Blockchain

Currencies and Platforms

Eoin Connolly

money

- **rai stones** in Yap Island
- **cowry shells** in Kenya
- **barley** in Mesopotamia
- **paper money** in China, backed by metal
- **fiat** currency
- **digital** money
- **cryptocurrency**

gold

- Store of value for **8000** years
- Corrosion resistant
- Fungible
- Rare/Scarce (165,000 metric tons)
- Pretty
- USA left gold standard in 1933
- (USA banned personal ownership of gold in1933 via Executive Order 6102)
- **8 Trillion** USD market cap

Precursor Digital Currencies

1

David Chaum's **Digital Cash**

- Paper published in 1983, used PKI to secure transactions
- Mark Twain Bank in Saint Louis MO 1995 – 1998
- Never widely adopted on internet, overtaken by VISA
- Bankrupt in 1998

2

e-gold

- Backed by gold
- Mobile transactions (on Palm Pilot)
- Popular with hackers and criminals
- In 2008, 3 directors pled guilty to running an illegal money transmitter

What makes bitcoin different to these other digital currencies?

Bitcoin – a decentralised cryptocurrency

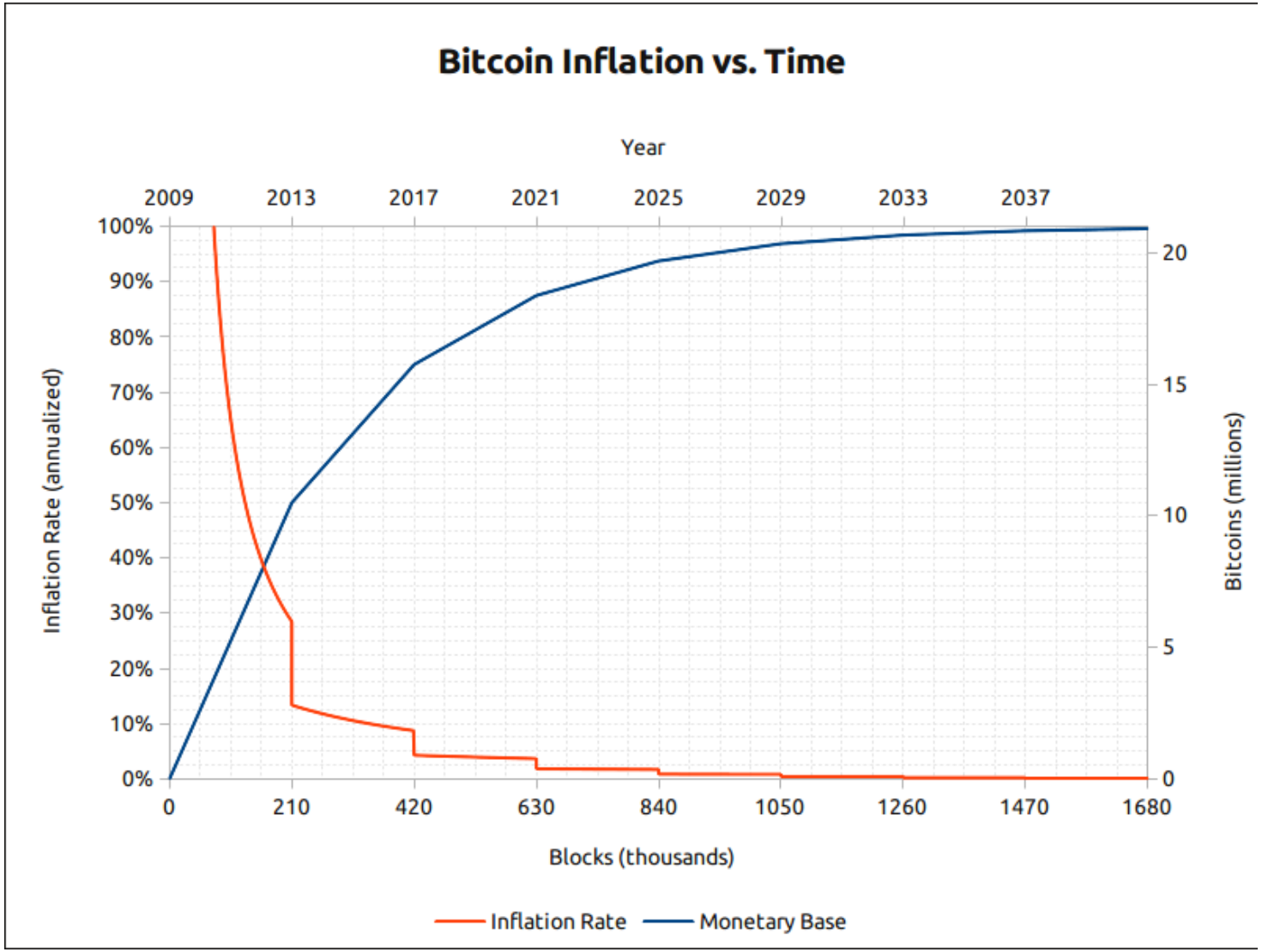
- Decentralised
- No controlling entity – no offices to raid, no creator to arrest
- No governance
- Who created it?

