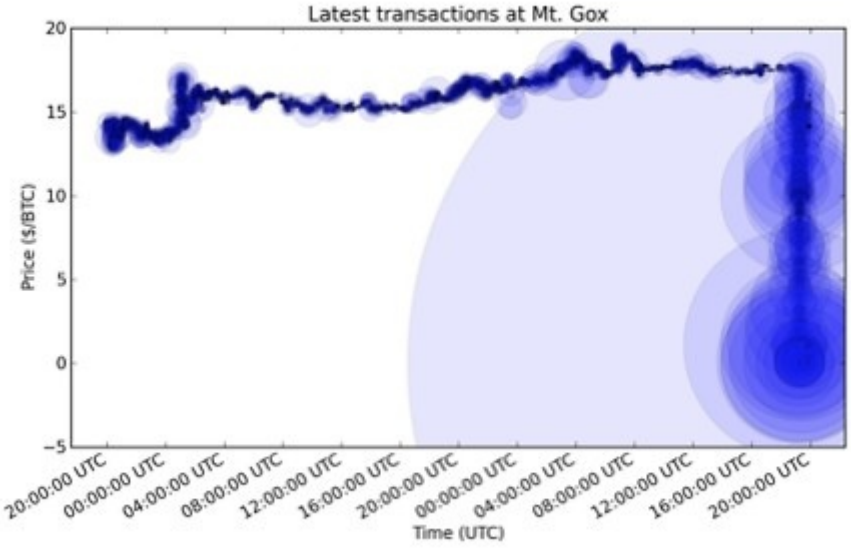
Bitcoin:
what it is & how it works

Max Uhlenhuth
November 1, 2011

Bitcoin - a history

- 2008 "Satoshi Nakamoto" whitepaper
- Mt. Gox (>80% of trade) founded July 2010
- June 21, 2011 flash crash



source: http://www.quora.com/Bitcoin/Is-the-cryptocurrency-Bitcoin-a-good-idea

Goals of any "e-cash" system

1. Hard to forge
2. Fast transactions
3. ***Prevent double-spending***
4. Anonymous

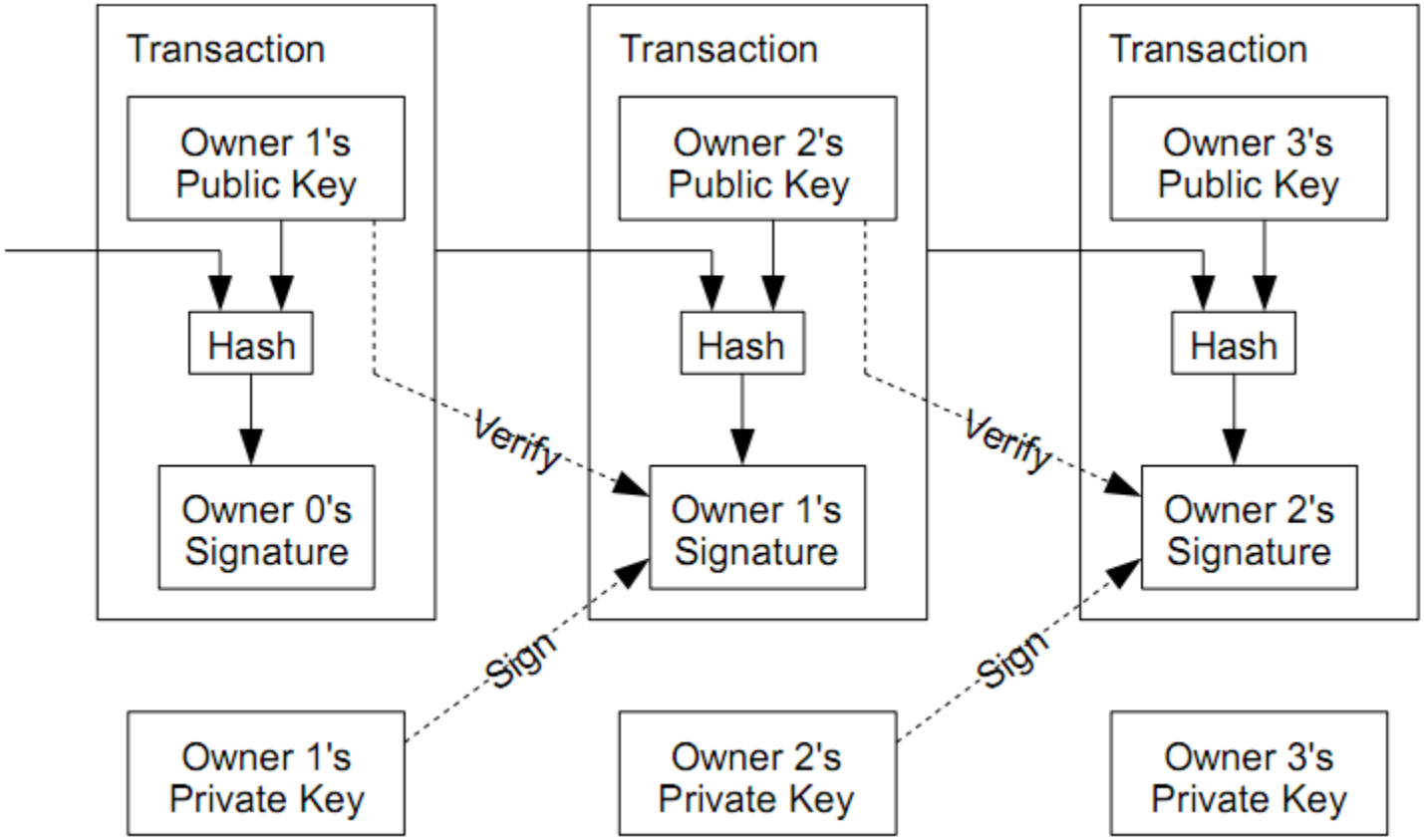
source: http://www.engr.sjsu.edu/gaojerry/course/cmpe296u/296z/e-cash-payment[1].v1.10.20.pdf

