FORENZNÍ ANALÝZA BITCOINŮ (kryptoměny)

Vladimír Veselý

2017-06-05

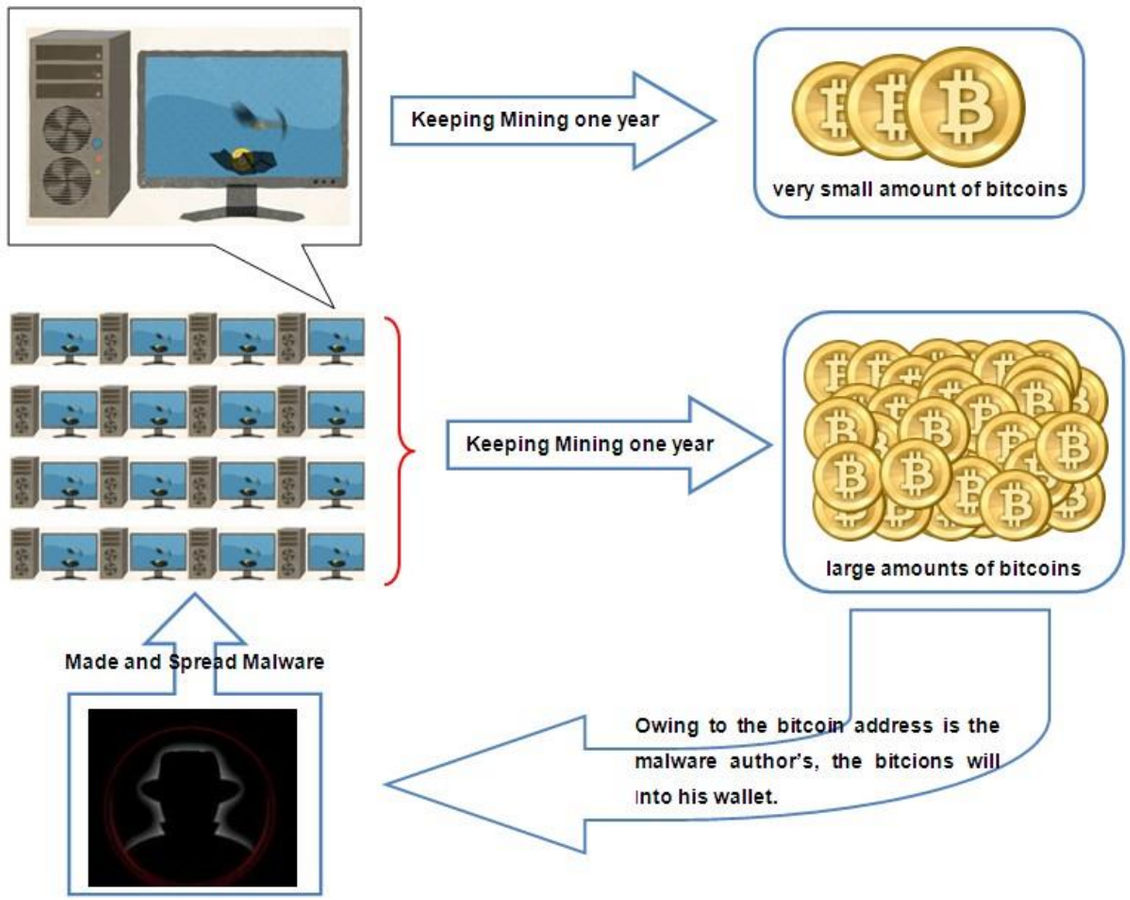
Agenda

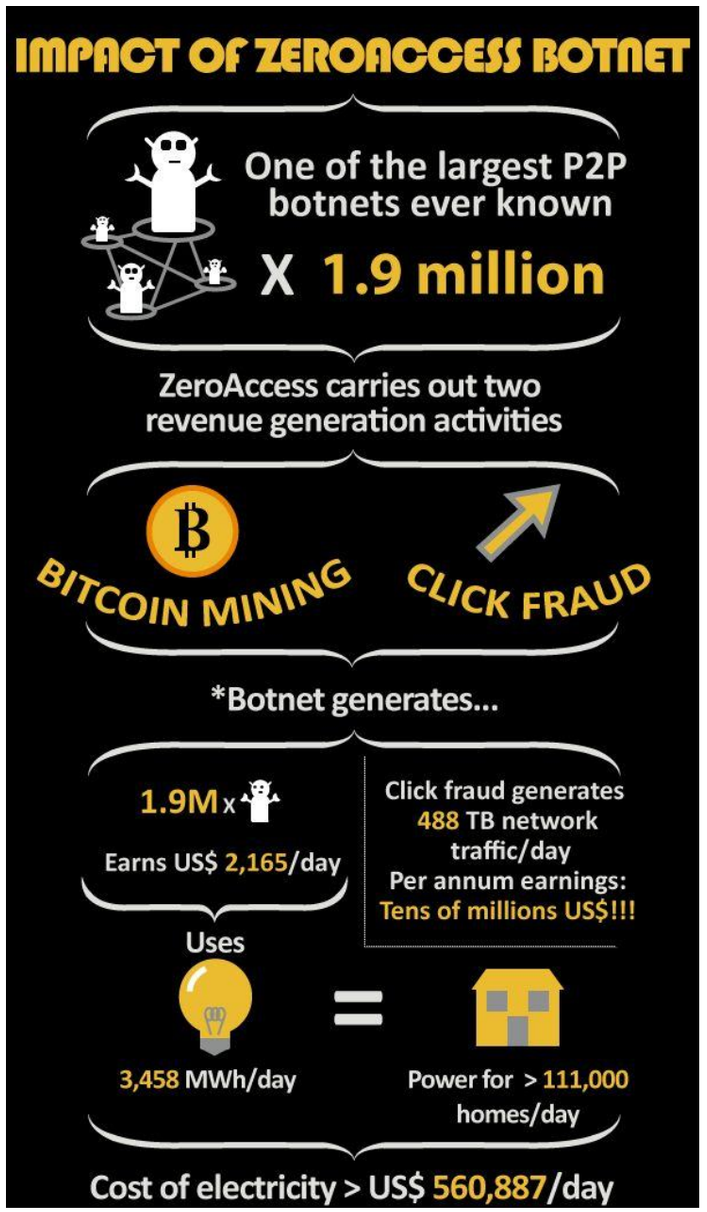
1) Detekce minérů

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)
  - proporcionální distribuce výdělku

- Protokoly
  - Stratum (TCP + JSON)
  - Getwork, Getworktemplate (HTTP + JSON)
  - dynamické porty, dynamické adresy

