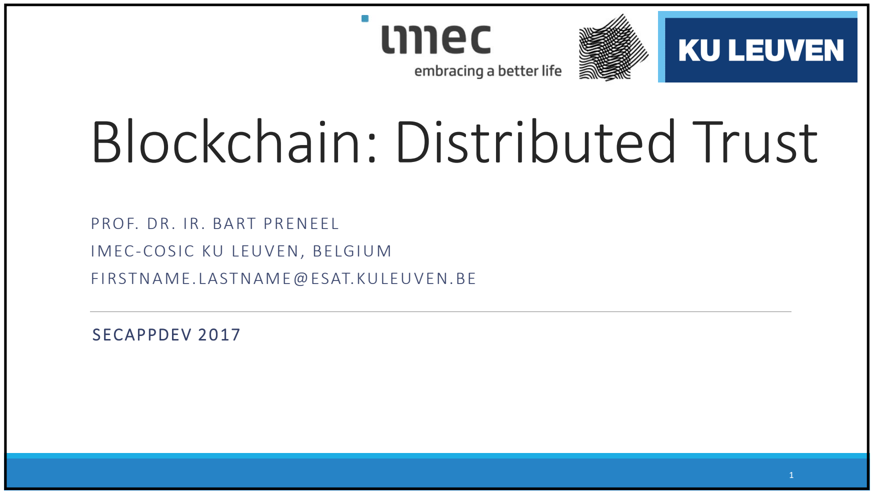


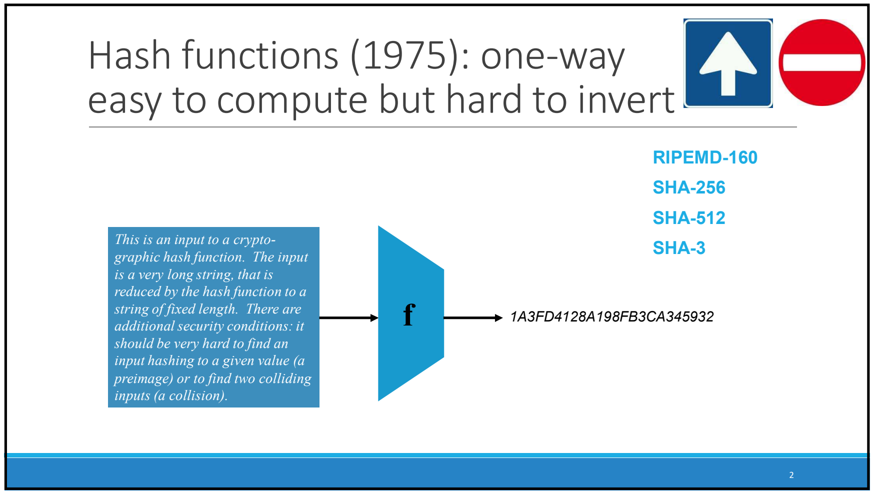
imec embracing a better life KU LEUVEN

Blockchain: Distributed Trust

PROF. DR. IR. BART PRENEEL
IMEC-COSIC KU LEUVEN, BELGIUM
FIRSTNAME.LASTNAME@ESAT.KULEUVEN.BE

SECAPPDEV 2017

1

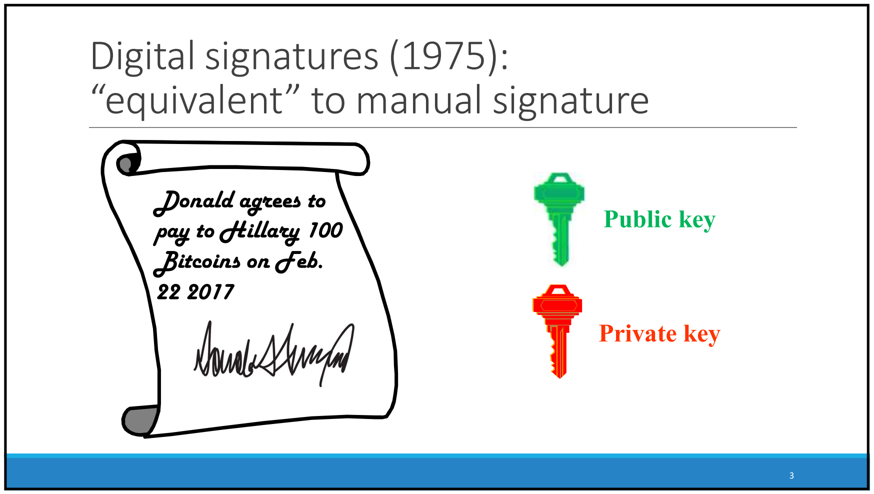


Hash functions (1975): one-way easy to compute but hard to invert

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).

2



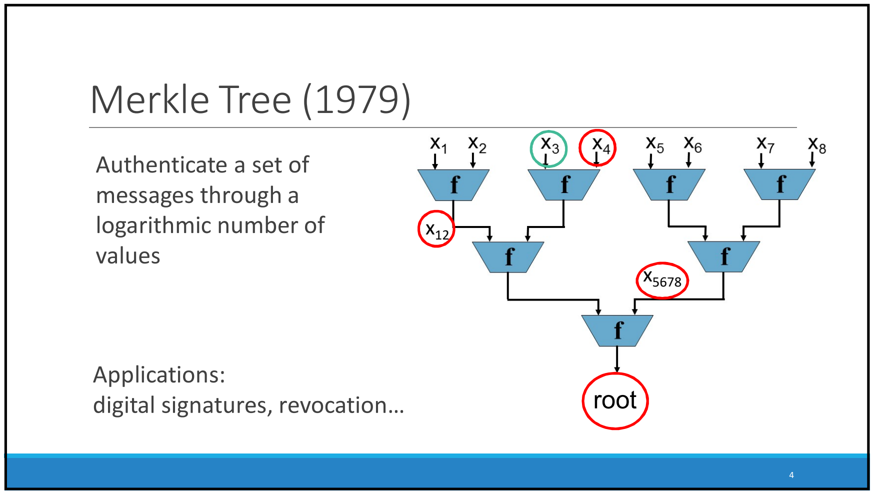
Digital signatures (1975): "equivalent" to manual signature

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

Public key

Private key

3



Merkle Tree (1979)

Authenticate a set of messages through a logarithmic number of values

x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
f
f
f
f
x_{12}
f
f
x_{5678}
f
root

Applications:
digital signatures, revocation…

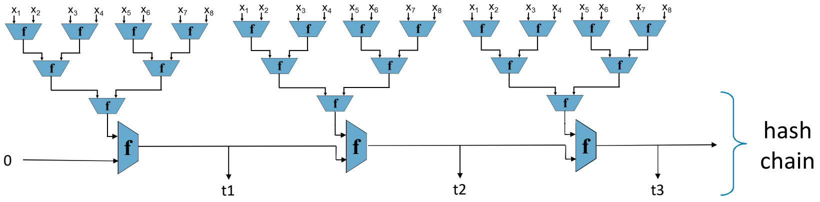
4

Timestamping (1990)

Collect documents and hash them with a Merkle tree

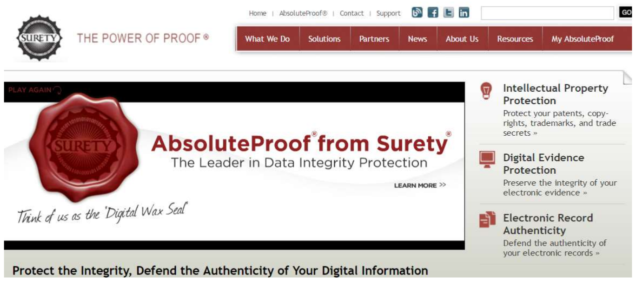
Chain these trees together with a hash chain

Publish intermediate values on a regular basis



Timestamping: Surety Technologies (°1994)

http://www.surety.com/


Home | AbsoluteProof® | Contact | Support

GO

THE POWER OF PROOF ®

What We Do | Solutions | Partners | News | About Us | Resources | My AbsoluteProof

PLAY AGAIN

AbsoluteProof® from Surety®

The Leader in Data Integrity Protection

LEARN MORE >>

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

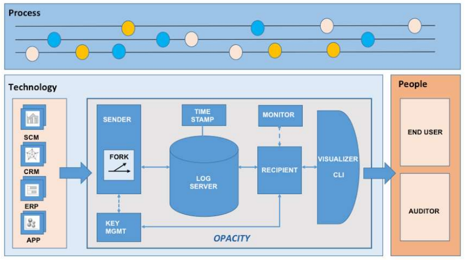
Defend the authenticity of your electronic records »

