

Fintech and Cryptocurrencies

Co-Pierre Georg¹
University of Cape Town

This version: 2018-06-16

¹These slides are published under the Gnu LGPL v3.0 license. Developed in collaboration with Qobolwakhe Dube and Sabine Bertram. Please contact me at co-pierre.georg@uct.ac.za if you have any comments or find mistakes in these slides. Perpetual work in progress.

Housekeeping

- The most important thing first: this is **not** supposed to be a normal class!!
- You are here to learn and experiment, not to pass an exam.
- Class participation: 10%; Participation in tuts: 10%; Theoretical exam (**13 August**): 20%; Whitepaper (28 June): 20%; Final project (1 September): **40%**;
- Final projects in three groups of four. The final project is continued in Financial Software Engineering. Here: focus on backend / solidity.
- Updated timetable can be found [here](#).
- Everybody can attend classes, but tutorials are reserved for registered students because of capacity constraints.

Housekeeping

- The most important thing first: this is **not** supposed to be a normal class!!
- You are here to learn and experiment, not to pass an exam.
- Class participation: 10%; Participation in tuts: 10%; Theoretical exam (**13 August**): 20%; Whitepaper (28 June): 20%; Final project (1 September): **40%**;
- Final projects in three groups of four. The final project is continued in Financial Software Engineering. Here: focus on backend / solidity.
- Updated timetable can be found [here](#).
- Everybody can attend classes, but tutorials are reserved for registered students because of capacity constraints.

Housekeeping

- The most important thing first: this is **not** supposed to be a normal class!!
- You are here to learn and experiment, not to pass an exam.
- Class participation: 10%; Participation in tuts: 10%; Theoretical exam (**13 August**): 20%; Whitepaper (28 June): 20%; Final project (1 September): **40%**;
- Final projects in three groups of four. The final project is continued in Financial Software Engineering. Here: focus on backend / solidity.
- Updated timetable can be found [here](#).
- Everybody can attend classes, but tutorials are reserved for registered students because of capacity constraints.

Housekeeping

- The most important thing first: this is **not** supposed to be a normal class!!
- You are here to learn and experiment, not to pass an exam.
- Class participation: 10%; Participation in tuts: 10%; Theoretical exam (**13 August**): 20%; Whitepaper (28 June): 20%; Final project (1 September): **40%**;
- Final projects in three groups of four. The final project is continued in Financial Software Engineering. Here: focus on backend / solidity.
- Updated timetable can be found [here](#).
- Everybody can attend classes, but tutorials are reserved for registered students because of capacity constraints.

Final Project Option A - DORC

- Key idea: create a blockchain registry for digital objects
 - Developers can register class templates they have developed
 - Users can register classes they are using
- Deliverable: Develop a prototype + business plan for this company

Final Project Option B - A truly decentralized blockchain

- Key idea: develop your own blockchain that works on ad-hoc networks
- The problem is that on ad-hoc networks it is easy to end up with different (possibly competing) ledgers
- Find ways to reconcile these ledgers
- Deliverable: Develop a prototype

Final Project Option C - Cryptopia (four groups of three)

- Key idea: Build the ingredients of a crypto-economy
- Build simple platforms for different parts of a crypto economy:
 - A government using DLT for its administration (e.g. of land deeds)
 - A central bank issuing a CBCC
 - A decentralized bank
 - A decentralized trading company
- Deliverable: Develop four prototypes and make them interact with one another

Final Project Option D - BYOF (Build your own firm)

- Key idea: Build your own company
- We have five weeks in total to work on something amazing. I am sure you have ideas what you want to do.
⇒ DO IT!
- Deliverable: Develop a prototype and business plan for your company

What is FinTech?

- The use of technology and other innovations to support or enable the delivery of banking and other financial services
- The term has come to collectively represent technologies that are disrupting traditional financial services, including mobile payments, money transfers, loans, fund raising, and asset management
- This technology is being used to develop innovative ways of producing and consuming financial products and services that can meet consumer needs more efficiently or cheaply

Digital disruption

The Harvard Business Review describes "Disruption" as a process whereby a smaller company with fewer resources is able to successfully challenge established incumbent businesses

Disruptive innovations originate in low-end or new-market footholds

- Established firms typically provide and innovate only for their most profitable and demanding customers segments, while paying less attention to less-demanding customers. This creates an opportunity for new market entrants
- Alternatively, disrupters create a market where none existed as, they find a way to turn non-consumers into consumers

Digital disruption



UBER

World's largest
taxi company

Owning No
taxis



World's largest
accommodation provider

Owning No
real estate



Most popular
media provider

Don't create
content



World's most
valuable retailer

Owning No
inventory



World's largest
movie house

Owning No
cinemas



World's largest
phone companies

Owning No
telecoms infrastructure

Digital disruption

According to PricewaterhouseCoopers' 2017 Global FinTech Report, large financial institutions across the world could lose 24 percent of their revenues to FinTech companies over the next three to five years

A Citigroup report published in 2016 warned that European and American banks could lose almost 2 million jobs in the next 10 years

A NBER paper by Buchak et al. (2017) found that FinTech firms accounted for roughly a quarter of shadow bank loan origination in 2015, partially benefiting from their online origination technology

Global investment

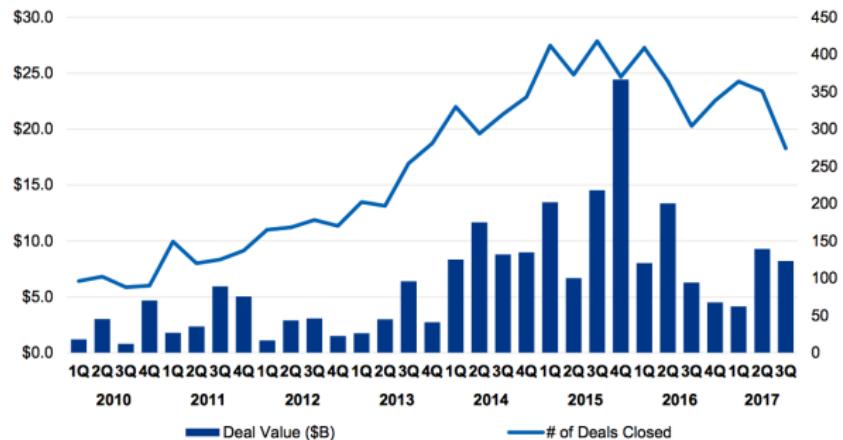
Investment in FinTech has grown from \$1.8 billion in 2010 to \$19 billion in 2015, with an estimated market worth of \$4.7 trillion, according to Goldman Sachs

In 2016 the total value of investment in FinTech among the top 10 countries by deal value accounted for 95% of global investment

KPMG reported that the top 10 largest deals of 2017 occurred in the United States, China, Germany and Canada

Global investment

Global investment activity (VC, PE and M&A) in fintech companies
2010 – Q3'17



Source: KPMG: The Pulse of Fintech Q3 2017

Disrupting finance

Why is FinTech so important?

- These innovations are not just changing the competitive patterns within the industry but are leading a paradigm shift in the way in which industry operates and services its customers
 - The emphasis on peer to peer interaction challenges the role of traditional intermediaries in the financial markets
 - Many of these innovations harness the ability to transact in real time through low cost payment channels
 - The ability to conduct real time analysis of the market has the potential to improve the efficiency of regulatory functions
 - Fintech further addresses frictions that come as a result of information asymmetries by making information more accessible

Disrupting finance

- The rapid emergence of new service providers offering solutions based on these technologies is changing the financial ecosystem
- Some traditional financial institutions are responding by transforming their own operations, either by adopting similar technologies or collaborating with FinTech companies
- At its core, FinTech has the potential to
 - Empower customers who will be able to deal directly, more seamlessly, and flexibly with product and service providers
 - Empower businesses to deliver a better value proposition and customer experience to their customer base

Key drivers



Non-FS Players

Technology giants, telcos



Regulation

Conducive regulatory environment



Adoption

Increasing adoption of various forms of payment modes



Technology

Technology is the key enabler of the Internet and fintech



Consumer

Growing middle class and millennial adoption



Mobile Penetration

Exponentially increasing mobile and smartphone penetration

Source: <https://www.slideshare.net/JoeSeunghyunCho/fintech-in-asia-epayments-marvelstone-tech-at-sgx-event>

Financial inclusion

- According to the World Bank, the number of people globally with no access to banking and financial services is almost two billion
- There are many reasons for this, including
 - Insufficient credit history
 - Bad credit history
 - Limited access to credit and other financial services

Financial inclusion

- These advances in technology are poised to make financial services accessible for the un-banked
 - Access is no longer restricted by geographical location or other physical barriers
 - Services become more affordable as institutions pass on reduced costs to customers
- Digital platforms further improve the personalization of services and lead to more relevant product offerings
- The spread of mobile technologies and mobile network coverage has driven the interest in mobile based financial services

Mobile penetration

- Relative to developed economies, FinTech investment is low, however Africa is often seen at the forefront of mobile financial innovation
- Access to digital services has largely been supported by the mobile phone. A 2017 report by Ericsson found that Sub Saharan Africa has the highest growth rate in mobile subscriptions globally
- South Africa has been ranked as the most developed digital economy in Africa
 - Mobile phone penetration exceeds 90% of the adult population with 69% using smartphones
 - Internet penetration has been rising steadily from 46% in 2015 to 52% in 2017

Digital Innovation

- Innovation is occurring across the financial services industry
 - Distributed ledger technologies are being used as new ways for structuring market infrastructures and payment services. The market for payments is often the most attractive area for innovation as it is typically the least regulated banking function
 - Transaction data and artificial intelligence are being leveraged for credit appraisals
 - The markets for deposits, lending and capital raising are seeing an increase in peer to peer activity and crowdfunding
 - In the field of investment management, advances are being made in the automated processing and dissemination of investment advice

Payments

- The payments sector has seen advances both within and outside the traditional payment infrastructure and channels
- The development of smartphone payments and card-based payment platforms by streamlining electronic fund transfer (EFT) payments has led to a shift toward non-cash channels
- These developments are being supported by next generation security measures such as location-based identification and biometrics, which protect customers and increase confidence in digital channels
- Outside of the traditional payment channels, has empowered consumers to securely transfer value with limited transaction costs, near real time settlement and without the need for intermediaries

Deposits and lending

- This banking function is being disrupted by innovation particularly in the credit market and in the way customers are being serviced
- New service providers are emerging, offering alternative ways to assess credit and secure funding for lending products outside of the banking system
- Crowd-based funding platforms to secure funding for lending are gaining popularity, and in some cases passing the risk on to the investors
- Furthermore, traditional financial intermediaries are being eliminated in some instances by the rise in peer-to-peer lending.

Capital markets

- Alternative funding platforms have begun to emerge, which allow individuals and start-ups to source funding from a collection of investors directly through an online market place, i.e. crowdfunding
- There are four forms of crowdfunding
 - ① Donations-based funding - provided on a charitable basis without any expectation of a reward
 - ② Reward-based - provides an item of clear monetary value in exchange for the funding provided
 - ③ Loan-based - investors expect to earn interest and capital repayments on the amount funded i.e. peer-to-peer lending
 - ④ Investment-based - funding provided to earn capital gains and dividends.
- These platforms continue to increase in popularity as they can also provide investors with access to a far wider array of investment opportunities not bounded by geography
- It also becomes easier to give investors more control over where and how their funds are invested

Investment management

- Technology enabled solutions are being used to provide advice, market information and easy to use investment tools.
 - Robo-advisors are being used to administer advisory services and guide investors' decisions in the absence of human oversight.
 - Platforms are being designed to give investors the ability to automate trade execution, based on a predefined set of rules and automated quantitative investment strategies
 - Investment managers' administrative processes can be automated and streamlined through the use of artificial intelligence and in so doing reducing the likelihood of human error
- These factors all contribute towards efficiencies and reduced costs passed on to consumers, consequently making investment products more affordable and attractive.

Market microstructure

- Markets are seeing a rise in high frequency trading strategies (i.e. exploiting arbitrage opportunities through low-latency access to exchanges) being supported by big data analytics and artificial intelligence
- Algorithms make use of new machine-readable data sources and AI capabilities, providing traders with the opportunity to react to real time events more quickly, in doing so, providing the market with liquidity
- Technology is also changing the way in which buyers and sellers connect in the OTC market
- In many ways, the OTC market is being formalized without necessarily involving financial intermediaries
- These platforms being used to connect market participants are providing the opportunity for greater price transparency and improved liquidity

South Africa's Fintech ecosystem



Source: <http://ventureburn.com/wp-content/uploads/2016/09/uncovered-ventureburn-lists-south-africas-fintech-ecosystem-update-01.jpg>

Fintech in action

Digital payments

- Google wallet - Mobile application that digitizes users' cards to facilitate P2P and P2P payments online and at points of sale
- WiGroup - Started off as the first mobile wallet in SA in 2008, and has since evolved into a facilitator of mobile transaction services.
- Snapscan - A pay-by-proxy allowing businesses to accept card transactions with mobile phones
- MasterPass A mobile application digitizing users' cards allowing payment through QR codes and online

Fintech in action

Smartphone payments

- Yoco - Mobile payments service provider that targets small to medium companies who require the portability of a card reader. In the past two years of operation, raised US\$7 million
- Apple pay - A mobile wallet with NFC enabled capabilities allowing for P2P and contactless POS payments
- FitPay - A provider that enables contactless payments through wearable devices
- CardsPlus - A South African producer and supplier of contactless and contact chip cards

Fintech in action

Compliance and regulation

- Alyne - a regtech Software as a Service for cyber security, risk management and compliance. Provides scalable assessments to measure current maturity and delivers deep insights through advanced risk analytics.
- Bokio - Automates accounting and serves as a decision-making platform for small businesses. The system automatically handles invoicing, payroll and accounting
- Suade - focused on prudential regulation stemming from Basel III and Mifid II, and provides products including a stress testing platform for capital requirements and scenario testing for liquidity management
- ComplyAdvantage - A London based anti money laundering and sanctions database
- Gusto - A comprehensive HR, payroll, and benefits service, enabling businesses to set up and run payroll from any web-enabled device.

Fintech in action

Security & ID

- Entersekt - Provider of push-based security and authentication, as well as biometric verification.
- Prosper Daily - A personal finance security company that analyzes users' card based transactions to alert them to potential fraud
- ThisIsMe - an online verification system or individuals, businesses, regulators, and financial institutions that works by linking into Home Affairs and major banks
- Virtual Card Services - A card payments service provider that offers 3D secure solutions

Fintech in action

Payment platforms

- Stripe - provides a set of unified APIs and tools that instantly enable businesses to accept and manage online payments
- Ant Financial - an online payment services provider founded by the Alibaba group. Its platform, Alipay, is the world's largest mobile and online payments platform
- ShieldPay - Operates an instant digital escrow facility that enables secure Peer-Peer transactions

Fintech in action

Domestic and international remittances

- M-Pesa - An agency based mobile money operator based in Kenya that provides money transfer, financing and microfinancing services
- Shoprite Money Market - A large South African retailer providing almost instant cash-in cash-out transfers from its branches
- TransferWise - An international remittance platform that pairs senders and receivers in local markets
- Mukuru Money - An international remittance platform that operates through partnership with retailers and banks

Fintech in action

Blockchains

- Blockchain - A web-based bitcoin platform that provides Bitcoin wallet services, Bitcoin APIs, and a block explorer
- Coinbase - A digital currency wallet service provider that allows merchants, consumers, and traders to buy and sell digital currency
- Luno(formerly BitX) - A digital wallet that allows consumers to easily buy and sell Bitcoin and Ether.
- The Sun exchange - A market place where you can buy into commercial solar projects at the scale of one cell at a time, using blockchains and smart contracts to facilitate transactions

Fintech in action

Insurance

- Riovic - Directly connects risk managers and risk underwriters. It also allows private investors to accept a stream of certain cash flows in exchange for an uncertain future liability.
- Robin - Provides a mobile interface presenting all the present and past retirement and pension funds under your name. Allowing you to monitor the fees you are paying, the ROI, the predicted monthly pension and how much can be saved on fees by upgrading existing plans with better ones
- LeO Chief Of Stuff - Applies Machine Learning and Artificial Intelligence technologies on user's profile and on real-time data, to deliver a optimized insurance experience and match the user with the most relevant insurance products
- eCOIDA - an online insurance technology platform that links employers and medical service providers

Fintech in action

Credit facilities

- Salaryo - Provides credit facilities to freelancers with unstable income. The platform verifies the applicant's identity, checks financial health in real time and analyses the freelancer's professional pulse with a proprietary risk management model
- Flexpay - Provides an automated purchase platform that enables customers to afford goods via convenient flexible mobile phone payments.
- FOMO Travel - An online lay-buy platform where one can pay a small deposit towards a travel goal and pay the rest through installments or crowdfunding. Recently entered into a partnership with SA Tourism

Fintech in action

Alternative credit scoring

- Commuscore - A South African provider of credit scoring that integrates data from informal social saving and lending groups
- Kreditech - A German online lender which offers loans to individuals based on their creditworthiness which is analyzed using their social media and online data
- Compuscan - A credit bureau integrating psychometric data into credit scoring

Fintech in action

Asset financing

- Ownerhood - By breaking properties into smaller tradeable slices
Ownerhood removes barriers to homeownership and promotes frictionless access to the residential real-estate market via a simple, digital, crowd driven marketplace
- BenBen - A digital land database that provides fast and easy access to trusted information about land through Blockchain technology. Provides access to paid-for-property information, mortgage origination, licensing, thematic data analysis.
- Carvana - A online platform that enables users to trade, finance, buy, and sell used cars using a fully-automated service scheme
- Tugende - A Ugandan platform allowing users to finance and payoff a motorcycle in 18 months or less

Fintech in action

Peer-to-peer lending

- Lending Club - A US provider of peer to peer unsecured personal loans of up to \$40,000
- Upstart - An online lending marketplace that provides personal loans using alternative scoring methods, like education and employment, to predict creditworthiness
- RainFin - An online lending marketplace that connects borrowers seeking transparent, cost effective loans with lenders. It uses an 'intelligent' scorecard to review the applicant's transaction history, financial health, and other aspects such as social media profiles.
- Stokfella - A digitized social lending and savings platform
- Firstp2p - A Chinese online peer to peer financing site that matches borrowers with investors

Fintech in action

Automated advice and investment management

- CapitalWise - A cost-effective micro-investment platform for financial institutions. Delivers personal investing literacy, rule-based micro investing empowered by machine learning and predictive analytics to retail users of financial institutions
- Easy Equities - Provides a low cost web based stock trading platform that allows investors to purchase $1/1000^{th}$ of a share on the JSE
- Wealth Migrate - An online platform that allows domestic investors to invest in foreign real-estate developments
- Wealth Front - An automated investment service firm providing robo-advice reflecting investors' observed financial behavior

Fintech in action

Banking and Micro-finance

- Abe.ai - Designs artificial intelligence solutions for the banking industry, helping banks better engage and support their customers at scale
- Nomanini - Payments platform provider that optimizes transactions in the informal retail sector. Selected as one of four finalists in the financial inclusion category of the MIT Inclusive Innovation Challenge
- Byte Money - Provides solutions that help avoid mismanagement of payments in the informal finance sector with the ability to service remote areas with real time payments

Recap

- Fintech is the use of technology to support delivery of financial services
- With the advent of blockchain technology, this sector has seen a significant increase in investment flows
- The disruption caused by blockchain technology spans across a wide range of functions within financial services
- Mobile phone penetration has been found to be one of the key drivers of the adoption of technology in financial services
- Banks and other financial institutions face the biggest risk of disintermediation in the functions of payments and investment management

Blockchains



- Blockchains are a new type of data structure that allows data to be stored on a peer to peer network
- Consensus mechanisms are used to determine the contents of the database, which are accessible by anyone but can not be tampered with
- Together, the features of transparency, immutability and consensus allow peers to transact in an environment of conflicting interests without the need for trust
- Blockchains are expected to revolutionize record keeping practices in the financial sector

History of bookkeeping

Double entry bookkeeping revolutionized the field of financial accounting during the Renaissance period; it solved the problem of managers knowing whether they could trust their own books

It has since become the basic foundation of how value is accounted for

However, due to its complexity, the task of ensuring trustworthiness of records in financial markets is best left to a central authority.

- This makes it easier to deal with high transaction volumes as it is far more efficient to maintain a central ledger where all transactions can be reconciled
- It also increases efficiency and reduces the cost of transactions e.g. banks reduce search costs for depositors looking to earn interest and lenders looking for finance

History of bookkeeping

Single entry bookkeeping

- Each financial transaction is a single entry in a journal or transaction log
- Firms using single entry approach are effectively limited to reporting on a cash basis.
- Provides insufficient records and control for public companies and other organizations that must publish audited financial statements

Double entry bookkeeping

- Every financial event brings at least two equal and offsetting entries
- Firms using the double entry approach report financial results with an accrual reporting system
- Provides several forms of error checking that are absent in a single entry system e.g. Balance sheet equation

Blockchain

The latest innovation that has been posited to disrupt the FinTech space is the *blockchain*

This technology offers a new form of storage, use, maintenance and control of records

It has garnered interest not only because of the potential impact on how financial intermediaries will transact with society, but also because of the effect of its application in processes complementary to these financial transactions

This includes but not limited to:

- Identity management
- Civil registries of land and asset ownership
- Protection of customer privacy

What is a blockchain?

A distributed database, that records transactions and ownership, operated within a peer to peer network

Designed to serve as irreversible and incorruptible repositories of information; a digital platform that stores and verifies the entire history of transactions between users across the network.

Instead of using double entry and keeping separate records based on transaction receipts, the technology allows parties to write their transactions directly into a joint ledger, eliminating the need for a trusted intermediary and creating an interlocking system of enduring records

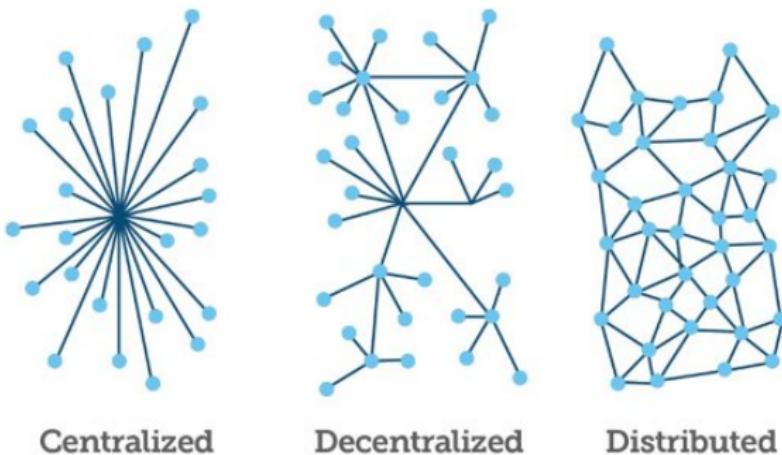


Figure: A comparison of database network topologies. With both centralized and decentralized networks, nodes retrieve data from a central location, the only difference being that a centralized network has a single point of failure. Whereas with the distributed database architecture, all nodes act as peers, all maintaining local copies of the database, the contents of which are determined by a consensus protocol

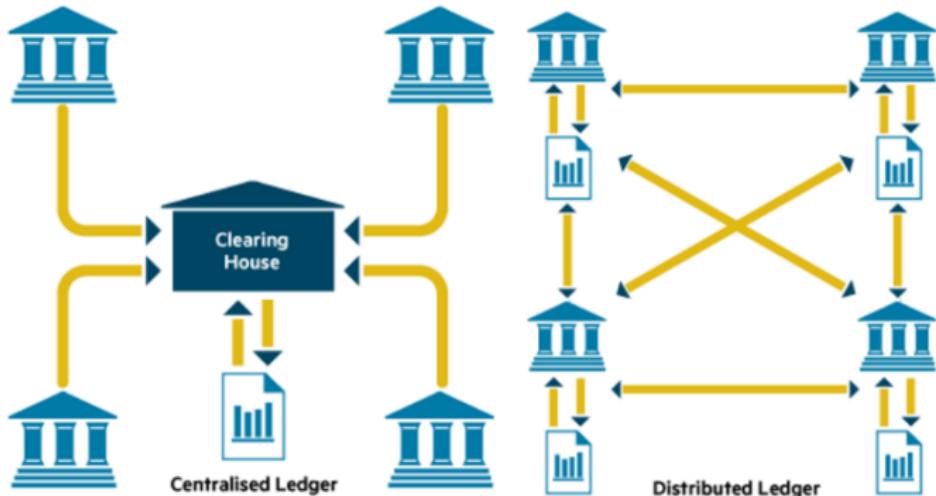


Figure: In a traditional market structure shown on the left, central clearing houses act as trusted intermediaries to facilitate the transfer of value and maintain a record of such transactions. Institutions keep their own records, but the single trusted source of information is the intermediary. If the market were to switch to blockchain based infrastructure, every institution would maintain its own copy of the ledger, the contents of which are visible to all other peers on the network and determined by a consensus protocol

What is a blockchain?

