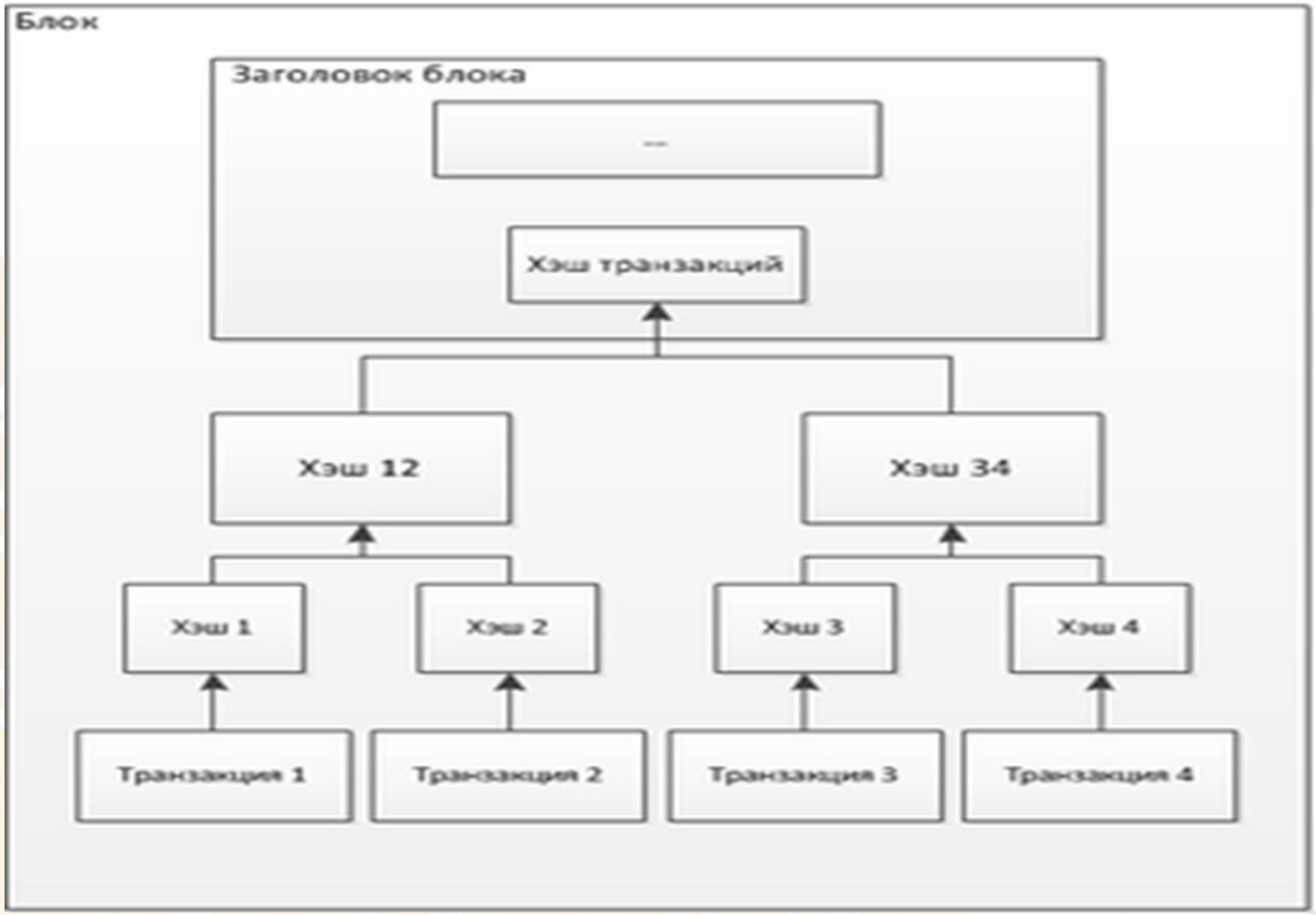
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Личность Satoshi Nacamoto никому не известна

