A Perspective on Cryptocurrencies

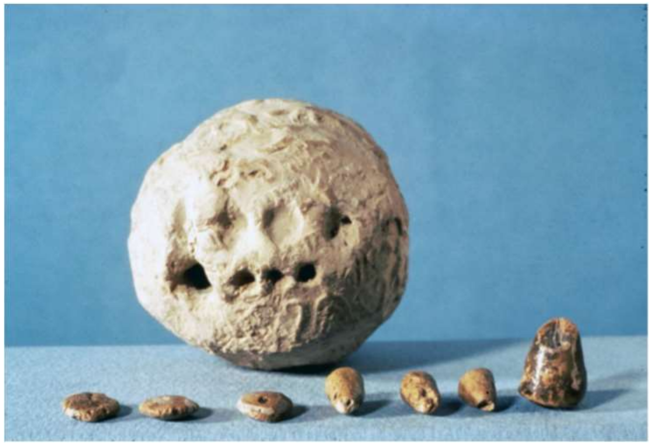
BART PRENEEL

IMEC-COSIC KU LEUVEN

BART.PRENEEL(AT)ESAT.KULEUVEN.BE

4 SEPTEMBER 2017

Currencies = maintaining memory



“Envelope and contents from Susa, Iran, ca **3300 BCE**”

“Each lenticular disc stands for “a flock” (perhaps 10 animals). The large cone represents a very large measure of grain; the small cones designate small measures of grain.”

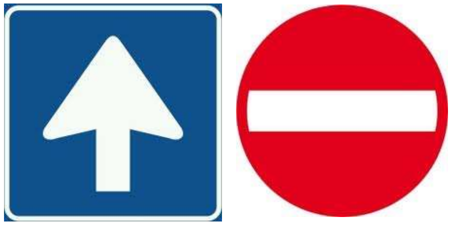
Tensions between centralized and de-centralized ways to remember value exchanges, debts, and what is due

- **Centralization (clay tablet):** economies of scale, high-integrity, vulnerable
- **Decentralized (coins):** high-availability, difficult to destroy as a system, forgery

Image provided courtesy of Denise Schmandt-Besseratand Musée du Louvre, Département des Antiquités Orientales

Slide credit: George Danezis

Hash functions (1975): one-way easy to compute but hard to invert



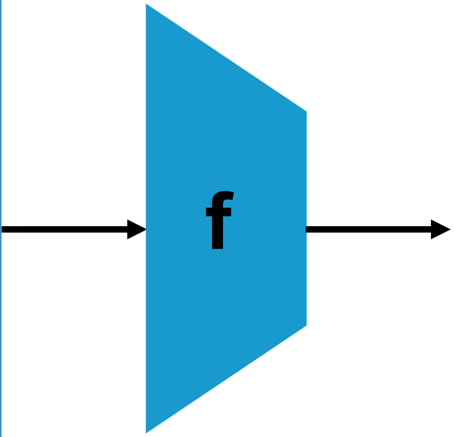
RIPEMD-160

SHA-256

SHA-512

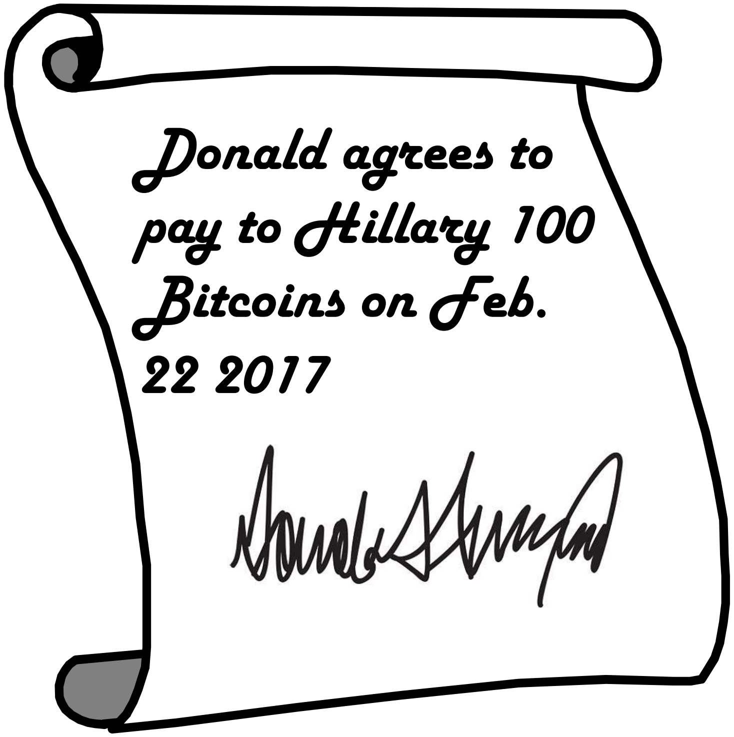
SHA-3

This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).



1A3FD4128A198FB3CA345932

Digital signatures (1975): “equivalent” to manual signature



Donald agrees to pay to Hillary 100 Bitcoins on Feb. 22 2017

Public key

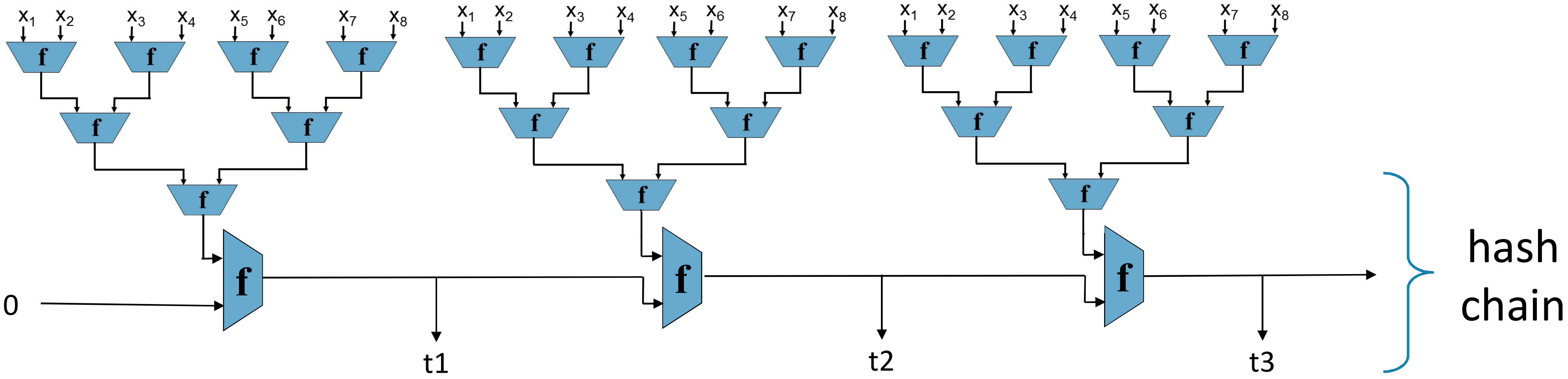
Private key

Timestamping (1990)

Collect documents and hash them with a Merkle tree

Chain these trees together with a hash chain

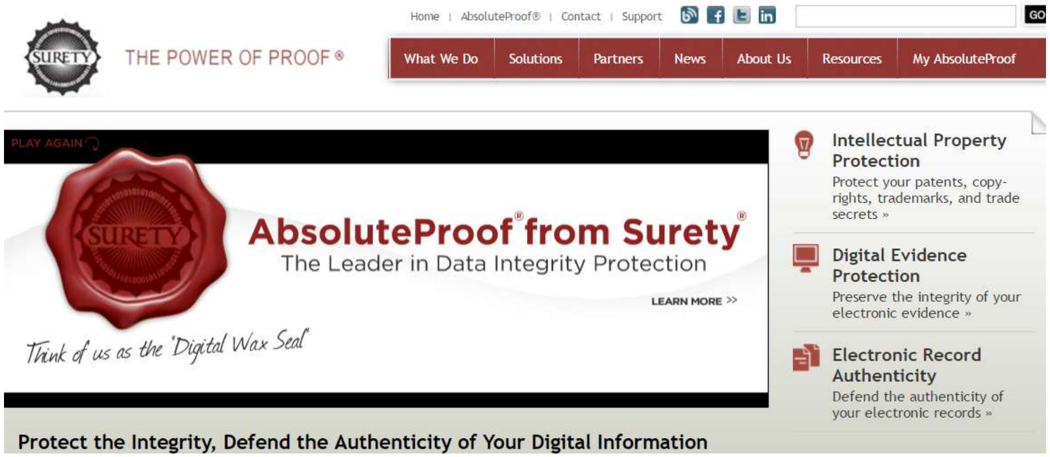
Publish intermediate values on a regular basis



x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
f
0
t1
t2
t3
hash
chain

Timestamping: Surety Technologies (°1994)

http://www.surety.com/



AbsoluteProof® from Surety®

The Leader in Data Integrity Protection

Think of us as the 'Digital Wax Seal'

Intellectual Property Protection

Protect your patents, copyrights, trademarks, and trade secrets »

Digital Evidence Protection

Preserve the integrity of your electronic evidence »

Electronic Record Authenticity

Defend the authenticity of your electronic records »

Protect the Integrity, Defend the Authenticity of Your Digital Information

https://www.belspo.be/belspo/organisation/Publ/pub_ostc/NO/rNOb007_en.pdf
Belgian TIMESEC project (1997-1999)

Estonia: Cybernetica

Bitcoin? (white paper Oct’08 – live Jan ‘09)

http://www.bitcoin.org http://www.blokchain.info

E-currency with distributed generation and verification of money

Transactions

- irreversible
- inexpensive
- over anonymous peer-to-peer network
- broadcast within seconds and verified within 10 to 60 minutes by inclusion in hash chain
- pay using private key (digital signature); verify with public key
- double spending prevention using a public decentralized ledger (chaining mechanism)

Pseudonymous

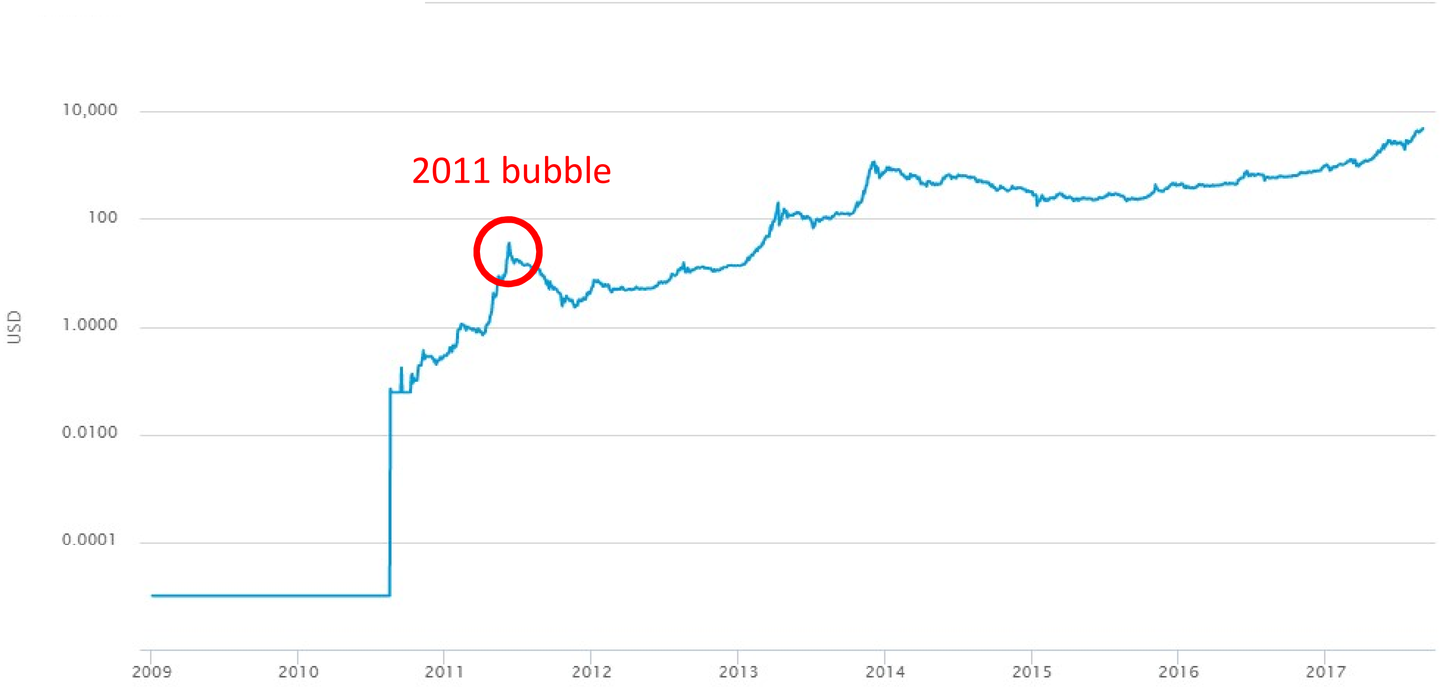
- Money is linked to public key – can generate arbitrary key pairs and move money around
  - But in many cases identification is possible

Market price in USD (market cap ≈ 81 B$)

