Blockchain

the future of blockchain

eoin connolly

2020

blockchain

is a regular, predictable, digital pulse that can be trusted not to be changed (because at least you run a node)

the pulse is tiny, and you pay by the byte

and the possibilities the concept opens up (like replacing money) then creates more blockchains and off-chain anchored transactions and proof of stake and tokens to help make it happen

all decentralised, including storage and messaging

and now the question is

once we build it (and we reckon we can) what will we do with it?

stablecoins

Answer to the volatility challenge of traditional cryptocurrencies

Can be deposit-based (USDC, USDT) or algorithmic (DAI)

Trusting link between token and physical asset a challenge

With Facebook bringing out Libra (Diem) in 2021, there will be more regulatory attention paid to stablecoins (STABLE act) in an effort to stop Facebook from undermining central banks

Digital Yuan is also coming, but not necessarily on chain

Multiple countries looking at CDBCs (France, Thailand, Sweden, Switzerland, The Philippines)

DAI Algorithmic Stablecoin

Runs off smart contracts on ETH mainnet

Deposit ETH to withdraw DAI

Collateral must not fall below 150% (liquidation + penalties)

Originally was just ETH, but evolved into a mixed bag of assets (ETH, BAT, wBTC, USDC)

Assets like USDC only require 101% collateral (101 USDC give you 100 DAI)

Arbitrage opportunites in small DAI volatility (e.g. exchange 100 DAI for 102 USDC)

DAI governance is controlled by MKR, a governance token (adjusting interest rates)

Tradfi & blockchain

US Banks can offer crypto custody as of 2020

https://www.coindesk.com/banks-in-us-can-now-offer-crypto-custody-services-regulator-says

As banks offer crypto custody services, and crypto custody services are forced to obtain banking licences, the lines between the two will blur

But, banks will move slowly into the crypto custody space – regulatory and compliance concerns, ancient technology, risk aversion, failed ‘blockchain’ innovation experiments all contributing to the slow uptake

European banks not forbidden from holding crypto, but AML challenges around origins of the coins and a lack of regulatory clarity will slow the process

Still a focus on private blockchains (JP Morgan coin), rather than use of mainnet is also slowing the uptake

Regulatory focus on not repeating the mistakes of 2008 will also slow down traditional banks from crypto adoption/usage

Private vs Public Blockchains

- Public Blockchains:
  - Can be decentralised (ETH, BTC), but (semi)centralised chains are also possible (EOS)
  - Have fixed issuance rules (no minting of base currency by centralised agency)
  - Restrict access only by token ownership and internet connection
  - Censor transactions with difficulty (requires miner collusion)
  - Are trustless – participants rely on monetary incentivisation, rather than trust
  - Require a hard fork to reverse transactions (ETH DAO Attack)
  - Have no single governing body (although centralising elements such as Bitcoin Core, Ethereum Foundation do exist)
  - Being decentralised, public blockchains have no clear governance and rely on miner voting + social elements (UASF)

Private vs Public Blockchains

- Private Blockchains:
  - Are centralised with validation being performed by small number (<30) of trusted, legally-onboarded validators
  - Restrict access to the chain data via onboarding process
  - Typically have official governance body and operating body (can be same org)
  - Require a level of trust between participants
  - Censorship of transactions, reversion of transactions usually required and enabled
  - Participants can be added/removed by rule of central agency (governing body)
  - Do not use Proof of Work, but instead rely on PBFT, POA, RAFT etc.
  - Governing Body can mint tokens (if they have a token)
  - Governing Body can burn tokens (if they have a token)
  - Essentially expensive, slow databases

ETH 2.0

- Live Dec 2020
- Blocks every 12 seconds
- 20k validators using BLS signatures to confirm blocks every epoch (6 minutes)
- 32 ETH in ETH1.0 contract required to stake
- Rewards about 2ETH per year per validator
- Blocks are basically empty, so is test of consensus mechanism only
- RandDAO used to determine block validator randomly
- All validators participate in epoch validation
- Inactivity or invalid activity causes slashing (.25ETH stake removed)
- Essential first step to a decentralised POS sharded chain

Challenges

- Quantum Computing breaks Elliptic Curve cryptography
- Fusion energy reducing cost to attack POW chains
- Coordinated government regulation eliminates ability for retail investors to hold cryptocurrency
- Taxation on gains, not at outflow could reduce desire to hold crypto
- Increased regulation stifles innovation and tradfi steps in with regulated private-chain stablecoins with concealed accountability and censorship
- Ownership of cryptocurrency becomes illegal (similar to ownership of gold in US early in 20th century)

Potential Future Activities

- Pegged assets such as stocks issued similar to USD-backed stablecoins
- Fractional ownership of property (large regulatory difficulties)
- IPOs performed on chain (token launches)
- Enterprise Tokens to avoid ownership of ETH by enterprises
- Tradfi payment rails accepting using cryptocurrencies (Paypal (BTC, ETH, LTC, BCH), Visa (USDC)) will accelerate adoptions
- Institutional investment in BTC (e.g. Grayscale owns $600M of BTC) due to BTC being possible hedge against inflation/devaluation will reduce volatility and potentially increase price
- Central Banks could hold BTC, similar to Gold (but not soon!)

Conclusion

- Blockchain is not going anywhere, although private blockchains will continue to struggle for relevance
- The technology’s money equivalence combined with fast innovation loops will lead regulation until addressed systematically
- The killer use cases of blockchain are still SoV, ToV
- Summer of DeFi showed potential, but lessons need to be implemented
- Stablecoins will be focus of much short-term regulation (Facebook)
- Market is still tiny (1.5T) compared to TradFi(100T) Gold (8T)