Bitcoin – crypto currency of the future or heaven for criminals?

Bojan Ždrnja, CISSP, GCIA, GCIH
Bojan.Zdrnja@infigo.hr

INFIGO IS http://www.infigo.hr

INFIGO Information security

Agenda

- What is Bitcoin?
  - An in-depth overview of how Bitcoin works
    - Identities
    - Transactions
    - Mining
- Bitcoin security
  - Attacks against Bitcoin …
  - … and Bitcoin users

INFIGO information security

Virtual money basics

- Two major virtual money systems
- Centralized system
  - There is a central body that everyone trusts
    - Like a national bank
  - Central body prevents abuse
    - Biggest problem: double spending
  - Central body handles all transactions
  - Examples: PayPal, WebMoney, CashU
- Decentralized system
  - No central body
  - Mainly academic …
  - … until Bitcoin!

INFIGO information security

What is Bitcoin?

- First decentralized virtual currency
- Published by Satoshi Nakomoto in 2009
  - Real author's identity unknown
- Based on strong encryption
- Fully uses P2P for transactions
- Allows almost anonymous transactions
  - Identities are anonymous, but not transactions themselves
- Very interesting economic model
  - Not my area of expertise

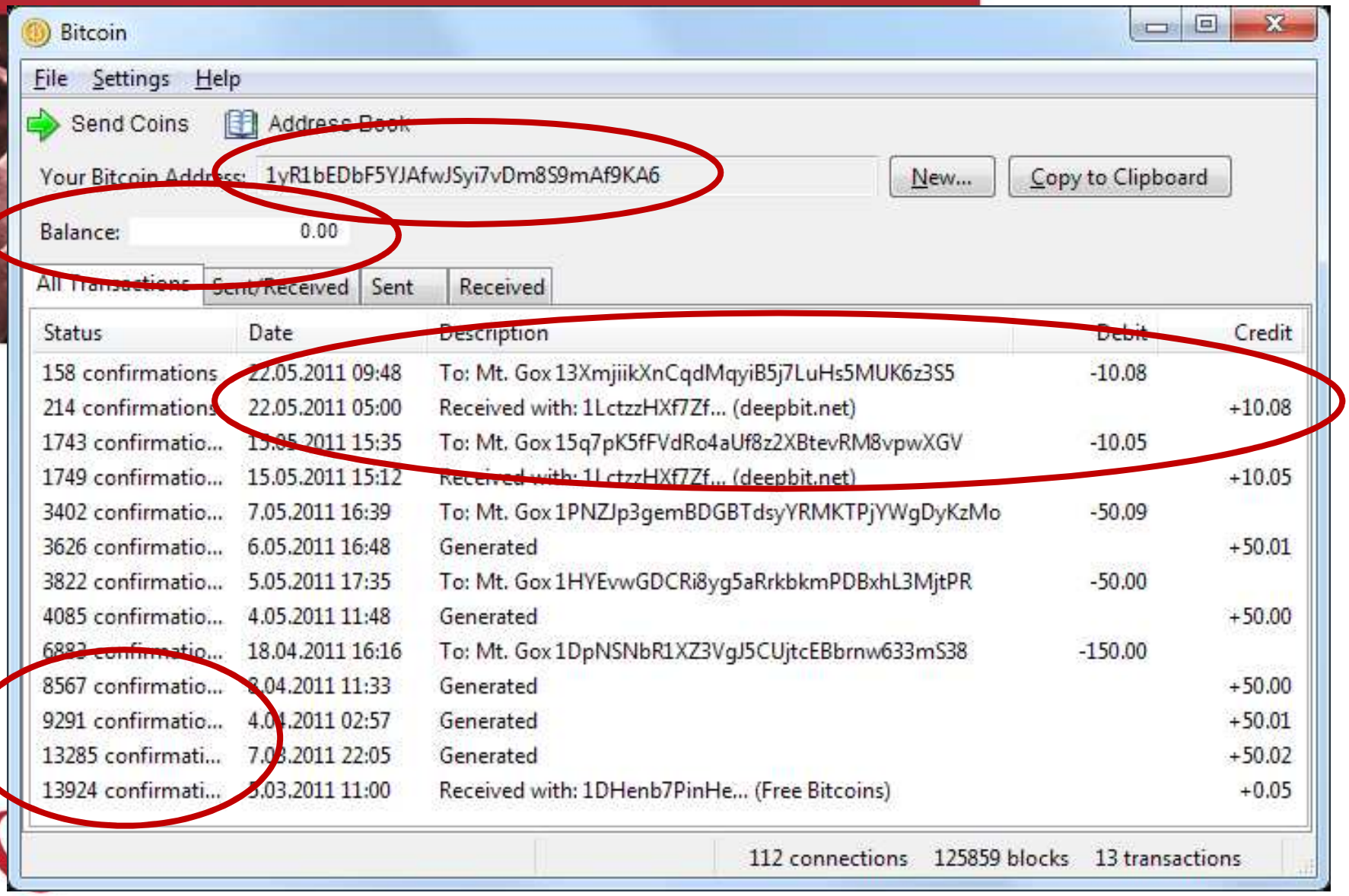
INFIGO information security

Virtual currency problems

- Virtual currencies have two main problems:
  - User identities
    - We have to know who is the recipient
    - Users can be anonymous, but their accounts must be identified
    - Bitcoin solves this through asymmetric cryptography
  - Double spending
    - Virtual money can be easily copied
    - Double spending is a problem
      - Create one transaction (spend money) and then immediately another
    - Bitcoin solves this through "proof-of-work" (problem solving through hashing)

INFIGO information security

Bitcoin client



How do we identify accounts?

- Generate a pair of keys
  - Bitcoin uses ECC (Elliptic Curve Cryptography)
- 1H37GVAcAMCbv9pfa9qwZwSw2x7nhdsrv8
  - This is actually a user's public key
    - ripemd160(sha256(public key))
    - Apply Base58 on it and get the public address
  - We can generate as many pairs as we want!
