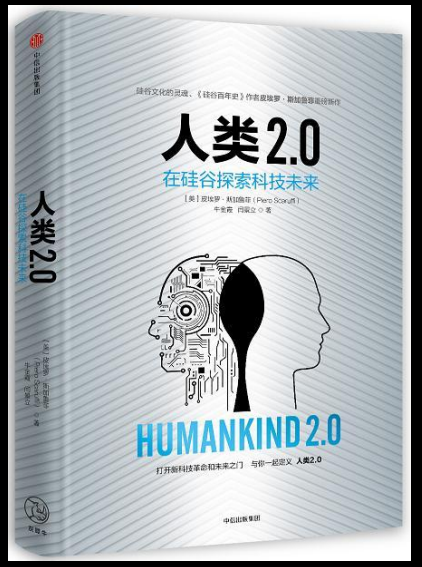
Blockchain Technology

Piero Scaruffi, 2018



https://www.scaruffi.com/singular/ppt/blockchain.pdf

Lesson #1

- Introduction to blockchain introduction and why it is a disruptive technology

The Historical and Sociological Context

- Society is an organized system of transactions
- You do things with others, and these things involve transactions: assets move from you to others and from others to you
- The invention of software allowed people to digitize information and communication, and to carry out invisible transactions (e-commerce existed before the Internet!)
- The invention of the World-wide Web allowed ordinary people to post, retrieve and search for information, and to shop online

The Historical and Sociological Context

- But there was always a intermediary (IBM, Microsoft, Amazon, eBay, Google, Facebook, PayPal…): the intermediary controls which transactions can be made and makes money out of the transactions
- The intermediary is always insecure: you give them a lot of personal data and they store it somewhere – easy to steal data
- The user is also untrustable: easy to make copies of digital goods (of data)

The Historical and Sociological Context

- Users cannot trust the intermediaries (too easy to steal data) and the intermediaries cannot trust the users (too easy to copy data)
- Boom of cryptography…
- …and of hacking!
- Escalating problems of privacy and security
- 2008: the global financial crash causes a loss of trust in the entire system of intermediaries

The Past and the Future

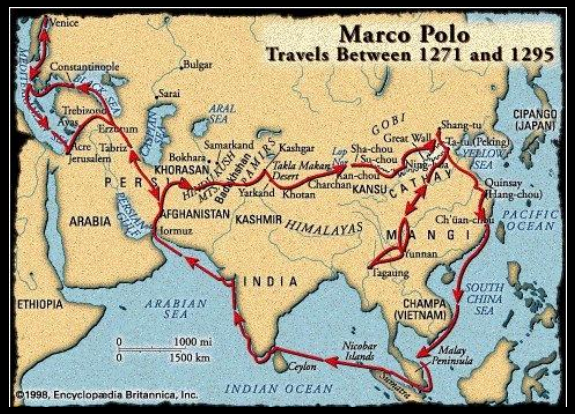
- The Internet (and all preceding networks) is a distributed "untrusted" network
- Trusted transactions depended on corporations motivated by profit (or on government agencies)
- Need for a distributed TRUST network
- Utopia: trusted transactions without a intermediary, directly between "peers", authenticated by peer collaboration and powered by collective computing

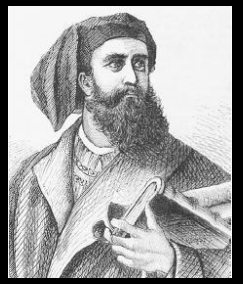
The Problem and the Solution

- Problem: how to build a global peer-to-peer trust network?
- Who found the solution? A kid who wanted to share music (illegally!) with friends (Napster) and a mysterious anarchist who wanted to get rid of governments

Historical Footnote

- Medieval Italy invented double-entry bookkeeping
- Italian trading cities needed to reorganize their society around physical transactions
- That invention reorganized society around transactions and led to capitalism and the nation-state

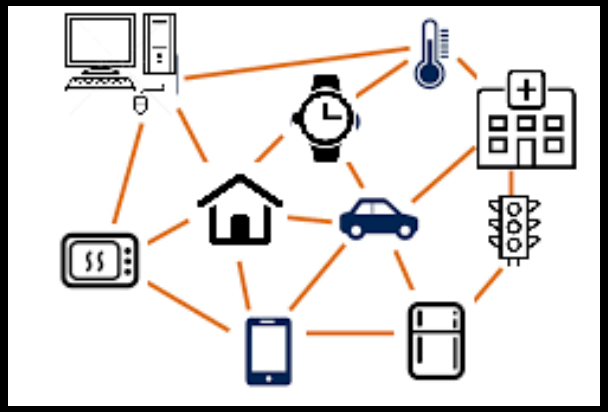


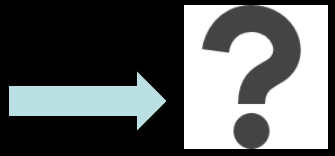


Marco Polo

Historical Footnote

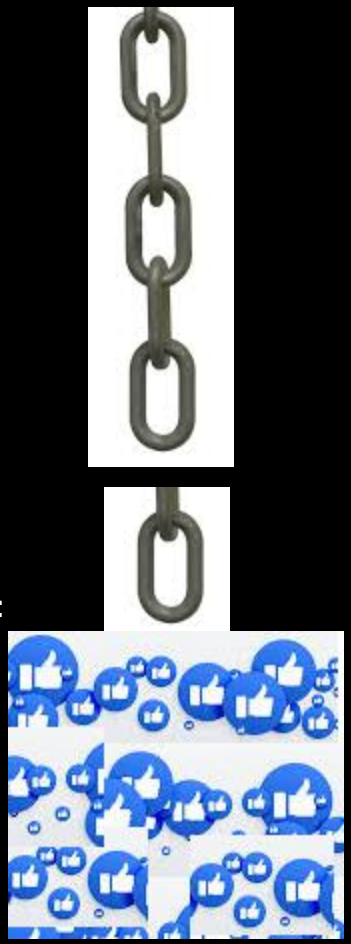
- The 21st Century needs to reorganize society around digital transactions
- Billions of smart devices need to share data
- The invention that solves this problem will change the next 500 years of history





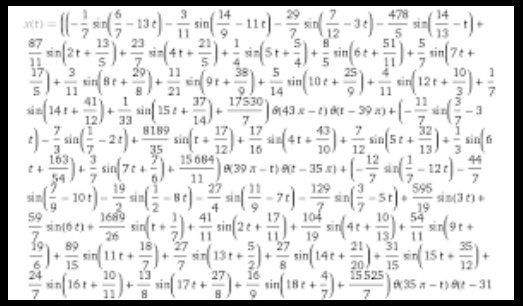
Blockchain

- A record of all transactions that take place in the world
- Every 10 minutes all new transactions are verified and stored in a block that is linked to the preceding block within a chain
- The blockchain is a history of the digital world, a history authorized by the digital world
- The blockchain guarantees a single version of the truth of any digital event



Blockchain

- The blockchain summarizes a network consensus of all transactions that ever occurred (consensus on the real history of the world)
- In order to add a block to the chain, the block needs to be validated by 51% of all the computers within the network
- Validation is cryptographic: a complex mathematical equation has to be solved
- If you want to cheat, you have to rewrite the entire history on the blockchain



Blockchain

- This digital history of the world's transactions can record every asset (birth certificates, deeds and titles of ownership, and, of course, money)

- Free gift to the people: transparency and accountability. (We can even record on the blockchain all the ingredients that went into your sandwich and you'll be able to know that the tomatoes come from Mexico, the wheat from Nebraska and the lettuce from California)

Fundamental Innovations

- Removing the counterparty (intermediary): blockchains are really good for automatically executing “contracts”
- The blockchain as a rewards engine for automatically dispensing tokens to those who do the work: token as a reward for a type of work that is provided, whether it is computational or human work.
- Decentralization: improved security, faster decision-making, fair distribution of benefits, fault-tolerance

Disruption at Multiple Levels

- Technical: beyond the database
- Business: tokenomics
- Legal: smart contracts

Lesson #2

- Bitcoin and the blockchain technology

What is the problem?

- We digitize information
- We distribute information
- How can we make sure that digital information is distributed but not copied?
- Originally, this was a problem of cryptography
- Meanwhile, P2P had created a way to easily copy and distribute digital information
- Then someone realized that you can use P2P to distribute information in a way that makes it impossible to copy it!
- Decentralization

Cryptography

- Public key cryptography
  - A method for establishing a key without using a prior shared secret
  - 1973: Clifford Cocks' encryption algorithm (Oxford)
  - 1976: Whitfield Diffie and Martin Hellman's key exchange (Stanford)
  - 1978: Ron Rivest, Adi Shamir and Leonard Adleman's RSA encryption (MIT)

Cryptography

- Public key cryptography
  - 1994: Netscape introduces the Secure Sockets Layer (SSL) protocol
  - A pair of keys – one private, one public – to authenticate, secure and manage secure connection

Cryptography

- Post-quantum cryptography
- Zero-knowledge proofs
- Indistinguishability obfuscation
- Secure multi-party computation
- …
- Blockchain

Makart Steg in Salzburg
With thousands of love padlocks

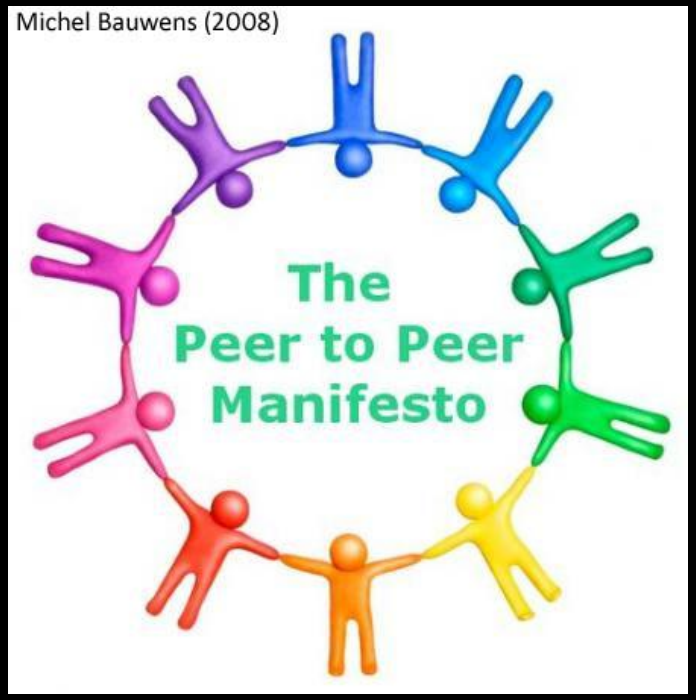
The Peer-to-peer World

The Peer-to-peer World

The Peer-to-peer World

- 1999: Shawn Fanning’s Napster (P2P)
- 2000: Jim McCoy's MojoNation (a cybercurrency that is not for money)
- 2000: Justin Frankel's Gnutella (truly P2P, totally decentralized)
- 2002: Bram Cohen's BitTorrent
- 2002: "The Darknet and the Future of Content Distribution"

The Peer-to-peer World



Cypherpunk Movement

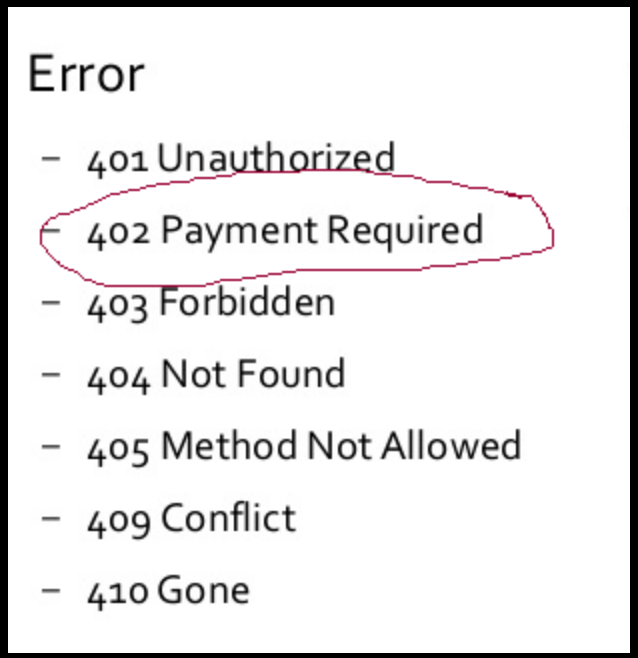
- 1992: Timothy May's Crypto Anarchist Manifestoand cypherpunk mailing list

Cybercurrency

- DigiCash (David Chaum, 1990)
- E-gold (Douglas Jackson, 1996): 5 million users by 2009 - shut down by the USA
- WebMoney (Russia, 1998)
- Tencent's qq coins (China, 2005) - shut down by China
- Liberty Reserve (Costa Rica, 2006) - shut down by the USA
- Perfect Money (Andrew Draper, Switzerland, 2007)
- Bitcoin (2009) - decentralized!

Cybercurrency

- 402 error code never implemented



Cybercurrency

- Cynthia Dwork (1992): punish spammers with computational processing, i.e. comp. processing is a cost (proof of work)
- Adam Back (1997): hashcash (cryptographic hash functions on a network, no need for central authority)
- Nick Szabo (1997): a distributed trust model (“The God Protocol”, 1998)
- Wei Dai’s mathematical method for an unbreakable cybercurrency (1998)
- Miguel Castro and Barbara Liskov (1999): Practical Byzantine Fault Tolerance





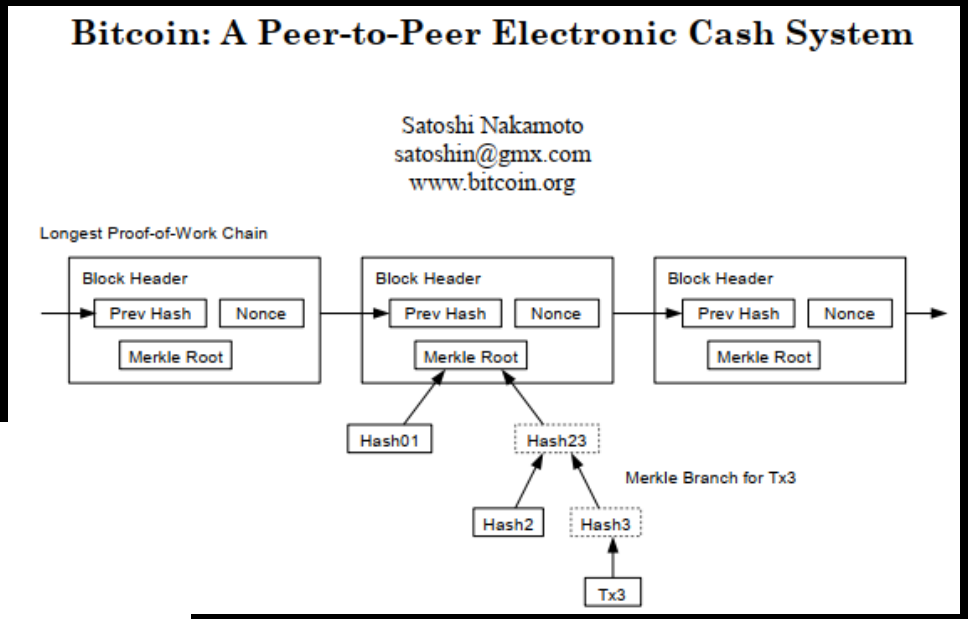
Cybercurrency

- Satoshi Nakamoto (Oct 2008): paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System" on the Metzdowd Cryptography mailing list
- Satoshi Nakamoto (Jan 2009): the cryptocurrency Bitcoin
- Satoshi Nakamoto sends 10 bitcoins to Hal Finney (Jan 2009)
- Dave Kleiman & Craig Wright: Nakamoto?

Craig Wright

Cybercurrency

- Satoshi Nakamoto (2009): first release of Bitcoin



http://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html

Bitcoin v0.1 released

Satoshi Nakamoto satoshi at vistomail.com
Thu Jan 8 14:27:40 EST 2009

```
Announcing the first release of Bitcoin, a new electronic cash
system that uses a peer-to-peer network to prevent double-spending.
It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar
```

Cybercurrency

- Martti Malmi (2009): second release
- Gavin Andresen (2012): Bitcoin Foundation

Author | Topic: Bitcoin 0.2 released! (Read 26270 times)

satoshi
Founder
Sr. Member

Activity: 364
Merit: 1509

Bitcoin 0.2 released!
December 16, 2009, 10:45:36 PM #1
Merited by OgNasty (1), HI-TEC99 (1), hakka (1)

Bitcoin version 0.2 is here!

Download links:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.2.0-win32-setup.exe/download
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.2.0-win32.zip/download
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.2.0-linux.tar.gz/download

New Features

Martti Malmi
- Minimize to system tray option
- Autostart on boot option so you can keep it running in the background automatically
- New options dialog layout for future expansion
- Setup program for Windows
- Linux version (tested on Ubuntu)

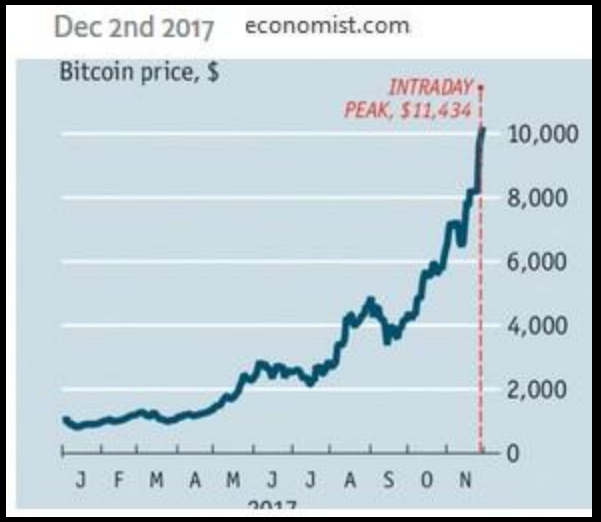
Satoshi Nakamoto
- Multi-processor support for coin generation
- Proxy support for use with TOR
- Fixed some slowdowns in the initial block download

Cybercurrency

- Bitcoin (2009)
  - The first successful currency not to be printed by a government
  - A system capable of creating copies that cannot be copied
  - Peer-to-peer
- Bitcoin's distributed blockchain mechanism makes central authorities of trust obsolete
- Virtually invulnerable to hacking (unlike government databases)

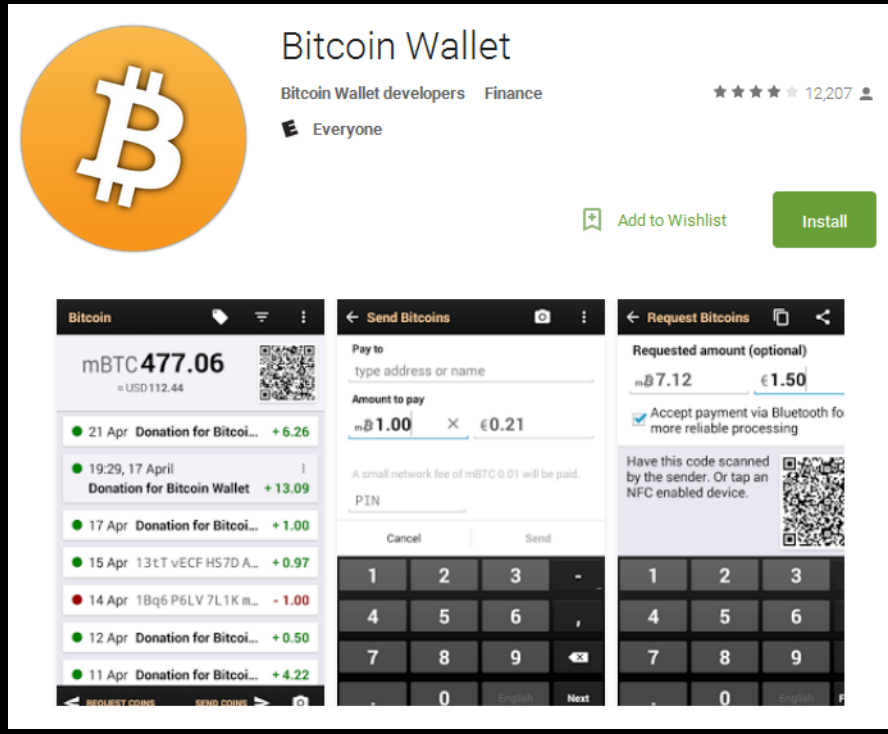
Cybercurrency

- Jan 2017: Bitcoin surges past $1000 for the first time in 3 years
- Dec 2017: Bitcoin surges past $10,000 for the first time

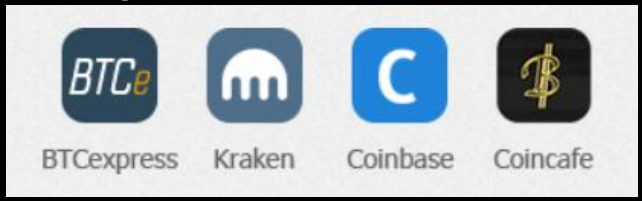


How does Bitcoin work?