Bitcoin innovations

- "Proof of work" by P2P network:
  - validate transactions
  - "mine" currency
  - difficult to corrupt network
- Proof of work grows more difficult over time
- Merkle tree to store large transaction history

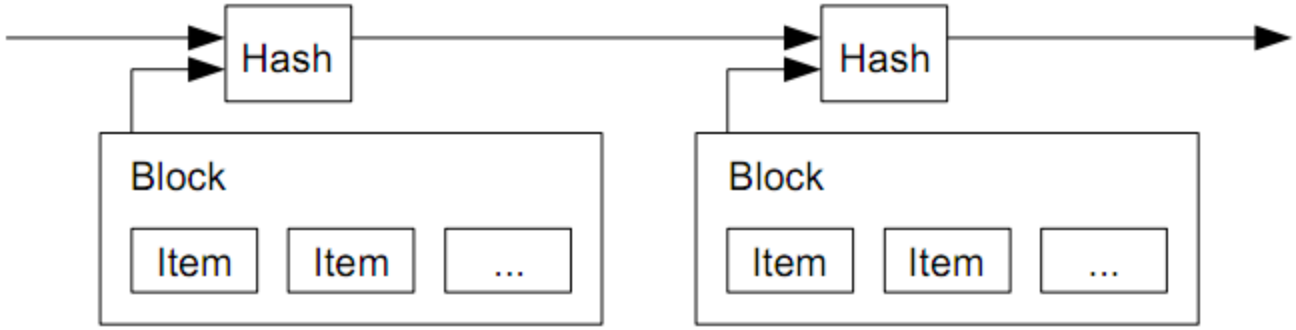
source: http://bitcoin.org/bitcoin.pdf

Bitcoin basics: transactions

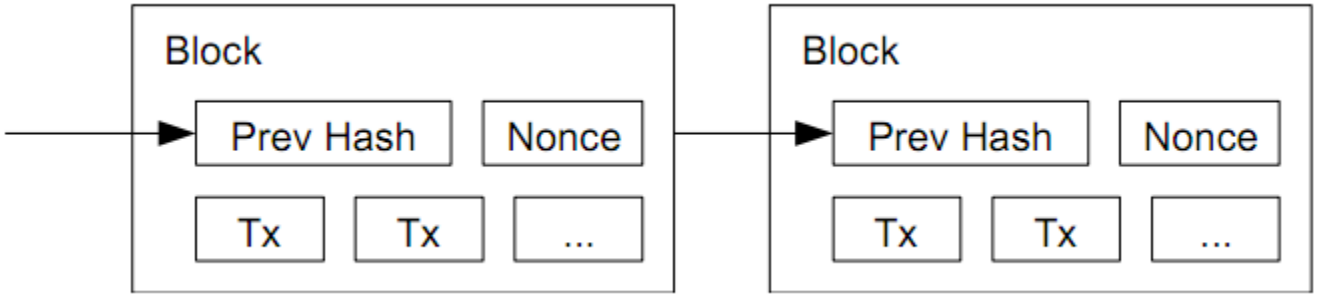


source: http://bitcoin.org/bitcoin.pdf

Bitcoin basics: timestamping blocks



Bitcoin basics: proof of work



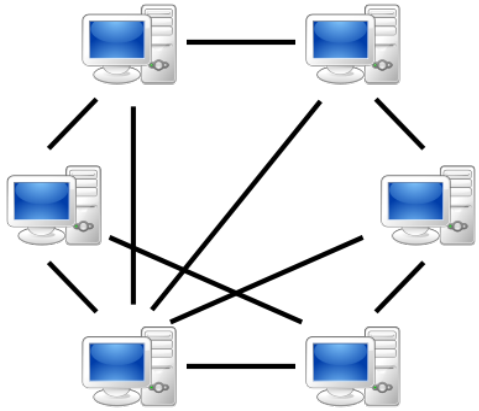
- Scanning for hash beginning with # of 0 bits
  - Increment "nonce" until find desired hash

- Exponentially hard in number of 0 bits

Bitcoin: the magic