    - Actually you can use a new pair for every transaction
- When someone sends you BTC they use your public key
- You claim BTC with your private key

INFIGO information security

Bitcoin transactions

- Basically work like this:
  - Take a previous transaction you claim
  - Define recipients with their addresses
    - Remaining amount goes back to you
  - Generate a transaction containing these details
  - Sign it with our private key
    - This way we can claim the previous transaction
  - Broadcast the transaction to everyone on the Internet
    - Bitcoin transactions are public
    - Everyone can verify the signature with our public key
- Key question: how do we stop double spending?

INFIGO information security

Bitcoin transactions

- Transactions can contain a Forth-like, SCRIPT language
  - Stack based language
  - Allows very complex operations, contracts etc.
    - Currently mostly used for standard transactions
- The embedded SCRIPT language defines how a transaction is verified

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

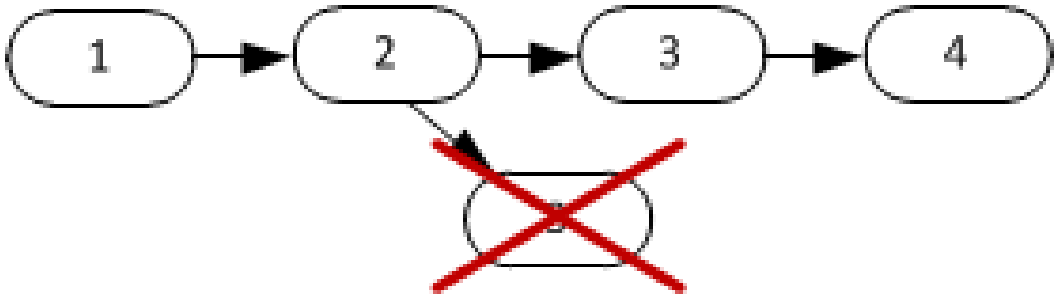
Transaction blocks

- Bitcoin combines information about transactions in blocks
- A block contains various information:
  - Merkle root of all transactions
    - 256-bit hash
    - Makes all transactions in a block confirmed
  - Hash of the previous block
  - Timestamp
  - Target
  - Nonce
- And now calculate SHA256(SHA256(this))

INFIGO information security

Transaction blocks

- So what is so special about blocks?
  - They have to solve a certain complexity (the target)
    - Target is a 256 bit number
    - The generated hash must be lower than the target to be accepted
      - i.e. it has to have leading N zeroes
- Link to the previous block creates a block chain



INFIGO information security

Bitcoin mining

- First client that calculates a hash below the target wins
  - Announce to the whole network
  - All transactions in the block are considered confirmed
    - Merkle root is used to verify them
- This solves the double spending problem
  - If a malicious client generates two transactions only one will be accepted
    - We can’t know which one!