Protect the Integrity, Defend the Authenticity of Your Digital Information

Distributed logging + Privacy

OPACITY

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



Payment instructions and currencies

Payment Instruments: mechanism of how we transfer value

- cash
- letters of credit
- cheques
- bank transfer
- debit card

Each payment instrument has a cost

- actual monetary cost
- handling cost

Instruments have different security properties

- integrity/authenticity
- privacy: compare cash to bank or credit card payments

Slide credit: George Danezis

Cash

bearer instrument

off-line payments

low and medium value

privacy, coins not traceable

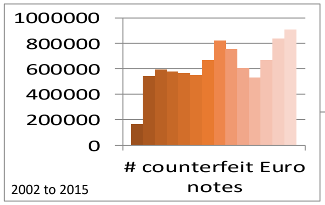
widely accepted

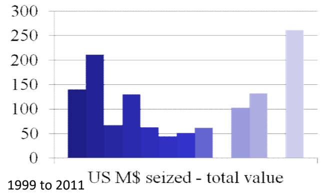
bank: risk of forgery, cost of transport

user: theft and loss, change, physical presence

government: money laundering

€/$/£ Counterfeiting





2014/5

> 17 billion notes in circulation

fraudulent: 838,000 or 1 in 20,000

+/- € 800 billion genuine in 2011

new 5/10/20 € bill in May'13/Sep'14/Nov'15

UK pound: 1 in 4170 counterfeit!

1995: $15.5 million (1% digitally produced)

2005: $61 million (45% digitally produced)

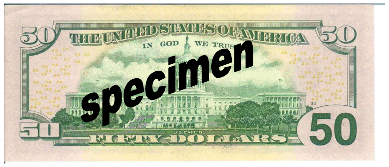
Fraudulent: 1 to 2 in 10000

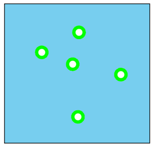
$1000 billion genuine in 2013

redesign: 1928, 1990, 1996-2003, 2003-2013

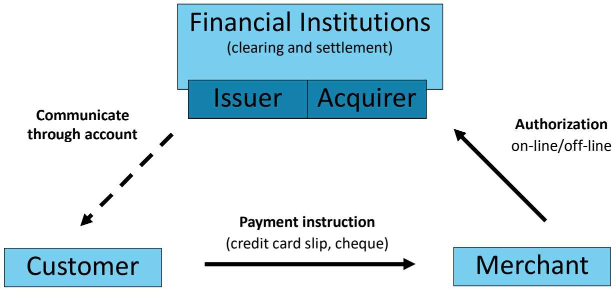
Common features e.g. $/€

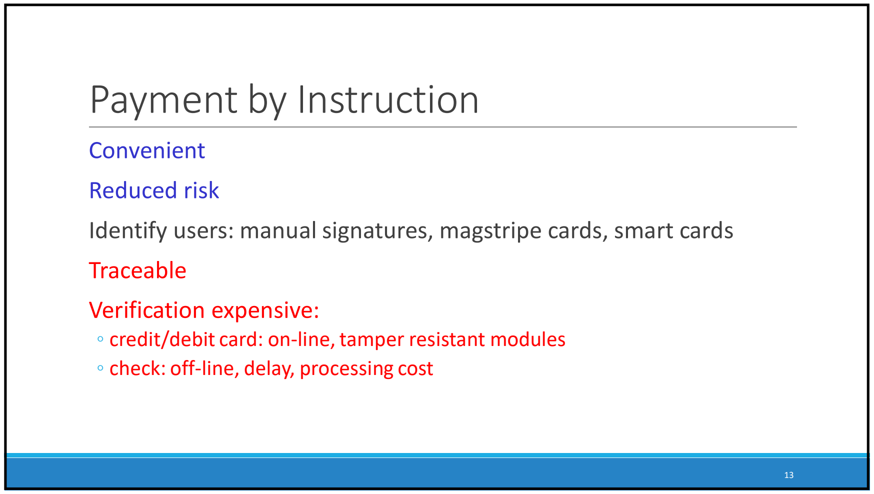
pattern detected by scanners and copiers





Payment by Instruction





Payment by Instruction

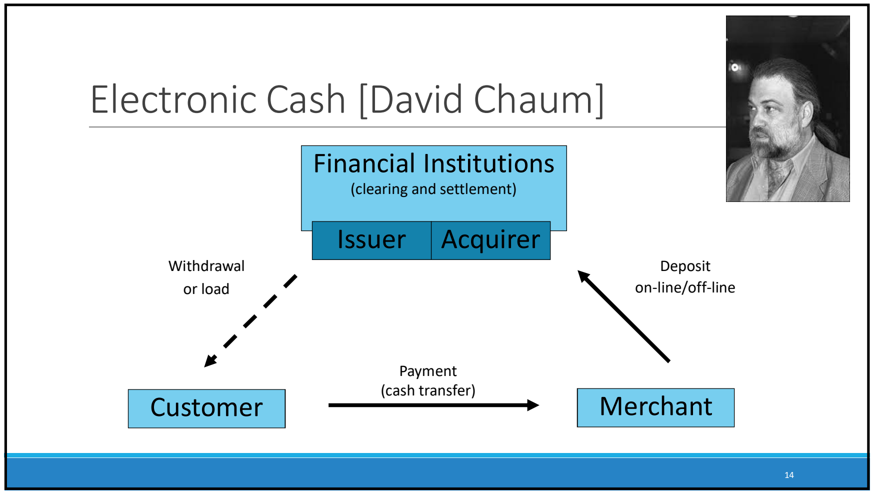
Convenient

Reduced risk

Identify users: manual signatures, magstripe cards, smart cards

Traceable

Verification expensive:
- credit/debit card: on-line, tamper resistant modules
- check: off-line, delay, processing cost



Electronic Cash [David Chaum]

Financial Institutions
(clearing and settlement)

Issuer | Acquirer

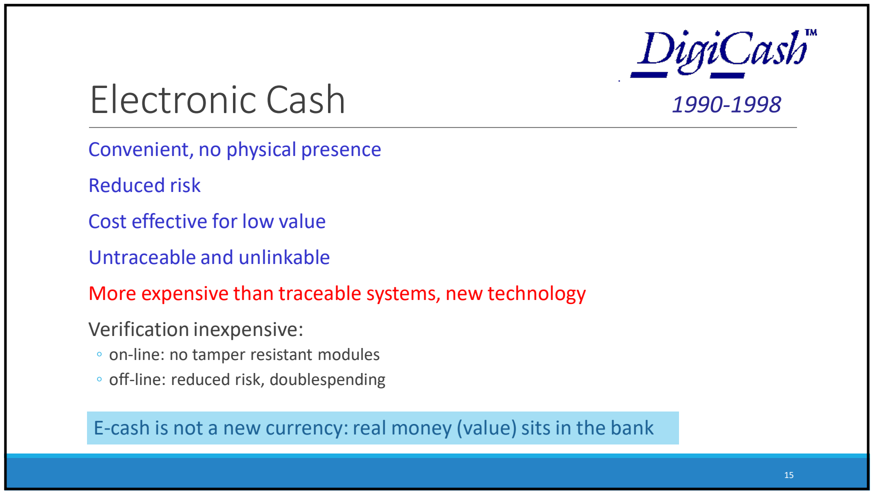
Withdrawal
or load

Deposit
on-line/off-line

Customer

Payment
(cash transfer)

Merchant



Electronic Cash

DigiCash™

1990-1998

Convenient, no physical presence

Reduced risk

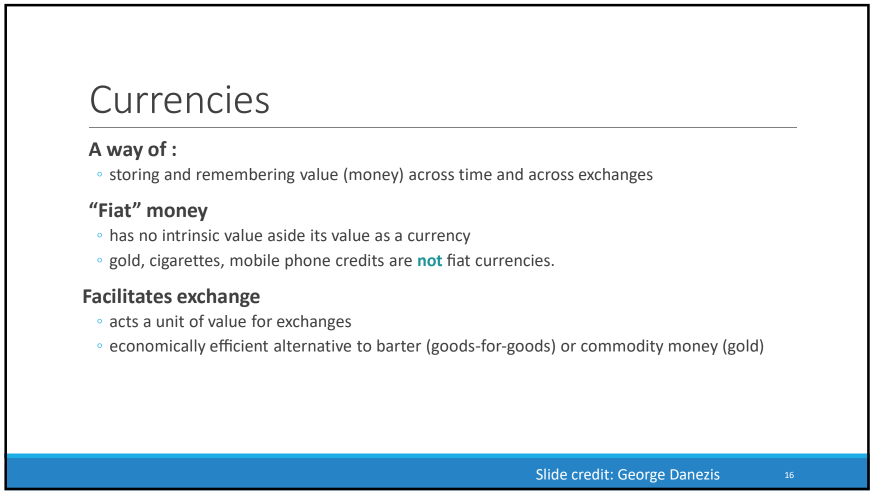
Cost effective for low value

Untraceable and unlinkable

More expensive than traceable systems, new technology

Verification inexpensive:
- on-line: no tamper resistant modules
- off-line: reduced risk, doublespending

E-cash is not a new currency: real money (value) sits in the bank



Currencies

A way of :
- storing and remembering value (money) across time and across exchanges

“Fiat” money
- has no intrinsic value aside its value as a currency
- gold, cigarettes, mobile phone credits are **not** fiat currencies.

