Blockchain

Blockchain Management

v1.0.0

Contents

- Transaction Types
- Use Cases
- Evolution of Blockchain to Date
- Storing and Using Cryptocurrencies
- Blockchain Ledgers
- Mining
- (Smart) Contracts
- Centralisation vs Decentralisation
- Distributed Consensus and Autonomy

Transaction Types

Transaction

- From Address
- To Address
- Amount
- Digital Signature

Ethereum Transaction

- Nonce (number used only once)
- GasPrice (how much you’re willing to pay for gas)
- GasLimit (how much gas you’re willing to consume)
- Recipient
- Value (can be zero – if it’s a contract interaction, for example)
- Data (can be empty – if it’s a value transfer, for example)
- Signature

The multi-signature transaction

- Available in Bitcoin, but not in Ethereum (without smart contract)
- N signatures required to perform interaction
- M of N signatures possible
- Many uses, such as wallets and forms foundation of layer 2 scaling in BTC

Transaction to Block

Use Cases

Source: Deloitte

Blockchain Use Cases

- Store of Value
- Transfer of Value
- Identity
- Asset Tracking (property, land, warranties)
- Track and Trace
- Trade Finance
- Counterfeit Protection
- Decentralised Finance

Store of Value

- Cryptocurrencies as digital gold
- Does not require medium of exchange properties
- Secure, transferrable, digital, global

Transfer of Value

- Digital transference of value via transaction
- No third party
- Global, digital, instant?

Asset Tracking

- Tokenisation of real world assets
  - Property
  - Land
  - Shares
  - Warranty
- Strict ownership of asset by private key
- Data migration issues
- Still need for real world entities
- Challenges associating real-world entity with digital asset

Track and Trace

- Blockchains not useful for collation of tracking and tracing data
- Typically tracking and tracing data provided to single entity
- Data monetisation shows promise
- Some benefits around multiple sources writing to common platform

Trade Finance

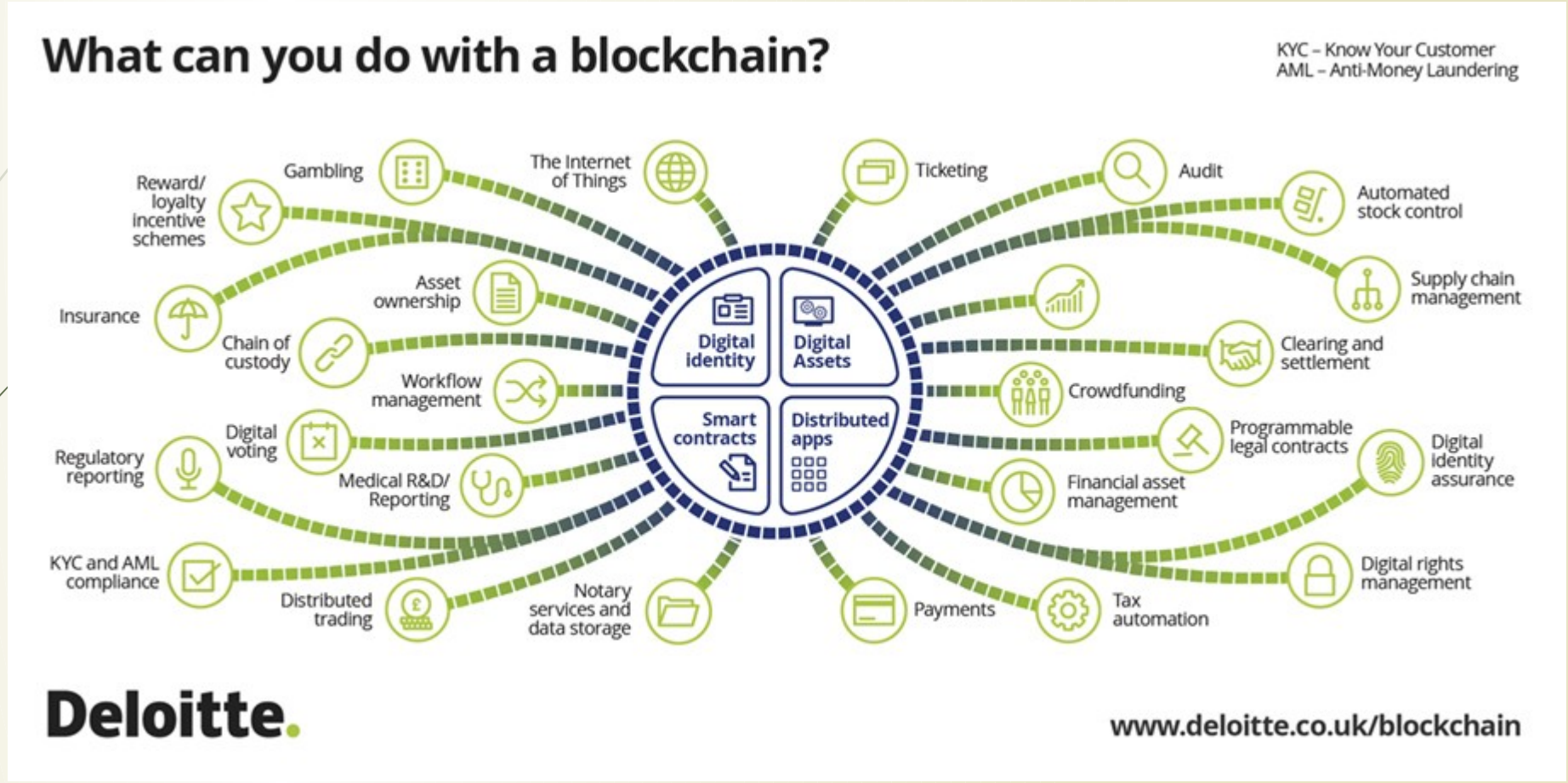
- Up to 50% of the cost of a shipping container is its paperwork
- A blockchain can act as the single source of truth
- Letters of credit – prevention of financing fraud
- Large ecosystem challenge, potentially a digitisation challenge, rather than blockchain challenge without sufficient network effects

