Bitcoin Values and Implementation

“What Happens when the Internet dies?” lecture

December 10, 2018
By Raul Nohea Goodness

What is Bitcoin and why does it matter to people and the Internet?

"The Net interprets censorship as damage and routes around it." -- John Gilmore

- A decentralized peer-to-peer network
- A public transaction ledger (blockchain)
- Decentralized currency issuance (mining)
- A decentralized transaction verification system

Case study: Wikileaks and the funding shutdown

December 2010: Wikileaks releases 250,000 classified State Dept cables.

Paypal, MasterCard, Visa suspended service or froze Wikileaks accounts. Swiss bank account frozen. Amazon terminates hosting. Domain name disabled. Wikileaks declares a funding crisis.

December 2010: discussion of using Bitcoin to fund Wikileaks. Satoshi Nakamoto speaks against it, due to bitcoin being in infancy stage, where the attention could “destroy” the small beta community.

June 2011: Wikileaks starts accepting bitcoin donations.

Case study: Wikileaks and the funding shutdown

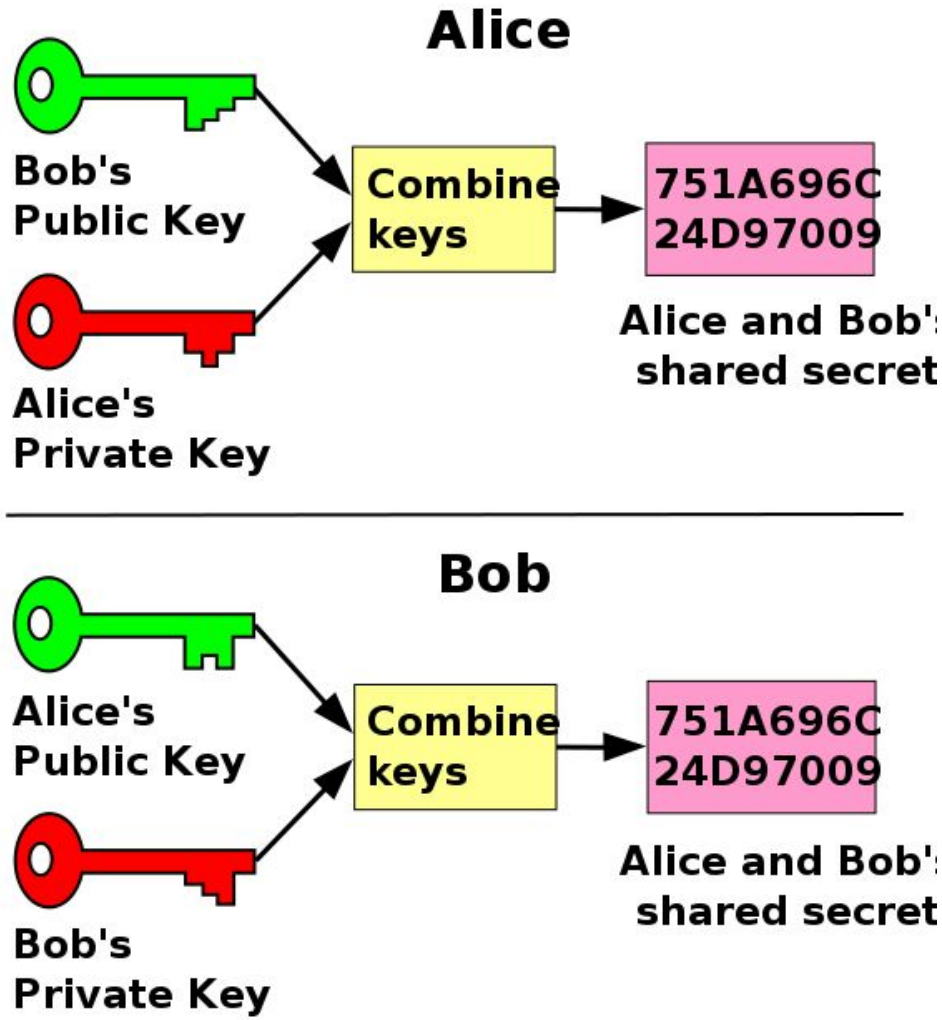
Takeaways:

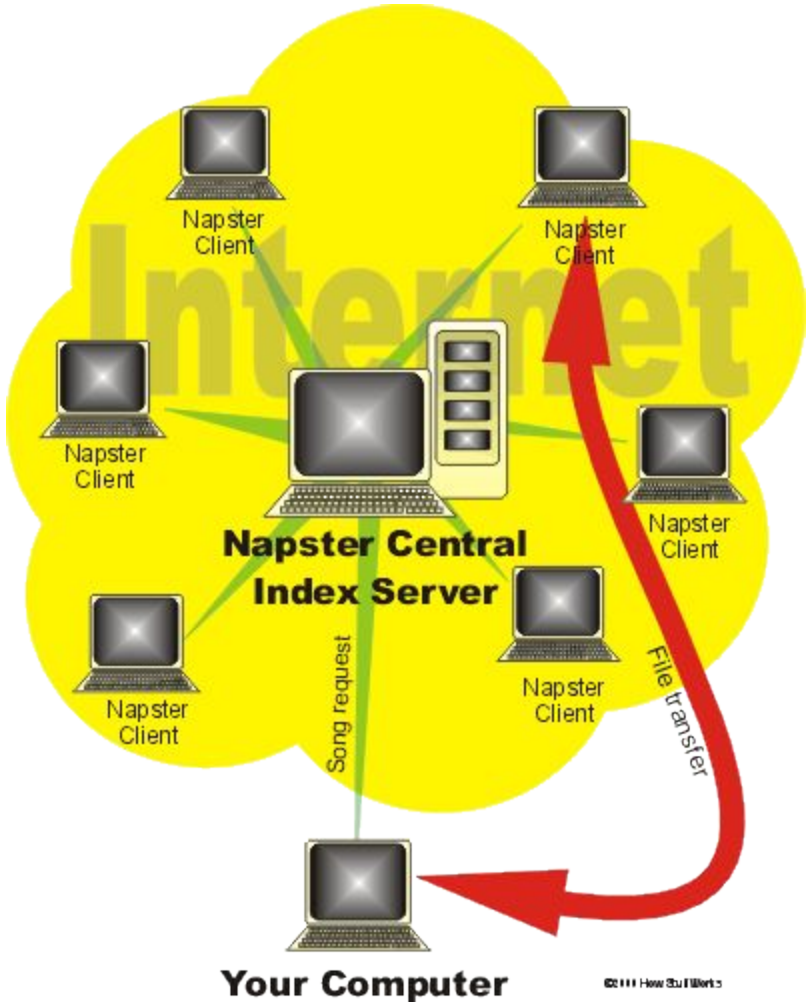
Centralized financial services are susceptible to State control or pressure, with or without explicit law.

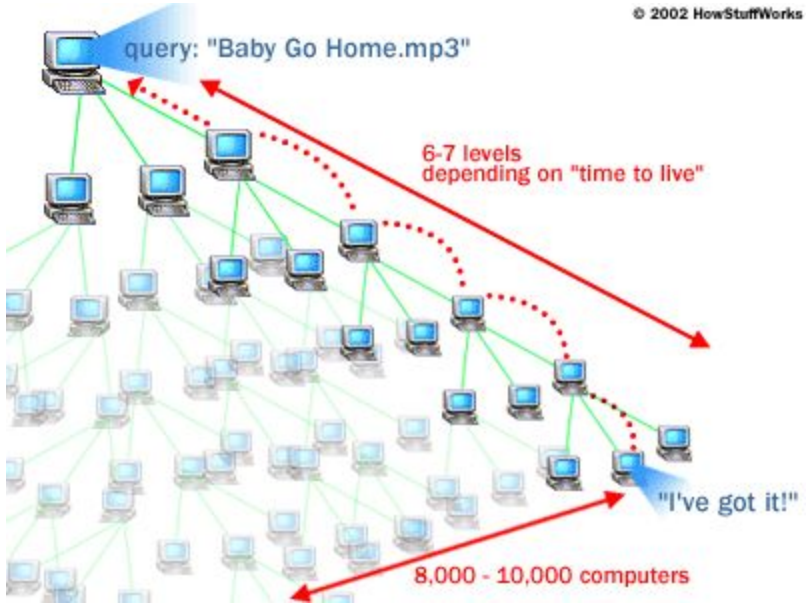
If every “node” clears transactions, then there is no place to “pull the plug” on the system.

