Bitcoin
A Peer-to-Peer Electronic Cash System

Author: Satoshi Nakamoto

Presenter:	Flavio Vit
Course:	UNICAMP –IA368
Professors:	Christian Esteve Rothenberg, Mauricio Ferreira Magalhães

May 25, 2014

Agenda

- Introduction
- Key Concepts
- BTC Transactions
- BTC Mining
- Bitcoins
- Proof of Work
- Digital Wallet
- Security
- Legal Considerations
- Conclusion

Introduction

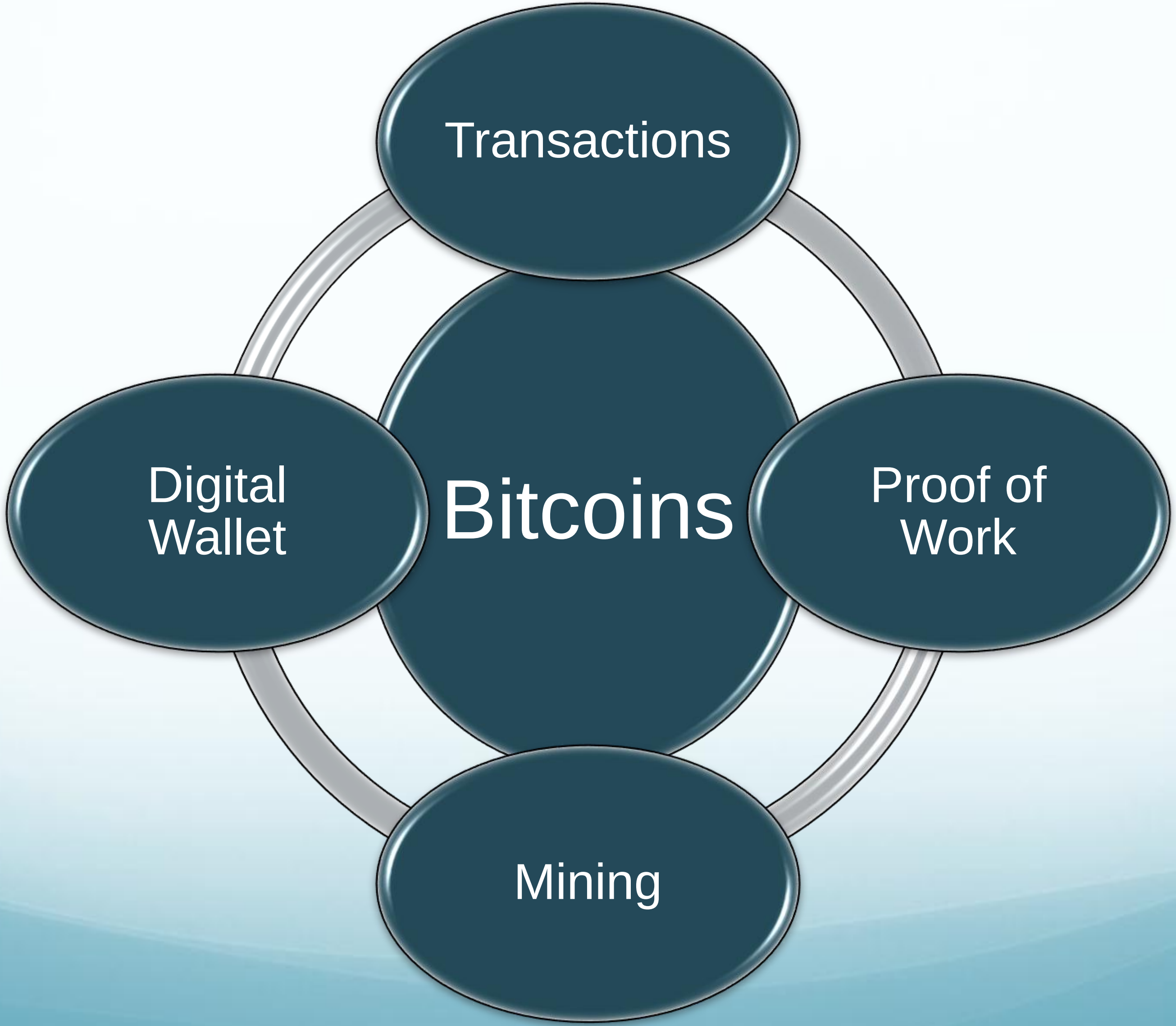
What is Bitcoin?

