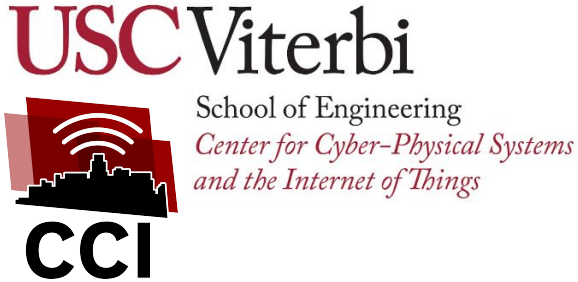


Blockchain Technology

Bhaskar Krishnamachari
Professor of Electrical Engineering and Computer Science
USC Viterbi School of Engineering
bkrishna@usc.edu

April 19, 2018, LA AITP meeting

HOW THE BITCOIN BLOCKCHAIN WORKS

1. Alice sends Bob some bitcoins, a digitally signed transaction.

2. This and other pending transactions are all broadcast to the whole network.

3. Miners around the world race each other to solve a “Proof of Work puzzle.”

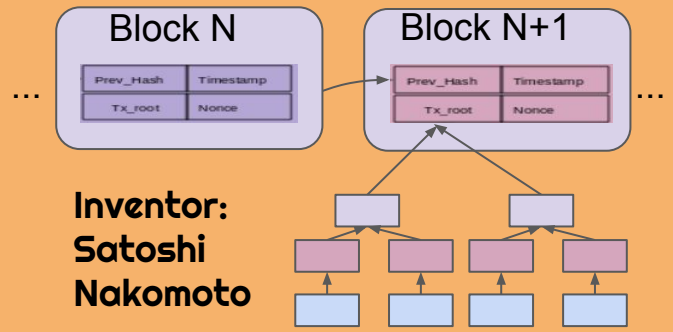
4. Winner combines several hundred pending transactions into a “block”, & collects fees. This happens every ~10 mins.

5. The new block is appended to the chain and broadcast to the whole network

6. In case of conflicts, the longest chain wins, i.e. is worked on; this results in consensus on which blocks are on the chain.

7. Any transaction that is 3-4 blocks into the blockchain cannot, for all practical purposes, be reversed

8. Bob can use wallet software to verify the transaction doesn’t involve Alice “double spending” her money.



Inventor: Satoshi Nakomoto

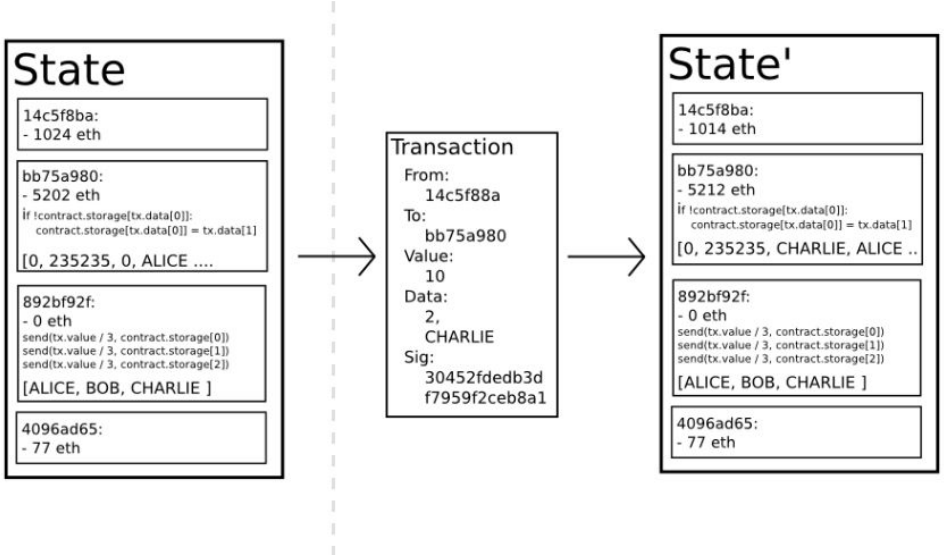
Distributed Ledger Technology

- A type of database to record transactions in chronological order (in the form of a blockchain), that is shared, replicated and synchronized