Although initially designed solely for Bitcoin network, blockchains can be used in any function that requires record keeping

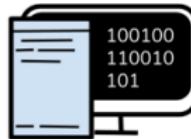
The technology has gained popularity in the financial services industry, because it enables multiple entities of conflicting interests to collaborate on maintaining a shared ledger of records and transact securely without the need for trust

One of the core features of the technology is complete transparency

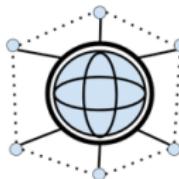
- Publicly accessible pseudonymous ownership records and complete transaction auditability are synonymous with the technology
- Blockchains therefore have the potential to provide unprecedented levels of transparency in the financial services industry



A digital ledger that keeps record of all transactions taking place on a peer-to-peer network



All information transferred via blockchain is encrypted and every occurrence recorded, meaning it can't be altered



The network is decentralized, eliminating the need for a central certifying authority

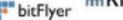


It can be used for more than the transfer of currency; contracts, records and any other kind of data that can be stored



Encrypted information can be shared across multiple providers without risk of a privacy breach

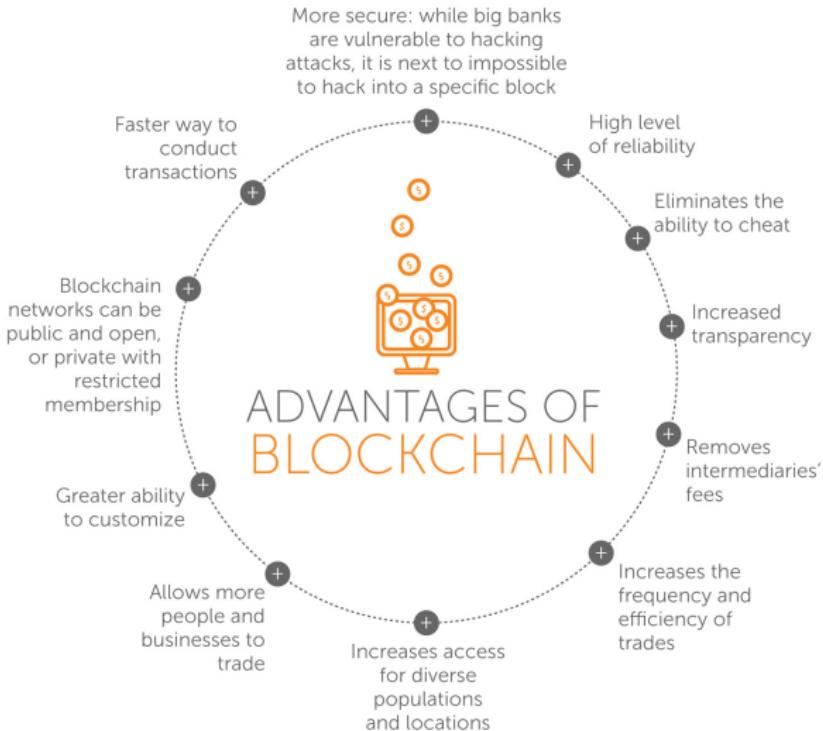
Blockchain Startup Landscape

Blockchain Consulting/ App Dev	Payments	Identity & Reputation	Governance & Transparency
 CONSENSYS  LedgerLabs  BTL 	 CIRCLE  CoinPip  vogogo  bitpay  ABRA 	 NETKI  Cambridge Blockchain  uport  ShoCard  civic 	 OTONOMOS  BoardRoom  BITNATION 
Mining	Exchange, Trading & Investing		Media
 BITMAIN  Genesis Mining  BitFury 	 coinbase  @LedgerX  bitFlyer  GEMINI  Kraken  Mirror  BITSTAMP  BTCC  coinfloor  POLONIEX  SHAPE SHIFT  @KCoin 		 coindesk  Crypto Compare  BTC MEDIA  BRAVE NEW COIN 
Legal, Audit & Tax	Content Management	Data Analytics, Compliance & Security	Social Network
 PEERNNOVA  Libra clause	 ALEXANDRIA  CD JAAK  res()nate  LBRY  DC MUSIC  DC DECENT  Revelator 	 Delliptic  simplex  Skry  CHAINANALYSIS  coinfirm 	 synereo  AKASHA  steemit
Wallet	Data Provenance & Notary		Supply Chain & Logistics
 xapo  TREZOR  BLOCKCHAIN  BITX 	 factom  blockai  PROVENANCE 	 bitproof.io  guardtime  everledger 	 FILAMENT  Hijro 
Prediction Markets	Public Chain Infrastructure		Commerce & Advertising
 GNOSIS  Hivemind 	 Bitcoin Foundation  ethereum  ②CASH  MONERO  LISK  party 	 @vijaymichalik  @Frost_Sullivan  @lawrenceclundy 	 OB1  safemarket  Purse 
Financial Services Infrastructure		Enterprise Infrastructure	
 ripple  SETL  Digital Asset Holdings  PAXOS  symbiont  R  clearmatics  TALLYSTICKS  UBIDI 		 Gem  Filecoin  Tendermint  STORE  NUCO  HYPERLEDGER PROJECT  bloq  BIGCHAINDB  MONAX	

Source: https://www.frost.com/files/cache/a701d7ea2011161d4eaeed6364153683_f16618.jpg

Blockchain 101

- Block - a dataset containing multiple records, and cryptographic elements to be appended onto the blockchain
- Blockchain - a data structure used to create a decentralized ledger
- Consensus - a process of agreement between distrustful nodes on a final state of data
- Cryptography - a set of techniques used for secure communication and storage of data
- Distributed system - a computing system where two or more nodes work together in a coordinated fashion to achieve a common outcome
- Distributed ledger - a append only list of records that is maintained using a consensus protocol
- Mining - the process of appending new information onto the distributed ledger, in the form of new blocks
- Peer to peer - communication protocol in which participating nodes have equal permissions and rights
- Proof of work - a consensus mechanism used to verify the validity of a block



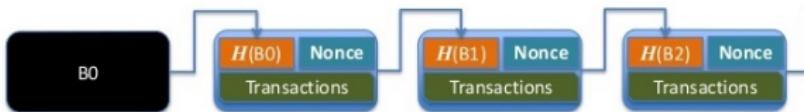
Source: <http://www.arreverie.com/blogs/wp-content/uploads/2017/08/advantages-of-bitcoin-1024x845.jpg>

What is a blockchain?

A blockchain consists of 'blocks' linked together in a linear sequential chain

Each block contains an encrypted identifier of the previous block (i.e. a hash), new transactions, a timestamp and a cryptographic nonce

A nonce is an arbitrary 32-Bit number that may only be used once to verify the validity of the block that has been added to the chain

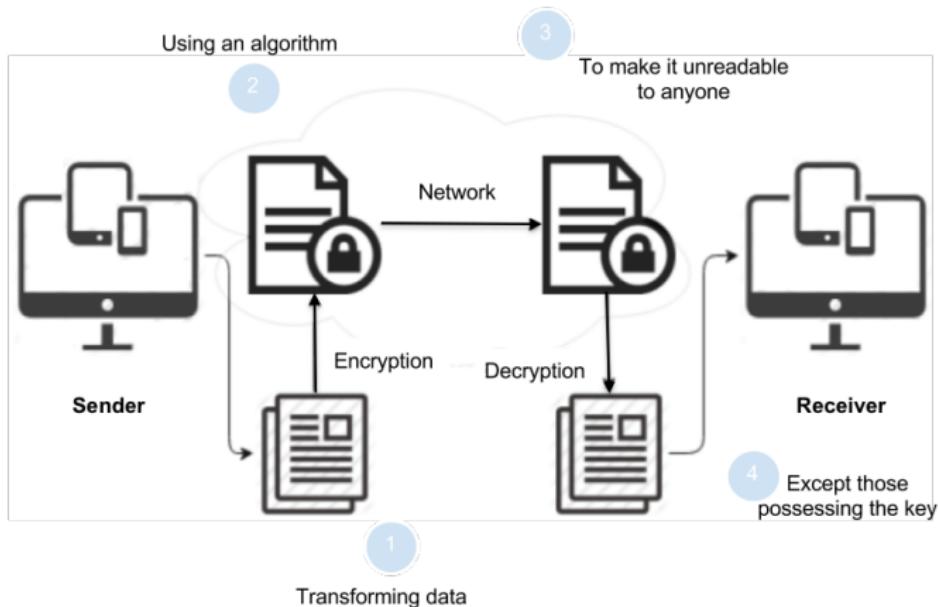


The size of the blocks determines the scalability of the network i.e. the number of transactions that are processed with each block that is added

Cryptography

- Cryptography refers to a set of techniques used for secure communication and storage of data, such that it can be read and processed only by those with access rights
- Blockchains effectively make use of cryptography in multiple different and complementary ways
- Its use includes and is not limited to
 - The creation of pseudonymous identities
 - Providing secure communication that guarantees data integrity across the network

Cryptography



Cryptography - Hash functions

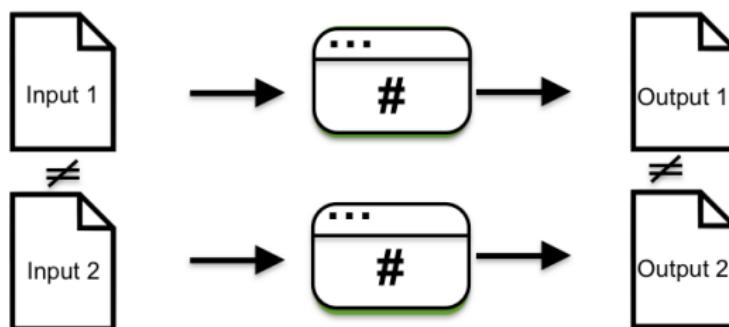
Hash function

- A function that can be used to map data of arbitrary size to data of fixed size
- By comparing the output of the data to a known and expected hash value, one can determine the data's integrity
- Hash functions accelerate table or database lookup by detecting duplicated records in a large file
- A cryptographic hash function is a special class of hash function that is suitable for use in cryptography

Cryptography - Hash functions

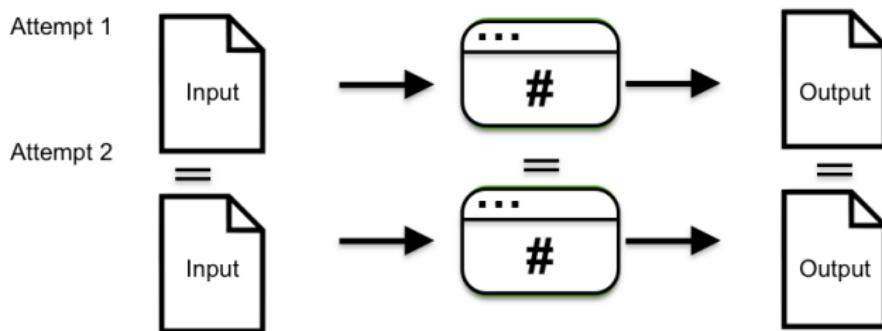
The ideal cryptographic hash function has the following properties

- 1 Collision resistant - output is sufficiently distinct hence it is infeasible to find two different messages with the same hash value



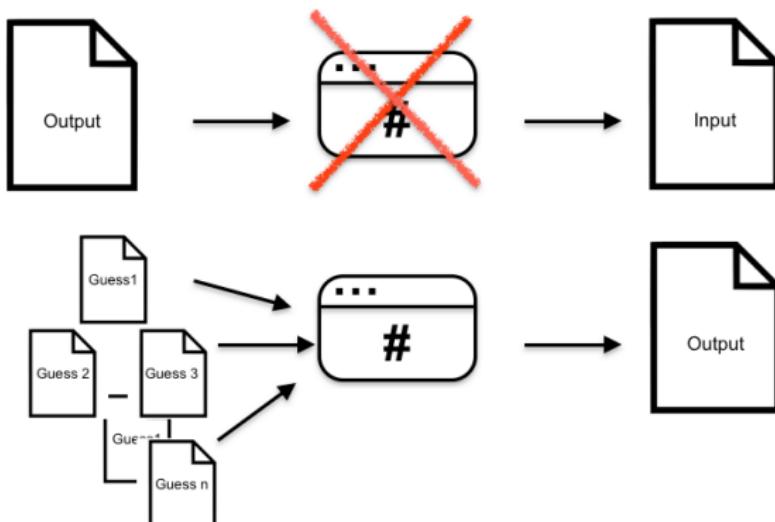
Cryptography - Hash functions

- 2 Deterministic - the same message always results in the same hash



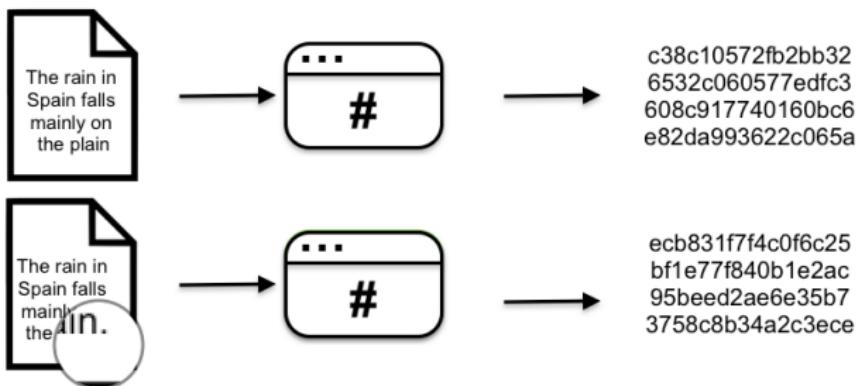
Cryptography - Hash functions

- 3 Concealing - it is infeasible to generate a message from its hash value except by trying all possible messages i.e. brute force search



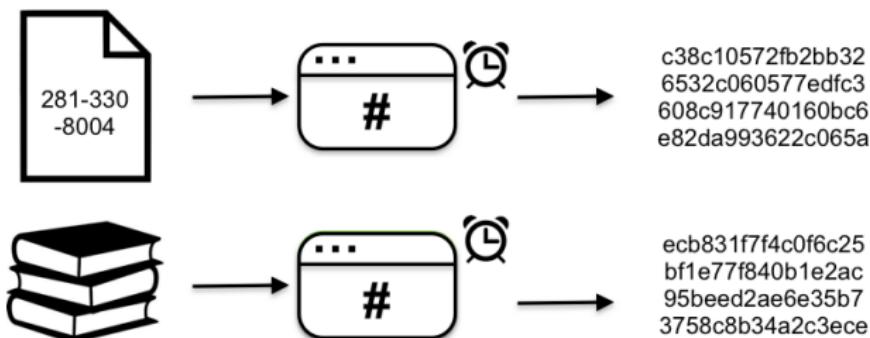
Cryptography - Hash functions

- 4 High avalanche effect - a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value



Cryptography - Hash functions

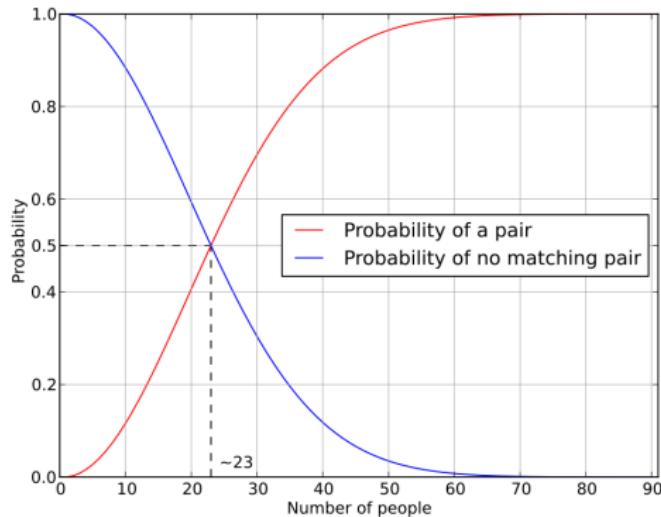
- 5 Efficient - quick to compute the hash value for any given message



Cryptography - Hash functions

- Collision resistance does not mean that no collisions exist; simply that they are hard to find
- The 'birthday paradox' can be used to understand why there exists an upper bound on collision resistance
 - in a set of n randomly chosen people, the probability that some pair will have the same birthday increases with n
 - The probability reaches 100% when the number of people reaches 367, since there are only 366 possible birthdays (99.9% probability is reached with just 70 people)
 - The same concept applies to hashes, given that they are of fixed length
 - Theoretically, every hash function with more inputs than outputs will necessarily have collisions

Birthday paradox



Source: https://en.wikipedia.org/wiki/File:Birthday_probability.svg

Cryptography - Hash functions

- Some hash functions that were previously thought to be collision resistant have been broken e.g. MD5 and SHA-1
- Currently there no hash function that is provably collision resistant, but there are hash functions for which a collision has not yet been found.
- NB. collision resistance is not sufficient to ensure the function is concealing
 - Suppose the input has a known probability distribution that makes certain values more likely than others
 - For practical purposes, one would need to know only the hashes associated with these inputs since the others are unlikely
 - Hashes could therefore be pre-computed, stored in a hash table and looked up when required

Cryptography - Hash functions

SHA256 hash

- Part of the SHA-2 set of cryptographic hash functions designed by the United States NSA
- One of the strongest hash functions to date, and has yet to be compromised in any way
- Several cryptocurrencies use SHA-256 for verifying transactions and calculating proof-of-work or proof-of-stake
- It is also used in the creation of node addresses in order to improve security and privacy

Cryptography - Hash functions

SHA256 hash

- SHA256 is a 256 bit hashing algorithm which can produce a hash for input up to $2^{64} - 1$ bits (≈ 2091752 terabytes)
- The message to be hashed is first encoded into bytes, using character-encoding such as ASCII or UTF-8. After which it is:
 - ① padded to the right with zeros and the length of the original message in bits, such that the length of the resulting message is a multiple of 512
 - ② parsed into 512-bit message blocks on which functions are performed that mix up the data in a non linear fashion that is difficult to analyze cryptographically
- The calculated hash will be a 64 digit hexadecimal number

Cryptography - Binary trees

Blockchains use binary trees to store data

This is a tree data structure in which each node has at most two children, which are referred to as the left child and the right child

This data structure is often preferred as it enables efficient searching of large data sets through the use of the principle of binary search

When searching for a specific point in the tree, lookups and other operations will traverse the tree from root to leaf (i.e. top to bottom)

At each point the operation decide to continue searching in the left or right subtrees and this significantly reduces search time, as on average this allows the operations to skip half the tree

Cryptography - Binary trees

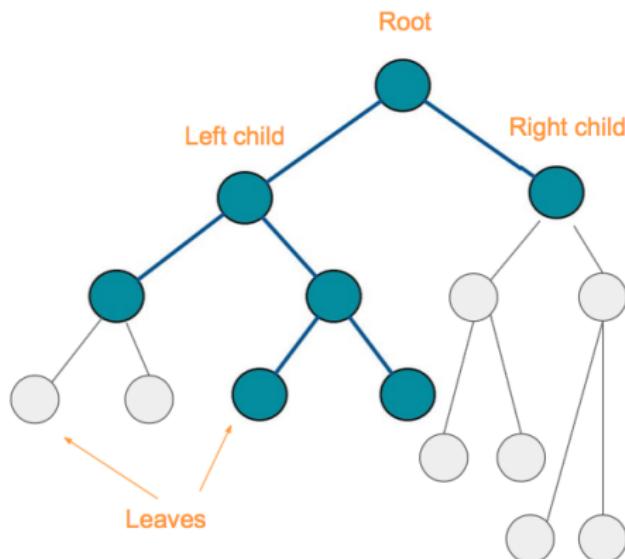


Figure: A binary tree

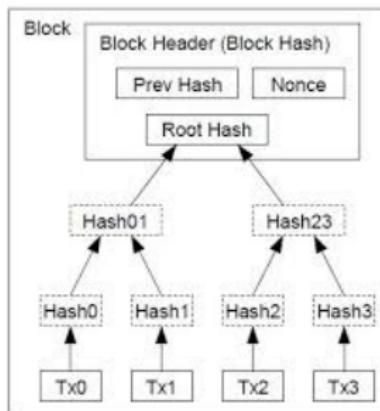
Cryptography - Merkle trees

Merkle tree roots

- Some blockchains store transactions in block headers, in the form of a Merkle tree root
- This is a type of binary tree in which every non-leaf is constructed from the hashes of its child nodes, with the transaction IDs - the hashes of the transaction data - as the leaf nodes
- This allows for efficient and secure verification of the contents of large data structures

Cryptography - Merkle trees

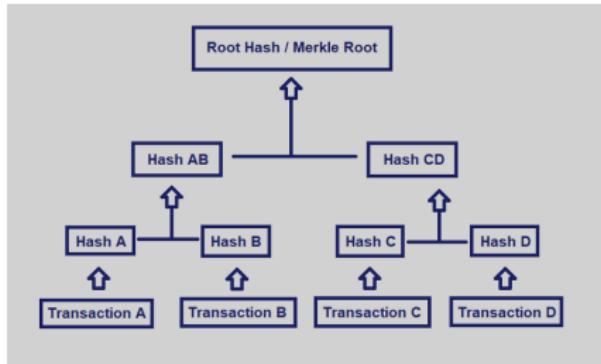
The Merkle root is cryptographic proof of which transactions are in the block, and which order they are included.



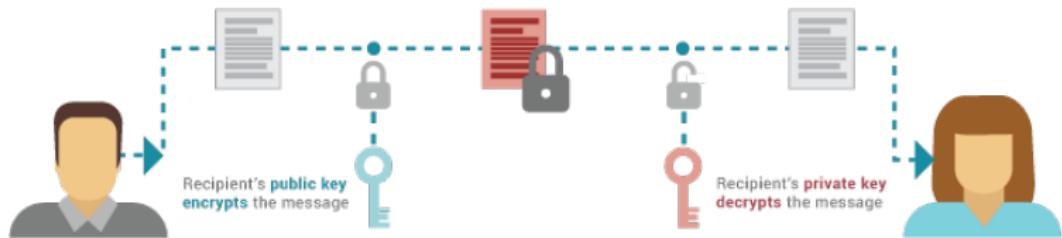
Source: <https://bitcoin.org/bitcoin.pdf>

Simple payment verification

- It is possible to confirm the existence of a transaction in a block without having to download the entire blockchain
- By keeping copies of only the block headers, transactions can be verified using Merkle trees
- A user only needs to obtain the Merkle branch linking the transaction to the Merkle tree root
- Proof of inclusion is obtained by reconstructing the root using the transaction hash and non leaf nodes of the pruned Merkle branch



PUBLIC KEY CRYPTOGRAPHY



Source: https://eng.paxos.com/hs-fs/hubfs/_02_Paxos_Engineering/Public-Key-Cryptography-1.png?t=1513284613258&width=1024&name=Public-Key-Cryptography-1.png

Public key cryptography

- Traditional blockchain implementations make use of public key/asymmetric cryptography
- This is a form of cryptography where there are two keys: a private key and a public key
- The public key is derived from an algorithmic transformation of the private key
- Hashing the public key give the blockchain address



Public key cryptography

Encryption and signing

- Data encrypted with the private key can only be decrypted with the corresponding public key and vice versa
- A message can be signed with the sender's private key and then encrypted with the recipient's public key
 - ① Sender signs message with her private key
 - ② Sender encrypts message with recipient's public key
 - ③ Recipient decrypts message with her private key
 - ④ Recipient can verify the signature with the sender's public key
- The integrity of a blockchain is dependent on private keys remaining hidden

Public key cryptography

- Traditional blockchain implementations make use of the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign transactions and generate key pairs
- Each coin is associated with its current owner's public ECDSA key
- Transactions are fundamentally messages containing the new owner's public key, the amount of the item being transferred and signed by the sender's private key
- The signature is used to verify the authenticity of the message

Public key cryptography

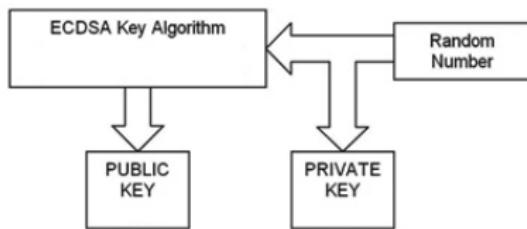


Figure: Key pair generation

- A random number generator is used to produce a value that becomes the private key
- Next the public key is computed according to the ECDSA key pair algorithm

Source: <https://m.eet.com/media/1203927/Maxim%20ECDSA%20Figure%202.jpg>

Public key cryptography

- A digital signature allows the recipient of a message to verify its authenticity using the senders public key
- To produce a signature, the message first has to be converted to a fixed length message using a secure hash algorithm
- To produce the signature the ECDSA signature algorithm takes in as input the message hash, the sender's private key and a random number

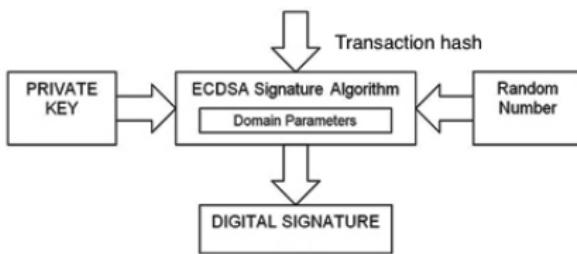
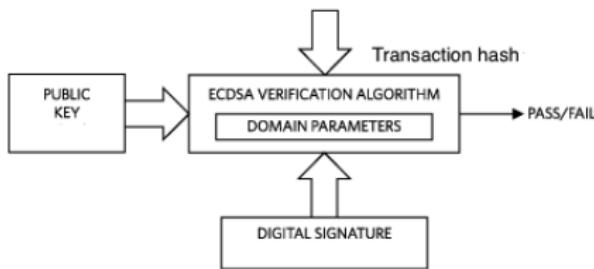


Figure: Signature computation process

Source: <https://m.eet.com/media/1203929/Maxim%20ECDSA%20Figure%203.jpg>

Public key cryptography

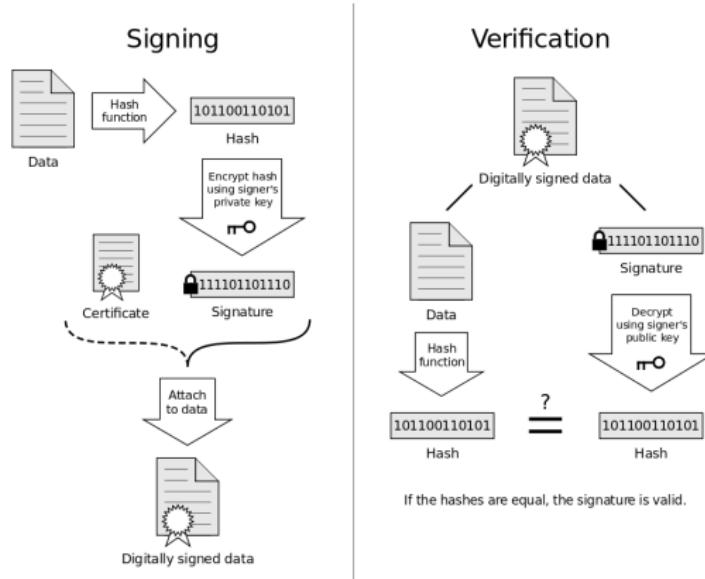


- Using the same secure hash algorithm as the signature algorithm, the message hash is computed
- The verification algorithm takes in as input the digital signature, the sender's public key and the hashed message

Figure: Signature verification process

Source: <https://m.eet.com/media/1203932/Maxim%20ECDSA%20Figure%204.jpg>

Public key cryptography



Source: https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg

Failure of public key cryptography - Mt Gox hack

Mt. Gox was a Bitcoin exchange based in Tokyo that collapsed in 2014 after it was hacked; at its peak, Mt Gox handled 70% of bitcoin transactions worldwide

Hackers breached the exchanges security to access private keys it held on behalf of customers, after which they stole over \$450million from the exchanges' 'hot wallet' (i.e. a cryptocurrency wallet that is connected to the internet)

This incident led to the exchange going bankrupt as it was near impossible to recover the funds that were now under the control of a new set of private keys

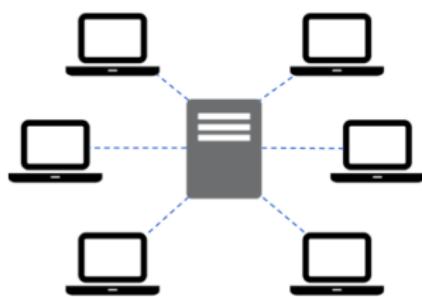
This marked the second major hack that the company faced

- Previously in June 2011 hackers got away with the equivalent of \$8.75million
- Allegedly hackers had been skimming money from the company for years

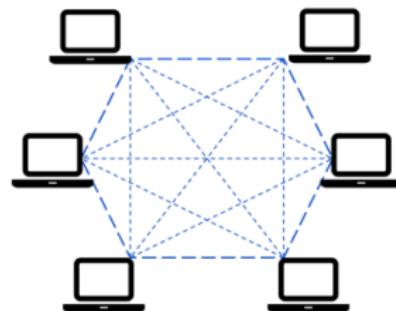
Peer to peer networks

- In peer to peer networks, peers are equally privileged, equipotent participants
- Peers are both suppliers and consumers of resources as there are no client-server relationships
- All nodes have the ability to directly communicate
- Blockchains are designed to be peer to peer networks, every node is allowed to send new transactions, verify transactions, and create new blocks

