BITCOINS

Andy Pepperdine

2016-05-26

Outline

- What Bitcoin claims
- What is money?
- Brief history of money
- History of digital money
- Key problems with earlier systems
- How Bitcoin addresses those problems
- Vulnerabilities
- Conclusion

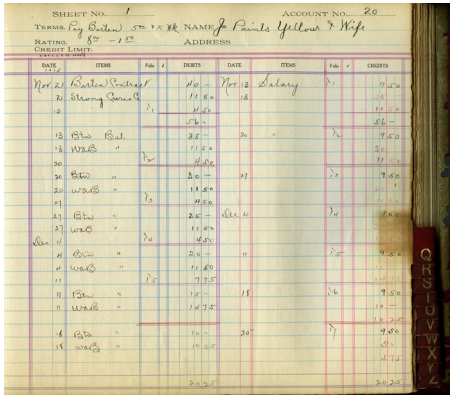
Claims

- Method of accounting
  - Who owns what amount of bitcoins
- Private and anonymous
- Independent of any central authority
- Trust is embodied in the total solution
- Payment method and currency

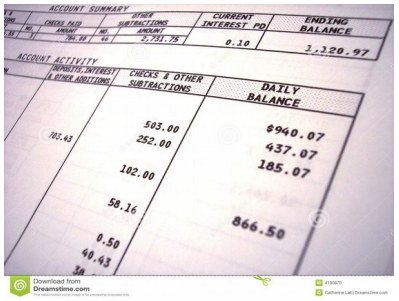
What is money?

- Two philosophies of what money is
- It has an intrinsic value
  - like gold (metallists)

- Bookkeeping convention
  - no actual value (chartalists)



What is currency?



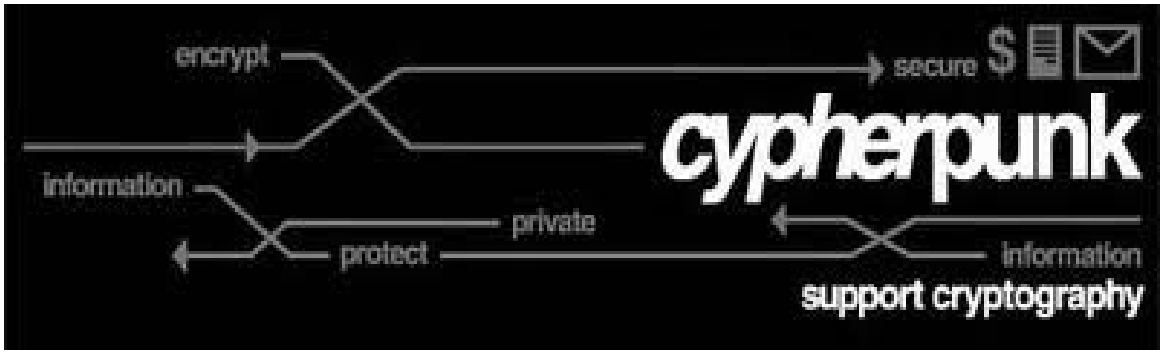
- Medium of exchange
- Store of value
- Unit of account

History – I

- Barter, where no intermediate items are held
- Coins, shells, stones, etc.
  - Represents the value of something
  - Aids in transferring value remotely
  - Trust is expected and agreed on its use
- Banking holds values in trust
  - IOUs and credit
  - Later started to invest on their own account

