



nes  fit

FORENZNÍ ANALÝZA BITCOINŮ (kryptoměny)

Vladimír Veselý
2017-06-05

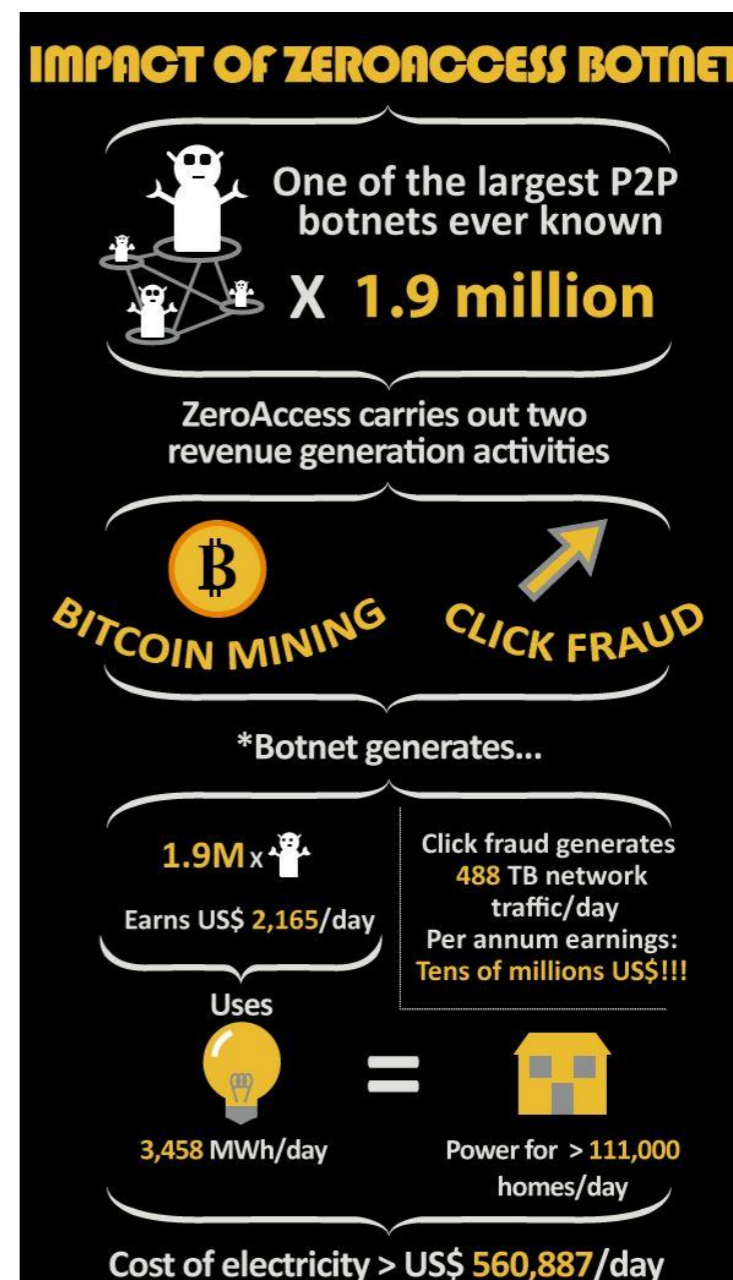
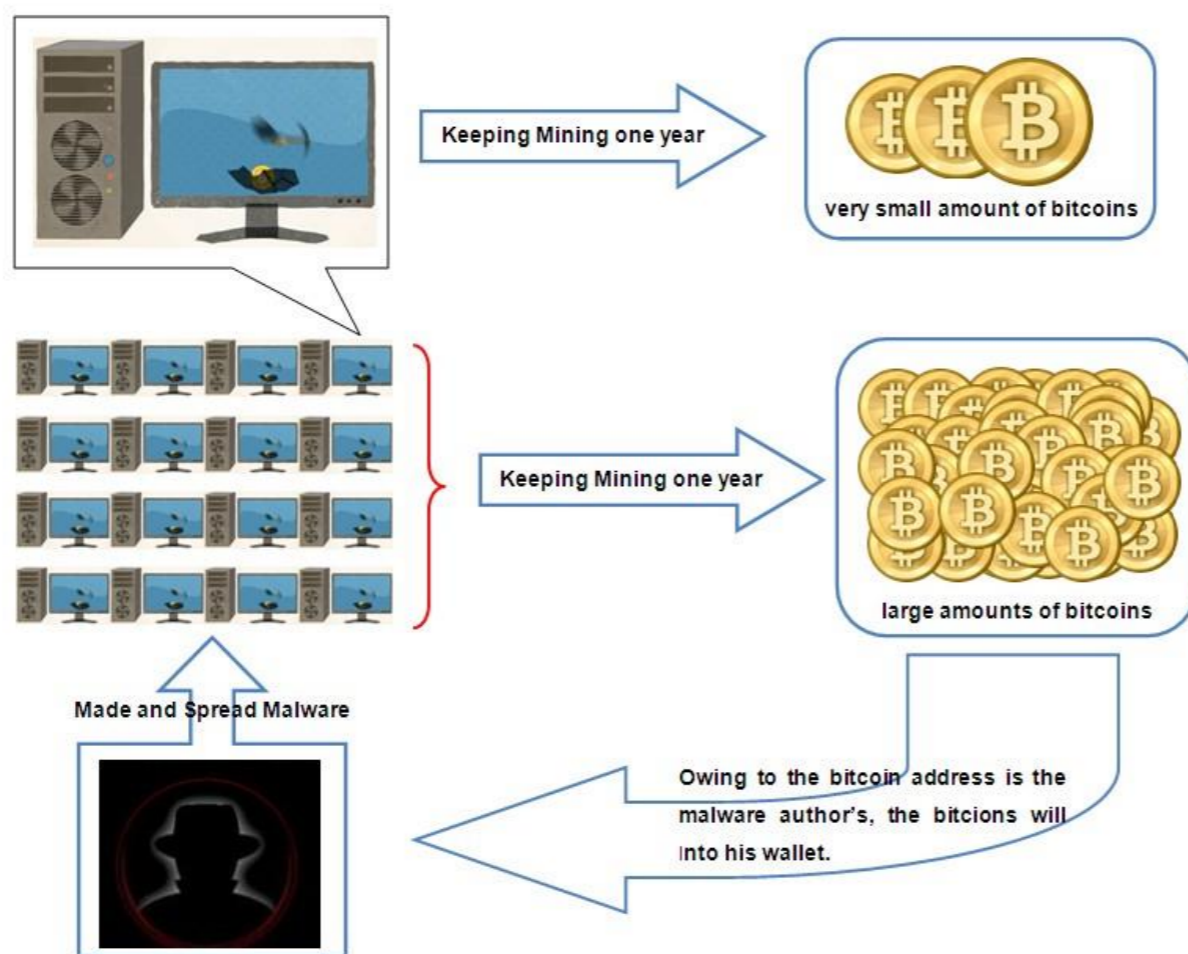