Facilitates exchange
- acts a unit of value for exchanges
- economically efficient alternative to barter (goods-for-goods) or commodity money (gold)

Slide credit: George Danezis

Currencies = maintaining memory

"Envelope and contents from Susa, Iran, circa **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

Slide credit: George Danezis

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

Currencies

Money is like a commodity: it may go up, down or stay the same

- laws of supply and demand: deflation, inflation, …

Control of supply: who has control? Euro: European Central Bank (ECB)

Creation/deletion: who gets the new money? Who deletes the old money?

- give/delete money to those that already have money
- give/delete money to those that do work
- give/delete money at random, or equally to all

Memory: how do we make sure we will always remember who has how much money?

Initial allocation: If money is like a good: how do we bootstrap it? Who has it to start with? (does it matter?)

Bruce Champ, Scott Freeman, Joseph Haslag. **Modelling Monetary Economies**. (3rd Edition) Cambridge University Press.

Slide credit: George Danezis

Early examples: MojoNation (2000-2002) and BitTorrent

MojoNation

- Peer-to-peer file storage service paid with "Mojo"
- Employed Bram Cohen (BitTorrent) and Zooko
- Collapsed under hyperinflation

BitTorrent

- Simplification of MojoNation
- One can think of BitTorrent's tit-for-tat incentives as being **time-limited**, **file-specific**, and **non-transferrable** bilateral accounting
- No need for "full" currency

Slide credit: George Danezis

Early examples (2): e-gold (1996-2008)

1 million user accounts by 2002
centralized ledger of transactions
currency backed by real commodity, gold
network of international e-gold resellers

Becomes a crime magnet: difficult to identify customers yet easy to transfer internationally

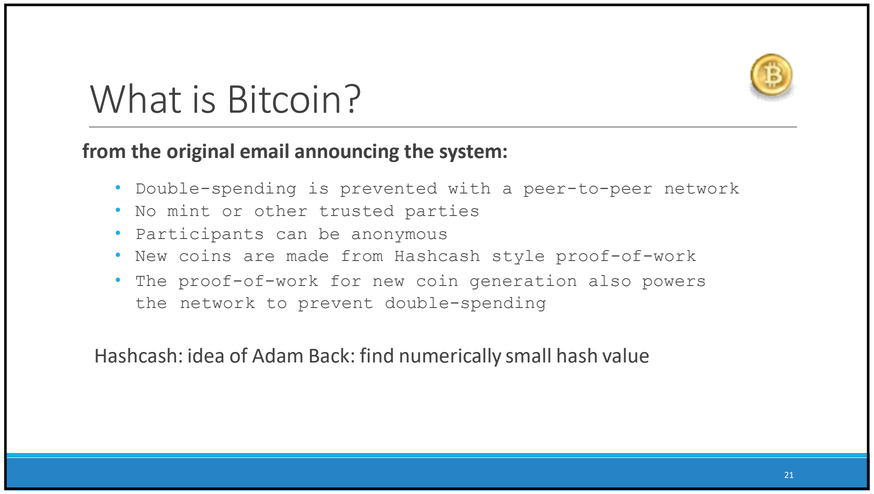
- US Patriot Act (2001) requires money transmitters to be regulated
- In **2008** directors face charges of money laundering and operating without a license. They are found guilty and get away with fines, and suspended sentence.

Asserts liquidated: $90M in gold (more than the central banks of bottom 1/3 countries)

- California (2010) and other states: all digital value transfer systems are money transmitters

Risk of centralized system out of control

Slide credit: George Danezis

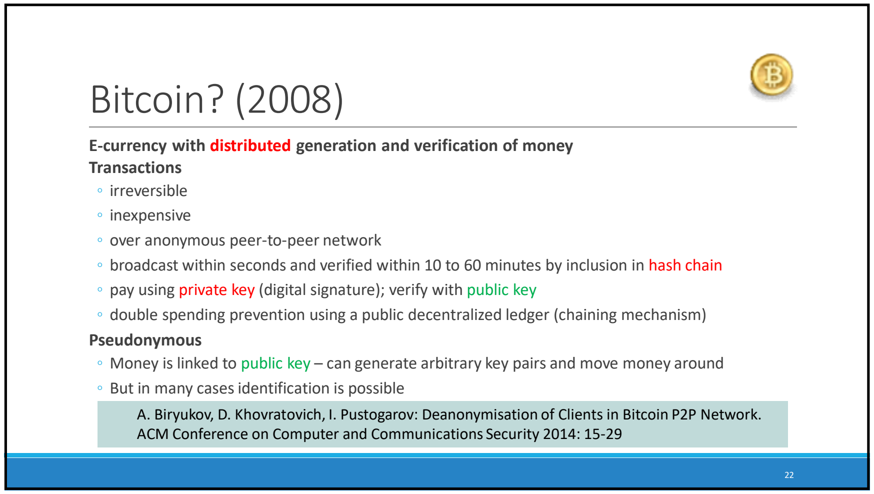


What is Bitcoin?

from the original email announcing the system:

```
• Double-spending is prevented with a peer-to-peer network
• No mint or other trusted parties
• Participants can be anonymous
• New coins are made from Hashcash style proof-of-work
• The proof-of-work for new coin generation also powers
  the network to prevent double-spending
```

Hashcash: idea of Adam Back: find numerically small hash value



Bitcoin? (2008)

E-currency with distributed generation and verification of money

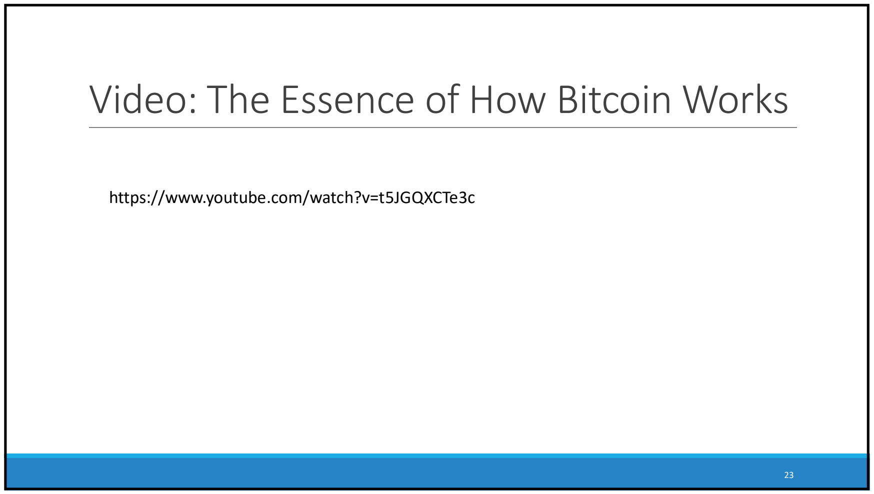
Transactions

- 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

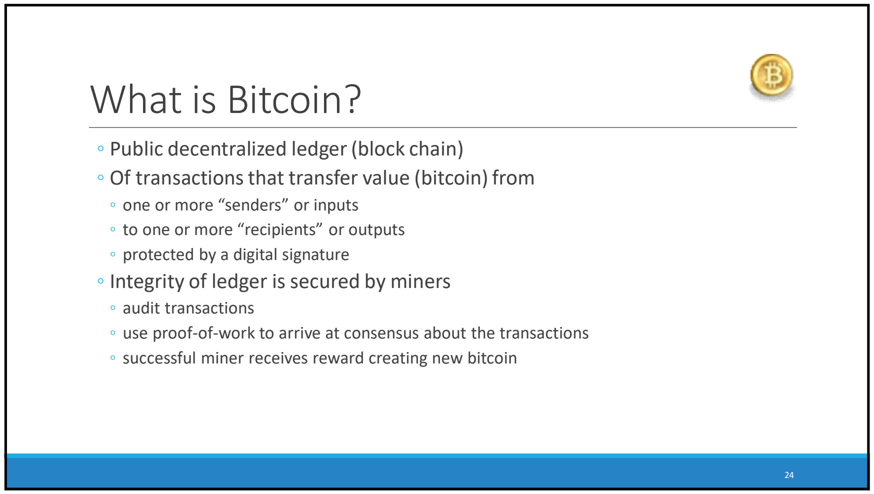
- Money is linked to public key – can generate arbitrary key pairs and move money around
- But in many cases identification is possible

