The Age of Cryptocurrencies: Bitcoin and Sisters

Ghada Almashaqbeh
Columbia University

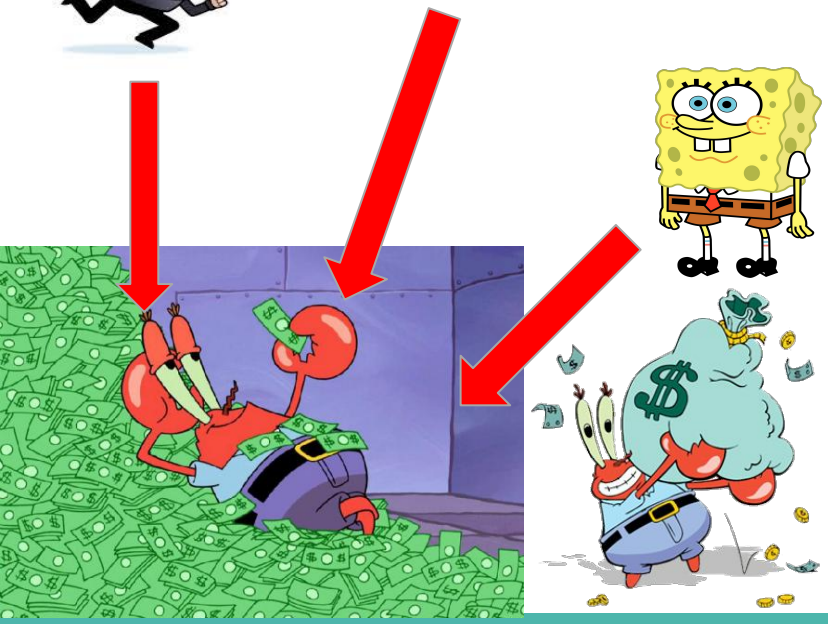
April 2019

Outline

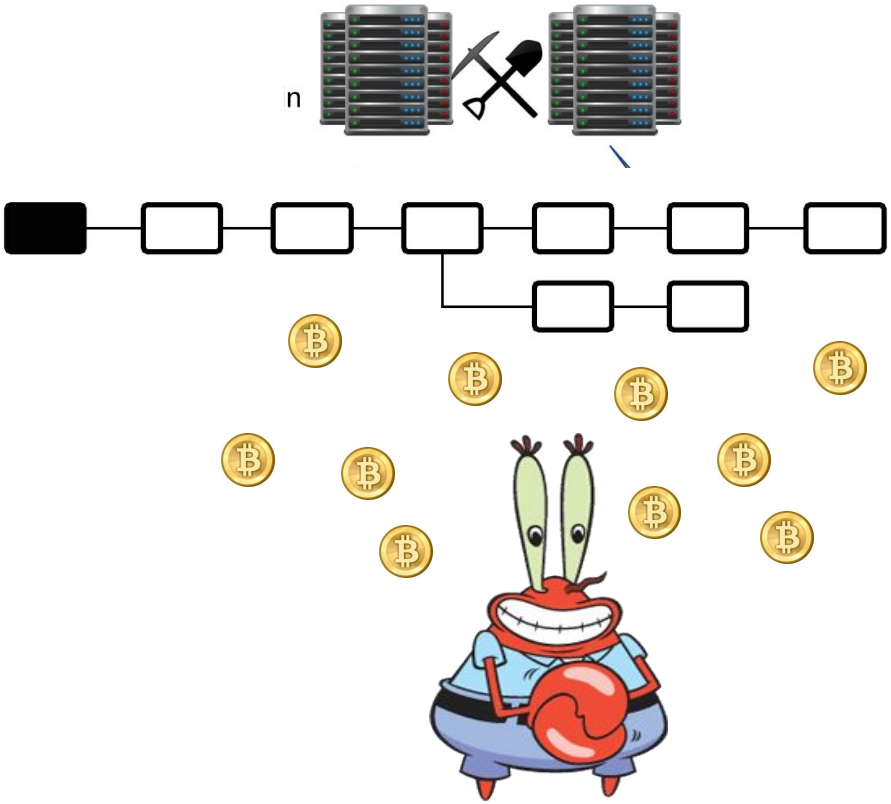
- Motivation.
- Main concepts.
  - Operation; transactions, mining, blockchain, consensus.
- Main problems and potential solutions:
  - Supported functionality,
  - Anonymity,
- Conclusions.