- First decentralized digital / virtual currency
- Crypto Peer to Peer currency
- Electronic payment system based on cryptographic proof instead of trust
- Developed by a person or group under the pseudonym of

Satoshi Nakamoto in 2008 / Operational since early 2009

- No financial institutions is managing

Key Concepts



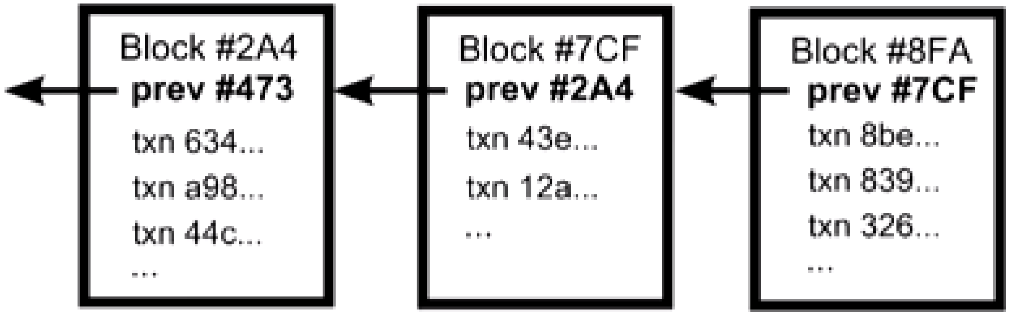
BTC Transactions

- Straight between the owner and the receiver
- Broadcasted through the P2P network
- All are public but anonymous
- Mining nodes collects the transactions into **Blocks**

BTC Transactions

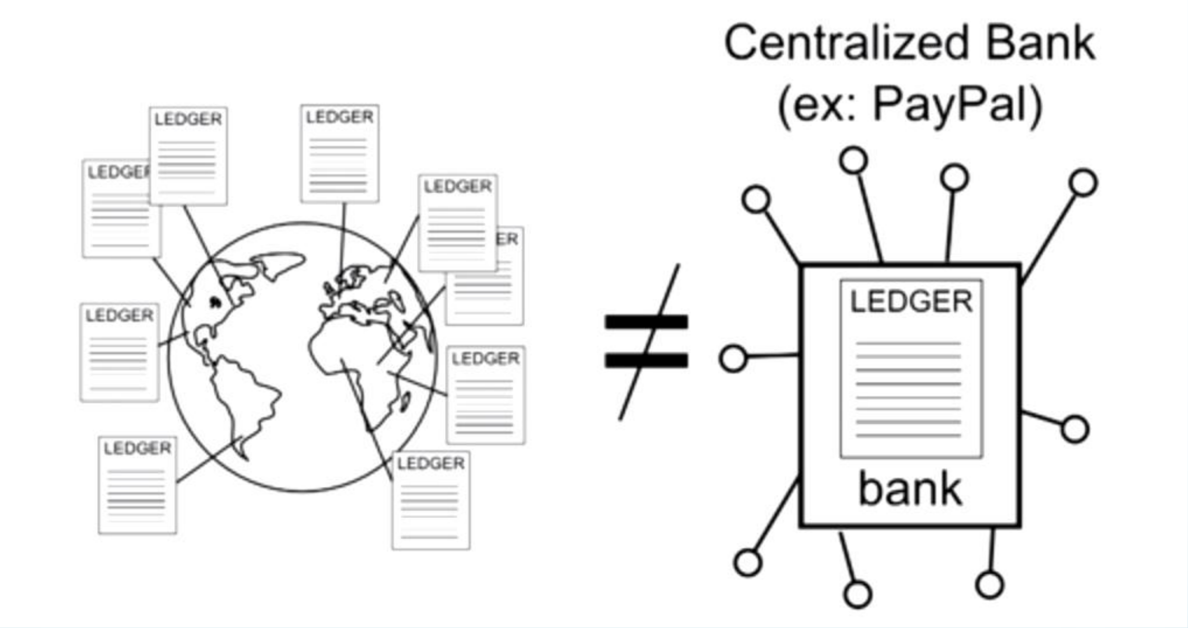
- **Transactions Blocks** ⬄ Full page in a Ledger Book