1. Download a software wallet app

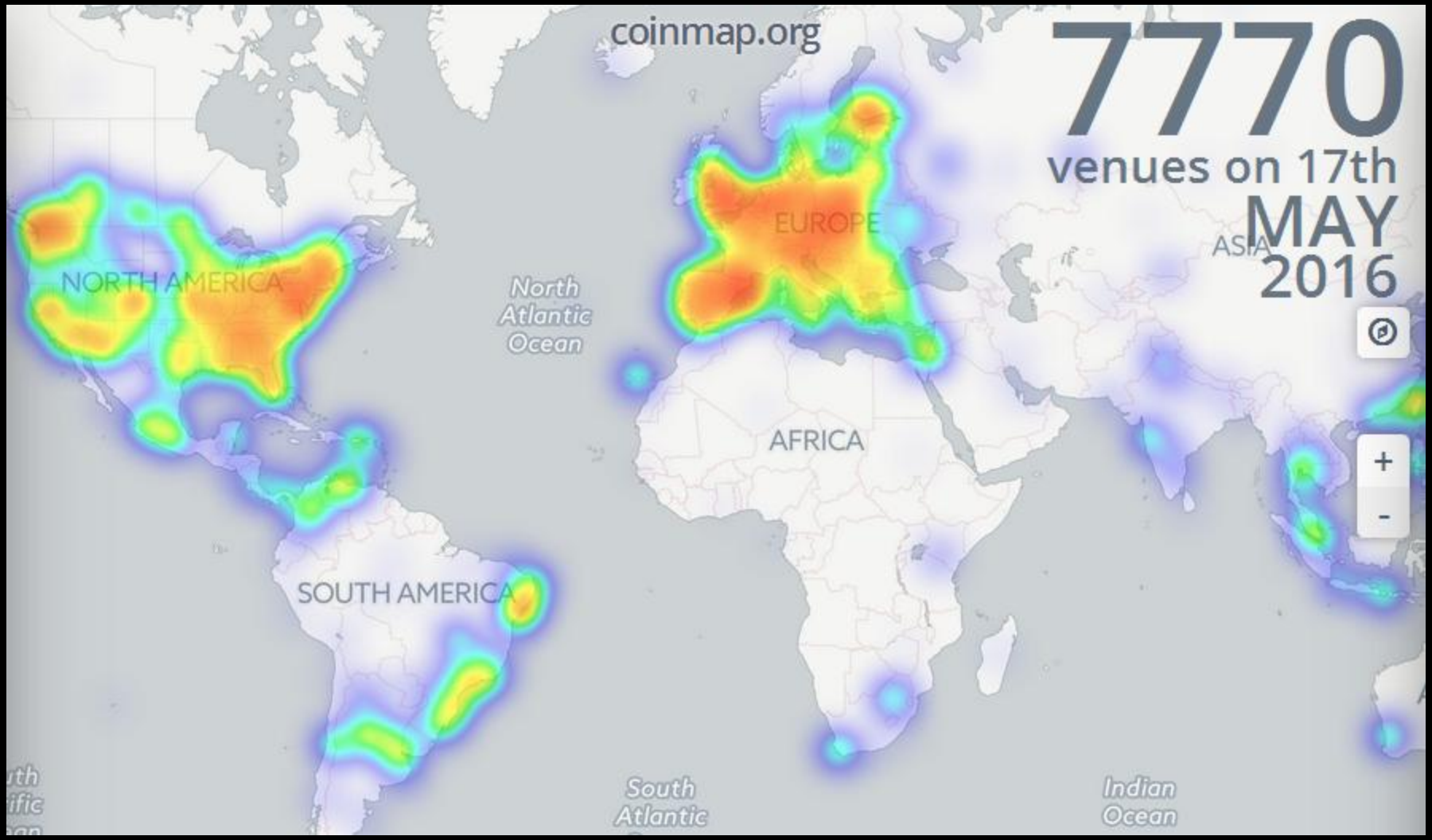


2. Buy bitcoins



3. Spend bitcoins

Where can I use Bitcoin?

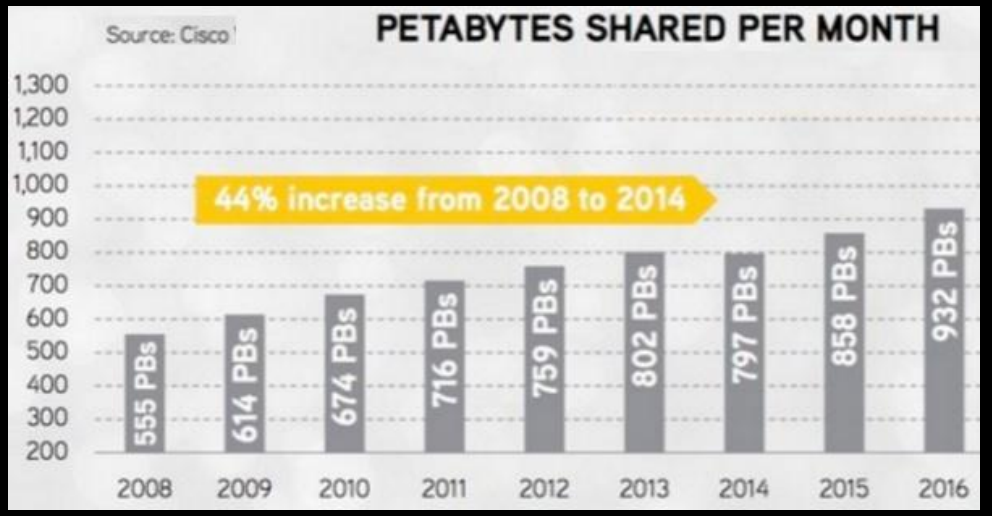


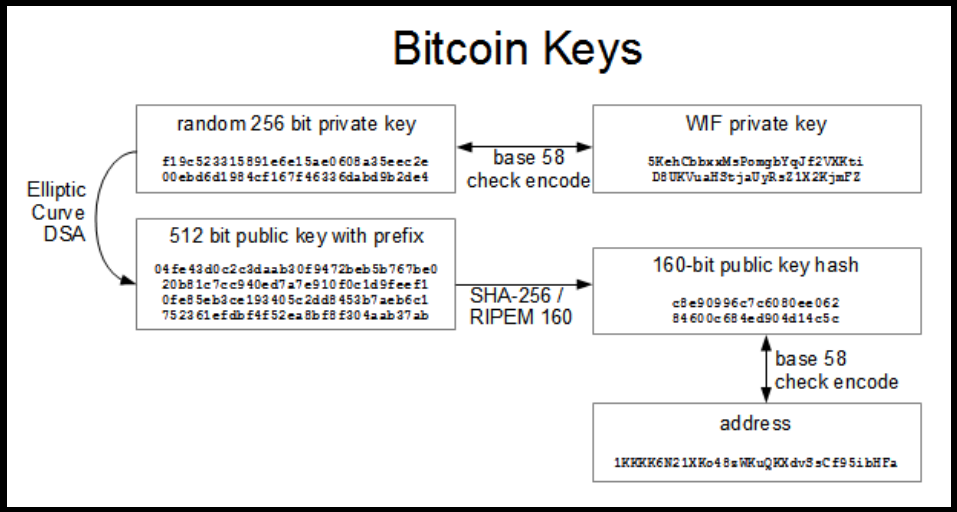
Bitcoin

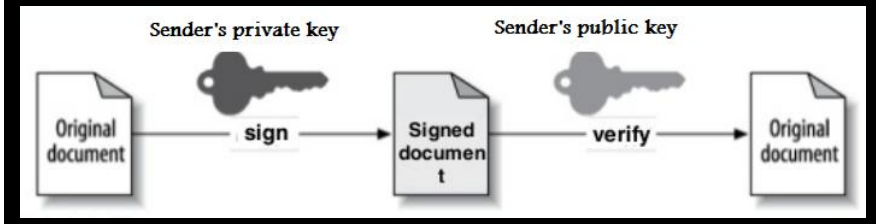
- Dec 2017: listing on the Chicago Board Options Exchange (CBOE) causes boom of cyrptocurrencies

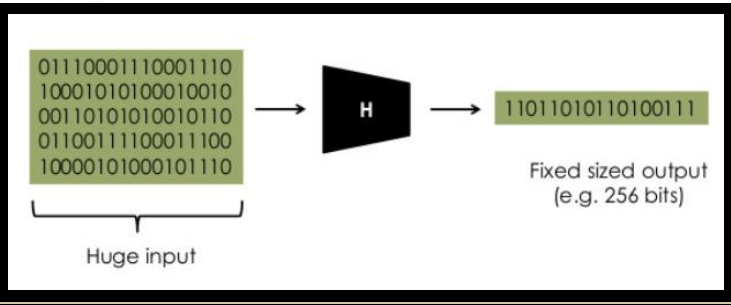
Bitcoin

- Enabling technologies:
  - distributed file sharing,
  - digital signature,
  - hashing,
  - and… blockchain









Lesson #3

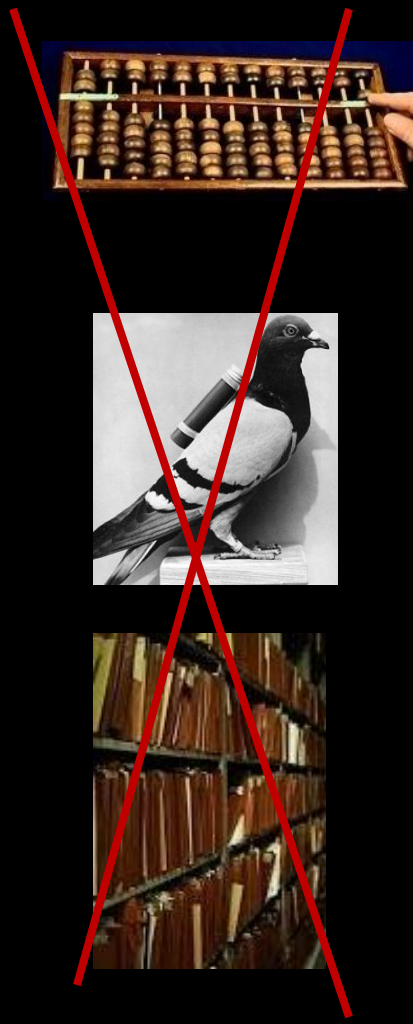
- Blockchain

Blockchain

- The missing disruption
- The world runs on three processes: storage, computation, and communication.

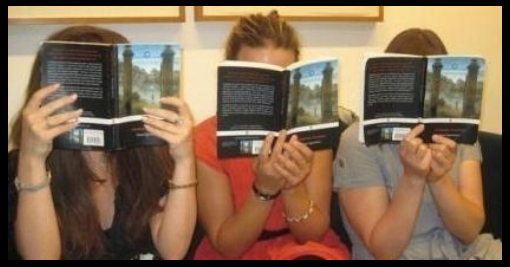
Blockchain

- The personal computer disrupted computation.
- The Internet disrupted communications.
- Blockchain disrupts storage.



Blockchain

- The blockchain is the main innovation of Bitcoin
- A blockchain contains every transaction ever executed in the currency
- The network shares a transaction book (or public ledger)
- Double-spending of bitcoins impossible
- In order to add a new block to the Bitcoin blockchain, a Bitcoin “miner” must include a “proof of work”



Blockchain

- The blockchain
  - a distributed electronic ledger that records all the transactions that happen on the network
  - similar to a relational database
  - an unchangeable record of all transactions (“blocks”)
  - a true and verifiable record of each and every transaction ever made in the network
  - no need for an administrator
  - "This is TCP/IP applied to the world of business and transactions" (Karim Lakhani, Harvard Univ)

Blockchain

- Public blockchains: anyone can see and send transactions
- Private blockchains: only some organizations can create a record in the blockchain (e.g. a group of banks use the blockchain and each node is associated with a step in their transactions)

Blockchain Technology

- The stack:
  - Blockchain (blocks maintained and replicated by thousands of nodes)
  - Protocol (designed and maintained by the open-source Bitcoin community or Ethereum or other community)
  - Token (what are you exchanging? money? cars? houses?)
  - Applications (wallets, services,etc)

Mining

- The process of adding transaction records to the public ledger
- “Proof of work”: a computing task that is costly to execute but easy to verify (SHA-256 computations)
- Bitcoin mining implements a distributed consensus system
- Custom-built supercomputers are needed for parallel processing

Mining

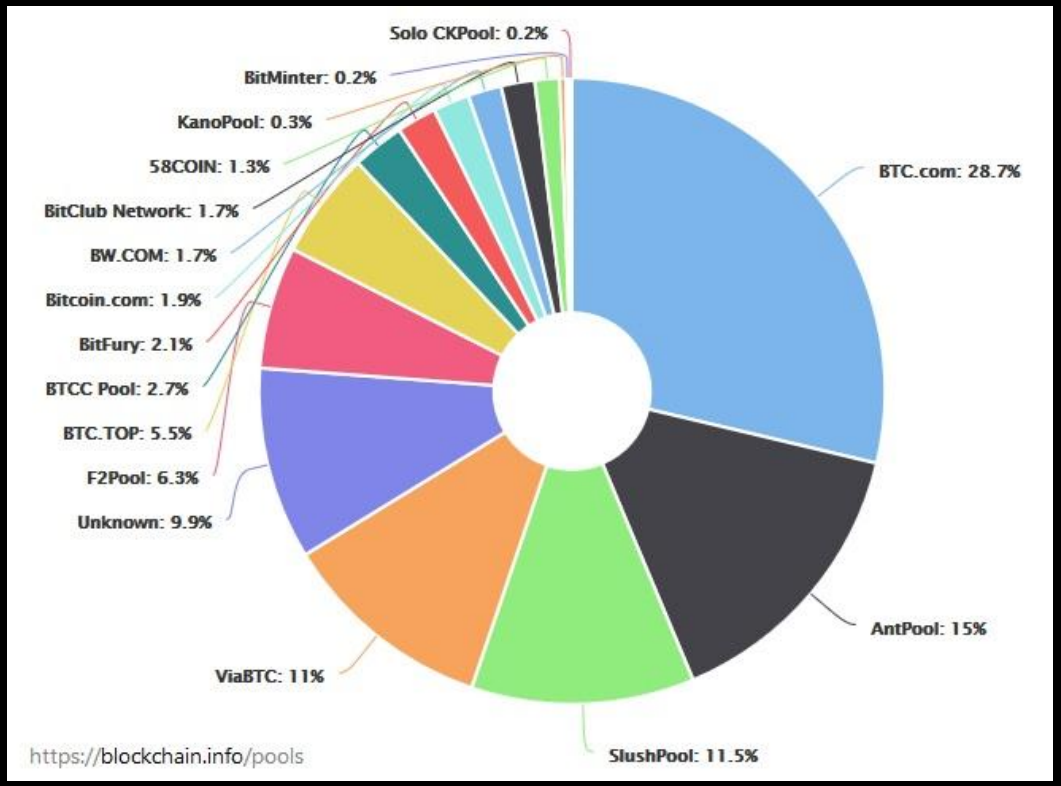
- Canaan Avalon (China,2012): the first ASIC mining chip
- BitFury (San Francisco, 2011): 16nm “green” ASIC chip that can deliver 100 gigahash per second (2015)
- **21** (San Francisco, 2013): embeddable bitcoin mining chip (2013) and the first computer with native hardware and software support for Bitcoin (2015)
- Bitmain (China, 2013): Antminer

Mining

- BitFury
- Bitmain (China, 2013)

Mining

- The richer you are the richer you get
- In 2018 just three mining pools created more than 50% of bitcoins



Lesson #4

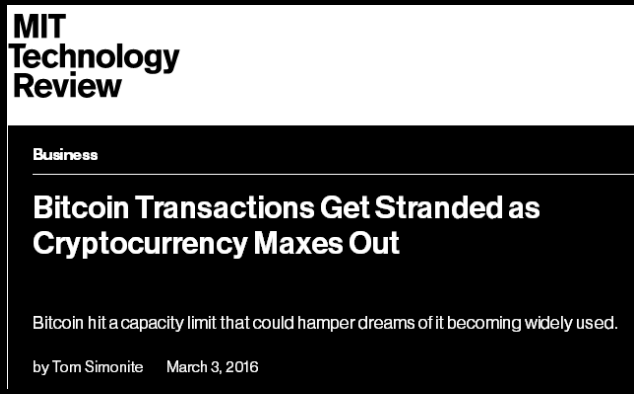
- The issues and the alternatives

Bitcoin issues

- A world currency administered not by a central bank but by
  - Developers, whose software determines how the currency is created and used
  - Miners, whose computers mint the currency

Bitcoin issues

- Bitcoin transactions take an average of ten minutes to be confirmed
- Scalability: capable of processing only seven transactions per second.
- Bitcoin runs on open source software



MIT Technology Review

Business

Bitcoin Transactions Get Stranded as Cryptocurrency Maxes Out

Bitcoin hit a capacity limit that could hamper dreams of it becoming widely used.

by Tom Simonite March 3, 2016

Bitcoin issues

- Solution: increase the block size - the Bitcoin XT fork (Mike Hearn and Gavin Andresen, 2014)… but all the computers on the bitcoin network must install a new version at the same time!
- Solution: SegWit optimization (Pieter Wuille, 2015, adopted 2016) that increases the volume of transactions fitting into a block without increasing the block size (1 Mbyte)
- Solution: 2 Mbyte block size (up from the original 1 Mbyte) + "segregated witness" code optimization – the Segwit2x fork (Jeff Garzik, 2017)

Bitcoin issues

- Skyrocketing transaction fees of bitcoin
- Solution: Bitcoin Cash (BCH) with a blocksize limit of 8Mbytes allowing for ~2,000,000 transactions per day (versus Bitcoin's blocksize limit of 1 Mbyte allowing for ~250,000 transactions per day)
- August 2017: Bitcoin Cash (BCH) forks from Bitcoin (BTC)
- Bitcoin Cash (BCH) is more spendable than Bitcoin (BTC)

BCH evangelist Roger Ver

Bitcoin issues

- November 2018: Jihan Wu's Bitmain and Haipo Yang's ViaBTC (Bitcoin ABC - BCHABC) vs Craig Wright's nChain and Calvin Ayre'sCoinGeek (Bitcoin SV - BCHSV)

Bitcoin ABC lead developer Amaury Séchet

Alternative Cryptocurrencies

- “Colored” currencies: user-issued currencies running on the bitcoin protocol
- More than 70 in 2015
- Cryptsy, the largest altcoin exchange, lists hundreds of cryptocurrencies
- Omni/Mastercoin (JR Willett, 2013) uses the same blockchain as Bitcoin

Cryptsy Markets

24 Hour Volume

Display Markets: All BTC LTC

Market	24hr Vol BTC	Price
LTC/BTC	243.59198824	0.01074350
DOGE/BTC	116.54566712	0.00000035
DASH/BTC	90.21066788	0.00601221
BTC/USD	79.00119318	413.53126891
ETH/BTC	61.66069621	0.00195472
LTC/USD	50.60971200	4.44000000
XRP/BTC	24.85799690	0.00001250
EAC/BTC	22.81309278	0.00000011
DGB/BTC	17.62607422	0.00000106

Alternative Cryptocurrencies

- Different “proof of work” algorithms than Bitcoin’s SHA-256 (hence do not use Bitcoin’s blockchain):
  - Litecoin (former Google engineer Charles Lee, 2011, second for market capitalization in 2015, a 333% increase in value in Dec 2017)
  - PPCoin/Peercoin (“Sunny King”, 2012) to replace mining with a less costly (“green”) alternative, i.e. to reduce energy consumption of mining

litecoin

Peercoin

Alternative Cryptocurrencies

- Proof of Stake (POS)
  - PPCoin/Peercoin (“Sunny King”, 2012) to replace mining with a less costly (“green”) alternative, first cryptocurrency to implement PoS
  - Evolved into Primecoin (“Sunny King”, 2013)
  - 2013: “BCNext”'s NXT, second based on POS: a platform to build financial applications

Alternative Cryptocurrencies

- Proof of Stake (POS)
  - 2014: Jae Kwon's Tendermint = Practical Byzantine Fault Tolerant (PBFT) – based PoS
  - 2015: Vlad Zamfir's Casper the Friendly Ghost, the first "chain-based PoS"

Mining

- ‘Green’ mining projects
  - Primecoin
  - Foldingcoin
  - Gridcoin
  - Zennet
- Cloud-based mining: Genesis

Bitcoin Banking

- Cook Investment Firm (Andrew Cook, Chile, 2011): world's largest bitcoin investment fund (he founded it when he was 20)
- Epiphyte (San Francisco, 2013): banking with crypto-currencies
- NextBank (2015): the first all-bitcoin institution

epiphyte

NEXT BANK PROJECT

Bitcoin Payment

- CoinBase (San Francisco, 2012): bitcoin wallet – cryptocurrency exchange
- Circle (Ireland, 2013): sending bitcoins to friends and family
- Quickcoin (San Francisco, 2014): a Facebook-Integrated bitcoin wallet to send bitcoins as messages

Bitcoin BTM

- CoinCloud (Menlo Park, 2014): trading bitcoins for cash

Life in the Bitcoin world

- Exchange dollars for bitcoins and viceversa: Coinbase (San Francisco), Gemini (New York), Binance (Canada)

Life in the Bitcoin world

- Personal wallet: software or hardware
- Software (“hot” wallet): Mycelium, Breadwallet, Copay.io and Jaxx.io
- Hardware: Keepkey, Trezor, Ledger
- Spend bitcoins, e.g. Purse.io that allows to buy Amazon goods

Blockchain Banking

- BitShares/ Invictus Innovations (Daniel Larimer, Virginia, 2013): financial services (including exchange and banking)
  - a ledger to track ownership of digital assets
  - based on blockchain but not the Bitcoin blockchain
  - delegated Proof of Stake (PoS) algorithm
  - Graphene: open-source blockchain implementation in C++

Blockchain goes mainstream

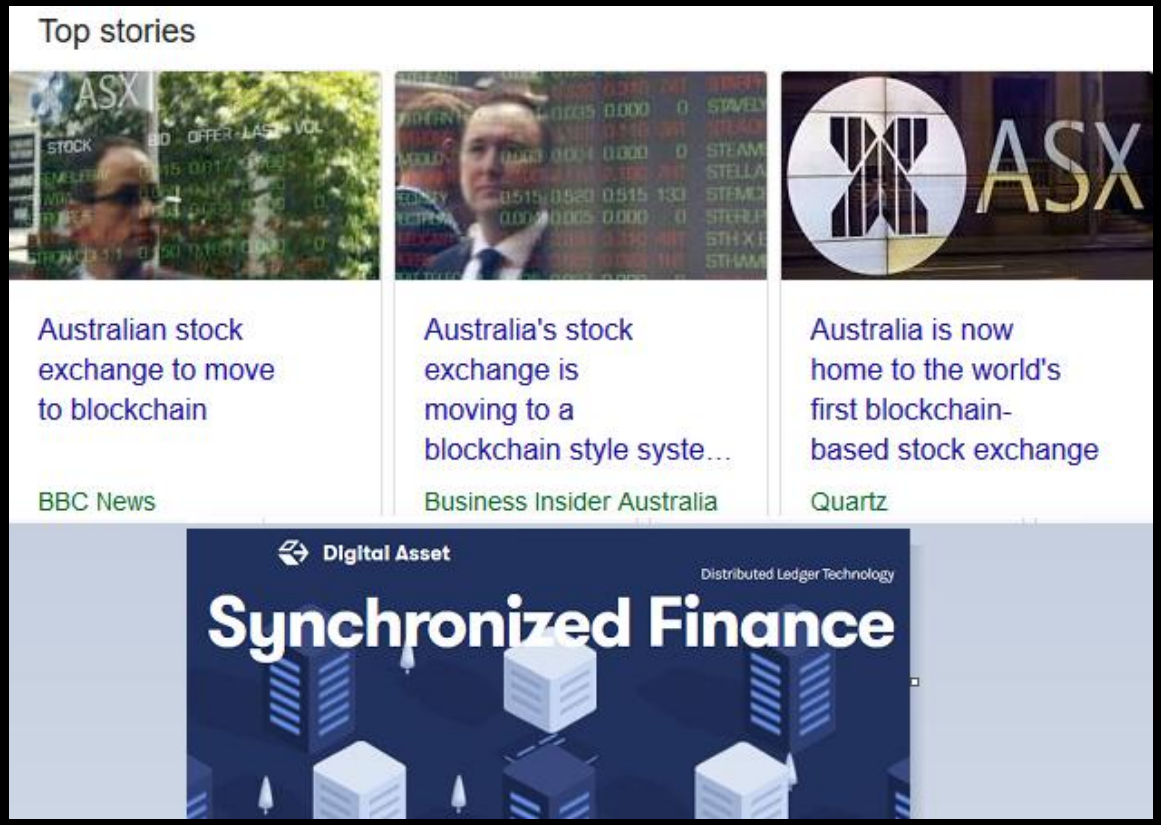
- 2017: Mastercard adopts blockchain technology for cross-border payments (no cryptocurrency though)
- 2017: IBM cross-border payments in the South Pacific (using Stellar's cryptocurrency Lumens)
- J.P. Morgan's Interbank Information Network (IIN): a blockchain payments network for cross-border payments

Blockchain goes mainstream

- R3 Partnership (2015): consortium of 45 of the biggest financial institutions (using Corda)
- Utility Settlement Coin (2016): consortium of banks (UBS, Barclays, CIBC, Credit Suisse, HSBC, MUFG, BNY Mellon, Deutsche Bank, Santander, NEX) to develop the digital counterpart of each of the major fiat currencies so that business transactions can be processed in real-time.