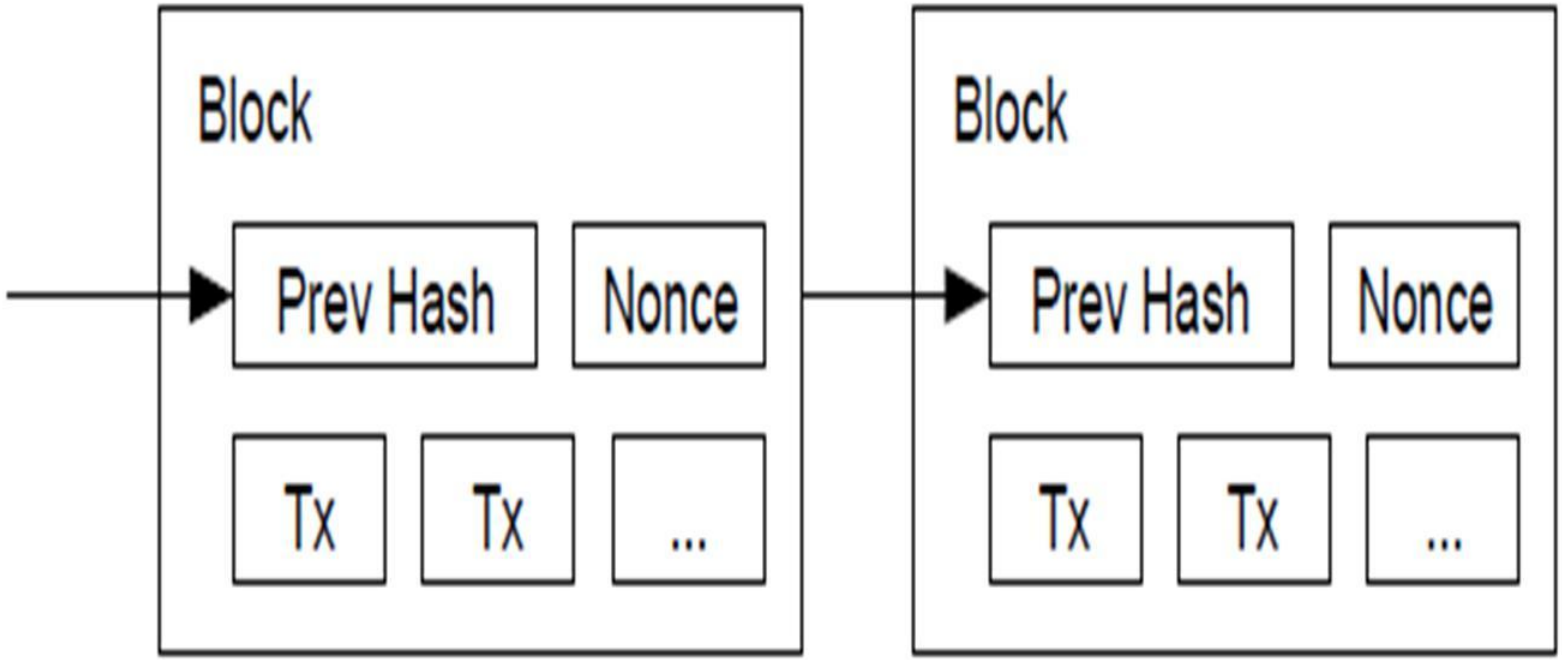
Транзакции:


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Verify
Owner 1's Signature
Sign
Owner 1's Private Key
Transaction
Owner 2's Public Key
Hash
Verify
Owner 2's Signature
Sign
Owner 2's Private Key
Transaction
Owner 3's Public Key
Hash
Owner 3's Signature
Owner 3's Private Key