- **Block** => contains information about transactions and previous Block (**Block Chain**) linking to the first block when Bitcoin Network started



BTC Transactions

- The Block Chain file is maintained on every node



BTC Transactions

- Each Block carries a Proof of Work
- BTC are generated for the machine which solved the Proof of Work
- New block is started and linked to the block chain
- First transaction in a block = Special transaction = new coins owned by the creator of the block
- New block chain status is broadcasted to the network

BTC Transactions

Fighting Transactions Hackers

- Transaction history cannot be changed unless redoing all Proof of Work of all blocks in the chain
- Redoing the proof of work since the very first transaction block => **Enormous computational power**
- **Double spending problem** => solved using a P2P distributed timestamp server to generate computational proof of the chronological order of transactions

BTC Mining

- No centralized entity for generating BTC
- Mining Process => Solve the **Proof of Work** from a **Transaction Block**
- Confirms transactions and increase security
- User can be miners and are rewarded by:
  - Transactions fees for the transactions they confirm
  - New block created / proof of work solved? => **25 BTC today**
- Mining is a competitive market **$$$$$$**
- More miners => More secure network

BTC Mining

- September 2013 => 11,5 Million Bitcoins
- Bitcoins are generated in blocks
- Currently 25 Bitcoins are mined per block
- A New Block are generated every 10 minutes
- The mined BTC are kept with the PC which solved the proof of work

BTC Mining

- BTC are generated in a steady rate
- In Jan 2009, 1 Transaction Block solved = 50 BTC
- After 210.000 transaction blocks, the reward drops by 50%
- BTC generation => to stop by 2140
  - **21 Million Bitcoins will be generated**
- After 2140 the incentive will be only the **transaction fee**

BTC Mining

Mining nodes

- Initially, CPU power to solve the Proof of Work for Transaction Blocks
- Graphic cards solve faster the Proof of Work
- New dedicated chips for performing mining
- Miners are crucial BTC network by ensuring:
  - **Impartial**
  - **Stable**
  - **Secure**

Bitcoins

- BTC are entries in the transactions blocks / in the ledger book

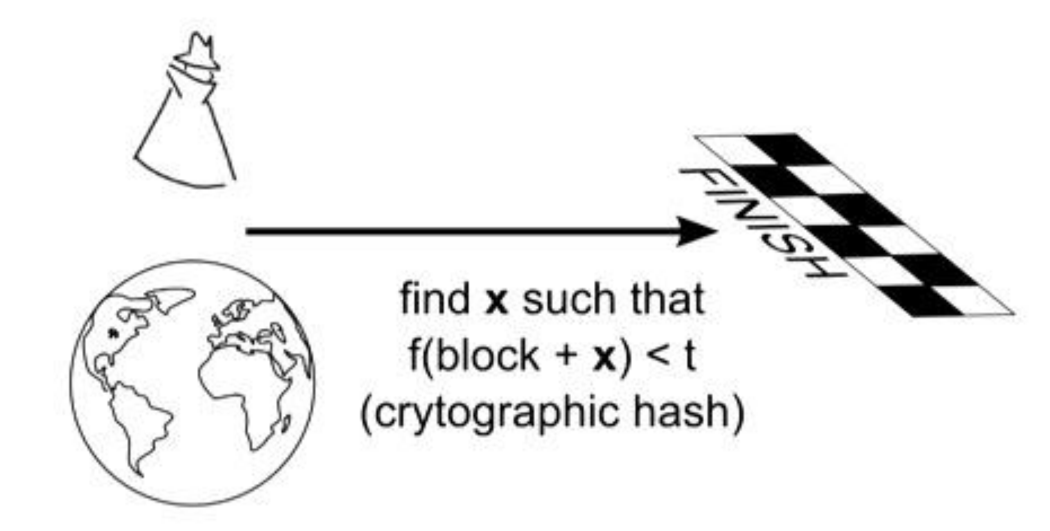
- Someone receives a BTC => transaction logged in the transaction block chain (unconfirmed until Proof of Work is solved)
- BTC ownership and transfer are ensured by digital signatures (crypto private and public keys)