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



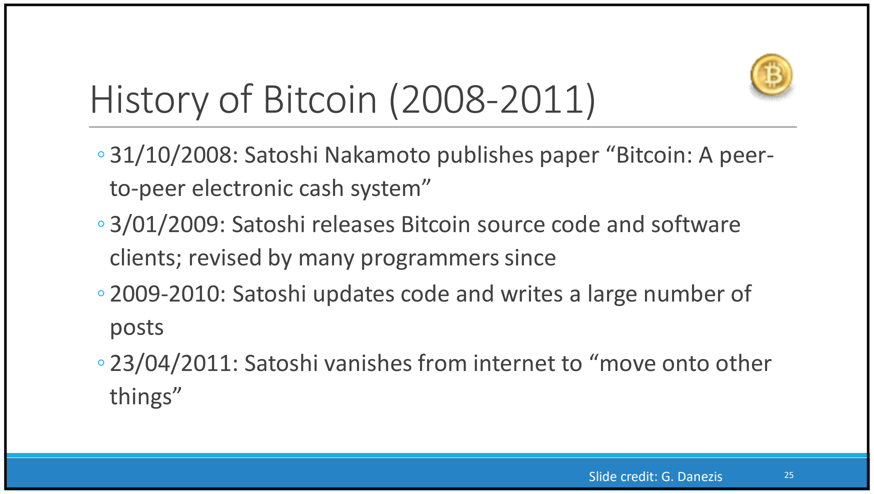
Video: The Essence of How Bitcoin Works

https://www.youtube.com/watch?v=t5JGQXCTe3c



What is Bitcoin?

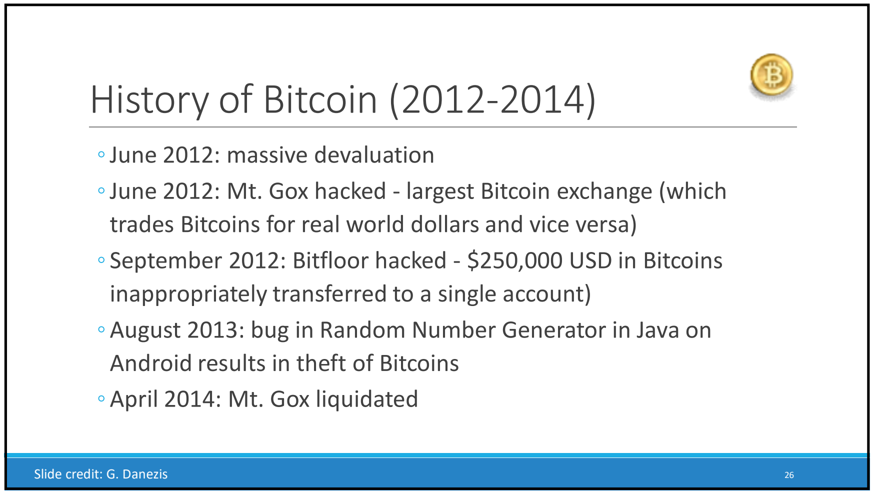
- Public decentralized ledger (block chain)
- Of transactions that transfer value (bitcoin) from
  - one or more “senders” or inputs
  - to one or more “recipients” or outputs
  - protected by a digital signature
- Integrity of ledger is secured by miners
  - audit transactions
  - use proof-of-work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



History of Bitcoin (2008-2011)

- 31/10/2008: Satoshi Nakamoto publishes paper “Bitcoin: A peer-to-peer electronic cash system”
- 3/01/2009: Satoshi releases Bitcoin source code and software clients; revised by many programmers since
- 2009-2010: Satoshi updates code and writes a large number of posts
- 23/04/2011: Satoshi vanishes from internet to “move onto other things”

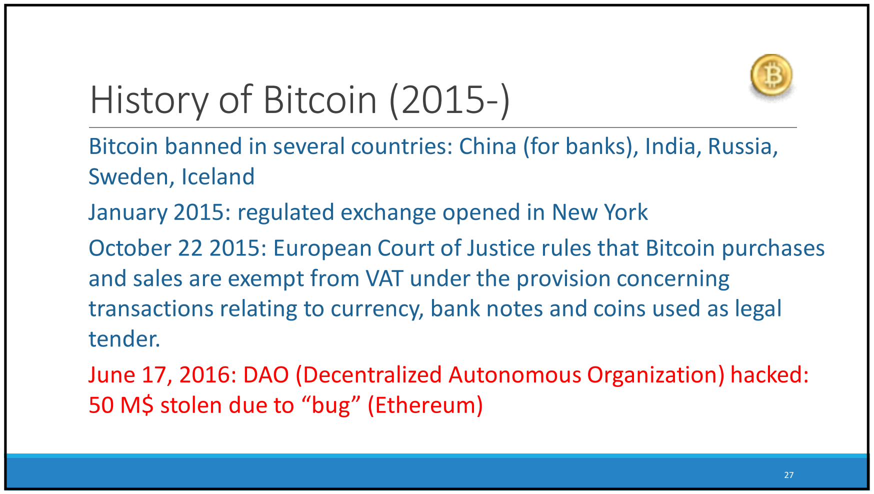
Slide credit: G. Danezis



History of Bitcoin (2012-2014)

- June 2012: massive devaluation
- June 2012: Mt. Gox hacked - largest Bitcoin exchange (which trades Bitcoins for real world dollars and vice versa)
- September 2012: Bitfloor hacked - $250,000 USD in Bitcoins inappropriately transferred to a single account)
- August 2013: bug in Random Number Generator in Java on Android results in theft of Bitcoins
- April 2014: Mt. Gox liquidated

Slide credit: G. Danezis



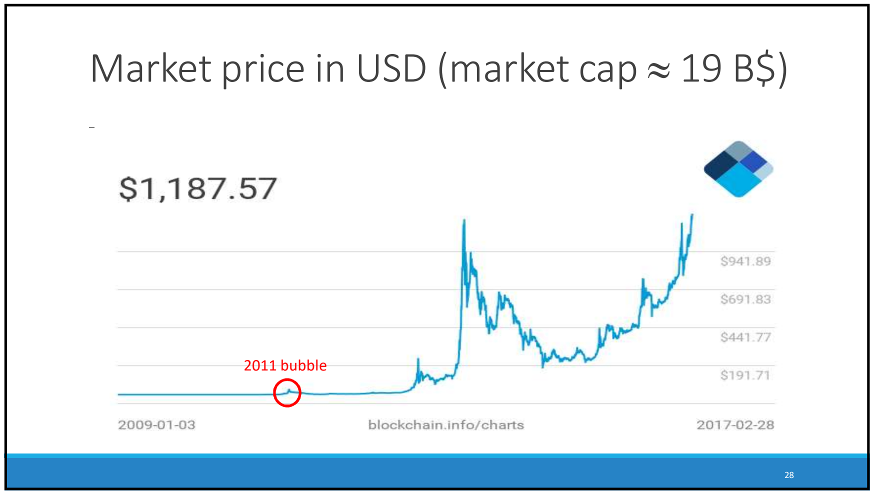
History of Bitcoin (2015-)

Bitcoin banned in several countries: China (for banks), India, Russia, Sweden, Iceland

January 2015: regulated exchange opened in New York

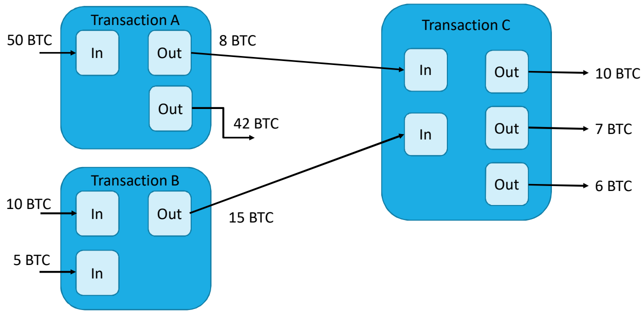
October 22 2015: European Court of Justice rules that Bitcoin purchases and sales are exempt from VAT under the provision concerning transactions relating to currency, bank notes and coins used as legal tender.