Peer to peer networks



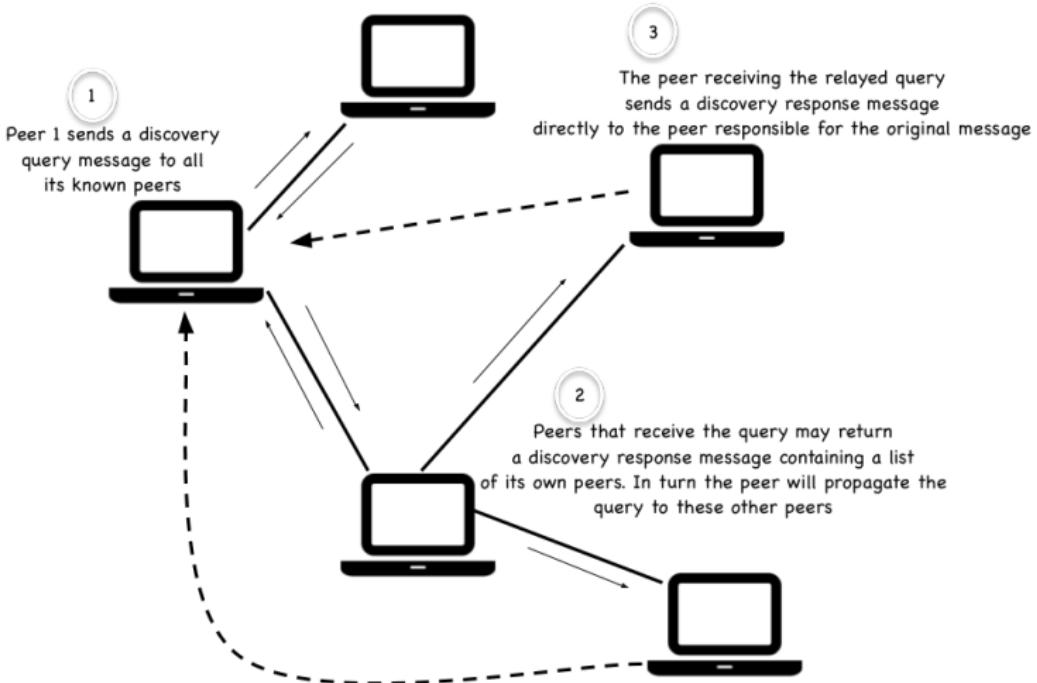
Server-Based



Peer-to-peer

Peer discovery

- Peer to peer networks do not impose a particular structure on how communication occurs
- A node does not need to connect to every node in the network in order to broadcast and listen to new transactions/blocks
- By connecting to a few neighbors, which in turn connect to their neighbors, the whole network remains connected
- The way in which peers locate each other will vary by blockchain design
- One way is for the client to use a list of nodes from a previous connection to the network



Peer discovery

- Another way is through the use of bootnodes i.e. a node hardcoded in the node discovery protocol, that maintains a list of all nodes that have recently connected to it.
- When a node connects to the network, it will automatically connect to the bootnode, which will then share the list of peers to which it can connect
- Nodes can generally be split into 3 categories, each with multiple variations: Full nodes, Pruned full nodes and Simple payment verification nodes

Node design

① Full nodes

- Download every block and transaction and check them against the blockchain's core consensus rules
- Require significant bandwidth to allow efficient propagation of data and substantial RAM to process a certain number of transactions per second
- There are two types of full nodes. Regular nodes only keep copies of the blockchain, and mining nodes build the blockchain

② Pruned full nodes

- Technically still a full node, however it prunes its local blockchain in order to save disk space
- Pruned nodes download the full blockchain once and when they are done verifying, they keep only the most recent blocks
- Only store the most recent blocks, but are still able to verify all transactions that occur on the blockchain

③ Simple payment verification (SPV) nodes

- Request transactions/merkle branches from full node if needed
- Can validate the existence of transactions without being subjected to the load of operating a full node

Node design



Reference Client

Contains a Wallet, Miner, full blockchain database and a network routing node on the P2P network



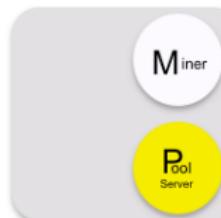
Lightweight SPV wallet

Contains a Wallet and a network routing node on the P2P network without a blockchain



Full Blockchain Node

Contains a full blockchain database and a network routing node on the P2P network



Mining Nodes

Contains a mining function without a blockchain and gateway router connecting the P2P network to other nodes running pool mining protocols



Solo Miner

Contains a mining function with a full copy of the blockchain and a network routing node on the P2P network

Types of blockchains

- Blockchains were initially intended to be public and completely transparent in all aspects
- However, efforts are continually being made by institutions to leverage this database structure in examples with varying levels of transparency, anonymity and decentralization
- We can therefore divide blockchains into multiple types with distinct but sometimes partly overlapping attributes

Public blockchains

- As the name suggests, these blockchains are open to the public and anyone can participate as a node in the decision making process
- These blockchains are also known as permission-less ledgers
- All users maintain a copy of the ledger on their local nodes, and use a distributed consensus mechanism in order to reach a decision about the eventual state of the ledger
- The majority of cryptocurrencies fall under this category

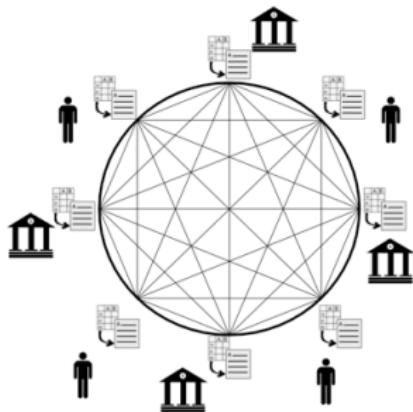
Private blockchains

- Open only to a consortium or group of individuals or organizations that has decided to share the ledger among themselves
- These do away with pseudonymous identities, hence all participating nodes are known.
- Proprietary blockchains are a subset of private blockchains that deviate from the fundamental idea of decentralization of the technology
- These are typically used within an organization, hence many traditional features become superfluous due to the absence of conflicting interests

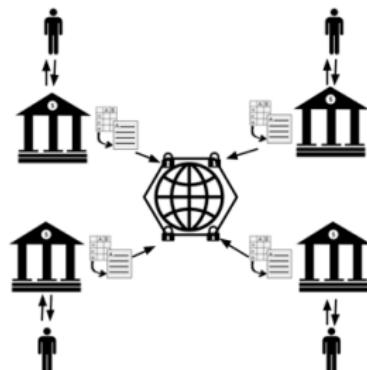
Permissioned ledgers

- A class of blockchains that also does away with pseudonymous identities
- Access is controlled by a group of nodes
- These do not need to use a distributed consensus mechanism, instead an agreement protocol can be used to maintain a shared version of truth about the state of the records
- There is no requirement for permissioned blockchains to be private as they can be public blockchains but with regulated access control

Public blockchains



Private blockchains



- No authoritative permission required in order to participate (anyone can read or write data)
- Participants are not vetted
- Mechanisms for maintaining the network against attacks and unwanted parties therefore add cost and complexity to the network

- Participants are known and trusted
- Legal contracts can replace system mechanisms where straightforward
- No longer a “trustless” system

Genesis block

- This is the very first block of a blockchain and it is assigned to block number zero
- It is a special block in that it does not reference a previous block, neither does it contain any transactions
- Two nodes in a network will only pair with each other and synchronize if they have identical genesis blocks
- This block is typically hardcoded into the clients used to access the network

Bitcoin genesis

Block #0

Summary		Hashes
Number Of Transactions	1	Hash 00000000019d6689c085ae165531e934ff763ae48a2a6c172b3f1b60a8ce26f
Output Total	50 BTC	Previous Block 000
Estimated Transaction Volume	0 BTC	Next Block(s) 00000000839ae0886ab5951d76411475428afc90947ee320161bbf18eb0048
Transaction Fees	0 BTC	Merkle Root 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Height	0 (Main Chain)	
Timestamp	2009-01-03 18:15:05	
Received Time	2009-01-03 18:15:05	
Relayed By	Unknown	
Difficulty	1	
Bits	486604799	
Size	0.285 kB	
Weight	0.898 kWU	
Version	1	
Nonce	2083236893	
Block Reward	50 BTC	

Transactions

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b	2009-01-03 18:15:05
No Inputs (Newly Generated Coins)	 1A1zP1eP5QGefi... (Genesis of Bitcoin @) 50 BTC

Source: blockchain.info

Bitcoin blocks

Bitcoin block information

Block #485226

Summary		Hashes
Number Of Transactions	1685	Hash 000000000000000000000046c024b001ad95db6fbfdac377fd3241ff780a3afc0ddf
Output Total	4,797.37965875 BTC	Previous Block 000000000000000000000761703d7078fe41387d7423ea1e85b8e982a0bfd65b2
Estimated Transaction Volume	1,214.76072845 BTC	Next Block(s)
Transaction Fees	0.64893797 BTC	Merkle Root 85c02e73b85e3851836bf7badf6e543934aea4dc82b233887263e26814c72c47
Height	485226 (Main Chain)	
Timestamp	2017-09-14 14:17:13	
Received Time	2017-09-14 14:17:13	
Relayed By	BitClub Network	
Difficulty	922,724,699,725.96	
Bits	402731275	
Size	1227.087 kB	
Weight	3992.607 kWU	
Version	0x20000000	
Nonce	2314934057	
Block Reward	12.5 BTC	

Source: blockchain.info

Bitcoin transaction structure

- Because Bitcoins exist only as records of transactions, there is no actual balance of a wallet but the balance is the sum of transactions to an address
- These records are not automatically combined but instead sit there as different transaction records
- When sending a new transaction, the sender has to provide proof that associated address has enough funds to do so
- Each transaction outputs an Unspent Transaction Output (UTXO) that can be used as proof (input) in a future transaction

Bitcoin transaction structure

- To allow value to be split and combined, transactions contain multiple inputs and outputs
 - Input - A reference to an output from a previous transaction i.e. a record of the value and address used to send the coins being sent in the current transaction. The value being sent in a transaction can be the combination of the value received in multiple previous transactions
 - Output - Contain instructions for the sending of Bitcoins i.e. recipient address and value. Each output then waits as an Unspent Transaction Output (UTXO) until a later input spends it
- Although it would be possible to handle coins individually, it would be inefficient to make a separate transaction for every cent in a transfer

Bitcoin transaction structure

- Every transaction must refer to one or more previously mined transactions
- Furthermore, the entire combined value of inputs needs to be spent as output
- For example, if the input is worth 50 BTC but you only want to send 25 BTC, two outputs worth 25 BTC will be created: one to the destination, and one back to you (i.e. change)
- Any input bitcoins not redeemed in an output is considered a transaction fee, hence whoever generates the block will get it

Bitcoin transaction structure

- A transaction at a high level contains the following
 - Metadata - This part contains values such as the size of the transaction and its hash
 - Input includes:
 - output index number: transaction identifier of a previously received transaction (+ n, which is a counter)
 - signature script: allows sender to provide data parameters that satisfy the conditionals in the pubkey script
 - transaction identifier: an identifier used to uniquely identify a particular transaction from which the output was generated; specifically, the sha256 hash of the transaction
 - Note that the signature and public key script are executable lines of code!
 - Output includes:
 - value: the value/amount being sent by the transaction
 - public key script: sets the conditions that must be fulfilled for amount to be spent

Bitcoin transaction structure



Image by Venzen <venzen@mail.bithai.net> 2014 CC-SA
conditions of reuse: <http://jafala.bithai.net/works/txinout.htm>

Source: https://248qms3nhmvl15d4ne1i4pxl-wpengine.netdna-ssl.com/wp-content/uploads/2014/07/Bitcoin_tx_example.png

Bitcoin transaction structure

- Because each transaction spends value previously received in one or more earlier transactions, transactions are also chained together
- All transactions included in the blockchain are categorized as either UTXOs or spent transaction outputs.
- For a payment to be valid, it must only use UTXOs as inputs, and if the value of outputs exceeds that of inputs, the transaction will be rejected
- Outputs are tied to transaction identifiers (TXIDs), which are the hashes of signed transactions

Bitcoin transaction structure

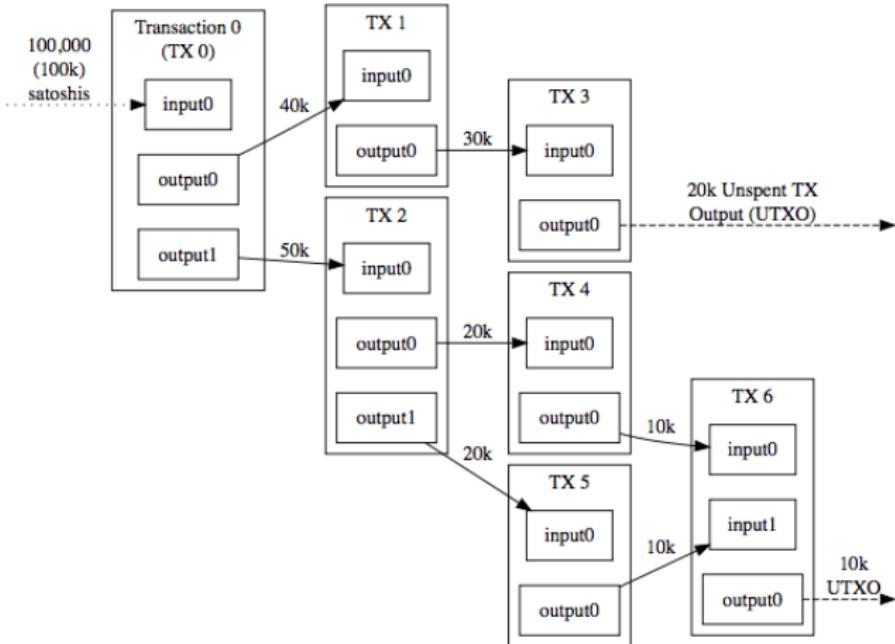


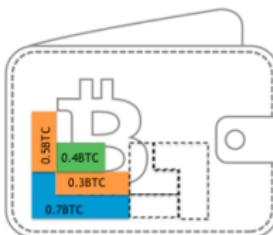
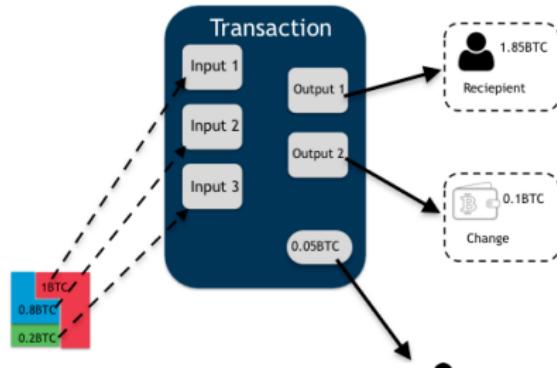
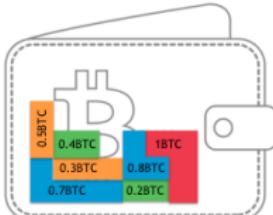
Figure: Transaction chain with a fee of 10k satoshi

Source: <https://blog-archive.bitgo.com/content/images/2015/05/txchains.png>

Choosing which output to spend



All funds are organized by transaction in the wallet



The wallet picks the best way to spend UTXOs



Transaction fees

- The sender is required to pay the full transaction fee on top of the amount being transferred
- Considering that block size is limited, transaction fees can be seen as the cost of purchasing a portion of block space for a transaction, an incentive to mining nodes to include a particular transaction in the next block
- This fee is therefore determined by the size of the transaction data and is independent of the value being transferred
- The price of this block space is completely driven by supply and demand. When demand is high, fees are higher

Transaction fees

- Typically, users will pay a fee imposed by cryptocurrency wallet providers that use predictive algorithms to determine the required fee per byte of transaction data
- However, transaction fees are voluntary on the part of the person making the transaction. A user may opt to pay lower fees or no fees at all, although, this will lower the priority of the transaction and increase confirmation time
- Transactions that generate higher fees will always be confirmed faster, as participating mining nodes set out maximize their utility

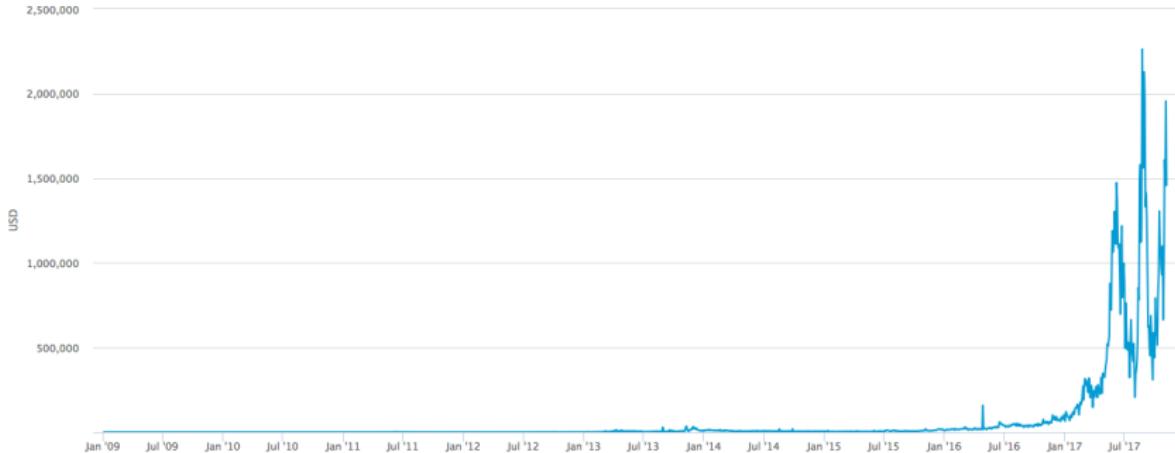


Figure: Total value of all Bitcoin transaction fees paid to miners

Source: blockchain.info

Block reward

- Processing nodes (miners) are offered a block reward as an additional incentive for securing the blockchain
- The reward given to the miner that successfully posts a valid block is usually in the form of newly generated coins/tokens
- Ultimately, value/type of the reward is determined by the architecture of the blockchain. Some blockchains don't even offer rewards, but will have different economic incentives in place
- The Bitcoin reward started at 50 BTC in the first block and halves every 210000 blocks (\approx 4 years). It is currently 12.5 BTC
- Ethereum offers a static block reward of 3 Ether

Coinbase transactions

- The block reward is assigned using a coinbase transaction
- This is a special type of transaction used to create new units of the cryptocurrency
- Each block will contain one and only one coinbase transaction to reward the block miner, and it must be the first transaction of the block
- Coinbase transactions are the only transactions without real inputs as they are not linked to any previous transaction

Coinbase transactions

- The coinbase transaction can have an arbitrary input of 100 byte size. E.g. the Bitcoin genesis block coinbase parameter contained the newspaper headline "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", probably believed to be proof that the block was created on or after January 3, 2009
- The transaction's output is used to send the block reward and transaction fees to the miners address
- The k-block rule applies to these transactions i.e. Bitcoin's coinbase transactions cannot be spent until they have received at least 100 confirmations on the blockchain (\approx 16hrs 40min)
- This prevents double spending in the event of a fork (i.e. a split) in the chain



Figure: Total value of Bitcoin block rewards and transaction fees paid to miners

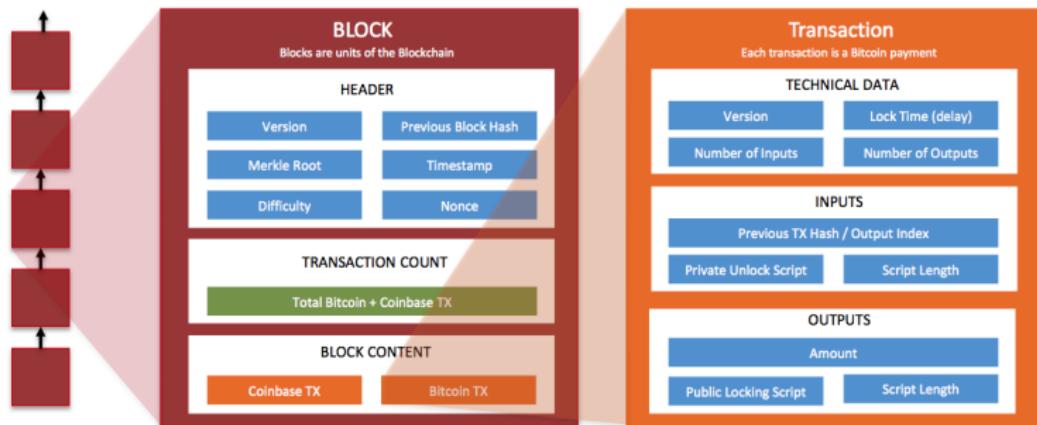
Source: blockchain.info

Bitcoin transaction ledger

861608b43d209e0d3c1cc1036b103a01327b9e51cc7f568b0c1414e5bc0d572e	2017-09-14 14:17:13
No Inputs (Newly Generated Coins)	
	 155fzaEBHy9Ri2bMQ8uuuR3tv1YzcDwyd4 Unable to decode output address
	13.14893797 BTC 0 BTC
	13.14893797 BTC
29a28f608e9105fec54b708b157a847a4be152127b9e847cc41195379aee517	2017-09-14 14:15:09
136GDc7t14nBs5JmvXLBgdj2XhMFxgC7lA	
	 1NqetnS5R861EUipzPzMpkLJWzNq79i6Q6 1N68Xm7A1FeahHcN7DLRfrTFIOtnPKoJW
	0.225848 BTC 0.005 BTC
	0.230848 BTC
87712e12171f5070313079566c3cd79317a7358090a31709ed25201428c3d9a	2017-09-14 14:16:28
16RqkjpJo1JKNMWKQ9rdcmDyg4GJL3RntKF	
	 38Zh9qjqzq8YAfqqUPs7eJWR4ky7Wmfz5 1LNYb3h71wxir6o6HT5J8y1h7asV6yp4X
	0.0200352 BTC 0.0983576 BTC
	0.1183928 BTC

Source: blockchain.info

Blockchain anatomy



Source: <https://www.slideshare.net/arcatomia/anatomy-of-a-blockchain>

Broadcasting transactions

- Peers will exchange information until it is available to every node on the network
- When a transaction is executed on a node and its validity is confirmed, the node stores it and then announces it to its nearest neighbors
- The neighbor nodes will in turn confirm the validity of the transaction and broadcast the transaction information to their respective neighbors
- This process goes on until the transaction is propagated across the network
- Transmission across the entire Bitcoin network takes 1-2 seconds

Broadcasting transactions

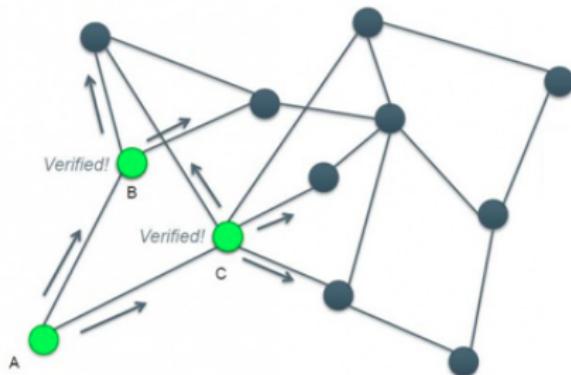


Figure: Node A announces a transaction to its peers B and C. If the transaction is verified, B and C announce it to their peers

Consensus

- Consensus is a process of agreement between distrusting nodes on a final state of data
- To maintain the transaction ledger, blockchains use a variety of distributed consensus mechanisms i.e. consensus is achieved between multiple nodes on the network
- A consensus mechanism describes the set of steps that are taken by all, or most, nodes in order to agree on a proposed state of the data
- In order to achieve the desired outcome, a blockchain's consensus mechanism must meet the following requirements
 - ① Agreement
 - ② Termination
 - ③ Validity
 - ④ Byzantine fault tolerant
 - ⑤ Integrity

Consensus



Agreement

All nodes must decide on the same values

Termination

All honest nodes terminate execution of the consensus process and eventually reach a decision



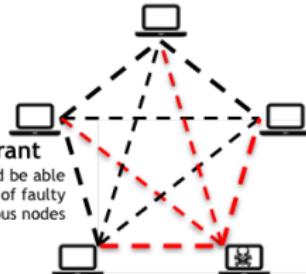
Integrity

Each node makes a decision only once in a single consensus cycle



Validity

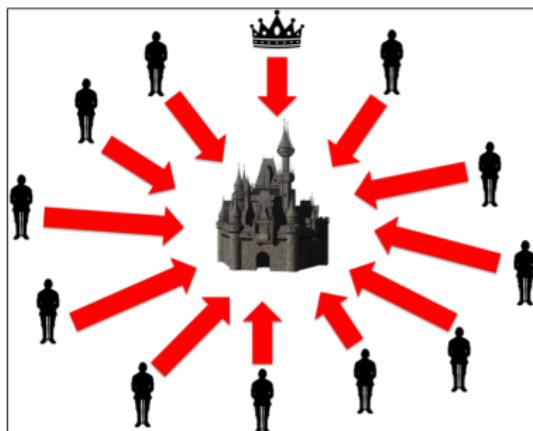
The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node



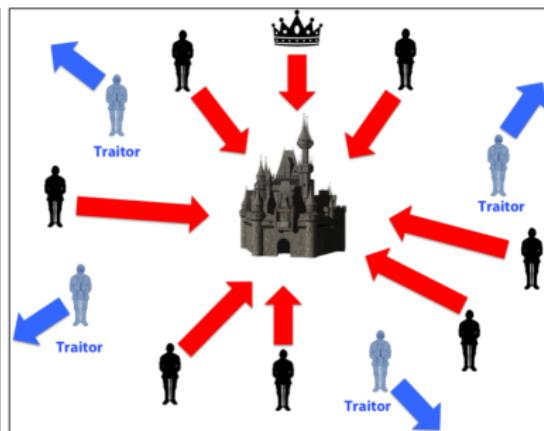
Byzantine fault tolerant

The consensus algorithm should be able to run in the presence of faulty or malicious nodes

Byzantine Generals' Problem



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

Source: https://cdn-images-1.medium.com/max/800/0*-xCD-EI4LZ48dji1.png

Byzantine Generals' Problem

- An agreement problem in which a group of generals, each commanding a portion of the Byzantine army, encircle a city
- In its simplest form, the generals only need to reach consensus on whether to attack or retreat
- For a halfhearted attack by a few generals would become a rout and be worse than a coordinated attack or a coordinated retreat
- Byzantine fault tolerance is achieved if all loyal generals are able to reach a unanimous agreement on their strategy and if every loyal general does not deviate from that common decision as a result of the influence of traitorous generals
- In computer science, a Byzantine failure is defined as an arbitrary deviation of a process from its assumed behavior based on the algorithm it is supposed to be running and the inputs it receives

Byzantine Fault Tolerance

- Formally, the conditions for a consensus protocol tolerating Byzantine failures are
 - Termination - every non faulty process (participant) decides on some value
 - Validity - If all non faulty processes propose the same value, then all correct processes decide on that exact value
 - Integrity - The value that has been decided on must have been proposed by some process
 - Agreement - Every non faulty process must agree on the same value

Byzantine Fault Tolerance

- The ability to tolerate byzantine failures is a crucial part of a blockchain's ability to maintain reliable records of transactions in a transparent, tamper-proof way
- The need for trust when transacting on a network, that is borne out of fear of malicious entities, is eliminated given that the integrity of the system can be maintained even in the presence of these entities
- This allows users to transact in a hostile environment
- Fundamentally, Byzantine Fault Tolerant (BFT) systems assign a threshold for consensus, by way of the system allowing for a proportion of processes to fail (reject consensus) and still achieve consensus, before the whole system fails