INFIGO information security

Bitcoin mining

- The target is automatically adjusted
  - All Bitcoin clients in the world should generate one block every 10 minutes
    - More clients? Increase the complexity!
    - Complexity revised every 2016 blocks
      - Approximately every 2 weeks
- So why would anyone do this?
  - We waste electricity, need cooling … Why?
  - Answer: money
    - The winner gets (currently) 50 BTC
    - And also charge for transactions

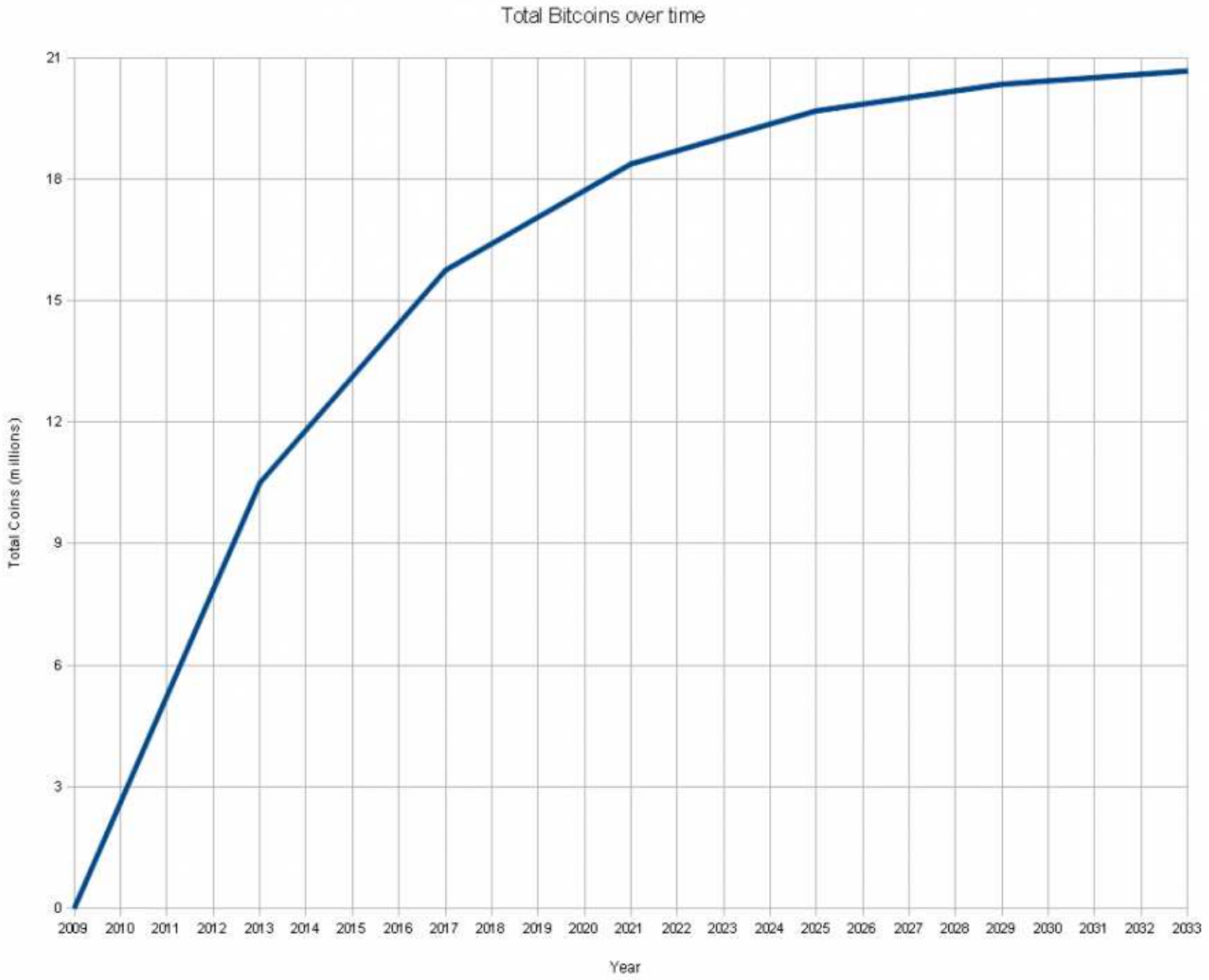
INFIGO information security

Bitcoin mining

- Satoshi's solution for constant money generation
  - Something like extracting minerals or gold
- Currently the block solver gets 50 BTC
  - Halved every 210.000 blocks
- Total possible number of BTC in the future is ~21 million
  - This is not a problem for the currency since payments can be up to the 8th decimal
- Today 1 BTC sells for ~5.3 USD
  - Solve 1 block, you get 250 USD!