June 17, 2016: DAO (Decentralized Autonomous Organization) hacked: 50 M$ stolen due to “bug” (Ethereum)



Market price in USD (market cap ≈ 19 B$)

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



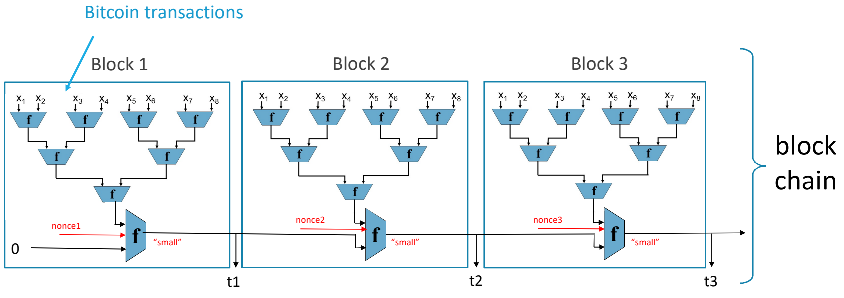
Transaction A
50 BTC
In
Out
8 BTC
Out
42 BTC

Transaction B
10 BTC
In
5 BTC
In
Out
15 BTC

Transaction C
In
In
Out
10 BTC
Out
7 BTC
Out
6 BTC

Slide credit: F. Vercauteren

Block Chain: a public decentralized ledger



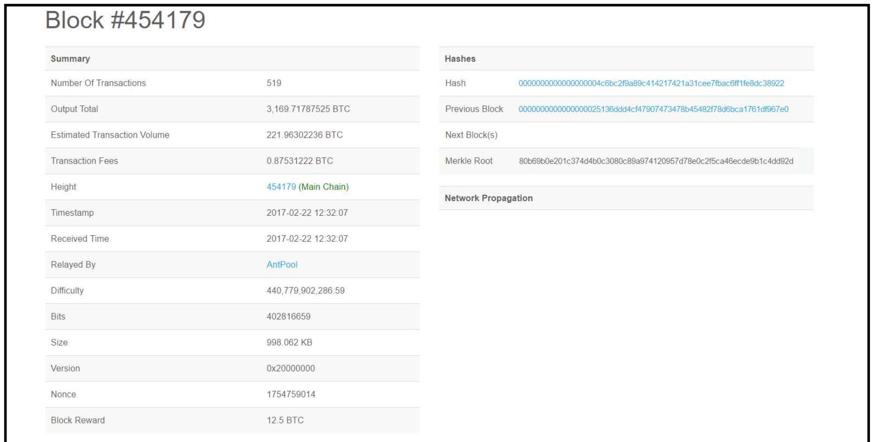
Bitcoin transactions

Block 1
Block 2
Block 3

block chain

Also include in every block timestamp and difficulty level of puzzle

Block #454179

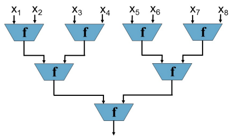


Summary	
Number Of Transactions	519
Output Total	3,169.71787525 BTC
Estimated Transaction Volume	221.96302236 BTC
Transaction Fees	0.87531222 BTC
Height	454179 (Main Chain)
Timestamp	2017-02-22 12:32:07
Received Time	2017-02-22 12:32:07
Relayed By	AntPool
Difficulty	440,779,902,286.59
Bits	402816659
Size	998.062 KB
Version	0x20000000
Nonce	1754759014
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000004c6bc2f9a89c414217421a31cee7fbac6ff1fe8dc38922
Previous Block	00000000000000000025136ddd4cf47907473478b45482f78d6bca1761df967e0
Next Block(s)	
Merkle Root	80b69b0e201c374d4b0c3080c89a974120957d78e0c2f5ca46ecde9b1c4dd92d

Network Propagation

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())

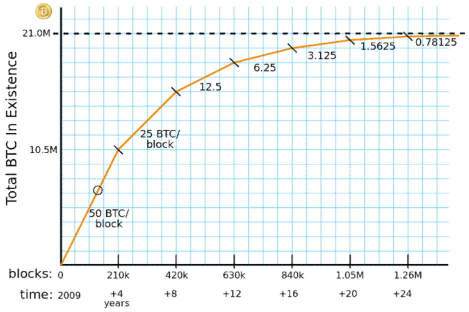
Header then consists of
- previous block header hash
- timestamp
- difficulty level
- Merkle tree root
- nonce

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

Mining Rewards: coinbase + fees



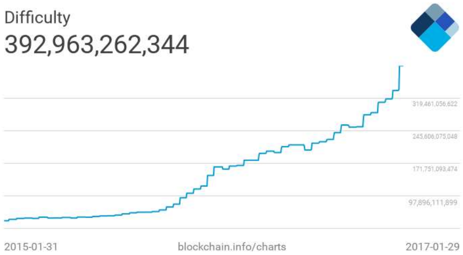
Total number of Bitcoins is limited to 21 million, each divided in 8 decimal places leading to 21×10^{14} units

Figure by Chris Pacia

Mining Difficulty Level

Target: mining 1 block should take roughly 10 minutes

mining computing power changes over time; update level every 2016 blocks



Mining Hash Rate of Bitcoin Network

1 EH/s = 1 ExaHash per second = 10^{18} hash/second = 2^{60} hash/second

Kilo

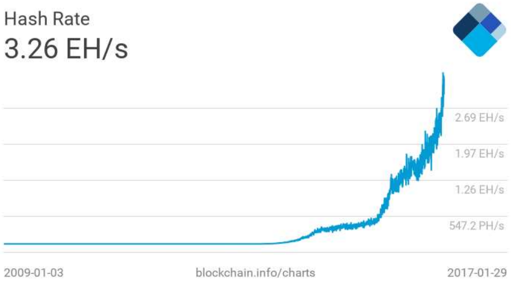
Mega

Giga

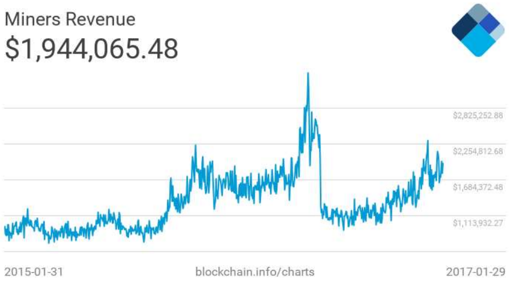
Tera

Peta

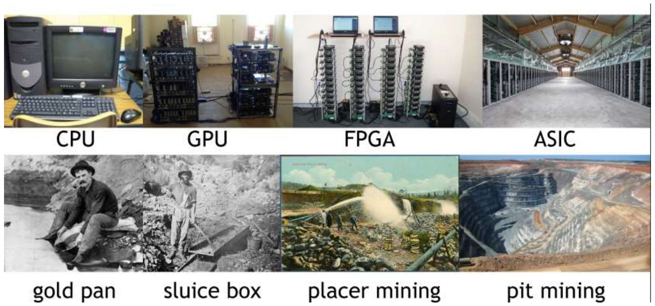
Exa



Miners Revenue (per day)

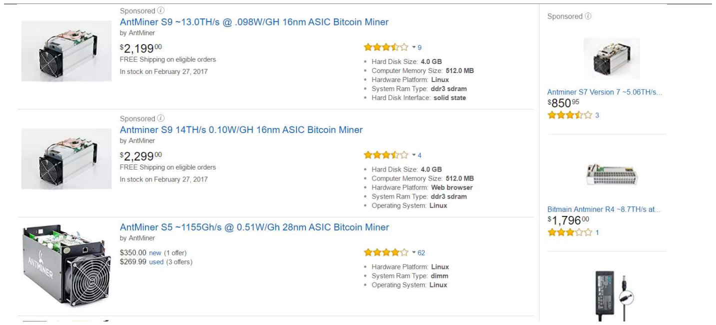


Mining has become industrial



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**

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**

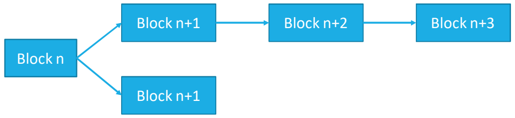
Sponsored ⓘ

Antminer S7 Version 7 ~5.06TH/s...
$850.95
★★★½☆ 3

Bitmain Antminer R4 ~8.7TH/s at...
$1,796.00
★★★☆☆ 1

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

Bitcoin Crypto

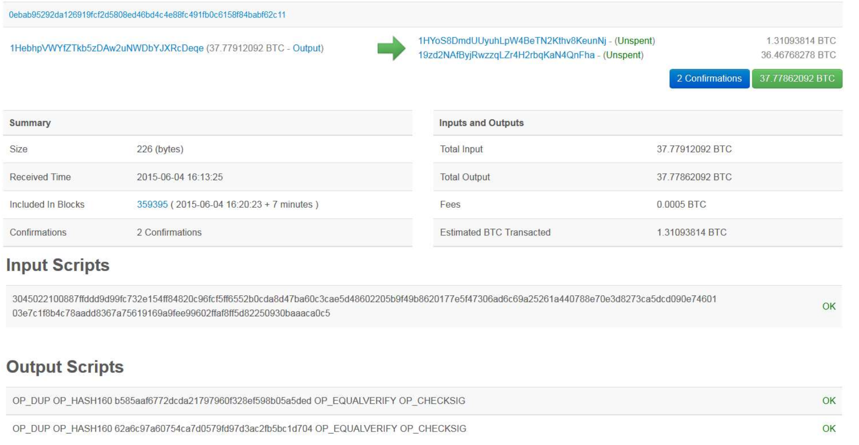
Hash functions:

- 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

2 Confirmations 37.77862092 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
```

Bitcoin Address (P2PKH)

The simplest form of Bitcoin address is Pay-to-Public-Key-Hash (P2PKH)

- Public key is point Q = (xQ, yQ) on the elliptic curve E
- Can be represented as:
  - Uncompressed form 04 || xQ || yQ
  - Compressed form 02 || xQ if yQ is even or 03 || xQ if yQ is odd
- Bitcoin address is derived as RIPEMD160(SHA256(public key representation))

Example:

- point P = 02 c1fd6adf6f1aec1b1d28d3bb36039453269fa7bddfcc5a3bd473212c85acdfcd
- Gives RIPEMD160(SHA256(P)) = eb21d80903ba7b3323aaa001d55a3c86b1199277

20-byte result is then encoded using Base58Check encoded (version byte 00 for mainnet)

Example: bitcoin address 1NSGLbVWJW1bZhMGQ3oHwpq2jut7N7XfvD

Slide credit: F. Vercauteren

Bitcoin Script

Script is simple scripting system that is stack-based

- List of instructions that has to be satisfied when claiming an output of a transaction

Occurs in two places in a transaction:

- In an output: called the pubKeyScript, has to be satisfied to claim the value
- In an input: called the scriptSig, a proof that satisfies the pubKeyScript

Simplest example: pay to Pay-to-Public-Key-Hash

- pubKeyScript is of form OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
- scriptSig is of form <sig> <pubKey>
  - Sig is a signature computed using the private key (corresponding to the public key)

Slide credit: F. Vercauteren

Bitcoin Script

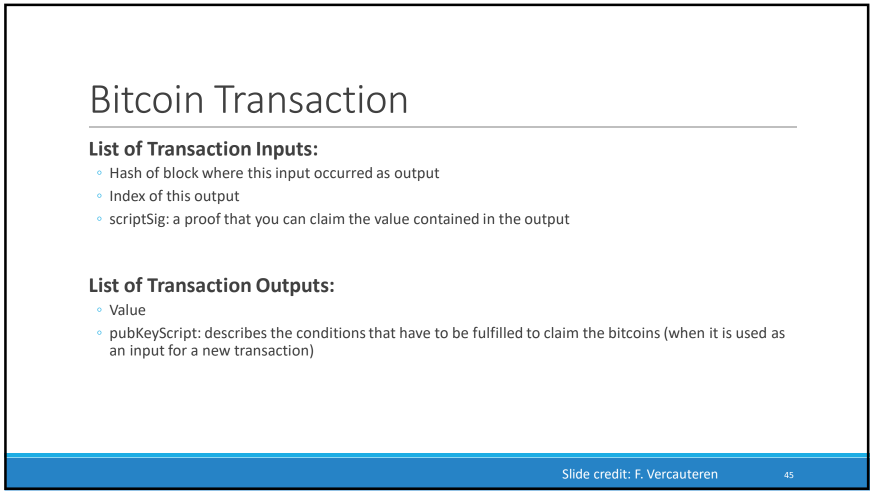
The value in an output can be claimed if the input that refers to it leads to a valid script

- Consisting of the concatenation of the scriptSig and pubKeyScript

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- <sig> <pubKey> : The signature and pubKey are pushed onto stack
- OP_DUP: The pubKey is duplicated
- OP_HASH160: The copy of the pubKey is hashed using RIPEMD160(SHA256()) and put onto the stack
- <pubKeyHash>: The pubKeyHash is pushed onto the stack
- OP_EQUALVERIFY: the top two items are the stack are popped and compared; if not equal, script is not valid
- OP_CHECKSIG: the signature is verified using the pubKey
  - The signature was computed using ECDSA-SHA256 on the SHA256 hash of a serialized form of the transaction

Slide credit: F. Vercauteren



Bitcoin Transaction

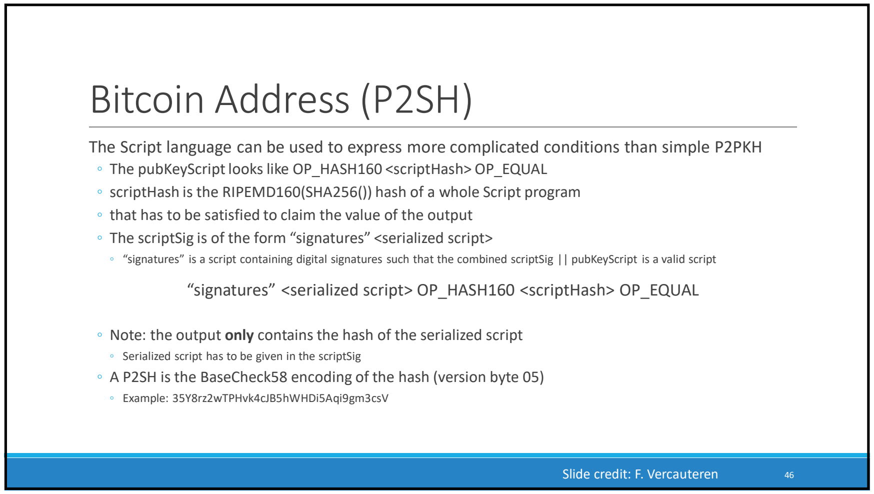
List of Transaction Inputs:

- Hash of block where this input occurred as output
- Index of this output
- scriptSig: a proof that you can claim the value contained in the output

List of Transaction Outputs:

- Value
- pubKeyScript: describes the conditions that have to be fulfilled to claim the bitcoins (when it is used as an input for a new transaction)

Slide credit: F. Vercauteren 45



Bitcoin Address (P2SH)

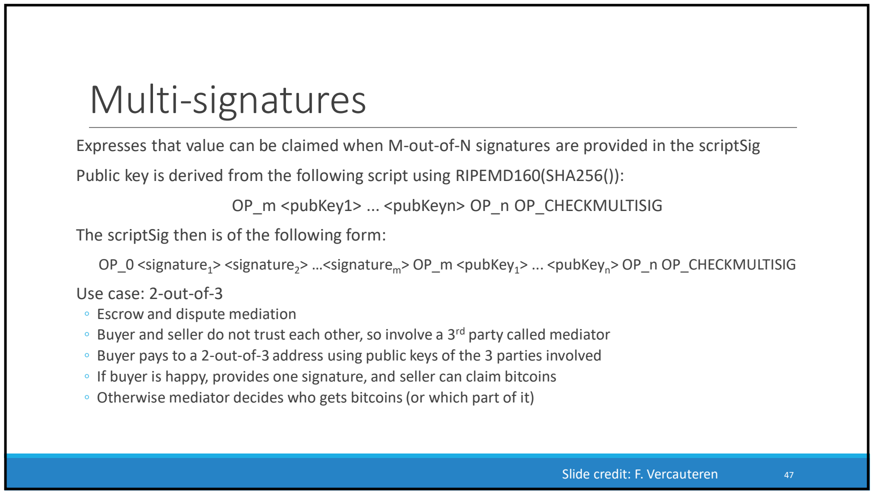
The Script language can be used to express more complicated conditions than simple P2PKH

- The pubKeyScript looks like OP_HASH160 <scriptHash> OP_EQUAL
- scriptHash is the RIPEMD160(SHA256()) hash of a whole Script program
- that has to be satisfied to claim the value of the output
- The scriptSig is of the form “signatures” <serialized script>
  - “signatures” is a script containing digital signatures such that the combined scriptSig || pubKeyScript is a valid script

“signatures” <serialized script> OP_HASH160 <scriptHash> OP_EQUAL

- Note: the output **only** contains the hash of the serialized script
  - Serialized script has to be given in the scriptSig
- A P2SH is the BaseCheck58 encoding of the hash (version byte 05)
  - Example: 35Y8rz2wTPHvk4cJB5hWHDi5Aqi9gm3csV

Slide credit: F. Vercauteren 46



Multi-signatures

Expresses that value can be claimed when M-out-of-N signatures are provided in the scriptSig