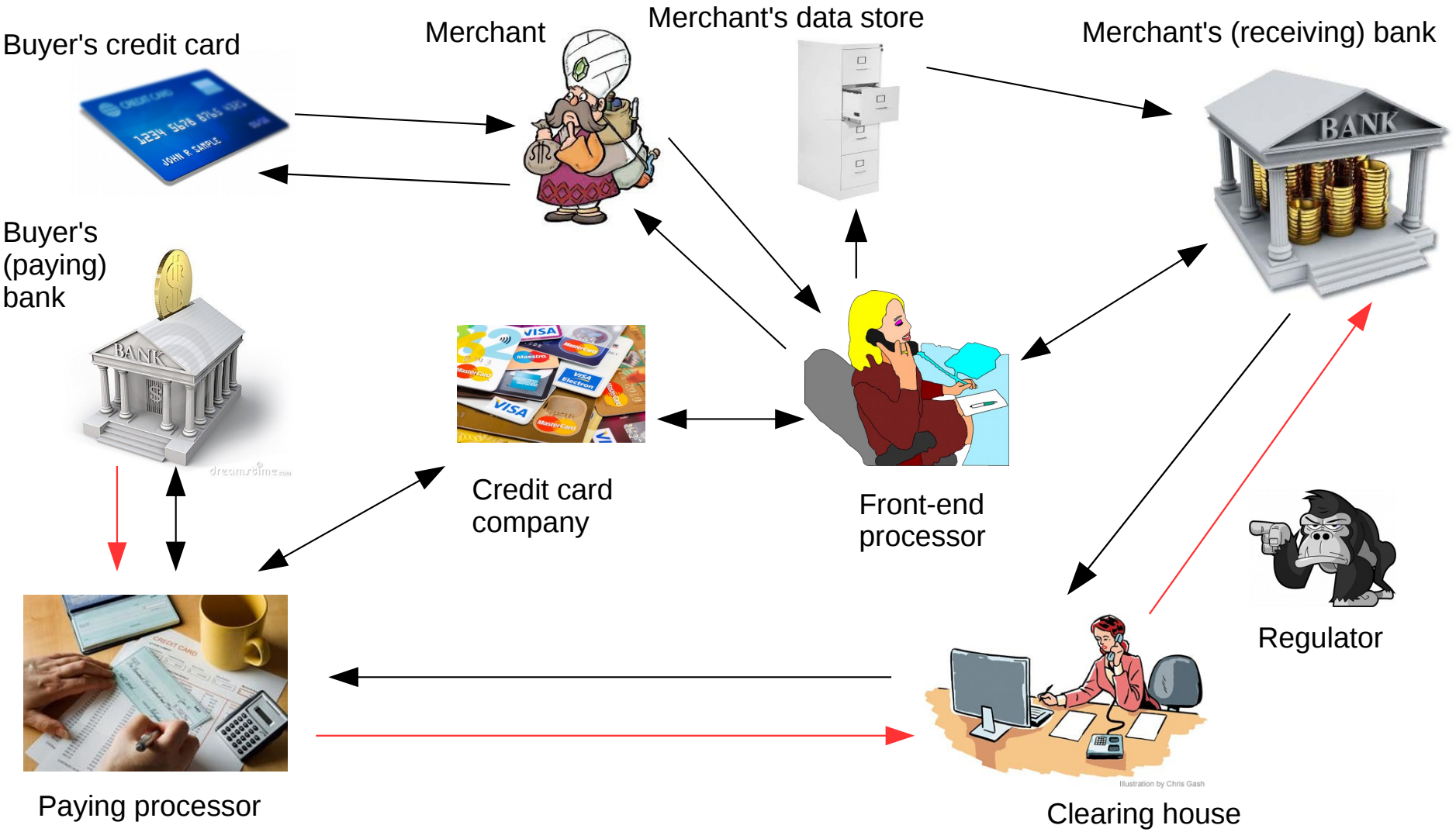
History – II

- Use tokens (coins, notes, etc) to represent who has what wealth
- Difficult to forge
  - Control of total amount of money
  - Prevent spending the same thing twice
- Most of it now is in form of contracts & IOUs
- Trust the keepers of the ledgers and accounts



- During the 1980s
- Loose association of Cryptographers
- Electronic privacy
- Made encryption tools – e-mail, files, etc.
- Spawned Wikileaks, TOR, SecureDrop

Card Payment Process



Electronic payments

- Immediate transfer of small amounts directly from one person to another
- Negligible overhead or fees
- Absolute trust in the system
- Prevent duplicate spending
- Started by trying to improve the existing transfer mechanisms

Digicash

- First attempt to create private monetary transactions
- David Chaum 1990
- Needed backing of the banks
- Moderately successful, especially in NE of the US for road tolls
- Lost support and went bankrupt in 1998 and sold
- Now a mobile payment system

Chaum's Innovations

- Batching and mixing of messages to anonymise them
- Trustworthy electronic voting systems
- Undeniable signatures
- Group signatures

The currency problem

- Cypherpunks started to discuss how to make a currency independent of any central authority
- Trusting the clearing house
- Regulation is typical way to control centralised resources
- Who watches the watchmen?
- Little headway made, until ...

