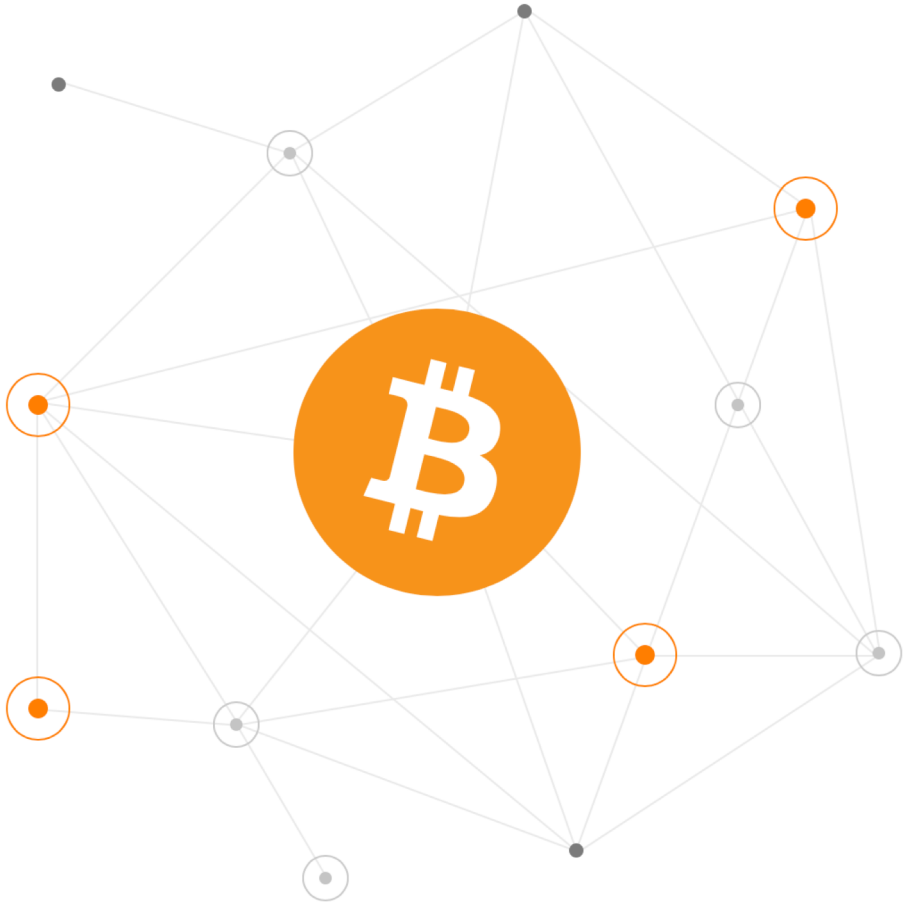
Decentralised Future Education Program

History of Bitcoin and blockchain & how to get started with crypto

bitfwd Community



NEXT GENIUS

Blockchain Technology

- Growing chain of blocks of data with each new block linking to its predecessor or ‘parent’
- Solution to time-stamping of digital documents
  - Duplication or falsification
- Cryptographically secured immutability

Bitcoin: A Peer-to-Peer Electronic Cash System

- Private electronic p2p value transfer

- Cypherpunk movement
  - Mailing list of 700 top cryptographers in the world
    - Developer of the Tor network
    - Julian Assange

  - “Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. (…) Privacy is the power to selectively reveal oneself to the world.”
    - Creating a new society through the internet

Bitcoin: A Peer-to-Peer Electronic Cash System

- 1982: “Digital cash” or “ecash” by Dr. David Chaum
  - “Make big brother obsolete”
- 1998: “b-money” by Wei Dai
  - “individual database” & “incentivized parties”
- 2002: “hashcash” and “Proof-of-Work” by Dr. Adam Back
  - Hash: algorithm that maps data of a certain size into a bit string of fixed size
  - Add costs to make spam infeasible
- 2004: “Reusable-Proof-of-Work” by Hal Finney
  - Transformed hashcash into unique tokens used only once → UTXO
  - Ledger kept by centralized servers
- 2005: “bit gold” proposal by Nick Szabo
  - Vulnerable to Sybil attacks
  - Coined the term ‘smart contract’

Bitcoin: A Peer-to-Peer Electronic Cash System

- September 2008: Bankruptcy Lehmann Brothers
- October 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System“
- A decentralized P2P protocol of tracking the ownership of electronic coins via a public ledger
  - Nodes can sign over ownership
  - Every node keeps their own ledger
  - Sub-section are incentivized to add blocks to the chain via POW.
    - Consensus: Most work expended = longest chain propagated through the network
- -cue banking on bitcoin opening @ 2.56