Bitcoin precursors and genealogy

- Public key encryption (Diffie Hellman key exchange). One-way hashing functions.
- PGP – Pretty-good privacy (1991). Files/email using public-key encryption. Phil Zimmerman target of criminal investigation “munitions export without license” (dropped).
- Napster – first mainstream peer-to-peer (p2p) file sharing. Central server directory, but peers transferred files directly. Later Gnutella network uses decentralized directories, thus resistant to court order shutdown.
- HashCash – used proof-of-work functions as an anti-spam and anti-Denial-of-service (DoS) system. Used by early digital cash experiments (RPOW, B-money, Bit Gold)


Alice
Bob's
Public Key
Alice's
Private Key
Combine
keys
751A696C
24D97009
Alice and Bob'
shared secret
Bob
Alice's
Public Key
Bob's
Private Key
Combine
keys
751A696C
24D97009
Alice and Bob'
shared secret


Internet
Napster Client
Napster Client
Napster Client
Napster Client
Napster Client
Napster Client
Napster Central Index Server
Song request
File transfer
Your Computer


© 2002 HowStuffWorks
query: "Baby Go Home.mp3"
6-7 levels
depending on "time to live"
"I've got it!"
8,000 - 10,000 computers

What is Money?

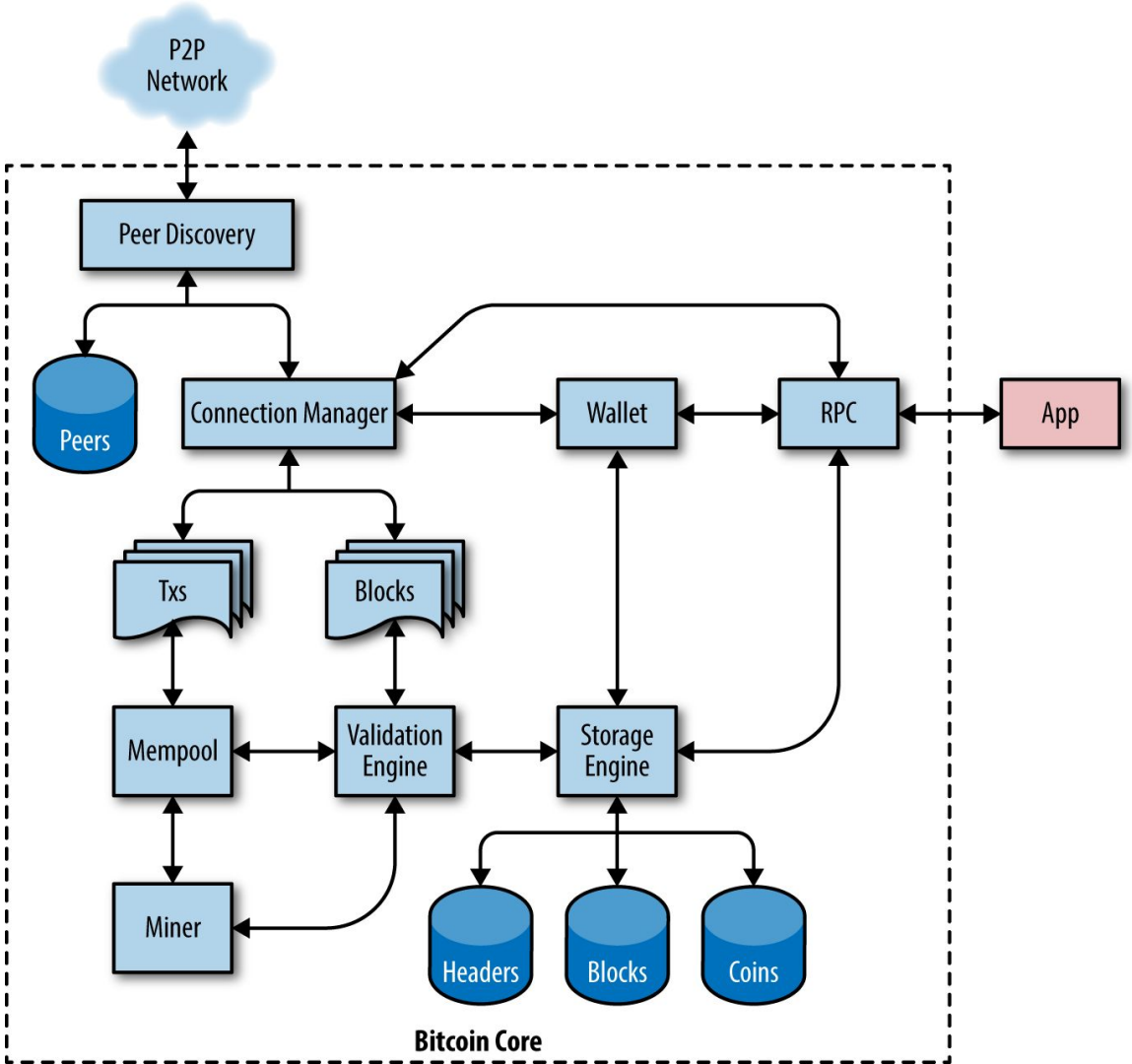
- Rare (scarcity)
  - Can not be easily counterfeited (double-spent)
- Portable
- Fungible (interchangeable)
  - One dollar is the same as any other
- An abstraction (if not, it is barter). Represents something else. “Shared hallucination of paper money” (A. Antonopoulos)