1 Bitcoin = 4,620.06$

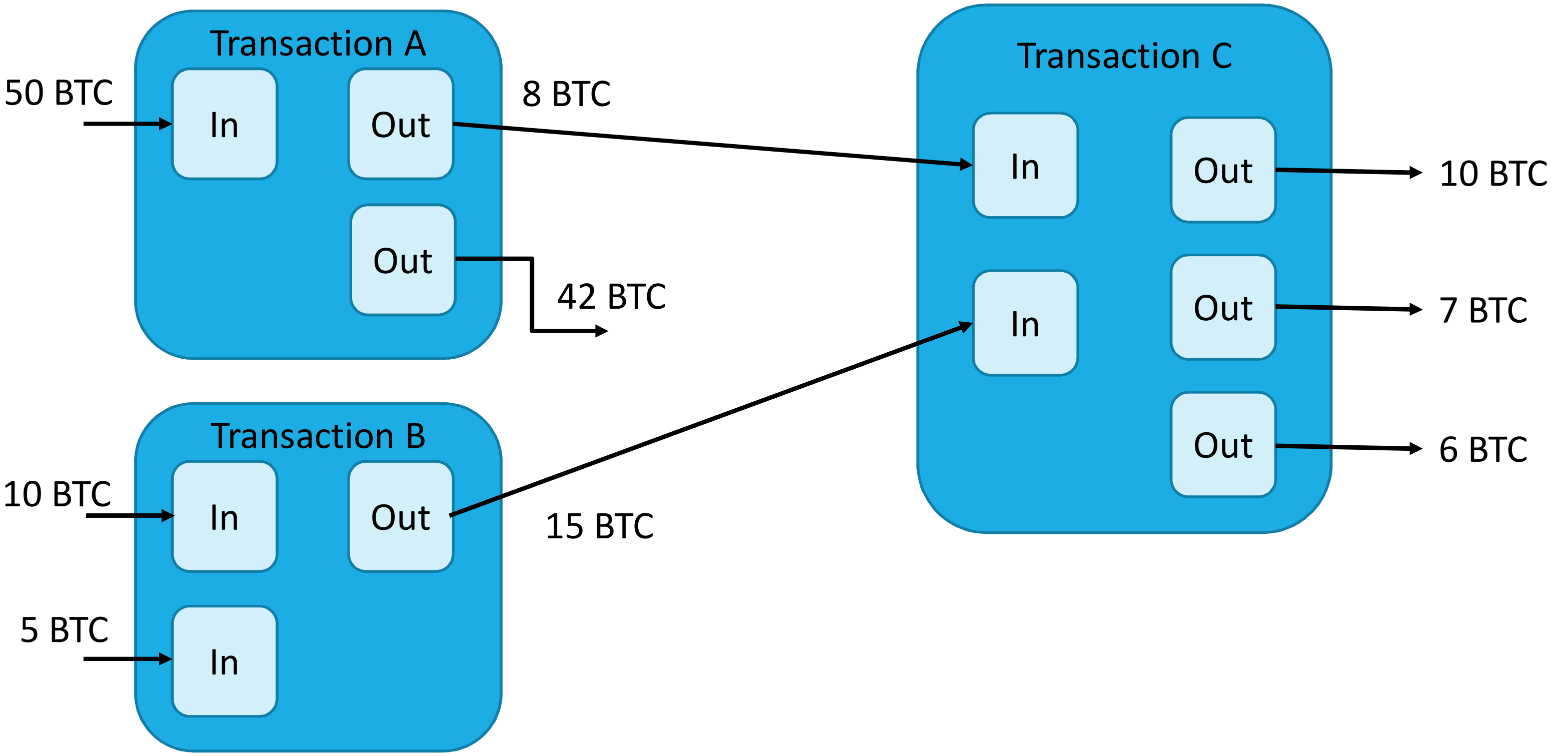
Market Price (USD)

source: blockchain.info



2011 bubble

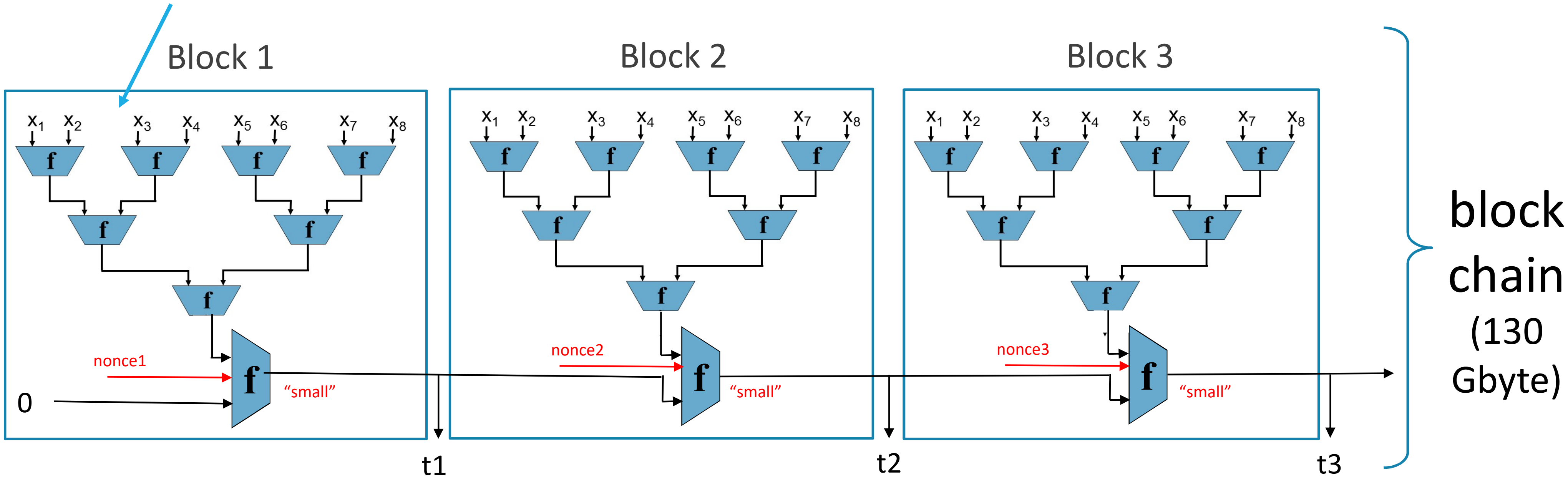
Bitcoin Transaction: send money from one public key (address) to another one



Slide credit: F. Vercauteren

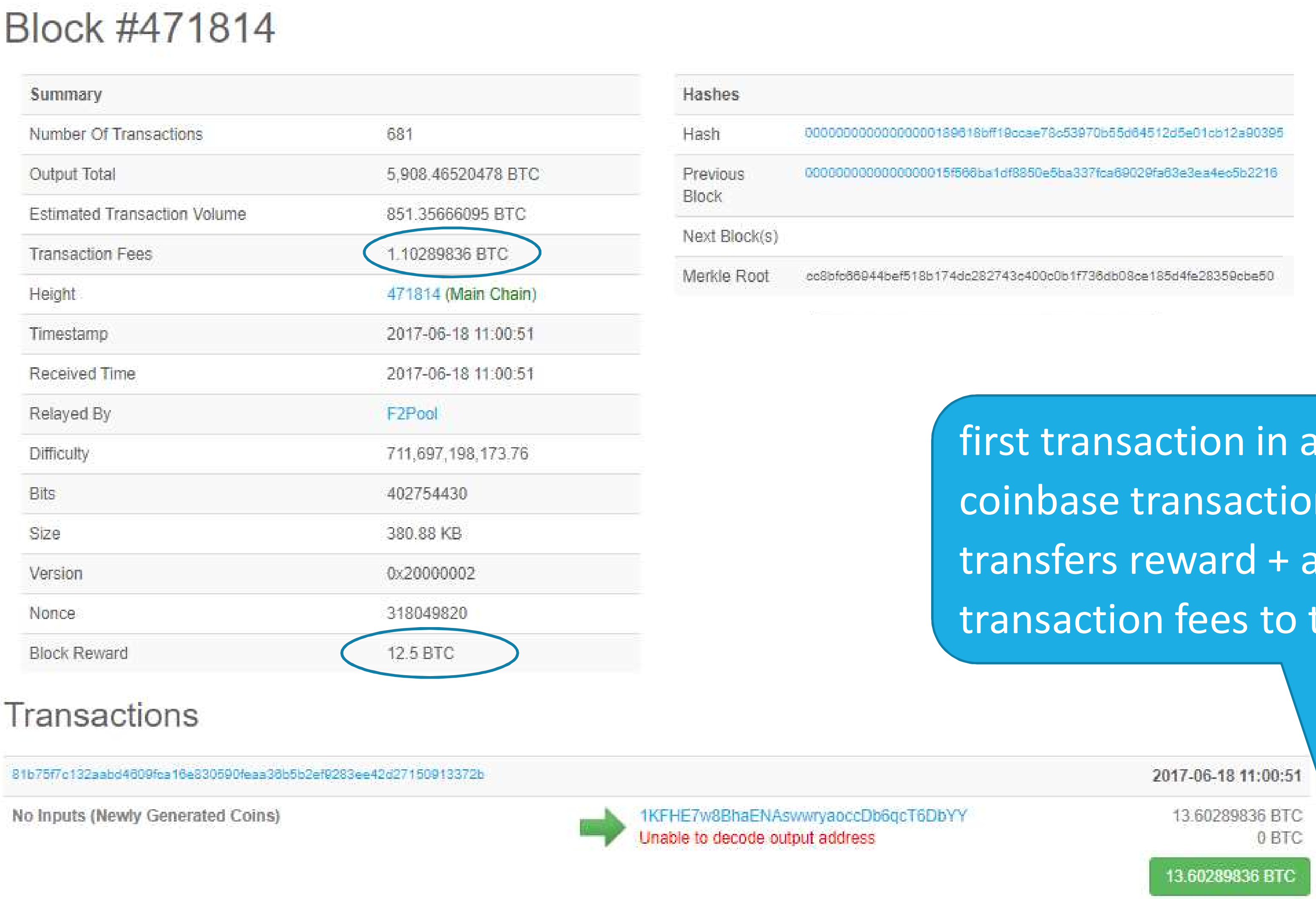
Block Chain: a public decentralized ledger

Bitcoin transactions



block chain (130 Gbyte)

Also include in every block timestamp and difficulty level of puzzle



Block #471814

Summary	
Number Of Transactions	681
Output Total	5,908.46520478 BTC
Estimated Transaction Volume	851.35666095 BTC
Transaction Fees	1.10289836 BTC
Height	471814 (Main Chain)
Timestamp	2017-06-18 11:00:51
Received Time	2017-06-18 11:00:51
Relayed By	F2Pool
Difficulty	711,697,198,173.76
Bits	402754430
Size	380.88 KB
Version	0x20000002
Nonce	318049820
Block Reward	12.5 BTC

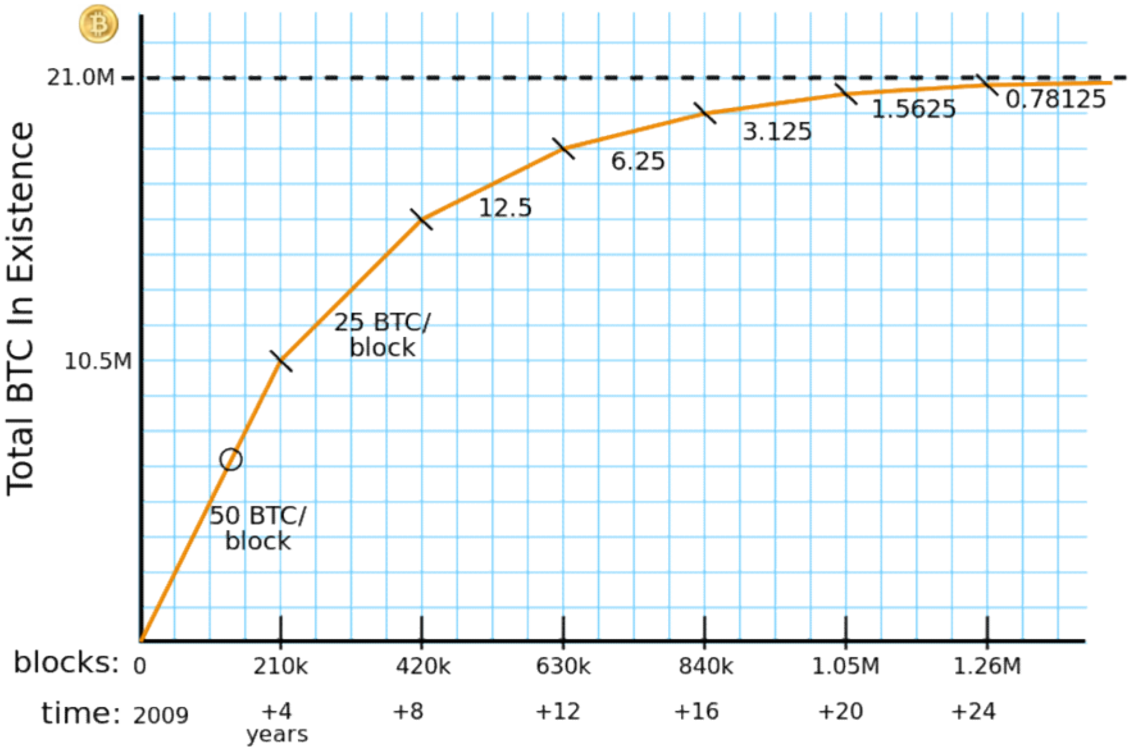
Hashes	
Hash	000000000000000000189618bff19ccae78c53970b55d64512d5e01cb12a90395
Previous Block	0000000000000000015f566ba1df8850e5ba337fca69029fa63e3ea4ec5b2216
Next Block(s)	
Merkle Root	cc8bfc66944bef518b174dc282743c400c0b1f736db08ce185d4fe28359cbe50

Transactions

81b75f7c132aabd4609fca16e830590feaa36b5b2ef9283ee42d27150913372b		2017-06-18 11:00:51
No Inputs (Newly Generated Coins)	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY Unable to decode output address	13.60289836 BTC 0 BTC
		13.60289836 BTC

first transaction in a block is a coinbase transaction: transfers reward + all transaction fees to the miner

Mining Rewards: coinbase + fees



Total number of Bitcoins is limited to 21 million, each divided in 8 decimal places leading to 21×10^{14} units

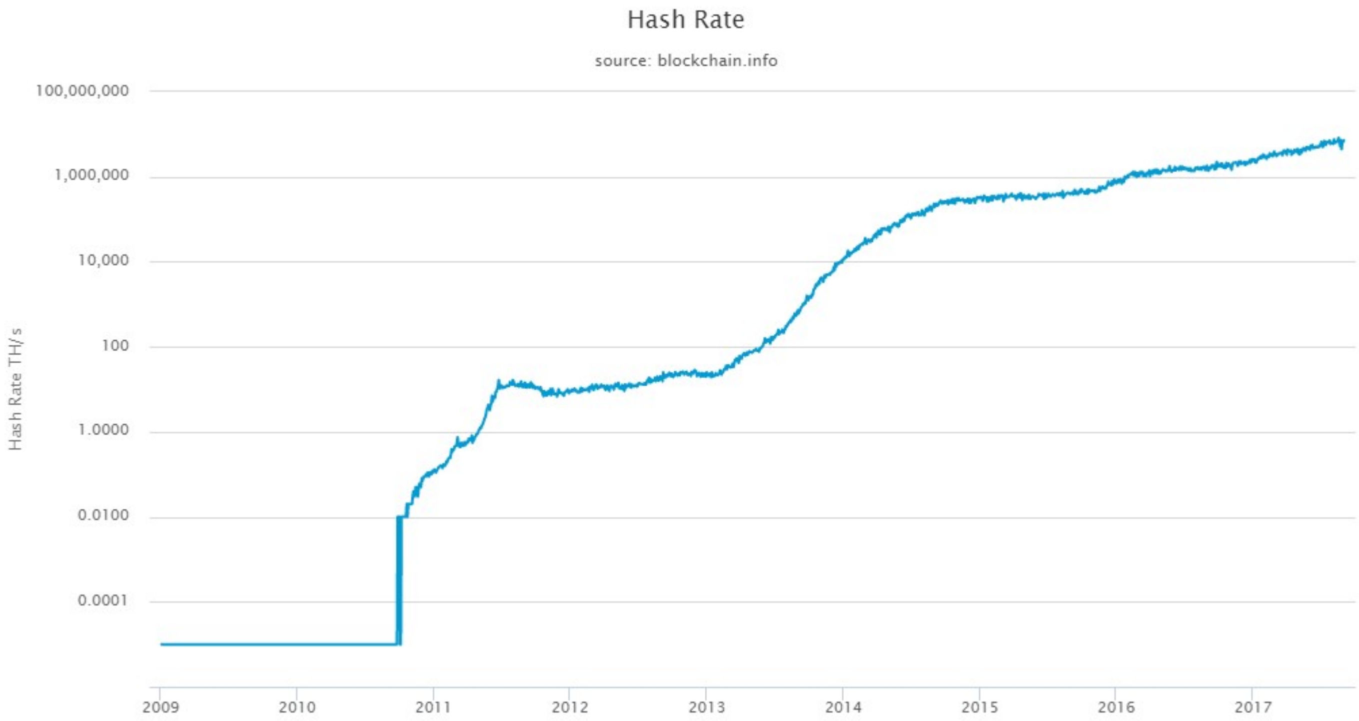
Figure by Chris Pacia

Bitcoin summary

- Public decentralized ledger (block chain)
- Of transactions that transfer value (bitcoin) from
  - one or more “senders” or inputs
  - to one or more “recipients” or outputs
  - protected by a digital signature
- Integrity of ledger is secured by miners
  - audit transactions
  - use proof-of-work to arrive at consensus about the transactions
  - successful miner receives reward creating new bitcoin