Counterfeit Prevention

- Determination of chain of custody from manufacturer to purchaser
- Can only sell one counterfeit example
- Tokenisation of luxury good, loyalty schemes
- Blockchain?

Decentralised Finance

- Collaterlised Loans (DAI)
- Flash Loans
- Liquidity Providers
- Oracles
- Decentralised vs. Centralised exchanges


What can you do with a blockchain?
KYC – Know Your Customer
AML – Anti-Money Laundering
Reward/ loyalty incentive schemes
Gambling
The Internet of Things
Ticketing
Audit
Automated stock control
Supply chain management
Insurance
Asset ownership
Chain of custody
Workflow management
Digital identity
Digital Assets
Smart contracts
Distributed apps
Clearing and settlement
Crowdfunding
Programmable legal contracts
Digital identity assurance
Regulatory reporting
Digital voting
Medical R&D/ Reporting
Financial asset management
KYC and AML compliance
Distributed trading
Notary services and data storage
Payments
Tax automation
Digital rights management
Deloitte.
www.deloitte.co.uk/blockchain

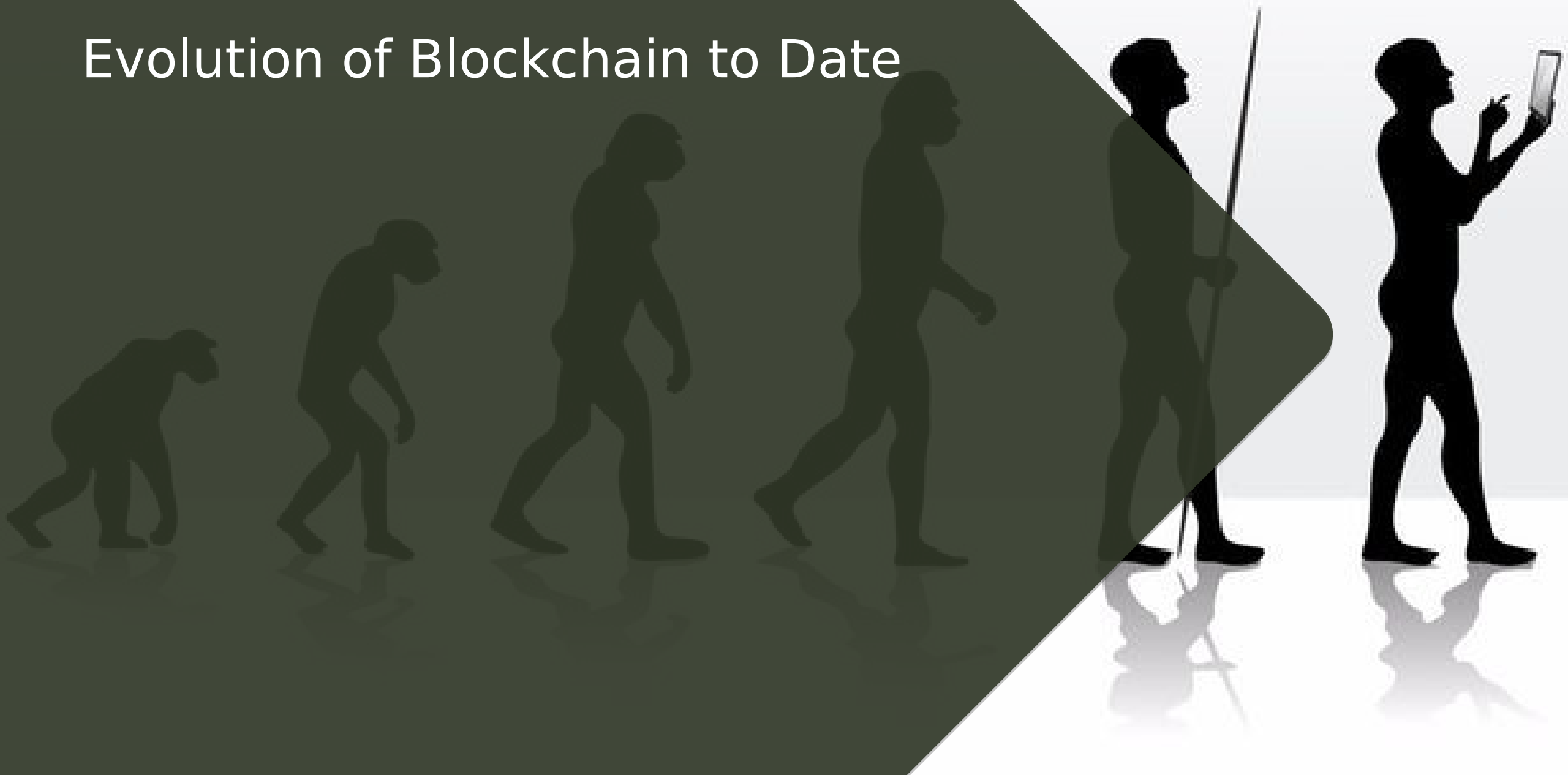
Blockchain Use Cases

- Other than its poor Medium of Exchange properties, bitcoin can also be used as the immutable, cryptographically signed and secured platform for a number of other uses
- Currently digital identities are owned by corporations (Google, Facebook, Twitter, Yahoo, etc.), rather than the individuals. How can blockchain provide an alternative to this?

Identity

- PKI at its core, identity backed by ownership of a private key
- Identity owner pattern (uPort)
- Key recovery and security
- Encryption key vs. Identity key (symmetric vs asymmetric encryption)
- Biometrics are username, not password
- Attestations
- Permissioned Sharing

Evolution of Blockchain to Date



Evolution of Blockchains

- Bitcoin
  - First decentralised cryptocurrency
  - Has limited scripting capabilities (to provide extensibility)
- Ethereum
  - Turing-complete smart contracts
  - Platforms can run directly on-chain

- Current focus is on Scaling and Privacy

Layer 2 Networks

- Lightning Network
- Raiden Network

- Use the blockchain as a settlement layer
- Uses payment channels
- A payment channel requires 2 transactions on-chain (open and close)