Blockchain goes mainstream

- 2017: Australian Stock Exchange (collaboration with Digital Asset)



Blockchain goes mainstream

- 2016: $1 billion invested by Wall Street

Lesson #5

- Smart contracts

Smart contracts

- Physical and intellectual property can be registered and transacted via blockchains as *smart property*

Smart property = property whose ownership is controlled via the Bitcoin blockchain

- Nick Szabo (1997): any contract (even governance) can be implemented as self-executing *smart contracts*

Smart Contract = a program stored on the blockchain that can automatically execute the terms of a contract (Ripple Lab's Codius and Ethereum)

Smart contracts

- A smart contract is a program stored on the blockchain that can automatically execute the terms of a contract.
- With smart contracts, auto-executing code replaces the legal process of enforcing a contract.
- Smart contracts make the legal system redundant.

Smart contracts

- Today it takes a specialist to verify a contract and usually the proof is some kind of official (and expensive) certificate.
- In a future driven by blockchain, we will simply perform a search operation, just like today we search with Google or Baidu for some information, and we will simply email the "certificate" that we found with that search.
- Sorry for the attorneys, but there will be no need for filing patents or wills.

Smart Contracts

- Decentralization had historically meant chaos, but blockchain is a system based on decentralization that actually guarantees order.
- It sounds like a contradiction, but its technology is basically order enforced through chaos.

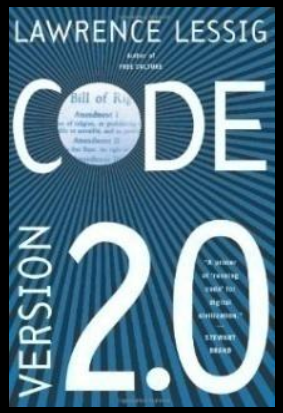
Smart Contracts

- Agreements between parties posted to the blockchain for automated execution
- Every contract in human societies can be reduced to a math problem
- Smart contracts model patterns of interaction in society
- A whole new dimension for blockchain technology (eg Ethereum)

The world's first Blockchain marriage: David Mondrus and Joyce Bayo (October 5, 2014, Disney World)

Smart Law

- The traditional world: legally-binding
  - Flexible interpretation of the law, rhetorical power of attorneys
- The blockchain world: technologically-binding
  - Software inexorably executes the contract no matter what
- Auto-executing code replaces lawyers, courtrooms, judges and prisons
- No need for a legal system if the world moves to smart contracts



Smart Contracts

- Notary Service to register documents
  - Proof of Existence (2014)
  - Factom (Texas, 2014)
  - Empowered Law (Chicago, 2015)

Proof of Existence

factom

Factom is a system for securing millions of realtime records in the blockchain with a single hash

Empowered Law

Smart Contracts

- Register and transact IP (intellectual property): Monegraph, Ascribe, …
- Helping artists and writers protect their work from copyright infringement
- Easier than registering a work with the Library of Congress

Smart Contracts

- Music Industry
  - Blockchain can usher in a new era of digital rights management (DRM)
  - Blockchain can reinvent the music and media industry
  - No more piracy
  - Liberate musicians from music labels and streaming services

Smart Contracts

- Music Industry
  - PeerTracks: an “artist equity trading system”
  - Bittunes: an “independent music market”
  - Ujo Music: global royalty distribution and licensing

Smart Contracts

- Medical records
  - MedVault (2015): to record medical information on the bitcoin blockchain
  - Factom's partnership with medical services provider HealthNautica (2015)
  - DeepMind (?)

Smart Contracts

- Medical records

Verifiable Data Audit

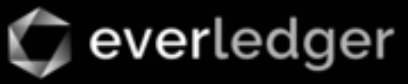
DeepMind's New Blockchain-Style System Will Track Health-Care Records

March 9, 2017

Alphabet's artificial intelligence outfit, DeepMind, plans to build a blockchain-style system that will carefully track how every shred of patient data is used.

Blockchain applications

- Smart Property
  - *Everledger* ledger tracks diamonds
  - *Provenance.org* tracks supply chain authenticity
  - *OpenBazaar* decentralized Craigslist exchange
  - *Factom-HealthNautica* securing medical bills and claims



Bitcoin 2.0

- Non-Banking Applications
  - Sidekik
    - On-demand tele-attorney
    - Private police
  - Namecoin: decentralized DNS

Bitcoin 2.0

- Applications beyond fintech all the way to governance
- Any kind of peer-to-peer contract can be implemented as a secure and unbreakable blockchain application
- Computer algorithms can maintain order and trust without the need for a government

Bitcoin 2.0

- Government
  - Identification documents
    - National ids
    - Visas
    - Voting registration

Applications

Supply chain

- Each participant in the shipping supply chain can view the progress of goods through the supply chain
- E.g., Provenance offers supply chain auditing
- E.g., Maersk s shipping containers (a shipping platform)

Applications

Global finance

- Cross-border payments (multiple layers of communication to verify transactions)
- E.g., JP Morgan

Sharing economy

- Peer-to-peer payments without intermediaries such as Uber and Airbnb
- E.g., OpenBazaar is a peer-to-peer eBay

Applications

Crowfunding

- E.g., the ICO

Governance

- Fully transparent and publicly accessible governance that can work through smart contracts
- E.g., Boardroom supports organizational decision-making

Applications

File storage

- Hacker-proof distributed data

Identity management

- Identity verification for online financial transactions

Intellectual property

- E.g., Imogen Heap's Mycelia enables musicians to sell their music directly to the fans

Applications

Land titles

- E.g., Georgia & Bitfury Group are developing a blockchain system for property titles.

Applications

Art collections

- The Non-fungible token (NFT)
- Non-fungible = unique

Applications

NFTs

- May 2014: The first-ever non-fungible token (NFT), "Quantum", is minted by artist Kevin McCoy and engineer Anil Dish
- April 2015: Spells of Genesis by Shaban Shaame (EverdreamSoft) on Counterparty, the first blockchain game
- 2015: Ari Meilich’s and Esteban Ordano’s blockchain game Decentraland June 2017: Cryptopunks by Larva Labs (John Watkinson and Matt Hall)
- October 2017: CryptoKitties by Axiom Zen
- 2019: James Ferguson's and Robbie Ferguson's blockchain game Gods Unchained
- 2021: a collage of Beeple's first 5,000 "everydays" sells for a record $69 million, the first NFT to be sold by a major auction house (Christie's)

Bitcoin 2.0

Non-Banking Applications

- Decentralised social messenger Gems (Daniel Peled, Israel, 2014) on bitcoin blockchain
- Supply chain finance app Skuchain (Mountain View, 2014)

Bitcoin 2.0

Gaming

- Forte & Ripple fund (2019)
- Tron fund (2020)

Bitcoin 2.0

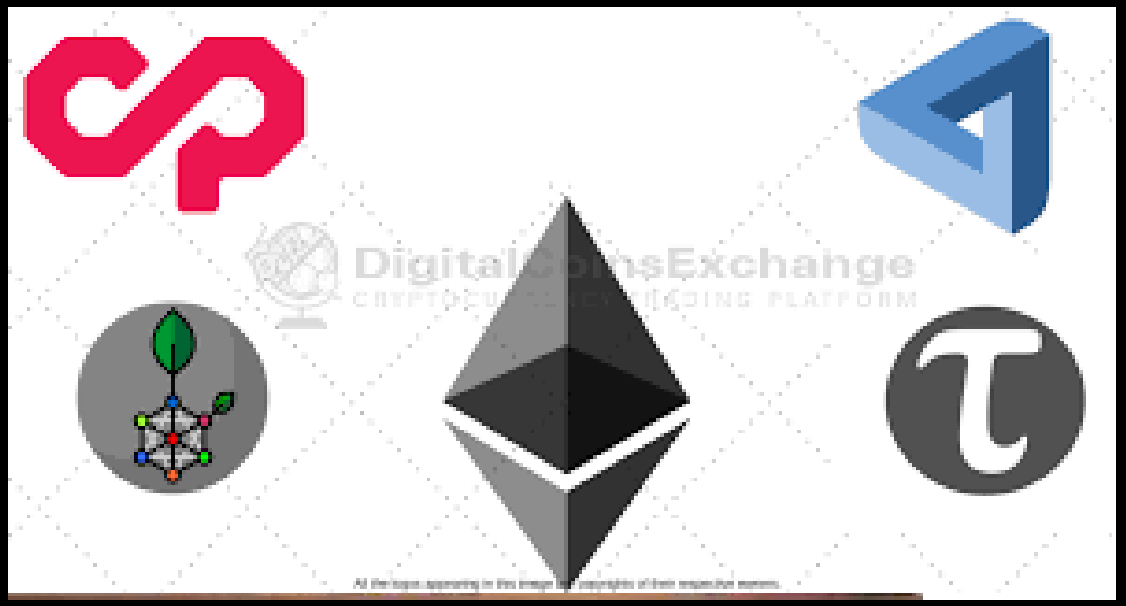
- Filecoin (Juan Benet, 2017): earn filecoins for hosting files on your computer, e.g. for offering storage to those who need it

Bitcoin 2.0

- Golem (Julian Zawistowski, 2017): a decentralized supercomputer
- Rent out processing time on your home computers

Bitcoin 2.0

- Bitcoin 2.0 technologies for developing decentralized applications (“app coins”):
  - Counterparty
  - Maidsafe
  - Ethereum
  - …
  - Rootstock
  - Tauchain
  - …



Lesson #6

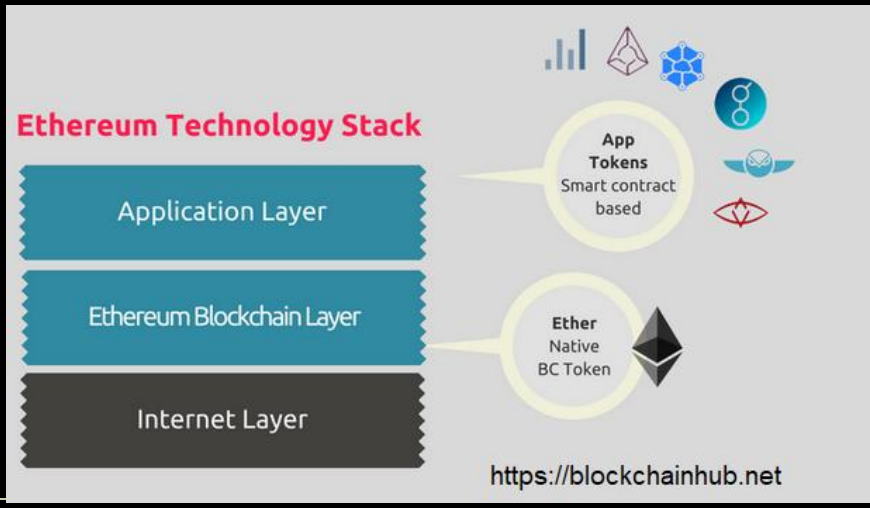
- Ethereum

Dapps

- The smart contract is the simplest form of decentralized automation
- Decentralized Application: a smart contract with an unlimited number of participants (e.g., Tor, BitTorrent, MaidSafe)
- Decentralized Applications are smart contracts
- No server: the blockchain serves as the "backend"
- No centralized intermediary

Bitcoin 2.0

- Ethereum (Vitalik Buterin, 2013)
  - A platform to develop Bitcoin-like "currencies"
  - A platform to develop secure digital contracts
  - A platform to develop decentralized applications
  - Optimized version of the blockchain to save storage space



Bitcoin 2.0

- Ethereum (Vitalik Buterin, 2013)
  - A simplified version of the Ghost protocol (Greedy Heaviest Observed Subtree), a proposed modification for the Bitcoin blockchain to speed up the blockchain (Yonatan Sompolinsky and Aviv Zohar)

Bitcoin 2.0

- Ethereum
  - Ethereum doesn't store massive data within the blockchain itself
  - It uses an additional component (originally Swarm, later cancelled, now IPFS)
  - Ethereum = Contracts (decentralized logic) + Swarm/IPFS (decentralized storage) + Whisper (decentralized messaging, under development)

Bitcoin 2.0

- Ethereum
  - InterPlanetary File System/IPFS (Juan Benet, 2015) for decentralized storage (not Swarm)
  - All data on IPFS are perpetually recorded online via P2P distribution
  - An encrypted address for each piece of information
  - A piece of information in IPFS cannot be manipulated
  - IPFS protocol replaces HTTP

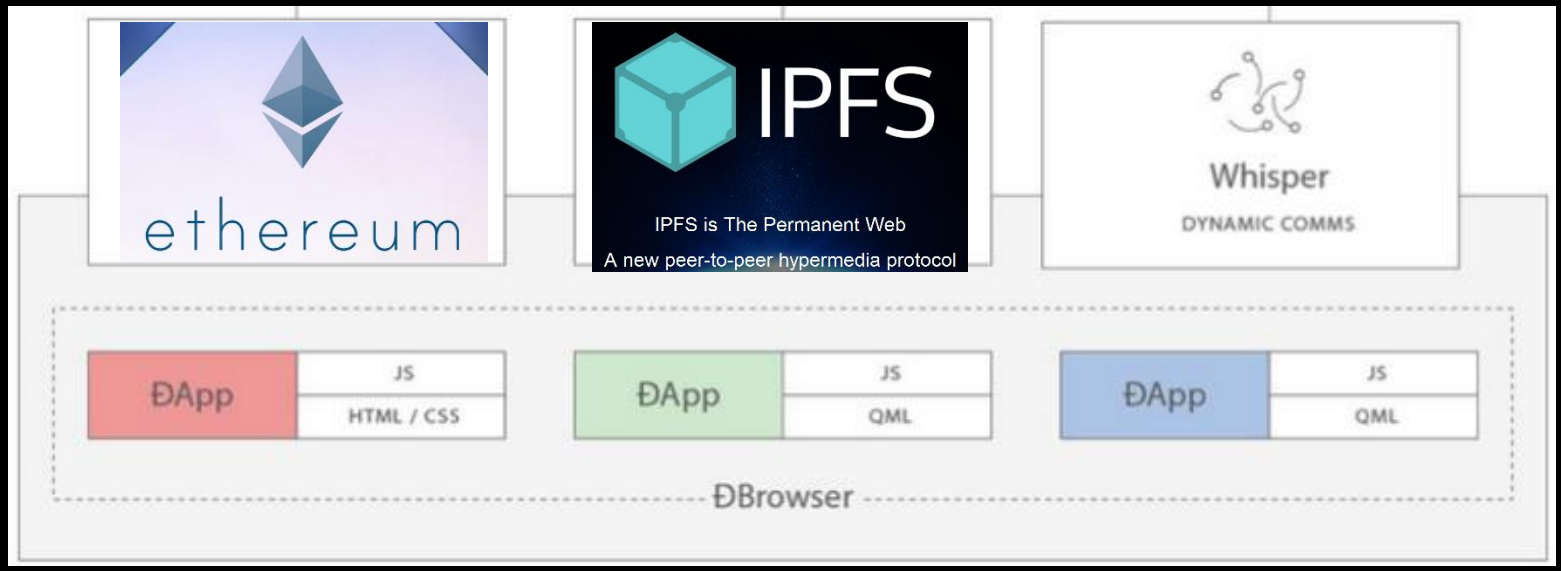
IPFS

IPFS is The Permanent Web

A new peer-to-peer hypermedia protocol

Bitcoin 2.0

- Ethereum
  - Whisper (201?) for messaging



Bitcoin 2.0

- Ethereum
  - Ethereum is “Turing-complete“ (it can implement any program)
  - a universal, general-purpose software development framework for creating decentralized applications
  - Vision of Ethereum as the "world computer"
  - Most vulnerable to Ethereum: the intermediaries (Amazon, Uber, Airbnb...)

Bitcoin 2.0

Ethereum

- Criticism:
  - Ethereum not designed for distributed computing
  - Ethereum designed for consensus
  - The blockchain was designed to avoid cheating: it was not designed to be the backend of a distributed system
  - Ethereum uses Bitcoin’s Proof of Work (slow)

Bitcoin 2.0

Ethereum

- Cryptokitties: a digital cat game
- 2017: 20% of all ethereum computations
- Highlights Ethereum's scaling limitations: Ethereum claims to be a world computer, but then CryptoKitties breaks it

Bitcoin 2.0

Ethereum

- United Nations helps refugees in Jordan with Ethereum (2017)
- … but also $53 million theft

Bitcoin 2.0

Ethereum smart contracts

- Smart contracts are a series of instructions, written in solidity (also serpent and viper)
- When the first set of instructions are done then execute the next function and after that the next etc
- Each step is recorded by all the nodes
- Each step in a smart contract is a transaction and has a cost that is measured in “gas”
- The price of gas is paid in “ether”
- Ether measures the market value, gas measures computational use

```
1 contract Purchase
2 {
3   uint public value;
4   address public seller;
5   address public buyer;
6 }
7
```

Bitcoin 2.0

- Ethereum tokens
  - Each DAPP has its own native currency, which is called a token
  - Once you are inside the DAPP, you use its token, just like inside a movie theater you use a movie ticket
  - You bought the movie ticket with money
  - The equivalent of your money is ether, that allows you to buy all sorts of tokens, the equivalent of movie tickets

Bitcoin 2.0

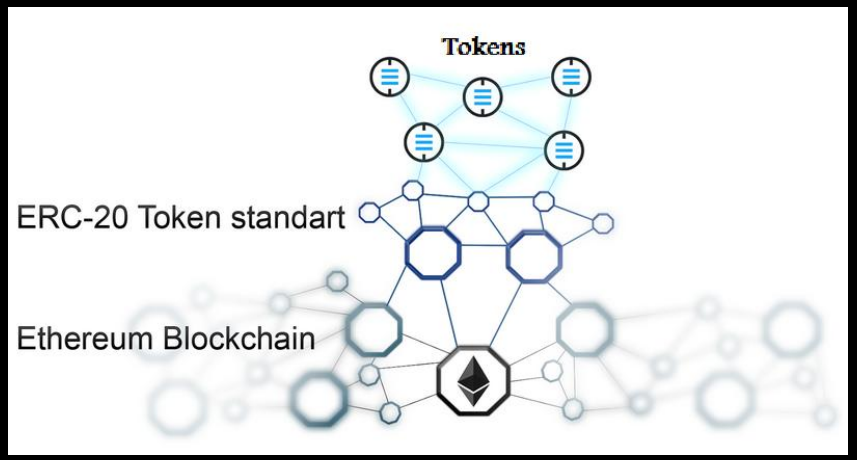
- Ethereum tokens
  - The creator of a DAPP must create the DAPP's own token: the Token Factory or write the code directly in Solidity (the programming language of Ethereum)
  - Initially you own all the tokens. Then you sell tokens for ether.
  - The price of a token depends on supply and demand

Bitcoin 2.0

- Ethereum tokens
  - Originally, each DAPP had its own token, incompatible with the tokens of other DAPPs
  - A smart contract interacting with several DAPPS had to deal with the complexity of using different tokens.
  - but then Ethereum came up with a standard to make tokens compatible with each other.