Bitcoin: A Peer-to-Peer Electronic Cash System

- “Commerce on the internet relies on trusted third parties for transfers”
- Credit shift vs. cash handover
- Reversible transactions
  - More trust required
    - KYC/AML
- Payment based on cryptographic proof
  - “routine escrow mechanisms could easily be implemented to protect buyers”

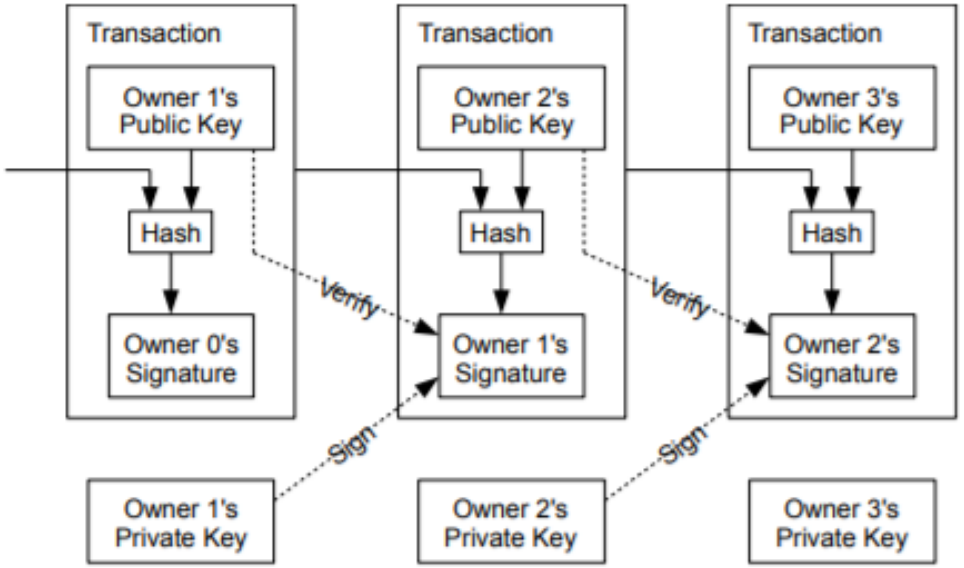
Bitcoin: A Peer-to-Peer Electronic Cash System

- “a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.”

- a coin is a chain of digital signatures
  - Transferring balances between public key addresses, with private keys

- By keeping track of all transactions, you know the origin of each coin

Bitcoin: A Peer-to-Peer Electronic Cash System



Owner 1 uses a previous transaction to prove he has coins on his address and creates a transaction with Owner 2 and uses his private key to create a signature that proves he controls this address and signs ownership over to Owner 2.

A hash is a one-way function that, given the same input, will create the same output. The ‘proof’ is the ability to recreate the end-hash of a transaction. All transaction details are public, except your private key mixed into the signature.

Bitcoin: A Peer-to-Peer Electronic Cash System

- Transactions within a block are hashed together and provided with a time stamp and propagated through the network.

- These blocks of information linking back to their predecessors will form a chain.

Bitcoin: A Peer-to-Peer Electronic Cash System

- POW: spending computing power by changing a nonce added to a block of hashed transactions in order to find a very low number that fits the protocol's goal structure
- POW ensures honesty in the chain by requiring 'miners' to spend computing power in order to be able to add a block to a chain.
- The longest chain incurred the most and honest work and is considered the truth.

Bitcoin: A Peer-to-Peer Electronic Cash System

- Transactions are sent throughout the network and added to a pool
- Miners combine these transactions into blocks of fixed size
- Spend computing power to solve their puzzle first
- The first to solve their puzzle broadcasts their solution to the network
- The network checks the validity of all transactions
- True? Miners accept their loss (‘I didn’t work hard enough’) and create a new block linking back to the freshly added block in the chain and try to solve the puzzle

Bitcoin: A Peer-to-Peer Electronic Cash System

- Miners spend computing power to keep the ledger honest

- Incentivized by:
  - Block rewards for solving the puzzle roughly every 10 minutes
    - To stumble upon the solution after labourious numbercrushing is like striking gold
    - Currently 12.5 BTC, halved every 210 ‘000 blocks
    - Next ~ May 2020
    - ~2140: 21 million btc in circulation
  - Transaction fees

Bitcoin: A Peer-to-Peer Electronic Cash System

- Save space by removing the physical input details but keeping a hashed version of it.