- Key Ingredients:
  - consensus to ensure that the shared ledgers are exact copies
  - digital signatures to validate original sender
  - Hashes to ensure records are tamper-evident

- Business benefits:
  - Can use in a business network spanning multiple organizations
  - Provides audit trail / provenance tracking
  - Immutable, tamper-proof ledger
  - Impartial dispute resolution: contract as code

Ethereum Smart Contracts



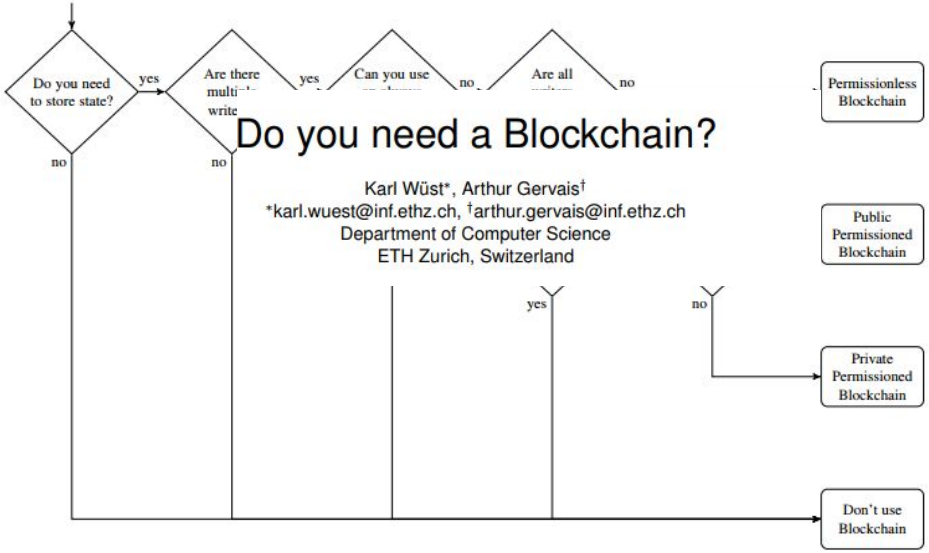
Ethereum innovated over Bitcoin by adding a Turing-complete computational model over it. The Ethereum Virtual Machine (EVM) allows the design and deployment of programmable “smart” contracts.