Once Upon A Time

Centralized Currency



Decentralized Currency



History

- A whitepaper posted online in 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System”.
  - By Satoshi Nakamoto.
  - Described a distributed cryptocurrency system not regulated by any government.
- The system went live on January 2009.
- Now “Satoshi Nakamoto” is only associated with certain public keys on Bitcoin blockchain.
  - She/He/They was/were active on forums/emails/etc. till 2010.
- Currently there are ***2129 cryptocurrencies*** (https://coinmarketcap.com/).

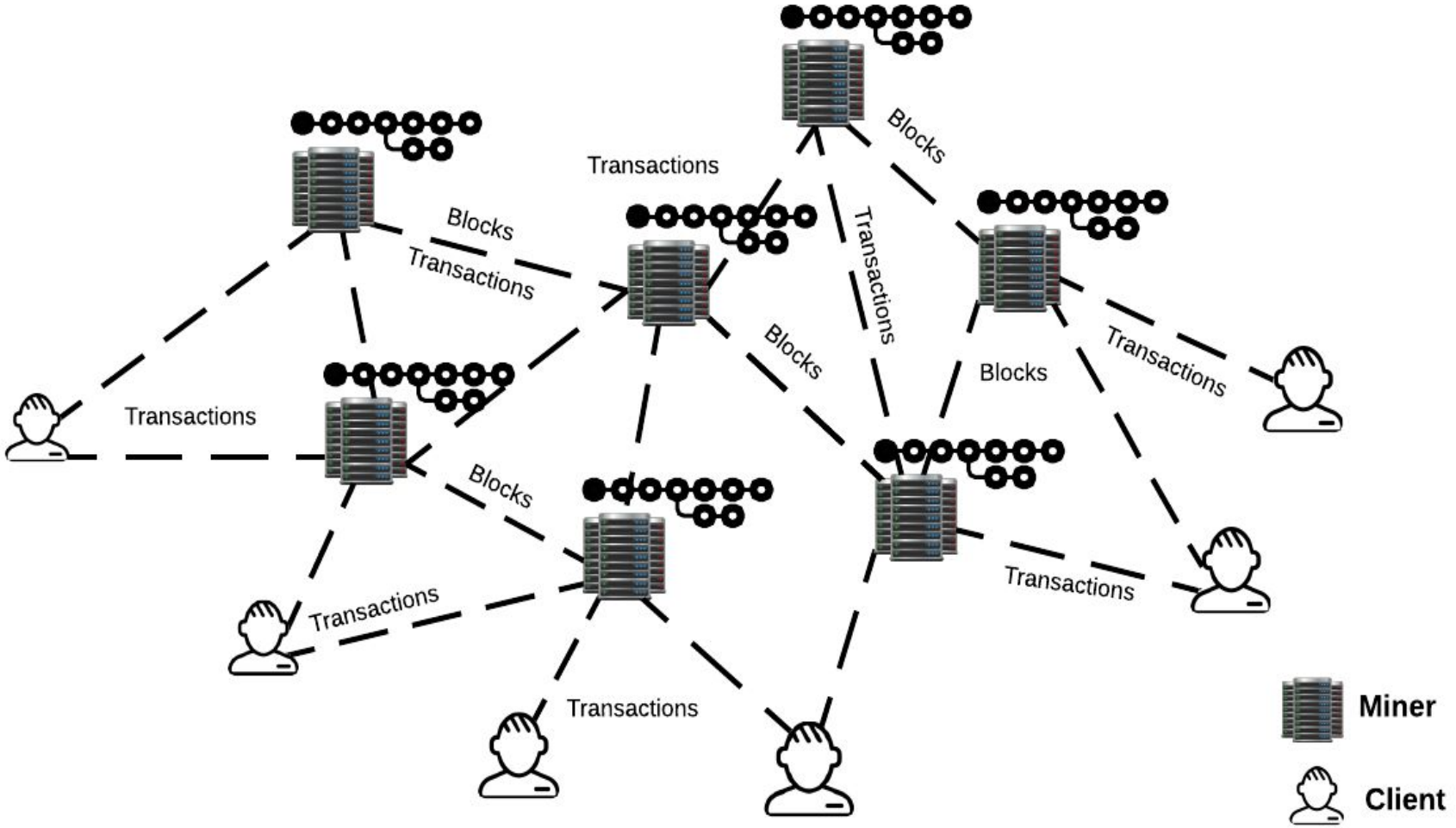
Bitcoin in a Nutshell I

- A distributed currency exchange medium open to anyone to join.
- Utilize basic cryptographic primitives to control money flow in the system.
- Main components:
  - **Players:** miners and clients.
  - **Transactions:** messages exchanged.
  - **Blockchain:** an append-only log.
  - **Mining:** extending the blockchain.
  - **Consensus:** agreeing on the current state of the blockchain.