Sybil attacks

- Traditional blockchain implementations have at a 50% threshold before the integrity of the system can be compromised (i.e. 51% attack also called a Sybil attack)
- Because many distributed systems have no form of identity management beyond accounts that are trivially created, such a system would be at risk of a Sybil attack
- In a Sybil attack, the attacker challenges the integrity of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence
- A Sybil attacker would therefore have to control more than 50% of the processes in order to pose a threat

Sybil attacks

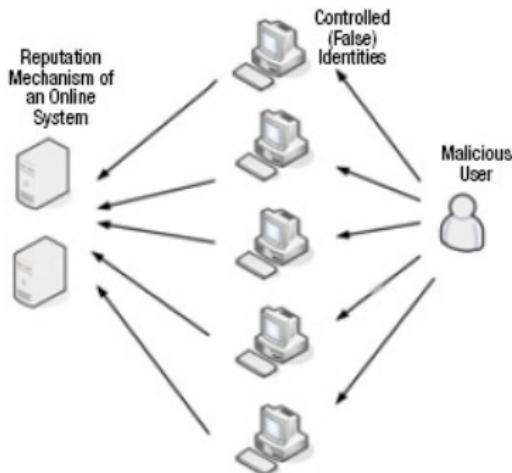


Figure: A malicious user takes on multiple identities on the network in an attempt to undermine the integrity of the decision making process

Source: <https://www.isaca.org/Journal/archives/2010/Volume-4/PublishingImages/10v4auditing-electronic.jpg>

Proof of Work

- The Bitcoin blockchain hinders Sybil attacks by tying the ability to generate a new block to the user's available computing power
- A malicious user would therefore require more than 50% of the network's computational power to become a threat to the system
- This rule is enforced through the use of the Proof-of-Work (PoW) consensus mechanism
- A proof-of-work system involves finding a computationally intensive solution to a rather trivial puzzle in order to create a valid block
- The process of creating blocks in the proof-of-work system is called mining

Proof of Work

- To solve the puzzle, nodes must find a nonce that can be used to generate a valid block
- A block will only be valid, if it was at least as difficult to compute than the most recent valid block in the chain
- Where this difficulty is defined by the number of leading zeros in the block's hash
- This is achieved by manipulating the nonce until the new block's hash satisfies this condition i.e. the nonce is used as proof that sufficient labor has been undertaken
- SHA256 is used as the underlying cryptographic hash function

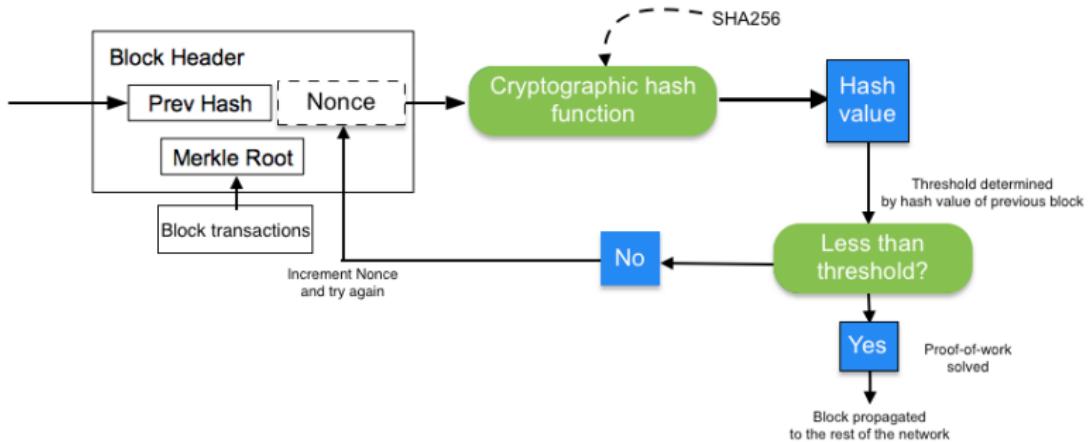
Proof of Work

- This design makes the entire process inherently resource intensive, providing strong cryptographic guarantees of Sybil resilience.
- If a malicious node decides to alter some transactions in a previous block, then the node will need to compute a nonce for all the succeeding blocks
- By the time it re-finds the nonce of all the succeeding blocks, more blocks will have been mined, making it infeasible to edit the history of a blockchain

Proof of Work

- However there is no guarantee that the node with the highest hash rate will always find the nonce first, due to the randomness involved in the process
- A higher hashrate only means the node can make attempts at finding the nonce at a faster rate
- The hash of the block being mined will be different for every miner because the has depends on variable factors like the time stamp and the miners address
- As a result, the nonce will be different for every miner
- Therefore, it's not a race to solve the puzzle; rather, it's a lottery system where the likelihood of getting lucky is determined by the miner's hash power

Proof of Work



Achieving consensus

Once a 'solution' has been found, nodes do not explicitly express their acceptance of a new block

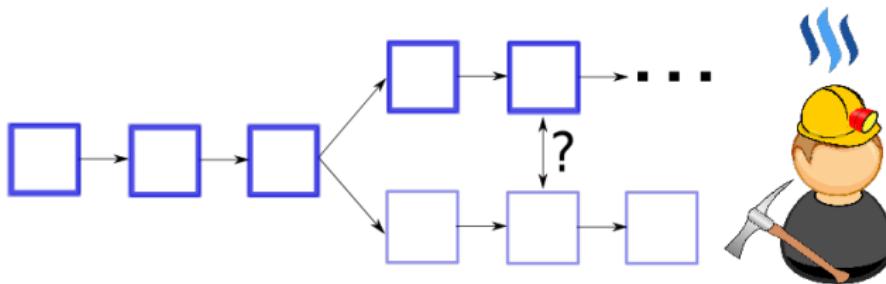
Instead, consensus is implied by the nodes moving on to 'solve' the next block, with a header that points to the recently accepted block as the previous block in the chain

Consensus is not guaranteed; failure to achieve it could result in a 'fork' in the blockchain i.e a split in the chain where nodes start operating on different versions of the chain

Forking

- A fork happens when there is a conflict among nodes regarding the validity of a blockchain
- Forks will lead to situations where more than one blockchain is being validated by different parts of the network
- When more than one blockchain exists on the network and every blockchain is validated for some miners
- Three types of forks exist: A regular fork, soft fork and a hard fork

Forking

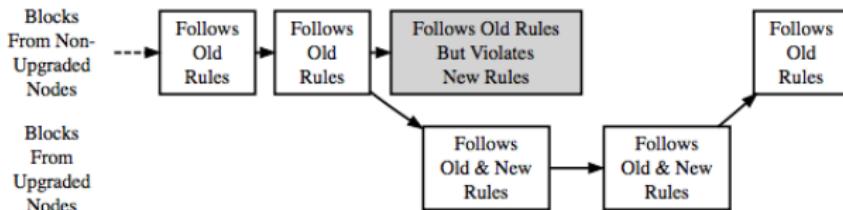


Source: <https://steemitimages.com/DQmb6KJRQfAwHxQdFbAhrqMq2ZdWSQ9v7687tHViG3EExpD/chain.png>

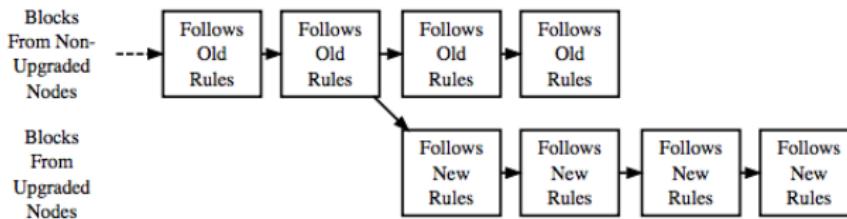
Forking

- ① Regular fork/ chain split: A temporary fork that happens when two miners find a block at nearly the same time. Resolved by coordination among the miners
- ② Soft fork: Happens when a change to the software protocols invalidates a subset of old blocks/transactions
 - This type of fork is forward compatible i.e. all blocks considered valid by the newer version are also valid in the old version
 - If majority hash power shifts to the newer version, the system will self correct
- ③ Hard fork: A change in software protocols that requires all miners to upgrade in order to resolve the conflict
 - Hard forks are not forward compatible as previously invalid blocks become valid
 - Older versions will not accept the new blocks, causing the users of the old software to remain on their own blockchain fork indefinitely

Soft vs hard forks



A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Source: <https://bitcoin.org/en/developer-guide>

Coordination in mining

Mining as a coordination game

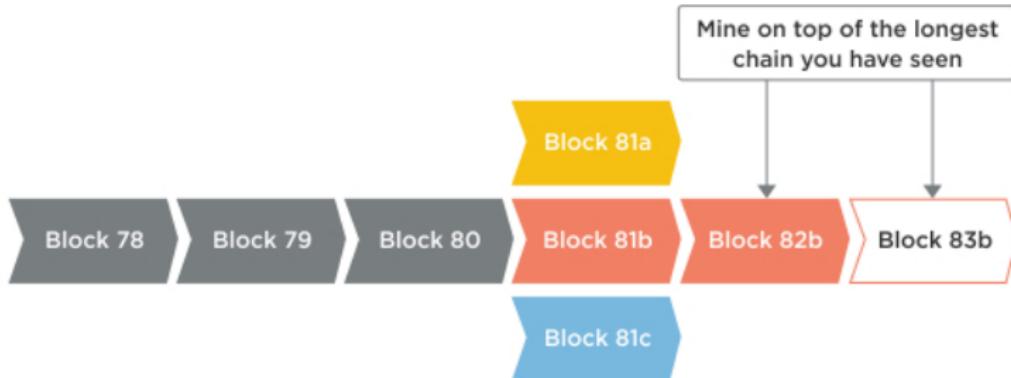
- A direct result of the consensus mechanism is that mining becomes a coordination game
- Longest chain rule (LCR): Nodes will always consider the longest chain to be the canonical one and will keep working on extending that chain
- Theoretically, if miners follow this rule, there will be no forks and only a single chain
- In practice forks sometimes occur, and consensus temporarily disappears

Longest chain rule

To understand the significance of LCR consider the following scenario

- Suppose two miners both find a valid block within a few seconds of each other and broadcast them to the network. This is entirely feasible, given that it is a peer to peer network
- And because the network is global, latency will result in some nodes seeing the first miner's block and others will see the second
- Now there are two chains with identical history up until this point, and neither is longer than the other, resulting in a temporary fork
- Eventually another miner will find the next valid block, which will be attached to either one of the the chains
- This becomes the longest chain, and it becomes the definitive blockchain
- Transactions in the alternate fork do not disappear, they get put back in the pool of unconfirmed transactions and wait to be put in subsequent blocks

Longest chain rule



Source: <https://shiftnrg.nl/wp-content/uploads/2017/05/start-mining-on-longest-1024x382.jpg>

Coordination in mining

- Coordination is required, as each miners will want to attach their blocks to the chain to which they expect the others will attach their blocks
- And because of the k-block rule, each miner will have a vested interest in the survival of that chain in order to protect the value of their block rewards
- Miners decisions of which chain to mine are therefore strategic complements (i.e. they mutually reinforce one another)

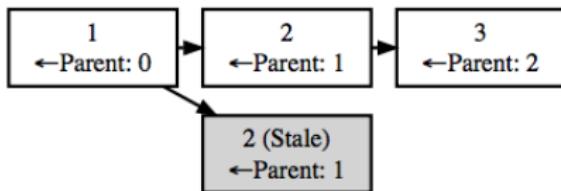
Coordination in mining

- Bitcoin's protocol uses a 'winner takes it all' reward scheme
- If a miner posts a valid block that is subsequently rejected after the fork has been resolved (i.e. a stale block), she loses her block rewards
- Hence miners will always try to avoid forks as there's the risk of loss of block rewards
- Essentially, it is game theoretically optimal for every miner to mine on the longest chain and avoid mining forks

Stale blocks

- The total number of stale blocks produced in the network is inversely proportional to the average time it takes to generate a new block
 - Shorter block generation time means less time for the newly mined block to propagate throughout the network, increasing the probability of more than one miner finding a valid block, thereby creating stakes
 - If the average block generation time is longer, there is less chance that multiple miners will be able to find a valid block, increasing the time for the first solved block to be propagated across the network
- The problem with stale blocks is that they may delay the confirmation of a transaction, as when two miners post a block at the same time, they won't necessarily always include the same set of transactions
- Hence the average confirmation time is not equal to average block generation time

Stale blocks



Stale blocks are valid but not part of the best block chain

Source: <https://bitcoin.org/en/developer-guide>

Stale blocks

- Stale blocks also have the effect of incentivizing pooled mining, as miners try to avoid wasting computational effort
- Ethereum tackles the issues caused by stale blocks using a modified version of the GHOST (Greedy Heaviest Observed Subtree) protocol
- GHOST originally was a protocol modification, a chain selection rule, that makes use of blocks that are off the main chain to obtain a more secure and scalable system
- With this modification, it is possible to speed up the blockchain to a velocity of up to 1 block per second, increasing the possible transaction rate without compromising the blockchain consensus and security
- This protocol is the reason why, relative to Bitcoin, Ethereum can achieve shorter block times while reducing the incentive for pooled mining

GHOST protocol

Ethereum refers to stale blocks as uncle blocks and its implementation of the GHOST protocol is defined as follows

- Block B must specify a parent block A and zero or more uncles
- An uncle U included in a block B must have the following properties:
 - U must be a direct child of any one of the 6 most recent ancestors of B
 - U cannot be an ancestor of B
 - U must have a valid block header
 - U must be different from all other uncles included in previous blocks and the other uncles included in B
- For every uncle U in block B, the miner of B gets an additional 3.125% added to its coinbase reward and the miner of U gets 93.75% of a standard coinbase reward

Uncle mining in Ethereum

- A maximum of 2 uncles are allowed per block
- The inclusion of uncle blocks has two main effects
 - It decreases the incentive for centralization in the form of mining pools as producers of stale blocks are still rewarded
 - It increases the security of the chain by augmenting the amount of work on the main chain by that done in the uncles i.e. the overall difficulty of the blockchain also includes the sum of difficulties of the stale blocks
- However, uncle mining also introduces additional economic complexity as some miners now have an incentive to mine empty uncles

Mining hardware

- CPU mining was the first type of mining available in the original bitcoin blockchain, however this quickly became obsolete as nodes switched to GPU mining
- GPUs support faster and parallelized calculations, but even these did not last long
- Miners started using Field Programmable Gate Arrays (FPGAs), integrated circuits programmed to perform SHA256 calculations
- Eventually miners started using Application Specific Integrated Circuits (ASICs) designed to perform the SHA256 operation at a very high hashing rate
- Due to the quickly increasing mining difficulty level, single-unit ASICs are no longer profitable

Mining hardware

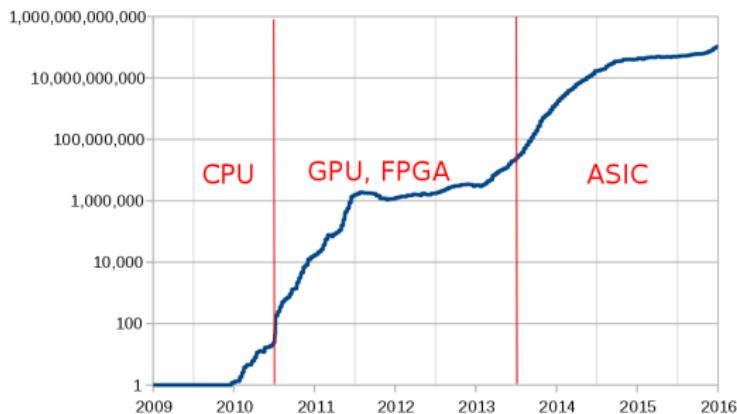


Figure: Bitcoin relative mining difficulty chart with logarithmic vertical scale. Relative difficulty defined as 1 at 9 January 2009. Higher number means higher difficulty

Source: https://commons.wikimedia.org/wiki/File:History_of_Bitcoin_difficulty_and_mining_hardware.svg

Achieving consensus

- It is possible to use alternative consensus mechanisms that are less centralized and more energy-efficient
- This includes Proof of Stake, Proof of Activity, Threshold signature schemes, Proof of Burn
- Multiple game theoretic considerations are feasible; with the caveat that the system has to be Byzantine fault tolerant
- However, each method will have its own advantages over the others that will make it more desirable, depending on the intended function of the blockchain

Alternative consensus mechanisms

Proof of stake

- Likelihood of updating the chain is determined by the wealth of the node.
- The definition of wealth is subjective and depends on the function of the blockchain e.g. value or age of currency or assets linked to the node
- This system works on the idea that if a node or user has enough stake in the system, acting truthfully would outweigh the benefits of performing an attack on the system
- The model aims to provide the same type of fairness in the distribution of the right to create a block without requiring miners to burn external resources
- Proof of stake systems are more decentralized, however they must work hard to build communities around their tokens

Alternative consensus mechanisms

Proof of stake

- There are no block rewards, instead the incentive for miners lies in wanting to guard their own wealth given that they have a vested interest in maintaining the integrity of the blockchain
- This design has been criticized for the fact that the wealthiest nodes will always stand to benefit the most from the transaction fees
- The concept of coin age can alleviate this; the probability of forging the next block reaches a maximum after an arbitrary number of days in order to prevent very old or very large collections of stakes from dominating the blockchain through centralized mining pools

Proof of Work vs ***Proof of Stake***



proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



Proof of Stake currencies can be several thousand times more cost effective.

source: <https://blockgeeks-assets.scdn7.secure.raxcdn.com/wp-content/uploads/2017/03/infographics2017-01.png>

Alternative consensus mechanisms

Threshold signature schemes

- Uses a multi-signature scheme with a subset of nodes that can be tolerated to fail or be corrupted before the system fails
- The ability to construct a single signature used to sign a valid block is distributed across the network, with each node producing only a partial signature
- Consensus on an update is considered to be reached if the signature threshold k has been met i.e. k out of n signing nodes have generated valid signatures
- The rest of the $n - k$ participating nodes can fail to deliver any or can deliver invalid signature shares

Alternative consensus mechanisms

Threshold signature schemes

- Desired network latency and tolerance to network failure will determine the value of n
- k will vary with the desired tolerance to Byzantine failures
- In a round robin fashion, nodes will take turns to create the next block within a specified time frame, to allow for the communication required to create the multi-signature to take place
- While significantly less resource intensive relative to the other consensus models, it reintroduces the requirement of trust

Alternative consensus mechanisms

Reputation based schemes

- The node to post the next block is selected on the basis of the reputation it has built over time
- This can be based on the voting of other member nodes

Federated byzantine consensus

- Nodes keep a group of publicly trusted peers and propagate only those transactions that have been validated by the majority of trusted nodes
- In turn, those trusted nodes do not agree to the transaction until the nodes they consider important agree as well, and so on

Alternative consensus mechanisms

Proof of burn

- The idea is that miners should show proof that they burned some coins i.e. sent them to a verifiably unspendable address
- This is intended such that an individual miner finds the task expensive, discouraging malicious activity without having to consume real resources

Proof of activity

- Designed as a combination of Proof of Work and Proof of Stake
- The nodes responsible for signing the next block are identified using a routine called *follow-the-satoshi*
- N satoshis (smallest unit of the Bitcoin) are chosen at random from the available supply. The N addresses identified as those that control these satoshis are then given the right to each sign the block header and a block will be valid only if all N addresses have signed it

Digital tokens

- Blockchains have the ability to store digital tokens
- These tokens exist conceptually as entries in the ledger
- You own these tokens because you have a key that lets you create a new entry re-assigning the ownership to someone else
- These can be used to represent assets such as USD, gold, company stocks, individual tokens representing smart property, secure unforgeable coupons, and even token systems with no ties to conventional value at all, used as point/loyalty systems

Digital tokens

Two types of digital tokens can be issued on a blockchain

① Intrinsic tokens

- These are also called native tokens
- They are not backed by anything and their utility lies within the token itself
- The value of these tokens is determined within the system that they are created, by the people who own them
- Cryptocurrencies are the most common intrinsic tokens

② Asset backed tokens

- Represent claims to an underlying asset
- The tokens can be transferred from person to person and anyone holding the token can go back to the issuer and claim the underlying asset
- Unlike native tokens, these have no fungibility

Token rights

Payment

Token is the only way to make payments on the network



Transfer of value occurs only through BTC

Access

Token provides the ability to use the platform itself



etherium

Eth is used to purchase gas which pays for transactions

Profit or fee

Holders get a share of revenue or profits



Dividends distributed to DigixDAO token holders come from fees of storage of gold

Contribution

Tokens needed to play certain roles on the platform



1ST tokens allow holders to determine who won a sports bet placed on the platform

Block creation

Tokens determine who secures the blockchain



Ethereum's security-deposit based Proof-of-stake consensus protocol

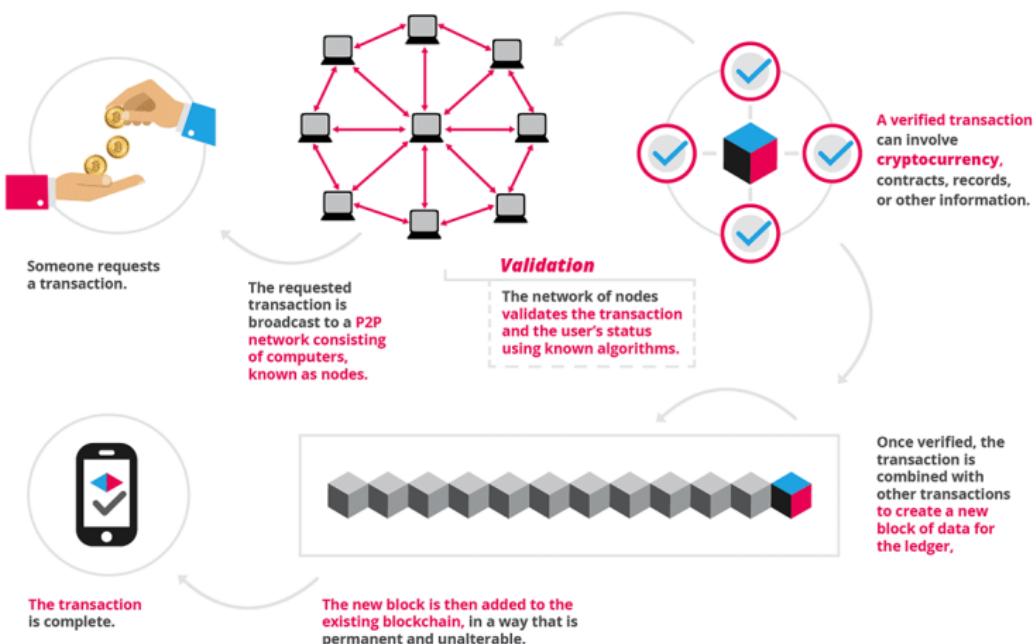
Governance

Holders influence features, project direction, protocol details, or more



Token holders determine the flow of funds by voting on potential projects

How Bitcoin's blockchain works



source: <https://blockgeeks-assets.scdn7.secure.raxcdn.com/wp-content/uploads/2016/09/infographics0517-01-1.png>

How Bitcoin's blockchain works

The network runs in the following way

- ① New transactions are validated and broadcasted
- ② Each mining node collects new transactions into a block
- ③ Mining nodes work on the computationally intensive task of finding a valid proof-of-work
- ④ When a node finds a valid block, it broadcasts it to its neighboring nodes to propagate across the network
- ⑤ Nodes accept the block only if it has a valid block header
- ⑥ Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the new parent hash

How Bitcoin's blockchain works

- ① New transactions are validated and broadcasted
 - Distributed databases require synchronicity in order to maintain a uniform record of information
 - Once a transaction is executed by a node, it is broadcast to its nearest peers which in turn validate it and then broadcast it to their nearest peers until the entire network has received the transaction details
 - The validation process involves filtering out transactions not properly signed by private keys or transactions from accounts with insufficient balances
 - After peers exchange their information they store it to be processed.

How Bitcoin's blockchain works

- ② Each mining node collects new transactions into a block
 - Miners collect all the new un-mined and valid transactions waiting to be confirmed and construct a merkle tree
 - The miner creates a block, whose header contains the Merkle tree root of all the transactions, a timestamp, nonce, a version number, the hash of the parent block and the difficulty target for the block
 - Using a Merkle tree is preferable over a hash chain or a hash of concatenated transactions because it allows for a much quicker and simpler test of whether a particular transaction is included in the set

How Bitcoin's blockchain works

- ③ Mining nodes work on the computationally intensive task of finding a valid proof-of-work
 - The nonce is the output of the proof-of-work algorithm
 - Mining nodes are incentivised to participate in the computationally intensive search, by being offered a 'block reward' in addition to the fees generated by the transactions included in the mined block

How Bitcoin's blockchain works

- ④ When a node finds a valid block, it broadcasts it to its neighboring nodes to propagate across the network
- ⑤ Nodes accept the block only if it has a valid block header
 - A block is valid only if it hashes to a value less than or equal to the defined difficulty
 - Furthermore, a block is valid if and only if all included transactions are valid, the block's time stamp is correct, and the miner has assigned the block reward
- ⑥ Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the new parent hash.