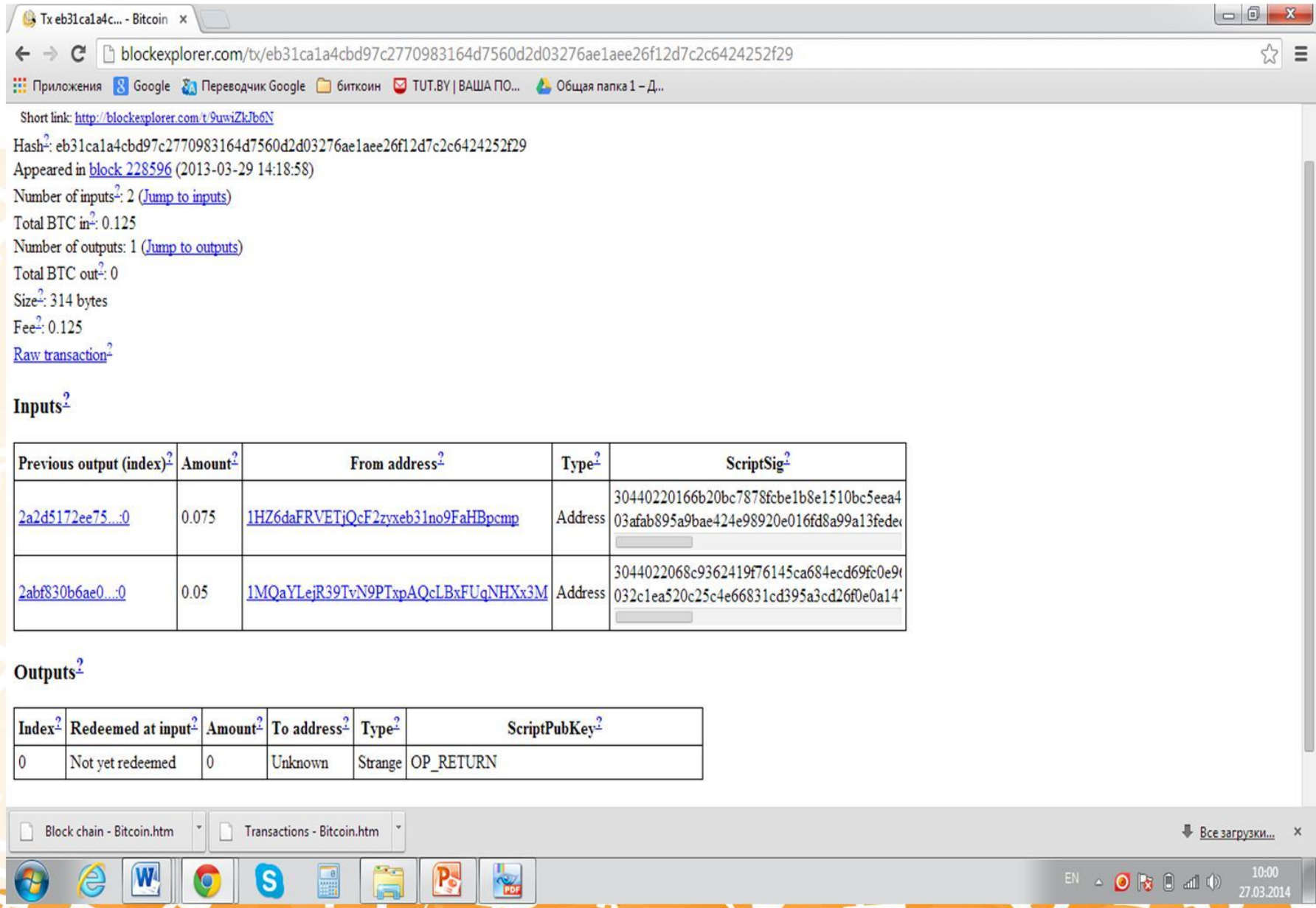
Структура блока:



Цепочка блоков:



Транзакция:



Tx eb31ca1a4c... - Bitcoin

blockexplorer.com/tx/eb31ca1a4cbd97c2770983164d7560d2d03276ae1aee26f12d7c2c6424252f29

Приложения | Google | Переводчик Google | биткоин | TUT.BY | ВАША ПО... | Общая папка 1 – Д...

Short link: http://blockexplorer.com/t/9uwiZkJb6N

Hash: eb31ca1a4cbd97c2770983164d7560d2d03276ae1aee26f12d7c2c6424252f29

Appeared in block 228596 (2013-03-29 14:18:58)

Number of inputs: 2 (Jump to inputs)

Total BTC in: 0.125

Number of outputs: 1 (Jump to outputs)

Total BTC out: 0

Size: 314 bytes

Fee: 0.125

Raw transaction

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
2a2d5172ee75...:0	0.075	1HZ6daFRVETjQcF2zyxeb31no9FaHBpcmp	Address	30440220166b20bc7878fcbe1b8e1510bc5eea4 03afab895a9bae424e98920e016fd8a99a13fede
2abf830b6ae0...:0	0.05	1MQaYLejR39TvN9PTxpAQcLBxFUqNHXx3M	Address	3044022068c9362419f76145ca684ecd69fc0e9 032c1ea520c25c4e66831cd395a3cd26f0e0a14

Outputs

Index	Redeemed at input	Amount	To address	Type	ScriptPubKey
0	Not yet redeemed	0	Unknown	Strange	OP_RETURN

Block chain - Bitcoin.htm | Transactions - Bitcoin.htm | Все загрузки...