https://ethereum.org/
https://github.com/ethereum/wiki/wiki/White-Paper

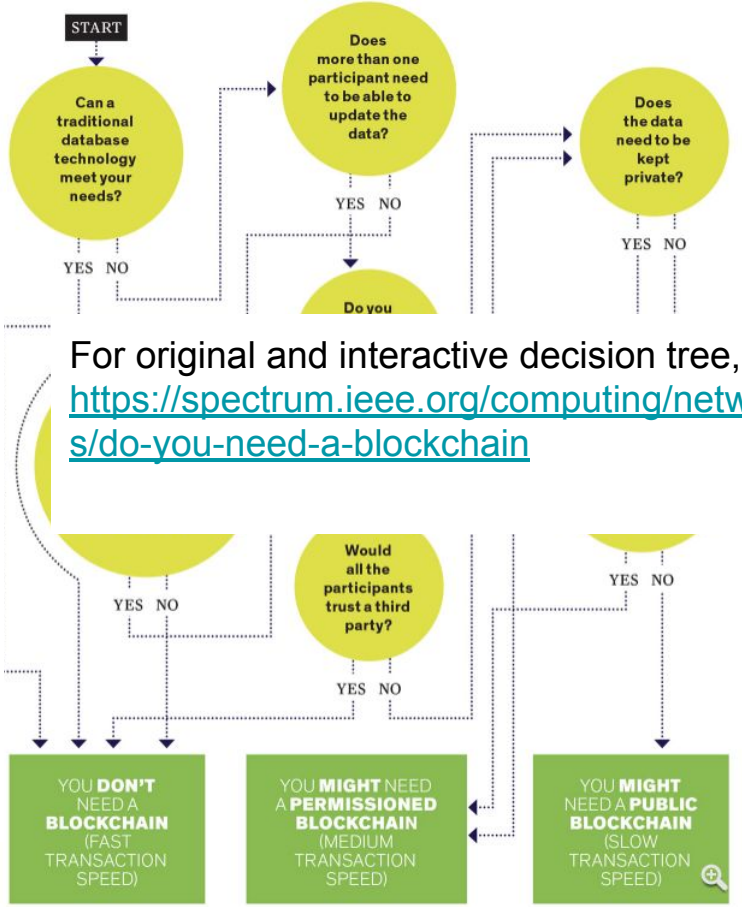
Types of Blockchain

Permissionless	Permissioned
Public	Private / Consortium / Public
Anonymous users	Identified users
Slow	Fast
Proof of work, Proof of stake, Proof of importance, Proof of time-elapsed	Consensus Protocols: PBFT, RAFT, Tendermint
Examples: Bitcoin, Ethereum, NEM, IOTA	Examples: Hyperledger Fabric, R3 (Corda), Ripple, Quorum

Do you need a Blockchain?



https://eprint.iacr.org/2017/375.pdf



For original and interactive decision tree, see https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

Problems with Proof of Work

- Computational Arms Race
- Not Green: huge electricity consumption

Bitcoin mining consumes more electricity a year than Ireland

Network's estimated power use also exceeds that of 19 other European countries, consuming more than five times output of continent's largest windfarm

- 51% attack: miners controlling 50% of the compute power can halt or even reverse transactions
- Slow