INFIGO information security

Bitcoin distribution



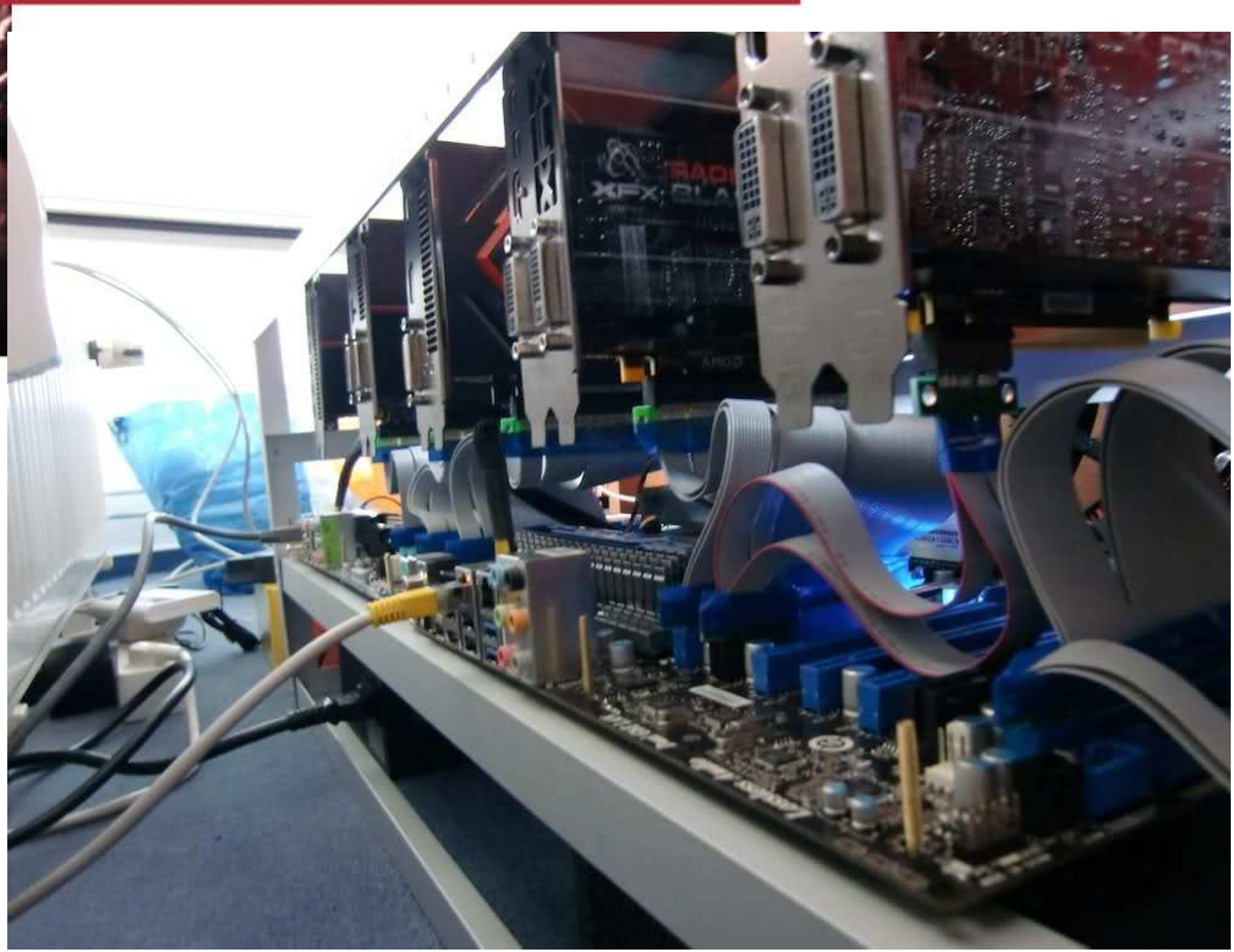
Can we make money with this?

INFIGO information security

Can we make money with this?

INFIGO information security

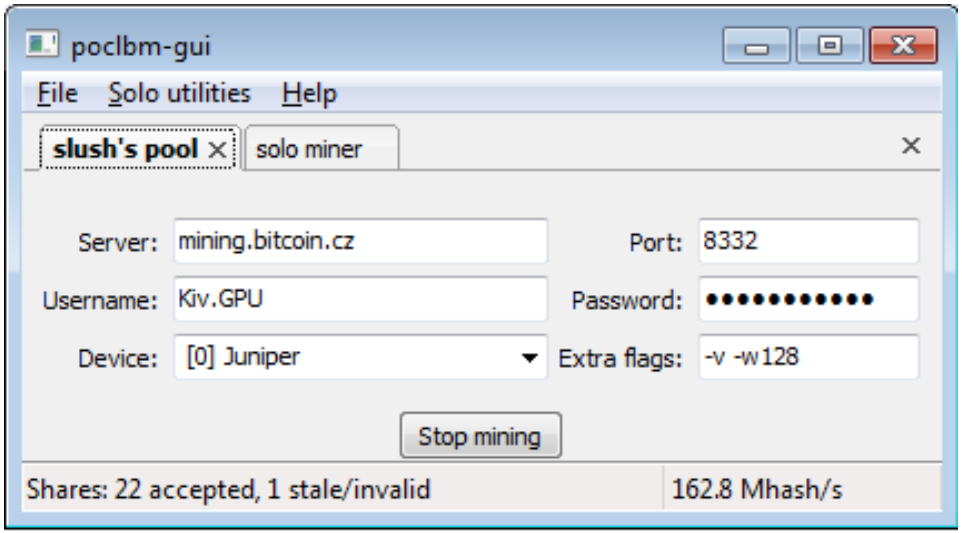
Or the world will run out of GPU cards?