EN 10:00 27.03.2014

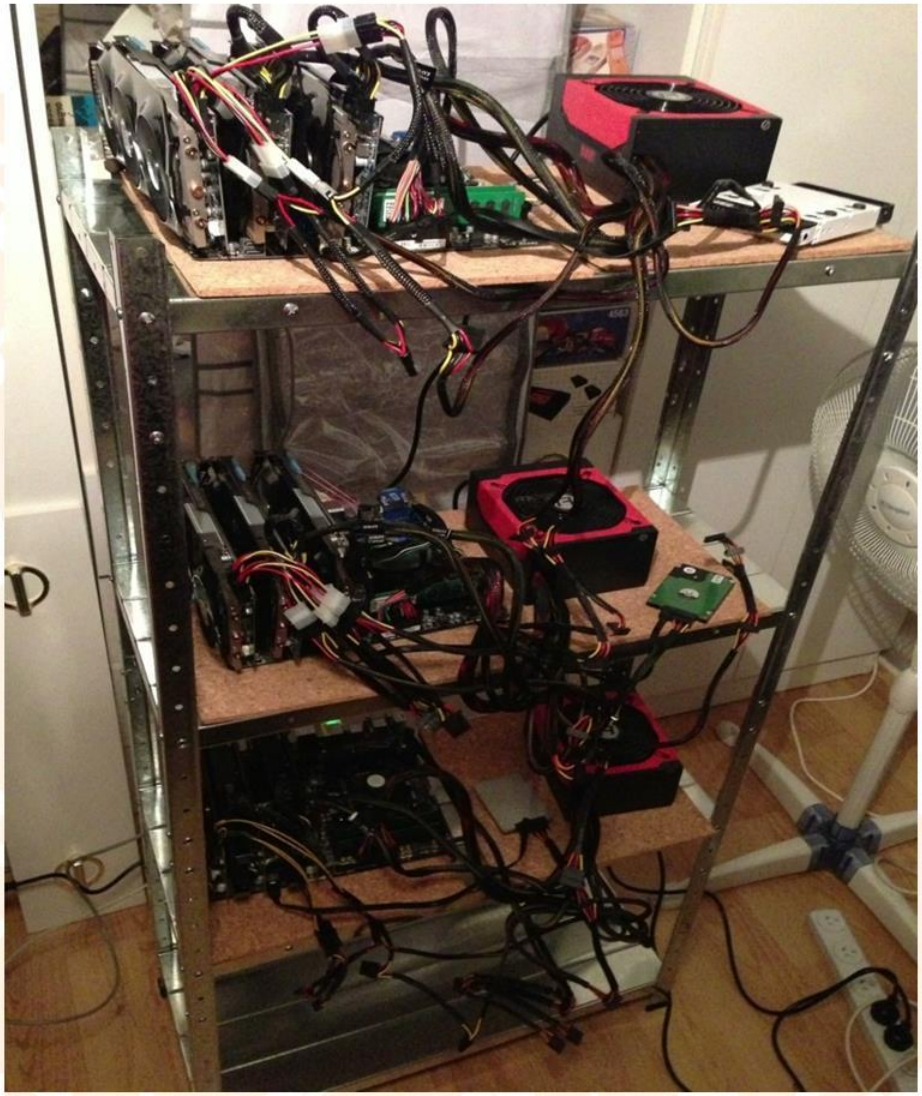
Понятие сложности

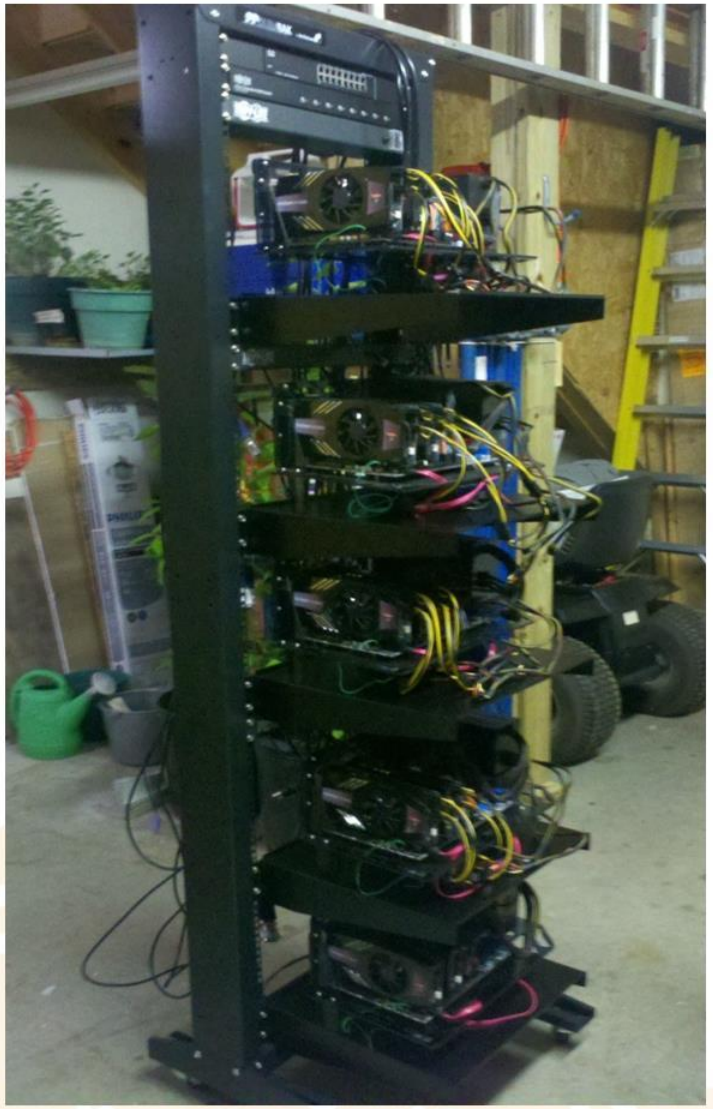
Сложность регулируется сетью путем ее пересчета после нахождения очередных 2016 блоков.

Вычисляется время нахождения очередных 2016 блоков. Если оно больше предыдущего значения, то сложность пропорционально уменьшается. Иначе – увеличивается.