Bitcoin in a Nutshell II

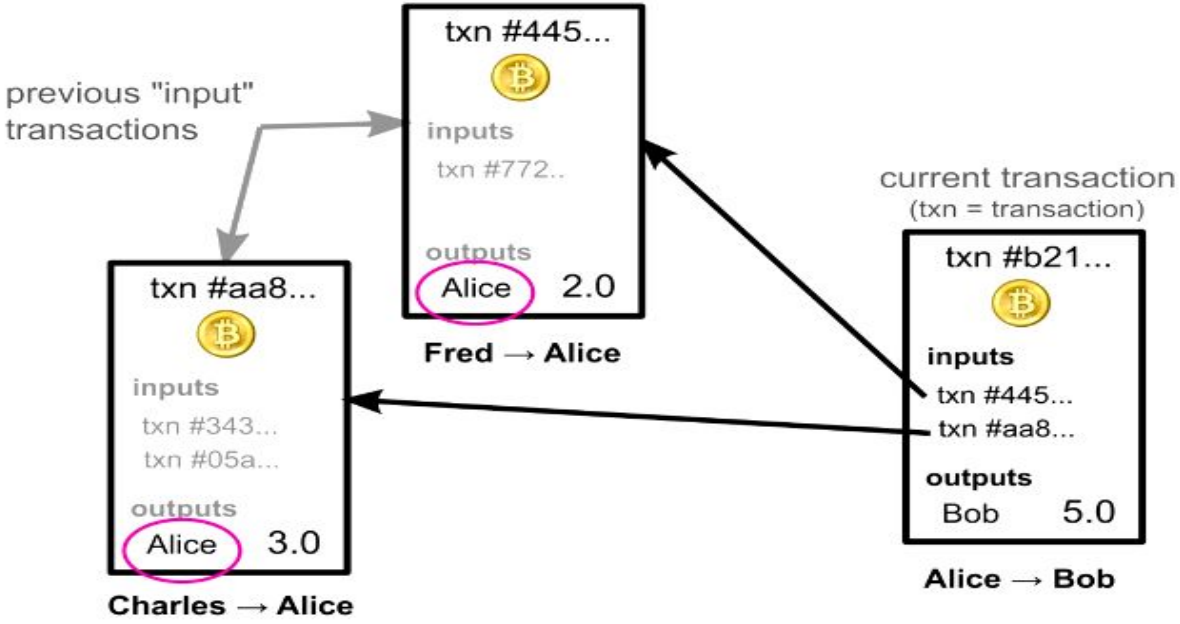
- No real identities are required, just a key pair.
  - Usually the hash of the public key is used as an address.
- Losing the private key of a specific address means losing the coins associated to this address forever.
  - Wallets take care of tracking coins, issuing transactions, etc.
- Clients, or simple payment verification (SPV) nodes, are concerned with their transactions only.
  - Do not mine or hold full copies of the blockchain.
- Miners, or fully validating nodes, track everything and mine.

Bitcoin Pictorially



Virtual Coins

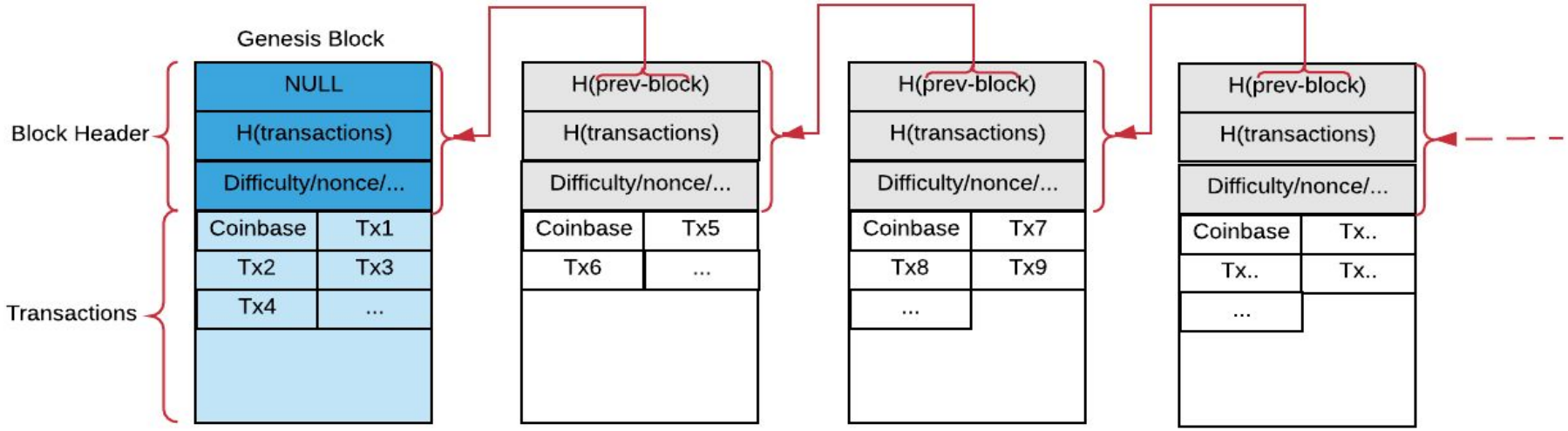
- Digital tokens, or transactions, that can be spent by providing signatures.
- No notion of accounts, track chains of transactions.
  - Wallets do that transparently for users.
  - Other cryptocurrencies do it differently, e.g., Ethereum have accounts for users.