Blockchains outside of finance

A number of use cases of blockchains have been emerged across different industries since the technology's introduction

This includes but is not limited to the Internet of Things, recording of events, medical records, identity management or any type of data that needs tracking

Many of the leaders in the cloud space have since started offering blockchain solutions to their customers. Microsoft (Azure), IBM (BlueMix) and Amazon (AWS) are the the leaders in the space for Blockchain as a Service (BaaS)

Blockchains outside of finance

Internet of Things

- The concept of connecting devices embedded with sensors, software and network connectivity to the internet
- This enables these devices to communicate and collect and exchange data
- IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems
- This has led to concepts such as wearables, smart homes, smart grids, smart connected cars, and smart cities, all based on the basic concept of an IoT device
- Blockchains are promising for IoT security for the same reasons they work for cryptocurrency; immutability of data and authentication protocols guarantee fast, low cost and secure peer-to-peer communication between devices

Energy	Manufacturing	Supply Chain and Logistics	Healthcare	Retail	Smart Building
Security					
Payment Platforms					
Data Analytics					
Cloud and Software Platform					
Hardware					
Network and Connectivity					

source: <https://acceleratingbiz.com/wp-content/uploads/2017/08/Internet-of-Things.png>

Blockchains outside of finance

Cloud storage

- Blockchains are continually being developed in an attempt to address concerns regarding existing models of cloud-based storage which are all centralized solutions.
- The technology is being used to provide decentralized and distributed storage across communities instead of a single central organization
- Nodes avail storage space on their hard drives and are able to act autonomously to perform various functions such as data transfer, validation and perform data integrity checks
- Files are encrypted and divided into small pieces (shards) to be distributed across the network
- Participating nodes are typically compensated with some cryptocurrency tokens for their contribution to the storage space available on the network

Blockchains outside of finance

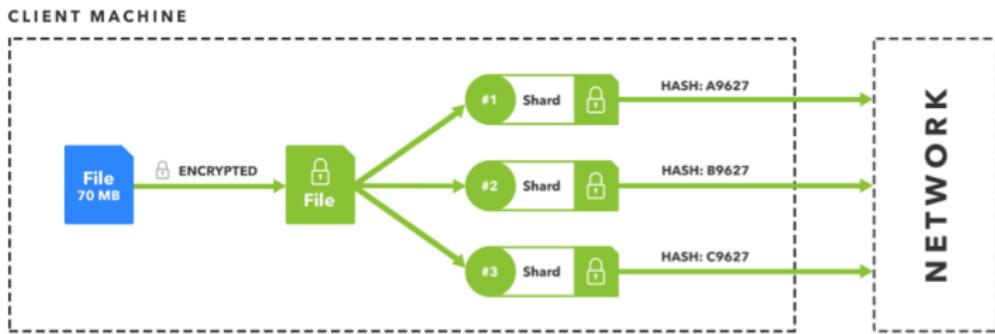


Figure: The sharding process

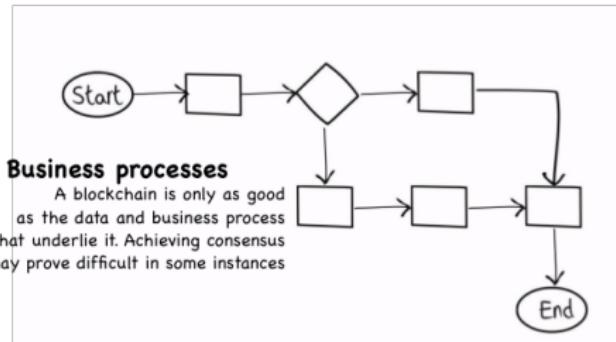
source: <https://decentralize.today/simplifying-the-storj-whitepaper-ef38ad0ea7de>

Implementation challenges



Standards

Technical standards will be needed to ensure similar technical implementations across industries, particularly in cases where multiple blockchains need to interoperate with each other



Privacy

There are still concerns regarding the ethics involved with organizations sharing information about counterparties and the ability to permanently impact their reputations



Speed and performance

The question whether blockchains will one day be able to perform at scale, making the technology suitable for high-speed and high volume transactions still remains unanswered

Streamlining existing markets



Real Estate

\$2-4bn annual US cost savings

Recording property records on a blockchain, could meaningfully lower transactional risk associated with existing property registration. The tamper-proof ledger could also help lower real estate fraud in emerging markets



Capital Markets

\$11-12bn annual global cost savings

Blockchain-based systems can significantly shorten trade settlement time and cut reconciliation costs. Additional savings could also be achieved through the reduction in information assymmetries



Anti-money laundering compliance

\$3-5bn annual global cost savings

Increased transparency and efficiency could improve data quality, allowing regulatory functions to operate more efficiently

Blockchain consortia

A handful of consortia with the intention of advancing the use of blockchains in the financial services industry have also since emerged

- R3
 - A distributed database technology company that leads a consortium of more than 70 of the world's biggest financial institutions in blockchain research and development
 - The consortium started on September 15, 2015 with nine financial companies, including Barclays, Credit Suisse, Goldman Sachs and J.P. Morgan
 - Their flagship product is Corda, a distributed ledger platform designed for financial institutions to record, manage and automate legal agreements between business partners
 - Although it is inspired by blockchain databases and is expected to have many of the benefits of blockchains, it is not a blockchain
 - Makes use of "supervisory observer nodes", which can be used by regulators to monitor the system

Blockchain consortiums

- Hyperledger
 - An umbrella project of open source blockchains and related tools started in December 2015 by the Linux Foundation, with the objective of advance cross-industry collaboration and a focus on improving the performance and reliability of blockchains and distributed ledgers
 - Early members include IBM, Intel, J.P. Morgan, Wells Fargo and SAP
 - Has multiple blockchain platforms including Hyperledger Burrow, Hyperledger Fabric, Hyperledger Iroha and Hyperledger Sawtooth
 - Hyperledger Fabric is a permissioned blockchain infrastructure, originally contributed by IBM and Digital Asset
 - It provides a modular architecture with a delineation of roles between the nodes in the infrastructure, execution of Smart Contracts, and configurable consensus and membership services

Blockchain consortiums

- South African Financial Blockchain Consortium
 - A collective of 24 institutions that have come together to explore the use of blockchain technology in the South African financial market
 - Members include Capitec, the Reserve Bank of South Africa and UCT
 - In addition to Ethereum, they are exploring the use of the Corda, Hyperledger and Chain Core platforms
 - Primary objectives include reducing inefficiencies and creating opportunities to save costs for institutions and end consumers
 - It also intends to explore using a permissioned distributed ledger to store identity information to alleviate administrative requirements and costs associated with Know-Your-Customer (KYC) and the Financial Intelligence Centre Act (Fica)

Recap

- Blockchains reintroduce a form of single entry bookkeeping in financial services
- Cryptography is used to enable secure communication and guarantee overall security of the system
- The integrity of a blockchain depends on private keys remaining private

Recap

- There are multiple consensus mechanisms preferable over Proof-of-Work as they are significantly less resource intensive. The ideal choice ultimately depends on the desired function of the blockchain
- Ethereum makes use of the GHOST protocol to prevent wastage of resources that comes with mining stale blocks under Proof-of-work
- Two kinds of digital tokens can be issued on a blockchain; intrinsic tokens and asset backed tokens

Recap

The five key components of a blockchain

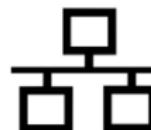


Cryptography

Hash functions, Merkle trees and public key cryptography

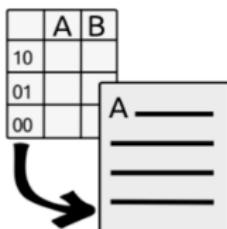
Consensus mechanism

Algorithm that determines the order of transactions in an environment of conflicting interests



P2P network

Network for peer discovery and data sharing in a peer-to-peer fashion



Ledger

List of transactions bundled together in cryptographically linked blocks



Validity rules

Common set of rules of the network i.e what transactions are considered valid and how the ledger gets updated

Recap

Benefits of using a blockchain

Cost reduction
Reduces costs by removing overheads associated with intermediaries



Trustless agreements
The ability to transact with peers in an environment of conflicting interests without the need for trust



Security

Secure and transparent decentralized transactions on a database with no single point of failure



Efficiency gains

Increased efficiency and reduced settlement times in multiparty transactions

Recap

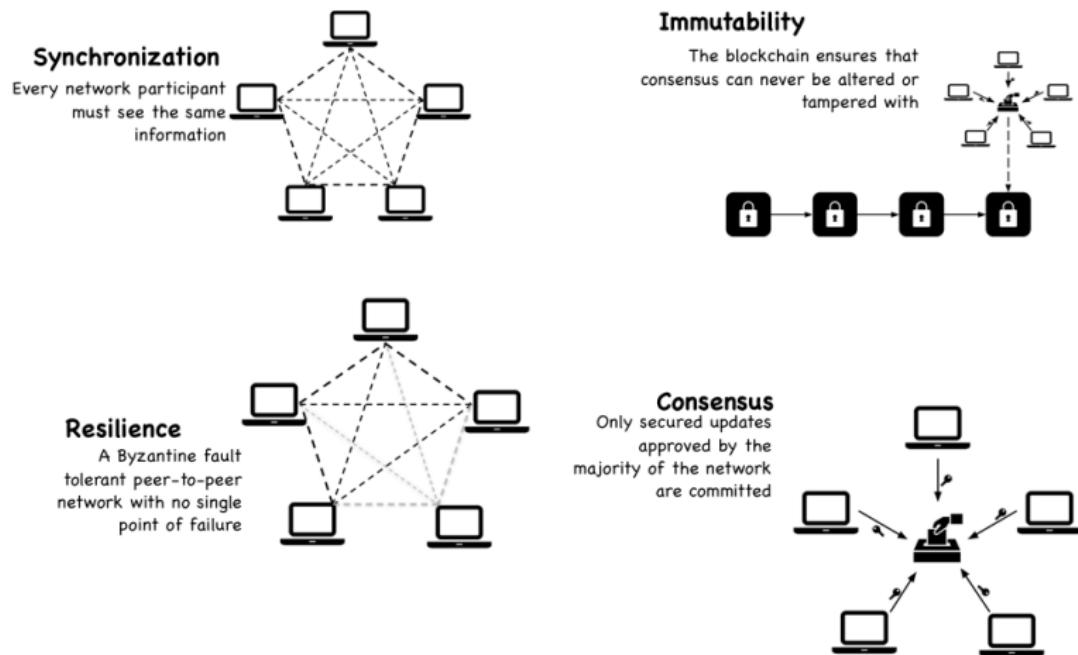


Figure: A basic consensus model

Cryptocurrency

- A cryptocurrency is a form of digital cash issued on a blockchain platform
- Bitcoin was the first cryptocurrency launched in 2009 and since then well over 1600 other cryptocurrencies have emerged
- Generally no two cryptocurrencies are alike as they all leverage blockchains in unique ways
- Some blockchain platforms allow users to issue their own cryptocurrency through the use of smart contracts
- Cryptocurrencies were designed with the intention of not having to require sovereign backing, however multiple central banks are looking to leverage the benefits of blockchains by developing their own digital currencies

Currency

Currency is a generally accepted form of money that is accepted within an economy

A sovereign state retains the right to decide which currency it shall use, therefore a currency will have limited boundaries of acceptance

Modern financial systems evolved and have come to use fiat money

This is a currency without intrinsic value, established as money by government regulation or law. It was introduced as an alternative to commodity money i.e. money created from precious metal such as gold or silver and hence intrinsically valuable

Cryptocurrency

A decentralized digital currency that uses cryptography to regulate the issuing of new units of the currency, to verify transactions and ownership of the currency and maintain the security of the system independent of a central authority



Cryptocurrency

"Digital tokens like bitcoin, ethereum that are stateless, do not have sovereign endorsement, a qualified issuing body or a country's trust, are not legal currencies and should not be spoken of as digital currencies"- *Li Lihui, former president of the Bank of China*

Cryptocurrency

- As of June 2018 there were 1640 cryptocurrencies available online
- The combined value of all digital currencies stood at \$17.5bn at the start of 2017 and reached an all time high of \$150bn in August of the same year
- Prior to the existence of cryptocurrencies, peer-to-peer exchange was restricted to physical forms of money

Cryptocurrency

Typically, the main features of a cryptocurrency are

- ① Has no intrinsic value that is redeemable for another commodity or asset of value
- ② Has no physical form and exists only on the network
- ③ Supply is not determined by a central issuing authority and the network is completely decentralized

Cryptocurrency



Cryptocurrency



Fiat currency

Created by computers	Issued by governments
Limited supply determined by source code	Unlimited supply and can be produced by the government when necessary
Represented by pieces of code	Form of coins or paper money
Decentralized and not controlled by any entity	Centralized and controlled by government
Value is determined by market demand	Value is determined by markets and regulations

Cryptocurrency

Some, but not all of the features of a cryptocurrency are also common to other forms of money

- Cash is peer-to-peer, but it is not electronic, and it is the liability of a central bank
- Commercial bank deposits are a liability of the bank that issues them and exchanged in a centralized manner either across the books of a given bank or between different banks via the central bank
- Commodity money may also be transferred in a peer-to-peer fashion but it is neither the liability of anyone nor electronic

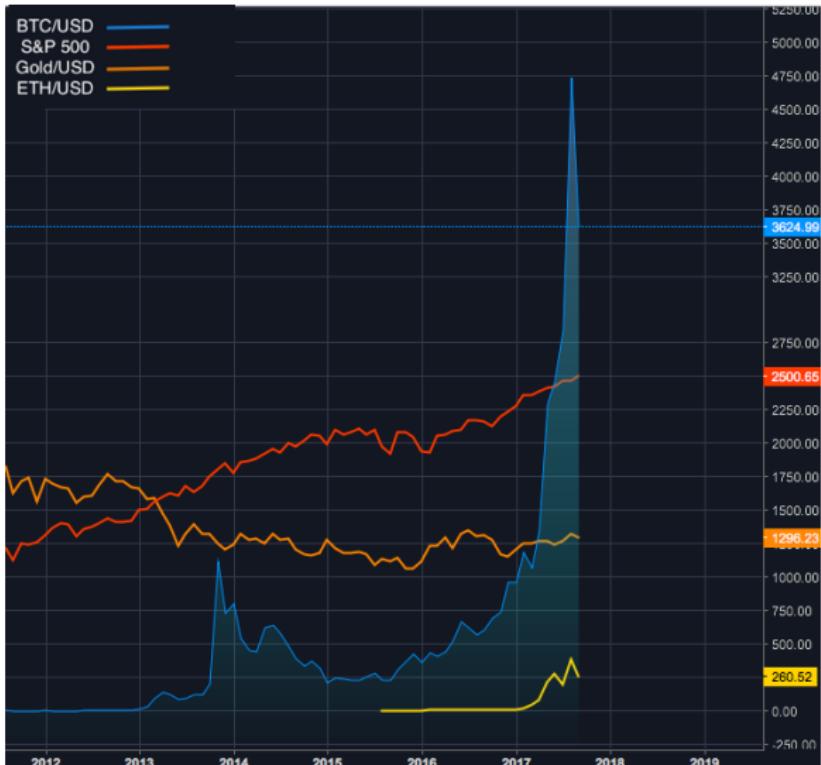
Cryptocurrency

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	\$128,225,430,991	\$7,512.82	\$4,957,270,000	17,067,550 BTC
2	Ethereum	\$57,548,475,718	\$576.67	\$1,991,830,000	99,795,160 ETH
3	Ripple	\$23,940,642,128	\$0.610887	\$265,439,000	39,189,968,239 XRP *
4	Bitcoin Cash	\$17,030,126,404	\$992.49	\$636,842,000	17,159,025 BCH
5	EOS	\$10,863,022,973	\$12.15	\$1,127,070,000	893,995,027 EOS *
6	Litecoin	\$6,723,145,997	\$118.40	\$293,549,000	56,782,848 LTC
7	Cardano	\$5,679,947,051	\$0.219074	\$191,641,000	25,927,070,538 ADA *
8	Stellar	\$5,416,930,235	\$0.291560	\$80,491,800	18,579,126,887 XLM *
9	IOTA	\$4,896,781,885	\$1.76	\$124,831,000	2,779,530,283 MIOTA *
10	TRON	\$3,881,735,637	\$0.059040	\$267,858,000	65,748,111,645 TRX *

*not mineable

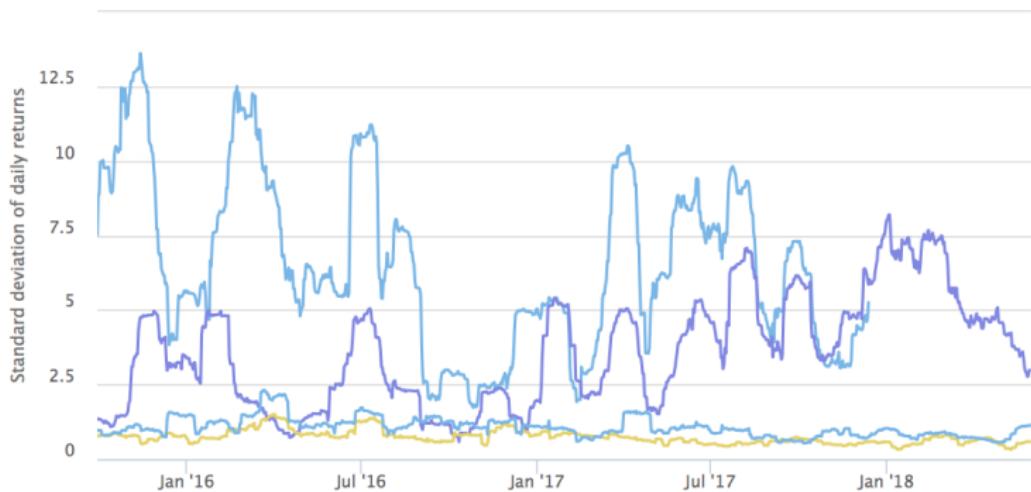
as at 1 June 2018

Cryptocurrency



source <https://www.tradingview.com>

Cryptocurrency



source <https://www.buybitcoinworldwide.com/ethereum-volatility/>

Cryptocurrency

Unlike conventional currencies, there is no issuing authority to regulate the supply in circulation

This lack of regulation is the main reason why the People's Bank of China has explicitly stated discontentment with cryptocurrencies on multiple occasions

In September 2017, Chinese authorities ordered Beijing-based cryptocurrency exchanges to stop trading and immediately notify users of their closure, in an attempt to contain financial risks

Authorities cited concerns about illegal fund flows and limiting risks to consumers amid a highly speculative market that has grown rapidly

Cryptocurrency

New units are typically issued in a deterministic way as currencies are either mined or pre-mined

- In the case of mined currencies, new units are created in the form of block rewards with the creation of new blocks e.g. Bitcoin, Ethereum, Litecoin
- 'pre-mined' currencies will have a fixed supply from the inception of the blockchain and all the available coin will be active and readily available e.g. Ripple
- Most currencies are pre-mined to ensure that developers and founders keep a major share in their project

Bitcoin (BTC), Ethereum (ETH) and Ripple (XRP) are the most relevant platforms in terms of their potential contribution to the financial services industry



Bitcoin



source

<https://disruptdecentralisedisintermediate.files.wordpress.com/2015/04/dilbert.png?w=700&h=222>

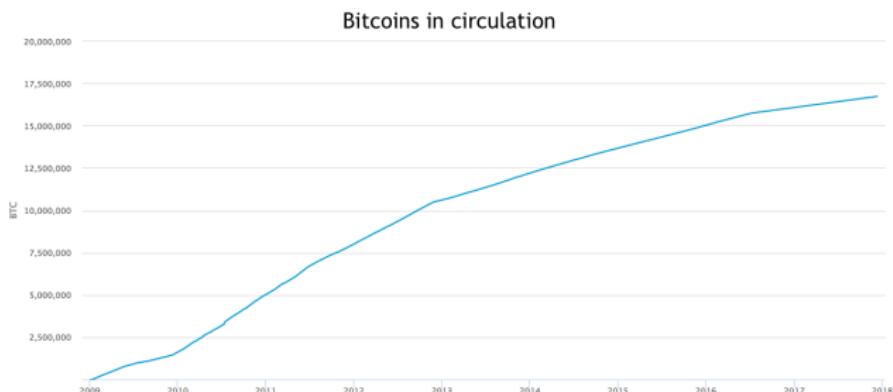
Bitcoin

- Introduced by Nakamoto in 2008 as a decentralized peer-to-peer electronic cash system
- The first viable, decentralized, reliable form of digital cash. Previous attempts include:
 - e-cash, an anonymous cryptographic electronic cash system conceived by David Chaum in 1983
 - B-money, an early proposal created by Wei Dai for an "anonymous, distributed electronic cash system" in 1998. Nakamoto referenced b-money when creating Bitcoin
 - At the same time, Nick Szabo introduced BitGold, also based on the PoW mechanism
- Operates on a public blockchain with over 10000 functioning nodes worldwide

Bitcoin

- Bitcoin can be defined in various ways; it is a protocol, a digital currency and a platform
- Supply of the currency is controlled and limited to 21million BTC. By June 2018, over 17 million Bitcoins were in circulation
- The smallest unit of measurement is a satoshi (10^{-8} BTC)
- The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks(\approx 4 years)
- It is estimated that by 2140, there will be no more Bitcoin left to mine and at that point, miners will only be incentivised by transaction fees
- Approximately 1800 Bitcoins are mined every day

Bitcoin supply



source: <https://blockchain.info/charts/total-bitcoins?timespan=all>

Bitcoin

To date, there is no clear regulatory stance on whether Bitcoin should be classified as investment or as a currency

Nonetheless, many vendors and merchants already accept it as a form of payment

- In May 2010, a developer bought two pizzas using 10,000BTC worth \$41 at the time. Today the pizzas are worth more than \$31million
- Microsoft allows users to buy content with on Xbox and Windows store
- Tesla also accepts bitcoin as a method of payment

Bitcoin

Author Topic: Pizza for bitcoins? (Read 653123 times)

laszlo
Full Member

Activity: 199

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHR1Bx3yDxeMvBRh45aUet

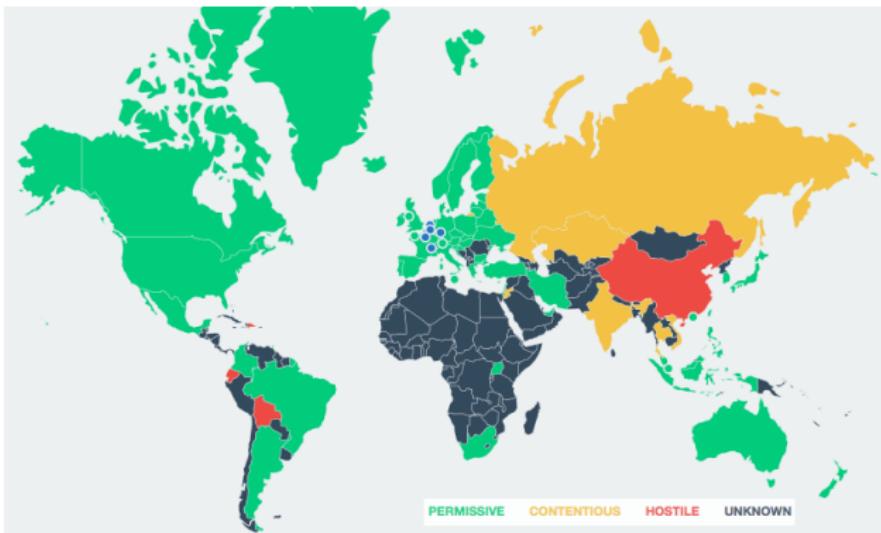
Bitcoin

bitcoin2paysafe Newbie 	 Re: Pizza for bitcoins? May 18, 2010, 06:42:11 PM	#2
In which country do you live?		
Activity: 12 	 Re: Pizza for bitcoins? May 18, 2010, 06:46:48 PM	#3
Jacksonville, Florida zip code 32224 United States		
Activity: 199 	 BC: 157fRrqAKrDyGHR1Bx3yDxeMv8Rh45aUet	
ender_x Newbie 	 Re: Pizza for bitcoins? May 18, 2010, 07:01:50 PM	#4
Activity: 10 	10,000... Thats quite a bit.. you could sell those on https://www.bitcoinmarket.com/ for \$41USD right now.. good luck on getting your free pizza.	

Bitcoin

- Underpinning the security of the network is a the Proof of Work consensus mechanism
- Miners operating full nodes update the system and are incentivised to by being offered Bitcoin as a reward for their work
- The use of Bitcoin has extended beyond trading and investment to being used as a channel for low cost global remittances
- Currently, Asia has the biggest market for cryptocurrency remittances with Bitcoin handling about 20% of the remittances being made to the Philippines from South Korea
- In Venezuela, Bitcoin has become the leading parallel currency as people use it to conduct every day transactions

Bitcoin legality



source: <http://bitlegal.io>

Block difficulty

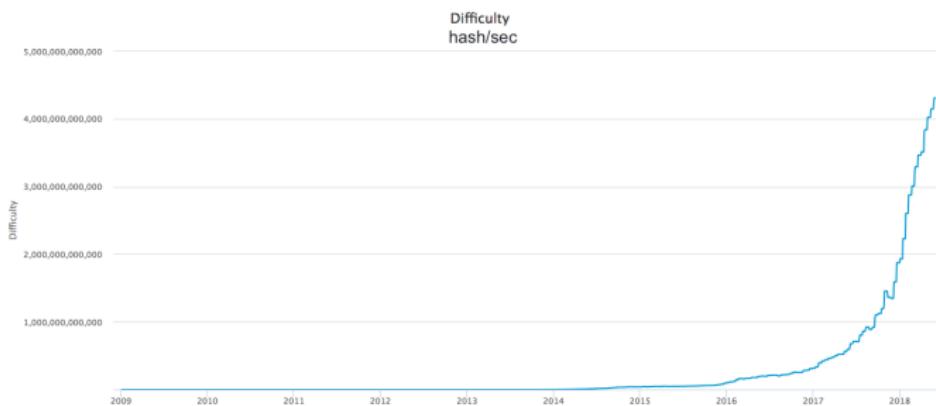
Bitcoin uses the Hashcash cost-function to determine the difficulty of updating the blockchain

Miners hope to recoup the costs imposed by hashcash by winning the block reward for cooperation

Hashcash is fundamentally a way to publicly prove that sufficient energy was spent on finding an arbitrary solution (i.e. finding a valid nonce), using a hashing algorithm

- Block difficulty adjusts with the computing power (network hashrate measured in GH/sec) of the nodes participating in the mining process
- The difficulty is controlled by fixing the number of zeros the proof-of-work nonce is required to start with
- The hash target value is updated every 2016 blocks (\approx 2 weeks) so that blocks get generated once every 10 minutes on average.

Bitcoin difficulty



source: <https://blockchain.info/charts/difficulty?timespan=2years>

Bitcoin ownership

- Because Bitcoin operates on a public blockchain, anyone with access to a functioning node can access the information stored on the network and map out transaction histories
- A coin can be represented as a series of transactions between successive owners such that only the current owner can "spend" it by digitally signing the next transaction
- This way, anyone can verify who the coin currently belongs to. However, pseudonymous identities still protect the privacy of the owners

Bitcoin ownership

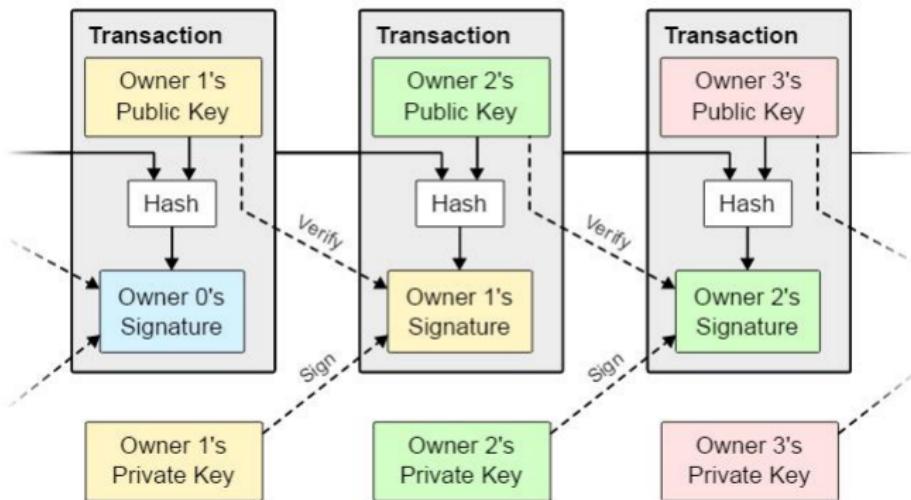


Figure: The chain of ownership of a bitcoin

Bitcoin bubble?

- In 2017 alone, the price of Bitcoin went up nearly five times compared to its value at the beginning of the year
- Much of its growth has been due to the network effect i.e. the more users the network has, the more valuable it becomes
- On a percent change basis, Bitcoin's surge in 2017 surpassed that of any major stock market bubble
- However, the market capitalization of all cryptocurrencies combined is still less than 5% of the market capitalization of all stocks that made up the dot com bubble, which summed up to an inflation adjusted value of \$4 trillion

Bitcoin bubble?



source: The Wall Street Journal

Criticism

Are cryptocurrencies really democratized?