Bitcoin values and design objectives

- Cypherpunk – use of cryptography and privacy for social and political change
  - Cypherpunks mailing list
- Decentralized
- Privacy – anonymous addresses on public ledger.
- Censorship resistance (Decentralized + privacy)
- Trustless – all nodes can independently verify all transactions on the blockchain or mempool (unconfirmed transactions). Assumes some bad actors.
- “What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”

Bitcoin Implementation

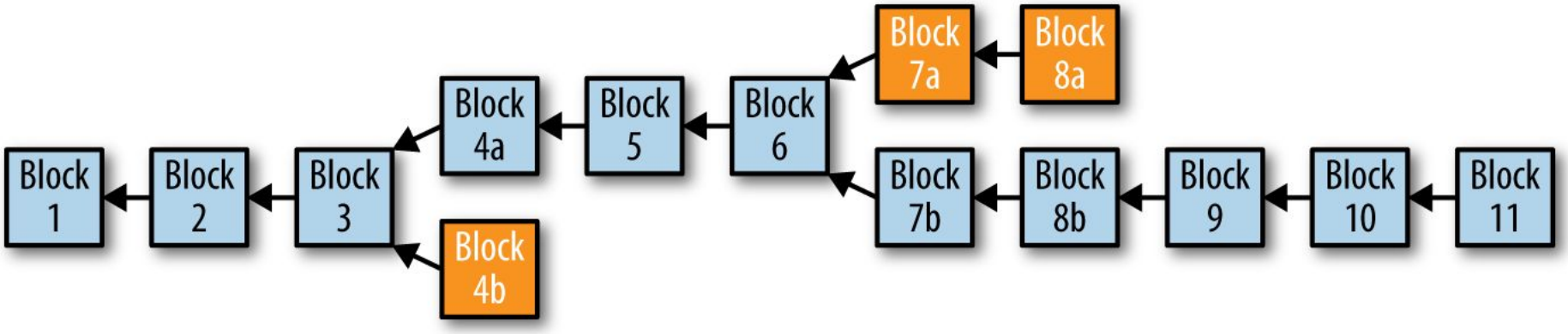
- Roles of a bitcoin node: Wallet, Miner, Routing node, Blockchain database.
- Public Key encryption
- One-way hashing algorithm (hard to forge, easy to validate)
- Proof-of-work
  - First distributed computing solution to the Byzantine Generals Problem
- Peer-to-Peer: all nodes validate all transactions and blocks independently. Invalid tx and blocks are rejected. Transactions are cleared to the ledger by consensus (not central authority).
- Blockchain – each block's hash (fingerprint) is derived from the hash of the prior block along with its transactions.
- Free open source software – may be inspected, built independently.