Payment Networks

- If Bob has a channel with Alice
- And Bob has a channel with Carol
- Alice can send payments to Carol, through Bob, with the participants updating their channel totals through a number of transaction swaps
- Performed by hashing secrets (Alice demands the secret off Bob, and Bob obtains it from Carol for the payment amount)
- To ensure Carol doesn’t just take Bob’s money, all transactions are hash time-locked transactions

- https://bitcoinmagazine.com/articles/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791/

Token Issuance (ICOs)

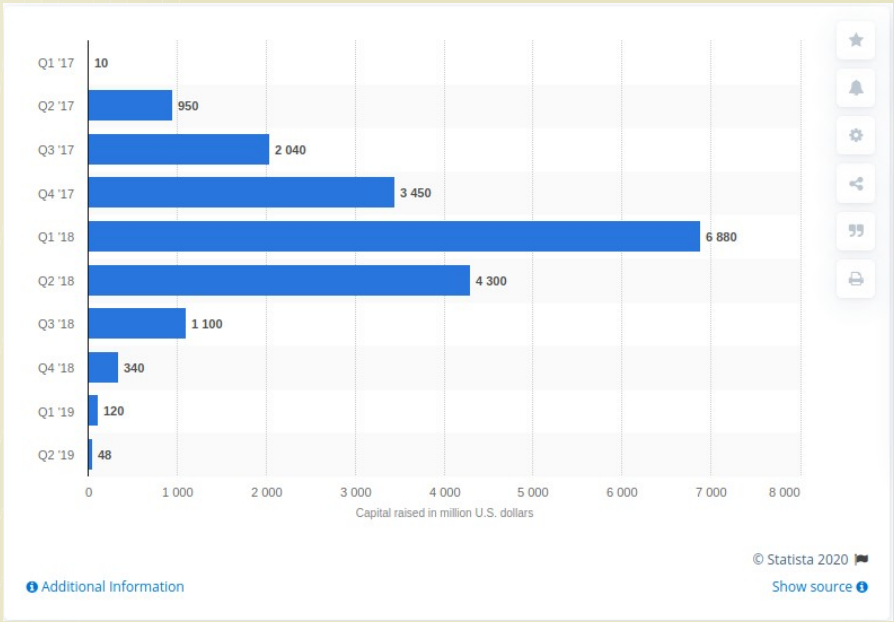
- ERC20 Token smart contract standard
- https://theethereum.wiki/w/index.php/ERC20_Token_Standard

```
// https://github.com/ethereum/EIPs/issues/20
 2 contract ERC20 {
 3     function totalSupply() constant returns (uint totalSupply);
 4     function balanceOf(address _owner) constant returns (uint balance);
 5     function transfer(address _to, uint _value) returns (bool success);
 6     function transferFrom(address _from, address _to, uint _value) returns (bool success);
 7     function approve(address _spender, uint _value) returns (bool success);
 8     function allowance(address _owner, address _spender) constant returns (uint remaining);
 9     event Transfer(address indexed _from, address indexed _to, uint _value);
10     event Approval(address indexed _owner, address indexed _spender, uint _value);
11 }
```


DID SOMEONE SAY ICO?

ICOs

- Issue a token for ether, with the rate set by the issuers
- The token will nominally be required for the platform
- The issuers can potentially create more tokens
- The token is not based on utility, and is the only code required
- ~~$2.4B raised in 2017~~
  - EOS: 4.2B
  - Gram: 1.7B
  - Petro: 735M
  - Filecoin: 257M
  - Ethereum: 5.2M



https://www.statista.com/statistics/804748/worldwide-amount-crytocurrency-ico-projects/

Scaling and Privacy

- Scaling
  - On-chain scaling will never work without centralisation occurring
  - Layer 2 networks required to provide required transaction throughput
  - Layer 3 network papers being released (lightning on lightning)
- Privacy
  - All data on-chain is visible to all participants
  - Data on-chain must either be encrypted or provide an anchor to off-chain data
  - Lightning transactions are private, but opening and closing states are public
  - Zcash, Monero provide private transactions via different mechanisms