Bitcoin 2.0

- Ethereum
  - 2015: ERC20 Token Standard (ERC = Ethereum Request for Comments)
  - 2017: more than 21,000 ERC20 token contracts
  - 2017: 99% issued ICO tokens implement ERC20
  - 2017: Ethereum owns the market for DApps

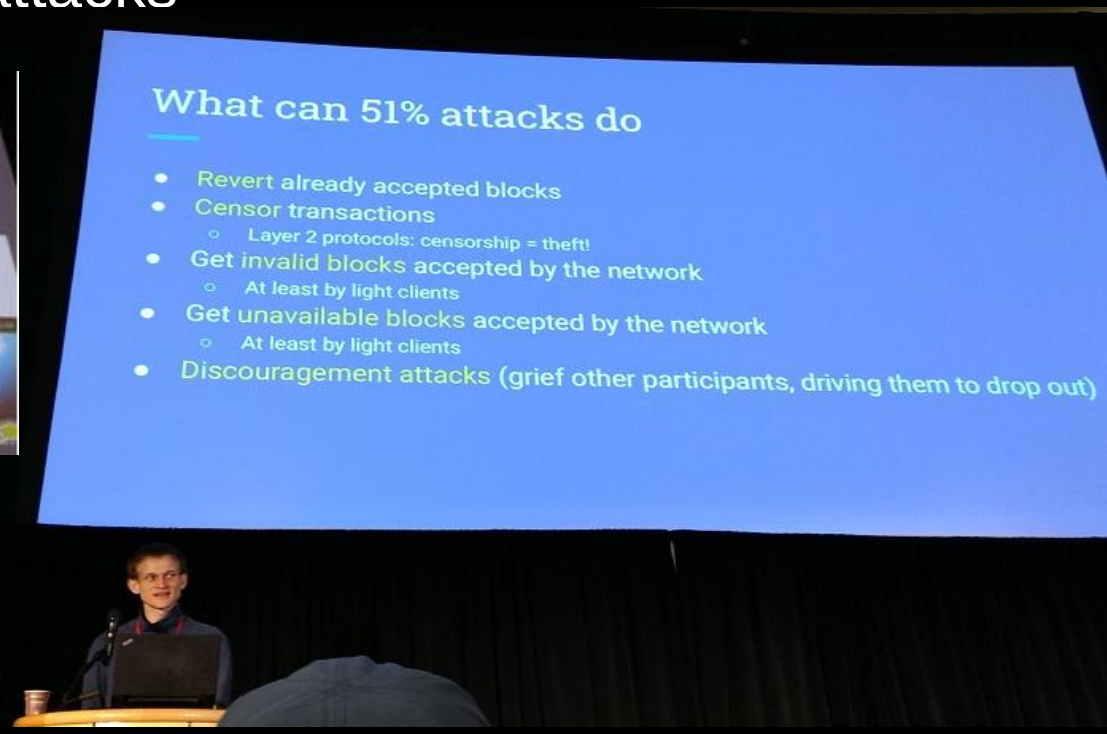


Bitcoin 2.0

- ERC-20 standard enabled the proliferation of cryptotokens
- Cryptocurrency token: a type of privately issued currency
- A unit of value that an organization creates to self-govern its business model, and to empower its users to interact with its products
- A cryptocurrency token represents a programmable currency unit that is bolted to a blockchain
- A token a cog in a logic of smart contracts that implement an application

Bitcoin 2.0

- Defending from 51% attacks



Vitalic Buterin at Stanford Blockchain Conference 2020

Bitcoin 2.0

- Defending from 51% attacks

Spawn camp attack

- Get enough hardware to attack a chain
- Attack it
- Wait for the chain to recover
- Attack it again
- Repeat until PoW algo changes
- Rent CPU/GPU hashpower to attack

PoS break the cycle?

A Proof of Stake Design Philosophy

Vitalik Buterin
Dec 30, 2016 · 7 min read

Systems like Ethereum (and Bitcoin, and NXT, and Bitshares, etc) are a fundamentally new class of cryptoeconomic organisms — decentralized, jurisdictionless entities that exist entirely in cyberspace, ma
combination of cryptography, economics and social consens

- **Proof of stake breaks this symmetry by relying not on security, but rather penalties**. Validators put money ("d stake, are rewarded slightly to compensate them for lock capital and maintaining nodes and taking extra precaut their private key safety, but the bulk of the cost of rever comes from penalties that are hundreds or thousands than the rewards that they got in the meantime. **The "**

Spawn camp attack on PoS

- Buy enough coins to attack a chain
- Attack it
- Get slashed
- Buy enough coins to attack a chain (price is higher now)
- Attack it
- Get slashed
- Try to buy enough coins to attack a chain (price is even higher)
- Go bankrupt

2/3 commit HASH1

1/3 slashe

Bitcoin 2.0

- Defending from other attacks

Problem: what about other kinds of attacks?

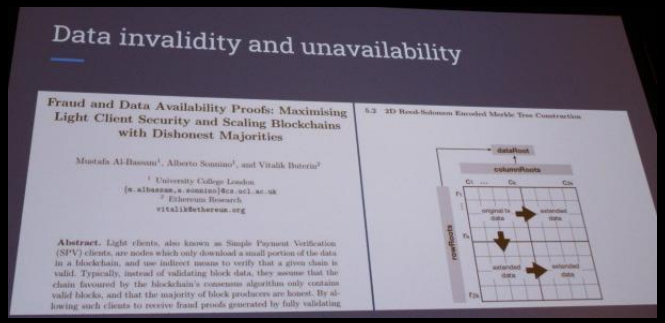
- Data invalidity
- Data unavailability
- Censorship
- Griefing

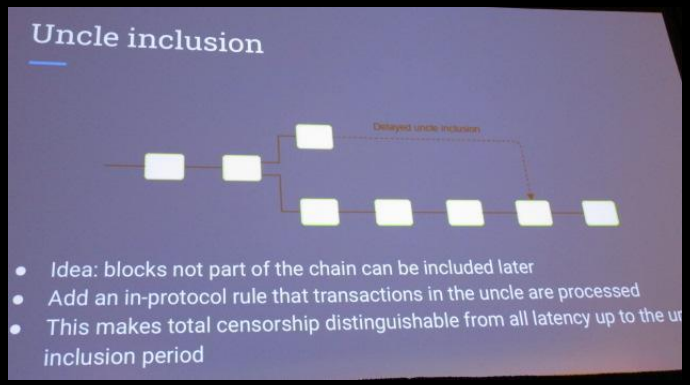
Problem: what about other kinds of attacks?

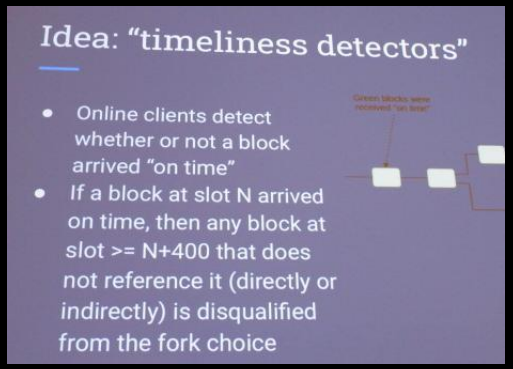
- Data availability + censorship resistance -> data validity (interactive computation / rollups)
- Non-censorship -> limited griefing (if incentives are done right)
- So we have **data availability** and **censorship resistance** as key targets

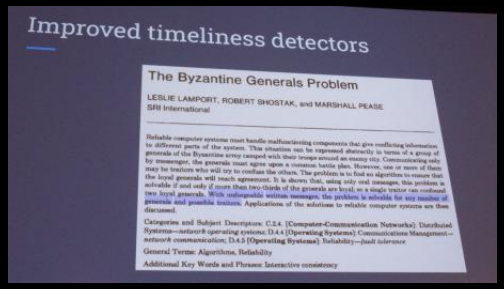
Bitcoin 2.0

- Defending from other attacks









Bitcoin 2.0

- Defending from other attacks

Summary...

Attack	Response
Publish unavailable chain	Ignore due to data availability checks
Publish invalid chain	Ignore due to fraud proofs (layer 1 or layer 2)
Censor blocks for a short time	Include as uncles
Censor blocks for a medium time	Use timeliness detectors to disambiguate into above or below case
Censor blocks for a long time	Ignore the chain
Don't participate in committees	Don't use committees

Lesson #7

- Tokenomics

Tokenomics

- Every asset is destined to become liquid on the blockchain
- The world’s non-liquid assets will be traded on the blockchain
- Tokens allow owners to
  - transfer ownership without moving the object from its location
  - track the provenance of the object

Tokenomics

- Intrinsic tokens
- BTC on the Bitcoin blockchain (number of tokens increases over time)
- XRP on the Ripple network (tokens decrease over time)
- NXT on the NXT platform (tokens remain constant)
- ETH on Ethereum (tokens increase)

Tokenomics

- Asset tokens represent assets and can be anything
  - stocks
  - debts
  - gold
  - IPOs
  - diamonds
  - artworks
  - organisations
  - music
- Utility tokens:
  - Filecoin

Bitcoin 2.0

- Ethereum
  - Ether is the native currency of the Ethereum blockchain
  - But different tokens can be implemented on Ethereum
  - Tokens are crypto currencies representing dapps that make use of the Ethereum blockchain
  - ERC-20 compliant token can be exchanged for other tokens

Tokens Cap: $ 27.5 B (2.7 %) for 513 Tokens.

#	Token	Cap
	Ethereum (ETH)	$ 40,259 M
1	EOS (EOS)	$ 4,738 M
2	Tronix (TRX)	$ 2,411 M
3	VeChain Token (VEN)	$ 1,408 M
4	BNB (BNB)	$ 1,404 M
5	OMGToken (OMG)	$ 941 M
6	ICON (ICX)	$ 808 M
7	Bytom (BTM)	$ 558 M
8	Populous Platform (PPT)	$ 438 M
9	Digix DAO (DGD)	$ 414 M
10	RHOC (RHOC)	$ 351 M
11	Maker (MKR)	$ 334 M

Bitcoin 2.0

- Ethereum tokens of 2018
  - Tron connects content creators with ordinary users
  - VeChain: supply chain management
  - OmiseGo provides all financial services
  - Icon connects blockchains
  - Populous: peer-to-peer lending
  - Status enables users to turn their phones or tablets into Ethereum nodes

Bitcoin 2.0

- Ethereum tokens of 2018
- Spritzle/HitFin (Nathalie & Patrick Salami, San Mateo, 2015)
  - Ethereum-based platform for trading derivatives

Bitcoin 2.0

- Ethereum
  - 2018: 46 of the top 100 cryptocurrencies by market cap are Ethereum-based tokens

Tokens Cap: $ 27.5 B (2.7 %) for 513 Tokens.

#	Token	Cap
	Ethereum (ETH)	$ 40,259 M
1	EOS (EOS)	$ 4,738 M
2	Tronix (TRX)	$ 2,411 M
3	VeChain Token (VEN)	$ 1,408 M
4	BNB (BNB)	$ 1,404 M
5	OMGToken (OMG)	$ 941 M
6	ICON (ICX)	$ 808 M
7	Bytom (BTM)	$ 558 M
8	Populous Platform (PPT)	$ 438 M
9	Digix DAO (DGD)	$ 414 M
10	RHOC (RHOC)	$ 351 M
11	Maker (MKR)	$ 334 M

Bitcoin 2.0

Ethereum tokens

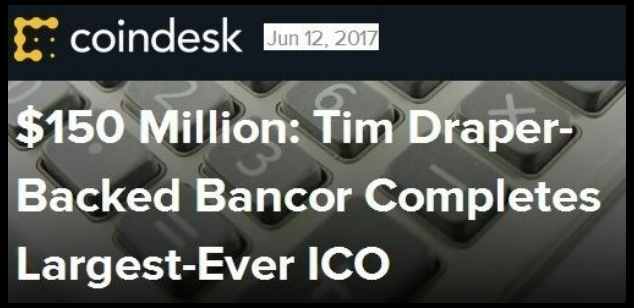
- Bancor (Israel, 2017): an alternative exchange for tokens
- Convert any token to any token in the Bancor network with no counter party at automatically calculated price Balance/(Supply*CRR)
- Smart tokens: tokens with smart contracts built inside it
- All tokens in the network can be converted to and from the BNT, Bancor Network Token

BANCOR
Protocol for Smart-tokens

Bitcoin 2.0

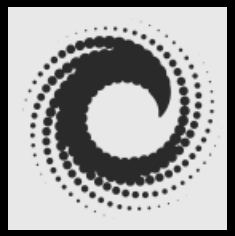
Ethereum tokens

- Bancor (Israel, 2017): a Bancor's ICO passes the DAO as the biggest ICO of all time ($152m)…
- … but crashes almost immediately



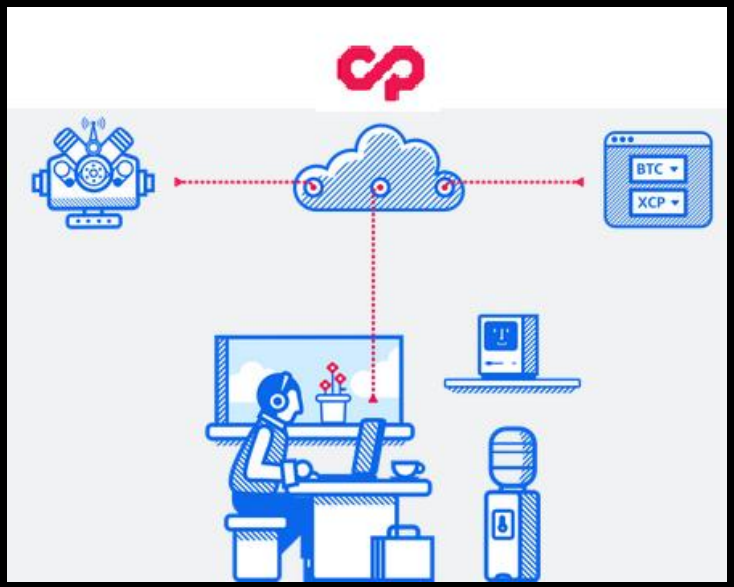
Bitcoin 2.0

- Consensus Systems/ ConsenSys (Martin Koeppelmann and Joseph Lubin, New York, 2014)
  - Custom “decentralized applications” (dapps) for blockchain ecosystems on top of Ethereum
- Etherparty (Los Angeles, 2015): cloud-based, no programming required (runs on Ethereum)



Bitcoin 2.0

- Counterparty (Chris DeRose, 2014)
  - A platform to foster the creation of P2P financial apps on the bitcoin blockchain
  - E.g., users can create their own currency and set up exchanges of digital currencies
  - Counterparty uses the bitcoin blockchain
  - Ethereum uses a non-bitcoin blockchain



Bitcoin 2.0

- Swarm (Joel Dietz, Palo Alto, 2014): an incubator of Counterparty projects; a platform for launching Counterparty projects and the initial mentorship and funding; a crowdfunding platform for creating decentralized apps
- Storj (Shawn Wilkinson, Georgia, 2014), a distributed peer-to-peer encrypted cloud storage (similar to Dropbox but distributed, like Swarm/IPFS but running on Counterparty instead of Ethereum)

Swarm

STORJ.IO

Bitcoin 2.0

- OpenCoin/ Ripple (Jed McCaleb)
  - OpenCoin (2012): a bitcoin network that did not require on mining to process transactions
  - Ripple (2013): secure and instant global financial transactions with no chargebacks
  - 2016: third-largest cryptocurrency by market capitalization after bitcoin and ethereum
  - 2017: Ripple's price up 84% in one day
  - Based on a trust graph, not a blockchain

Bitcoin 2.0

- Ripple's Codius (San Francisco, 2013): a platform for decentralization of applications

Blockchain

Ripple and Gates Foundation's distributed ledger Level One Project: open-source software called Mojaloop for creating a real-time, interoperable payments platform on a national scale to reach the world's poor with essential financial tools.

Bitcoin 2.0

Stellar (founded by Ripple's founder Jed McCaleb in 2014)

stellar

- David Mazieres professor of Computer Science at Stanford University
- improved the Ripple consensus algorithm into the Federated Byzantine Agreement algorithm
- Non-profit, open-source, distributed payment infrastructure with a focus on the developing world
- Low-cost financial services

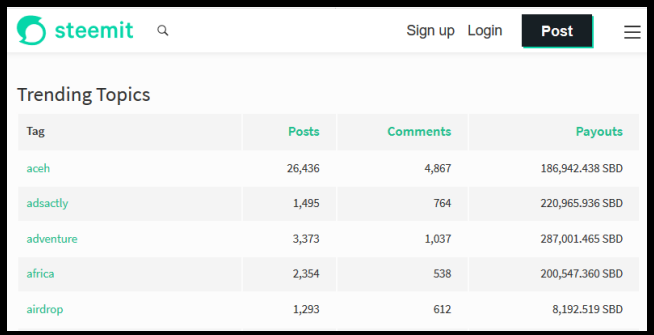
Bitcoin 2.0

Ripple: liquidity on demand (banks and multinational corporations use Ripple to make international payments by transferring the XRP token through the Ripple network)

Stellar: individuals trade money directly with each other using lumens

Blockchain as a Reward Engine

- Steemit (Ned Scott & Dan Larimer, New York, 2016)
  - A blogging and social networking website on top of the Steem circlechain database
  - Based on the Smart Media Tokens (SMT) protocol
  - The Steem blockchain produces tokens (steems) that users gain for posting, discovering, and commenting on content.
  - Authors rewarded with steem when their content is upvoted
  - Curators rewarded with steem for discovering popular content



Blockchain as a Reward Engine

- Steemit (2016, Ned Scott and Dan Larimer)
  - Steem: blockchain-based rewards platform for publishers
  - D.tube: decentralized video platform based on the InterPlanetary File System (IPFS) protocol (producers obtain steem when their videos are upvoted)
  - Dec 2017: Steem tokens ranked 32nd of 1,358 cryptocurrencies
  - Dec 2017: 450,000 user accounts

Blockchain as a Reward Engine

- Steemit: $1.6 billion market capitalization of Steem crashes to a low of 17 million on March 2017

Blockchain for Gaming

- Ripple + Forte fund to encourage game developers to develop blockchain-based games (2019)
- Tron's similar fun (2018)

Lesson #8

- The Boom of Decentralization

Bitcoin 2.0

- The biggest problem of blockchain technology: scalability
  - Visa manages 1667 transactions per second
  - Paypal manages 193 transactions per second
  - Bitcoin manages just 3-4 transactions per second
  - Ethereum manages 20 transactions per second

Bitcoin 2.0

- Other platforms for easy decentralization of applications:
- Eris/Monax (New York, 2014)
  - Founded by two lawyers, Preston Byrne & Casey Kuhlman
  - A universal blockchain platform
  - It can clone Ethereum, Bitcoin and many other blockchains
  - A blockchain is a database, and each user should have its own
  - Uses IPFS for storage

Bitcoin 2.0

- Tools to develop blockchain apps
  - Lisk (2016, Max Kordek and Oliver Beddows): open-source, written in Javascript

Bitcoin 2.0

- Tools to develop dapps:
  - Cardano (2017, by Ethereum's cofounder Charles Hoskinson)
  - open-source project
  - ADA coin
  - More robust proof-of-stake algorithm (Ouroboros)
  - Jan 2018: $31 billion market capitalization
  - the "Ethereum of Japan" because 95% of the participants in the ADA Initial Coin Offering (2015) were from Japan

Bitcoin 2.0

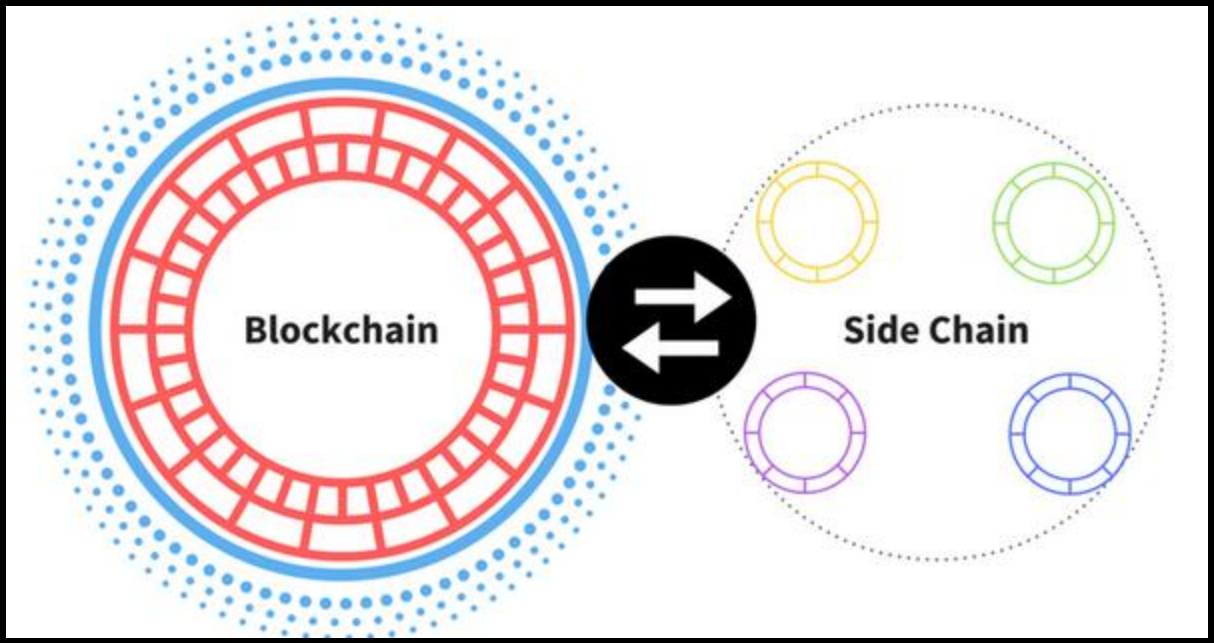
- Tools to develop dapps:
  - Cardano: Ripple (payments) + Ethereum (smart contracts)
  - Designed by a global team of academics
  - Team of lawyers and regulators to make sure that its ADA coin will integrate with the financial world.
  - Quote: *“the best of Bitcoin (store of value), Litecoin (cheap, fast p2p transactions), and Ethereum (smart contracts) into one coin”*