- 2013 Bitcoin fork
 - Versions 0.7 and 0.8 of the software diverged from each other in behavior due to a bug, causing the blockchain to fork into two
 - Mining is a coordination game, therefore it was essential for consensus to be reached on which chain to continue mining
 - In the end the decision was made by a few individuals in the developers chat-room and the BTC Guild mining pool operator was able to single handedly roll back the software by tilting the majority hash power
 - This contradicts the idea of decentralization and distributing power among thousands of small independent miners; and is hence serious threat to the security and integrity of the system

2013 Bitcoin fork

```
23:06 Luke Dashjr      so??? yay accidental hardfork? :x  
23:06 Jouke Hofman    Holy crap
```

Five minutes later the first measure to mitigate the damage is taken by Mark Karpeles, founder of Mt. Gox

```
23:11 Mark Karpeles   I've disabled the import of bitcoin blocks for now  
                      until this is sorted out  
23:13 Luke Dashjr     I'm trying to contact poolops [mining pool operators]
```

2013 Bitcoin fork

Developers start to debate about the appropriate action and come to the conclusion that a downgrade is the pragmatic choice

```
23:23 Gavin Andresen      first rule of bitcoin: majority hashpower wins
23:23 Luke Dashjr        if we go with 0.8, we are hardforking
23:23 Pieter Wuille       the forking action is a too large block
                           if we ask miners to switch temporarily to smaller blocks again,
                           we should get to a single chain soon
                           with a majority of miners on small blocks, there is no risk
23:24 Luke Dashjr        so it's either 1) lose 6 blocks, or 2) hardfork for no benefit
23:25 BTC Guild           We'll lose more than 6

23:25 Pieter Wuille       all old miners will stick to their own chain
                           regardless of the mining power behind the other
23:25 Luke Dashjr         and the sooner we decide on #1, the fewer it loses
23:26 Pieter Wuille       even with 90% of mining power on 0.8
                           all merchants on an old client will be vulnerable
23:26 Luke Dashjr         if we hardfork, all Bitcoin service providers have an emergency situation
23:30 Pieter Wuille       and we _cannot_ get every bitcoin user in the world
                           to now instantly switch to 0.8
                           so no, we need to rollback to the 0.7 chain
```

2013 Bitcoin fork

At this point the hashpower is 2/3 vs 1/3 in favor of the 0.8 branch, with no clear way how to end the fork. Then the BTC guild operator offers to end it

23:43 BTC Guild	I can single handedly put 0.7 back to the majority hash power I just need confirmation that that's what should be done
23:44 Pieter Wuille	BTC Guild: imho, that is what you should do, but we should have consensus first

BTC Guild controlled somewhere between 20% and 30% of total hash power, which made coordinating the downgrade feasible

Consensus is eventually reached and the downgrade happens

Source: <http://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork>

Criticism - Scalability

- The scalability problem is a consequence of the fact that blocks are limited to one megabyte in size
- This is widely regarded as the single most important problem that could mean the difference between blockchains being widely adapted or being limited to small scale use only by niche markets and private consortiums
- The general approaches to tackling this problem can be divided into two categories
 - On-chain solutions - revolve around protocol level enhancements e.g. increasing the block size
 - Off chain solutions - make use of network and processing resources off-chain in order to increase efficiency of the blockchain e.g. state channels

Block size increase

- The current block size limit restricts the network to a rate of about 3-7 transactions per second (tps)
- The limit has created a bottleneck in bitcoin, resulting in increasing transaction fees and delayed processing of transactions that cannot fit into a block
- This has also been a major inhibiting factor in the adaptation of the bitcoin blockchain for processing micro-transactions
- In comparison, on average VISA handles around 2000tps

Block size increase

While a 1MB hard limit remains in place, miners aren't obliged to fill blocks all the way up; The standard bitcoin client has a default setting of around 732KB

Increasing the block size has implications for hardware and bandwidth requirements that cannot be overlooked

- Storage requirement for full nodes will increase significantly; As of June 2018 the size of the entire blockchain was in excess of 160GB and will continue to grow
- Mining on desktops is no longer feasible, a task now left to specialized nodes, thereby further contributing to the problem of centralized mining

Block size increase

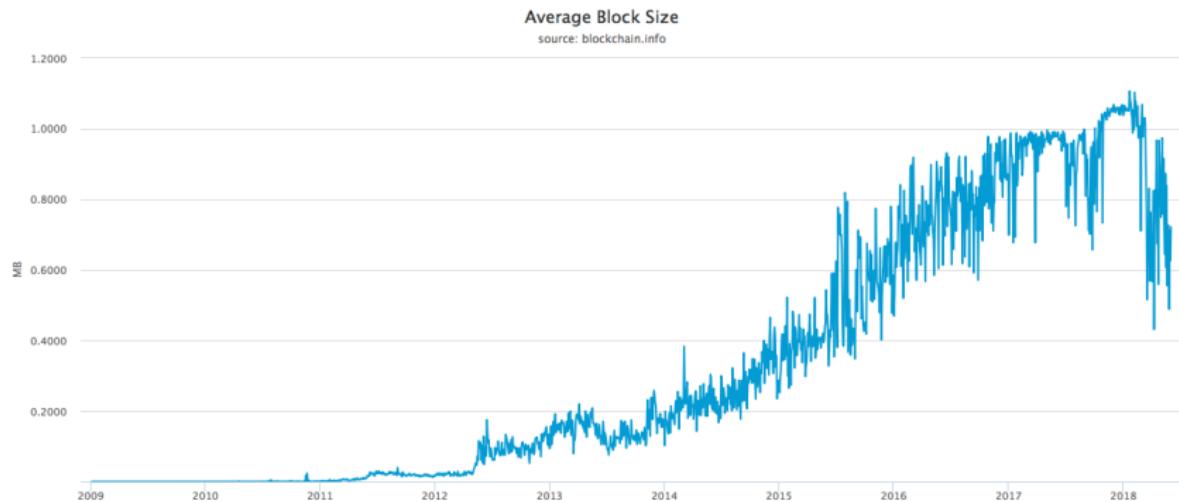


Figure: Average Bitcoin block size

Block size increase

Larger blocks will improve throughput and reduce transaction confirmation times

This prevents the network from being overloaded with data in which case some transactions could be severely delayed or even rejected altogether

Transaction fees, which are fundamentally a bid to purchase block space, are also likely to decrease as the supply of block space increases

The argument for larger blocks is not necessarily out of benevolence as larger blocks means that miners are able to collect more transaction fees

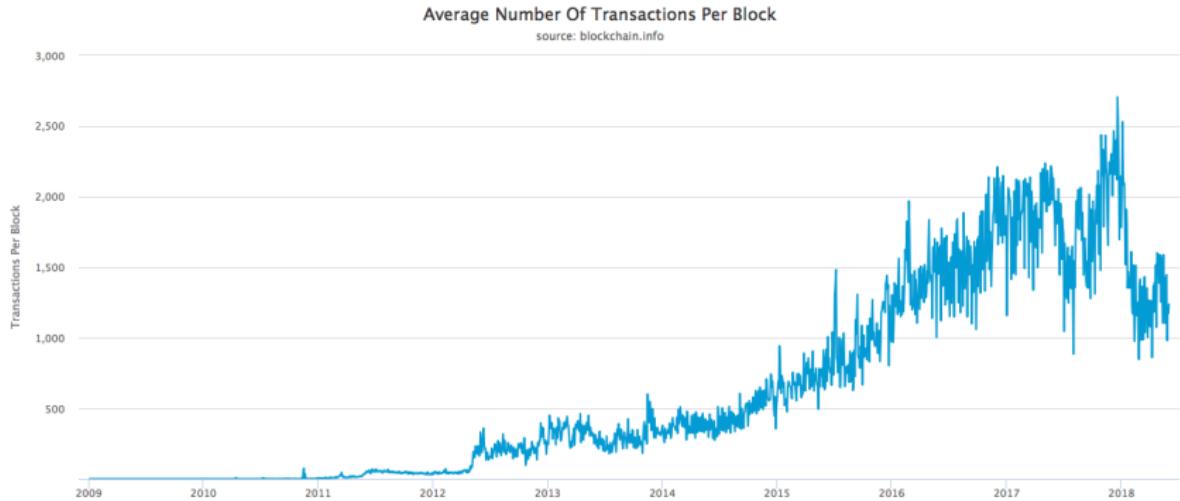


Figure: Average number of transactions per block

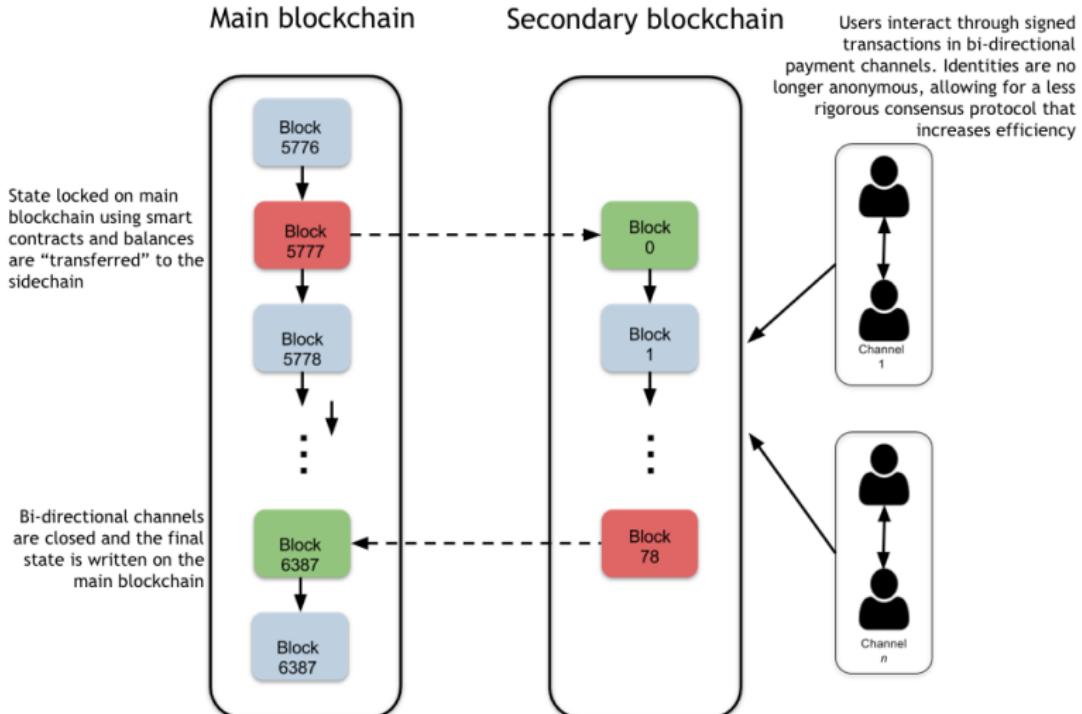
Sidechains

- A sidechain is a blockchain that runs parallel to the main bitcoin network, and allows transfer of value between them
- Two types of sidechains exist; a one-way pegged sidechain allows for coins to be sent only from the main chain to the side chain, whereas a two-way pegged sidechain allows for movement back and forth between the main chain and side chain
- There is no real transfer of coin between chains. The idea revolves around the concept of locking the same amount and value of coins on the main chain and unlocking the equivalent amount of tokens on the secondary chain

Sidechains

- They can improve scalability indirectly by allowing multiple sidechains to run along with the main blockchain, thereby reducing the load on the latter
- This implementation eliminates the need for major protocol changes or block size increase and can significantly increase transaction throughput
- Furthermore, sidechain protocols are easier to modify to allow for faster transaction confirmation times

Sidechains



State channels

- The fundamental idea behind state channels is to use off-chain channels for state updating and processing in order to offload time consuming operations from the main chain.
- State channels work by performing the following steps
 - ① A part of the blockchain state is locked under a smart contract, ensuring the agreement and business logic between participants
 - ② Off-chain transaction processing and interaction is started between the participants that update the state only between themselves. In this step, infinitely many transactions can be performed without requiring the blockchain for execution. All transactions have to be signed, in order to be valid
 - ③ Once the final state is achieved, the channel is closed and the final state is written back to the main blockchain

State channels

State channels have been implemented in bitcoin's Lightning Network and Ethereum's Raiden

- The Lightning Network is a proposed implementation of Hashed Timelock Contracts (HTLCs) with bi-directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels
- Parties are able to maintain a balance between themselves by exchanging valid signed transactions and the balance will be settled on the main blockchain via a final signed transaction
- Raiden was inspired by and for the most part functions like the Lightning network; the major difference being that Raiden is designed to also facilitate the transfer of any type of digital token and not just cryptocurrency

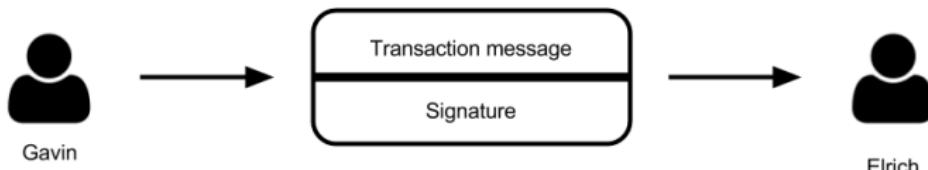
SegWit

SegWit refers to a change in the transaction format of bitcoin to increase the block size limit

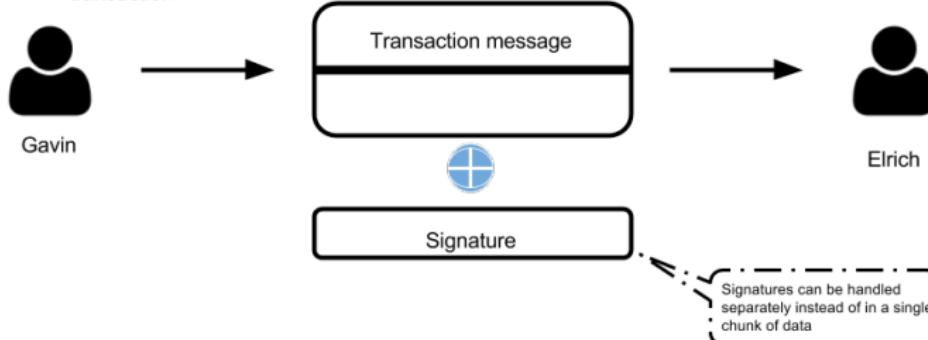
- The protocol achieves this by splitting the transaction into two segments
- Digital signatures are segregated from the transactions data, and are instead appended as a separate structure at a later stage
- This frees up space to include more transactions into a block as a digital signature accounts for 65% of the space in a given transaction
- The block size remains the same, but it can contain data more efficiently
- The original section will still contain the sender and receiver data, while the new 'witness' segment would now contain the scripts (signatures and the public key of sender)

SegWit

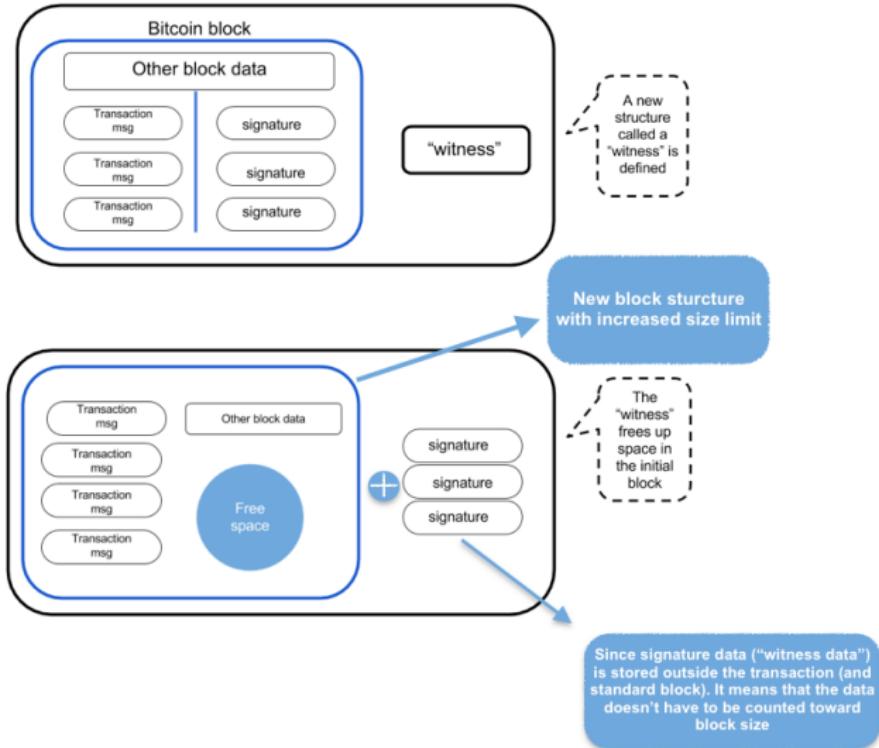
This is what a normal transaction looks like



SegWit separates the signature from the transaction



SegWit



SegWit2x

SegWit2x is an alternative proposal to address the network performance limitations

- Just like SegWit, this protocol segregates the witness data, but in addition to this, block size limit increases from 1 MB to 8 MB allowing for significantly greater transaction rates
- SegWit2x will be a hard fork, meaning it will not be compatible with previous blocks; a hard fork is a permanent divergence from the previous/existing blockchain
- SegWit2x does have the support of a significant number of high-profile businesses and individuals attached to Bitcoin, although the Bitcoin Core team itself does not endorse the proposal
- It is considered as a move towards ensuring bitcoin remains viable as transactional currency and not just as an investment

Bitcoin Cash

On 1 Aug 2017, bitcoin split into bitcoin and bitcoin cash, an alternative version supported by only a few developers

This was a hard fork in the blockchain after block # 478558 that happened after some developers were not satisfied with the implementation of SegWit, stating that it alone is not sufficient to address the scalability issue

97% of the bitcoin miners voted in favor of SegWit and the rest opted to adopt SegWit2x, hence the fork

Bitcoin Cash an is referred to as an "altcoin," a term that usually denotes a fork of the software that creates a new cryptocurrency, with its own market.

Criticism - Mining pools

Because mining is a coordination game, it is often beneficial for miners to pool their resources into 'mining pools'

- This contributes to the problem of centralized mining, which undermines the security of the blockchain
- The 2013 fork showed us what the implications of concentrated hashpower are
- This puts the network at risk of a 51% attack; an attack that occurs when a group of miners controls more than 50% of the network's computing power
- The attackers would be able to prevent new transactions from being confirmed/mined , allowing them to halt payments between some or all users or even reverse transactions
- Mining hardware is becoming more specialized and costly and hence inadvertently contributing to the problem
- Running a mining node on a desktop is no longer economically feasible, hence mining is gradually being left to a minute group of nodes in comparison to the rest of the network

Criticism - Mining pools

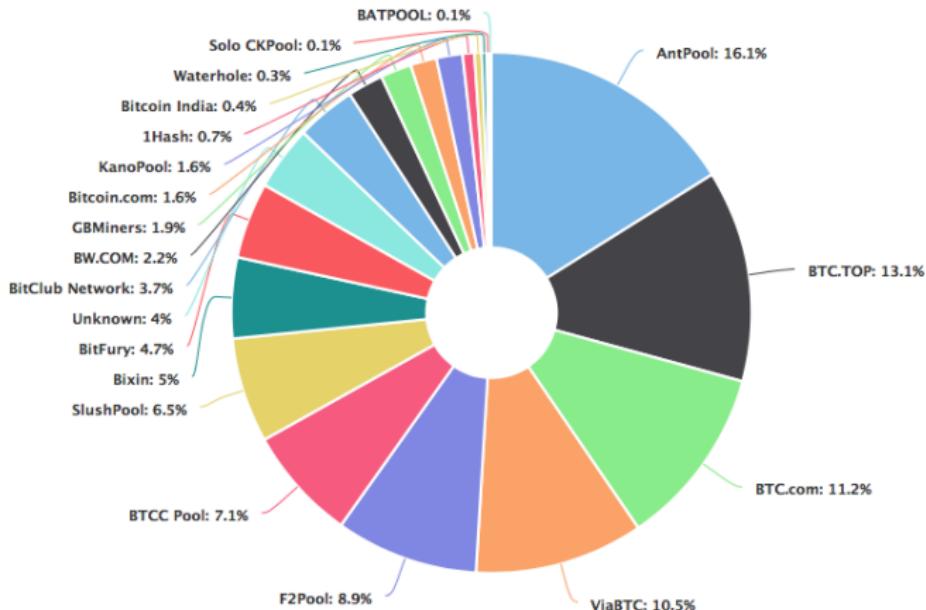


Figure: Bitcoin mining pools by block contribution

source: <https://blockchain.info/pools?timespan=4days>

Criticism - Proof of Work

By design, Proof of Work is resource intensive to deter malicious activity

- PoW powered blockchains accounted for more than 90% of the total market capitalization of existing digital currencies
- Bitcoin alone has been calculated to consume electricity comparable to Ireland's power consumption
- There have been suggestions to make PoW perform useful functions (e.g. finding prime numbers or computing gene sequences for cancer research)

Energy consumption

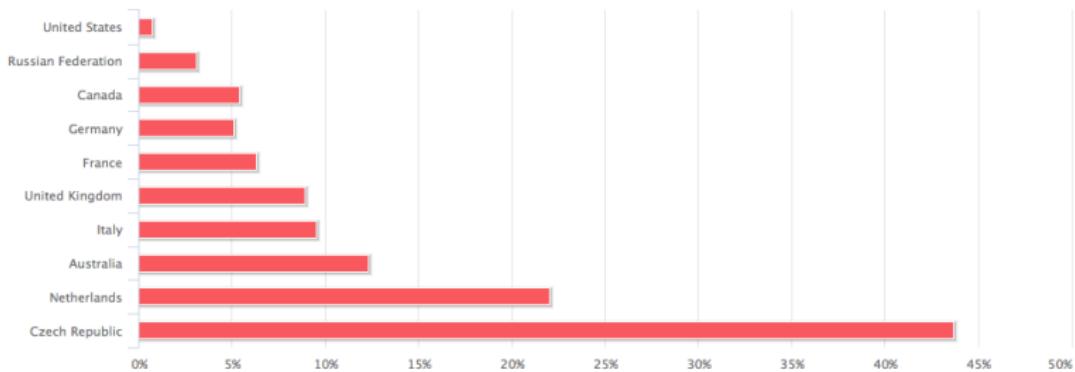


Figure: Bitcoin energy consumption relative to the energy consumption of several countries

source: <https://digiconomist.net/bitcoin-energy-consumption>

Alt-coins



ethereum

Ethereum

Second largest cryptocurrency by market capitalization

Designed to be an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications

Its biggest advantage over the Bitcoin platform is that it comes with a built-in "Turing complete" programming language i.e. you can write programs that can solve any reasonable computational problem given enough resources

The ethereum blockchain has the ability to execute smart contracts i.e. a self executing digital contract (computer code) that can facilitate the exchange of money, content, property, shares, or anything of value

Ethereum

- Around 72 million ETH were created for the crowdsale in July/Aug 2014
- It was decided that post-crowdsale, future ETH generation would be capped at 25% of that initial amount per year
- This means that no more than 18m ETH can be mined per year
- The smallest denomination of ether is a Wei (1e-18 ETH)

Ethereum supply



source: <https://etherscan.io/chart/ethersupplygrowth>

Ethereum supply

Breakdown By Supply Types



- Genesis (72009990.49948 ETH)
- Block Rewards (23657428.4063 ETH)
- Uncle Rewards (1324638.875 ETH)

source: <https://etherscan.io/stat/supply>

Accounts

- There are two types of accounts in Ethereum
- Externally owned accounts
 - Have an ether balance,
 - Can send transactions (ether transfer or trigger contract code)
 - Are controlled by private keys
 - Have no associated code
- Contract accounts
 - Have an ether balance
 - Have associated code
 - Code execution is triggered by transactions or messages (calls) received from other contracts
 - When executed, it can perform operations of arbitrary complexity and call other contracts

Transactions

- Transactions can be divided into two types based on the output they produce; either a message or a new autonomous object
 - Message call transactions - These produce a message call that passes messages from one account to another. Signed messages are transactions created using private keys. Unsigned messages are internal transactions created by contracts using a function call
 - Contract creation transactions - Result in the creation of a new contract with an associated address when executed successfully

Transactions

- Transactions typically contain the following parameters
 - to - this field contains the address of the recipient
 - signature - contains three fields, two representing the digital signature and the third being information that can be used to recover the public key linked to that signature
 - Value - represents the total number of wei to be transferred to the recipient address
 - gasPrice - represents the fee the sender is willing to pay for gas. One unit of gas corresponds to the execution of computational step
 - gasLimit - contains a value that represents the maximum amount of gas that can be used to execute the transaction
 - init - this is only used in transactions intended to create contracts. Specifies the EVM code to be used only once in the account initialization process
 - data - an optional field which can contain a message sent to a contract

Gas

- Gas is the name for the execution fee that senders of transactions need to pay for every operation made on an Ethereum blockchain
- It is paid for in ether to the miners that also determine its price as, they can refuse to process a transaction with a lower gas price than their minimum limit
- Ethereum clients automatically hold back gas in the form of ether, the value of which is defined by the `gasLimit` multiplied by the `gasPrice`

Gas

- Gas and ether are decoupled deliberately in order to stabilize the cost of mining from the volatility of the cryptocurrency
- If the total amount of gas used by the transaction, including any sub-messages that may be triggered, is less than or equal to the gas limit, then the transaction is processed
- If the total gas exceeds the gas limit, then all changes are reverted, but that the transaction is still valid and the fee can be collected by the miner

Transaction cost

- Total transaction costs are based on two factors
 - ① gasUsed - the total gas that is consumed by all the operations executed by the transaction. A spreadsheet is available on Ethereum's github repository detailing the gas cost of each type of possible operation
 - ② gasPrice - the price (in ether) of one unit of gas specified in the transaction

```
transaction= fee gasUsed * gasPrice
```

- If the transaction uses less gas than specified by the limit, the excess gas is reimbursed to the sender as Ether
- It is good practice to use the estimateGas function before execution



Figure: Network transaction fees

source: <https://etherscan.io/chart/transactionfee>

Transaction validation and execution

- In ethereum, each transaction will also contain a nonce
- This is a number that is incremented by one every time a transaction is sent by the sender. It must be equal to the number of transactions sent and is used as a unique identifier for the transaction
- A transaction is successfully executed after it passes the following tests
 - The digital signature used to sign the transaction is valid
 - The transaction nonce must be equal to the sender's current nonce
 - Gas limit must not be less than the gas use by the transaction
 - The sender's balance is sufficient to cover the execution cost

Block validation

- A block is considered valid if it passes the following tests
 - Consistent with uncles and transactions i.e. proposed uncles actually satisfy the property of being an uncle with valid proof of work
 - A valid parent (previous) block exists
 - The block has a valid timestamp less than 15mins after the parent block timestamp
- If any of these checks fail, the block will be rejected