Sharding

- Sharding is splitting the chain into multiple components, with each component only having to keep track of its own data
- Communication with other shards will be via asynchronous transactions
- Sharded chains do not have to be compatible
- Sharded chains are likely to have varying levels of security (particularly compared to the main chain)

Distributed Computing

- Paid to provide CPU cycles
- Paid to provide output to signed code
- Requires payment channels rather than on-chain transactions

Mixers and Tumblers

- Send your coins to a service
- Your coins get mixed with other coins and you get someone else’s coins
- Breaks the chain of custody of coins
- Requires trust of mixing service
- Some currencies (Dash) mix by default
- Mixing creates tainted coins (fungibility concern)
- Risk of a smaller than expected anonymity set

Ring Signatures

- Anyone in a group of keys can sign the transaction
- Computationally infeasible to determine who actually signed the transaction
- Invented by Ron Rivest, Adi Shamir, and Yael Tauman in 2001.
- Used by Monero to provide privacy

Zero Knowledge Proof

- Can be used to reveal a proof of a secret, without revealing the secret
- New crypto, “"The Knowledge Complexity of Interactive Proof-Systems" written in 1985 by Shafi Goldwasser, Silvio Micali, Charles Rackhoff
- Used in Zcash to prove the validity of a transaction without revealing the sender, recipient or amount
- Confidential transactions not mandatory in Zcash, and a confidential transaction takes several minutes to create

Homomorphic Encryption

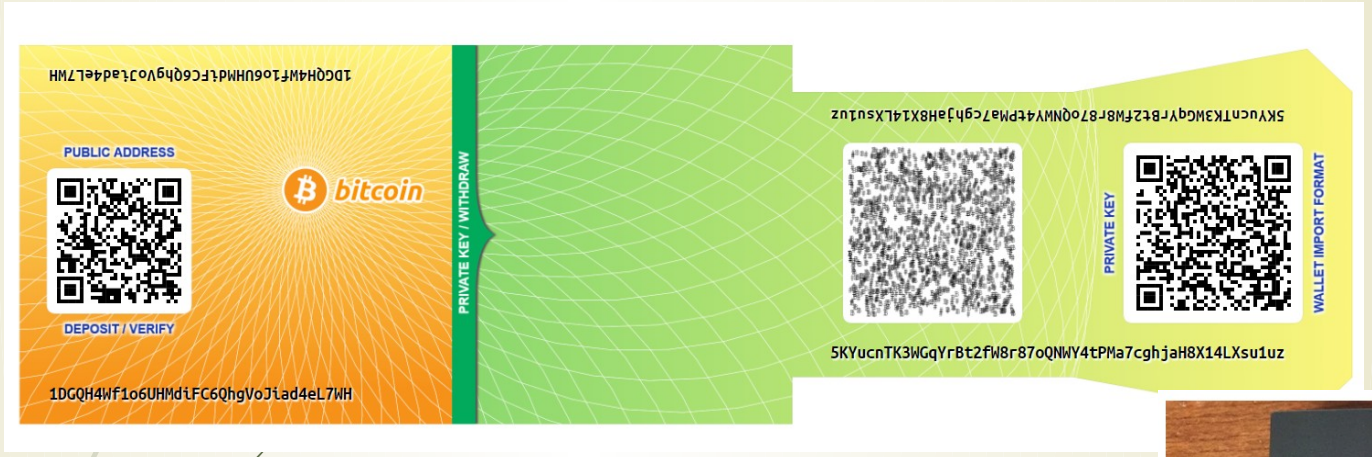
- Enables computation on encrypted data
- For example, adding an encrypted number to another encrypted number to provide a new encrypted number that is a sum of the inputs
- Computationally expensive, but getting faster slowly

Storing and Using Cryptocurrencies

Storing and Using Cryptocurrencies

- Exchange (trusted third party: Coinbase, XAPO, Bitfinex)
- Full Node
- Software Wallet (mobile phone, PC)
- Paper Wallet
- Hardware Wallet

Paper & Hardware Wallets



Blockchain Ledgers

Private Blockchains

- Ethereum
  - Uses public Ethereum client (Geth, Parity) or private (Quorum)
  - Gas not a concern, no value in private Ether
  - Can use different consensus mechanisms (PoA, PBFT)
- Hyperledger
  - Created by IBM, now open source (Hyperledger Foundation)
  - private only, no public implementation
  - contains centralised components (ordering service)
  - has private channels & high transaction throughput (700 tps)