Bitcoin 2.0

- Tools to develop dapps:
  - Cardano:
  - Written in Haskell (a functional language, not object-oriented like Java) and in Plutus (a Haskell for smart contracts)
  - Layered architecture:
    - PoS -based cryptocurrency called the Cardano Settlement Layer (CSL) which handles transactions (like Bitcoin or Ripple)
    - a set of protocols called the Cardano Computation Layer (CCL) which handles smart contracts (like Ethereum)

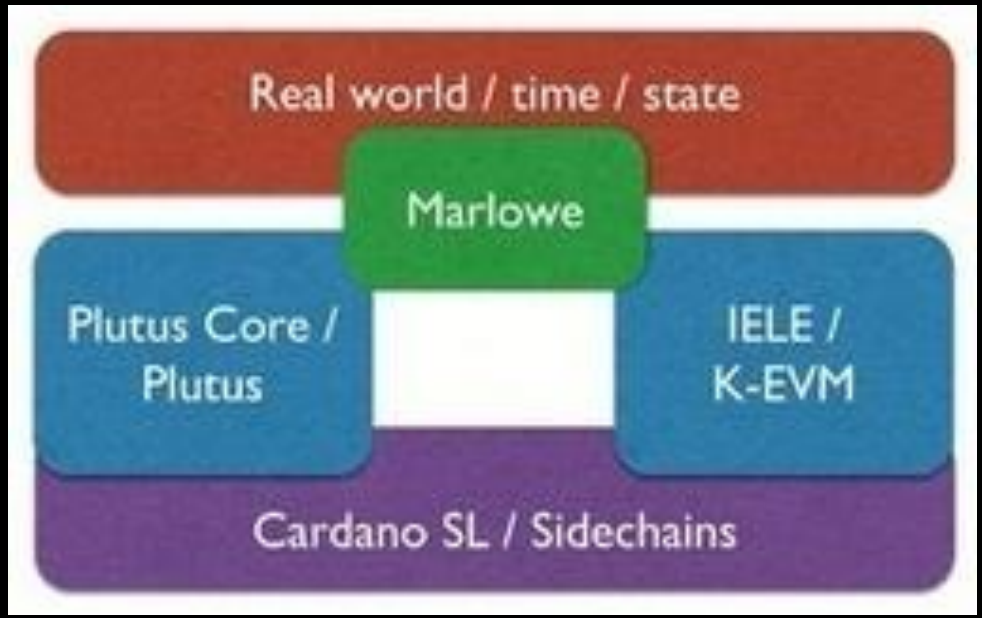
Bitcoin 2.0

- Tools to develop dapps:
  - Cardano: side chains



Bitcoin 2.0

- Tools to develop dapps:
  - Cardano: Iele virtual machine to execute smart contracts on the blockchain (based on LLVM from the University of Illinois), Marlowe programming language for financial accounting…



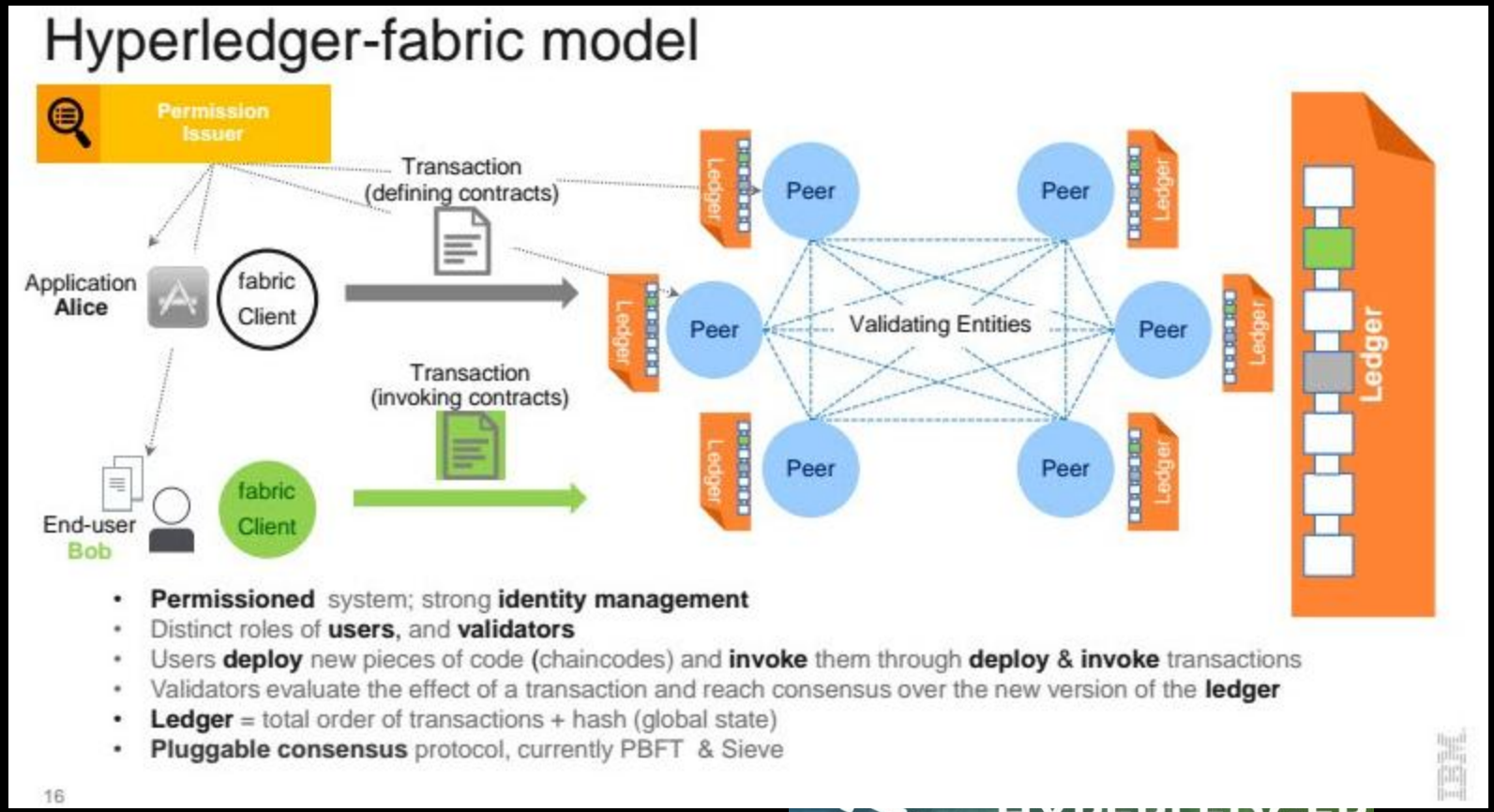
Bitcoin 2.0

- Tools to develop dapps:
  - Cardano: road map

Bitcoin 2.0

- Tools to develop dapps
  - Linux Foundation's Hyperledger Fabric (2017): modular architecture
  - Plug and play of components such as consensus algorithm
  - Based on IBM software
  - 2018: Amazon Web Services' service for launching blockchain networks for Ethereum and Hyperledger Fabric

Bitcoin 2.0


Hyperledger-fabric model
Permission Issuer
Transaction (defining contracts)
Application Alice
fabric Client
Transaction (invoking contracts)
End-user Bob
fabric Client
Peer
Validating Entities
Ledger
Permissioned system; strong identity management
Distinct roles of users, and validators
Users deploy new pieces of code (chaincodes) and invoke them through deploy & invoke transactions
Validators evaluate the effect of a transaction and reach consensus over the new version of the ledger
Ledger = total order of transactions + hash (global state)
Pluggable consensus protocol, currently PBFT & Sieve
16


HYPERLEDGER
FABRIC

Bitcoin 2.0

- Other platforms for dapps:
  - Distributed Ledger Group (2015): 40+ members consortium
  - Corda (2016, David Rutter): open-source distributed ledger
  - Partner with the Hyperledger Project

Bitcoin 2.0

- Tools to develop dapps
  - Tron (2017, Justin Sun) connects content creators with ordinary users
  - A shared economy in digital entertainment and gaming
  - April 2018: launches its own blockchain
  - Jan 2020: “TRON Arcade” fund to encourage game developers to develop blockchain-based games

Tron Labs
Apr 6 · 4 min read

TRON Founder Justin Sun Graduates Hupan University, Forges Ahead

Bitcoin 2.0

- Tools to develop dapps
  - Tron (2017, Justin Sun)
  - Launched in September 2017, trading at an initial price of $0.002
  - January 2018: $0.30 USD - market cap of over $16billion

Forbes DEC 14, 2017 @ 03:40 PM

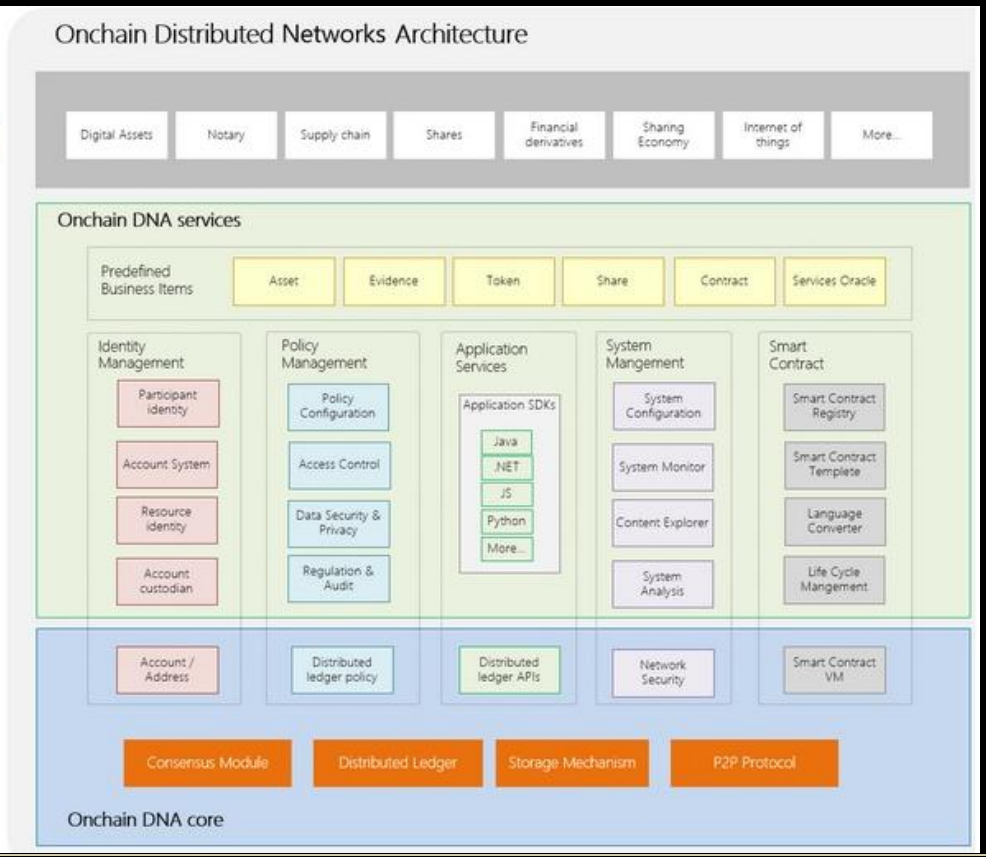
Crypto Watch: TRON (TRX) Price Surges Over 500% In A Week, Outperforming BTC, LTC, And ETH

Bitcoin 2.0

- Other platforms for dapps:
  - Antshares/NEO (2016): the Chinese Ethereum (uses Delegated Byzantine Fault Tolerance instead of PoW)
  - OnChain's DNA (Decentralized Network Architecture, 2016) links their blockchain technology with Chinese businesses and government.
  - NEO provides the public blockchain (the equivalent to the original blockchain) whereas OnChain's DNA provides private blockchains for businesses

Bitcoin 2.0

- Other platforms for easy decentralization of applications:
  - 分布科技 onchain

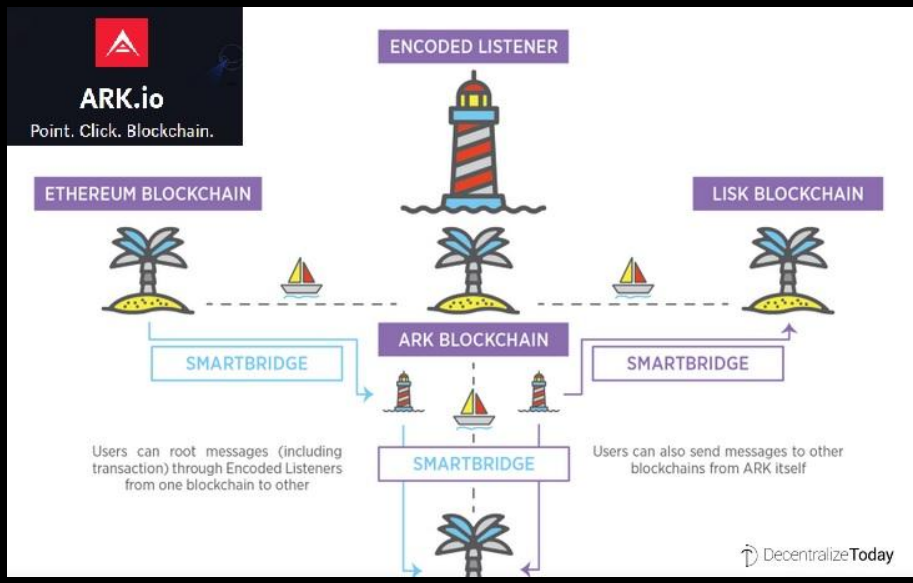


Bitcoin 2.0

- Other platforms for dapps:
  - Eos.io (2017, Dan Larimar)
  - Combines the scalability of Graphene (BitShares, Smeetit) and the power of Ethereum's smart contracts
  - Ethereum is a decentralized supercomputer, EOS is an operating system
  - Jan 2018: $6 billion market capitalization

Bitcoin 2.0

- Other platforms for dapps:
  - Ark SmartBridge (2017): make it easier for different blockchain networks to interoperate (uses Delegated Byzantine Fault Tolerance instead of PoW)



Bitcoin 2.0

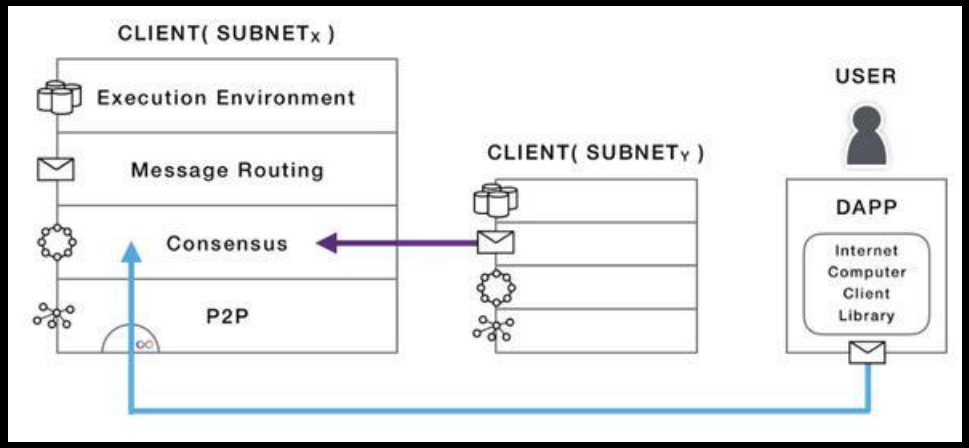
Dfinity (Dominic Williams) (Zug, Switzerland, 2015)

- A public decentralized network = A virtual computer of potentially unlimited capacity
- Similar in concept to Ethereum but has vastly improved performance
- All dapps built for Ethereum will be able to run on Dfinity

Bitcoin 2.0

Dfinity (Dominic Williams) (Zug, Switzerland, 2015)

- Motoko language



Bitcoin 2.0

Dfinity (Dominic Williams) (Zug, Switzerland, 2015)

- 2018: $100million funding from vcs

Bitcoin 2.0

- Rchain Cooperative (2016, Greg Meredith, ex Synereo)
  - A platform for smart contracts capable of processing 40,000 transactions per second
  - Infinitely scalable d-apps
  - Casper proof-of-stake
  - Rohlang programming language to build dapps

Blockchain-as-a-service

- Azure by Microsoft
- Ardor by Jelurida, founded by Petko Petkov (a core developer of NXT) and Lior Yaffe
- Stratis (Britain)

Blockchain-as-a-service

- Stratis (2016, Chris Trew)
  - Stratis allows corporations and businesses to develop their own custom blockchain applications
  - Blockchain applications can be developed in C# and make use of the Microsoft .NET framework
  - Apr 2018: $1.5billion market cap

Lesson #9

- Anonymity, Governance, ICO

Another issue: anonymity

- Bitcoin isn't anonymous at all: all transactions can be traced on the blockchain
- Zcash (2016, Zooko Wilcox)
  - All information about transactions is encrypted
  - Based on an extension for privacy on the Bitcoin blockchain invented by Mathew Green in 2014
  - 2017: market-cap surpassed $1 Billion

Another issue: anonymity

- Bitcoin isn't anonymous at all: all transactions can be traced on the blockchain
- Zcash criticism
  - A “corporate coin”: it is funded by a corporation (no company behind Bitcoin, Ethereum, etc)
  - Donor list to the Zerocash project include DARPA, the Air Force Research Laboratory, Office of Naval Research,…
  - Note: it is possible to add ZCash as a sidechain to the Bitcoin blockchain

Another issue: anonymity

- Zk-SNARKs (Alessandro Chiesa + Univ Tel Aviv, 2011)
  - Zero-knowledge proof: the prover proves to the verifier that a statement is true without revealing any information other than the validity of that statement
  - Zcash uses Groth16, a zero-knowledge SNARK
  - Universal zk-SNARK: Sonic (2019), Plonk (2019)
  - Aztec obscures part of Ethereum (2020)
- Zk-STARTs (Eli Ben-Sasson, 2018)
  - No need for trusted setup

Another issue: anonymity

- Zk-SNARKs
  - Universal zk-SNARK: Sonic (2019), Plonk (2019)

Classification of SNARKS	Common Reference String (CRS)		Structured Reference String (SRS)		
	Transparent arguments		Universal		Circuit Specific
Verification time			**Updatable**	**Static**	
Linear	Ligero, Aurora	Bulletproofs, Halo		AuroraLight	
Fast for all circuits	Fractal	Spartan, SuperSonic-CG	Sonic, Marlin, SuperSonic-RSA, Plonk		Groth16, BTCV14
Fast for optimized circuits	zk-STARK, Succinct Aurora	Hyrax		Libra	

Source: Ronald Mannak

Another issue: anonymity

- Monero (2014, Riccardo Spagni et al): obscuring sender, recipient and amount of every transaction
- “Stealth addresses“: the recipient of a transaction can retrieve the funds, but no one can link that stealth address to the owner
- Nicolas van Saberhagen ‘s CryptoNote protocol (2013) plus Gregory Maxwell's Confidential Transactions algorithm (2015, adopted in 2017)
- Best-performing cryptocurrency of 2016: +2,760%!