Public key is derived from the following script using RIPEMD160(SHA256()):

OP_m <pubKey1> ... <pubKeyn> OP_n OP_CHECKMULTISIG

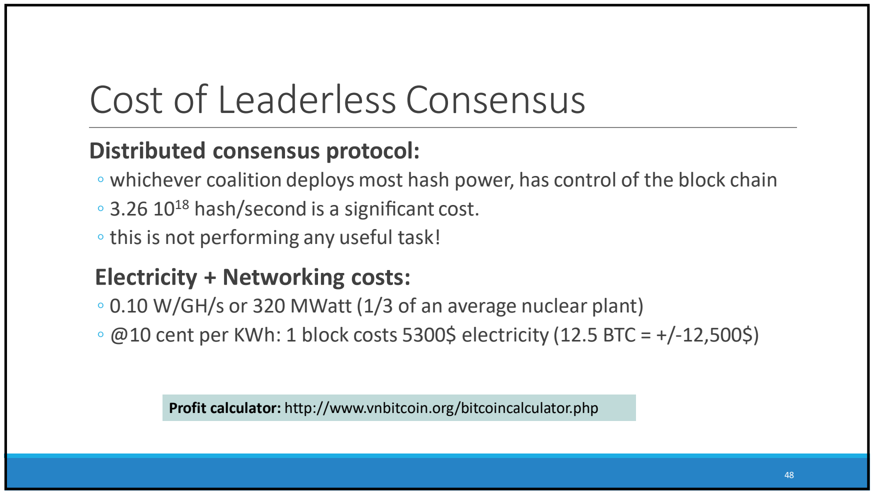
The scriptSig then is of the following form:

OP_0 <signature$_1$> <signature$_2$> …<signature$_m$> OP_m <pubKey$_1$> ... <pubKey$_n$> OP_n OP_CHECKMULTISIG

Use case: 2-out-of-3

- Escrow and dispute mediation
- Buyer and seller do not trust each other, so involve a 3rd party called mediator
- Buyer pays to a 2-out-of-3 address using public keys of the 3 parties involved
- If buyer is happy, provides one signature, and seller can claim bitcoins
- Otherwise mediator decides who gets bitcoins (or which part of it)

Slide credit: F. Vercauteren 47



Cost of Leaderless Consensus

Distributed consensus protocol:

- whichever coalition deploys most hash power, has control of the block chain
- 3.26 10^{18} hash/second is a significant cost.
- this is not performing any useful task!

Electricity + Networking costs:

- 0.10 W/GH/s or 320 MWatt (1/3 of an average nuclear plant)
- @10 cent per KWh: 1 block costs 5300$ electricity (12.5 BTC = +/-12,500$)

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

48

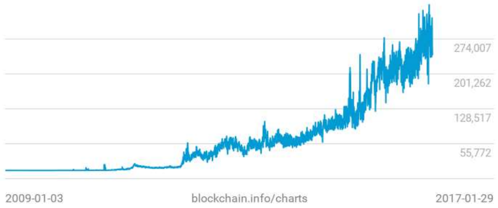
Number of Transactions Per Day

Large share goes to a few addresses

2.8 per second

Confirmed Transactions Per Day

241,627



Guestimate for card payments: a few 10.000 per second?

Bitcoin as a Currency

Who has control of the money supply in a currency?
- By convention it follows a well understood and committed curve that will max out
- Convention enforced by software

Who gets the new money? Who deletes the old money?
- No money is deleted (if you want a laugh: go suggest random deletions!)
- Money is created by hashing blocks and adding them to the block chain
- The miner gets the new coin

How do we make sure we will always remember who has how much money?
- Large block--chain is recorded by all (Jan'17 100 Gbyte!)
- Authoritative one is the longest – race for aggregate CPU power

Who has it to start with? (Does it matter?)
- Satoshi Nakamoto

Slide credit: George Danezis

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

Bitcoin Wallet

Payment associated to key pair (pay with digital signature)

Loss of signing key means loss of BTC

Secure key storage
- Software: if hacked, loss of BTC
- Exchange and wallet service: can also be hacked or corrupt insider risk
- Hardware: growing interest

Bitcoin Wallet

Public ledger allows to trace back any transaction to a coinbase transaction

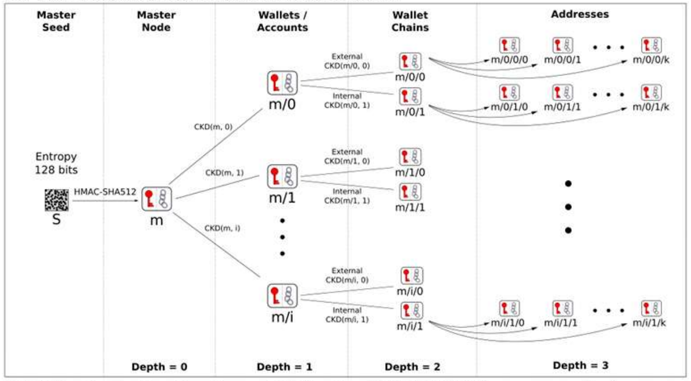
- Anonymity of transactions is not guaranteed

Avoid re-use of addresses (and thus public keys)

BIP32 + BIP44 proposal: hierarchical deterministic wallet

- Use each address only once
- Construct tree like structure of public keys derived from single master secret
- Private and public keys are “extended” with a chain code
- “Normal” child public key can be derived from parent **public** key, index and chain code
- “Hardened” child can only be derived from parent **private** key, index and chain code

BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ $\mathrm{CKD}(x,n) = \text{HMAC-SHA512}(x_{\mathrm{Chain}}, x_{\mathrm{PubKey}} \,||\, n)$

Alt Coins

Follow same design as Bitcoin, but with separate block chain and network

- Hundreds alternatives to Bitcoin, most of which are not very successful
- Different monetary policy
- Different proof of work or consensus mechanism
- Specific features, such as strong anonymity

08/2011: IXCoin is Bitcoin with increased reward (failed)

09/2011: Tenebrix changes proof-of-work algorithm to *scrypt* (failed)

- Memory intensive algorithm resistant to mining with GPUs and ASICs

10/2011: Litecoin uses *scrypt* as proof-of-work and faster block generation (still alive)