Proof of Work

- Protocol challenging the mining nodes
- **Tough** to be solved **X Easy** to be verified
- Every 2 weeks, BTC generation rate is auto adjusted.
- Increasing / decreasing the difficulty of the Proof of Work   => targeting 10 minutes block generation
- Solving the puzzle => Winning a lottery

Proof of Work

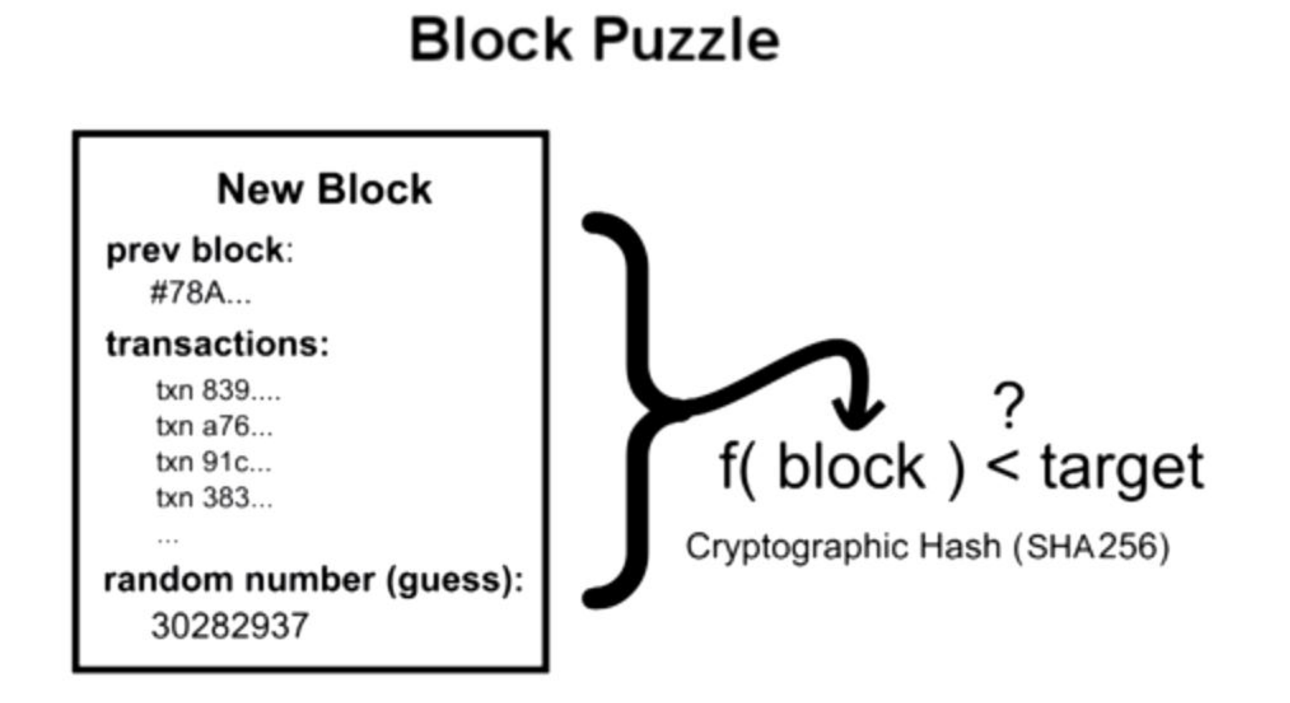
- Transactions in the Block Chain are protected by a mathematical race
- Attacker computational power **VERSUS** The entire network power



find **x** such that
f(block + **x**) < t
(crytographic hash)

Proof of Work

- BTC uses Adam Back **Hashcash** Proof of Work with configurable amount of work to compute
- Uses cryptographic hash SHA256



Block Puzzle

New Block

prev block:
#78A...

transactions:
txn 839....
txn a76...
txn 91c...
txn 383...
...