INFIGO
Information security

Mining pools and rigs

- One client has a very small chance of solving a block
- Today most miners join mining pools
  - Special servers that distribute work to clients
  - Any client can join
  - If a block is solved, mining pool owners distribute earned BTCs according to work done



INFIGO information security

Bitcoin security

- From a security point of view, it's amazing
  - Wonder if Satoshi will get rich with this?
  - Some say Bitcoin is a Ponzi scheme
- No major vulnerabilities found so far
- Dan Kaminsky had some interesting ideas at BH
  - Connecting to all clients in the world
    - We can see who created the transaction
- A vulnerability in ECC or SHA-256 can be a problem for Bitcoin
  - Satoshi allowed the possibility of using different crypto algorithms

INFIGO information security

Bitcoin security

- Currently Bitcoin uses IRC to bootstrap
  - irc.lfnet.org, #bitcoin00-#bitcoin99
    - Running a node there, will see who from .HR comes in 30 days ☺
  - Can be a problem with more clients
- Miners can influence the network
  - Imagine a government coming with huge processing power
    - They can double spend!
    - Or they can increase difficulty heavily
      - And process no transactions
      - Each miner decides which transactions will be processed
      - Normally you process all to get more BTC
    - Will limit target increase 4x per 2016 blocks

INFIGO information security

Bitcoin client security

- As always, clients are the weakest link
  - Malware attacking client machines
    - Steal wallets, send BTC to malware owner
      - There is NO chargeback in Bitcoin!
  - Some such attacks caused huge drops on the BTC market
    - MtGox – Bitcoin market
    - They got pwned, attacker tried to sell 400.000 BTC (was worth around 7 million USD)
  - Lately worms install bitcoin mining pool apps
    - Symantec spotted one in August
    - Trojan.Badminer
    - Joins a mining pool in India

INFIGO information security

Bitcoin abuse

- Since it is almost anonymous
  - Or very difficult to trace
  - Clients can use ToR to hide their IP addresses
  - Who likes anonymity the most?
    - Yep, criminal organizations
    - They can sell and buy various things
- Silk road – online drug market

Silk Road
anonymous marketplace

Welcome
messages(0) | orders(0) | account(฿0) | settings | log out
(0)

Drugs(343)
Cannabis(57)
Weed(9)
Hash(3)
Seeds(2)
Ecstasy(27)
Dissociatives(9)
Psychedelics(63)
Opiates(12)
Stimulants(13)
Other(159)
Lab Supplies(2)
Digital goods(12)
Services(19)

sort by seller feedback go

title	price	seller	ship to	ship from	
Early Outdoor x Congolese Sativa (Cannabis Seeds)	฿2.18	P4r4b0l4(98)	International	Canada	add to cart
Early Male x Chunky Monkey Cut (Cannabis Seeds)	฿2.18	P4r4b0l4(98)	International	Canada	add to cart
Early Nepalese Sativa (cannabis seeds)	฿7.78	P4r4b0l4(98)	International	Canada	add to cart
1/8oz (3.5g) of Sour 13	฿7.63	1UP of Canada(97)	Worldwide	Canada	add to cart
1/8oz (3.5g) of the infamous Jack Herer	฿8.72	1UP of Canada(97)	Worldwide	Canada	add to cart
1/8oz of dark Afghan hash M.T.V. stamp 4 rockstars	฿11.99	1UP of Canada(97)	Worldwide	Canada	add to cart

INFIGO information security

Bitcoin's future?

- Bitcoin lives and it will not disappear easily
  - Value can and will change
  - Even if Bitcoin disappears another crypto currency will emerge
- Could be a problem for governments and law enforcement
  - Controlling anything on the Internet is close to impossible
  - Government might decide to ban Bitcoin
- One thing is sure though …
  - Criminal organizations will love it

INFIGO information security