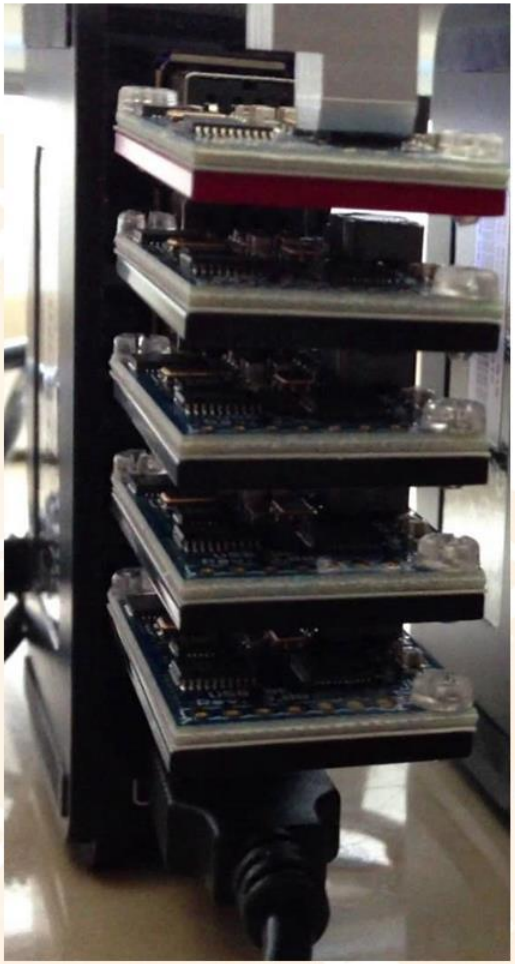
Изменяется значение цели

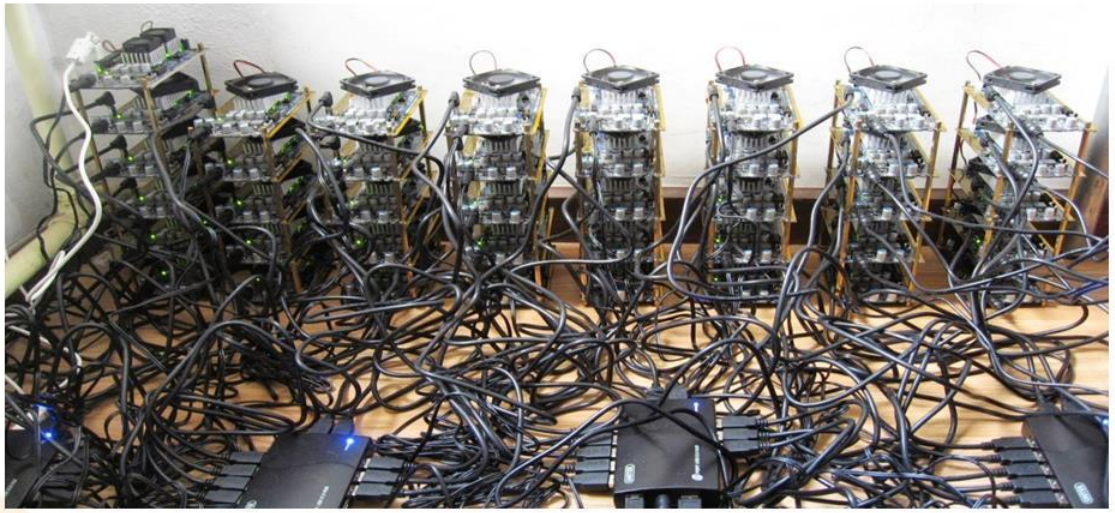
Маленькие системы:



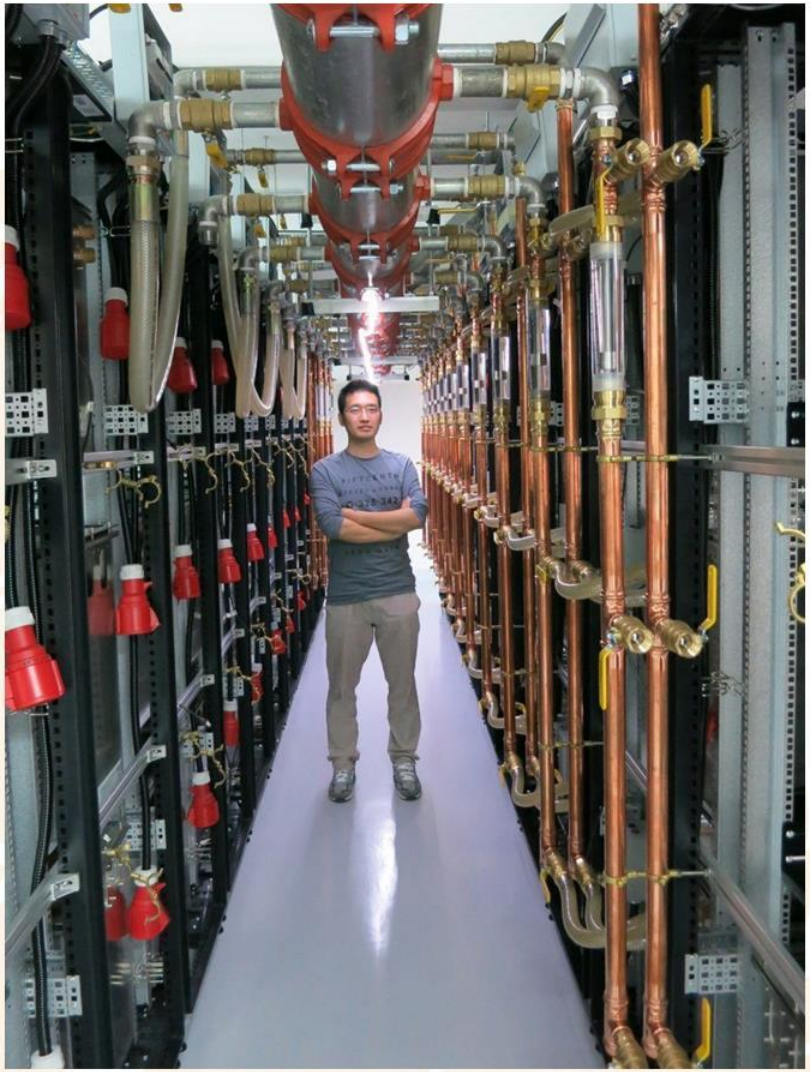


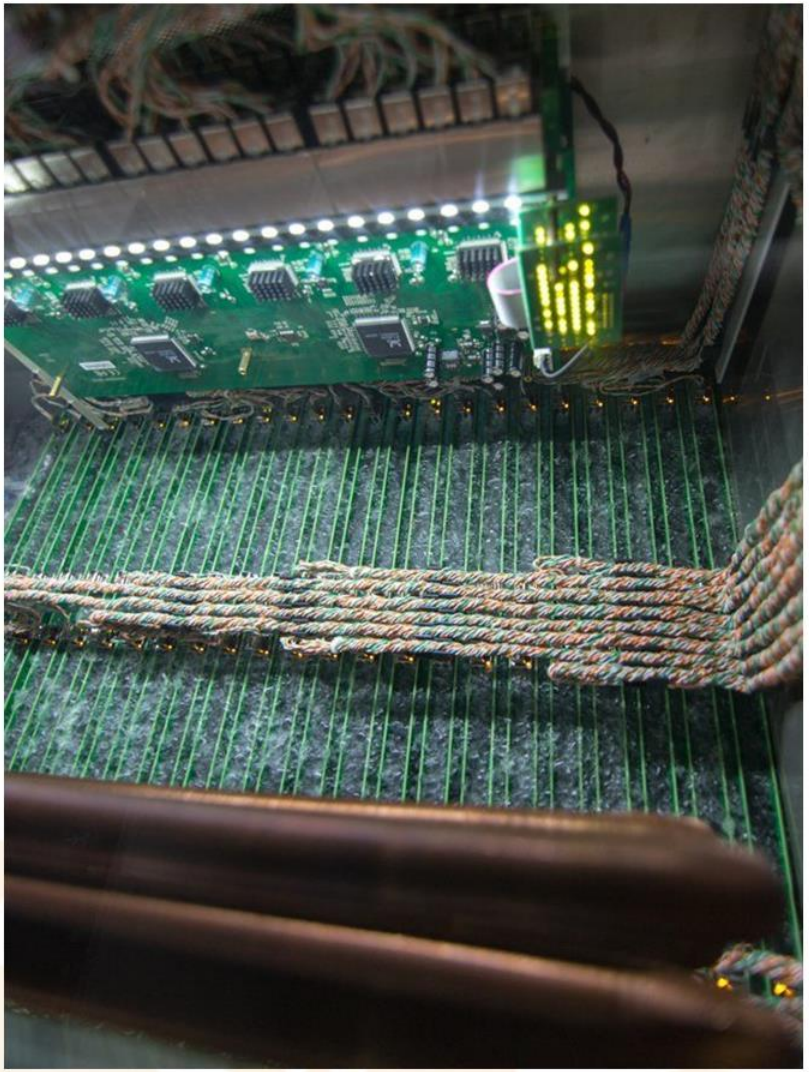
Усовершенствованные системы:





Большие фермы:





Большие фермы:

Рыночная капитализация:

Математическая модель:

Для оценки безопасности требуется точное описание. Оно отсутствует. Но есть исходный текст программы.