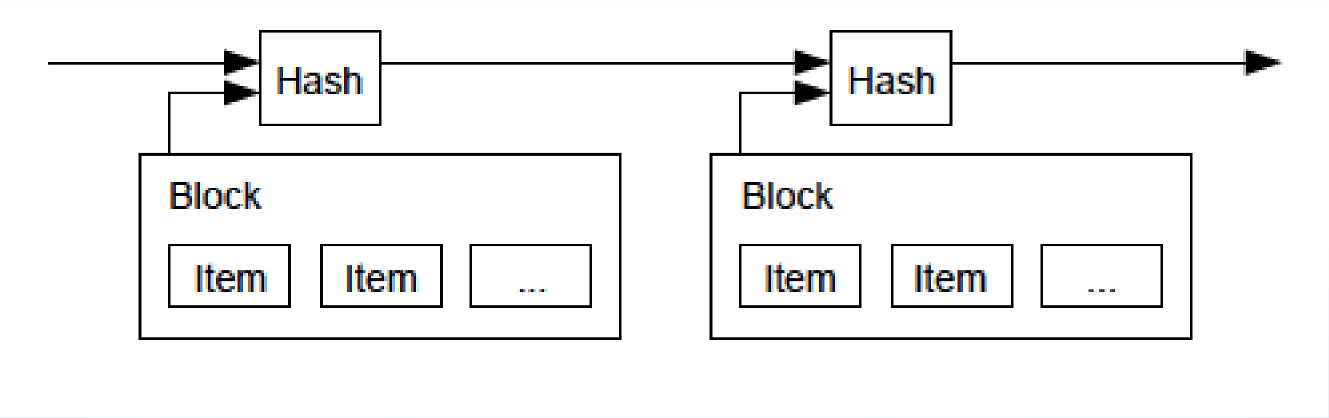
random number (guess):
30282937

$f(\text{ block }) \overset{?}{<} \text{target}$

Cryptographic Hash (SHA256)

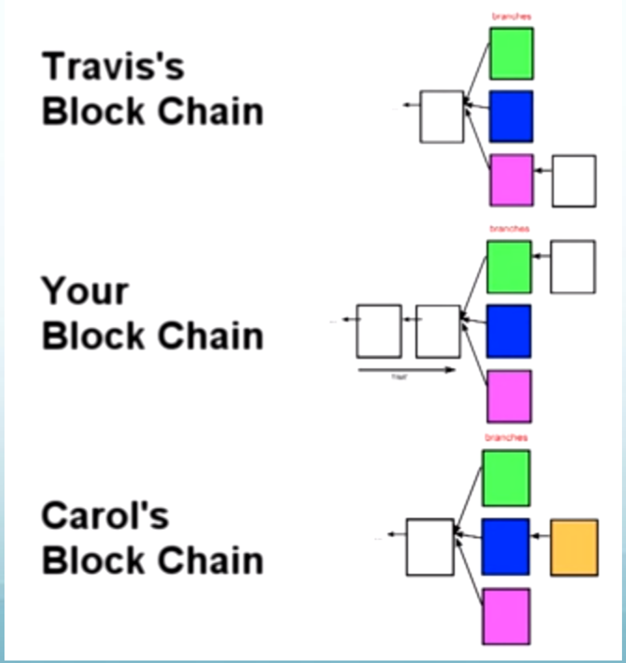
Proof of Work

- Time stamp server => hash of all data in a block including the hash from previous block
- Solution to order the Transaction Blocks



Proof of Work

- Typical PC may take several years to solve it
- Solved in 10 minutes using the BTC network
- Extremely unlikely, but 2 or more nodes may solve the Proof of Work at same time



Proof of Work

- Branches in the block chain are created in this case
- **Tie!!!** => to be broken when someone solves the next block
- Nodes will switch to the longest branch
- Blocks will be discarded and respective transactions will be handled by the wining branch
- The block chain stabilizes and nodes agree with the chain sequence

Digital Wallet

- BTC can be stored in a digital Wallet
  - Web services
  - Local applications
  - USB drivers
- BTC are protected by Private / Public keys
- Also possible to print the BTC

BITCOIN ADDRESS 1KEC5Qh36YtXDMCtVS8AUgcvVEfDrw4aCC
LOAD & VERIFY
BITCOINS
1 2 4 8 16 32 64 128
5Kk1LX3oiSLuYiTsp6v1VjR8rxdGmvYMbR1x72FWJ3n3vin6kLQ
SPEND