Source: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Blockchain and Mining

- It is an append only log containing a full record of all transactions.
  - Full history is needed to handle double spending.



Mining

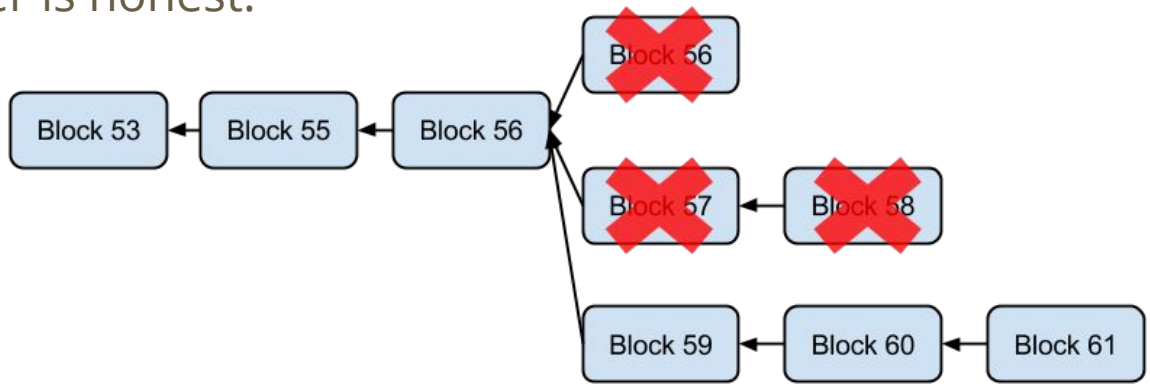
- Miners extend the blockchain by mining new blocks.
  - Proof-of-work in Bitcoin.
- Miners solve a hash puzzle,

SHA-256(SHA-256 (new block header)) < Difficulty Target

- Difficulty is adjusted periodically.
- This is needed to prevent Sybil attacks.
- Miners collect rewards: mining rewards + transaction fees.
- Total Bitcoin to mine is capped by 21 million BTC.
  - Currently there are around 17.6 million coins in circulation.