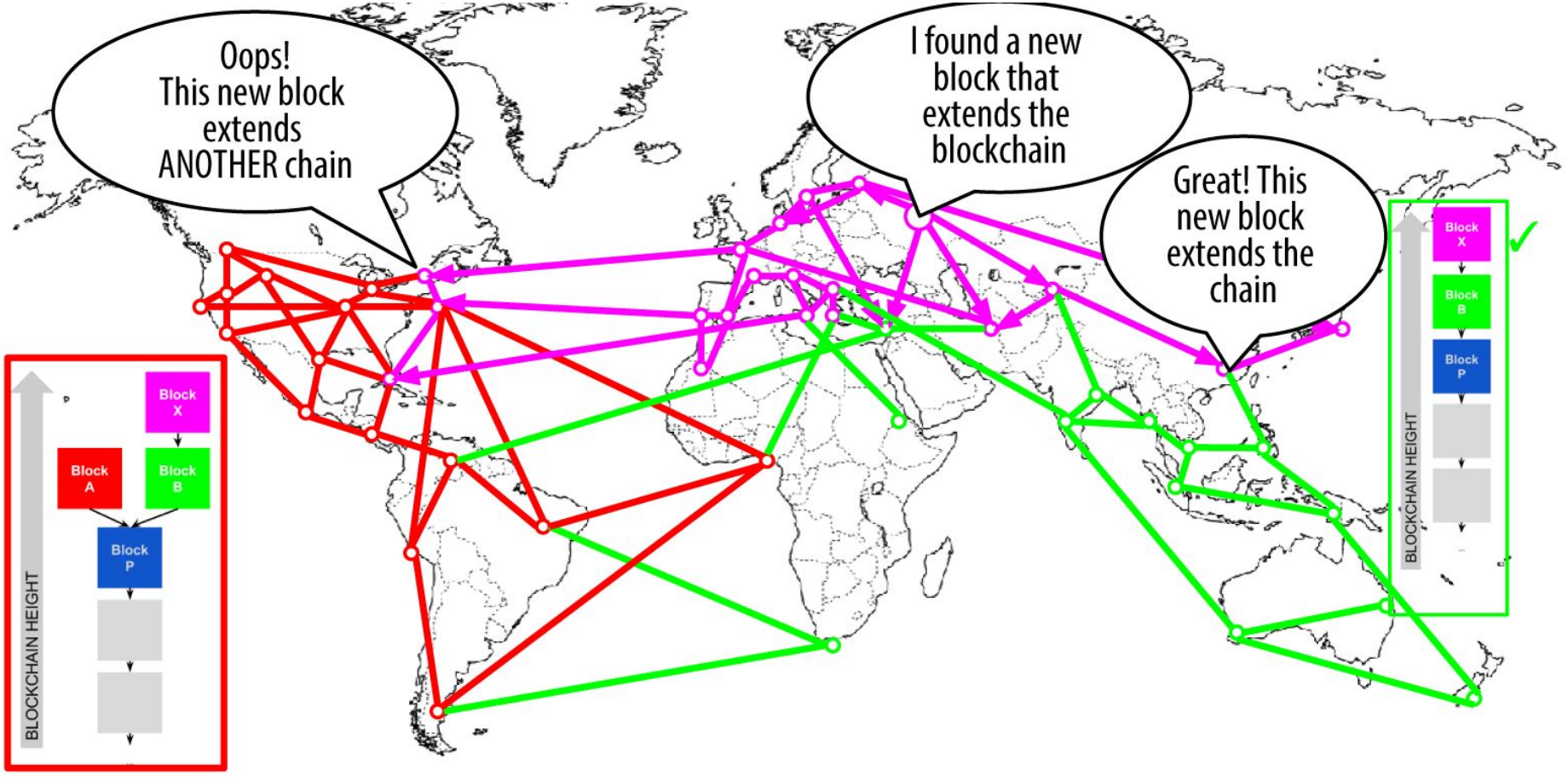

P2P
Network
Peer Discovery
Peers
Connection Manager
Wallet
RPC
App
Txs
Blocks
Mempool
Validation
Engine
Storage
Engine
Miner
Headers
Blocks
Coins
Bitcoin Core

Bitcoin Blockchain

- A Block is a group of recent transactions (tx), plus a “coinbase” transaction with the miner's block reward.
- “uncommitted” blocks are groups of transactions created by “miners” solving the Proof-of-work function.
- When a block is added to the blockchain, it is irrevocably tied to its parent block.
- To reverse a transaction, the block must be recreated, and every subsequent block as well. Due to the “work” involved, this makes it virtually impossible after 6 blocks.
- Even if a node has been following chain “A” of a fork, it would switch to chain “B” if it has more “work” and is valid.
- Blocks are targeted for issuance every 10 mins. If more hashpower is added to the network, the difficulty of mining blocks also goes up.

Bitcoin Blockchain - Forking




Oops!
This new block
extends
ANOTHER chain
I found a new
block that
extends the
blockchain
Great! This
new block
extends the
chain
Block
X
Block
A
Block
B
Block
P
BLOCKCHAIN HEIGHT
Block
X
Block
B
Block
P
BLOCKCHAIN HEIGHT

Conclusions

- Freedom of speech and political action requires resistance to economic control
- Centralized financial services are susceptible to State control or pressure
- If every financial “node” clears transactions, then there is no place to “pull the plug” on the system.
- The innovation of Bitcoin tech only exists because of the value systems of its creators, and its precursors.

References:

- https://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/#412042d97202
- https://www.cnet.com/news/mastercard-pulls-plug-on-wikileaks-payments/
- https://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive/
- https://en.bitcoin.it/wiki/Hashcash
- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- https://en.wikipedia.org/wiki/Cypherpunk
- https://www.youtube.com/watch?v=GSNo0JBFYcQ
- http://nakamotoinstitute.org/bitcoin/
- https://github.com/bitcoinbook/bitcoinbook