Mining

Mining

- Mining is the validation of blocks of transactions
- Proof of Work mining involves hashing the block with a nonce to obtain a hash below a certain value
- Proof of Work mining makes generating a valid block difficult to prevent the network being flooded with invalid blocks (PBFT solution)
- Attempts underway in Ethereum to move to Proof of Stake

History of Mining

- Initially mining was performed on desktop/laptop CPUs
- Then it moved to GPUs
- Then ASICs – specific chips whose only purpose is mining

- No longer efficient to mine without ASICs, and cheap/free electricity is essential to maintain profitability
- Note that Ethereum uses ASIC-resistant hashing algorithm (ethhash, variation of Dagger-Hashimoto), so GPUs must be used

Mining Centralisation

- Main mining hardware companies
  - Bitmain
  - Bitfury (don’t sell their hardware)
  - GMO (coming – but might be private operation)

- Additionally 60% of bitcoin mining operations are based in China
- Possibility that 10 individuals control 60% of mining power

Centralisation vs Decentralisation

Centralised Systems

- Excellent potential control and governance
- Rigorous onboarding (KYC)
- Trusted Third Parties
- Scale and Privacy
- Honeypots (2017 Equifax, 2006 Israeli Theft)
- Centralisation of Biometric Data ongoing (Aadhaar – 1bn biometric identities)

Decentralised Systems

- Poor governance by design
- Limited user tracking
- No central data source
- No trusted third parties
- Limited scale
- Censorship resistance