Consensus

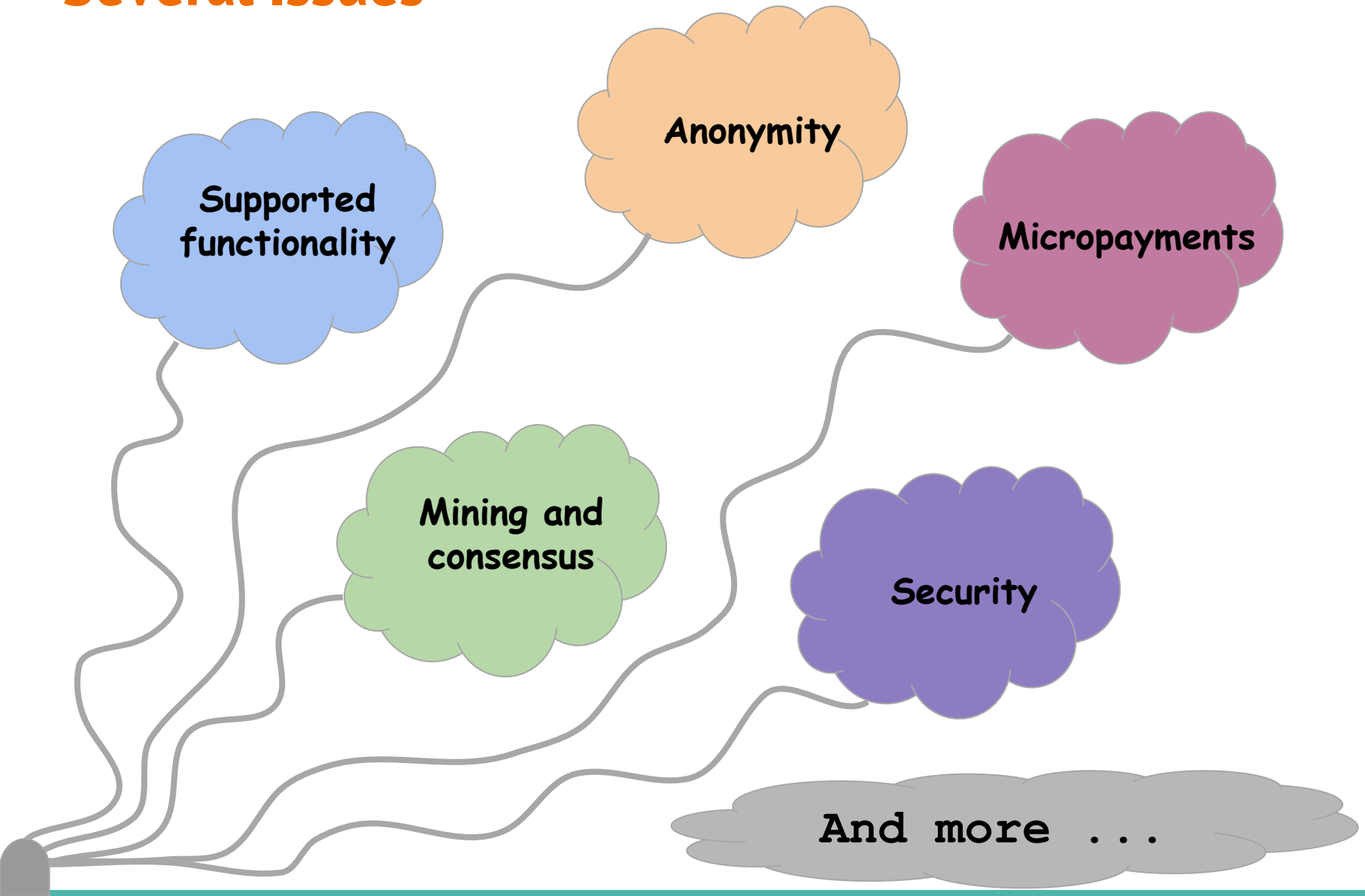
- Miners hold , hopefully, consistent copies of the blockchain.
  - Only differ in the recent unconfirmed blocks.
- A miner votes for a block implicitly by building on top of it.
- Forking the blockchain means that miners work on different branches
  - Caused by network propagation delays, adversarial actions, etc.
  - Resolved by adopting the longest branch.
- Security is subject to the assumption that at least 50% of the mining power is honest.



Source: http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

But …

Several Issues



Supported Functionality

Bitcoin

- **Vision:** distributed currency exchange medium with the virtue of simplicity.
  - Supports Turing-incomplete scripting language.
  - Tedious currency tracking model.

Ethereum

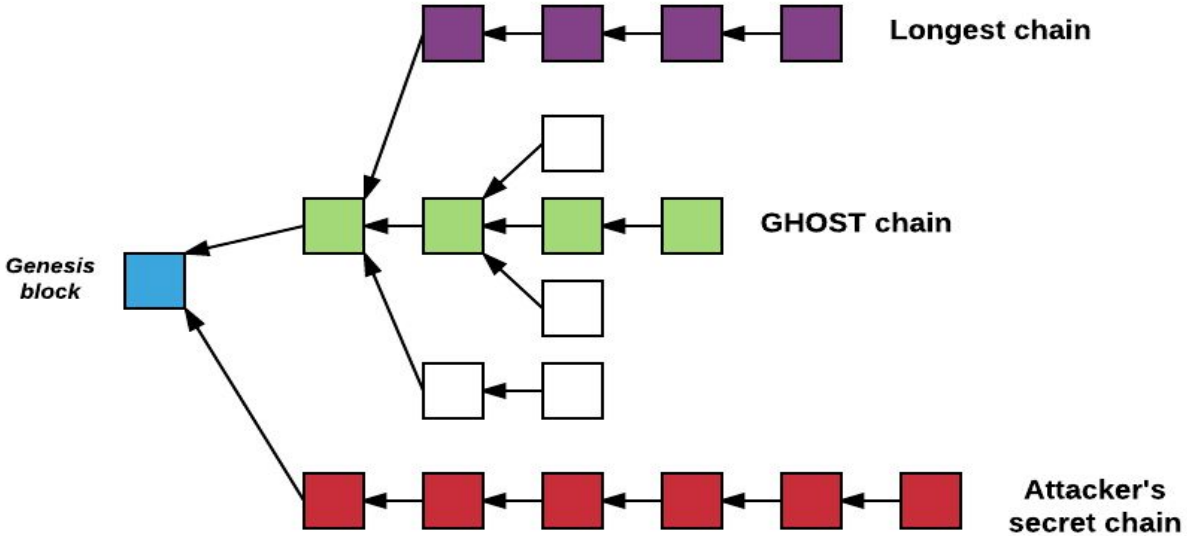
- **Vision:** a transaction-based state machine, or a virtual environment EVM, that runs distributed applications (Dapps).
  - Supports Turing-complete scripting language.
  - Global state, accounts, smart contracts, tokens, etc.