Block difficulty

- Ethereum allows each block to perform a positive or negative adjustment of a factor of at most 1/2048 of the previous difficulty
- In order to calculate the difficulty of the new block using the algorithm below, the following information is required; timestamps of the proposed block and the parent block, the block number and difficulty of the parent block

```
block_diff= parent_diff + parent_diff // 2048 *
            max(1 - (block_timestamp - parent_timestamp) // 10, -99)
            + int(2**((block.number // 100000) - 2))
```

Block difficulty

- If the time difference between the generation of the parent block and the current block is less than 10 seconds, the difficulty goes up.
- If the time difference is between 10 to 19 seconds, the difficulty level remains the same. And if the time difference is 20 seconds or more, the difficulty level decreases proportional to the time difference
- The average number of blocks required to stabilize the difficulty after a drop of 25% is 589 blocks (\approx 2 hours)

Block difficulty

- The last line of the difficulty formula shows the *difficulty time bomb* or *Ice age*
- This is a mechanism built into Ethereum that increases the difficulty exponentially every 100000 blocks
- It was intentionally put in place to encourage users to switch to the proposed Proof-of-Stake scheme (Casper) when mining on the PoW chain becomes prohibitively difficult
- Estimates suggest that increasing block difficulty will eventually make it impossible to mine on the PoW chain in 2021, forcing miners to switch over to Casper

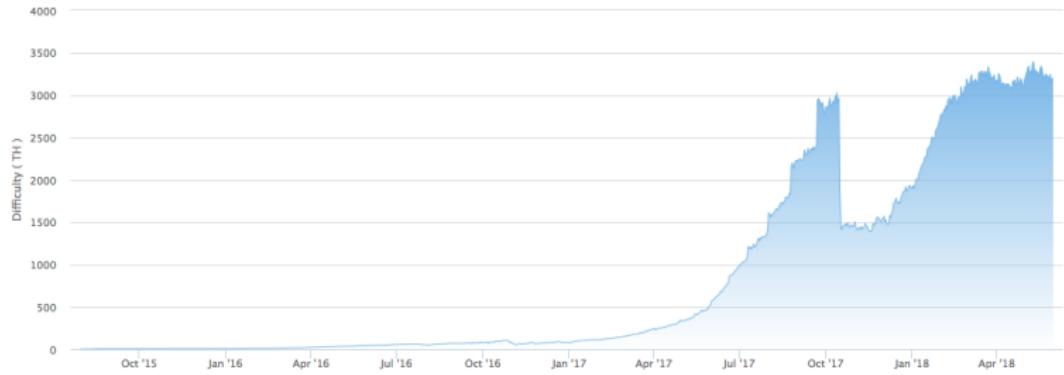


Figure: Ethereum block difficulty growth

source: <https://etherscan.io/chart/difficulty>

Mining

- Ehash is the name of the PoW work algorithm used in Ethereum
- It is a memory-hard algorithm (i.e. uses the most memory possible for a given number of operations), which makes it difficult to be implemented on specialized hardware, unlike Bitcoin where ASICs have been developed
- Computing the PoW requires choosing subsets of a fixed resource called DAG (Directed Acyclic Graph), a data structure that is often used to model a wide variety of computer science problems. It is fundamentally a tree where each node is allowed to have multiple parents
- Mining involves grabbing random slices of the DAG and hashing them together multiple times

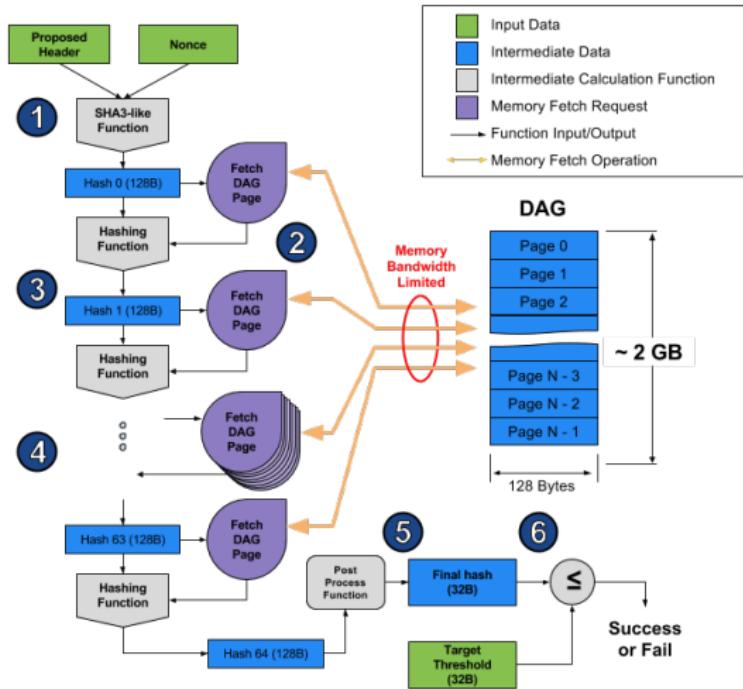
Ethash DAG

- The DAG is a large transient randomly generated dataset created using a version of the Dagger-Hashimoto Algorithm
- It changes after every epoch (30000 blocks \approx 100hrs), however, since it only depends on block height it can be generated prior to the epoch transition
- Because it takes a long time to generate, unless clients actually pre-cache DAGs ahead of time, the network may experience a massive block delay on each epoch transition
- It is currently \approx 2.5 GB in size and will continue to grow linearly with time
- Note that the DAG does not need to be generated for verifying the PoW only to produce it, therefore verifications by nodes with both low CPU speeds and small memory are still feasible
- Geth (ethereum's Go client) implements automatic DAG generation and maintains two DAGs at a time for smooth epoch transitions

Ethash

The flow of the Ethash hashing algorithm can be described as follows

- ① The header of the proposed block and the current nonce are combined using a SHA3-like algorithm to create a initial 128 byte hash
- ② This hash is then used to pseudorandomly pick which section to retrieve from the DAG
- ③ The hash is combined with the retrieved DAG page. This is done using a ethereum-specific hashing function to generate the next hash
- ④ Steps 2 & 3 are repeated 64 times
- ⑤ Hash 64 is post processed, yielding a shorter, 32 byte final hash
- ⑥ The final hash is compared against the predefined 32 byte target threshold. If it is less than or equal to the target threshold, then a valid nonce has been found and the block will be broadcast to the network



source: https://www.vijaypradeep.com/static/media/uploads/ethash_algorithm.png

Mining

- When a mining node starts its operation of verifying blocks, it starts with the highest paying transactions in the transaction pool and executes them one by one
- When the gas limit is reached or no more transactions are left to be processed in the transaction pool, the mining starts

Mining

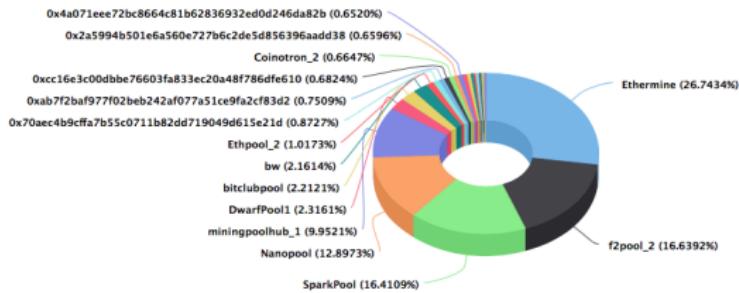


Figure: Top 25 miners by block contribution²

source: <https://etherscan.io/stat/miner/1?range=7&blocktype=blocks>

²as at 04 Jun 2018

Serenity

- Serenity is the name of the next major update for Ethereum that will require a hard fork
- The whole point of Serenity is to increase the flexibility of the platform by changing it into a general purpose decentralized computation platform through abstraction, and the implementation of Casper
- Abstraction will be increased through the ability to swap out consensus protocols, the elimination of external accounts (everything will be a contract account) and the flexibility to use different cryptographic hash functions
- Casper is a modified PoS mechanism that is an adaptation of some of the principles of the GHOST protocol
- The exact timing of this release is unknown as it has been delayed to allow development

Casper

- Casper is a security-deposit based economic consensus protocol
- Nodes will be required to place a security deposit (i.e. "bonding") in order to participate in the consensus process
- If a validator produces anything that Casper considers "invalid", their deposit is forfeited along with the privilege to participate in the consensus process
- This addresses the "nothing at stake" problem of PoS i.e. behaving badly is not expensive

Casper

- A validator's signature is therefore only economically meaningful as long as that validator has a current deposit
- Nodes will maintain a list of currently-bonded validators that will change over time and can be used to authenticate the consensus
- Once a validator has found a valid block, she will bet on it being appended to the chain, using her deposit as stake
- If the block is indeed appended, she will earn her deposit back along with transaction fees proportional to her stake

Casper

- Validators bet independently on blocks at every height by assigning it a probability and publishing it as a bet
- Each validator's incentive is to bet in the way that they expect others to bet in the future, driving the process toward convergence
- When every member of a supermajority of bonded validators bets on a block with a very high probability, the block is final because the fork-choice rule never accepts a fork which block does not win
- These features make Casper suitable for a trustless system by making the platform more Byzantine Fault Tolerant

Casper

Vitalik Buterin, Ethereum's founder, described it with a rough analogy:

- Imagine 100 people sitting around a circular table. One person has a bundle of papers, each with a different transaction history
- The first participant picks up a pen and signs one, then passes it onto the next person, who makes a similar choice
- Each participant only gets \$1 if they sign the transaction history that most of the participants sign in the end
- And if you sign one page and later sign a different page, your house burns down

Ethereum virtual machine

- The Ethereum Virtual Machine (EVM) is designed to serve as a runtime environment for smart contracts
- Not only is it sandboxed, but is actually completely isolated, which means that code running inside the EVM has no access to network, filesystem, or other processes
- Every full node on the network runs its own EVM and uses it to perform code execution locally, for the sake of security and it verifies computation results
- All nodes execute all the transactions that point to smart contracts using the EVM, so every node does the same calculations and stores the same values
- Smart contracts can therefore be tested using the EVM, without affecting the main blockchain operations

Smart Contracts

Fundamentally, smart contracts are

- pre-written logic
- that is stored and replicated on a distributed storage platform
- executed by a network of computers
- and can result in ledger updates

Smart contracts are typically written in Solidity, a high level object orientated language whose syntax is similar to that of JavaScript

They can also be written in LLL, a low level Lisp like language, or Vyper, a high level language designed to be very similar to Python

Just like accounts, smart contracts are able to hold ether

Smart Contracts

The execution of the contract is guaranteed by the blockchain. Once an agreement has been entered into, it cannot be rescinded

Contracts can be designed to function entirely by themselves as legally binding agreements, or in conjunction with already existing traditional contracts

A smart contract can have access to a number of accounts and can transfer assets according to the terms of the contract as soon as an event triggers the application of these terms

If the triggering event happens outside the chain, an 'off-chain event listener' is required

These contracts are able to provide for automatic transactions - such as crediting a dividend or coupon payment, issuing and reacting to margin calls

Using smart contracts

Why are smart contracts useful

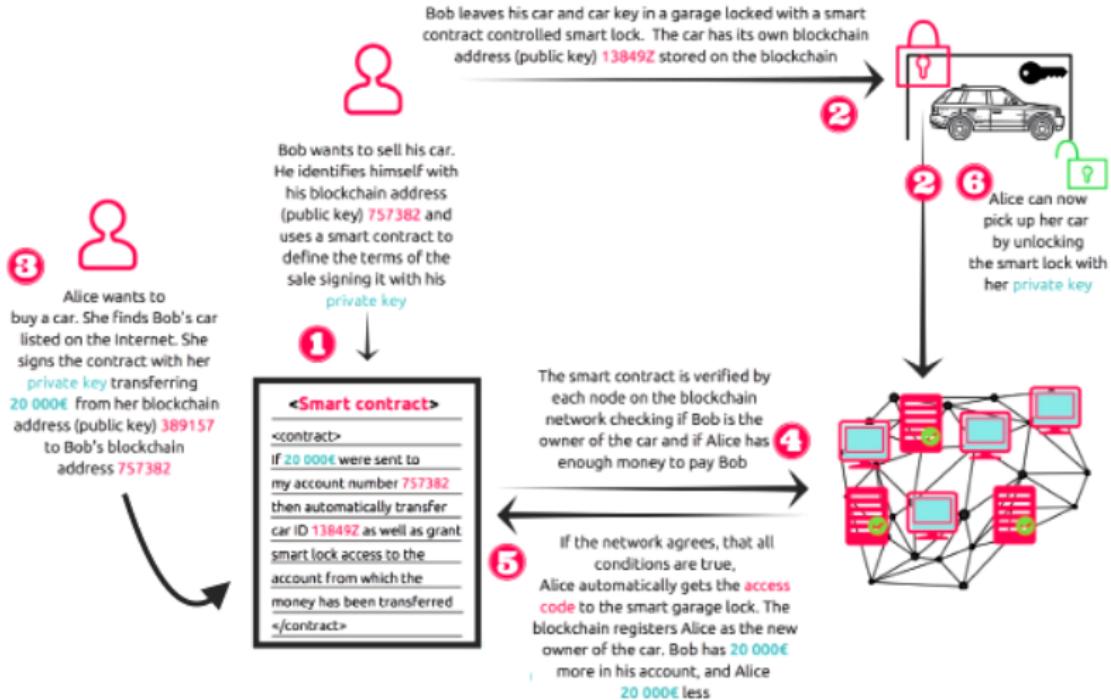
- They inherit the property of a trustless environment from the blockchain, allowing multiple parties to transact, who may not trust each other
- There is only one set of succinct terms of agreement written in computer code, which means there are less points of contention
- Smart contracts provide complete transparency in the context of the agreement
- The contracts can be designed to eliminate counterparty risk and introduce autonomy
- Turing complete contracts have the ability to fulfill any computationally feasible agreement.
- Smart contracts have the ability to decrease the costs of mediation, self-enforcement, and arbitration
- They are designed to run exactly as programmed without any possibility of downtime, censorship, fraud, or third party interface

Using smart contracts

Arguments have been made against using smart contracts in financial markets as lone standing agreements due to their robustness

- Changes in legislation can render an agreement invalid after it has been entered into, the immutability of the contract will inevitably be an issue once execution occurs
- Smart contracts also lose the benefit (or disadvantage) of linguistic nuances that come with the interpretation of the law. Code cannot be ambiguous, therefore conditions of execution have to be explicit
- Smart contracts cannot be renegotiated. This is a concern from a regulatory perspective, as entities may enter into completely legal agreements that may bring about significant systemic risk if executed in times of distress

Hence contracts would be best left to simple functions based on rules that are defined mathematically and enforced mechanically



source: <https://media.blockchainhub.net/wp-content/uploads/2017/08/Smart-Contracts-2.0.jpg>

Smart Contracts

Use cases

- Bank accounts with embedded instructions
 - Some elements of bank accounts already behave like smart contracts
 - Every month debit orders deduct fixed amounts.
 - If there isn't enough money, the payment fails, the account holder is fined and a different work-flow is triggered
 - A smart contract can also do this, the only difference being that the process is no longer controlled by a single central party
 - Smart contract can also increase the flexibility to the account holder
 - Logic that can be run within a normal bank account is limited to recurring payments, and some other basic functionalities
 - However, a Turing complete smart contract can do anything that a normal computer can do e.g. automate a payment from cheque account to savings every day it is sunny, then have it all sent back when there is a storm i.e. a rainy day smart contract

Smart Contracts

Other uses of smart contracts include and are not limited to:

- The pre-contracted resolution of a firm in financial distress
- Managing employment contracts and the automation of payroll systems
- SAFE (Simple Agreement for Future Equity) i.e. an agreement between an investor and a company that provides rights to the investor for equity in the company similar to a warrant, except without determining a specific price per share
- Supply chain management
- Insurance payouts

Smart contract platforms include ChromaWay, OpenLaw and Etherparty



Trade finance: Smart contracts can be set up as escrow accounts that monitor an exchange between two parties. It can track the location of the goods and when ownership has been transferred it can trigger payments.



P2P insurance: Insurance firms can automate the insurance policy by writing it into a smart contract. This technology can enable P2P insurance business models through templated smart contracts.



Loyalty and rewards: E-commerce, retail, and travel & tourism are some of the industries that can create a smart contract-driven loyalty and rewards system stored on a distributed ledger allowing interoperability.



Digital rights management and micropayments: Smart contracts that allow access to digital content such as music, images, and videos with access keys stored on distributed ledgers and also automates micropayments.



Land registry: Store the ownership of land/property on a distributed database and create safeguards for secure updates to this registry when transferring ownership through involvement of government/central body.



Securities issuance: Securities based on payments and rights to be executed according to predefined rules can be written as smart contracts. Current live examples being issuance of smart bonds and private stock markets.



Syndicated loans: Smart contracts can help reduce the settlement time for syndicated loans and help reduce loan issuance time and operational risks.



Event-driven insurance: Connected devices that store data on a distributed ledger help underwrite insurance and automate claims servicing.



Post-trade services: Smart contracts are triggered to ensure regulatory compliance of trades, ensure trade is executed as per the requirements, and take corrective steps as needed.



Distributed smart power grid: Ability for users to generate power and sell it over the grid that enables P2P payments and micro-transactions using smart contracts and distributed ledger.

source: <https://www.everestgrp.com/wp-content/uploads/2016/10/smrt-cntrcts-use-cases.png>

Decentralized Autonomous Organization

- A Decentralized Autonomous Organization (DAO) is an organization with the objective of codifying its rules and decision making apparatuses, eliminating the need for documents and people in governance, creating a structure with decentralized control
- How it works
 - ① Smart contracts that define the organizational structures and the procedures it requires to function are written
 - ② In an initial funding period, people add funds to the DAO by purchasing tokens that have rights attached. These tokens are not meant to represent equity and are only intended to give people voting rights
 - ③ When the funding period is over, the DAO begins to operate
 - ④ People then make proposals to the DAO on how to spend the money, and token holders vote to approve proposals

The DAO

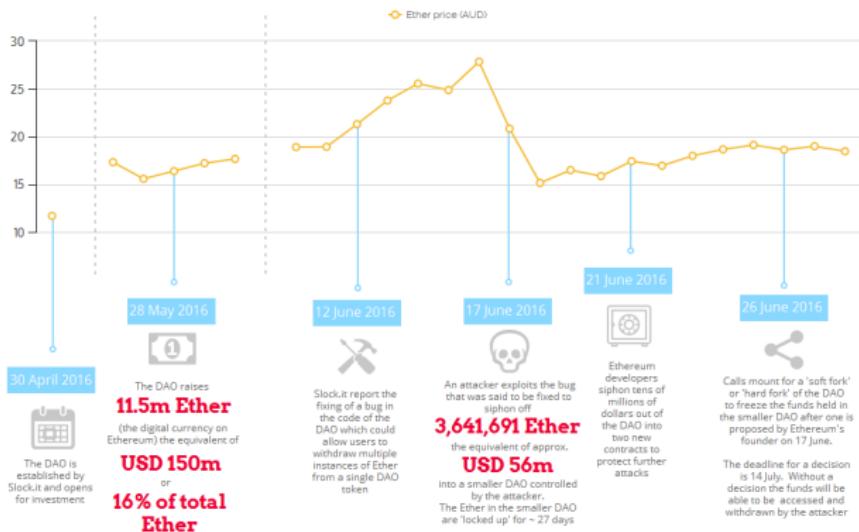
- The DAO was a smart contract on the Ethereum blockchain that operated like a venture fund
- DAO tokens were sold to purchasers in exchange for ether. The DAO was crowdfunded in May 2016, setting the record for the largest crowdfunding campaign in history at the time
- The ether was pooled, and then DAO token holders would vote on investments strategies to be applied portions of the pooled funds
- Token holders would then share in profits from the investments proportional to their holdings

The DAO

- In June 2016, The DAO was hacked and a user gained control of 3.6million Ether ($\approx \$50m$), a third of all funds raised
- All funds sent to the contract were subject to a 28 day holding period, hence they weren't actually gone, allowing The DAO and the Ethereum community to debate on what to do next
- Eventually a decision was made to hard-fork the Ethereum blockchain and restore all funds to the original contract
- The original un-forked blockchain was maintained as Ethereum Classic after some users rejected the hard fork on philosophical grounds, arguing that Ethereum worked exactly as intended and involvement of the Ethereum foundation in The DAO was a mistake

THE DAO ATTACK

times and figures



source: <http://www.kwm.com/media/library/Images/Knowledge/Insights/au/2016/06/30/dao-attack-times-figures-infographic.ashx?w=100%25&la=en>

Issuing a currency

The following contract will implement the simplest form of a cryptocurrency

```
1  pragma solidity ^0.4.20;
2
3  contract AIFMRMCoin {
4
5      address public minter;
6
7      mapping (address => uint) public balances;
8
9      event Transfer(address _from, address _to, uint _amount);
10
11     constructor public() {
12         minter = msg.sender;
13     }
14
15     function mint(address _receiver, uint _amount) external{
16         if (msg.sender != minter) return;
17         balances[_receiver] += amount;
18     }
19
20     function transfer(address _receiver, uint _amount) external{
21         if (balances[msg.sender] < _amount) return;
22         balances[msg.sender] -= _amount;
23         balances[_receiver] += _amount;
24         Transfer(msg.sender, _receiver, _amount);
25     }
26
27 }
```

Issuing a currency

```
1 pragma solidity ^0.4.20;
2
3 contract AIFMRMCoin {
4
5     address public minter;
6
7     mapping (address => uint) public balances;
8
9     event Transfer(address _from, address _to, uint _amount);
10
11    constructor public() {
12        minter = msg.sender;
13    }
14
15    function mint(address _receiver, uint _amount) external{
16        if (msg.sender != minter) return;
17        balances[_receiver] += amount;
18    }
19
20    function transfer(address _receiver, uint _amount) external{
21        if (balances[msg.sender] < _amount) return;
22        balances[msg.sender] -= _amount;
23        balances[_receiver] += _amount;
24        Transfer(msg.sender, _receiver, _amount);
25    }
26}
27}
```

- The first line, `address public minter` declares a state variable `minter` of type `address` that is publicly accessible
- The `address` type is a 160-bit value that does not allow any arithmetic operations. It is suitable for storing addresses of contracts or keypairs belonging to external persons

Issuing a currency

```
1 pragma solidity ^0.4.20;
2
3 contract AIFMRMCoin {
4
5     address public minter;
6
7     mapping (address => uint) public balances;
8
9     event Transfer(address _from, address _to, uint _amount);
10
11    constructor public() {
12        minter = msg.sender;
13    }
14
15    function mint(address _receiver, uint _amount) external{
16        if (msg.sender != minter) return;
17        balances[_receiver] += amount;
18    }
19
20    function transfer(address _receiver, uint _amount) external{
21        if (balances[msg.sender] < _amount) return;
22        balances[msg.sender] -= _amount;
23        balances[_receiver] += _amount;
24        Transfer(msg.sender, _receiver, _amount);
25    }
26}
27}
```

- Line 8, `mapping (address => unit) public balances`, also creates a public state variable, `balances`
- This variable allows addresses to be mapped to unsigned integers
- Using a function, one can easily query the balance of a single account

Issuing a currency

```
1 pragma solidity ^0.4.20;
2
3 contract AIFMMCoin {
4
5     address public minter;
6
7     mapping (address => uint) public balances;
8
9     event Transfer(address _from, address _to, uint _amount);
10
11    constructor public() {
12        minter = msg.sender;
13    }
14
15    function mint(address _receiver, uint _amount) external{
16        if (msg.sender != minter) return;
17        balances[_receiver] += amount;
18    }
19
20    function transfer(address _receiver, uint _amount) external{
21        if (balances[msg.sender] < _amount) return;
22        balances[msg.sender] -= _amount;
23        balances[_receiver] += _amount;
24        Transfer(msg.sender, _receiver, _amount);
25    }
26}
27 }
```

- Line 10, event

Transfer(address _from, address _to, unit _amount)
declares an event, Transfer which is fired by the function transfer

- Events allow the usage of the Ethereum Virtual Machine (EVM) logging facilities
- Each time an event is fired, its input variables _from, _to and _amount are logged
- Any node can easily track transactions by following these events

Issuing a currency

- The first function in the contract, starting in line 12 serves as a constructor
- This is a function that is executed only once when the contract is deployed and has the same name as the contract
- In this contract, the constructor permanently stores the address of the person creating the contract
- `msg` is a global variable that contains some properties which allow access to the blockchain.
- `msg.sender` is always the address where the current (external) function call came from

```
1 pragma solidity ^0.4.20;
2
3 contract AIPMMCoin {
4
5     address public minter;
6
7     mapping (address => uint) public balances;
8
9     event Transfer(address _from, address _to, uint _amount);
10
11    constructor public() {
12        minter = msg.sender;
13    }
14
15    function mint(address _receiver, uint _amount) external{
16        if (_msg.sender != minter) return;
17        balances[_receiver] += amount;
18    }
19
20    function transfer(address _receiver, uint _amount) external{
21        if (balances[_msg.sender] < _amount) return;
22        balances[_msg.sender] -= _amount;
23        balances[_receiver] += _amount;
24        Transfer(_msg.sender, _receiver, _amount);
25    }
26}
27 }
```

Issuing a currency

```
1 pragma solidity ^0.4.20;
2
3 contract AIFMMMCoin {
4
5     address public minter;
6
7     mapping (address => uint) public balances;
8
9     event Transfer(address _from, address _to, uint _amount);
10
11    constructor public() {
12        minter = msg.sender;
13    }
14
15    function mint(address _receiver, uint _amount) external{
16        if (msg.sender != minter) return;
17        balances[_receiver] += amount;
18    }
19
20    function transfer(address _receiver, uint _amount) external{
21        if (balances[msg.sender] < _amount) return;
22        balances[msg.sender] -= _amount;
23        balances[_receiver] += _amount;
24        Transfer(msg.sender, _receiver, _amount);
25    }
26
27 }
```

- The functions that will be ultimately accessible to users and contracts alike are `mint` and `transfer`.
- By default, functions are externally accessible, unless otherwise stated

Issuing a currency

- The `mint` function is used to control the supply of the currency by allowing the creator of the contract to issue new units to any address
- The `if` statement in line 17 ensures that the function can only be executed by the creator of the contract
- The `transfer` function can be used by anyone with a positive balance to send coins to anyone else
- The `if` statement in line 22 ensures that the sender is unable to send an amount greater than their available balance
- Balances of the sender and receiver are updated and the transaction is logged using the `Transfer` event in line 26

```
1 pragma solidity ^0.4.20;
2
3 contract AIFMMCoin {
4
5     address public minter;
6
7     mapping (address => uint) public balances;
8
9     event Transfer(address _from, address _to, uint _amount);
10
11    constructor public() {
12        minter = msg.sender;
13    }
14
15    function mint(address _receiver, uint _amount) external{
16        if (msg.sender != minter) return;
17        balances[_receiver] += amount;
18    }
19
20    function transfer(address _receiver, uint _amount) external{
21        if (balances[msg.sender] < _amount) return;
22        balances[msg.sender] -= _amount;
23        balances[_receiver] += _amount;
24        Transfer(msg.sender, _receiver, _amount);
25    }
26}
27 }
```

Issuing a currency

- The events can be used to create a "blockchain explorer" that tracks transactions and balances of that particular contract
- This is a useful feature, because transactions and balances of coins issued by a contract are only visible within that contract.
- The main blockchain will only show that a contract was created and deployed
- It is possible to create a UI to interact with the functions and query balances