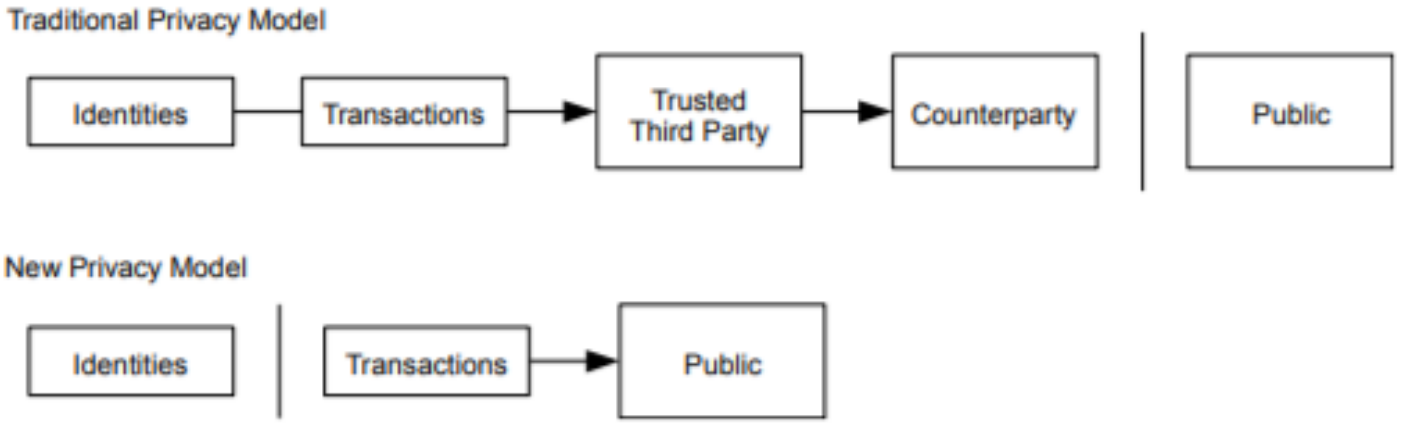
- To keep disk space manageable for everyone i.e. ‘accessible to everyone’
  - Ethereum blockchain > 1 TB

Bitcoin: A Peer-to-Peer Electronic Cash System

- Light nodes: only download the summaries or ‘headers’ of transactions
- Requires trust in other nodes for the longest chain and origin of coins

Bitcoin: A Peer-to-Peer Electronic Cash System

- Privacy



Bitcoin: A Peer-to-Peer Electronic Cash System

System safety

- Nodes will never accept invalid transactions of an attacker claiming previously un-owned money
  - Attackers controlling a network can only tamper with ‘their own’ transactions
- 51% attack refers to the ability to have a higher probability of consistently adding new blocks to the chain before others
- Multiple chains are possible temporarily, wait several blocks for definitive confirmation

Bitcoin: A Peer-to-Peer Electronic Cash System

- P2p network
- Permissionless
- Trustless
- Censorship resistant.
- Immutable data.
- Cryptographically secure.
- Consensus mechanism.

Cryptocurrencies disclaimer

- The information in this presentation and the links provided are for general information only and should not be taken as constituting professional advice from the presenter- Me, Jasper Verhoeven
- I am not a financial adviser. You should consider seeking independent legal, financial, taxation or other advice to check how the presentation relates to your unique circumstances.
- I am not liable for any loss caused, whether due to negligence or otherwise arising from the use of, or reliance on, the information provided directly or indirectly, by use of this presentation.
- Please do your own due diligence and research, for I am merely a student like you