Ethereum

- Proposed by Vitalik Buterin in 2013 and went live in 2015.
- Users can issue two types of transactions: message calls and smart contracts deployment.
- Miners mine new blocks and implement smart contracts for clients.
  - Pay gas to prevent DoS against miners.
- The blockchain contains:
  - a full record of transactions,
  - smart contracts code,
  - and the global state of the network.
- Famously known to create new digital currencies on top of its platform called Ethereum Tokens.

Mining and Consensus in Ethereum

- Currently it adopts a PoW based mining algorithm.
  - Plans announced to move to Casper, a proof-of-stake based mining.
- Ethereum has higher block generation rate than Bitcoin, around a block every 16 sec.
- Does the longest chain concept still work?



Smart Contracts

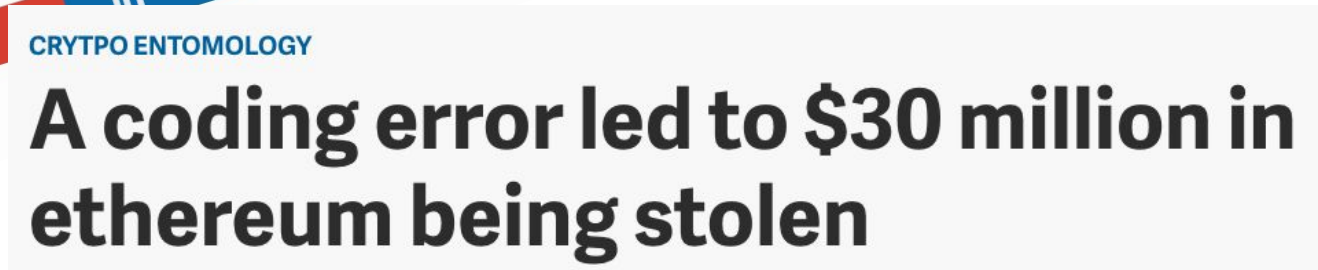
- Programs written in Ethereum scripting language, deployed on EVM and run by the miners.
- The full code of the smart contract and its current state are public on the blockchain.
- Once a contract is deployed, the contract owner cannot change its code.
  - Can ask the miners to destruct the contract (if it contains a function to do that) and deploy a new contract.
- Interacting with a contract is done by issuing transactions that invoke its functions.
- Each miner over the network implement the code of a smart contract but only one collects the gas cost.
  - The one who mines the next block.

Additional Features for Free?

- Security bugs in smart contracts.
- Gas cost (or transaction fees).
  - Limits the functionality scope of smart contracts.

Code was supposed to eliminate the need to trust humans. But humans, it turns out, are tough to take out of the equation.