Today: 716 currencies derived from Bitcoin (see http://mapofcoins.com/bitcoin)

Slide credit: F. Vercauteren

Alt Coins

Monetary policy:

- Litecoin: block every 2.5 minutes, 84 million coins by 2140, scrypt as proof-of-work
- Dogecoin: block every 60 sec, 10^{11} coins by 2015, scrypt as proof-of-work
- Freicoin: negative interest rate to encourage spending, block every 10 minutes, SHA256 proof-of-work

Consensus mechanism:

- scrypt, scrypt-N, Skein, Groestl, SHA3, X11, Blake, or a combination of these
- Proof-of-stake: stake currency to generate interest
- Peercoin, Myriad, Blackcoin, VeriCoin, NXT (not Bitcoin derivative)

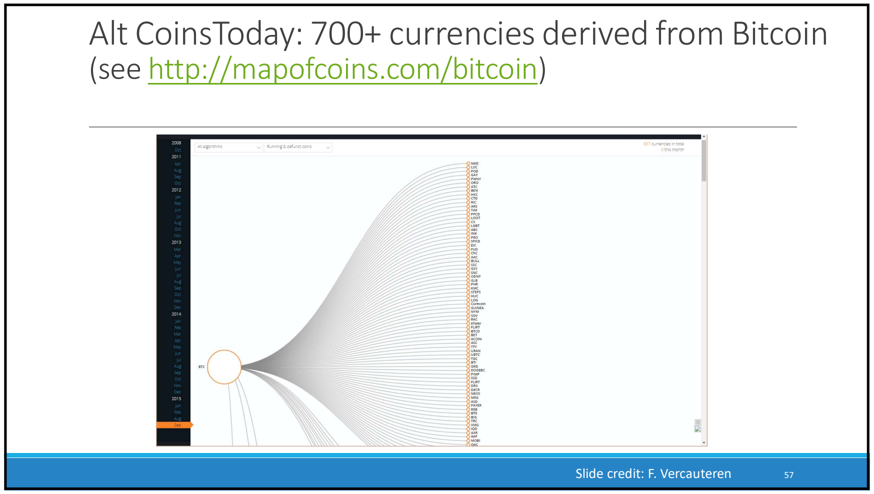
Dual purpose mining:

- Primecoin: finding primes; Curecoin: protein-folding; Gridcoin: BOINC grid computing

Anonymity:

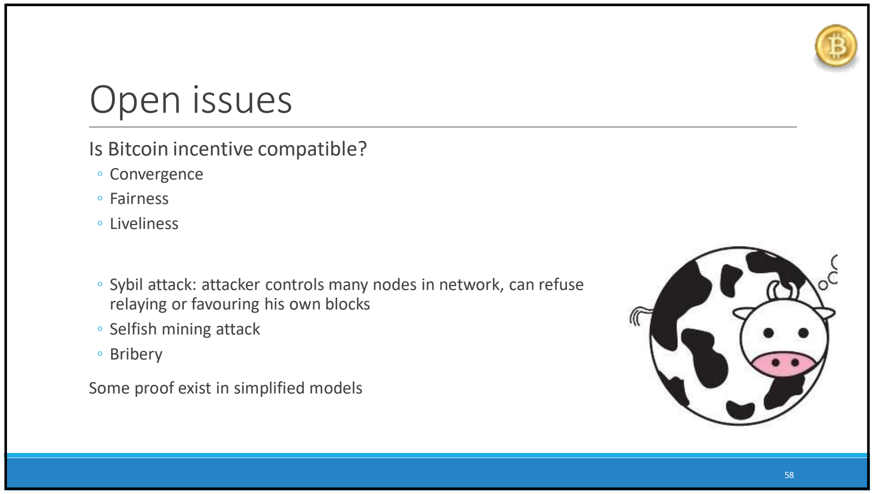
- Zerocoin/Zerocash: use zk-SNARKS; CryptoNote: using traceable ring signatures
- Darkcoin: re-mixing + multi-algorithm POW (X11)

Slide credit: F. Vercauteren



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

Slide credit: F. Vercauteren



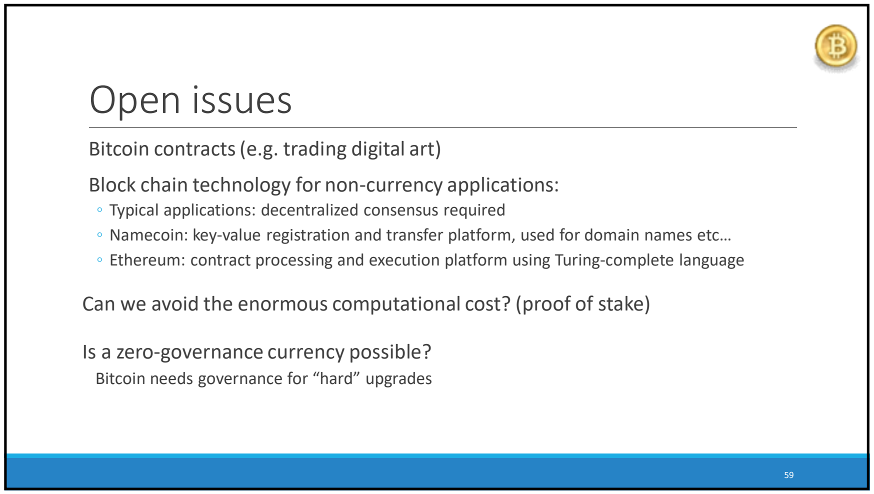
Open issues

Is Bitcoin incentive compatible?

- Convergence
- Fairness
- Liveliness

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

Some proof exist in simplified models



Open issues

Bitcoin contracts (e.g. trading digital art)

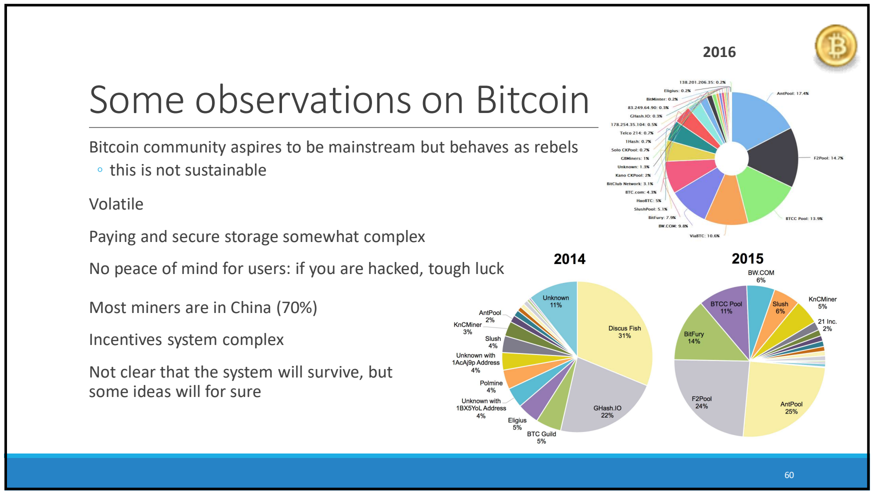
Block chain technology for non-currency applications:

- Typical applications: decentralized consensus required
- Namecoin: key-value registration and transfer platform, used for domain names etc…
- Ethereum: contract processing and execution platform using Turing-complete language

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

Is a zero-governance currency possible?

Bitcoin needs governance for “hard” upgrades



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

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	*Consortium/Hybrid Blockchain*	*Full private Blockchain*
• No central point of control by individuals, corporations or governments • Permissionless to participate • Concensus based on "proof ow work" • Examples: • *Bitcoin* • *Ethereum*	• Controlled by more than two 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 (UCLondon)	• 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

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

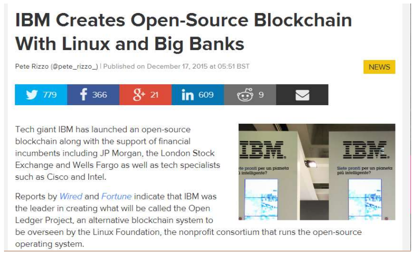
Financial world dislikes

- distributed control
- full transparency
- unclear governance
- uncontrolled money supply

IBM Open Ledger – Hyperledger

(public software)

Accenture, ANZ Bank, CLS, Credits, Digital Asset, Fujitsu, Initiative for CryptoCurrencies and Contracts, Mitsubishi UFJ Financial Group, State Street, SWIFT, VMware and Wells Fargo



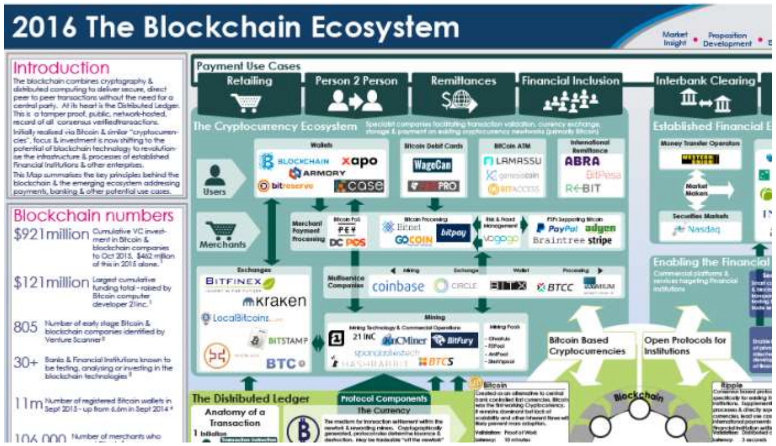
IBM Creates Open-Source Blockchain With Linux and Big Banks

Pete Rizzo (@pete_rizzo_) | Published on December 17, 2015 at 05:51 BST

NEWS

Tech giant IBM has launched an open-source blockchain along with the support of financial incumbents including JP Morgan, the London Stock Exchange and Wells Fargo as well as tech specialists such as Cisco and Intel.

Reports by *Wired* and *Fortune* indicate that IBM was the leader in creating what will be called the Open Ledger Project, an alternative blockchain system to be overseen by the Linux Foundation, the nonprofit consortium that runs the open-source operating system.



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[II]

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

11m Number of registered Bitcoin wallets in Sept 2015 - up from 6.6m in Sept 2014[4]

106,000 Number of merchants who

https://media.licdn.com

Pointers

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

Questions?

?

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