Distributed Consensus

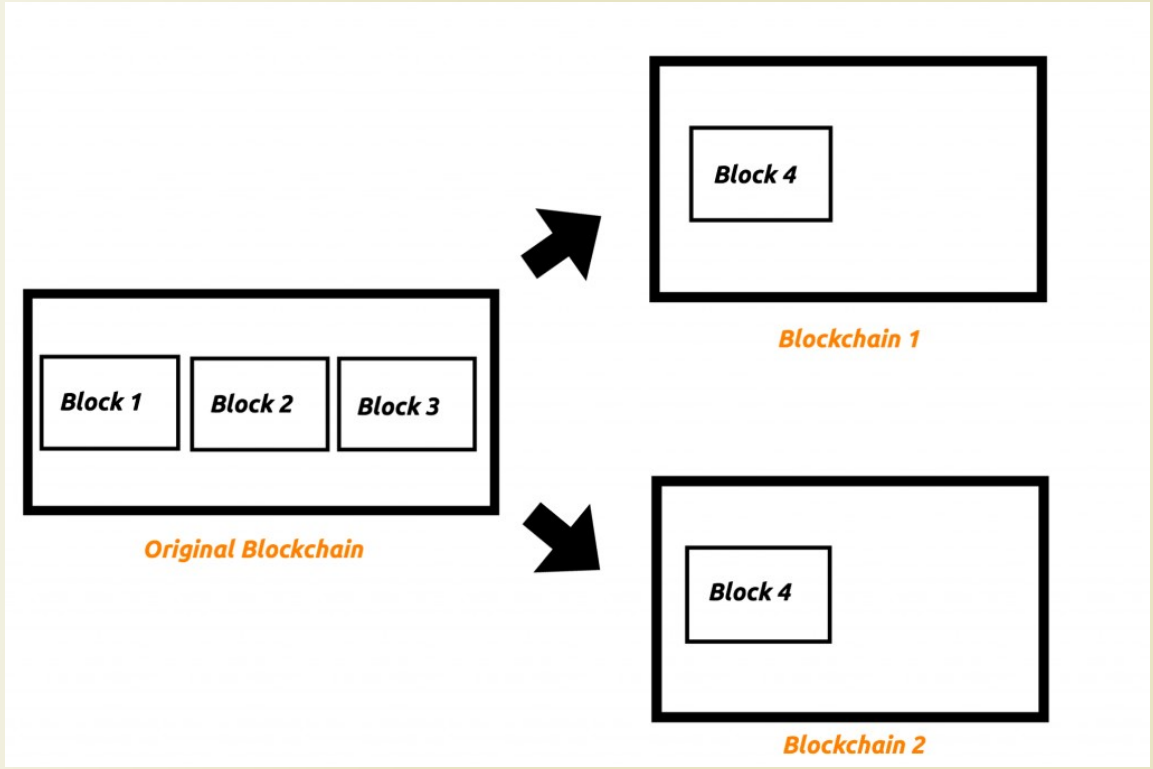
Governance Issues

- Do miners control bitcoin?
- Segwit2X was an attempt by corporations and miners to control bitcoin
- Segwit2X was called off by these same individuals
- There are a number of power structures in Bitcoin
  - Miners
  - Users (light wallets)
  - Full Nodes
  - Developers
  - Hodlers

- Lack of governance and control is a benefit for censorship resistance

Distributed Consensus and Autonomy

- Upgrading blockchain functionality while maintaining backwards compatibility with old clients is performed via a **soft fork**
- Upgrading blockchain functionality and removing backwards compatibility (forcing all clients to upgrade to remain on the valid chain) is called a **hard fork**
- If the network undergoes a hard fork, any clients that have not upgraded will fork to another chain



Examples of Hard Forks

- Ethereum Classic created when Ethereum hard forked to return the stolen DAO funds
- Bitcoin Cash forked from Bitcoin to provide 8MB blocks without segwit
- Bitcoin Gold forked from Bitcoin to provide its creators with 100,000 bitcoin gold (+ Segwit, GPU mining and replay protection)

- Replay Protection is removing the ability for a valid transaction on one fork to be replayed on another fork

- Note: exchanges have fiduciary duty to provide forked coins

Sybil Attacks

- “Proof-of-work is essentially one-CPU-one-vote.”
- Without proof of work, cost of creating a user is free (and there is no central authority to validate uniqueness)
- Ability for single individual to create hundreds or thousands of valid appearing addresses or services easily and cheaply
- Implications for governance

User Activated Soft Fork

- Segregated Witness (BIP141) was an attempted soft fork upgrade to the bitcoin network
- Required 95% miner signalling for 2 weeks by Nov 15th 2017
- Achieved no more than 45% miner agreement (via block signalling)