Mining hash rate of Bitcoin network

7.5 EH/s = 7.5 ExaHash per second = 7.5 10^{18} hash/second = $2^{62.7}$ hash/second = 2^{79} hash/day


Hash Rate

source: blockchain.info

Exa

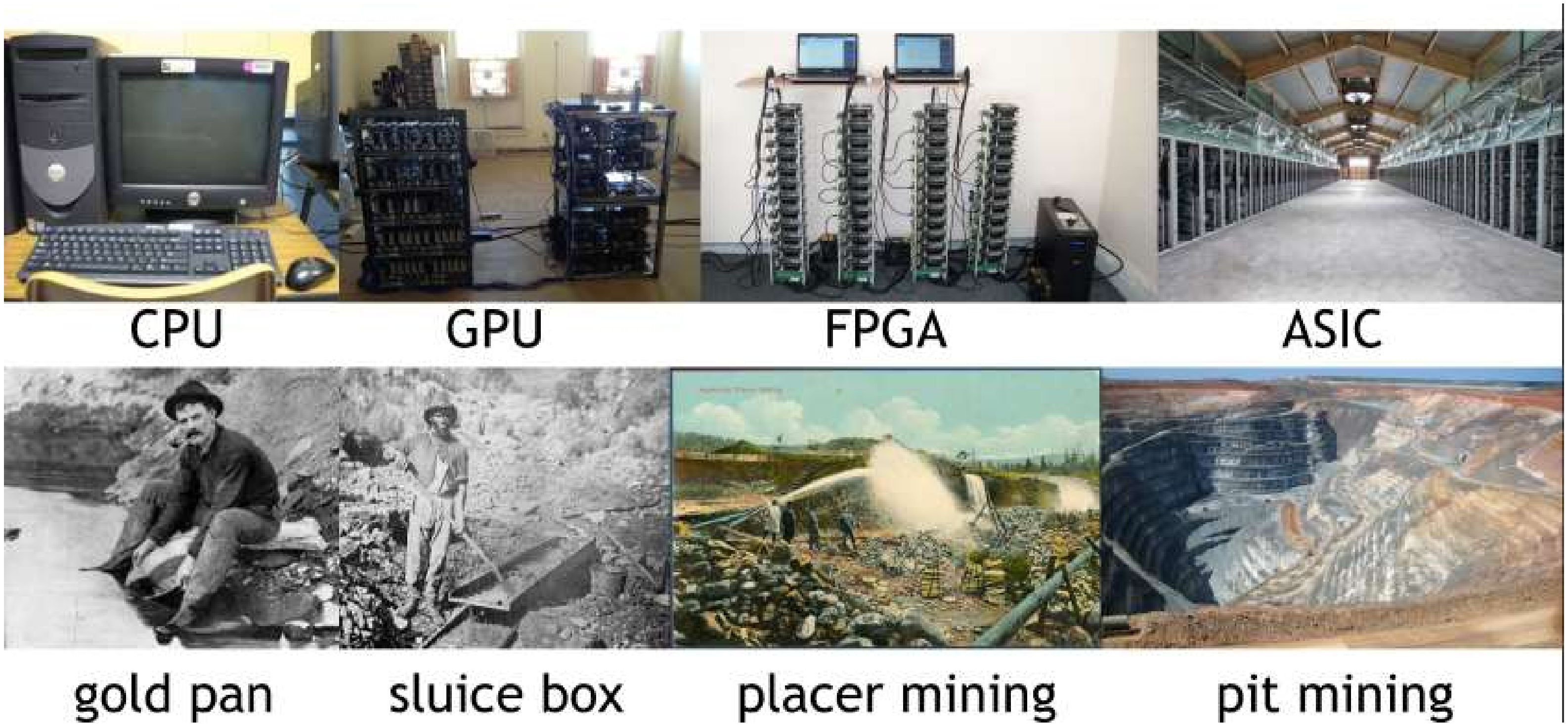
Peta

Tera

Giga

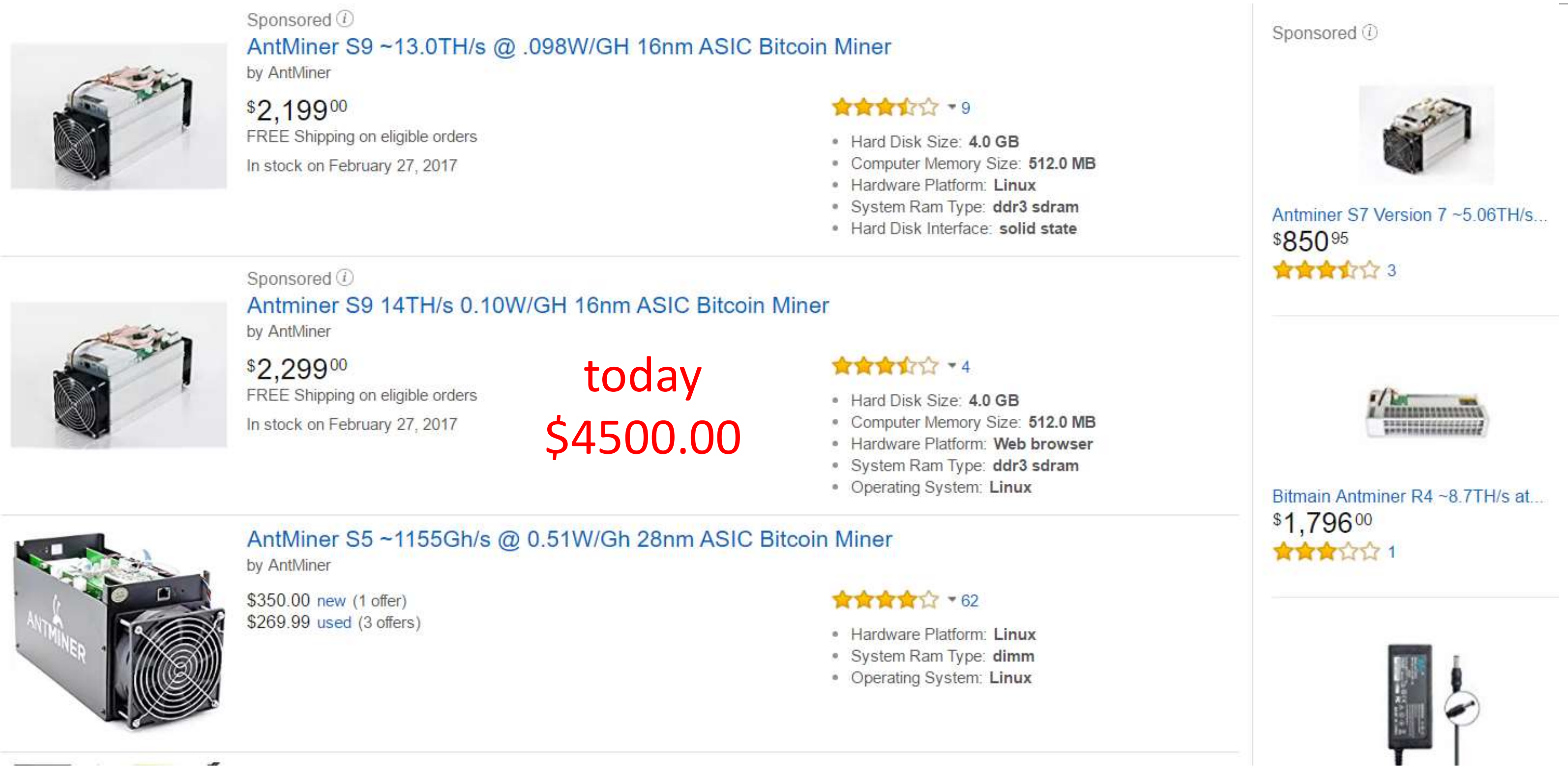
Mega

Mining has become industrial



Slide credit: Joseph Bonneau

Mining equipment on Amazon



Sponsored ⓘ

AntMiner S9 ~13.0TH/s @ .098W/GH 16nm ASIC Bitcoin Miner

by AntMiner

$2,199.00

FREE Shipping on eligible orders

In stock on February 27, 2017

★★★½☆ ▾ 9

- Hard Disk Size: **4.0 GB**
- Computer Memory Size: **512.0 MB**
- Hardware Platform: **Linux**
- System Ram Type: **ddr3 sdram**
- Hard Disk Interface: **solid state**

Sponsored ⓘ

Antminer S9 14TH/s 0.10W/GH 16nm ASIC Bitcoin Miner

by AntMiner

$2,299.00

FREE Shipping on eligible orders

In stock on February 27, 2017

★★★½☆ ▾ 4

- Hard Disk Size: **4.0 GB**
- Computer Memory Size: **512.0 MB**
- Hardware Platform: **Web browser**
- System Ram Type: **ddr3 sdram**
- Operating System: **Linux**

today
$4500.00

AntMiner S5 ~1155Gh/s @ 0.51W/Gh 28nm ASIC Bitcoin Miner

by AntMiner

$350.00 new (1 offer)
$269.99 used (3 offers)

★★★★☆ ▾ 62

- Hardware Platform: **Linux**
- System Ram Type: **dimm**
- Operating System: **Linux**

Sponsored ⓘ

Antminer S7 Version 7 ~5.06TH/s...

$850.95

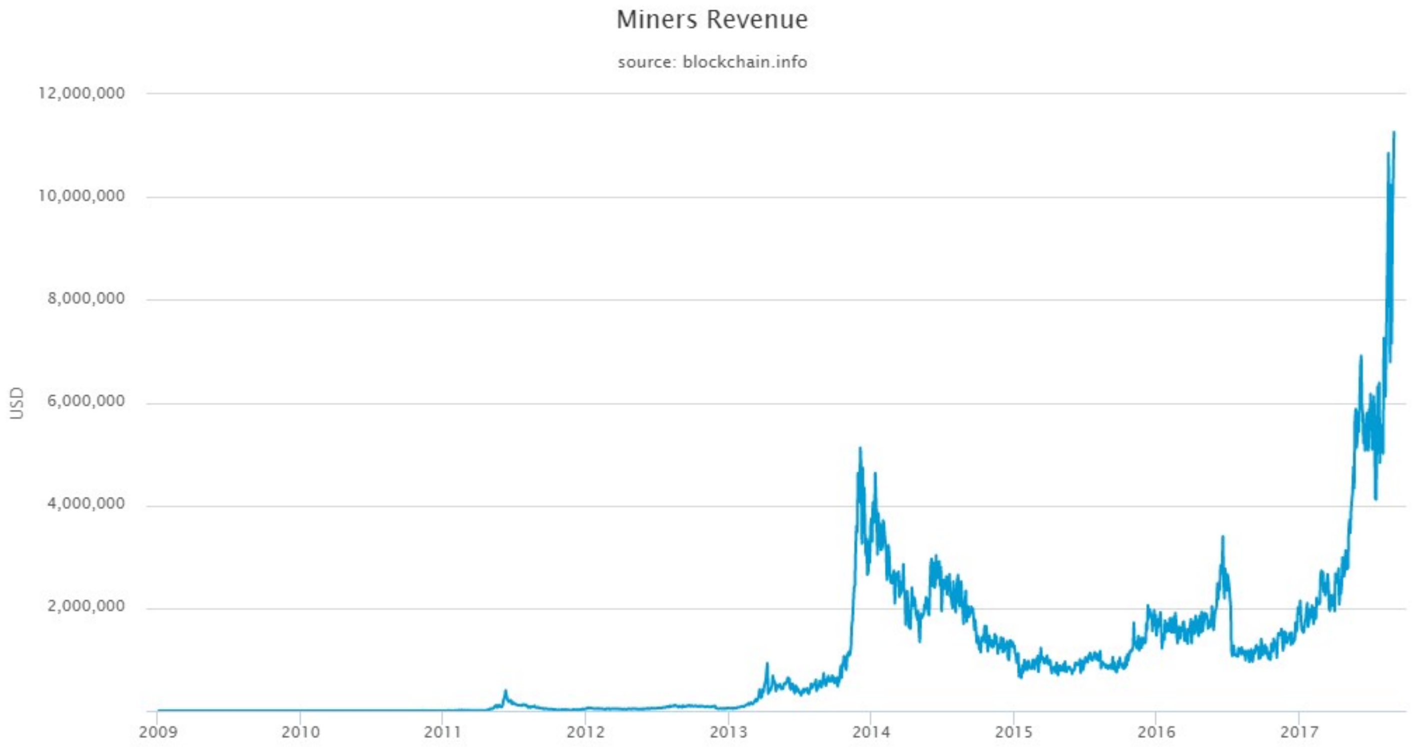
★★★½☆ 3

Bitmain Antminer R4 ~8.7TH/s at...

$1,796.00

★★★☆☆ 1

Miners Revenue



Miners Revenue

source: blockchain.info

Cost of Leaderless Consensus

Distributed consensus protocol:

- whichever coalition deploys most hash power, has control of the block chain
- 7.5 10^{18} hash/second is a significant cost.
- not performing any useful task!