Используемые криптографические алгоритмы и их параметры:

В системе используются алгоритмы генерации личных и открытых ключей, выработки и проверки электронной подписи, определенные в стандарте США ECDSA с параметрами secp256k1.
Для хэширования используется двойная sha256.
Хэш-функция ripe160 используется вычисления идентификаторов (ссылок; адресов)

STANDARDS FOR EFFICIENT CRYPTOGRAPHY

SEC 2: Recommended Elliptic Curve Domain Parameters

Certicom Research
Contact: secg-talk@lists.certicom.com

September 20, 2000
Version 1.0

Задача создания блока:

h – хэш-функция, являющаяся композицией двух *sha256*

t – цель (в битовом представлении имеет серию нулей в старших разрядах)

d – служебные данные (заголовок блока, хэши транзакций и прочее)

Задача получения блока:

Для фиксированных: t из Z_{256}, натурального n, d из V_n

Найти x из V_{256}, такой что

$$h(d||x) < t$$

Задача создания блока:

h **– хэш-функция, являющаяся композицией двух** ***sha256***

t – цель (в битовом представлении имеет серию нулей в старших разрядах)

d – служебные данные (заголовок блока, хэши транзакций и прочее)

Известный и широко используемый метод решения (переборный):

Последовательно перебирая (случайно выбирая) ***x*** **из** V_{256} **найти такой, что**

$$h(d||x) < t$$

Задача создания блока:

Можно посмотреть на эту задачу и по-другому:

Для фиксированных: t из Z_{256}, натурального n, d из V_n

Найти пару (x,y), где x из V_{256}, y из Z_{256} и $y < t$, такую что

$$h(d||x)=y$$

Связь со стойкостью функций хэширования, оценка взаимосвязи задач:

Для $h_d : Z_{256} \rightarrow Z_t$ (Z_t множество целых, меньших чем t) найти произвольные аргумент и соответствующее ему значение

Найти алгоритм со сложностью меньшей чем сложность метода перебора или случайного поиска

Защита личных ключей:

В кошельке создаётся пара ключей секретный ключ (PrivKey) и открытый ключ (PubKey). Для внесения энтропии в создание PrivKey используется Key Derivation Function (KDF), параметры которой задаются пользователем самостоятельно.

Воспользоваться биткоинами может владелец личного ключа, на адрес открытого ключа которого перечислена биткоины. То есть необходимо сохранять этот личный ключ в тайне.

В связи с анонимностью системы рекомендуется в каждом случае использовать новую пару ключей. А значит, у пользователя может храниться большое количество личных ключей.

Если все биткоина полученные на данный ключ расходованы – их можно уничтожать – но этим нужно управлять.

Могут использоваться различные способы защиты личных ключей (полная аналогия с проблематикой защиты ключей электронной подписи)

Подмена открытых ключей

Биткоины перечисляются на значение открытого ключа.
Расходовать их сможет тот, кто владеет соответствующим личным ключом
Тот, кто перечисляет биткоины должен убедиться, что личный ключ подписи, соответствующий открытому ключу, на который перечисляются биткоины, имеется именно у лица (получателя платежа)

Подходы к оценке безопасности:

Биткоин – как информационная система – значит применимы общие подходы к оценке ее безопасности включая, «Общие критерии»

Что сделано и делается:

- ✓ Построена математическая модель подсистемы, реализующей криптографические методы
- ✓ Начаты работы по описанию модели (алгоритмов и форматов данных) в формате стандартов (рекомендаций RFC)
- ✓ Начаты работы по формулировке модели нарушителей, описанию атак и угроз
- ✓ Начаты работы по оценке информационной безопасности системы по методологии «Общих критериев»

Личное мнение:

- ✓ Криптовалюты имеют право на жизнь, потому что они реально используются на практике и удобны в определенных случаях
- ✓ Пользователи должны предупреждаться о рисках, связанных с их использованием (по аналогии: «курение опасно для жизни»)
- ✓ Криптовалюты должны быть хорошо исследованы и оценены. Результатом оценки должны быть правила их безопасного использования и описания рисков. Рекомендации пользователям (в конечном итоге)
- ✓ Криптовалюты целесообразно описывать в публичных технических документах, как-то RFC или их аналогах

Феномен криптовалюты «Биткоин». Построение математических моделей децентрализованных информационных систем, реализующих функции платежных систем криптовалют. Подходы к комплексной оценке безопасности, в том числе оценке криптографической стойкости

Директор по развитию ЗАО «БЕЛТИМ СБ»,
директор ассоциации «РусКрипто»
Комисаренко Владимир Владимирович
229@tut.by,
специалист отдела информационной безопасности ОАО «Банк Москва-Минск»
Роговой Александр Сергеевич