- UASF (BIP148) was a reaction to the blocking of segwit by miners
- After August 1, any blocks not signalling Segwit would be rejected by nodes running BIP148, creating a fork in the network
- BIP91 created to activate segwit with 80% consensus for 2 days
- Segwit2X agreement gave network segwit and UASF not needed
- Suspicion still that Segwit2X was a reaction to BIP148

Smart Contracts

Smart Contracts

- A contract enforced by code
- Code runs on blockchain, so inherits immutable trust
- Much buzzword, such wow
- Bitcoin scripting is technically smart contract
- Turing-complete smart contracts
  - Provide limitless functionality, all running on chain
  - Provide a limitless surface area for attacks
  - Provide a simple prototyping mechanism for on-chain interactions
  - Are more powerful than bitcoin scripting

Example smart contract

```
contract simpleDNS {
    struct Record {
        address owner;
        string ipAddr;
    }
   mapping (string => Record) records;
   function addDomain(string domain, string ipAddr) {
        if records[domain].owner != msg.sender) { return; }
        records[_domain] = Record(msg.sender, ipAddr);
    }
    function getDomain(string domain) constant returns(string) {
        return records[domain].ipAddr;
    }
    function transfer(string domain, address toAddr) {
        if (records[domain].owner != msg.sender) { throw; }
        records[domain].owner = toAddr;
    }
}
```

Conclusion

Conclusion

- A multisig transaction is a very powerful smart contract
- There are many potential use cases – but Store of Value is primary one in use
- Payment channels are a powerful scaling mechanism, but still require too much on chain interaction
- ICOs are a killer app, new form of VC with a large side-order of scam
- Privacy mechanisms exist, but are complex and not yet in common operation
- Distributed consensus being hard is not a bad thing
- Use a hardware wallet