- Block can't be changed without redoing PoW
  - Have to redo all blocks after it as well
- "One-CPU-one-vote"
  - Rather than "one-IP-one-vote"
- Majority decision is longest chain
  - Majority CPUs honest --> honest chain grows fastest
- PoW grows harder over time
  - Compensates for better hardware

Bitcoin: the network

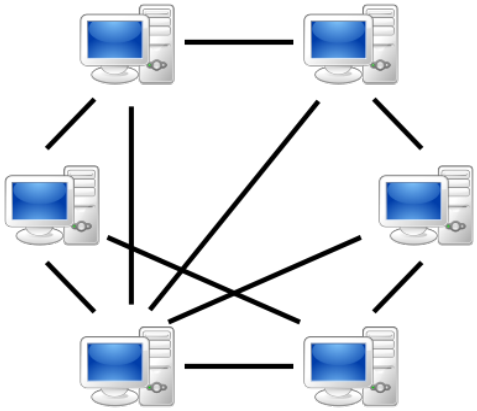


1. New transactions are broadcast to all nodes.

2. Each node collects new transactions into a block.

3. Each node works on finding a difficult PoW for its block.

Bitcoin: the network



4. When a node finds a PoW, broadcasts block to all nodes.

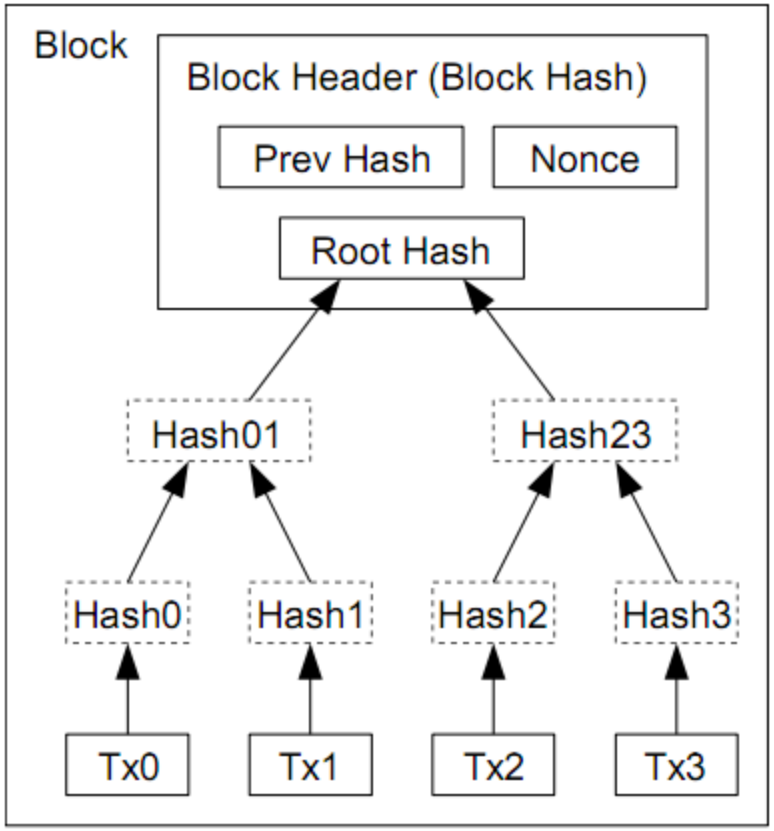
5. Nodes accept only if all transactions are not already spent.