MONERO

WIRED

ANDY GREENBERG SECURITY 01.25.17 07:00 AM

MONERO, THE DRUG DEALER'S CRYPTOCURRENCY OF CHOICE, IS ON FIRE

Another issue: anonymity

- Xcoin/Darkcoin/Dash (2014, Evan Duffield)
- First tier: miners secure the network by providing proof of work, just like in Bitcoin
- Second tier: masternodes, which perform PrivateSend, InstantSend, and governance functions
- PrivateSend based on Gregory Maxwell's "coinjoin" technique (2013) that allows bitcoin users to mix their transactions with a few other spenders

Another issue: anonymity

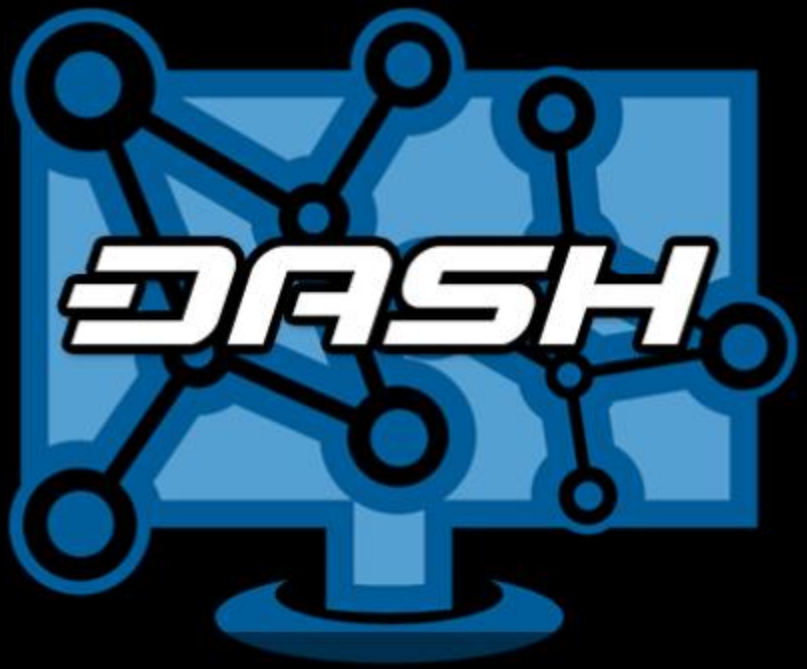
- Dash
- Pioneer of decentralized autonomous organizations (2016)
- 2017: market cap increases 8,000%

Governance

- Dash (2014: Evan Duffield)
- frustration that no decision was easy within the Bitcoin community
- faster than Bitcoin and has lower fees than Bitcoin
- built-in governance via a second-tier network ("masternodes")
- 2015: the first decentralized governance system, the Dash Budget System

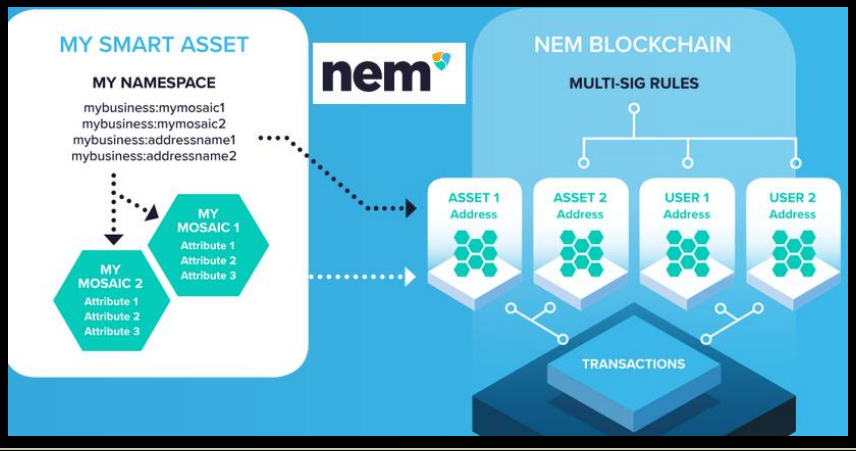
Dash Announces New Blockchain Research Lab at Arizona State University

Posted by Joël Valenzuela | Aug 18, 2017 | News | ★★★★½



Governance

- 2015: NEM (Japan)
- “Proof of Importance" (POI) method (PhD thesis of Makoto Takemiya)
- Instead of "mining", NEM has "harvesting“ (that ranks the importance of the “miner”)
- Eigentrust reputation system (Sep Kamvar, Mario Schlosser & Hector Garcia-Molina at Stanford, 2015)

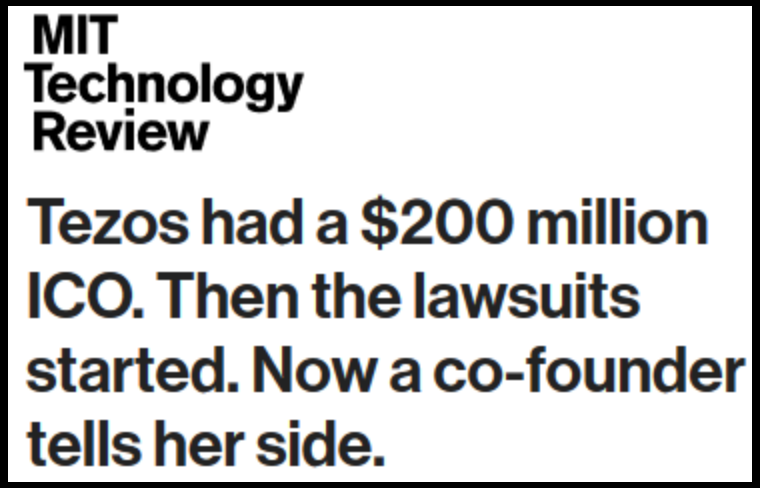


Governance

- 2017: Arthur & Kathleen Breitman's Tezos
- Frutration: chaos that surrounds the upgrades of Bitcoin and Ethereum
- A way to vote on upgrades to a blockchain network
- Democracy on the blockchain: each token is a vote
- "Proof of stake" method but even that can be subject to a democratic vote

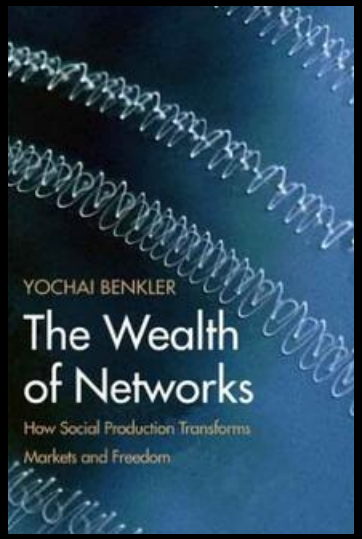
Governance

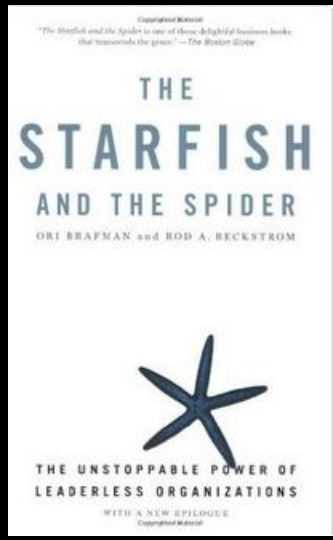
- Tezos
- Largest ever initial coin offering as of 2017



Governance 2.0

- DAOs (Decentralized Autonomous Organizations)
  - An unmanned organization under the control of an incorruptible algorithm
  - The algorithm is, in turn, a publicly auditable open-source software
  - DAOs are autonomous
  - DAOs are self-enforcing
  - DAOs have no central control





Governance 2.0

- Bitnation (Susanne Tarkowski Tempelhof, 2014)
  - a platform to create DAOs
  - *"Create Your Own Nation In 140 Lines Of Code"*
  - does not involve central authorities
  - a collaborative platform for DIY government
  - provides the same services that traditional governments provide, but in a decentralized way

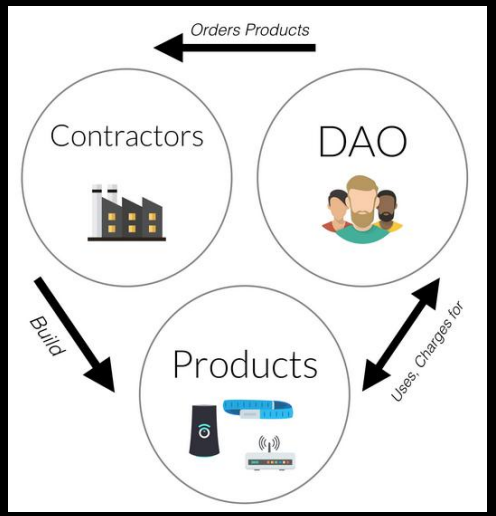
Governance 2.0

- Distributed Collaborative Organizations
  - 2014: Primavera De Filippi (Harvard Univ) and Houman Shadab (New York Law of School) invented an LLC-like organization for blockchain organizations
  - Integration of blockchain-based distributed organizations (DAOs) with the existing legal system

Governance 2.0

- The first DAO (May 2016, Christoph Jentzsch = Slock.it)
  - An autonomous crowd-sourced venture capital fund implemented by way of smart contracts, without the traditional legal intermediaries
  - the DAO raises the equivalent of $150m to invest in startups, 14% of all ether ever issued on Ethereum
  - Largest crowdfunding project until then
  - June 2016: hackers exploited a vulnerability in the DAO code to enable steal funds

Slock.it



Initial Coin Offerings (ICOs)

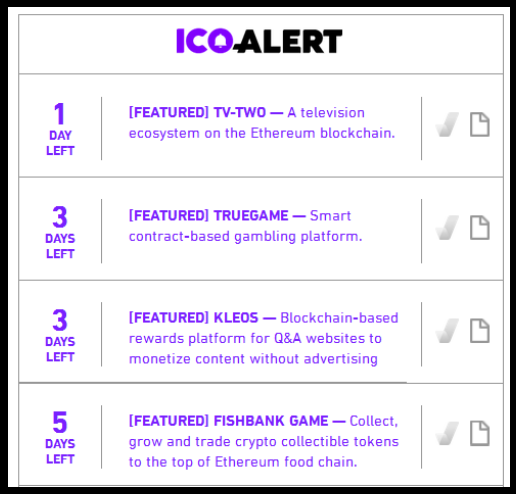
Initial Coin Offerings (ICOs)

- Digital coupons on the blockchain
- A project sells its crypto tokens in exchange for bitcoins and ethers
- Tokens are similar to shares of a startup in an IPO
- Investors send funds (usually bitcoin or ether) to a smart contract that stores the funds and distributes an equivalent value in the new token at a later point in time

Initial Coin Offerings

- Similar to crowdfunding for pre-product startups
- 2014: First ICO (Karmacoin)
- 2014: Ethereum's ICO
- DAO (2016): first fundraising for a new token on Ethereum (for a decentralized organization that would fund blockchain projects)
- 2017: Filecoin's record ICO

Aragon raised $25 million in just 15 minutes
Basic Attention Token raised $35 million in 30 seconds
Status.im raised $270 million in a few hours



Initial Coin Offerings

- 1946: The "Howey Test" created by the Supreme Court for determining whether a transaction qualifies as an "investment contract"
- 2015: ERC20 Token Standard makes it easier to create ICOs (ERC = Ethereum Request for Comments)
- 99% issued ICO tokens on top of the Ethereum implement this standard
- January 2018: more than 21,000 ERC20 token contracts

Crypto-bailouts

- 2017: Long Island Tea Corp. changes its name to Long Blockchain Corp
- 2018: Kodak's ICO

Crypto-bailouts

- Nor true cryptocurrencies but just schemes to avoid bankruptcy
- 2017: Venezuela's petro
  - Petro can only be sold on a government exchange for a government rate
  - It is just another ICO

Politics

- 2017: China and South Korea ban ICOs
- 2018: India bans cryptocurrency transactions

Politics

- 2019: blockchain core technology in China

China's President Xi Urges Accelerated Blockchain Technology Adoption

OCT 25, 2019

习近平强调，要加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，
律。要探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者
依法治网落实到区块链管理中，推动区块链安全有序发展。

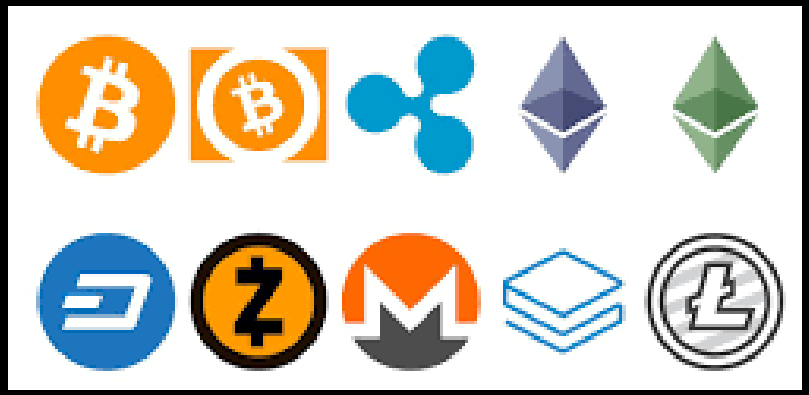
Governance and cryptoeconomics

- New types of organizations are issuing their own digital cryptocurrencies
  - To fund themselves
  - To govern themselves
  - To empower their users
  - To reward their contributors
- Each new crypto-organization sets in motion a new self-sustainable mini-economy

Lesson #10

- Distributed Ledger Technology: a summary and going beyond the blockchain

Summarizing Tokenomics…



Summarizing: Consensus Algorithms

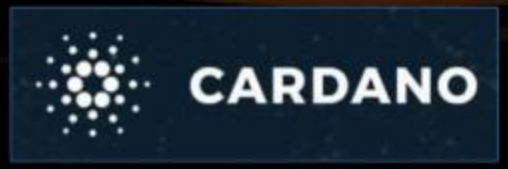
- Proof-of-work (Bitcoin, Ethereum, Litecoin, Dash, Monero, Zcash)
- Proof-of-stake (Peercoin, NXT, Blackcoin, Cardano)
- Delegated proof-of-stake (Bitshares, Lisk, Ark)
- Practical Byzantine Fault Tolerance (Hyperledger)
- Federated Byzantine Agreement (Stellar, Tendermint, Casper)
- Delegated Byzantine Fault Tolerance (NEO)
- Proof-of-Importance (NEM)
- Proof-of-Stake-Velocity (Reddcoin)
- Proof-of-capacity (Burstcoin)
- …

Summarizing consensus

- POW: unfair advantage to those who can afford the most powerful computing arrays
- POS: unfair advantage to coin hoarders (incentive to save coins instead of spending them because the rich get richer)
- POI tries to be fair to everybody who is active on the network

Summarizing: Consensus Algorithms

- Proof-of-stake cryptocurrencies
  - Cardano
  - Qtum
  - PIVX
  - BitConnect
  - Stratis



Stratis

Summarizing: Consensus Algorithms

- Delegated proof-of-stake

Summarizing: Hashing

- Bitcoin: SHA256 (ASIC mineable)
- Ethereum : ETHash (GPU mineable)
- Zcash: Equihash (CPU and GPU mineable)
- Monero: CryptoNight (CPU and GPU mineable)
- Litecoin : SCrypt (GPU mineable)
- Dash: X11 (ASIC, CPU and GPU mineable)
- Stratis: X13 (ASIC, CPU and GPU mineable)
- …

Summarizing: Programming languages

- Bitcoin: C++, C
- Ethereum: C++
- IOTA: Java
- Cardano: Haskell
- Lisk: JavaScript
- NEO: C#
- Stellar: C++
- Ripple: C++, C

Summarizing cores

Most important DLTs cores

	Bitcoin Core	Graphene	Tendermint	Ripple / Stellar
Language	C/C++	C++	Go	C++
Consensus	PoW	dPoS	PoS	
Blockchains	Bitcoin, Dash, Litecoin, ...	BitShares, Steem, Golos	Cosmos (under dev)	Ripple, Stellar, Infra (e-Auction)
"+"	Most proved	Blazingly fast	PoS	Fast & proved
"–"	Hard to understand	Complex model	Immature	Complex model

Blockchain Protocols

- Internet protocols: TCP/IP, HTTP, HTML, DNS, FTP, IMAP, and SMTP, etc
- Blockchain protocols: Bitcoin, Ethereum, IPFS for file sharing across any applications, industry specific (eg. Etherisc for insurance, or OpenBazaar for P2P commerce)

Blockchain Protocols

- Internet stack: "thin" protocols and "fat" applications
  - Protocols are worth nothing
  - Apps like Google and Facebook are worth billions
- Blockchain stack: “fat" protocols and “thin" applications
  - Bitcoin network: $10B market cap
  - Ethereum: $1B market cap
  - Apps running on the blockchain are worth very little

Blockchain Protocols

- Blockchain stack: “fat" protocols and “thin" applications
  - The market cap of the protocol always grows faster than the combined value of the applications built on top, since the success of the application layer drives further speculation at the protocol layer
  - Increasing value at the protocol layer attracts and motivates competition at the application layer

Blockchain Protocols

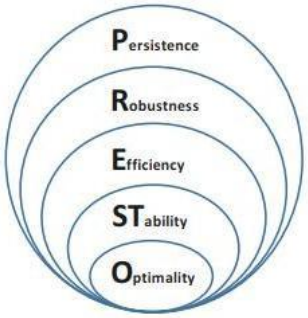
- Evaluating protocols: PRESTO (Singapore UTD)

Rethinking Blockchain Security: Position Pape
(preprint)

Apr 2019

Vincent Chia*, Pieter Hartel†, Qingze Hum†, Sebastian Ma*, Georgios Piliouras†
Daniël Reijsbergen†, Mark van Staalduinen*, Pawel Szalachowski†

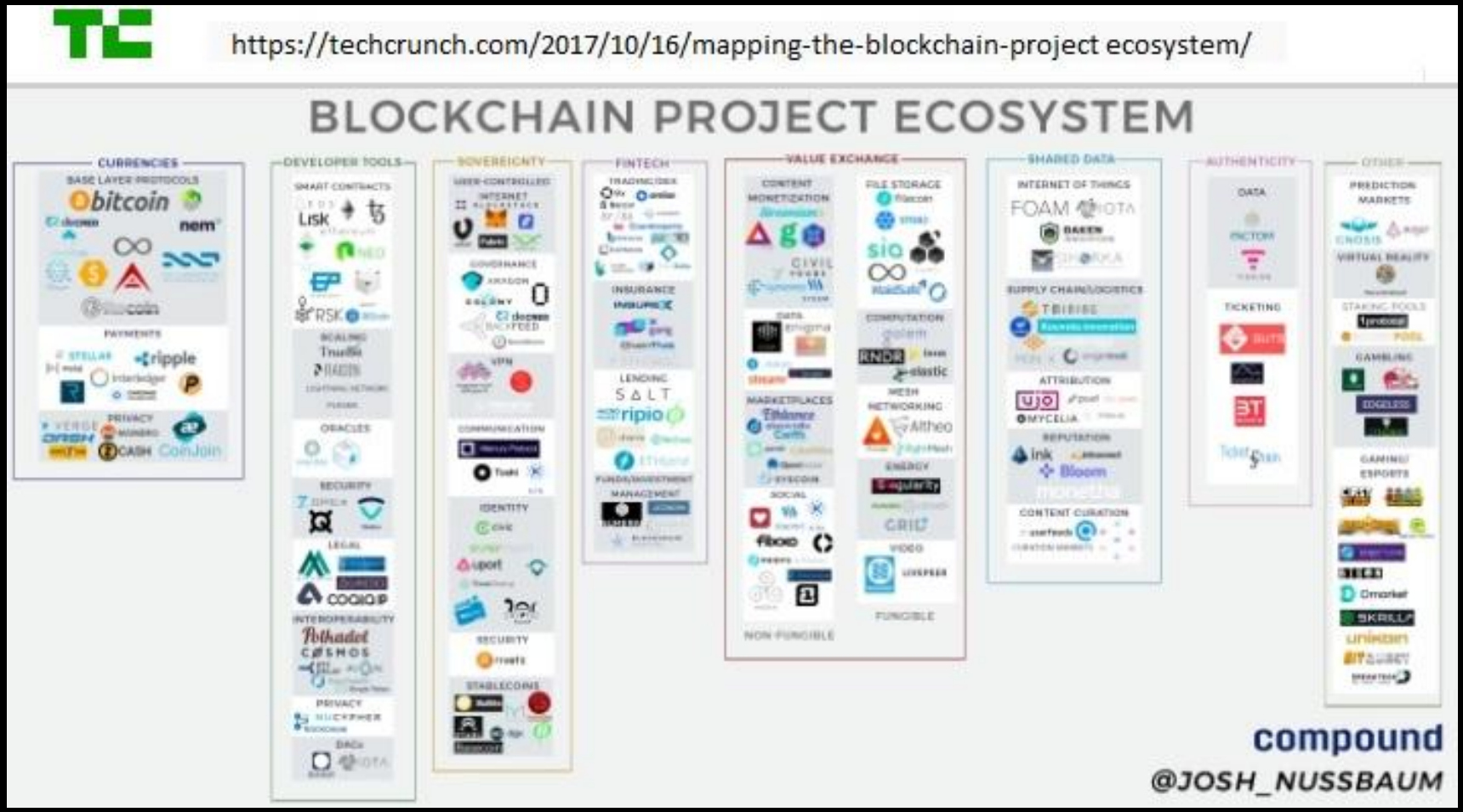
*The Netherlands Organisation for Applied Scientific Research (TNO)
†Singapore University of Technology and Design



PREStO: A Systematic Framework for Blockchain Consensus Protocols

Stefanos Leonardos, Daniël Reijsbergen, Georgios Piliouras
Singapore University of Technology and Design

Blockchain Ecosystem in 2017



Blockchain 2019

- Prism (MIT + Stanford)
  - Unit-e: a globally scalable decentralized payments network
  - Bitcoin couples performance and security
  - Prism decouples them

COMPUTERWORLD JAN 22, 2019

MIT, Stanford and others to build blockchain payments network to rival VisaNet

Seven universities are collaborating to create a blockchain-based online payment system that will solve issues of scalability, privacy, security and performance, enabling up to 10,000 transactions per second.

Prism: **Deconstructing the Blockchain to Approach Physical Limits**

Vivek Bagaria, Stanford University
Sreeram Kannan, University of Washington at Seattle
David Tse, Stanford University

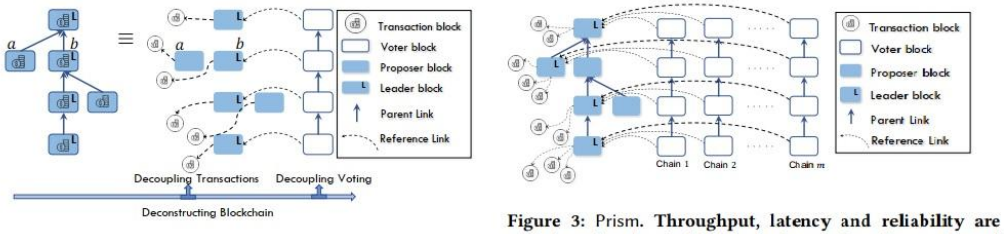
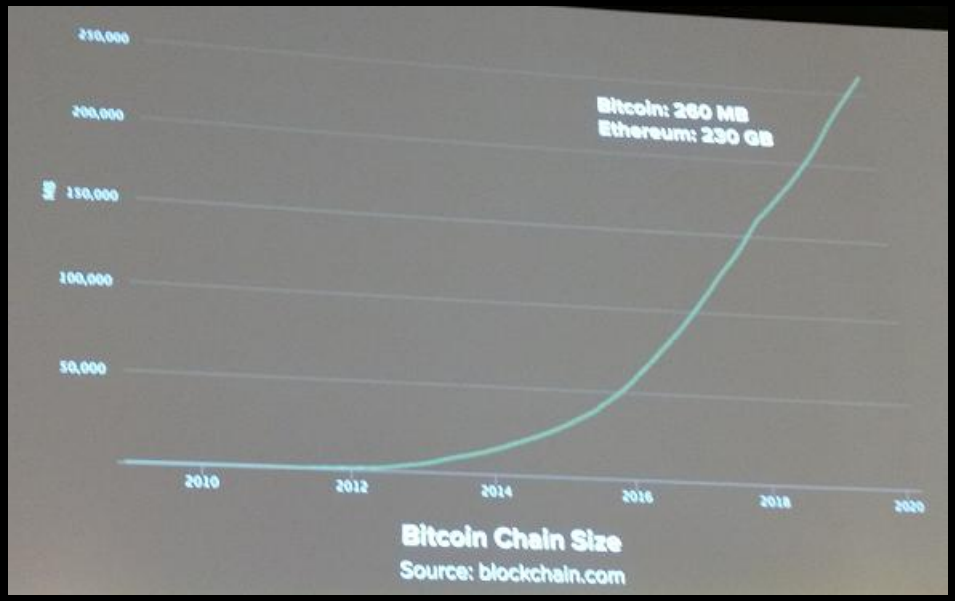


Figure 3: Prism. **Throughput, latency and reliability are scaled to the physical limits by increasing the number of transaction blocks and the number of parallel voting chains.**

Blockchain 2019

- Ultralight protocols for smartphone clients
  - Problem: size of Bitcoin and Ethereum blockchains exploding



Blockchain 2019

- Ultralight protocols for smartphone clients
  - NiPoPoW (Aggelos Kiayias, 2016) - PoW
  - Flyclient (Benedikt Bunz & Lucianna Kiffer, 2018) - PoW
  - Coda (Izaak Meckler & Evan Shapiro, 2018) - PoS

Proofs of Proofs of Work with Sublinear Complexity

Aggelos Kiayias, Nikolaos Lamprou, and Aikaterini-Panagiota Stouka
National and Kapodistrian University of Athens**

FlyClient: Super-Light Clients for Cryptocurrencies

Benedikt Bünz[1*†], Lucianna Kiffer[2*†], Loi Luu[3*], and Mahdi Zamani[4]
[1]*Stanford University*, [2]*Northeastern University*, [3]*Kyber Network*, [4]*Visa Research*

CODA

Blockchain 2019

- Ultralight protocols for smartphone clients
  - Celo (Rene Reinsberg, 2019) - PoS
    - Celo (Rene Reinsberg, 2017)
    - Proof-of-stake consensus
    - Celo is a fork of Ethereum client Geth.
    - Celo gold equivalent to ether in Ethereum
    - Plumo client protocol for the Celo network
  - Libra (Facebook, 2020)
  - Libra and Celo can provide the user with a "digital identity", a way to build up a "credit score" that can be used to apply for loans.
  - Both Libra and Celo target the "unbanked" population, the population that does not have a bank account.