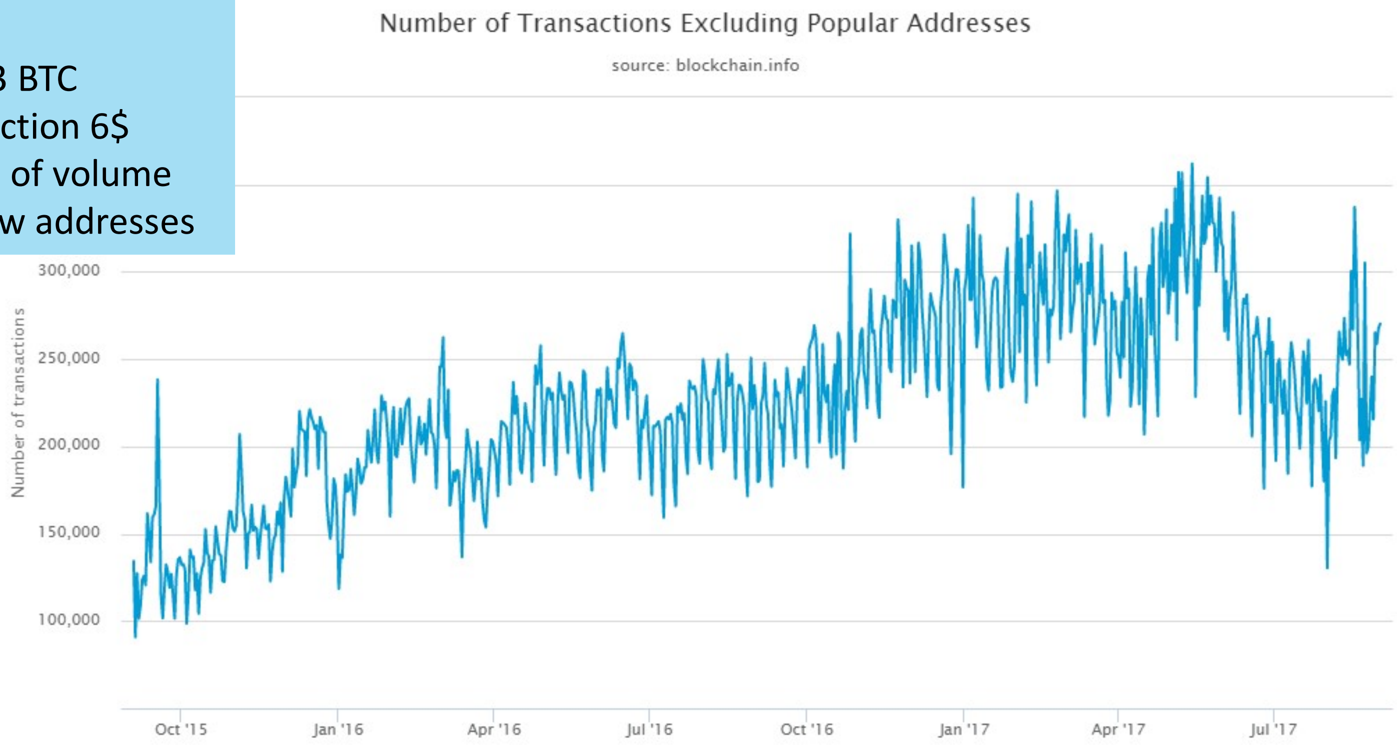
Electricity + Networking costs:

- 0.10 W/GH/s or 750 MWatt (3/4 of a nuclear plant)
- @10 cent per KWh: 1 block costs 12,500$ electricity (12.5 BTC = +/-57,750$)

Profit calculator: http://www.vnbitcoin.org/bitcoincalculator.php

Number of Transactions Per Day

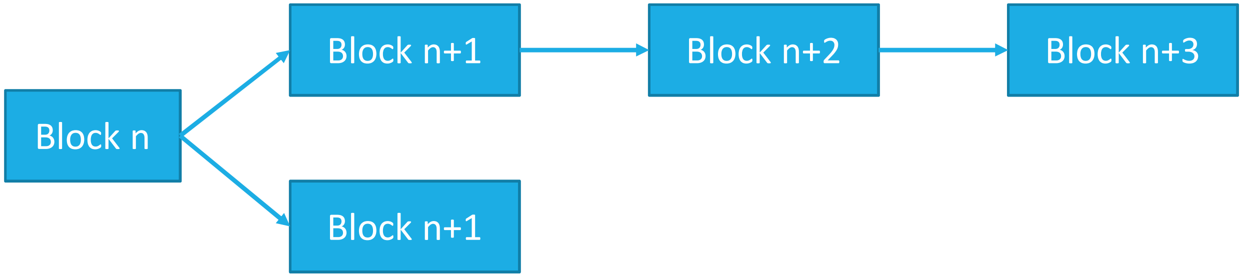
3.5 transactions/s
transaction fee/block: 3 BTC
average cost per transaction 6$
transaction fees: 0.15% of volume
large share goes to a few addresses



Bank card payments: around 10.000 per second?

Block Chain Forks

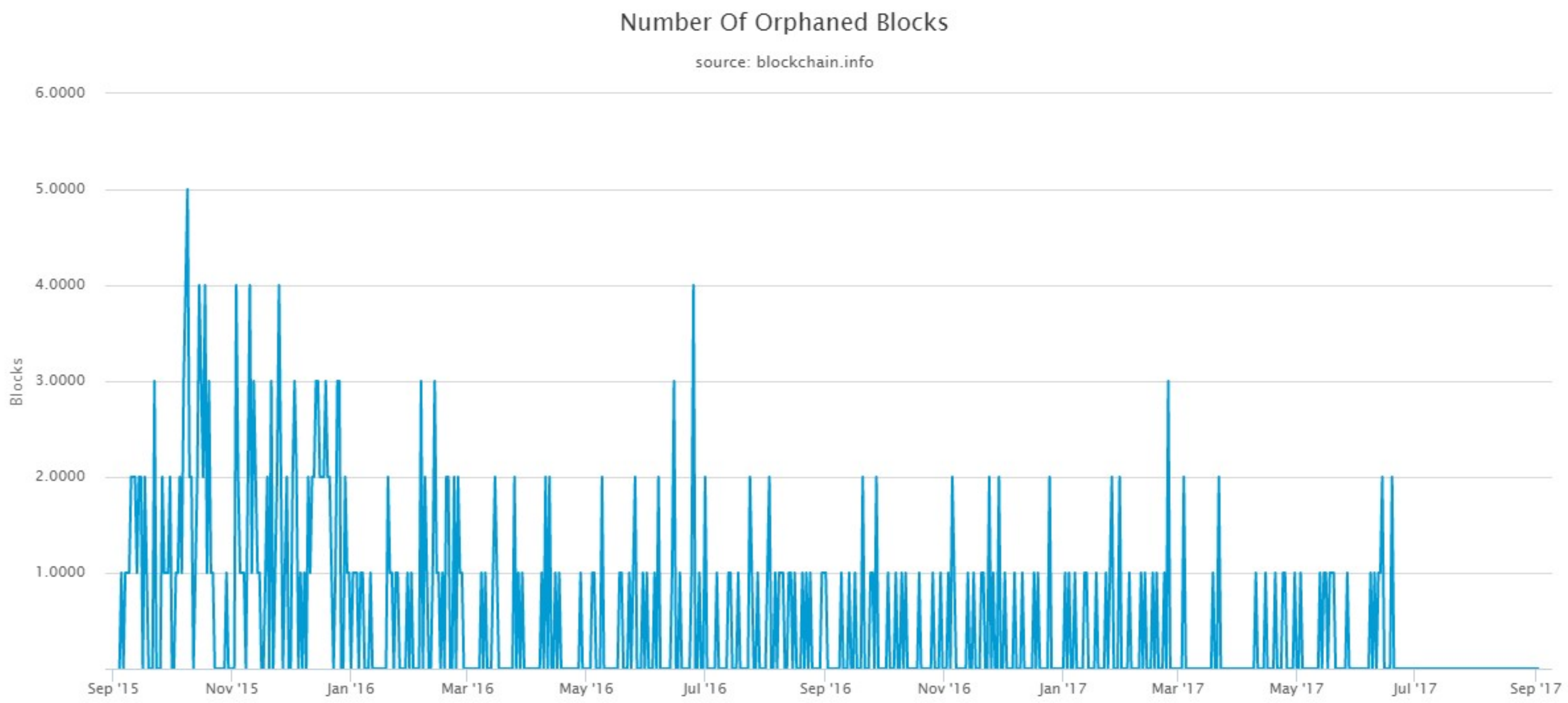
- Miners check for double spending before including a transaction
- Miners broadcast a new valid block to their neighbours immediately, who then propagate it to some of their neighbours etc…
- The block chain normally is one long chain
- Distributed nature of the network can lead to forks:



- Miners choose on which of 2 possible extensions to work
- Longest chain will become the main chain, transactions in orphan blocks are rebroadcast
- The more block that follow the harder it becomes to change a particular block
- Transaction is typically accepted after it is included in 6 blocks (60 minutes)

Slide credit: F. Vercauteren

Number of Orphaned blocks



Bitcoin Crypto

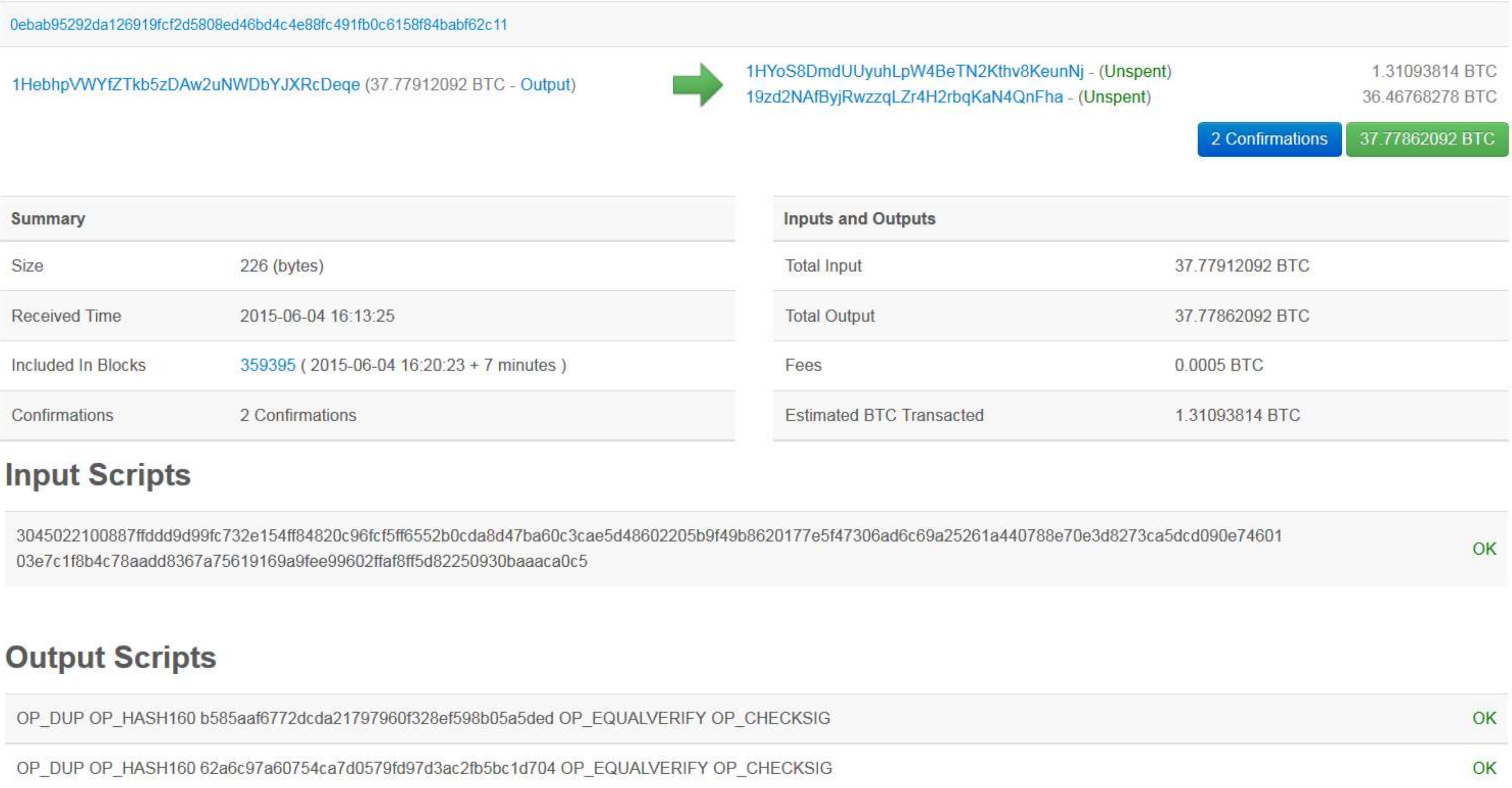
Hash functions:

- SHA-256:
  - Computing ID of block: double hash to avoid length extension
  - Hashing transaction before it is digitally signed (double hash)
  - Computing address given public key or script
- RIPEMD-160:
  - Computing address after SHA-256 to get 20-byte result

Digital signature algorithm:

- ECDSA-SHA256 using curve $y^2 = x^3 + 7$ modulo p where $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
- Private key: 256-bit scalar k, Public key: point [k]G on the curve E, with G base point
- Signature consists of two scalars (r,s) each having max 256 bits
- Can be verified using public key [k]G and the message m that was signed

Slide credit: F. Vercauteren



0ebab95292da126919fcf2d5808ed46bd4c4e88fc491fb0c6158f84babf62c11

1HebhpVWYfZTkb5zDAw2uNWDbYJXRcDeqe (37.77912092 BTC - Output)

1HYoS8DmdUUyuhLpW4BeTN2Kthv8KeunNj - (Unspent)	1.31093814 BTC
19zd2NAfByjRwzzqLZr4H2rbqKaN4QnFha - (Unspent)	36.46768278 BTC

Summary	
Size	226 (bytes)
Received Time	2015-06-04 16:13:25
Included In Blocks	359395 (2015-06-04 16:20:23 + 7 minutes)
Confirmations	2 Confirmations

Inputs and Outputs	
Total Input	37.77912092 BTC
Total Output	37.77862092 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	1.31093814 BTC

Input Scripts

```
3045022100887ffddd9d99fc732e154ff84820c96fcf5ff6552b0cda8d47ba60c3cae5d48602205b9f49b8620177e5f47306ad6c69a25261a440788e70e3d8273ca5dcd090e74601
03e7c1f8b4c78aadd8367a75619169a9fee99602ffaf8ff5d82250930baaaca0c5                                                      OK
```

Output Scripts

```
OP_DUP OP_HASH160 b585aaf6772dcda21797960f328ef598b05a5ded OP_EQUALVERIFY OP_CHECKSIG          OK
OP_DUP OP_HASH160 62a6c97a60754ca7d0579fd97d3ac2fb5bc1d704 OP_EQUALVERIFY OP_CHECKSIG          OK
```

Is Bitcoin Anonymous?