Agenda

- 1) Detekce minérů
- 2) Trasování financí

Problém 1)

- Vědomé či nevědomé zneužití prostředků organizace



Mining Pool

- Sdružení těžařů
- Zvýšení šance na vytěžení bloku
 - odměna 12,5 BTC (~650 tis. Kč)
 - proporcionalní distribuce výtěžku
- Protokoly
 - Stratum (TCP + JSON)
 - Getwork, Getworktemplate (HTTP + JSON)
 - dynamické porty, dynamické adresy



Těžba

- Patříčný HW



- Patříčný SW

The login credentials needed for your miner look like this: (please, fill your **user ID** and **worker name**)

```
URL: stratum+tcp://stratum.slushpool.com:3333
userID: userName.workerName
password: anything
```

The password can be an arbitrary text since there is no security issue present here. If someone tried to connect to our servers with your credentials, he would be just mining for your benefit.

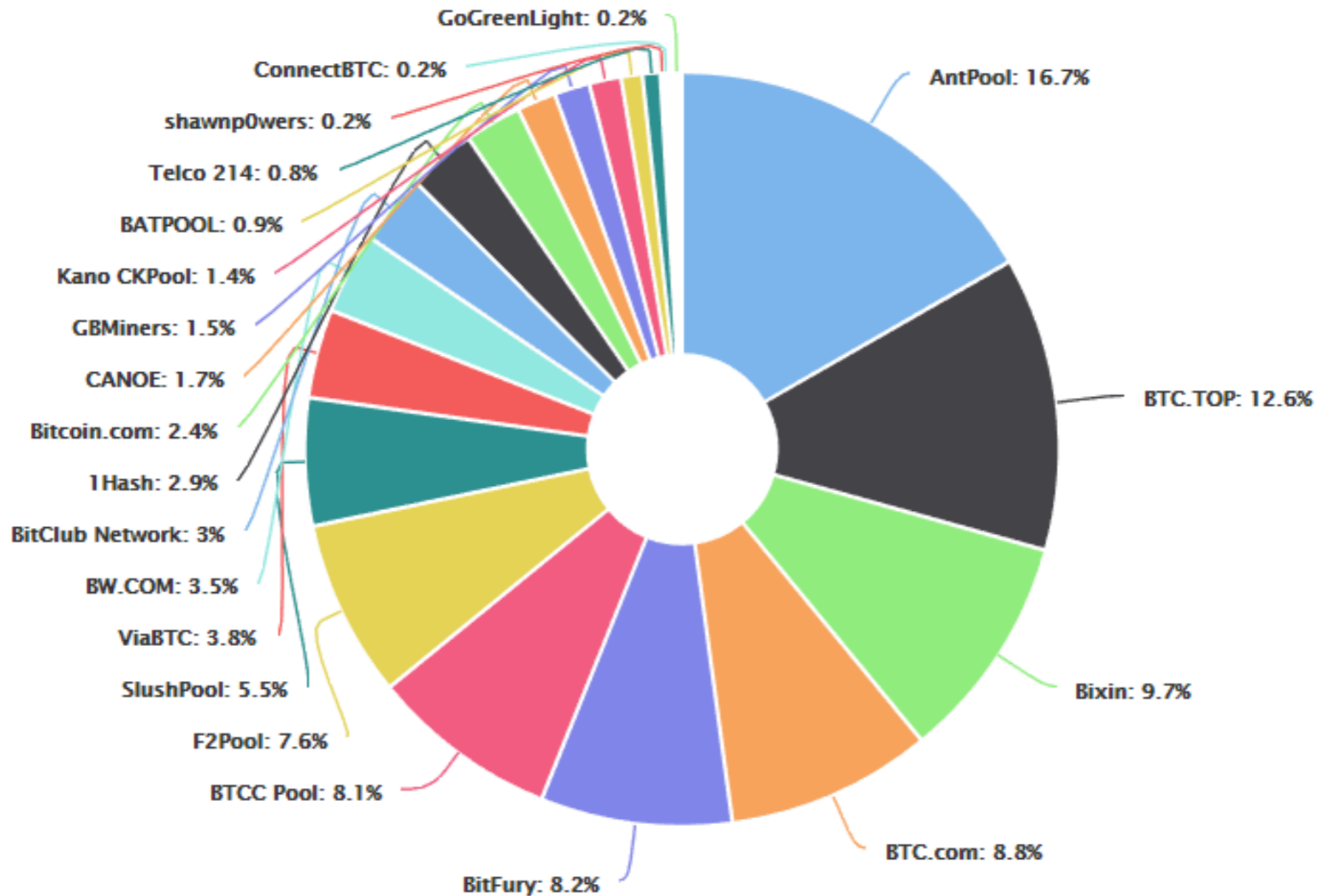
The servers can be chosen from the following list based on your geographical location:

Servers Location	Address
USA, east coast	stratum+tcp://us-east.stratum.slushpool.com:3333
Europe	stratum+tcp://eu.stratum.slushpool.com:3333
China, mainland	stratum+tcp://cn.stratum.slushpool.com:3333 stratum+tcp://cn.stratum.slushpool.com:443
Asia-Pacific/Singapore	stratum+tcp://sg.stratum.slushpool.com:3333

```
F:\cgminer-3.7.2-windows\cgminer.exe