Blockchain 2019

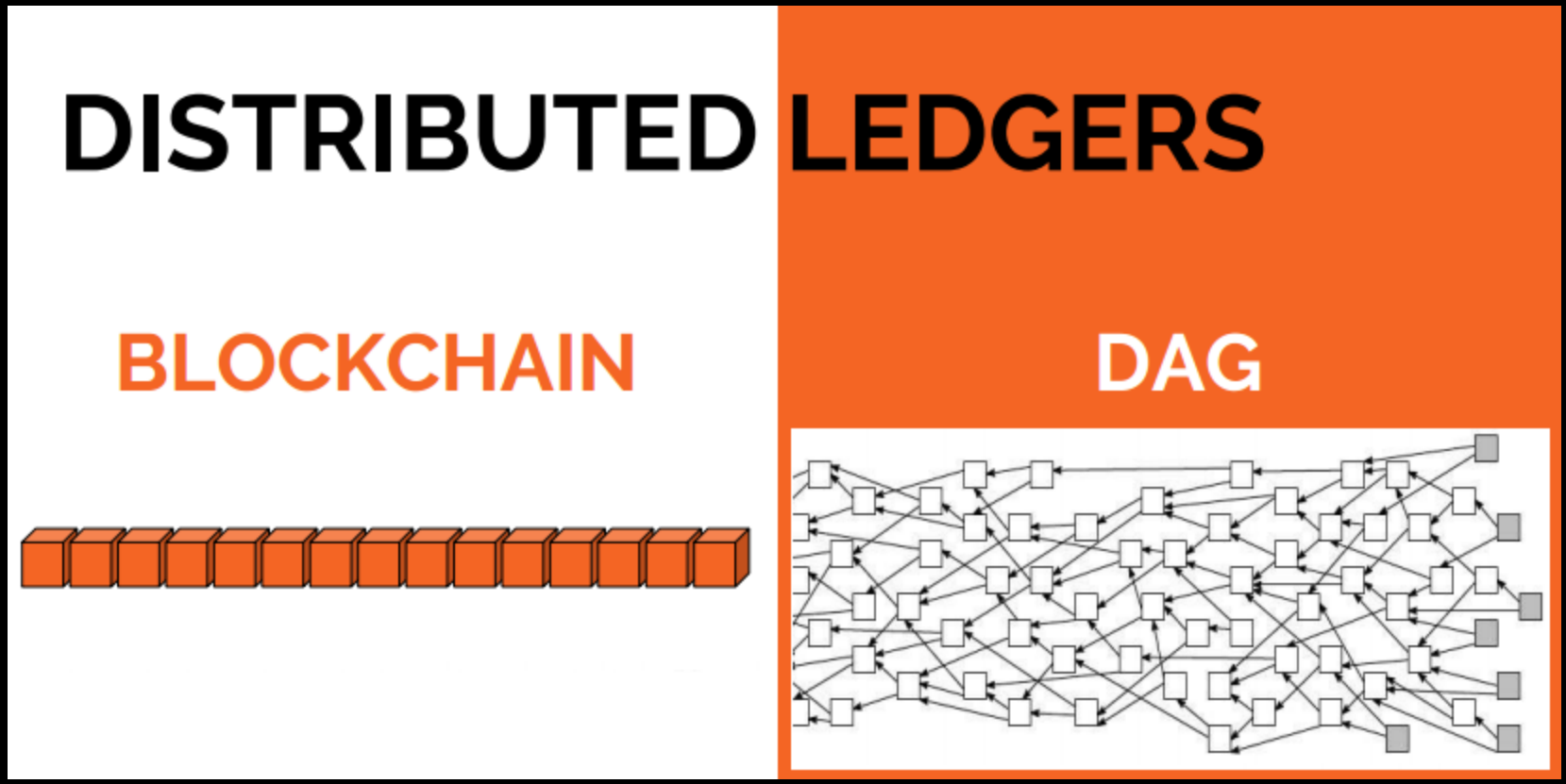
- Libra (Facebook)
  - Bring the blockchain to the smartphone (pay with Whatsapp)
  - Written in Rust (Graydon Hoare, 2012
  - A "stable coin", backed by traditional financial assets
  - Not decentralized
  - No miners
  - Consensus algorithm LibraBFT, a variant of HotStuff (Dahlia Malkhi, Guy Gueta and Ittai Abraham at Vmware, 2018)
  - Move language for smart contracts

Distributed Ledger Technology (DLT)

- Beyond the Bitcoin blockchain
- Beyond the blockchain

DLTs

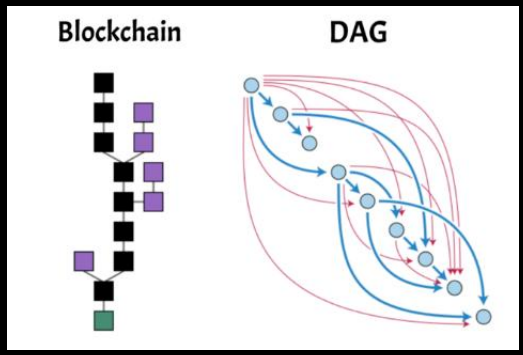
- Blockchain vs DAG



DLTs

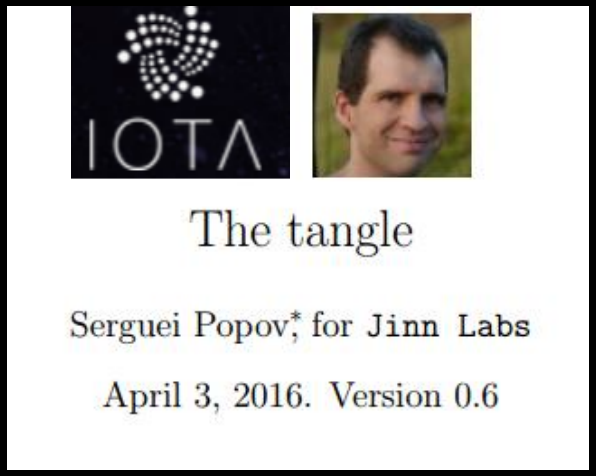
- 2015: Sergio Demian Lerner's DagCoin, the first block-less coin based on Directed Acyclic Graph
- There are no miners and there are no blocks
- Users confirm each other’s transactions via a process that confirms previous transactions with each new transaction
- Each user that transacts becomes automatically a miner
- Because there are no blocks, there is no blocksize issue

DAGCOIN



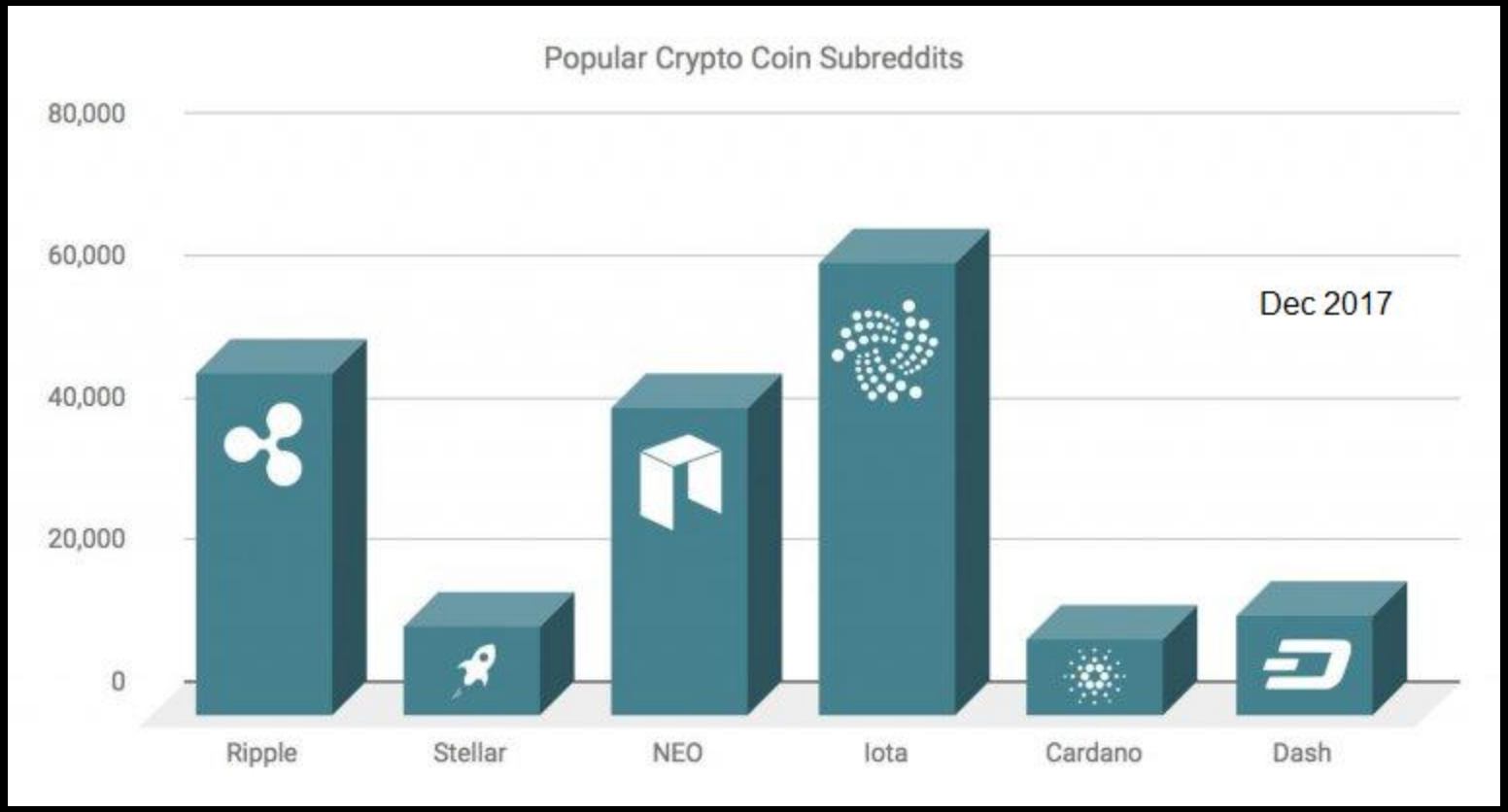
DLTs

- Iota, designed for micro-transactions (Serguei Popov et al, 2016)
- The tangle, based on "directed acyclic graph" (DAG), instead of the blockchain
- Zero transaction fees enabled by Tangle – a necessary step toward integration with the Internet of things
- A platform for “The Economy of Things”: autonomous machine economy



DLTs

- Iota


Popular Crypto Coin Subreddits
80,000
60,000
40,000
20,000
0
Dec 2017
Ripple
Stellar
NEO
Iota
Cardano
Dash

Beyond the Internet

- MaidSafe (David Irvine, Britain, 2006)
  - To decentralize the Internet leveraging the enormous amount of unused hard-disk space that exists around the world combined with peer-to-peer protocols and encryption
  - No central servers, no central databases

Beyond the Internet

- MaidSafe
  - MAID (Massive Array of Independent Disks) SAFE (Secure Access For Everyone)
  - Data are shredded and heavily encrypted, and the encrypted chunks are randomly distributed around the world
  - Only the owner can reassemble and decrypt these chunks
  - No blockchain: not a "proof of work" ("mining") algorithm but a "proof of resource" mechanism
  - Transactions are not stored in a blockchain: no traces of that transaction exist except with the two parties involved

Beyond the Internet

- MaidSafe
  - MaidSafe rewrites the Internet
  - SafeNet: a Tor-like platform that decentralizes all the services currently available on the Internet (messaging, email, social networks, data storage, video conferencing, etc); i.e. it makes them work without any need for servers and databases
  - The final solution to the problems of identity theft and surveillance

Beyond the Internet

MaidSafe

- MaidSafe
  - A P2P-based system for storage and routing
  - Decentralized storage a` la Storj: "farmers" offer spare storage to the network
  - A crowd-sourced Internet
  - A browser that lets people browse HTML pages securely and anonymously
  - The user can log into any computer of the network and the computer becomes "her" computer: her data, her applications, her profile.
  - When she logs out, no trace of her work is left behind.

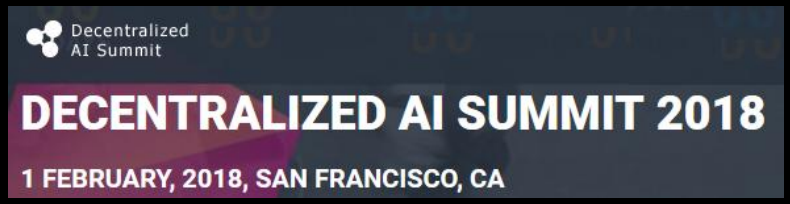
Substratum

- Substratum (2018?, Justin Tabb)
- promises to revolutionize the Internet by allowing equal access to the Internet for everyone
- Still in beta in 2018
- promises to allow anyone to host a node and receive Substrate in return for contributing to the network

Appcoins

- Aptoide (2011): an alternative to current app store duopoly (Android OS app with 200 million users worldwide)
- 2017: the first App Store powered by blockchain technology
- Appcoin: a cryptocurrency based on ERC20 tokens
- “Cost per attention” algorithm
- Tokens granted to users in exchange for downloading apps and giving them 2 minutes of their attention

Blockchain and AI: Decentralized Intelligence



Decentralizing the building blocks of A.I.

- Big Data
- Models
- Computing Power

MODELS

DATA

COMPUTING POWER

Blockchain and AI: Decentralized Intelligence

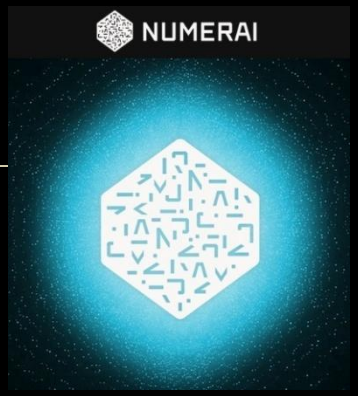
Ben Goertzel's SingularityNET

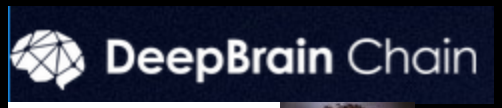
- Several A.I.s can cooperate to create a single brain
- Hanson robot Sophia
- The whole world can improve the brain of robot Sophia
- Oct 2017: Sophia granted citizenship in Saudi Arabia
- Dec 2017: ICO raised $36 million within 60 seconds

Singularity Net

Blockchain and AI: Decentralized Intelligence

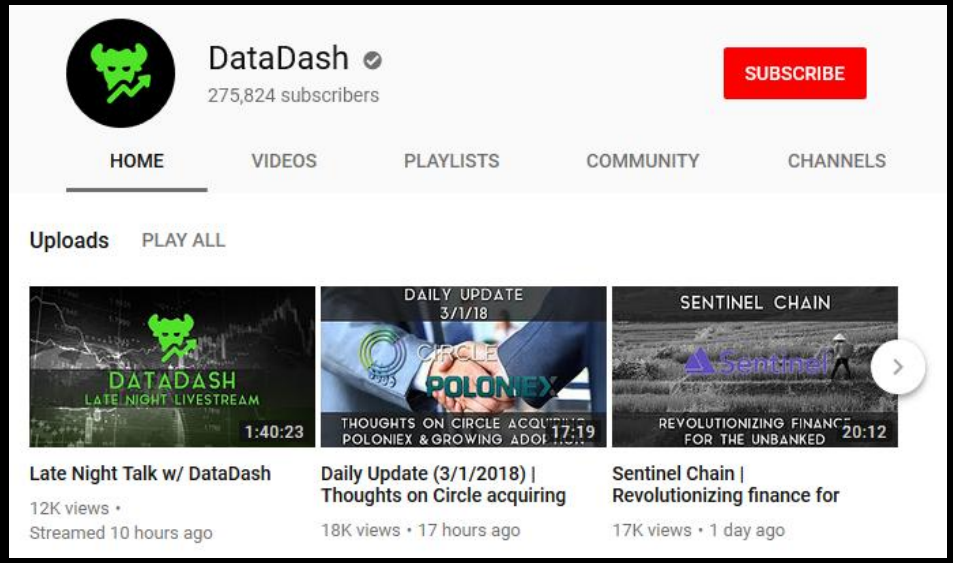
- Numer.ai : blockchain-powered, AI-coordinated hedge fund
- Neureal.net: peer-to-peer AI supercomputing for eternal data analysis
- Ai-blockchain.com: A.I. to build new blockchains
- Openmined.org: distributed dataset to train A.I.s
- Synapse.ai: distributed dataset to train A.I.s
- DeepBrain Chain: a decentralized neural network
- Matrix.org (Jon Crowcroft, Cambridge): decentralized bots
- Matrix AI Network (Steve Deng, China): improve smart contracts





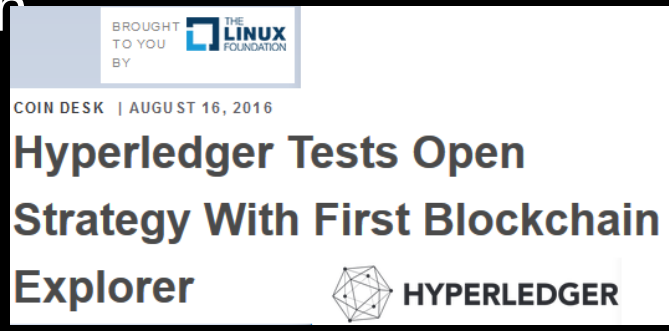
Blockchain education

- Zug in Switzerland = Crypto Valley
- Datadash, the largest crypto youtube channel with over 200k subscribers



Blockchain education

- Hyperledger Project (Dan O'Prey and Daniel Feichtinger, 2014 - Linux Foundation, 2016): a joint effort to advance blockchain technology (IBM, Accenture, Intel, Fujitsu, Hitachi, etc)
- The technology is almost entirely open source, written in Java
- Practical Byzantine Fault Tolerance

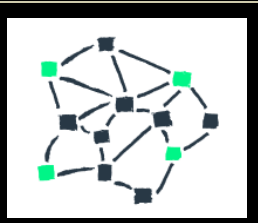


Blockchain

Blockchain technology: the blockchain is a history of the digital world

A decentralized database

Bitcoin protocol: a Byzantine fault tolerant system for mutually distrustful participants



Blockchain

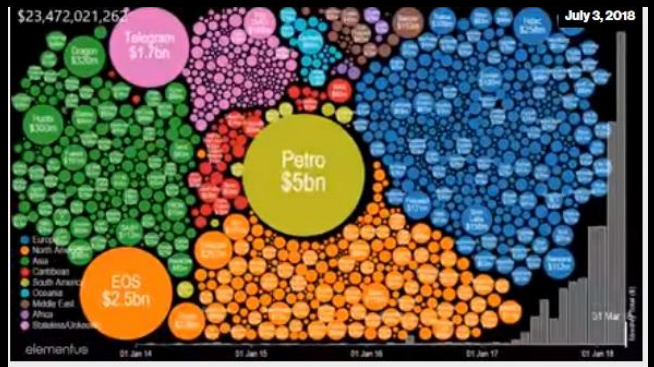
Ethereum generalizes Bitcoin's notion of transaction to include execution of arbitrary smart contracts

Ethereum is "Turing-complete" (it can implement any program)

A universal, general-purpose software development framework for creating decentralized applications

A token: to raise capital, to create and motivate a user base

New financial instruments: initial coin offerings (ICOs)



Despite shadiness and crackdowns, the ICO boom is bigger than ever www.technologyreview.com

Blockchain

- Disruption at multiple levels
  - Technical: beyond the database
  - Business: tokenomics
  - Legal: smart contracts

Verifiable Data Audit

DeepMind's New Blockchain-Style System Will Track Health-Care Records

March 9, 2017

Alphabet's artificial intelligence outfit, DeepMind, plans to build a blockchain-style system that will carefully track how every shred of patient data is used.