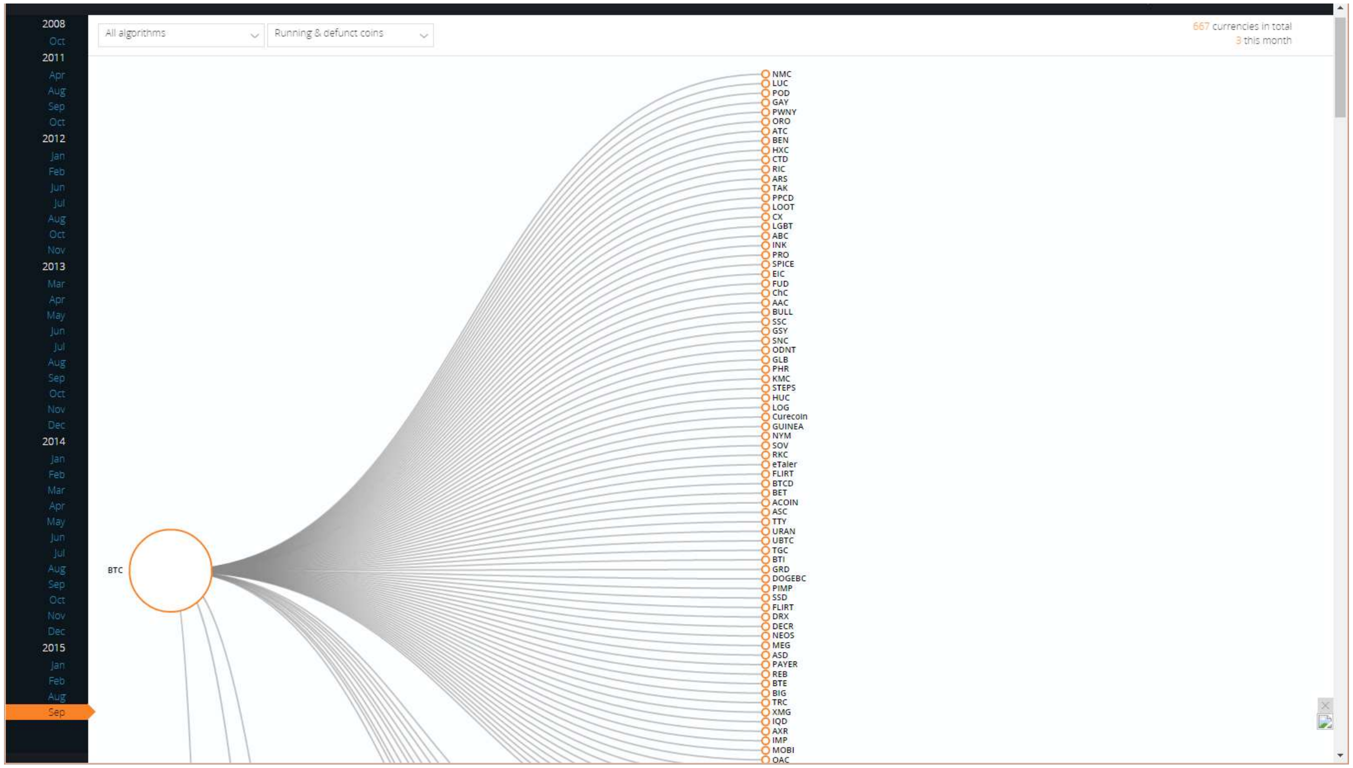
- Betcoin gambling site was hacked in April 2012
- 3,171 BTC were stolen in total (2902, 165, 17, and 87 BTC)
- Did not move until March 15 2013 (BTC goes up)
- Aggregated with other small addresses into one large address
- Then began a peeling chain
- After 10 hops, a peel went to Bitcoin-24
- And in another 10 hops a peel went to Mt. Gox

in total, 374.49 BTC go to known exchanges, all directly off the main peeling chain, which originated directly from the addresses known to belong to the thief.

S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage: A fistful of bitcoins: characterizing payments among men with no names. Internet Measurement Conference 2013: 127-140

Slide credit: George Danezis 24

Alt CoinsToday: 700+ currencies derived from Bitcoin (see http://mapofcoins.com/bitcoin)



All algorithms

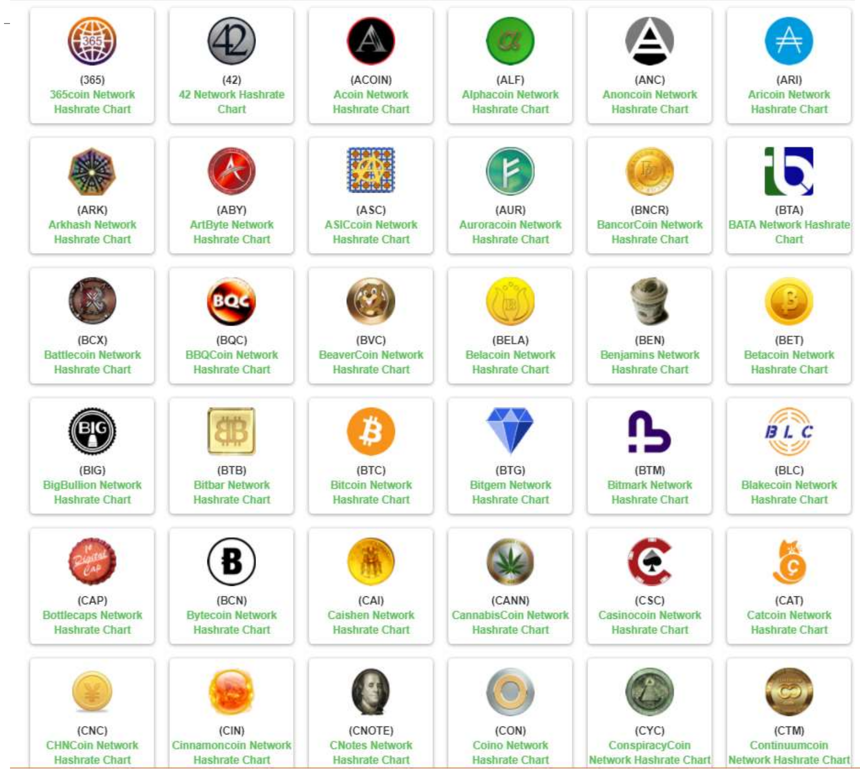
Running & defunct coins

667 currencies in total
3 this month

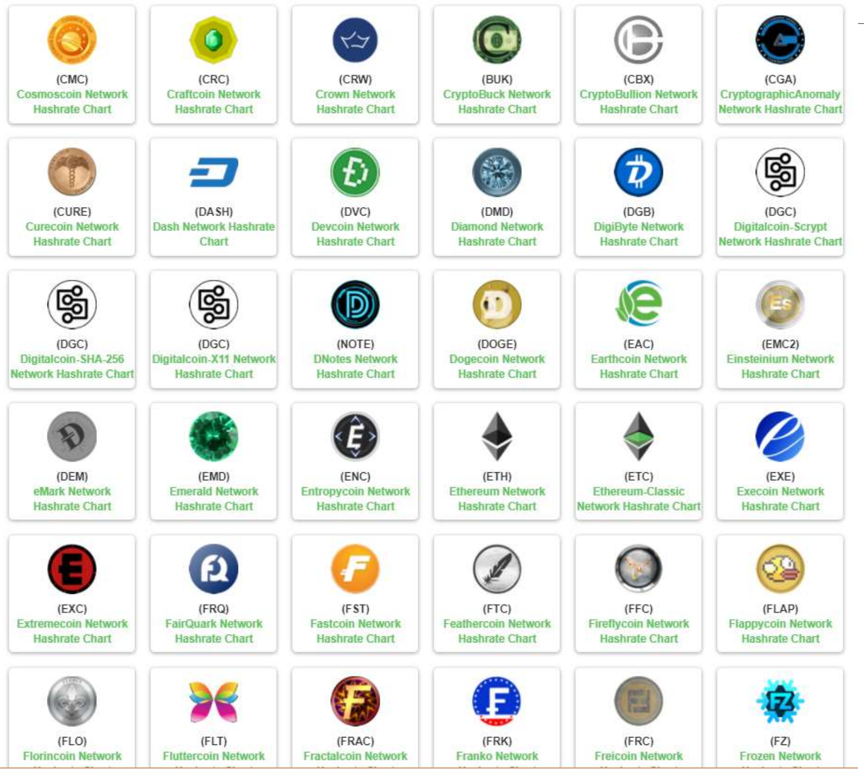
Slide credit: F. Vercauteren

> 180 are being mined

https://www.coinwarz.com/charts/network-hashrate-charts



(365) 365coin Network Hashrate Chart	(42) 42 Network Hashrate Chart	(ACOIN) Acoin Network Hashrate Chart	(ALF) Alphacoin Network Hashrate Chart	(ANC) Anoncoin Network Hashrate Chart	(ARI) Aricoin Network Hashrate Chart
(ARK) Arkhash Network Hashrate Chart	(ABY) ArtByte Network Hashrate Chart	(ASC) ASICcoin Network Hashrate Chart	(AUR) Auroracoin Network Hashrate Chart	(BNCR) BancorCoin Network Hashrate Chart	(BTA) BATA Network Hashrate Chart
(BCX) Battlecoin Network Hashrate Chart	(BQC) BBQCoin Network Hashrate Chart	(BVC) BeaverCoin Network Hashrate Chart	(BELA) Belacoin Network Hashrate Chart	(BEN) Benjamins Network Hashrate Chart	(BET) Betacoin Network Hashrate Chart
(BIG) BigBullion Network Hashrate Chart	(BTB) Bitbar Network Hashrate Chart	(BTC) Bitcoin Network Hashrate Chart	(BTG) Bitgem Network Hashrate Chart	(BTM) Bitmark Network Hashrate Chart	(BLC) Blakecoin Network Hashrate Chart
(CAP) Bottlecaps Network Hashrate Chart	(BCN) Bytecoin Network Hashrate Chart	(CAI) Caishen Network Hashrate Chart	(CANN) CannabisCoin Network Hashrate Chart	(CSC) Casinocoin Network Hashrate Chart	(CAT) Catcoin Network Hashrate Chart
(CNC) CHNCoin Network Hashrate Chart	(CIN) Cinnamoncoin Network Hashrate Chart	(CNOTE) CNotes Network Hashrate Chart	(CON) Coino Network Hashrate Chart	(CYC) ConspiracyCoin Network Hashrate Chart	(CTM) Continuumcoin Network Hashrate Chart



(CMC) Cosmoscoin Network Hashrate Chart	(CRC) Craftcoin Network Hashrate Chart	(CRW) Crown Network Hashrate Chart	(BUK) CryptoBuck Network Hashrate Chart	(CBX) CryptoBullion Network Hashrate Chart	(CGA) CryptographicAnomaly Network Hashrate Chart
(CURE) Curecoin Network Hashrate Chart	(DASH) Dash Network Hashrate Chart	(DVC) Devcoin Network Hashrate Chart	(DMD) Diamond Network Hashrate Chart	(DGB) DigiByte Network Hashrate Chart	(DGC) Digitalcoin-Scrypt Network Hashrate Chart
(DGC) Digitalcoin-SHA-256 Network Hashrate Chart	(DGC) Digitalcoin-X11 Network Hashrate Chart	(NOTE) DNotes Network Hashrate Chart	(DOGE) Dogecoin Network Hashrate Chart	(EAC) Earthcoin Network Hashrate Chart	(EMC2) Einsteinium Network Hashrate Chart
(DEM) eMark Network Hashrate Chart	(EMD) Emerald Network Hashrate Chart	(ENC) Entropycoin Network Hashrate Chart	(ETH) Ethereum Network Hashrate Chart	(ETC) Ethereum-Classic Network Hashrate Chart	(EXE) Execoin Network Hashrate Chart
(EXC) Extremecoin Network Hashrate Chart	(FRQ) FairQuark Network Hashrate Chart	(FST) Fastcoin Network Hashrate Chart	(FTC) Feathercoin Network Hashrate Chart	(FFC) Fireflycoin Network Hashrate Chart	(FLAP) Flappycoin Network Hashrate Chart
(FLO) Florincoin Network	(FLT) Fluttercoin Network	(FRAC) Fractalcoin Network	(FRK) Franko Network	(FRC) Freicoin Network	(FZ) Frozen Network

Ethereum (ETH)

https://www.ethereum.org/   https://etherscan.io/

White paper 2013, live July 2015

Smart contract (scripting) functionality: deterministic exchange mechanisms controlled by digital means that can carry out the direct transaction of value between untrusted agents

- E.g. self-contained fair casinos, currency swaps…

Decentralized Turing-complete virtual machine

Currency is called “ether” – internal transaction pricing with “gas” (anti-DDOS and spam)

Ethereum forks

- 2016: DAO hack led to ETC fork (Ethereum classic)
- Q4/2016: 2 additional forks

Quorum: permissioned ledger developed by Morgan-Stanley on top of Ethereum

Ethereum (ETH) (compared to Bitcoin)

block time of 12 s (600 s)

memory hard algorithm based on Keccak-256 – almost SHA-3 (SHA-256 on ASICs)

70 transactions per block (2000-2500)

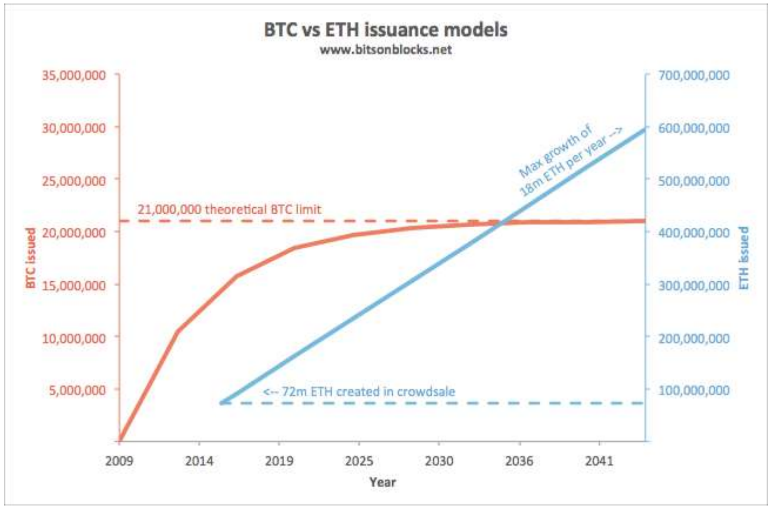
smart contracts (limited scripting)

more complex reward scheme, linear volume (decreasing to limit of 21 million BTC)

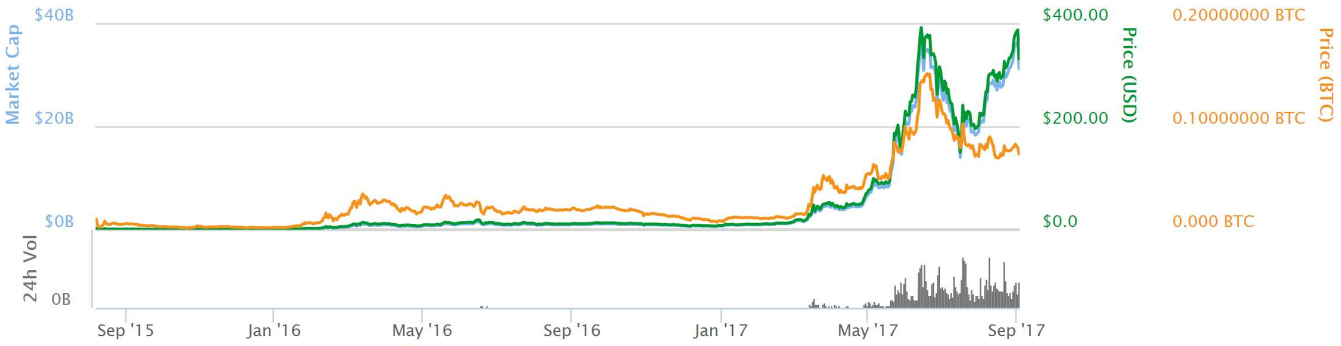
- reward 5 ETH per block (12.5 BTC per block but decreasing)
- uncles get reward so no pools (orphans get no reward)

proof-of-work may evolve to proof of stake (no plans)