Digital Wallet

- No one can lock or freeze your money like a bank account
- Bitcoins fraction => the smallest fraction:

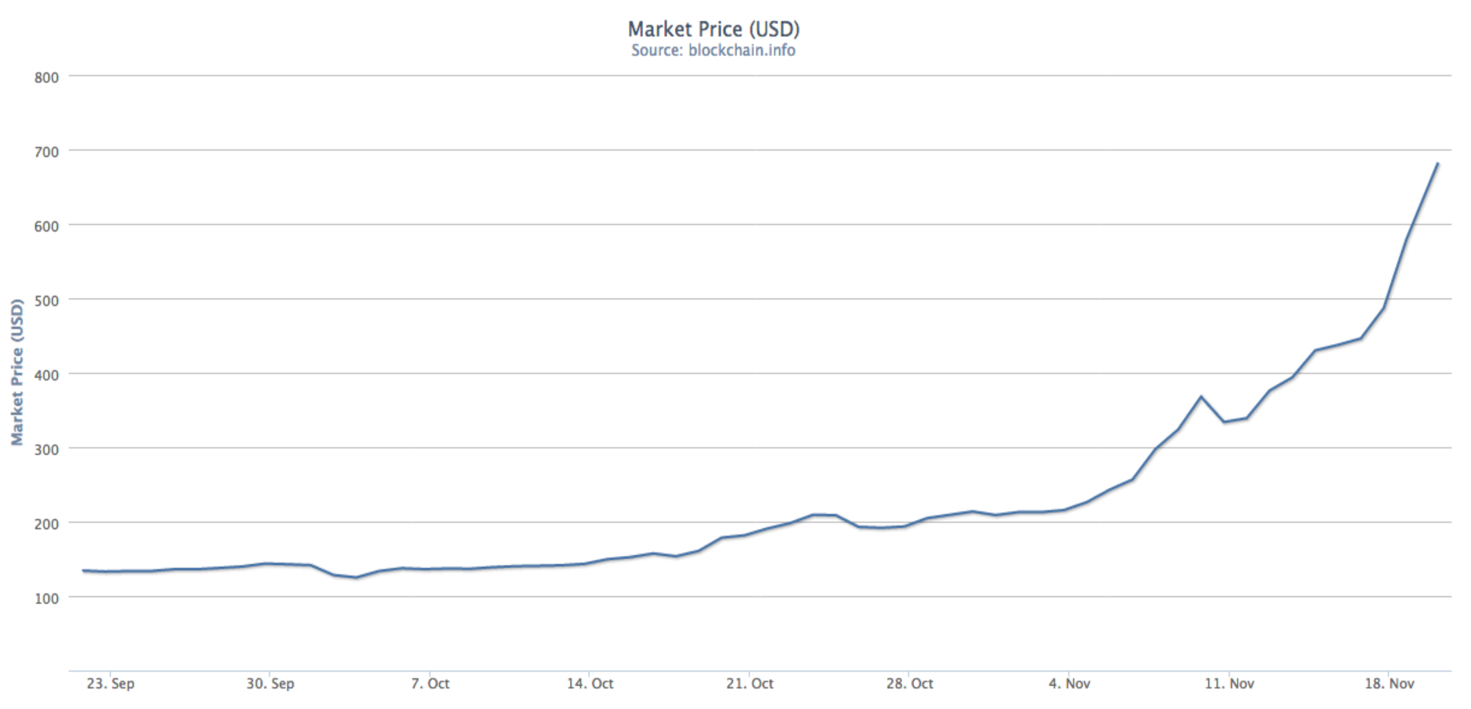
  1 Satoshi ⇔ 0.00000001 BTC

- Losing your private key => losing yours BTCs …Forever gone from BTC economy
- BTC is deflationary!