Decentralized Economies

- Google's business model: targeted advertising based on user-generated content
  - Private content could kill Google
- Uber's business model: the "middlema a centralized aggregator
  - Decentralized computing could kill Uber
- Open private ecosystems
  - Blockchain's decentralized model for content distribution could kill Netflix, cable TV and the studios

livepeer

VIULY.COM

Blockchain for Supply Chain

- Blockchain app: track a chain of events
  - Skuchain (2014), Silicon Valley
  - OriginTrail (2013, Slovenia)

skuchain

origintrail

MAERSK IBM

Maersk and IBM Introduce TradeLens Blockchain Shipping Solution

Published on 09 August 2018

Blockchain for Supply Chain

ORACLE

Oracle OpenWorld, San Francisco, Calif.—Oct 23, 2018

Press Release

Oracle Unveils Business-Ready Blockchain Applications

Blockchain for Supply Chain

- Blockchain app: track a chain of events
- Also for healthcare: DeepMind, Vechain…

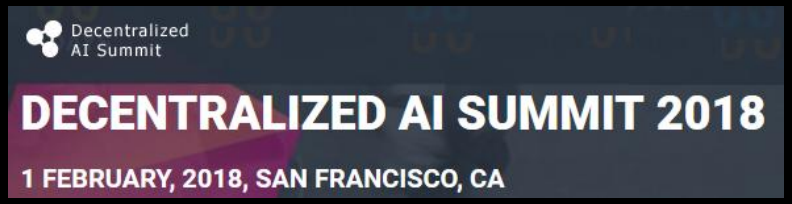
Verifiable Data Audit

DeepMind's New Blockchain-Style System Will Track Health-Care Records

March 9, 2017

Alphabet's artificial intelligence outfit, DeepMind, plans to build a blockchain-style system that will carefully track how every shred of patient data is used.

Blockchain and AI: Decentralized Intelligence



Decentralizing the building blocks of A.I.

- Big Data
- Models
- Computing Power

Blockchain and AI: Decentralized Intelligence

Ben Goertzel's SingularityNET

- Several A.I.s can cooperate to create a single brain
- Hanson robot Sophia
- The whole world can improve the brain of robot Sophia
- Oct 2017: Sophia granted citizenship in Saudi Arabia
- Dec 2017: ICO raised $36 million within 60 seconds

Singularity Net

Blockchain and AI: Decentralized Intelligence

Numer.ai : blockchain-powered, AI-coordinated hedge fund

Neureal.net: peer-to-peer AI supercomputing for eternal data analysis

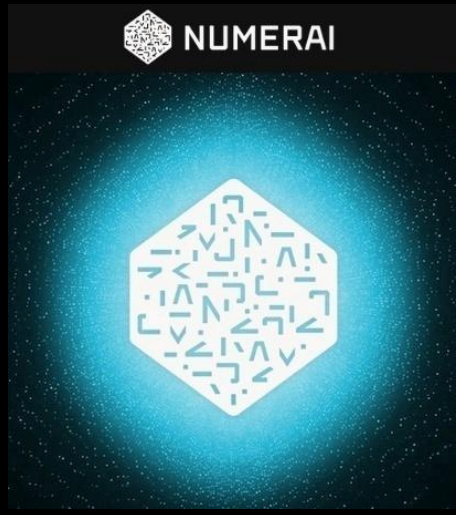
Ai-blockchain.com: A.I. to build new blockchains

Openmined.org: distributed dataset to train A.I.s

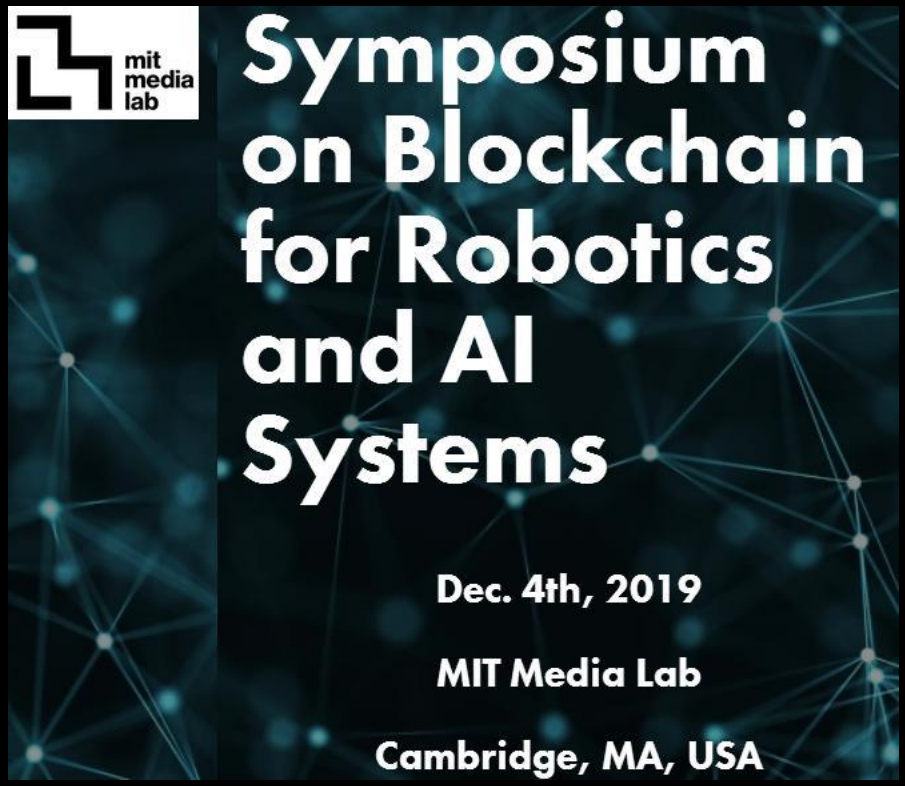
Synapse.ai: distributed dataset to train A.I.s

DeepBrain Chain: a decentralized neural

Matrix.org: decentralized bots



Blockchain and Robots



Bitcoin

Total capitalization of the cryptomarket: $600 billion

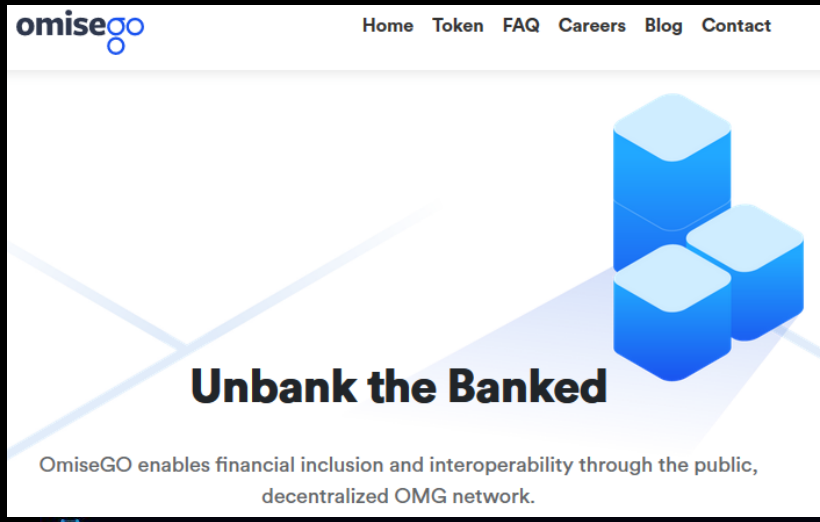
Cryptomarket

Unicorns

- Coinbase (2016): $1.6 billion valuation, first-ever cryptocurrency unicorn
- Circle (2018): $3 billion valuation (mostly funded by China-based Bitmain)
- Telegram (2018): $1.7 billion "private" ICO

Cryptomarket

- Total capitalization of the cryptomarket: $600 billion
- Unicorns
  - OmiseGo ERC20 token (Thailand, 2017): $1 billion valuation
  - a decentralized exchange of other blockchains and between multiple blockchains
  - Qtum ERC20 token (2018): $1 billion ICO
  - an Ethereum system on the Bitcoin blockchain



Bitcoin

Skepticism

Mike Hearn (2016): The bitcoin experiment failed and is finished (*"a system completely controlled by just a handful of*

Mike Hearn

Jan 14, 2016

The resolution of the Bitcoin experiment

- Couldn't move your existing money
- Had wildly unpredictable fees that were high and rising fast
- Allowed buyers to take back payments they'd made after walking out of shops, by simply pressing a button *(if you aren't aware of this "feature" that's because Bitcoin was only just changed to allow it)*
- Is suffering large backlogs and flaky payments
- … which is controlled by China
- … and in which the companies and people building it were in open civil war?

Bitcoin

Skepticism

- ICS Statis Group (July 2018): more than 70% of the ICOs in 2017 were scams
- TechCrunch (June 2018): more than 1,000 cryptoprojects are dead
- Limited supply of the cryptocurrency
- Alarming rise of transfer fee
- Lots of criminals around

Bitcoin

Skepticism

- A small number of people exercise control (1000 people hold almost 40% of all the Bitcoins)
- Cryptocurrencies banned by institutions and countries
- Insecure ICOs

December 8, 2017, 6:00 PM GMT+8 **Bloomberg Businessweek**

The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market

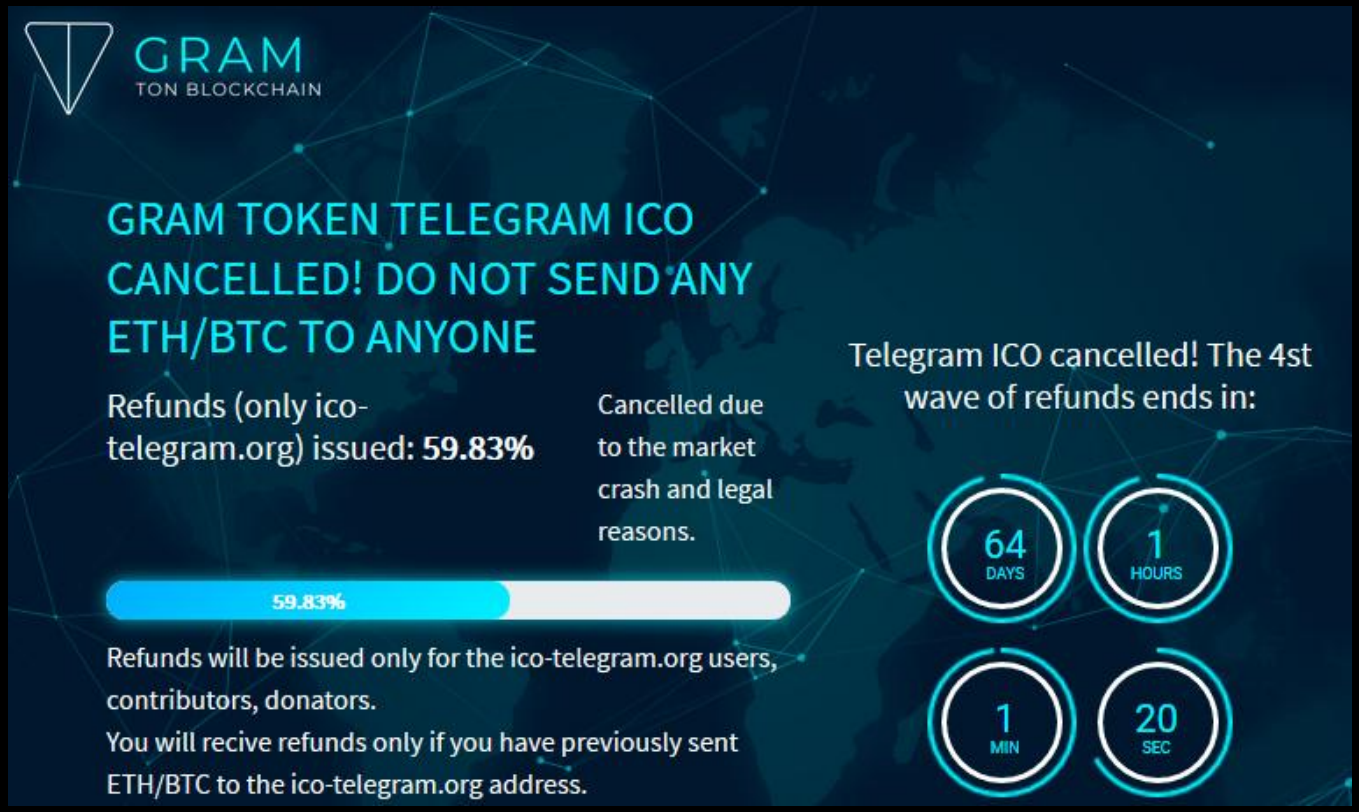
DhakaTribune

Police on the hunt for bitcoin users in Bangladesh

Bitcoin

Skepticism

- Insecure ICOs



Bitcoin

Skepticism

- What happens on 1/1/2020?
- If the Tulip Trust does exist, Satoshi Nakamoto or whoever owns it can release one million bitcoins into the market
- Phil Wilson's tweet of August 2018

Craig Wright

30 Aug 2018

Phil Wilson @_Phil_Wilson_ · 3h

Come 1st January, 2020, those addresses get unlocked and Craig will be able to transfer whatever coin hasn't been pre-sold to any backers.

If any version of Bitcoin is worth any price at that date then this will become the greatest heist in human history

Bitcoin

Skepticism

- Who benefits from Bitcoin?
- The early miners, who mined a lot of bitcoins at very low cost.
- Bitcoin is the very anti-thesis of money: its value depends on an artificial scarcity
- New miners can be profitable if
  - They get money from the crowd (which sometimes is a fraud)
  - They get money from VCs
  - They "steal" electricity (e.g. in China, where it's easier than in the USA)

Bitcoin

Reasons to believe in a future for cryptocurrencies:

- Cryptocurrencies allow performing multimillion transactions with minimum exchange rate costs
- Smart contracts are extremely transparent
- NKN (New Kind of Network)

NKN

Founders (2018): Yanbo Li, Bruce Li, Justin Wang, Yilun Zhang

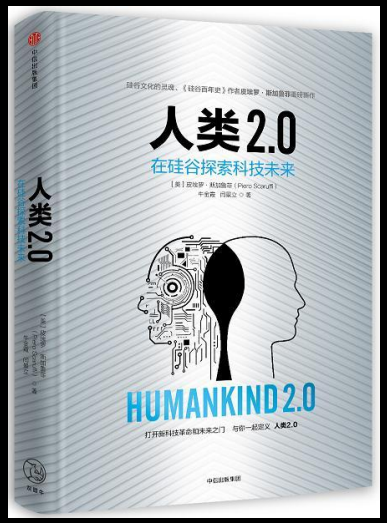
A fully decentralized and anonymous P2P protocol

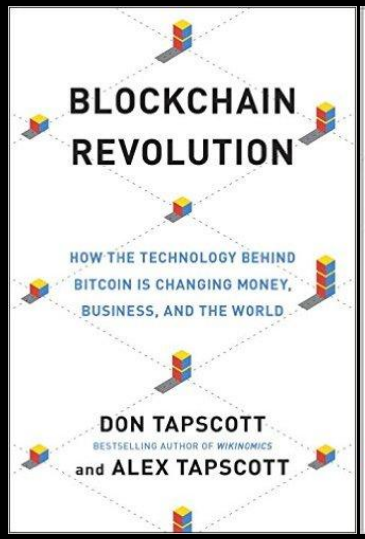
A TCP/IP for an Internet built on the blockchain

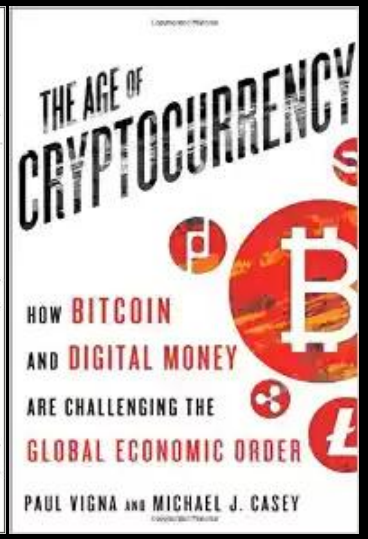
New consensus mechanism Proof of Relay (PoR) that rewards participants for contributing to the bandwidth of the network while they have to pay for using it

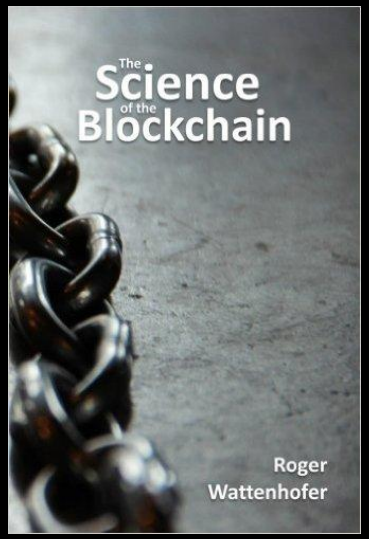
A self-evolving ecosystem based on cellular automata

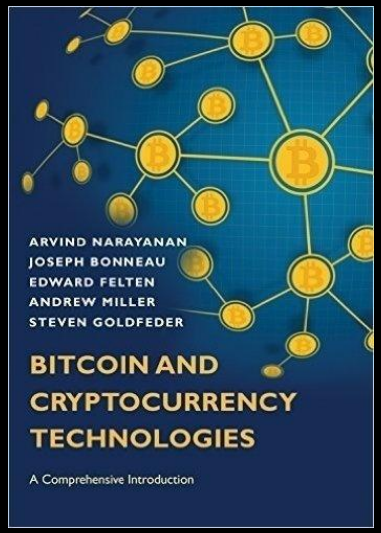
Bibliography

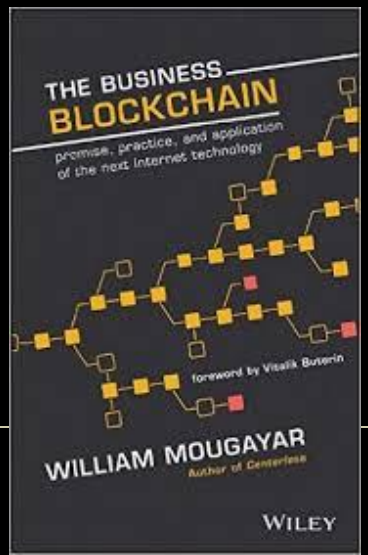


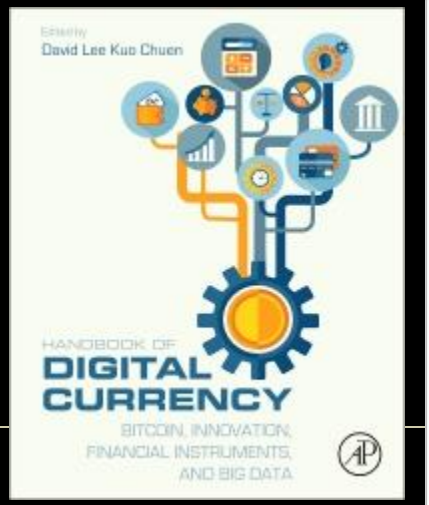


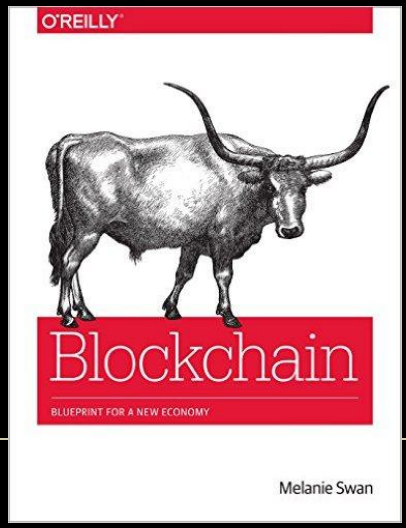






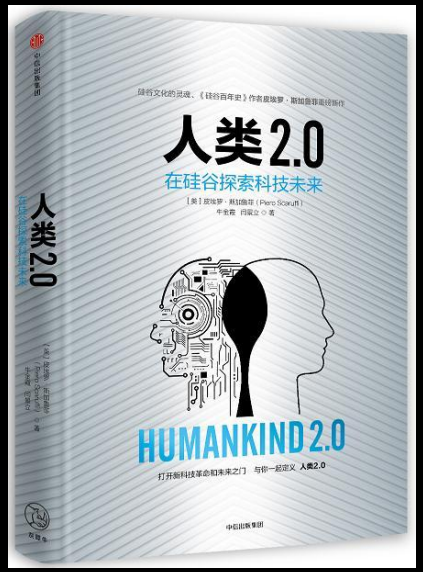


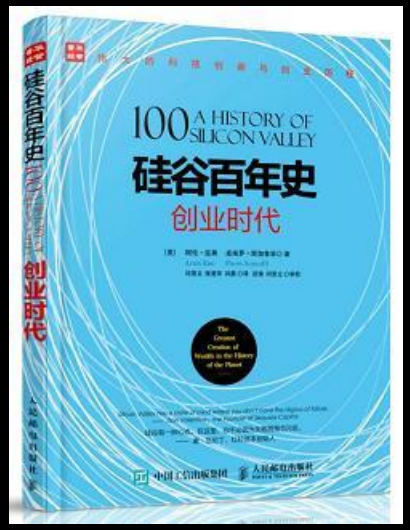


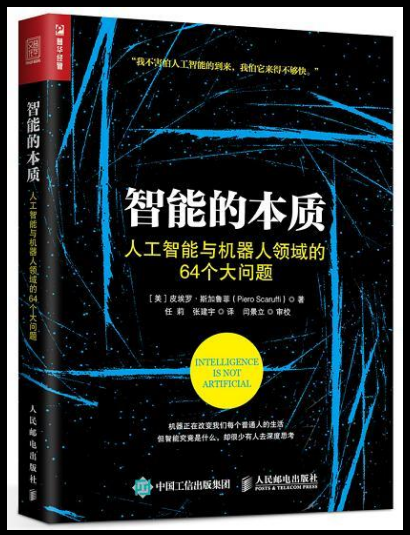


Contact

- www.scaruffi.com







This file: https://www.scaruffi.com/singular/ppt/blockchain.pdf