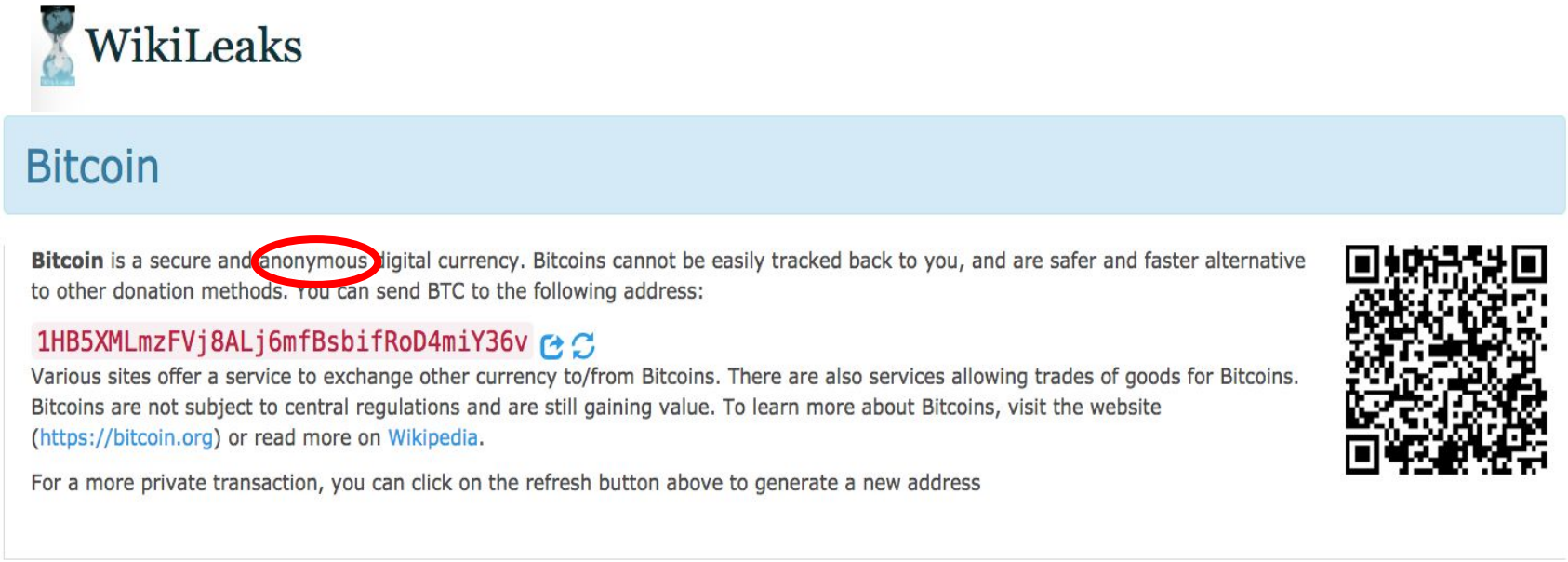
Source: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/



Anonymity

Is Bitcoin Anonymous?

- Believed to be, users are known by their public keys.
  - To protect privacy create new key pair for each new transaction.
  - Send the change to a new address each time.

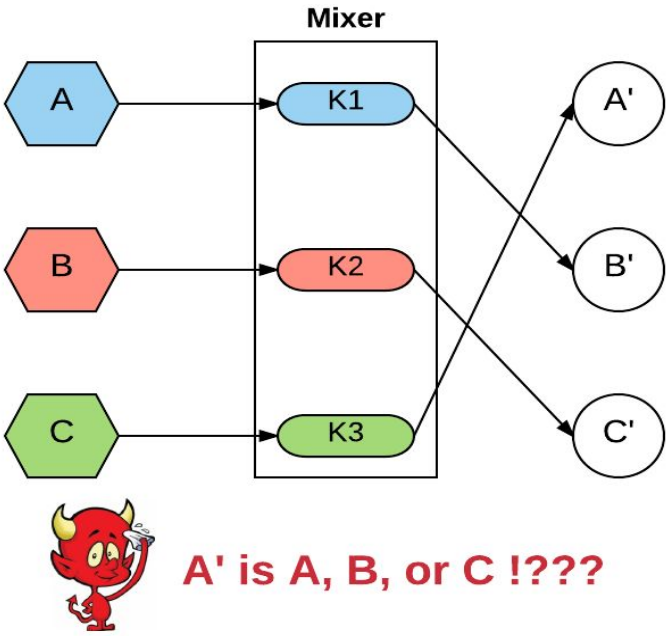


Source (accessed 11/23/2017): https://shop.wikileaks.org/donate

No, it is not ...