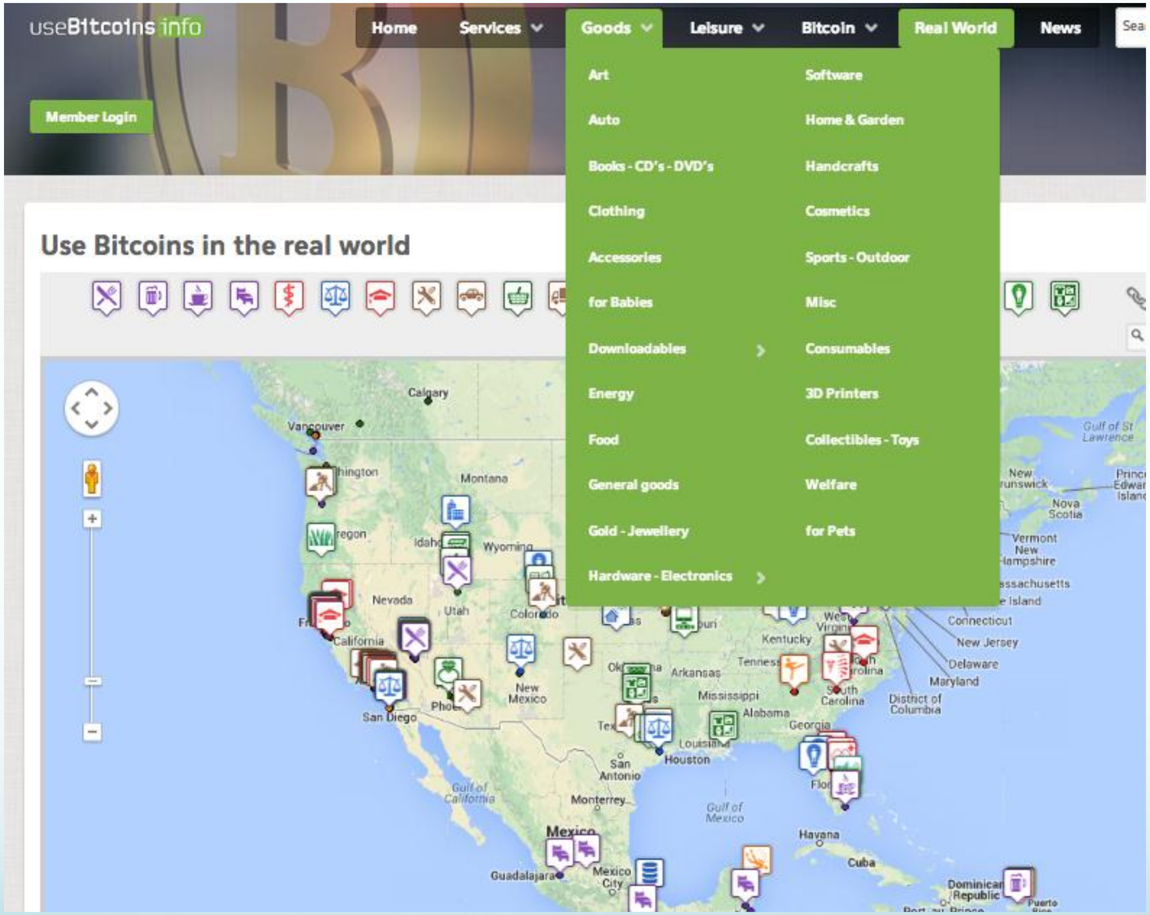
Security

- No one can change the BTC software without the majority of the entire network of users accepting the change
- While the majority of the nodes are honest, attackers cannot harm the system
- End of Block Chain Insecurity => Branches => Double Spending attack => Protected by the Hashcash / Time Stamp Server
- The attacker would need astronomical computer power to corrupt the block chain

Beware!!!


Market Price (USD)
Source: blockchain.info
Market Price (USD)
800
700
600
500
400
300
200
100
23. Sep
30. Sep
7. Oct
14. Oct
21. Oct
28. Oct
4. Nov
11. Nov
18. Nov