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: **Bitcoin P2P e-cash paper**
Newsgroups: **gmane.comp.encryption.general**
Date: 2008-10-31 18:10:00 GMT (7 years, 8 weeks, 2 days and 42 minutes ago)

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 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.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract.  A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
```

http://article.gmane.org/gmane.comp.encryption.general/12588/

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

https://bitcoin.org/bitcoin.pdf

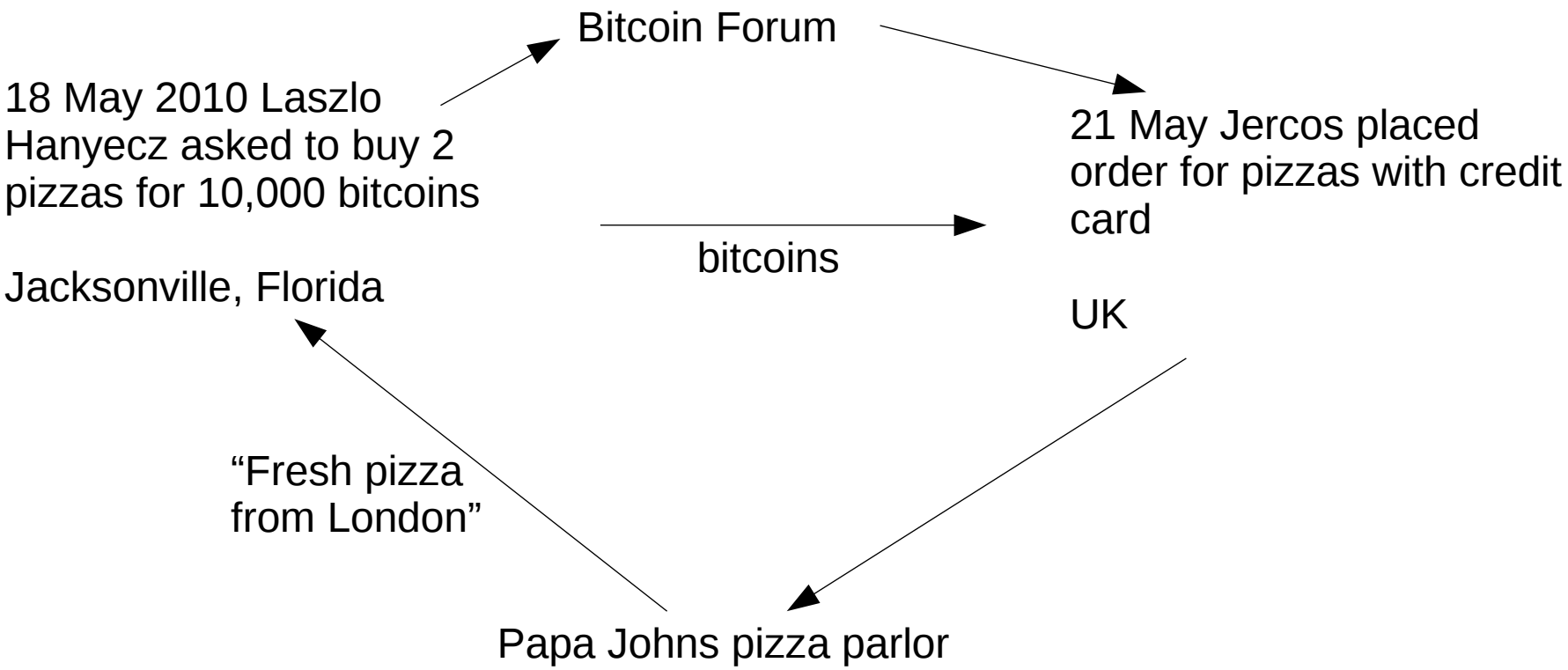
Satoshi Nakamoto

- No one has been identified as writing under this name
- Satoshi is a male Japanese name which could mean "wisdom"
- 31 Oct 2008 first message
- 4 Jan 2009 first "Genesis" block in the ledger
- 12 Dec 2010 last public message
- April 2011 last private message
- Massive speculation as to who it could be
- Craig Wright did not prove he was Satoshi – grave doubts

What do we know?

- Only the content of those messages, and code he produced to implement the system
- He started designing in 2007, and said that the design took a lot longer than the coding
- Lehman collapsed in September 2008 – one month before Satoshi's first announcement
- He selected Gavin Andresen to take over as the project leader

Showing they have value



2010 prices: $41

2015 prices > $5 milliion

Consequences

- Hanyecz had used gpus to boost mining power and had bitcoins to spare
- But others quickly caught up
- Jan 2013 Ng Zhang and Yifu Guo introduced ASIC dedicated mining chips
- Moved mining into realm only accessible to very deep pockets
- Arms race – energy intensive
- Estimated > $1 Billion invested in mining

Initial steps

- In two years he had accumulated an enthusiastic and idealistic group
- Bitcoins were being traded for real items
- Conversion exchanges had been established
- Mining technology had revolutionised the generation of bitcoins
- The system absorbed all the shocks as expected

Bitcoin Insight

- Use peer-to-peer network of nodes to assess one another's work
- Majority checking validity of proposed entries in the ledger
- Instead of penalties for misbehaviour, uses incentives for good behaviour
- Steady, but decreasing, rewards in new bitcoins
- Everything is open and public

Identifiers

Signing key – SA

Kept secret:
Used to sign
messages

PA is used to verify
the signed message

Public key – PA

Presented to the world
and is her
identifier

Cryptographic identity PA(SA(M)) = M = SA(PA(M))

Transaction

Alice

25 BTC from
Carol V(C,A)

20 BTC from
Dennis V(D,A)

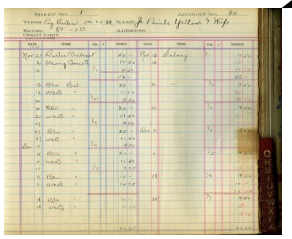
30 BTC to
Bob V(A,B)

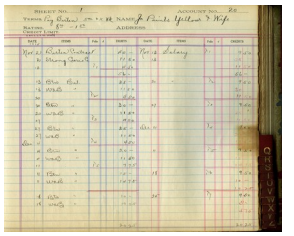
15 BTC back
to Alice V(A,A)

Bob

The ledger does not keep running totals of how many bitcoins are held overall by any one identifier

Bitcoin payment





Wallet

- Individual's record of bitcoins currently held