Top 100 Cryptocurrencies By Market Capitalization

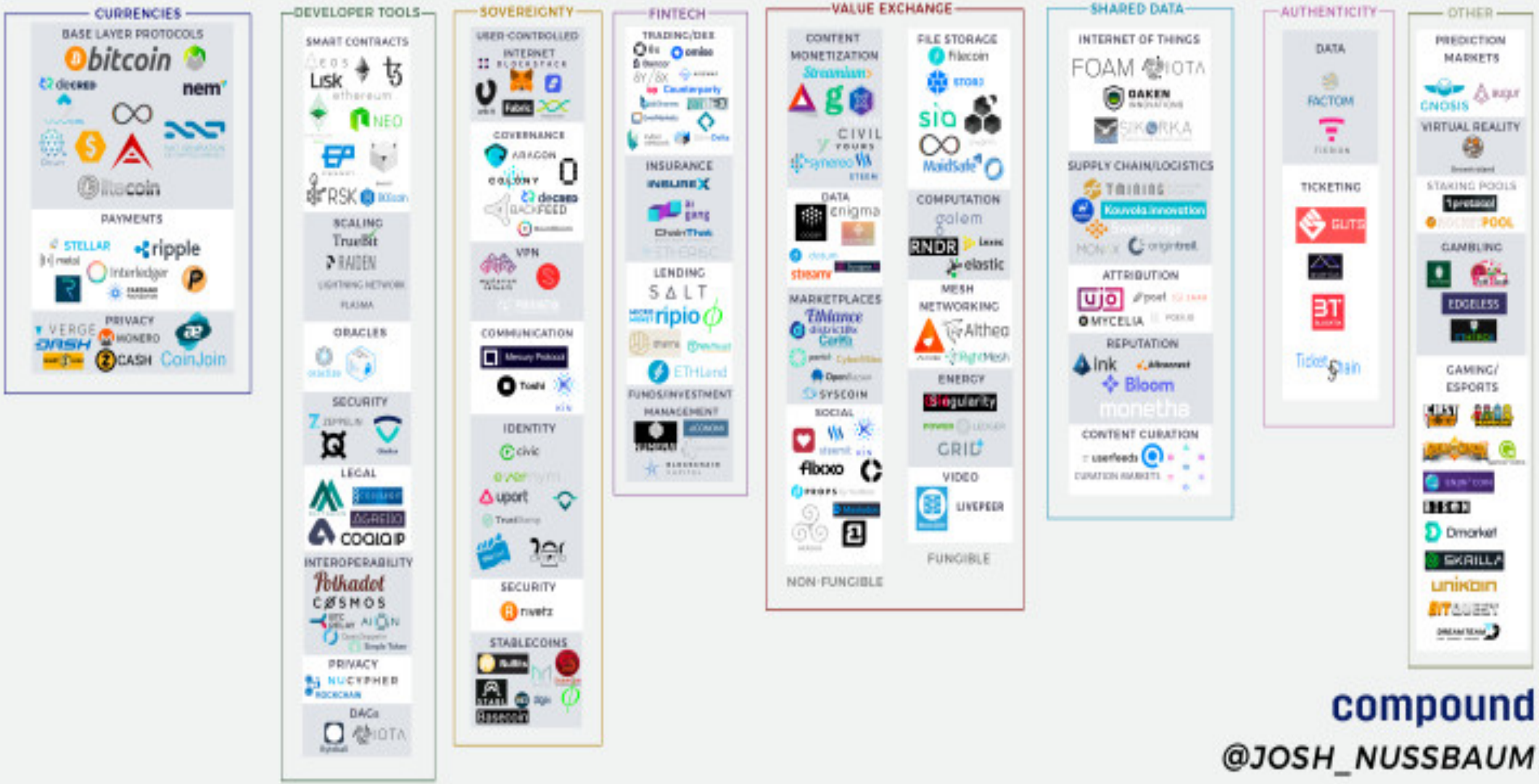
Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$111,235,322,862	$6,466.99	$4,297,549,607	17,200,475 BTC	1.71%	
2	Ethereum	$36,604,258,638	$361.59	$1,618,824,211	101,231,573 ETH	-0.55%	
3	XRP	$13,352,403,587	$0.339757	$296,700,457	39,299,874,590 XRP *	-3.69%	
4	Bitcoin Cash	$10,411,928,527	$602.39	$327,217,256	17,284,450 BCH	1.10%	
5	EOS	$5,180,804,180	$5.72	$706,796,975	906,245,118 EOS *	-0.20%	
6	Stellar	$4,117,642,874	$0.219357	$80,634,418	18,771,402,105 XLM *	5.65%	
7	Litecoin	$3,623,743,635	$62.71	$259,106,936	57,785,307 LTC	-1.69%	
8	Cardano	$3,173,427,765	$0.122398	$90,630,405	25,927,070,538 ADA *	1.92%	
9	Tether	$2,419,005,413	$1.00	$2,627,548,353	2,407,140,346 USDT *	0.31%	
10	IOTA	$1,753,565,392	$0.630886	$48,102,624	2,779,530,283 MIOTA *	-2.16%	

Cryptocurrency mania

- The internet of the early ’90s
  - Everyone creates their own protocol and is trying to be better or different to ‘win’ the market and dominate
    - Conveniently have their own payment model
    - ICOs ‘were’ the new crowd funding
  - “We do blockchain, not Bitcoin”
  - “A blockchain would be great in my industry. However not a public one. I remain in control of admission and data finality. ”

BLOCKCHAIN PROJECT ECOSYSTEM



compound

@JOSH_NUSSBAUM

How to get cryptocurrencies?

Standard issue government legalized tender aka “Fiat”

coinbase

CoinSpot

COINJAR

Consider your storage options!

Time, electricity and disk space consuming

coinbase

CoinSpot

COINJAR

Could be hacked

METAMASK

Convenient, but online

Secure, but costly

Decentralised Future Education Program

Thanks guys!