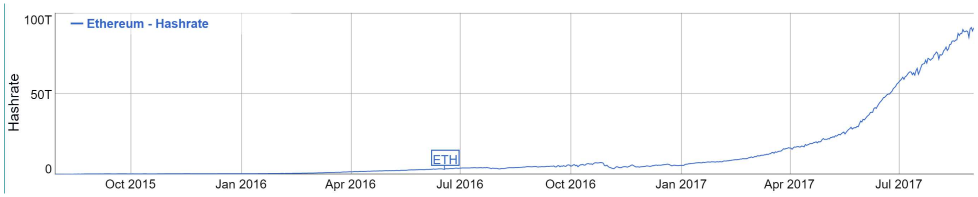
1 ETH = 10^{18} wei (1 BTC = 10^{8} satoshi)



Ethereum (ETH) graphs



1 ETH = 330$
91 THash/sec
Market cap 31 B$



Some observations on Bitcoin

Bitcoin community aspires to be mainstream but behaves as rebels

- this is not sustainable

Volatile

Paying and secure storage somewhat complex

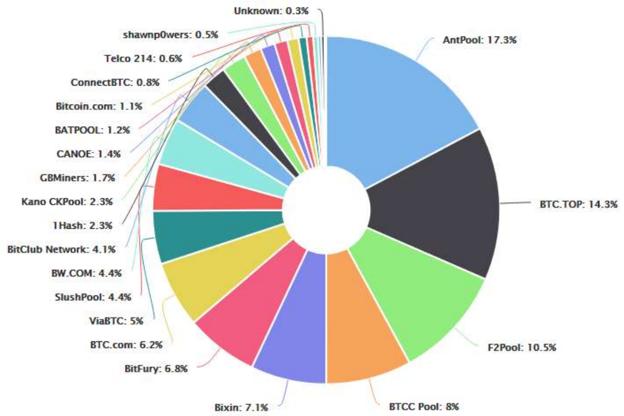
No peace of mind for users: if you are hacked, tough luck

Most miners are in China (70%)

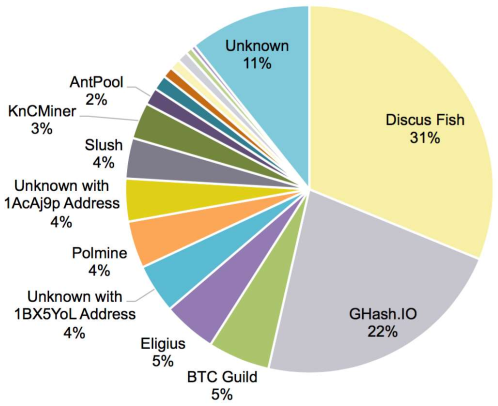
Incentives system complex

Not clear that the system will survive, but some ideas will for sure

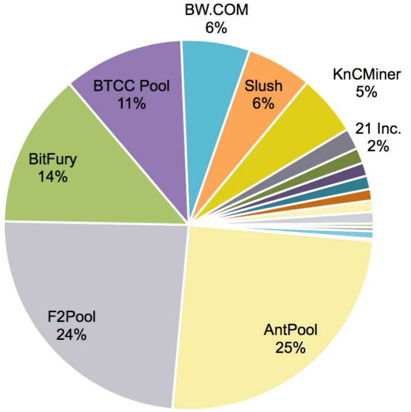
2017



2014



2015

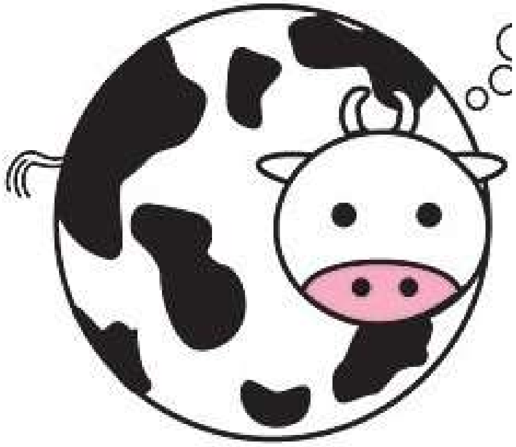


Open issues: Bitcoin

Is Bitcoin incentive compatible?

- Convergence
- Fairness: mining power fraction ~ revenue fraction
- Liveliness

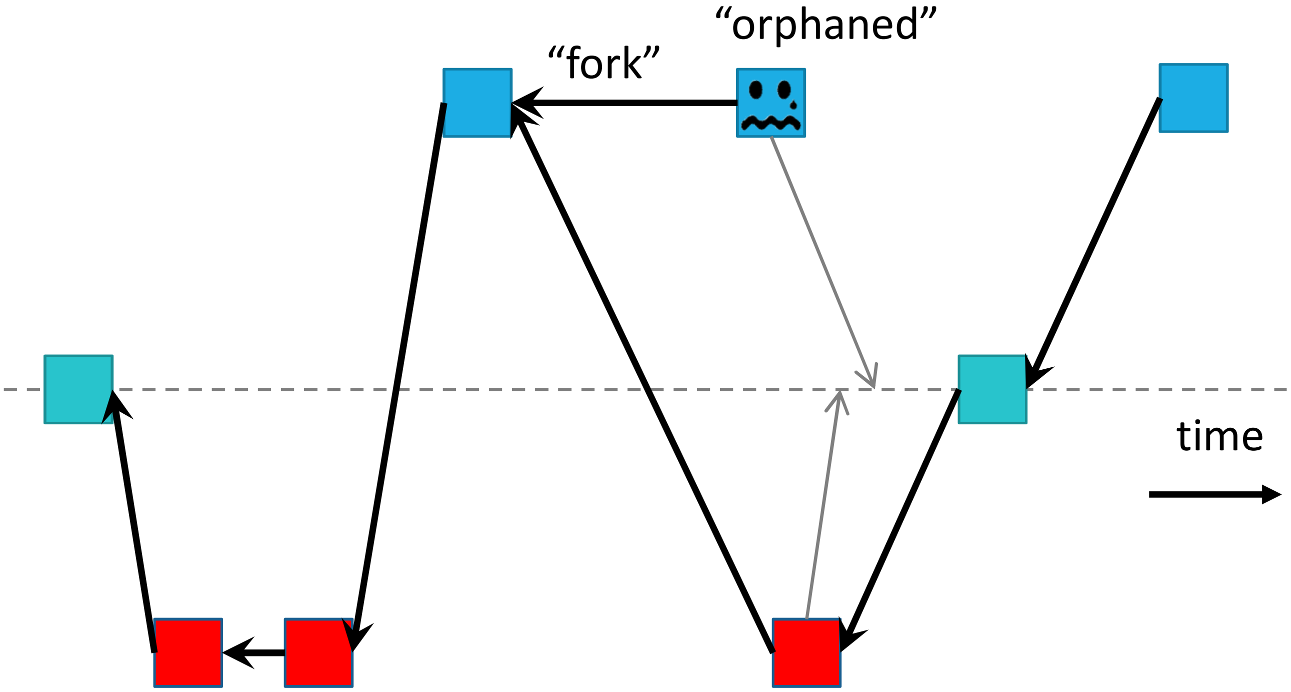
- Sybil attack: attacker controls many nodes in network, can refuse relaying or can favour her own blocks
- Selfish mining attack
- Bribery



Some proofs exist in simplified models e.g. [Garay-Kiayias-Leonardos, Crypto'17]

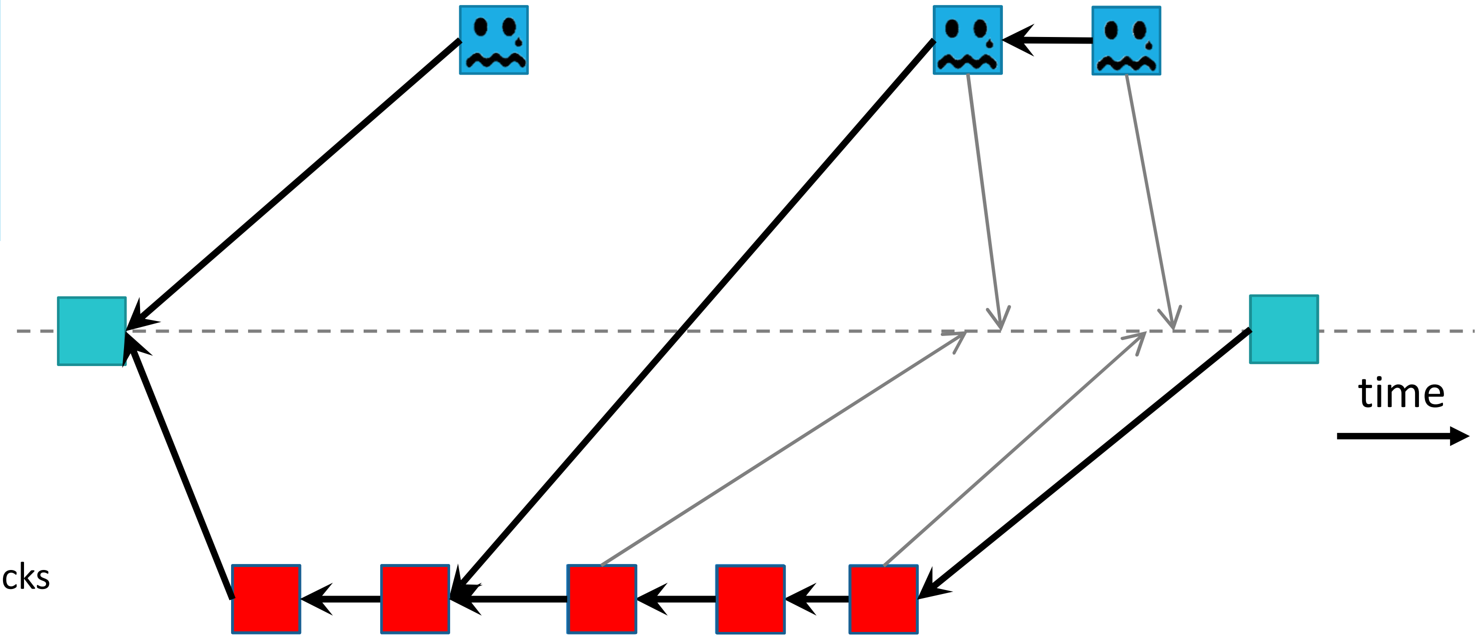
Bitcoin’s Fork Resolving Policy

- Longest chain wins
- Winner takes all



Selfish Mining [bitcointalk2010,Eyal-Sirer’13]

Can gain unfair advantage with 23.21% of the mining power



Selfish miner withholds blocks
(deviates from protocol)

Defenses against Selfish mining

Changing reward structure: no reward for competing blocks; if fork is included, get half of reward of orphaned block

- not backward compatible
- opens the door for other attacks

Coin flip to resolve a tie

- improvement but only if selfish miner has less than 23.21%
- does not work if miner is ahead

Incorporate time stamp issued by trusted third party

- modest improvement
- need trusted third party

Defenses against Selfish mining (2)

Decentralized

Incentive compatible

Backward compatible (avoid hard fork)

- block validity rules
- reward distribution policy: only rewards for blocks in main chain
- eventual consensus

Publish-or-Perish defense: uncles [Zhang-P'17]

Miner considers block **in time** if

- either: it extends its block chain by one
- or: same height as current last block but arrives within time τ with τ upper bound on block propagation time

A is an **uncle** of B if A is an "in time" block that competes with B's parent

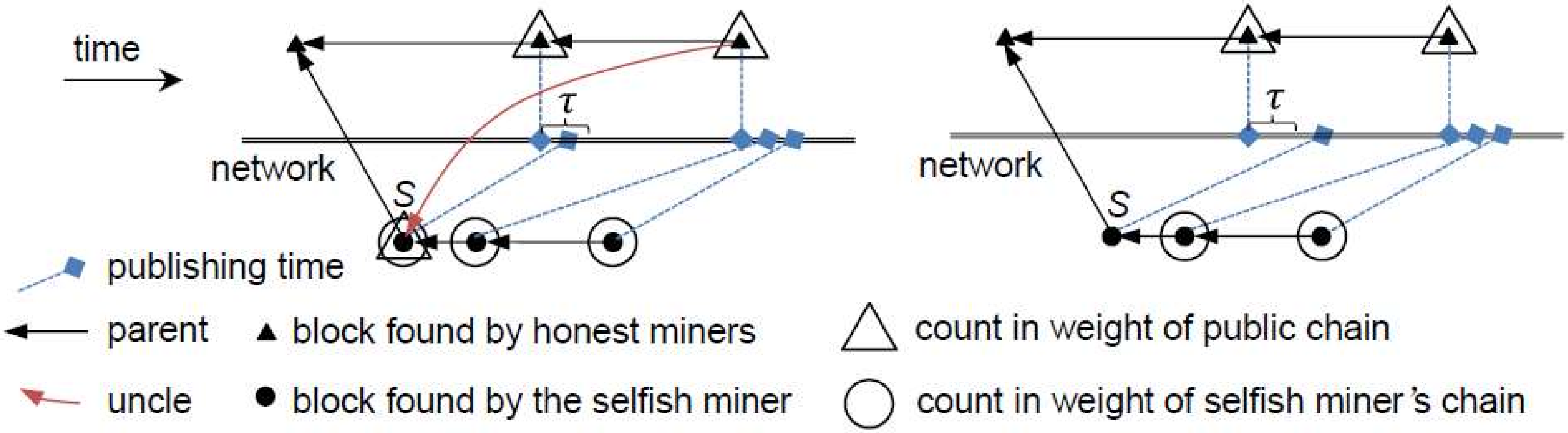
Assumption: attacker has zero propagation delay but it cannot delay blocks of others