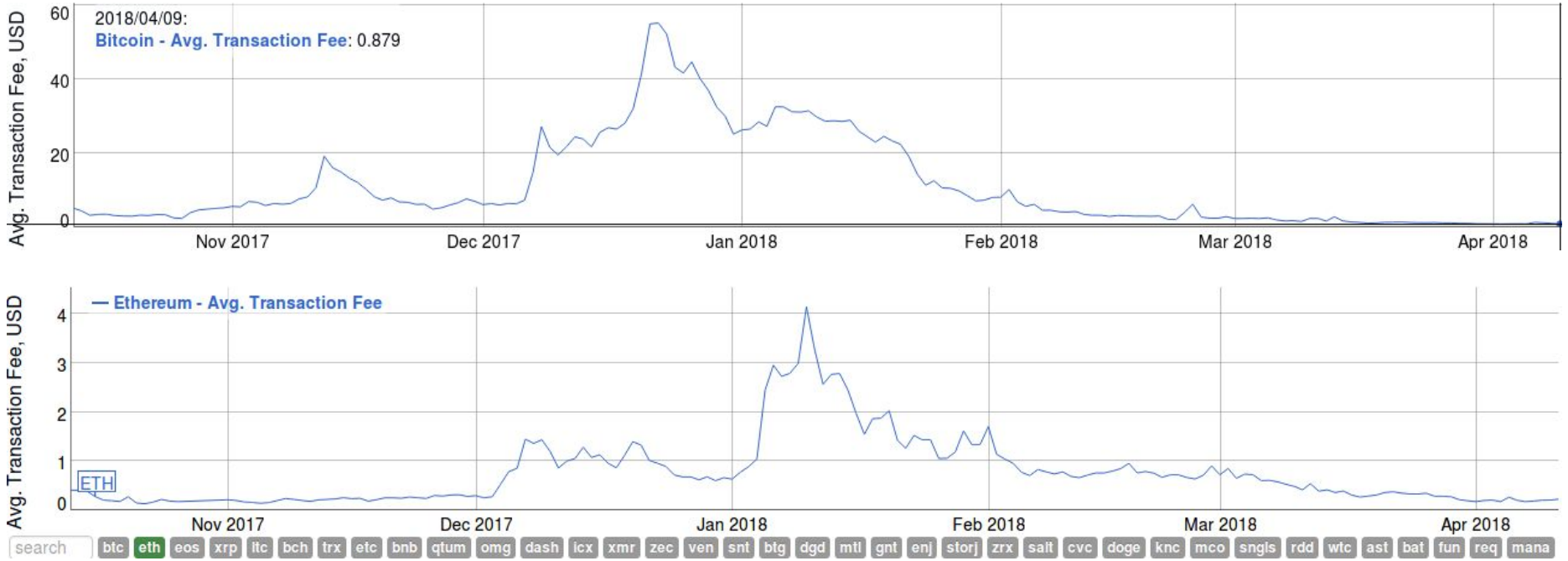
Emerging Alternatives to Proof of Work

- **Proof of Stake:** Mining power proportional to percentage of coins available. Someone with 51% stake in the coin would not have in their best interest to attack the network in which they hold the majority share. E.g.: Peercoin. Nxt, Blackcoin, and ShadowCoin. Ethereum slated to switch to PoS.

- **Proof of Importance:** Advocated by NEM. Every account is given an importance score. more coins, more transactions, reputation "measure of graph theoretic importance of the node in the transaction graph"

- **Proof of Elapsed Time:** Used in Hyperledger Sawtooth, contributed by Intel; uses SGX

Transaction Fees



Still too high..

Transaction Volume

VISA: 4000 tps
****
Hyperledger Fabric: 3500 tps
Ripple: 1500 tps
****
Paypal: 115 tps
****
Ethereum: 10-20 tps
Bitcoin: 7 tps
****

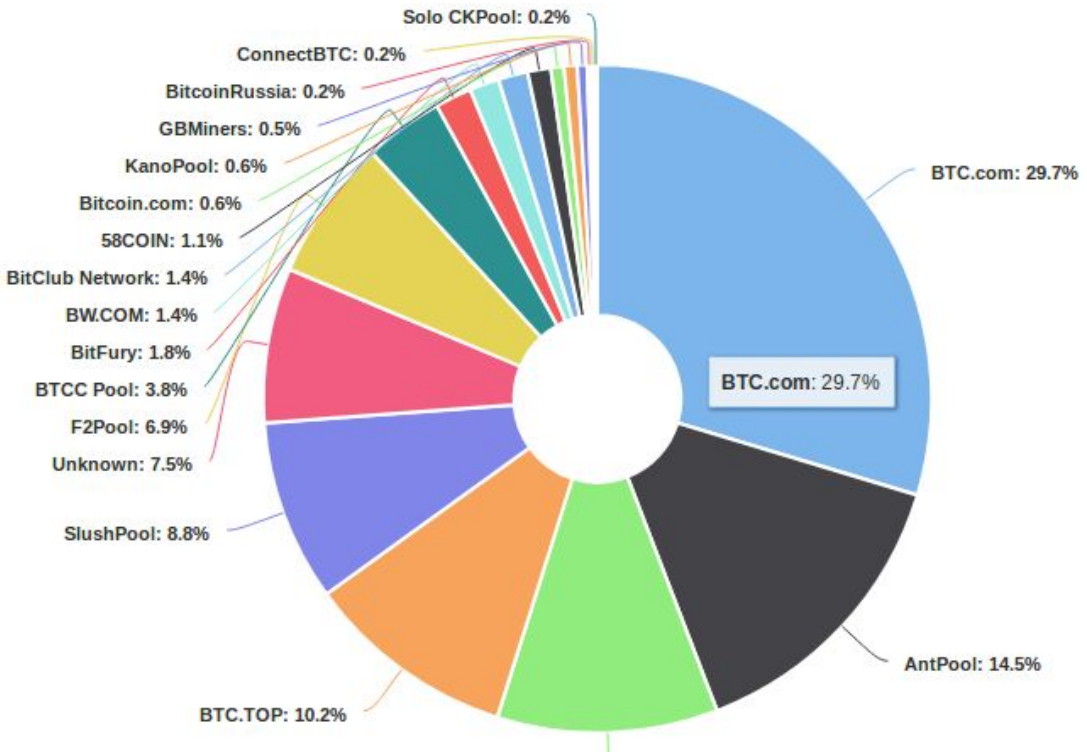
Permissioned blockchains offer high transaction rates, but are limited in size to dozen-odd nodes

Permissionless/open blockchains are large in size but have very low transaction rates

In part, per https://steemit.com/cryptocurrency/@steemhoops99/transaction-speed-bitcoin-visa-iota-paypal + https://ripple.com/xrp/

Centralization of Power

There is a tendency to bigger pool sizes to reduce variance of earnings from mining.. this could be viewed as a failure of the protocol.