Satoshi Nakamoto

- Wrote the white paper
- Wrote the first implementation – still under development today
- Not his/her real name
- All interactions conducted over Tor to protect IP address
- Stepped away from ecosystem after two years
- Has not spent any of the 1,000,000 coins mined (current value: 11 Billion USD)

Bitcoin Issuance over time

- Bitcoin is issued by mining a block
- Block reward is 6.25 BTC + fees
- There will only ever be 21 million BTC issued
- The genesis block issued 50 BTC
- This halves every 4 years, currently only 6.25 BTC are issued in each block
- All BTC will be issued by ~2140



China bans bitcoin

- China bans ICOs
- China bans exchanges
- China bans OTC exchanges
- China bans mining?
- China bans bitcoin?

- What have Gmail, Youtube, Twitter, Facebook, Github, Instagram, Slack, Vimeo, DuckDuckGo, Tumblr, Reuters, Flickr and the New York Times got in common?

- What happens to bitcoin if it is banned in China?

Properties of Money

- Medium of Exchange
- Unit of Account
- Store of Value

Medium of Exchange

1

Fiat Examples

- Cash transaction
- Bank transfer
- Credit/Debit card interaction

2

Question: How does bitcoin compare from a privacy, cost and scale perspective?

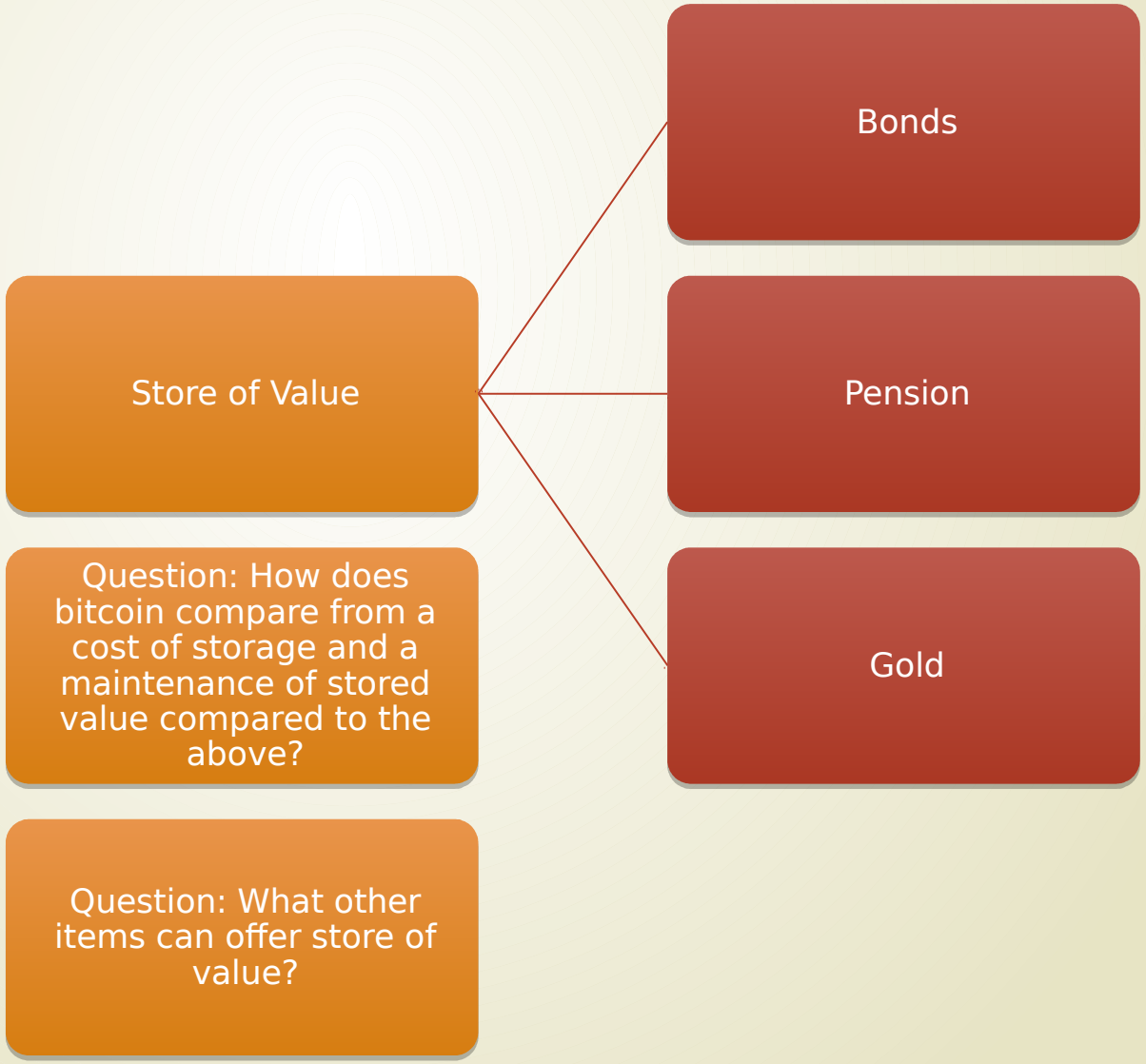
In 2010, Laszlo bought 2 pizzas for 10,000 BTC, then worth 41 USD.

