Blockchain

Community, Politics and Regulation

Contents

- Technical, Business, Cultural, Ethical and Regulatory Challenges
- Stakeholders: who’s in charge
- Regulating and Mitigating Illegal Behaviours

Technical, Business and Cultural Challenges

- Technical
  - Privacy
  - Scaling
- Business
  - Use Cases for ‘blockchain’
  - Private blockchains vs public blockchains
- Cultural
  - Blockchain and criminality
  - Environmental harm

Privacy

- There are serious implications of every single one of your financial transaction being identifiable and traceable
  - great for Anti Money Laundering (AML)
  - great for Credit Risk Analysis
  - great for identifying advertising opportunities
  - great for cross marketing campaigns
  - great for deep health analysis (you are what you eat)
  - great for tracking social graphs
  - data scientists will never be out of work

Privacy combined with Control

- Now let’s add the ability to censor transactions into that mix:
  - great for preventing criminals buying things they shouldn’t (drugs, guns, etc.)
  - great for freezing/seizing criminals’ financial assets
  - great for identifying associates of criminals and freezing/seizing their assets as well, pending investigation
  - great for temporarily restricting purchases (no alcohol before 1200)
  - great for health (can’t buy more cigarettes/donuts today!)
  - great for restricting movement (on bail = cannot buy plane ticket/rent a car/buy fuel/take a taxi/train/rent a bike etc.)

Scaling (recap)

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

- There are a few mechanisms to scale public chains
  - Ignore the public chain and use a private chain/database
  - Lots of centralised databases connected to public chains (exchanges, Liquid)
  - Side chains (BTC too expensive? Try ETH, or LTC, or xDAI or OMG)
  - Payment Channels (BTC, ETH)
    - Complex technically, use public chain as settlement layer, in operation now (Lightning Network ***) but very small operation (20k BTC). Capable of enormous scale (500k TPS)
  - ZKRollups (ETH)
    - Complex technically *, still work in progress
  - Plasma Chains
    - Complex technically, still security considerations, none in operation currently **

* https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups/
** https://docs.plasma.group/en/latest/src/plasma/sidechains.html
*** https://decrypt.co/resources/bitcoin-lightning-network

Business Challenges

- Years of enterprise blockchain projects using private blockchains
- Not appreciably different to a central service with a DB
- Ignore the primary novelty of blockchain (consensus) in return for shared traceability/accountability
- Ignored cryptocurrency use cases, to avoid being tainted by BTC association
- Tendency to inject a slow, expensive database into a digitisation need to gain differentiation from other platform

*

Business Challenges – Use Cases

- Production enterprise blockchain platforms rare, while actual production blockchain platforms common:
- Exchanges – regulated or unregulated, handling billions of $$$
- Wallets
- Custody Solutions (Xapo, Coinbase Custody)
- ICOs as VC replacement
- Decentralised Finance platforms
- Now: staking services
- All of the above are linked to public blockchains and cryptocurrency, not * business processes and a desire to inject a blockchain into a use case

Business Challenges

- Focus on private chains by enterprise
  - Unwillingness to interact with public chains (BTC taint)
  - Obsession for transactional throughput (“we need XTPS”)
  - Fear of public blockchain failure *
  - Fear of lack of privacy due to obsession with putting data on chain (Quorum)
  - Desire for control of the platform in the hands of a few friendly corporations
  - Need to interact with ‘trusted’ entities, not wild and woolly internet people
  - Ignoring SoV, ToV use cases entirely

* https://www.ethstats.net/

Business Challenges

- Private chains
  - Are basically a slow, expensive database
  - Require a governing body/organisation
  - Lends itself to trusted third-party paradigms
  - Require expertise/OPEX to run **
  - Have limited privacy, leading to complex privacy solutions
  - Limited to small numbers of validators (<20)
  - Are blockchains in name only, like calling Excel a database

* https://www.ethstats.net/

** https://www.kaleido.io/

Cultural Challenges

- Bitcoin is mostly used by criminals
- Blockchains are mostly ponzi schemes
- Not sound money (like gold, EUR, USD)
- ICOs are mostly scams
- Too volatile to be money
- Cannot inflate, therefore cannot control inflation
- Cannot create credit, because coins must exist *