Těžba

- Patřičný HW

- Patřičný SW

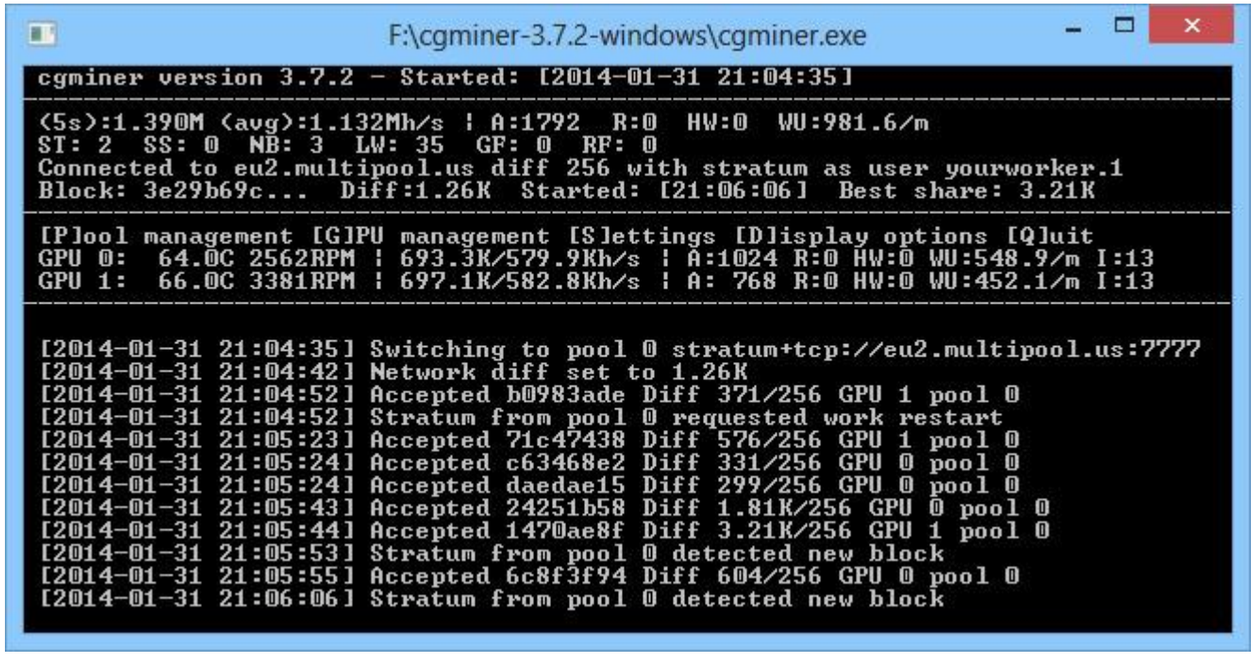
The login credentials needed for your miner look like this: (please, fill your user ID and worker name)

```
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.

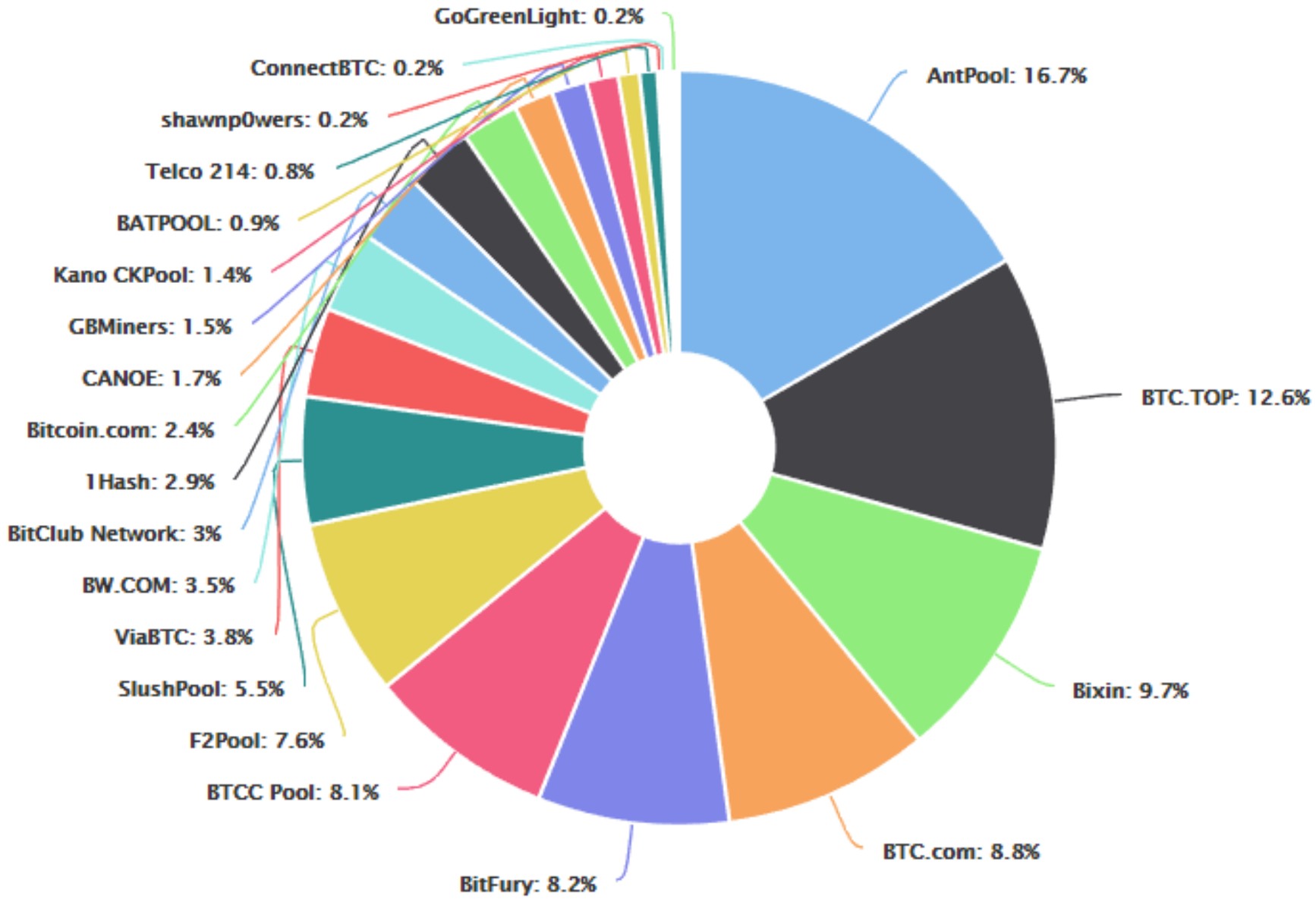
The servers can be chosen from the following list based on your geographical location:

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



Existující Pooly

- https://blockchain.info/pools



sMaSheD

- Mining Server Detector of Cryptocurrency Pools

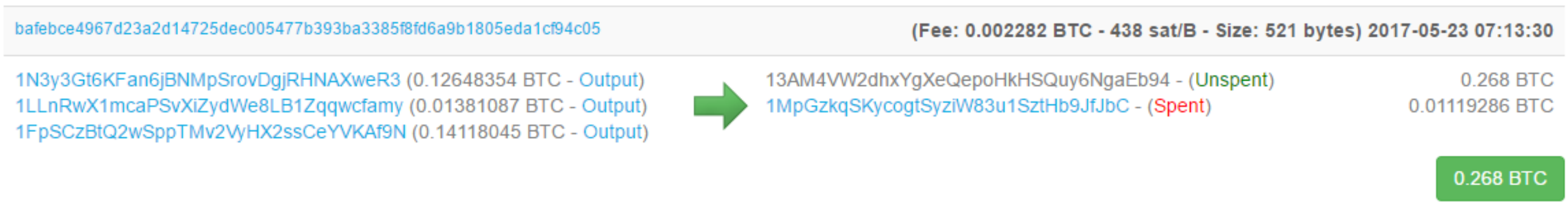
- *Demo*

Problém 2)

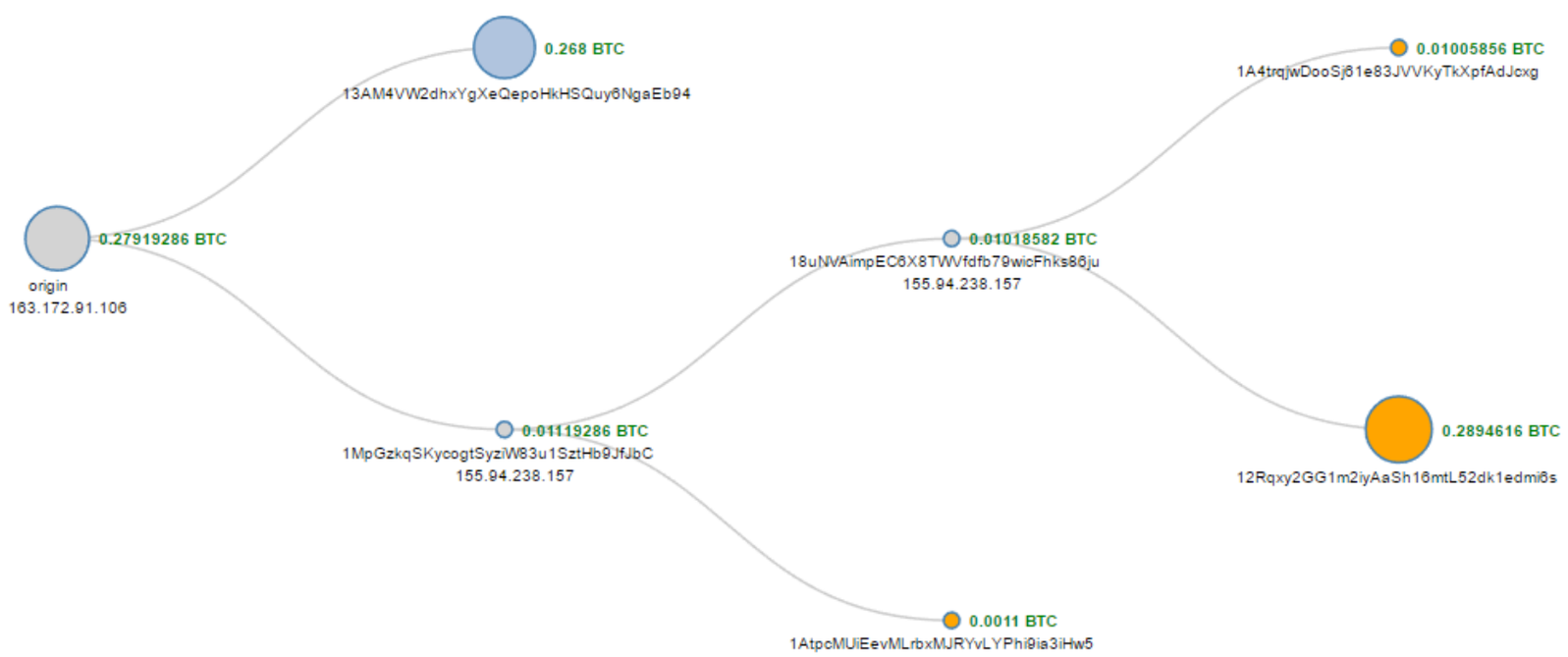