Unit of Account

- Have a standard numerical unit of measurement
- Like the dollar, yen, euro etc.

- One bitcoin is made up of 100,000,000 satoshi
- Fun fact: thanks to hyperinflation, by 2017, 1 satoshi had the same value as 1 Venezuelan Bolivar
  - https://cointelegraph.com/news/in-bitcoin-testbed-venezuela-1-bolivar-now-equals-1-satoshi

Store of Value



Money must be

- Fungible (all coins are equal if they have the equal value)
- Durable (capable of being used repeatedly)
- Divisible (can be divided into smaller units)
- Portable (can be carried and transferred)
- Acceptable (others should accept your money for transactions)
- Limited in Supply (infinite supply of money = hyperinflation)
- Uniform (all coins of same value the same – e.g. not diamonds)

Does cryptocurrency fulfil these criteria?

- Do cryptocurrencies like BTC/ETH fulfil the criteria for money?
- Are there different requirements for a cryptocurrency that purely wants to be a store of value – a digital gold, rather than a coin for buying coffee?
- How important is privacy in our transactions?
- What about stablecoins like DAI/SAI, USDT, USDC?
- What about Libra?

Scale

- Assuming cryptocurrencies solve fungibility and privacy, would they be able to replace money?
- BTC is limited to 3 – 5 transactions per second, ETH 10 – 15 per second
- If Venezuela only had bitcoin, each citizen would be able to make one transaction every two weeks, not good enough for money
- Currently bitcoin blockchain is < 300GB with 1MB blocks created every 10 minutes (note: blocks can be larger than 1MB thanks to segwit – segregated witness means not counting transaction signatures as part of block size. Segregated Witness is scaling mechanism)

Platform	Transactions Per Second
Bitcoin	**3 – 5**
Ethereum (public)	**10 - 15**
Ethereum (private)	**100 - 400**
SWIFT	**300**
Paypal	**500**
Hyperledger Fabric (private)	**700**
VISA (standard)	**2,000**
VISA (peak)	**65,000**
Alipay (singles day)	**255,000**

Scaling Bitcoin

- Ongoing challenge
- Conference held annually to showcase new scaling mechanisms (Scaling Bitcoin, Nov 2017 Stanford University)
- Target is 1 million transactions per second
- Cannot be all scaled on chain – would require petabyte blocks
- Off-chain scaling mechanisms currently being developed
  - Lightning Network (Bitcoin, Litecoin)
  - Raiden Network (Ethereum)
- Off-chain scaling networks are 12 – 24 months away * (more later)

** optimistic*

100 flavours of bitcoin

- 2017 brought us forks: bitcoin cash and bitcoin gold
- Ethereum forked after the DAO hack into ETH and ETC (Ethereum Classic)
- As exchanges have fiduciary duty to provide customers with their funds, these hard forks are likely to continue

- Question:
  - When a chain forks to create a new coin, does this benefit the ecosystem?

Other Cryptocurrencies

- There are close to 1000 other cryptocurrencies, not counting ICOs created on existing platforms like Ethereum
- 600 are forks of Bitcoin’s code, such as Litecoin
- Some are new and don’t have a blockchain, like IOTA
- Some have a particular property, like Monero’s privacy
- Some are centralised, like Ripple (or IOTA)
- Some are closed source, some are open

Other Platforms

- Ethereum
- Litecoin
- Monero
- Tezos
- IOTA

Ethereum

- Mines blocks every 15 seconds
- Has a native currency, Ether
- 5 Ether released in each new block
- No limit on Ether released (will require hard fork to change)
- Has forked multiple times, once creating a split currency (Ethereum Classic)
- Has Turing-complete smart contracts

Litecoin

- Fork of bitcoin code
- Mines every 2.5 minutes
- Fixed issuance of 84 million litecoin
- Functionally identical to bitcoin – also has segwit enabled
- Cross chain atomic swaps possible with bitcoin (more later)
- Silver to bitcoin’s gold
- Question: Is there a need for litecoin?

Monero

Has confidential transactions (hides amount, sender and receiver)

No issuance cap, but will reach limit of 1% inflation round 2022

Has 2 hard forks every year to introduce new features

Monero miners beginning to be used to replace ad revenue – potentially interesting space if it legitimises

IOTA

- More of a DAG (Directed Acyclic Graph) than a blockchain
- Designed for IOT use cases
- Created their own hashing function (turned out to be insecure)
- Application written in ternary rather than binary
- 10kb transaction sizes
- Revealed to be highly centralised when closed course ITOA-controlled Coordinator service outage stopped transactions from being verified for 50+ hours