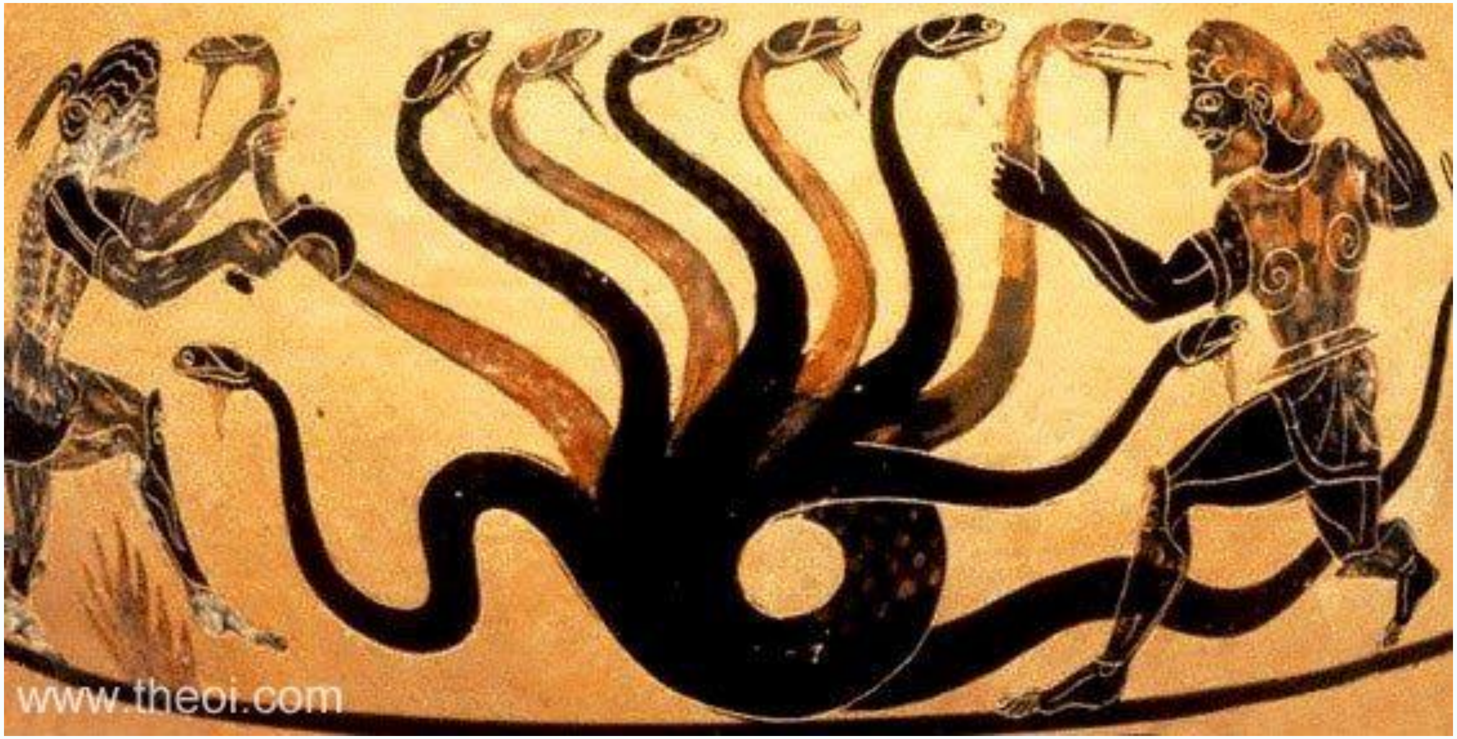
Where to use BTC?



Legal Considerations

- **Money laundry** – practically impossible to track BTC transactions

- **FBI x Silk Road** – Bitcoin used for trading drugs among other illicit products.



Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.”

Satoshi Nakamoto

Conclusions

- BTC: P2P digital currency with mathematic protection
- No centralized control / No evil Central Bank
- The exchange rates may oscillate drastically

***“…we don’t really understand how that worked, as economists.”* - Lawrence White, economics professor at George Mason University / IEEE Spectrum interview**

Conclusions

- No government can print more money
- Anonymity
- Lower global transaction costs
- A new bubble may emerge
  - Oct 2013 = 150 USD
  - Nov 2013 > 500 USD
- March 28th 2013: BTC passed the **1 Billion USD** (11 million Bitcoins in circulation)

References

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf
2. Khan Academy.http://www.youtube.com/user/khanacademy
3. Scott Driscoll. How Bitcoin Works Under the Hood.
4. http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
5. Adam Back. Hashcash. http://www.hashcash.org/