6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

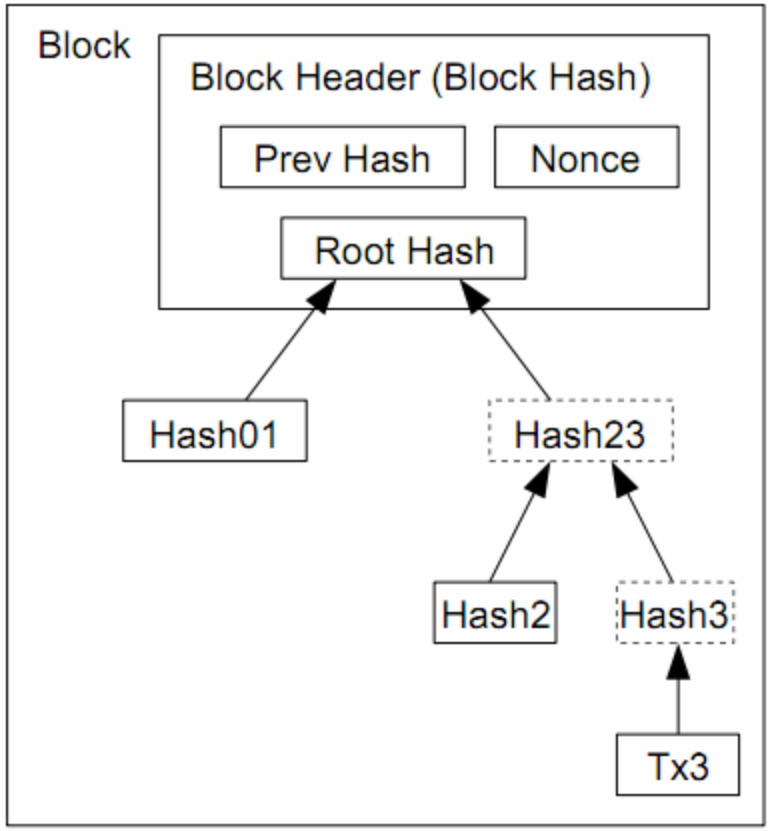
Bitcoin: mining

- First transaction in a block creates new coin
- Gives nodes incentive to support network
- Resources expended (electricity & CPU time) analagous expenditure by a "gold miner"