- Praní špinavých peněz
- Krádeže, výkupné

Transakce

- 1 transakce
  - transakční historie vytváří obousměrně vázaný seznam



- 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

CCA

- CryptoCurrency Analyzer

Otázky?

How a ₿itcoin 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.

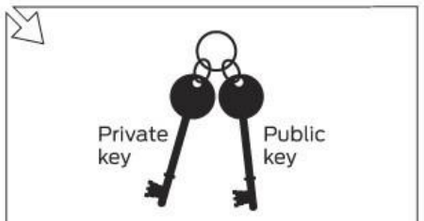
Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

CREATING A NEW ADDRESS

Each address has its own balance of bitcoins.

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



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.

SUBMITTING A PAYMENT

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

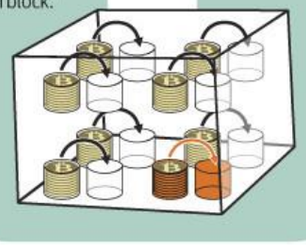
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

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

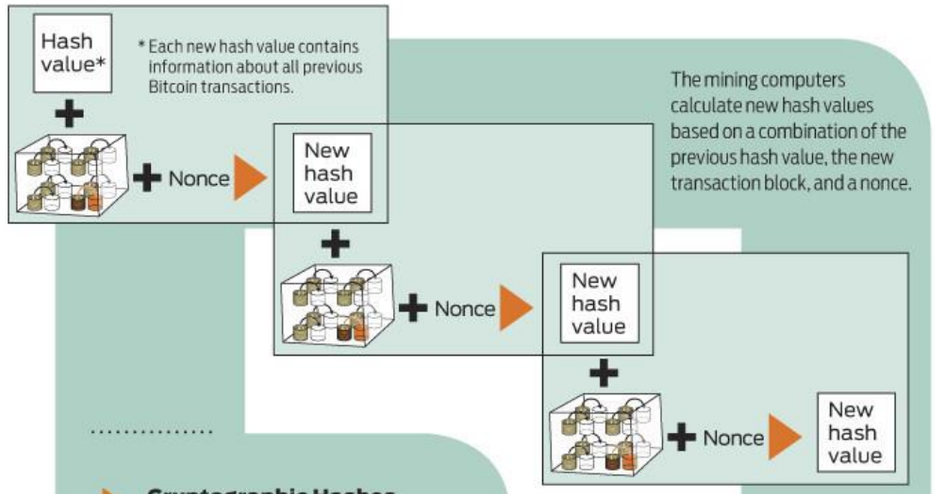
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

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.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

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 veil	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.

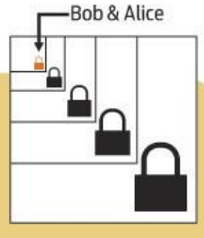
The root of all evil ???	0000 0000 0000 ...

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.

JOSHUA J. ROMERO, BRANDON PALACIO & KARL SSOWWLKER INC.