* https://www.youtube.com/watch?v=PHe0bXAIuk0

Environmental Challenges

- Bitcoin uses the electricity equivalent of Ireland
- Each Bitcoin transaction can power a home for a year
- Why burn electricity for nothing?
- Note:
  - BTC uses ~80TWh annually
  - EU uses ~20,000TWh annually
  - Transport uses ~ 30,000TWh annually *
- Energy usage from non-renewable resources is an issue
- POW chains convert energy to stored money (sort of)

* https://digiconomist.net/bitcoin-energy-consumption

** https://web.archive.org/web/20131014221749/http://webbshop.cm.se/System/DownloadResource.ashx?p=Energimyndigheten&rl=default%3A%2FResources%2FPermanent%2FStatic%2Fe0a2619a83294099a16519a0b5edd26f%2FET2010_46.pdf

Ethical and Regulatory Challenges

- Ethical
  - Potential for complete financial transparency
  - Dystopian future (unpeople)
  - Hyperbitcoinisation – yet another large unproven experiment with money
- Regulatory
  - Banning of ICOs, Cryptocurrencies
  - Legal restrictions on ownership (similar to gold, 1933)
  - Right to be forgotten
  - When cryptocurrencies become a threat to state-issued currencies…

Stakeholders: who’s in charge?

- Companies (Exchanges)
  - Does Coinbase, XAPO, Gemini, Bitfinex control bitcoin?
- Miners
  - Blocked Segwit for months
  - After UASF threat, forked to Bitcoin Cash
  - Can disrupt minority chains (hidden reorgs, 51% attacks)
- Developers (Bitcoin Core, Ethereum Foundation)
  - The individuals that maintain the bitcoin codebase can block subjectively bad ideas
  - Ethereum hopes Vitalik will solve all problems
- Full nodes, wallets?
  - Full nodes can cause forks with coordinated effort (UASF)
- Hodlers
  - Do crypto whales have power? 40,000 BTC exchanged to pump BCH in Nov, 2017

Regulating and mitigating illegal behaviours

- KYC/AML Regulations
  - Required to buy cryptocurrencies, not required for trades
- NYC Bitlicence
  - Stifled blockchain activity in New York, creator, Benjamin Lawsky, became blockchain consultant, ended up on board of Ripple
- Banning ICOs, or even cryptocurrencies
  - China has banned exchanges and ICOs. Malaysia threatened to ban all crypto
- SEC and Bitcoin ETFs
  - The SEC rejected the Winklevii attempt at a bitcoin ETF, but they have appealed and there are other ETFs coming
- Tether and the Bitcoin price

Crypto Corner: ECDH

- Diffie Hellman Key Exchange
- Using RSA: key exchange is relatively simple
  - Alice provides RSA public key
  - Bob encrypts secret S with Alice PubKey and returns
  - Alice decrypts S using Alice PrivKey
  - Alice and Bob use S to encrypt traffic

But what about using Elliptic Curves?

Crypto Corner: ECDH

- Diffie Hellman Key Exchange
- Using Elliptic Curves:
  - Alice provides Bob her PubKey
  - Bob provides Alice his PubKey
  - Alice uses Alice PrivKey and Bob PubKey to create secret S
  - Bob uses Bob PrivKey and Alice PubKey to create secret S
  - Alice and Bob use S to encrypt traffic

How is this possible?

Crypto Corner: ECDH

- Elliptic Curve basics:
- Private key is large number P
- Public key is P iterations around curve from generator point G
- G is the same for specific algorithms
- Private Key = P
- Public Key = G * P
- (very, very hard to get P from G*P)

https://www.youtube.com/watch?v=muIv8I6v1aE&t=32s

Crypto Corner: ECDH

- So Bob’s Public Key is G * P(b)
- And Alice’s Public Key is G * P(a)
- So Alice (using P(a) – has G * P(b) * P(a))
- And Bob (using P(b) – has G * P(a) * P(b))
- G*P(b)*P(a) = G*P(a)*P(b)
- So they can both get the same secret!