- note: today about 50% of nodes receive block within 10 seconds

Publish-or-Perish defense

New Fork Resolution Protocol with parameter k (k=3). Chain wins if

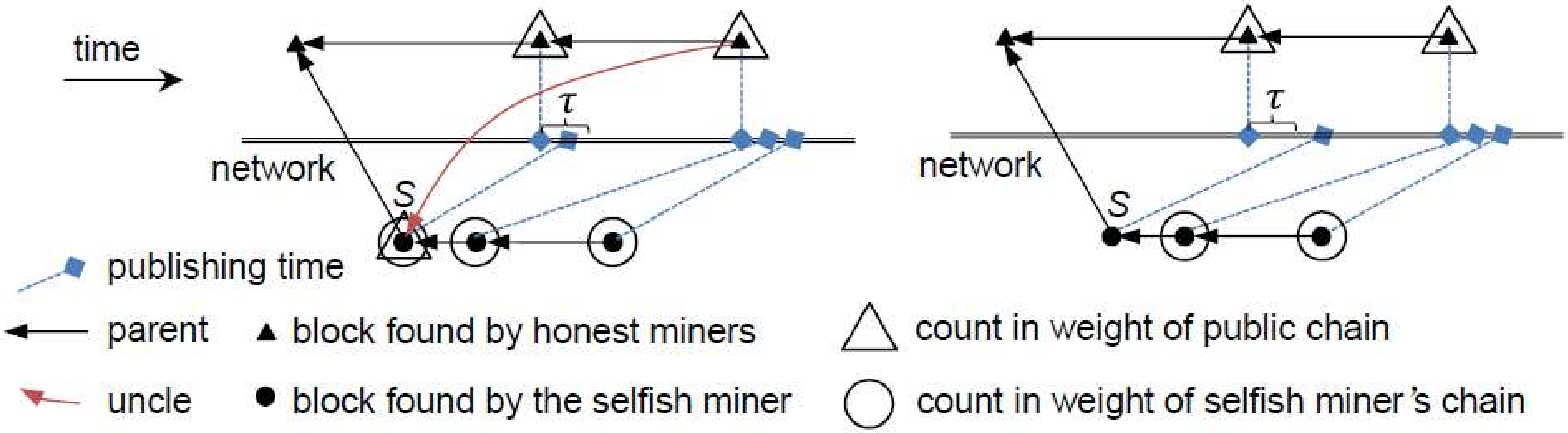
- it is ahead by k or more steps
- it has the largest weight, where weight is “in time blocks” + number of “in time uncles”
- if weights are tied: flip a coin


time
network
S
τ
network
S
τ
publishing time
parent
uncle
▲ block found by honest miners
● block found by the selfish miner
count in weight of public chain
count in weight of selfish miner's chain

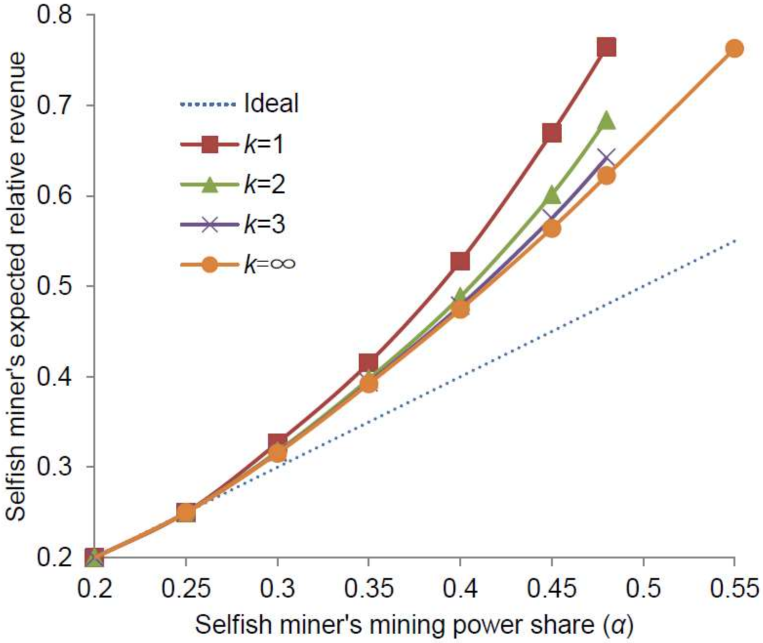
Publish-or-Perish defense

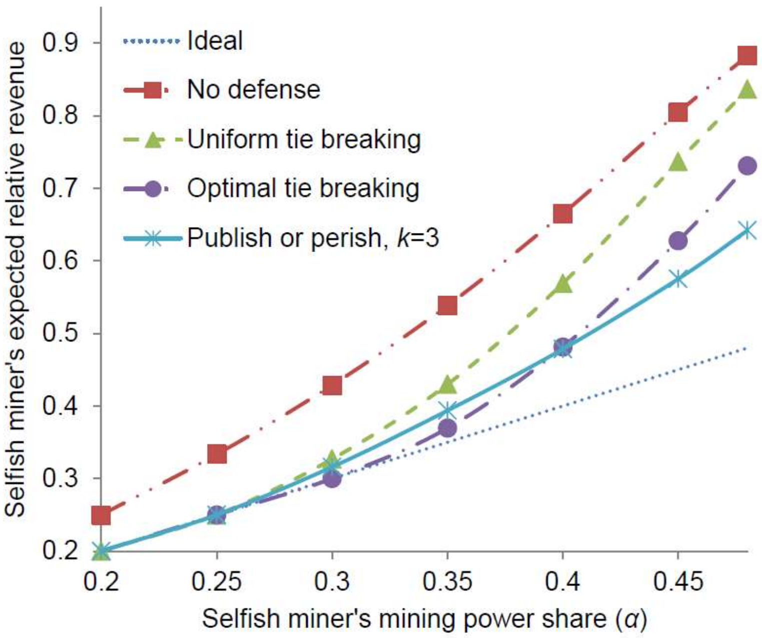
Dilemma for selfish miner

- if block S is published, it will be added to the weight of the honest chain as uncle
- if block S is hidden, it will be considered to be late and hence not add to the weight


time
network
S
τ
network
S
τ
publishing time
parent
uncle
▲ block found by honest miners
● block found by the selfish miner
count in weight of public chain
count in weight of selfish miner's chain

Publish-or-Perish results





Publish-or-Perish defense: limitations

Not 100% incentive compatible

Synchronous network

Broadcasts of blocks around cutoff time $t_i+\tau$

Double spending risk if some clients don’t adopt publish-or-perish

Natural forks

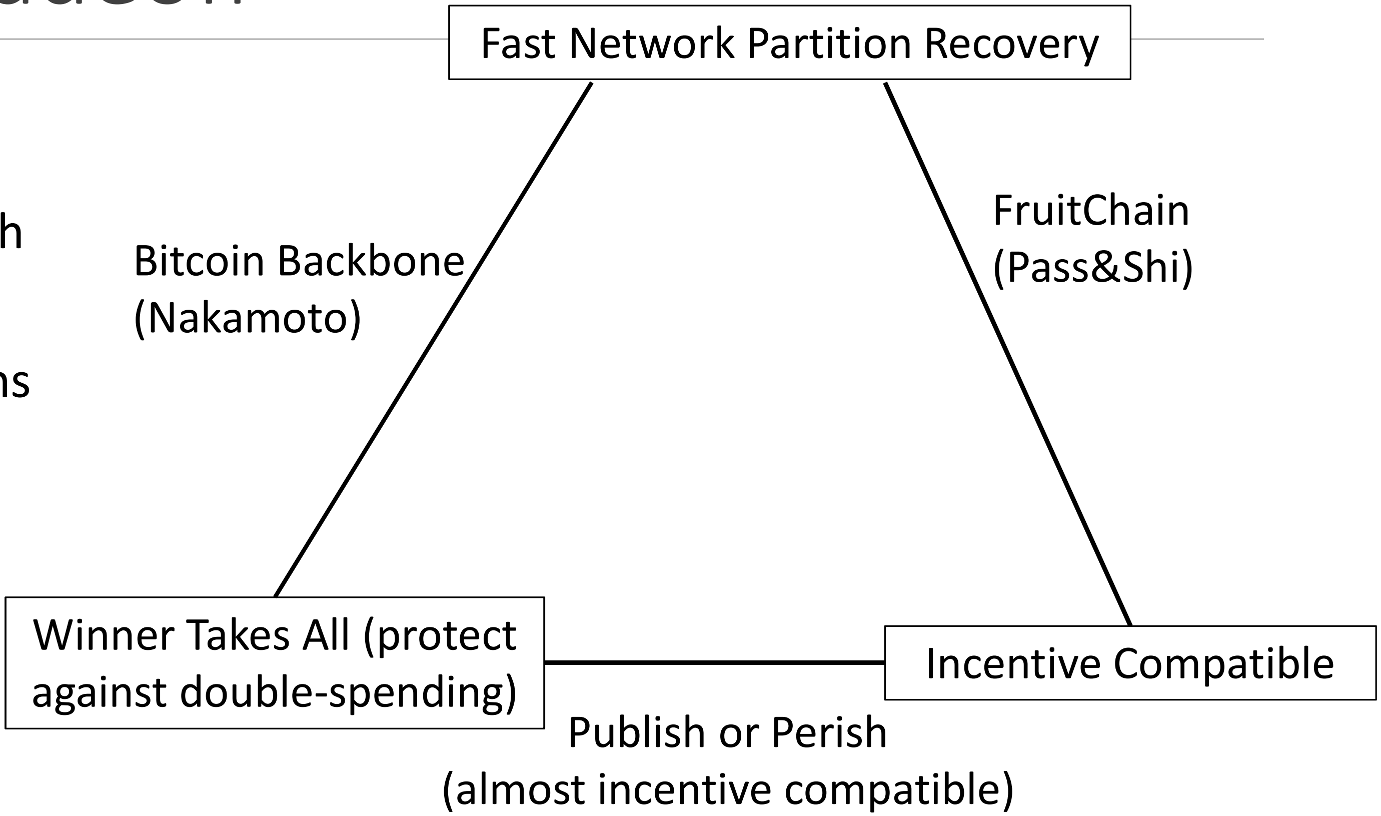
Transaction fees

Bribery

Complex tradeoff

Can’t distinguish between network partitioning and selfish mining

Winner takes all means that double spending incurs risks


Fast Network Partition Recovery
Bitcoin Backbone (Nakamoto)
FruitChain (Pass&Shi)
Winner Takes All (protect against double-spending)
Incentive Compatible
Publish or Perish (almost incentive compatible)

Recent history: hard fork on 1 August 2017

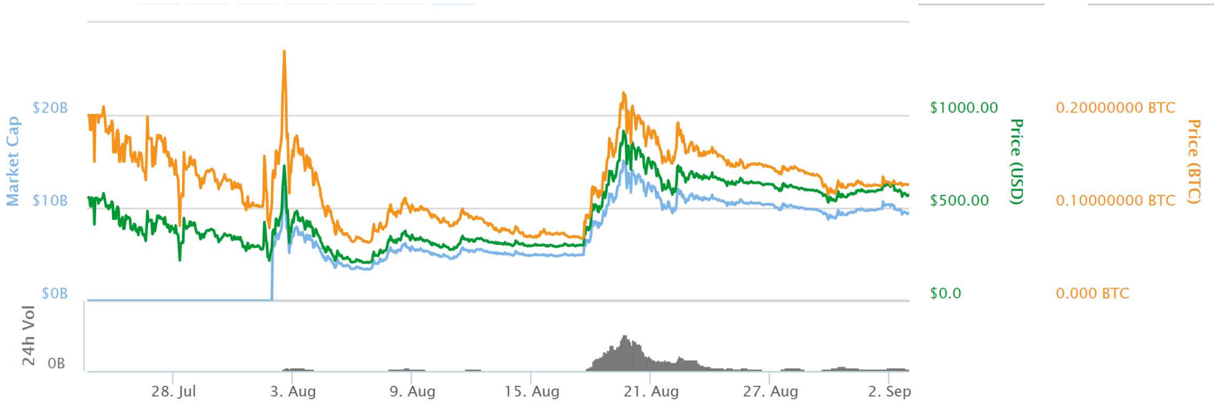
Debate on proposal to increase the block size from 1 Mbyte to 2 Mbyte (segwit2x – segregated witnesses)

Miners favor larger blocks: higher transaction volumes and more fees

Experts warn for instability due to more forks

No agreement on August 1: Bitcoin cash (Bitcoin ABC client) allows blocks of 8 Mbyte

Bitcoin cash market cap: 9.5B$



Segwith2x now plans a new hard fork in November 2017

Slide credit: George Danezis

BU (Bitcoin Unlimited): proposal to make block size variable

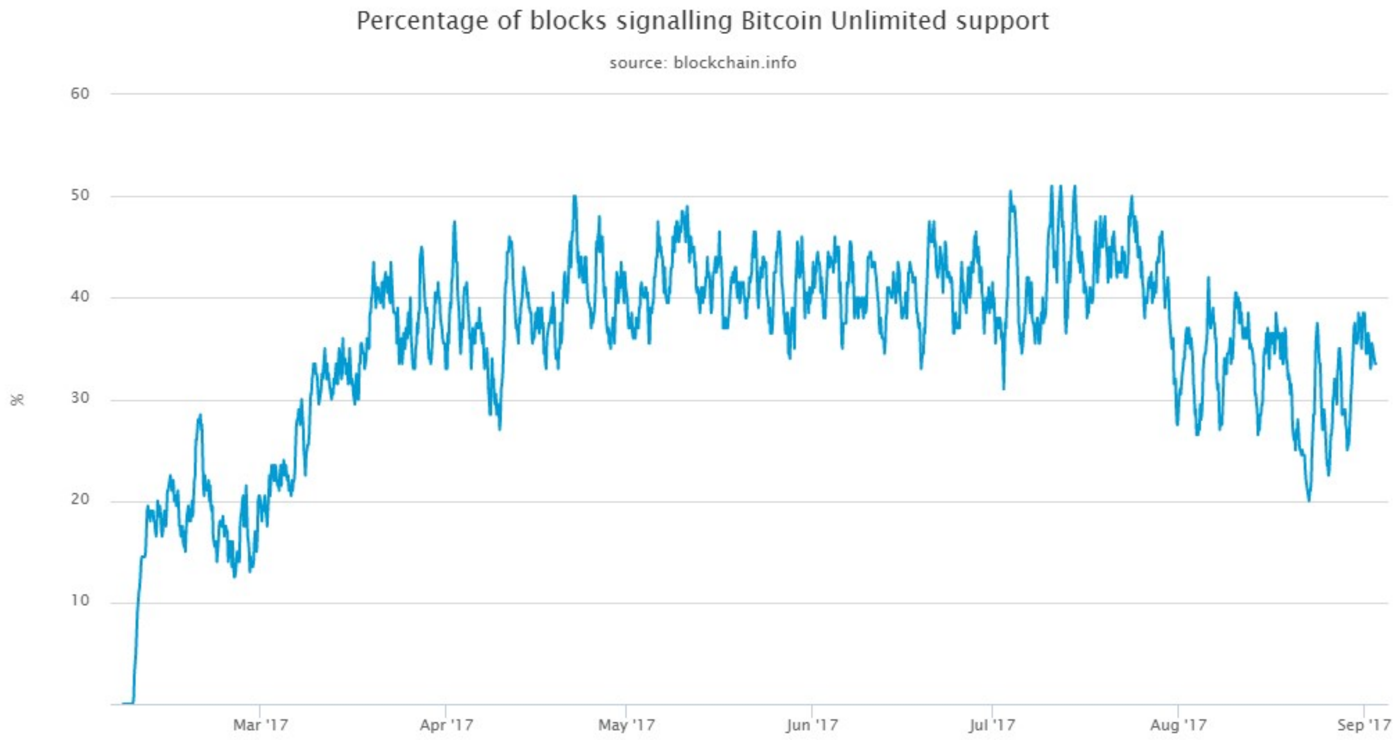
Recent analysis by [Zhang-P, CoNeXT '17]