Bitcoin: disk space



Transactions Hashed in a Merkle Tree

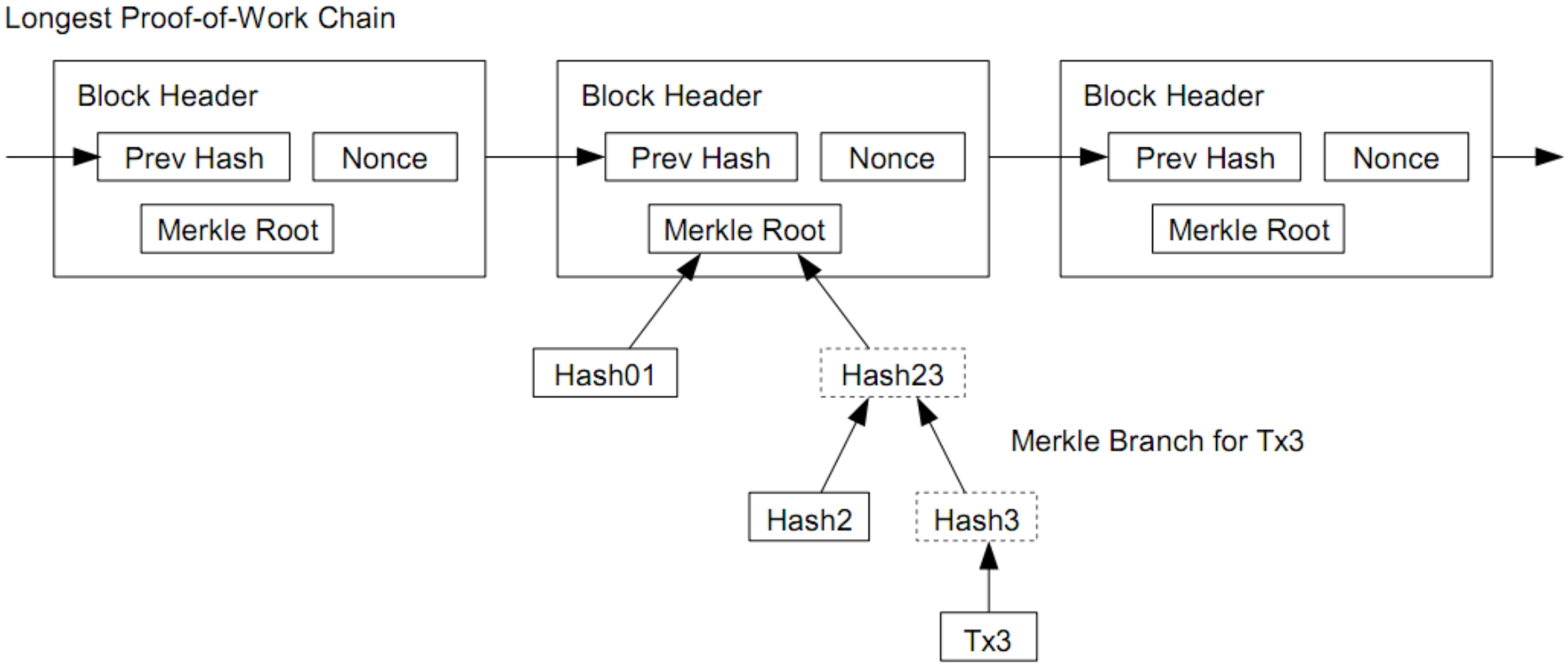


After Pruning Tx0-2 from the Block

Block generated every 10 minutes:

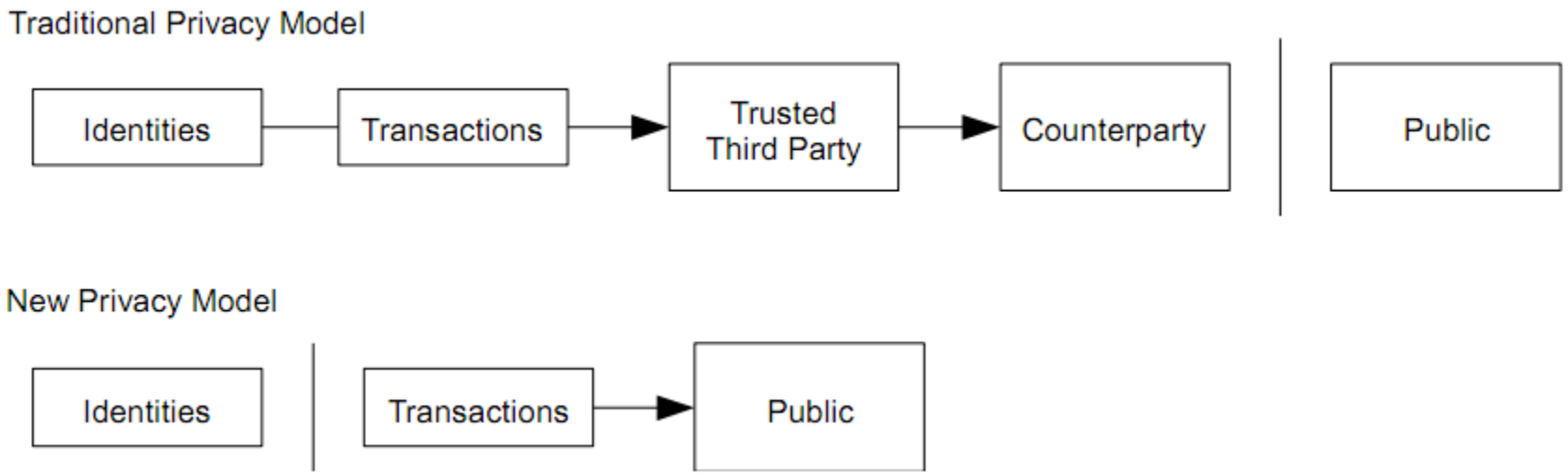
80 bytes/header * 6 * 24 * 365 = 4.2MB per year

Bitcoin: simple payment verification



1. Get Merkle branch Tx3 is timestamped in
2. Make sure it was accepted by network node

Bitcoin: privacy



- Keep public keys anonymous
  - New keypair for each transaction
- Similar to stock market ticker

Bitcoin: attack probabilities

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012
```

```
q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Bitcoin: implications

- Lower online transaction fees
- Anonymous online buying
- Alternative to sovereign currency
  - No debasing/inflation of the currency
- Universal currency
- Low infrastructure needs

Criticisms

- Initial seeding of wealth
- Deflation
- Convertibility issues
- Instability / lack of legal backing
- Bitcoin developer "invited" to see CIA already

Images from:

- http://commons.wikimedia.org/wiki/File:Light_Bulb_Icon.svg
- http://commons.wikimedia.org/wiki/File:Crystal_Project_wizard.png
- http://commons.wikimedia.org/wiki/File:P2P-network.svg
- http://commons.wikimedia.org/wiki/File:Schlaegel_und_Eisen_nach_DIN_21800_gedreht_um_180_Grad.svg
- http://de.wikipedia.org/wiki/Datei:Bitcoin.png
- http://en.wikipedia.org/wiki/File:CIA.svg