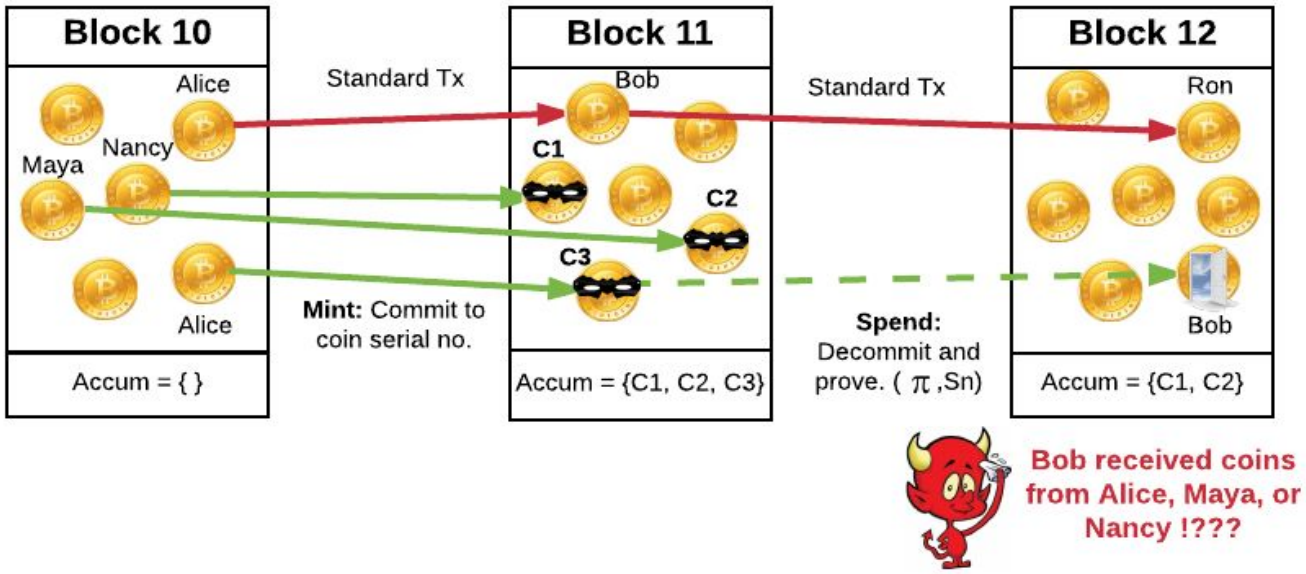
- Proved to be pseudo-anonymous:
  - The blockchain is public, track the flow of transactions.
  - Cluster Bitcoin addresses into entities, link them to identities and/or Bitcoin addresses posted by their owners on forums, etc., [Reid et al. 2014]
  - Link this flow to users' IPs based on Bitcoin protocol design [Koshy et al. 2014].
    - Track how the traffic is originated, a transaction source will broadcast this transaction several times to guarantee that it reaches miners. Same for destination.
    - Analyze these behaviors to link IP address to Bitcoin addresses.

Mixing



- **Goal:** Break transactions linkability.
  - This creates an anonymity set of the output.
- Will the mixer return the money back? Will it forget the mapping?
- **Mixcoin** [Bonneau et al., 2014]
  - Mixers issue warranties to customers.
  - Use a series of mixers to reduce the probability of local records risk.
  - Still linkable in several cases, does not guarantee anonymity.

Decentralized Mixer



Zercoin [Miers et al., 2013]:

- Distributed mixing.
- Utilize zero-knowledge proofs to prove that a coin with a specific serial number belongs to a set of Zerocoins on the ledger (anonymity set).
- Does not hide currency value or destination address.
- Computationally heavy.

Anonymous Cryptocurrencies

- Hide source, destination, and value.
- Example: Zerocash [Ben Sasson et al., 2014]:
  - Utilize zk-SNARKs (zero-knowledge succinct non-interactive argument of knowledge).
  - Mint and pour predicates to create and spend private coins.
  - Coins are tracked based on their sequence numbers that is revealed once it is spent.
  - More efficient than Zerocoin, but still requires a trusted setup.
  - Launched officially as Zcash in 2016.

Last Stop

Conclusions

- Cryptocurrencies provide a disruptive work model.
  - But also exhibit complicated relations between, financially motivated, untrusted parties.
- Great potential and huge arena of applications.
  - However, deeper thinking is needed to assess when/where to apply.
- Are they just a hype that will fade away?!
  - Still provide an elegant proof of concept.

Questions?

aNd ThANk yOU :)

References

[Nakamoto, 2008] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[Wood, 2014] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project Yellow Paper 151 (2014).

[Reid et al. 2014] Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." In Security and privacy in social networks, pp. 197-223. Springer New York, 2013.

[Koshy et al. 2014] Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In International Conference on Financial Cryptography and Data Security, pp. 469-485. Springer, Berlin, Heidelberg, 2014.

[Bonneau et al., 2014] Bonneau, Joseph, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. "Mixcoin: Anonymity for Bitcoin with accountable mixes." In International Conference on Financial Cryptography and Data Security, pp. 486-504. Springer, Berlin, Heidelberg, 2014.

[Miers et al., 2013] Miers, Ian, Christina Garman, Matthew Green, and Aviel D. Rubin. "Zerocoin: Anonymous distributed e-cash from bitcoin." In Security and Privacy (SP), 2013 IEEE Symposium on, pp. 397-411. IEEE, 2013.

Cont'd.

[Ben Sasson et al., 2014] Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized anonymous payments from bitcoin." In Security and Privacy (SP), 2014 IEEE Symposium on, pp. 459-474. IEEE, 2014.