Anonymity

Bitcoin - Who is Satoshi Nakomoto? But transaction graph is

Monero - ring signatures and mix-ins to improve anonymity

Zcash - uses zk-SNARK, which is an acronym for ‘zero-knowledge Succinct Non-interactive ARgument of Knowledge’, to provide anonymous transactions

BUT, how do these play with AML?
Standing for "Anti-money Laundering", it is a set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions. In most cases money launderers hide their actions through a series of steps that make it look like money coming from illegal or unethical sources was earned legitimately.
https://bitcointalk.org/index.php?topic=454795.0

- Large exchanges are responsible for implementing these

Software vulnerabilities

'$300m in cryptocurrency' accidentally lost forever due to bug

User mistakenly takes control of hundreds of wallets containing cryptocurrency Ether, destroying them in a panic while trying to give them back

Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong

Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist

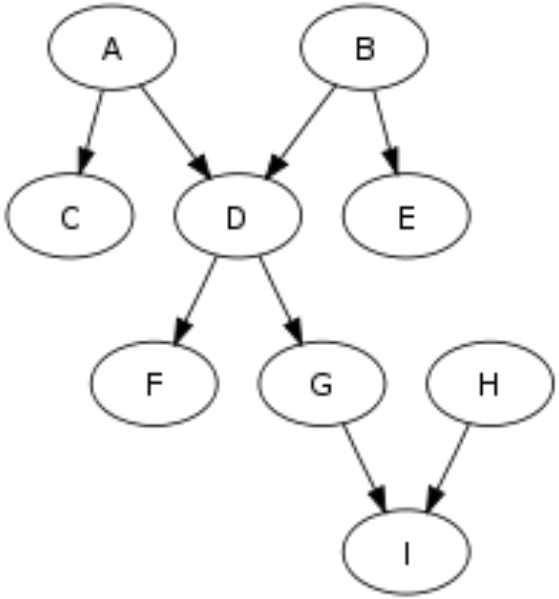
A $50 MILLION HACK JUST SHOWED THAT THE DAO WAS ALL TOO HUMAN

A hacker stole $31M of Ether—how it happened, and what it means for Ethereum

Is a linear chain the best solution?

DAG-based solutions:

- IOTA
- HashGraph



A Skeptical Voice

Blockchain is not only crappy technology but a bad vision for the future

- People have made a number of implausible claims about the future of blockchain, based on a misunderstanding of what a blockchain is.
- Tampering with data stored on a blockchain is hard, but it's false that blockchain is a good way to create data that has integrity.
- Blockchain systems are supposed to be more trustworthy, but in fact they are the least trustworthy systems in the world.

COMMENTARY

Kai Stinchcombe

Published 3:55 PM ET Mon, 9 April 2018

https://www.cnbc.com/2018/04/09/blockchain-is-not-only-crappy-technology-but-a-bad-vision-for-the-future.html

"A person who sprayed pesticides on a mango can still enter onto a blockchain system that the mangoes were organic."

"Projects based on the elimination of trust have failed to capture customers' interest *because trust is actually so damn valuable*. A lawless and mistrustful world where self-interest is the only principle and paranoia is the only source of safety is a not a paradise but a crypto-medieval hellhole."

Some Useful Resources

- Original Bitcoin paper: https://bitcoin.org/bitcoin.pdf
- A Blockchain Reading List from USC, Fall 2017: http://blockchain.usc.edu/index.php/blockchain-research-reading-group-fall-2017/
- Ethereum Solidity smart contract hello world, using remix: https://ethereum.stackexchange.com/questions/12348/hello-world-smart-contract-using-browser-solidity
- A good Hyperledger Composer tutorial using IBM Playground: https://ibm-blockchain.github.io/develop/tutorials/playground-tutorial.html
- Untangling Blockchain - a nice survey article of state of the art of blockchain as of 2017, from a data processing perspective: https://arxiv.org/pdf/1708.05665.pdf