cgminer version 3.7.2 - Started: [2014-01-31 21:04:35]
-----
<5s>:1.390M <avg>:1.132Mh/s | A:1792 R:0 HW:0 WU:981.6/m
ST: 2 SS: 0 MB: 3 LW: 35 GP: 0 RF: 0
Connected to eu2.multipool.us diff 256 with stratum as user yourworker.1
Block: 3e29b69c... Diff:1.26K Started: [21:06:06] Best share: 3.21K
-----
[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0: 64.0C 2562RPM | 693.3K/579.9Kh/s | A:1024 R:0 HW:0 WU:548.9/m I:13
GPU 1: 66.0C 3381RPM | 697.1K/582.8Kh/s | A: 768 R:0 HW:0 WU:452.1/m I:13
-----
[2014-01-31 21:04:35] Switching to pool @ stratum+tcp://eu2.multipool.us:7777
[2014-01-31 21:04:42] Network diff set to 1.26K
[2014-01-31 21:04:52] Accepted b0983ade Diff 371/256 GPU 1 pool @
[2014-01-31 21:04:52] Stratum from pool @ requested work restart
[2014-01-31 21:05:23] Accepted 71c47438 Diff 576/256 GPU 1 pool @
[2014-01-31 21:05:24] Accepted c63468e2 Diff 331/256 GPU 0 pool @
[2014-01-31 21:05:24] Accepted daedae15 Diff 299/256 GPU 0 pool @
[2014-01-31 21:05:43] Accepted 24251b58 Diff 1.81K/256 GPU 0 pool @
[2014-01-31 21:05:44] Accepted 1470ae8f Diff 3.21K/256 GPU 1 pool @
[2014-01-31 21:05:53] Stratum from pool @ detected new block
[2014-01-31 21:05:55] Accepted 6c8f3f94 Diff 604/256 GPU 0 pool @
[2014-01-31 21:06:06] Stratum from pool @ detected new block
```