Without BVC (= block validation consensus)

- BU is not incentive compatible, even if all miners follow the protocol
- Double spending becomes much more attractive, even with only 1% of mining power
- Not-for profit attacker can orphan many more blocks

When every miner has a maximal profitable block size, game theory shows that miners who can handle large blocks will form a coalition and crowd out the other miners

Miners “vote” on BU in block



Open issues: cryptocurrencies

Fully anonymous payments: ZeroCoin

Design of contracts (e.g. trading digital art)

Block chain technology for non-currency applications:

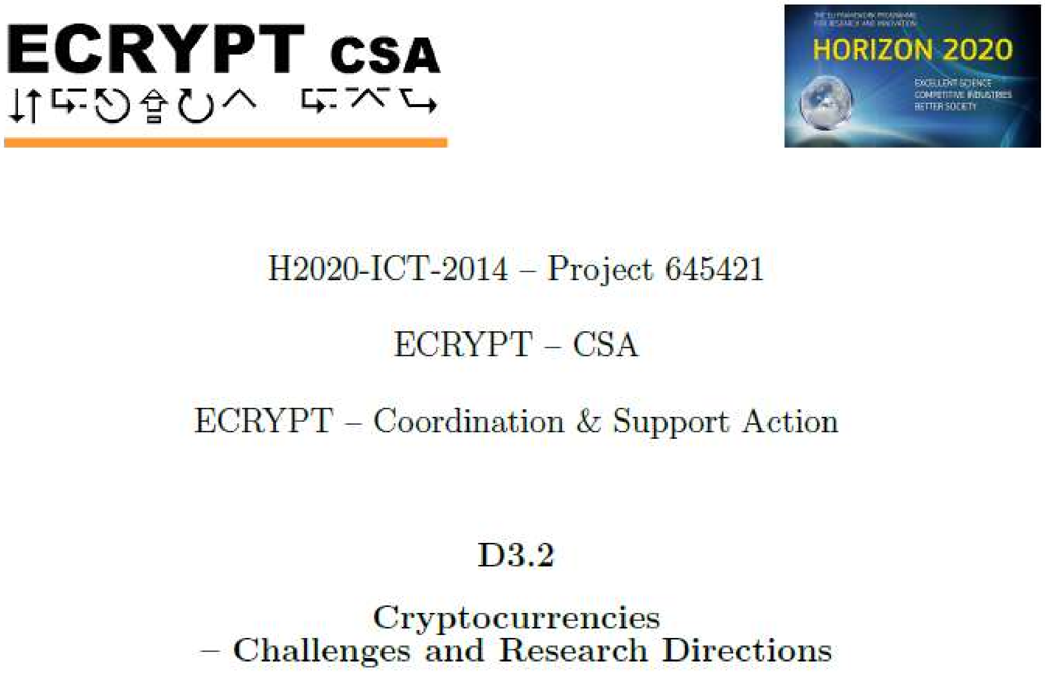
- typical applications: decentralized consensus required
- Namecoin: key-value registration and transfer platform, used for domain names etc…

Can we avoid the enormous computational cost? (proof of stake)

Is a zero-governance currency possible?

Bitcoin needs governance for “hard” upgrades

http://www.ecrypt.eu.org/csa/documents/D3.2-Cryptocurrencies.pdf



H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

D3.2

Cryptocurrencies
– Challenges and Research Directions

Pointers

http:www/ecrypt.eu.org

http://www.bitcoin.org

http://www.blockchain.com

http://www.vnbitcoin.org/bitcoincalculator.php

http://randomwalker.info/bitcoin/

http://www.coindesk.com/

Nathaniel Popper, Digital Gold, Harper, 2015

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcon and cryptocurrency technologies, Princeton University Press, 2016

A. Biryukov, D. Khovratovich, I. Pustogarov: Deanonymisation of Clients in Bitcoin P2P Network. ACM Conference on Computer and Communications Security 2014: 15-29

S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage: A fistful of bitcoins: characterizing payments among men with no names. Internet Measurement Conference 2013: 127-140

Financial Cryptography conference series

Bart Preneel, imec-COSIC KU Leuven

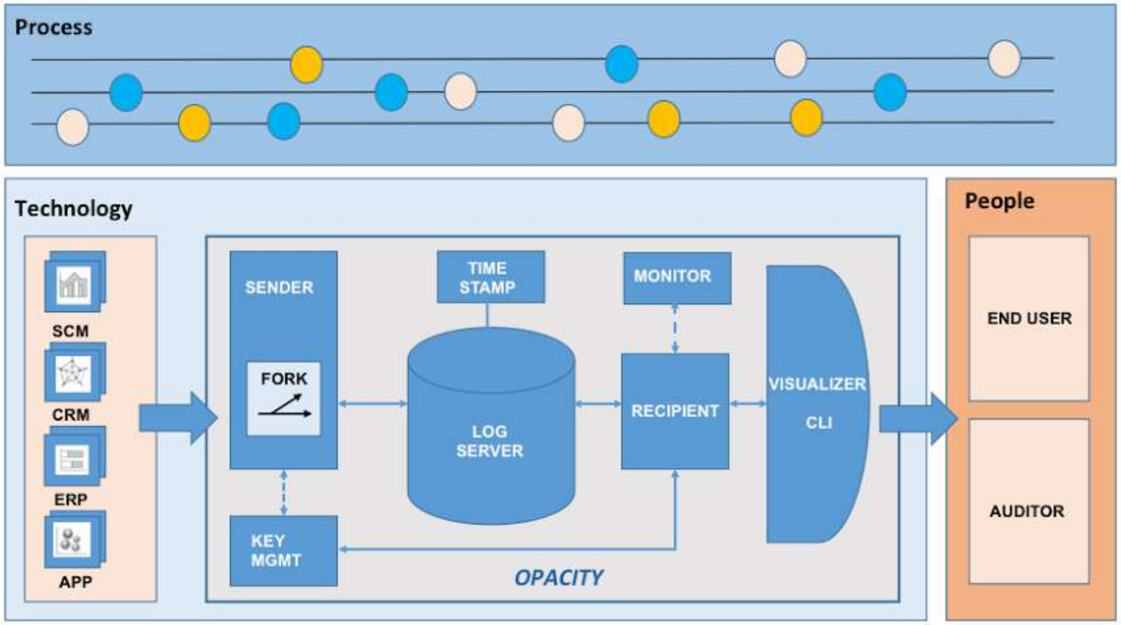
ADDRESS:	Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE:	homes.esat.kuleuven.be/~preneel/
EMAIL:	Bart.Preneel@esat.kuleuven.be
TWITTER:	@CosicBe
TELEPHONE:	+32 16 321148

ECRYPT CSA

http://www.ecrypt.eu.org

Distributed logging + Privacy

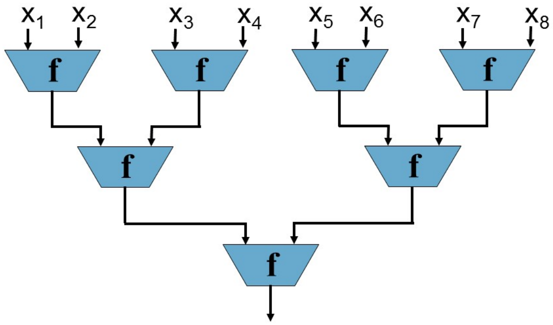
http://www.project-opacity.com/



Mining and Proof-Of-Work

Transactions in a block are hashed and assembled in a Merkle tree

- hash function used is double SHA-256, so SHA-256(SHA-256())



Header then consists of

- previous block header hash
- timestamp
- difficulty level
- Merkle tree root
- nonce

Mining: finding a nonce such that the double hash of the header results in a **hash value lower than the difficultly level**, e.g. a double hash value starting with loads of zeros.

- currently about 71 zeros are required

The first transaction in a block is a coinbase transaction

- transfers reward + all transaction fees to the miner

Slide credit: F. Vercauteren

Business

Financial world dislikes

- distributed control
- full transparency
- unclear governance (or anarchy)
- uncontrolled money supply

Restrict: write, verify or read (fully private block chain)

Distributed Ledger: a range of solutions

Public Blockchain

- No central point of control by individuals, corporations or governments
- Permissionless to participate
- Concensus based on "proof ow work"
- Examples:
  - *Bitcoin*
  - *Ethereum*

Consortium/Hybrid Blockchain

- Controlled by > 2 individuals, corporations or governments
- Permission on participation from consortium necessary
- Arbitrary consensus mechanism
- Readability of the blockchain can be public or restricted to the consortium
- Example: *RSCOIN (UC London)*

Full private Blockchain

- Controlled by one individual, corporation or government (no consensus needed)
- Permission on participation from owner necessary
- Readability of the blockchain can be public or restricted to one

Distributed Ledger

distributed database - only needed if

- multiple mutually distrustful writers
- no intermediate party that is trusted by all players
- interactions or dependencies between the transactions

Financial sector: disintermediation?

- 20% seriously investing
- 20% planning to invest
- 20% watching the space very closely

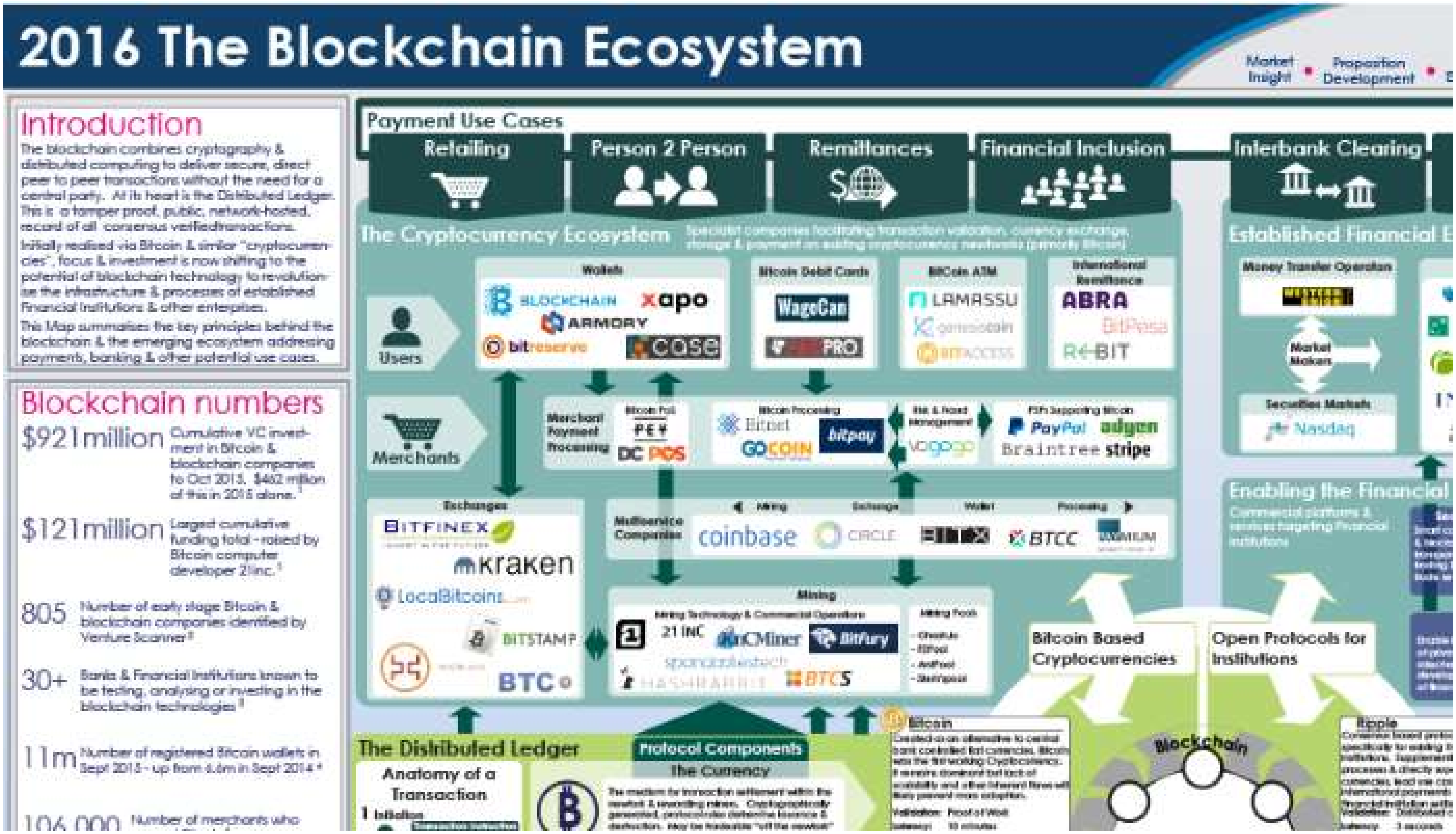
Aite Group: blockchain market could be worth as much as $400m in annual business by 2019

Distributed Ledger: open questions

Explore the continuum between fully open and fully restricted ledgers?

Develop a methodology to design restricted distributed ledgers as a function of the business requirements

Which advanced cryptographic and scripting techniques can be used in private or permissioned ledgers to improve privacy and to allow for complex transactions such as smart contracts?



2016 The Blockchain Ecosystem

Introduction

The blockchain combines cryptography & distributed computing to deliver secure, direct peer to peer transactions without the need for a central party. At its heart is the Distributed Ledger. This is a tamper proof, public, network-hosted, record of all consensus verifiedtransactions.

Initially realised via Bitcoin & similar "cryptocurrencies", focus & investment is now shifting to the potential of blockchain technology to revolutionise the infrastructure & processes of established Financial Institutions & other enterprises.

This Map summarises the key principles behind the blockchain & the emerging ecosystem addressing payments, banking & other potential use cases.

Blockchain numbers

$921million Cumulative VC investment in Bitcoin & blockchain companies to Oct 2015. $462 million of this in 2015 alone.[1]

$121million Largest cumulative funding total - raised by Bitcoin computer developer 21inc.[1]

805 Number of early stage Bitcoin & blockchain companies identified by Venture Scanner[2]

30+ Banks & Financial Institutions known to be testing, analysing or investing in the blockchain technologies[3]

11m Number of registered Bitcoin wallets in Sept 2015 - up from 4.6m in Sept 2014[4]

106,000 Number of merchants who

https://media.licdn.com