- Various apps available for this purpose, but not part of the essential Bitcoin infrastructure
- Wallet identified only by a public key – not by any name, address, or any other identifying information
- Transaction requests signed by the private key

Blockchain

- Contains records of ALL transactions
- Continually increasing as time goes on
- Built by "miners", who gain bitcoin rewards for performing that job
- Public – anyone can see what transactions have occurred
- Accounts are identified only by public keys

Proof of Work

- Free loaders are not welcome
- Must solve a puzzle (which has many different answers) in order to prove that the work has genuinely been done
- Puzzle depends on the block just built
- Find another piece so that a calculation gives a certain type of result

Hash functions

- Function where it is easy to compute $h = H(x)$ but (almost) impossible to compute $x = H^{-1}(h)$
- Bitcoin chose one called SHA-256, which is part of the cryptographically strong public key algorithms
- 256-bit (64-byte) result of hash
- Puzzle is to solve for y: $H(K(b) \circ y) < L$
- The lower the limit, the harder it is to solve

Vulnerabilities

- Centralised control of mining nodes
- Scaling up from 7 transactions per second to Visa's 10,000
- Pollution of the blockchain with "dust" (tiny amounts of bitcoin left in open accounts)
- Attacks from enormous numbers of tiny transactions
- Conversion to/from existing currencies

Limitations

- Number of bitcoins capped at ~ 21 million
- Smallest denomination is about 10^{-8} bitcoins, known as 1 satoshi
- Currently only 5 core developers, only 3 are full time, paid by their employers
- Only the lead developer, Gavin Andresen, is paid by a charitable foundation

Present statistics

- As of 31 Dec 2015
- Blocks in chain: 391,090
- Total bitcoins: 15,027,150
- Market capitalisation: $6,325,122,787.95
- Addresses (accounts) nearly 60,000,000
- In 2016, blockchain was > 60 GB in size

The Future

Many scenarios have been put forward

You choose

Further information

- The original paper: https://bitcoin.org/bitcoin.pdf
- Central site (English): https://bitcoin.org/en
- Wallets: https://bitcoin.org/en/choose-your-wallet
- To buy bitcoins in UK, try this site: http://www.coindesk.com/information/buy-bitcoin-uk/
- Locate ATMs: http://www.coindesk.com/bitcoin-atm-map/
- Also in Bristol: https://satoshipoint.com/
- Mycelium setup: http://bitcoin4less.com/bitcoin-wallet-setup-mycelium/

References

- Whitepaper https://bitcoin.org/bitcoin.pdf
- Statistics on blockchain at http://www.coindesk.com/data/bitcoin/
- State https://letstalkbitcoin.com/blog/post/the-state-of-the-blockchain-addresses
- Quotes from Satoshi at Motherboard blog https://motherboard.vice.com/blog/quotes-from-satoshi-understanding-bitcoin-through-the-lens-of-its-enigmatic-creator
- *The Age of Cryptocurrency*, Vigna & Casey, St. Martins, 2015, ISBN 978-1-250-07308-2