Existující Pooly

- <https://blockchain.info/pools>



sMaSheD

- Mining Server Detector of Cryptocurrency Pools
- *Demo*

Problém 2)

- Praní špinavých peněz
- Krádeže, výkupné



Wana Decrypt0r 2.0

Oops, your files have been encrypted!

English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Mondays to Friday.

Payment will be raised on 5/16/2017 00:47:55
Time Left 02:23:57:37

Your files will be lost on 5/20/2017 00:47:55
Time Left 06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

Transakce

- 1 transakce
 - transakční historie vytváří obousměrně vázaný seznam

bafebce4967d23a2d14725dec005477b393ba3385f8fd6a9b1805eda1cf94c05

(Fee: 0.002282 BTC - 438 sat/B - Size: 521 bytes) 2017-05-23 07:13:30

1N3y3Gt6KFan6jBNMpSrovDgjRHNAXweR3 (0.12648354 BTC - Output)
1LLnRwX1mcaPSvXiZydWe8LB1Zqqwcfamy (0.01381087 BTC - Output)
1FpSCzBtQ2wSppTMv2VyHX2ssCeYVKAf9N (0.14118045 BTC - Output)

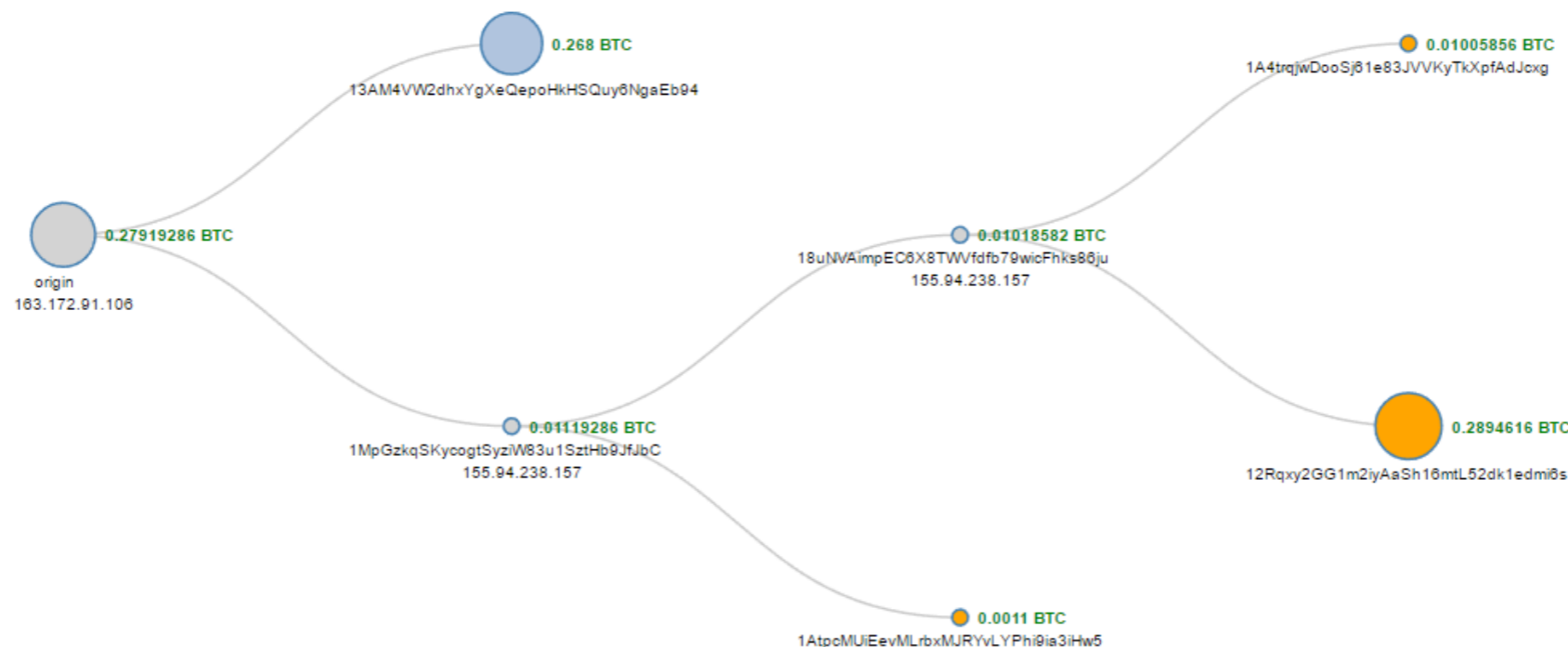


13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 - (Unspent) 0.268 BTC
1MpGzkqSKycogtSyziW83u1SztHb9JfJbC - (Spent) 0.01119286 BTC

0.268 BTC
0.01119286 BTC

0.268 BTC

- trasování utrácení



Blockchain

- Veřejná účetní kniha
 - má ji k dispozici každý
- 1 blok
 - vytváří se co 10 minut
 - obsahuje tolik transakcí, co se naskládá do 1 MB dat

LATEST BLOCKS

[SEE MORE →](#)

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
469200	11 minutes	1716	27,992.30 BTC	ViaBTC	999.11
469199	17 minutes	2202	33,188.84 BTC	F2Pool	999.83
469198	22 minutes	1858	32,770.28 BTC	BTCC Pool	989.18
469197	28 minutes	2602	26,945.10 BTC	BitFury	998.2

- CryptoCurrency Analyzer



Otázky?

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES



Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJLybLCWrDpN.



Bob creates a new Bitcoin address for Alice to send her payment to.

CREATING A NEW ADDRESS



Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

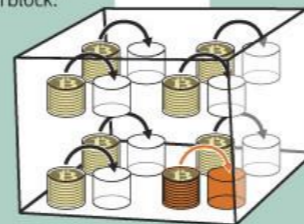


Gary, Garth, and Glenn are Bitcoin miners.

VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.



Private key

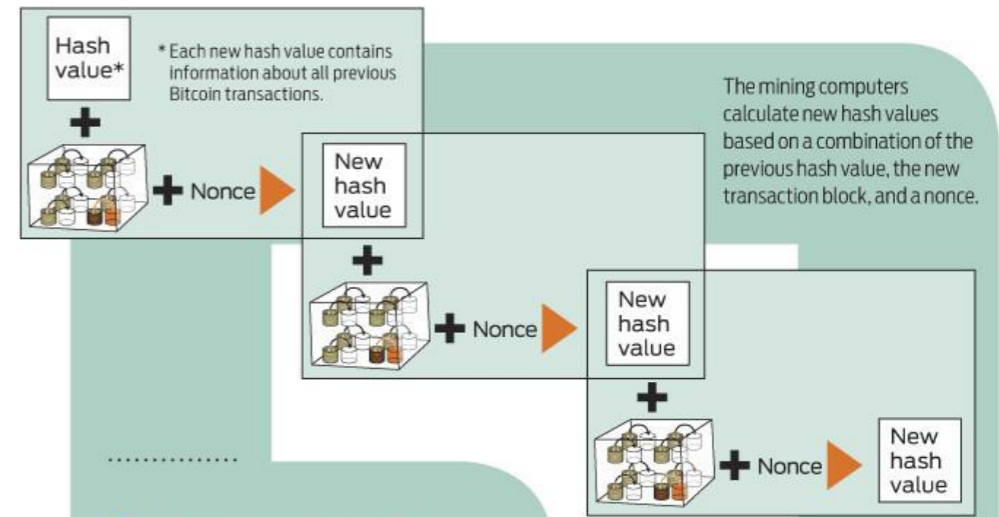


Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Public key



Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.



Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all evil	b8db 7ee9 8392...

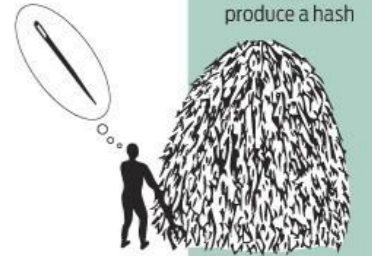
Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ??? → 0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash



value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.



TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