Smart Contract platforms

Other smart contract compatible blockchains include

- Bitcoin: Works well in processing bitcoin transactions but has limited capabilities when processing documents. The scope for processing documents can be improved through the use of sidechains (i.e. blockchains that run parallel to Bitcoin)
- NXT: A public blockchain that contains a selection of smart contract templates. However it is not Turing complete, therefore users are restricted to the templates and cannot code their own contracts
- Hyperledger Fabric: A blockchain framework implementation hosted by The Linux Foundation. Intended as a foundation for developing applications or solutions with a modular architecture. Leverages container technology to host smart contracts called "chaincode"

Setting up an Ethereum client - Ubuntu

1 Install geth

- To run an ethereum node on your machine you will first need to install geth (or parity)
- Geth is the command line interface for running a full node on the ethereum blockchain, written in the go programming language
- Geth supports both binary and scripted installation. The latter is recommended only if you want to modify the source code before installing geth. Binary installation is simpler and straight forward.
- To install from Ubuntu's Personal Package Archives (PPA) (a collection of software not included in Ubuntu by default), run the code below

```
sudo apt-get install software-properties-common  
sudo add-apt-repository -y ppa:ethereum/ethereum  
sudo apt-get update  
sudo apt-get install ethereum
```

Setting up an Ethereum client - macOS

- The recommended way to install geth in macOS is using Homebrew
- Homebrew is a open-source software package management system for macOS
- Once Homebrew has been installed, run the following commands in Terminal to install geth

```
brew tap ethereum/ethereum  
brew install ethereum
```

Setting up an Ethereum client - Windows

- Geth comes in an executable file for Windows available here
- Inside the zip archive you will find the `geth.exe` file, which can be used without installing
- Open a command prompt and change the working directory to the folder to which the `geth.exe` file has been extracted
- to use geth, open the `geth.exe` file

Setting up an Ethereum client

2 Connect to the network

- After geth has been successfully installed, run `geth console`
- This will set up a full node in the JavaScript interactive mode and instantly connect it to the Ethereum main network.
- Make sure to check the different options and commands with `geth --help`
- It is also possible to set up a custom network of nodes that are not connected to the main network nodes

Setting up an Ethereum client

3 Setting up a custom network

- Connections between nodes are valid only if peers have identical network IDs
- The network ID is used to identify exactly which blockchain your node will be connecting to
- Your network can effectively be isolated by setting this to a non default value. It is recommended that you use the `--networkid` command line option for this
- Its argument is an integer, the main network has ID 1 (the default). Ethereum also has multiple test networks where applications can be deployed and tested before being deployed on the main network. A list is available [here](#)
- So if you supply your own custom network ID which is different than the main network your nodes will not connect to other nodes and form a private network
- e.g. `geth --networkid 12345 console` will run a JavaScript console in the interactive mode

Setting up an Ethereum client

If the private network has been successfully set up, you should see a screen similar to the one below

```
C:\Users\lwakhe\Downloads\ethereum\geth-alltools>geth --networkid 12345 console
I1027 19:42:28.851958 node/config.go:445] Failed to start Ledger hub, disabling: libusb: not found [code -5]
I1027 19:42:28.862966 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\AppData\Roaming\Ethereum\geth\chaindata
I1027 19:42:31.213749 ethdb/database.go:176] closed db:C:\Users\lwakhe\AppData\Roaming\Ethereum\geth\chaindata
I1027 19:42:31.299259 node/node.go:176] instance: Geth/v1.5.9-stable/windows/go1.7.4
I1027 19:42:31.344206 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\AppData\Roaming\Ethereum\geth\chaindata
I1027 19:42:33.685497 eth/backend.go:187] Protocol Versions: [63 62], Network Id: 12345
I1027 19:42:33.694516 eth/backend.go:215] Chain config: {ChainID: 0 Homestead: <nil> DAO: <nil> DAOSupport: false EIP150: <nil> EIP155: <nil> EIP158: <nil>}
I1027 19:42:35.204738 core/blockchain.go:219] Last header: #378184 [82bbe6ef...] TD=1880046981264788259
I1027 19:42:35.212749 core/blockchain.go:220] Last block: #0 [4171d228...] TD=1024
I1027 19:42:35.218757 core/blockchain.go:221] Fast block: #378184 [82bbe6ef...] TD=1880046981264788259
I1027 19:42:45.6151340 p2p/server.go:340] Starting Server
I1027 19:42:39.409124 p2p/discover/udp.go:227] Listening, enode://fb9c19320d44234937c9d81cf2d510b987c318f8dc2e5cc6304ef7abf2885eb5dd708854e32f776e0d12aa0d2200266d3e418
I1027 19:42:39.657365 p2p/server.go:608] Listening on [::]:30303
I1027 19:42:46.044935 node/node.go:341] IPC endpoint opened: \\.\pipe\geth.ipc
Welcome to the Geth JavaScript console!
```

Instance: Geth/v1.5.9-stable/windows/go1.7.4
coinbase: 0xa1c63d3acfc8d9a5d5a4de249e664f0d7cd16f5c9
at block: 0 (Thu, 01 Jan 1970 02:00:00 SAST)
datadir: C:\Users\lwakhe\AppData\Roaming\Ethereum
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

>

Setting up an Ethereum client

- Users are also able to run geth with a custom genesis block from a JSON file by supplying the `--genesis` flag in the command line
- One can use this option to customize the blockchain even more e.g. adjusting mining difficulty or preallocation of ether
- If this option is left unspecified, the default Ethereum genesis block is used, leading up to the most recently published block on the main network
- It is advised that you keep the data directory of your private network separated, so do also specify a custom `--datadir` flag.
- The genesis JSON file should have format shown below. The input parameters are described here

Setting up an Ethereum client

```
{  
    "alloc": {  
        "dbbdb2cbd23b783741e8d7fcf51e459b497e4a6": {  
            "balance": "1606938044258990275541962092341162602522202993782792835301376"  
        },  
        "e6716f9544a56c530d868e4bfbacb172315bdead": {  
            "balance": "1606938044258990275541962092341162602522202993782792835301376"  
        },  
        "..."  
    },  
    "nonce": "0x0000000000000002a",  
    "difficulty": "0x020000",  
    "mixhash": "0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",  
    "coinbase": "0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",  
    "timestamp": "0x00",  
    "parentHash": "0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",  
    "extraData": "0x",  
    "gasLimit": "0x2fefd8"  
}
```

Setting up an Ethereum client

- In order to allocate pre-mined ether, you will need to first create an account
- To create an account, run `geth --datadir path/to/custom/data/folder account new`
- This will prompt you to provide a password that will be used to generate the private and public keys
- The output will be the public address of your newly created account, as shown below

```
C:\Users\Lwakhe\Downloads\Ethereum\geth-alltools>geth --datadir C:\Users\Lwakhe\Downloads\Ethereum\geth-alltools\data account new
[1027 19:55:07.070493 node/config.go:445] Failed to start Ledger hub, disabling: libusb: not found [code -5]
Your new account is locked with a password. Please give a password. Do not forget this password.
Passphrase:
Repeat passphrase:
Address: {d2e8cd46eff93aa27f131975e4fe730283eb32d2}
```

Setting up an Ethereum client

- To allocate ether to your new account, enter its address as the first argument in the "alloc" section of the `genesis.json` file
- Next to `balance` enter value of ether to be allocated, denominated in wei. It is possible to allocate ether to more than one account by creating a comma separated list of the accounts and balances as shown in our `genesis` file
- To create a blockchain that uses your custom genesis block, execute the following command: `geth --datadir path/to/custom/data/folder init genesis.json`
- Future runs of `geth` on this data directory will use the genesis block you have defined

Setting up an Ethereum client

- Running `geth --datadir path/to/custom/data/folder --networkid 12345` console will set up a node on the custom network running in the interactive JavaScript mode

```
C:\Users\lwakhe\Downloads\Ethereum\geth-alltools>geth --datadir C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1 init genesis.json
I1027 19:59:44.557108 node/config.go:445] Failed to start Ledger hub, disabling: libusb: not found [code -5]
I1027 19:59:44.559126 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1\geth\chaindata
I1027 19:59:44.678289 ethdb/database.go:176] closed db:C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1\geth\chaindata
I1027 19:59:44.688302 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1\geth\chaindata
I1027 19:59:44.738455 cmd/geth/chaincmd.go:132] successfully wrote genesis block and/or chain rule set: f331e85d72b26a81c028703b334e5dae2995864ad70c6a224b7698eca6c7e59f

C:\Users\lwakhe\Downloads\Ethereum\geth-alltools>geth --datadir C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1 --networkid 12345 console
I1027 20:01:11.591119 node/config.go:445] Failed to start Ledger hub, disabling: libusb: not found [code -5]
I1027 20:01:11.602299 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1\geth\chaindata
I1027 20:01:11.743982 ethdb/database.go:176] closed db:C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1\geth\chaindata
I1027 20:01:11.757922 node/node.go:176] instance: Geth/v1.5.9-stable/windows/go1.7.4
I1027 20:01:11.763938 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1\geth\chaindata
I1027 20:01:11.865553 eth/db_upgrade.go:346] upgrading db log bloom bins
I1027 20:01:11.878568 eth/db_upgrade.go:354] upgrade completed in 5.0068ms
I1027 20:01:11.877571 eth/backend.go:187] Protocol Versions: [63 62], Network Id: 12345
I1027 20:01:11.885586 eth/backend.go:215] Chain Config: {ChainID: 0 Homestead: <nil> DAO: <nil> DAOSupport: false EIP150: <nil> EIP155: <nil> EIP158: <nil>}
I1027 20:01:11.898081 core/blockchain.go:219] Last header: #0 [f331e85d..] ID:67108864
I1027 20:01:11.905613 core/blockchain.go:220] Last block: #0 [f331e85d..] ID:67108864
I1027 20:01:11.912621 core/blockchain.go:221] Fast block: #0 [f331e85d..] ID:67108864
I1027 20:01:11.922638 p2p/server.go:346] Starting Server
I1027 20:01:14.611762 p2p/discover/udp.go:227] Listening, enode://fe23c84438cdc40b13f2693ba4ee6925da600613f7428cf22e74676f9235c2a976ff8e789d78dec5731233e12aeaca5afbe84c
92bbdf9f64c9da9fa8c5fdea4e@[::]:30303
I1027 20:01:14.631796 p2p/server.go:606] Listening on [::]:30303
I1027 20:01:14.635797 node/node.go:341] IPC endpoint opened: \\.\pipe\geth.ipc
Welcome to the Geth JavaScript console!
```

Instance: Geth/v1.5.9-stable/windows/go1.7.4
coinbase: 0x42400ee3dd212043719e625aa9495b201455b1bbf
at block: 0 (Thu, 01 Jan 1970 02:00:00 SAST)
datadir: C:\Users\lwakhe\Downloads\Ethereum\geth-alltools\data1
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

Setting up an Ethereum client

4 Connecting member nodes

- Nodes can be added via the JavaScript console using `admin.addPeer()`
- This takes in as input the enode URL of the peer node, which can be viewed using `admin.nodeInfo`

```
> admin.nodeInfo.enode
> enode://fe23c84438cdc40b13f2693ba4ee6925da600613f7428cf22e74676f9235c2a976ff8e789d78dec5731233e12aeaca5afbeb4c92b8d9f564c9da9fa8c5fdeade@[::]:30303"
> admin.nodeInfo
{
  enode: "enode://fe23c84438cdc40b13f2693ba4ee6925da600613f7428cf22e74676f9235c2a976ff8e789d78dec5731233e12aeaca5afbeb4c92b8d9f564c9da9fa8c5fdeade@[::]:30303",
  id: "fe23c84438cdc40b13f2693ba4ee6925da600613f7428cf22e74676f9235c2a976ff8e789d78dec5731233e12aeaca5afbeb4c92b8d9f564c9da9fa8c5fdeade",
  ip: "::",
  listenAddr: "[::]:30303",
  name: "Geth/v1.5.9-stable/windows/go1.7.4",
  ports: {
    discovery: 30303,
    listener: 30303
  },
  protocols: {
    eth: {
      difficulty: 67108864,
      genesis: "0xf331e85d72b26a81c028703b334e5dae2995864ad70c6a224b7698eca6c7e59f",
      head: "0x31e85d72b26a81c028703b334e5dae2995864ad70c6a224b7698eca6c7e59f",
      network: 12345
    }
  }
}
```

Setting up an Ethereum client

- The [::] part of the enode url refers to the ipv4 address of the node
- Therefore, to add a peer, run
`admin.addPeer("enode://f4642fa65af50...66f416c0@ipv4:30303")`
- To check if a peer has been successfully added execute
`admin.peers` and this should output a list of all the connected peers along with their details

```
> admin.peers
[{
  caps: ["eth/62", "eth/63", "par/1", "par/2", "pip/1"],
  id: "a7235361cb6587d37460217281f6a786dcf1a5322245a654deb765ae71e4fcfd348a6e0ad82f34b663de79ede07560ed4da85477c857a253ae9ab06542105e23",
  name: "Parity/v1.7.8-stable-d5fcf3b-20171025/x86_64-linux-gnu/rustc1.21.0",
  network: {
    localAddress: "10.0.0.164:53134",
    remoteAddress: "207.154.205.103:30403"
  },
  protocols: {
    eth: "handshake"
  }
}]
```

Setting up an Ethereum client

5 Setting up multiple local nodes

- It is also possible to run multiple ethereum nodes locally on one machine
- In order to set them up, make sure the following flags are supplied in the command line
 - each instance has a separate data directory (`--datadir`)
 - each instance runs on different network and JSON RPC ports (`--port` and `--rpcport`)
 - in case of a cluster the instances must know about each other
 - the ipc endpoint is unique or the ipc interface is disabled (`--ipcpath` or `--ipcdisable`)
 - all nodes must have the same genesis block

Setting up an Ethereum client

- To set up an additional node locally, first set up a genesis block identical to the one of the initial node by executing

```
geth --datadir  
path/to/second/custom/data/folder init  
genesis.json
```

- making use of the flags defined in the previous slide, execute

```
geth --datadir  
path/to/second/custom/data/folder --networkid  
12345 --port 30304 --rpcport 3032 --ipcdisable  
console
```

Setting up an Ethereum client

```
C:\Users\lwakhe\Downloads\Ethereum\geth-alltools>geth --datadir C:\Users\lwakhe\Downloads\Ethereum\Node1\data init genesis.json
I1027 20:39:24.052428 node/config.go:445] Failed to start Ledger hub, disabling: libusb: not found [code -5]
I1027 20:39:24.062880 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\Node1\data\geth\chaindata
I1027 20:39:25.176238 ethdb/database.go:176] closed db:C:\Users\lwakhe\Downloads\Ethereum\Node1\data\geth\chaindata
I1027 20:39:25.185249 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\Node1\data\geth\chaindata
I1027 20:39:25.275383 core/genesis.go:95] Genesis block already in chain. Writing canonical number
I1027 20:39:25.281391 cmd/geth/chaincmd.go:132] successfully wrote genesis block and/or chain rule set: f331e85d72b26a81c028703b334e5dae2995864ad70c6a224b769Beca6c7e59

C:\Users\lwakhe\Downloads\Ethereum\geth-alltools>geth --datadir C:\Users\lwakhe\Downloads\Ethereum\Node1\data --networkid 12345 --port 30304 --rpcport 3032 --ipcdisable
console
I1027 20:40:42.392479 node/config.go:445] Failed to start Ledger hub, disabling: libusb: not found [code -5]
I1027 20:40:42.409494 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\Node1\data\geth\chaindata
I1027 20:40:42.697140 ethdb/database.go:176] closed db:C:\Users\lwakhe\Downloads\Ethereum\Node1\data\geth\chaindata
I1027 20:40:42.820857 node/node.go:176] instance: Geth/v1.5.9-stable/windows/goi.7.4
I1027 20:40:42.827868 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to C:\Users\lwakhe\Downloads\Ethereum\Node1\data\geth\chaindata
I1027 20:40:42.905982 eth/backend.go:187] Protocol Versions: [63 62], Network ID: 12345
I1027 20:40:42.914997 eth/backend.go:215] Chain config: {ChainID: 0 Homestead: <nil> DAO: <nil> DAOSupport: false EIP150: <nil> EIP155: <nil> EIP158: <nil>}
I1027 20:40:42.933024 core/blockchain.go:219] Last header: #0 [f331e85d..] TD:67108864
I1027 20:40:42.940032 core/blockchain.go:220] Last block: #0 [f331e85d..] TD:67108864
I1027 20:40:42.948045 core/blockchain.go:221] Fast block: #0 [f331e85d..] TD:67108864
I1027 20:40:42.957059 p2p/server.go:340] Starting Server
I1027 20:40:51.487253 p2p/discover/udp.go:227] Listening, enode://2d844e2482080a48730961cdeacaf852cc87dc83a1f2e29ee9453b4cb353b47fe42a32400c6e00c00854267f364459c1a988e
0e8511e64195122c4a389zaa6@::]:30304
I1027 20:40:51.505284 p2p/server.go:608] Listening on ::]:30304
Welcome to the Geth JavaScript console!
```



```
Instance: Geth/v1.5.9-stable/windows/goi.7.4
coinbase: 0xb3bed1adee175b502a974adf3450e239776c3d8d1
at block: 0 (Thu, 01 Jan 1970 02:00:00 SAST)
datadir: C:\Users\lwakhe\Downloads\Ethereum\Node1\data
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 rpc:1.0 txpool:1.0 web3:1.0
>
```



Ripple

Also known as the Ripple Transaction Protocol (RTXP) or Ripple protocol

A real-time gross settlement system (RTGS), that also operates as a currency exchange with its native currency known as XRP, and functions as a remittance network

Unlike Bitcoin and its peers, information is tracked using accounts instead of using transactions

It is the fastest (4secs) and most scalable (1000 transactions per second) of the major cryptocurrencies

Used by BBVA in April 2017 to complete first real-time international money transfer between Europe and Mexico

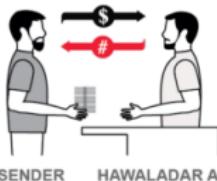
Hawala

The protocol was designed to function like the hawala system

- Hawala is an informal value transfer system based not on the movement of cash but on the performance and honor of a huge network of money brokers
- Payments occur by transfer of debt, which will either be settled in cash later or netted off if there are clients who wish to move money in the opposite direction
- A sender gives agent A the money and receives a passcode. Agent then communicates to agent B the amount received and the passcode. Agent B will release the funds to the recipient only if they can present the passcode
- Agents take the money and a password from the sender, then contact the payee's agent and instruct them to release funds to the person who can provide the password
- This design is what enables Ripple to be a payment system for arbitrary currencies with support for cross-currency transactions

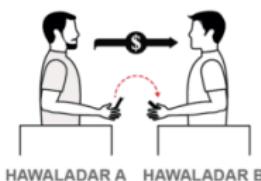
Hawala

STEP 1
In Country A...



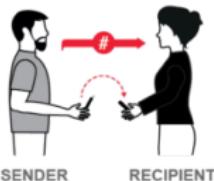
SENDER gives cash to hawala agent (Hawaladar A). Agent gives sender a code.

STEP 2
Hawaladar A to B...



Hawaladar A tells a counterpart in country B how much cash has been received.

STEP 3
Sender to Recipient...



SENDER passes the code to the recipient, saying how much cash was handed in.

STEP 4
In Country B...



Recipient gives code to Hawaladar B who hands over cash, minus fee. Hawala agents settle their account separately.

Sources: Financial Action Task Force (FATF); Interpol

Ripple

- The network is managed by a network of independent validating servers that constantly compare their transaction records
- Relative to other cryptocurrencies, Ripple is significantly centralized as there are network operators and regulators involved
- Currently, much of the network infrastructure is maintained by Ripple with only 55 validator nodes
- The validating process runs asynchronously every few seconds in rounds and the ledger is updated accordingly

Ripple Protocol Consensus Algorithm

- This network contains two types of nodes
 - ① User nodes - can send or receive payments
 - ② Validator nodes - participate in the consensus mechanism
- The blockchain uses a consensus mechanism akin to federated byzantine consensus, the Ripple Protocol Consensus Algorithm (RPCA), where each validator keeps a unique node list (UNL) of trusted validators
- This low latency protocol allows almost real time settlement on the platform

Ripple Protocol Consensus Algorithm

- The validation process is iterative and consensus on a set of transactions is eventually achieved as UNLs will inevitably overlap due to the size of the network
- Transactions that are agreed upon by a "supermajority" of peers are considered validated
- If the supermajority isn't in consensus, "[it] implies that transaction volume was too high or network latency too great for the consensus process to produce consistent proposals," and the consensus process is again attempted by the nodes

Ripple

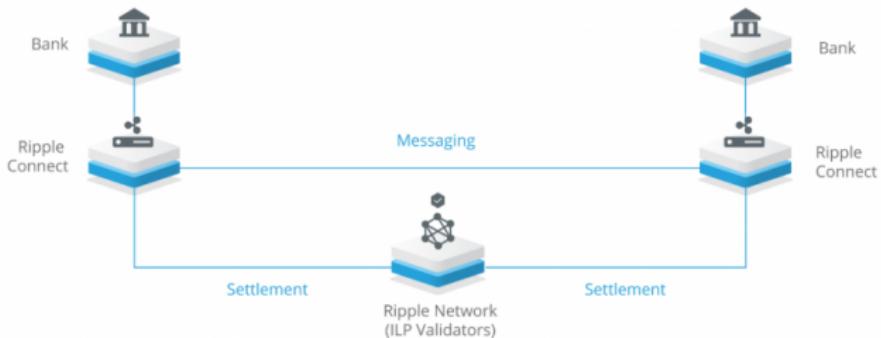
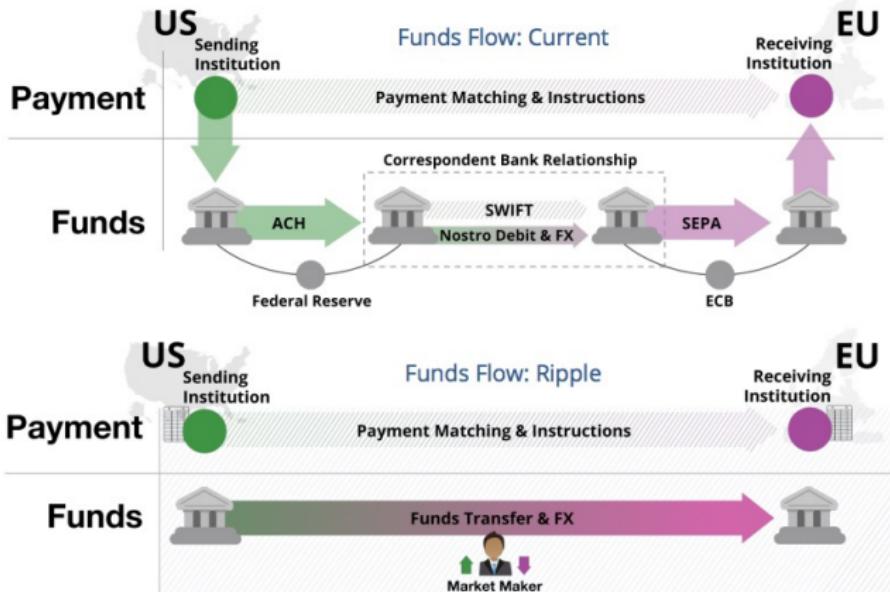


Figure: Ripple network structure

Ripple

- Unlike Bitcoin where transaction fees are optional, Ripple transactions always have an XRP (the native cryptocurrency) cost, which on average is still lower than that of the other cryptocurrencies
- This transaction cost is designed to increase along with the load on the network, making it very expensive to deliberately or inadvertently overload the network
- The transaction fees are not paid to any party. The XRP is irrevocably destroyed by being sent to an unspendable address
- In addition to account balances, the ledger holds information about offers to buy or sell currencies and assets

Ripple



Ripple transactions

- Transactions can be categorized into three types
 - ① Payments related - these are used to send funds to one another. Funds are sent through payment channels and transfers are facilitated by funding and claiming from the unidirectional channels
 - ② Order related - the ripple platform also functions as an exchange for assets and currencies. These transactions are used to create and withdraw limit orders on the ledger
 - ③ Account and security related - these transactions are responsible for modifying the attributes and signing keys of an account. They can also be used to create multi-signature transactions



- IOTA is an IoT blockchain which makes use of Tangle, a new data structure based on a Directed Acyclic Graph (DAG), instead of a conventional blockchain structure with blocks
- IOTA was born from the desire to address the problem that demand driven fees associated with cryptocurrency transactions will become impractical as the demand for micro-payments increases
- Transactions are free regardless of the size of the transaction, confirmation times are fast, the number of transactions the system can handle simultaneously is unlimited, and the system can easily scale
- At inception, a supply of 2,779,530,283,277,761 iota was created, and as there is no mining, no more will be created



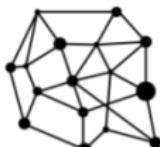
Scalable

Parallelized validation of transactions allows IOTA to achieve high transaction throughput with no limit as to the number of transactions that can be confirmed in a certain interval



No transaction fees

IOTA has no transaction fees



Distributed

IOTA has no miners. Every participant in the network that is making a transaction, actively participates in the consensus.

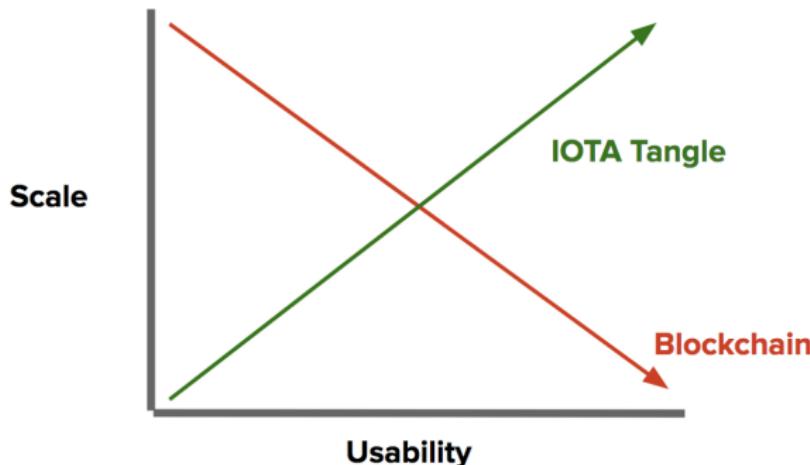


Quantum-immunity

IOTA uses the Curl hash function, which is quantum immune. A sufficiently large quantum computer would not be able to efficiently compute the proof of work to conduct an attack on the system

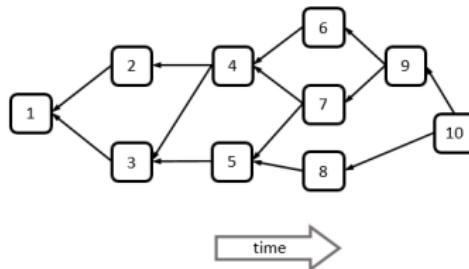
- At its core, the Tangle still has the same underlying principles as a Blockchain:
 - ① a distributed database,
 - ② a P2P Network
 - ③ and relies on a consensus and validation mechanism.
- The biggest differences are how the Tangle is structured and how consensus is achieved

Blockchain vs Tangle



source: https://cdn-images-1.medium.com/max/1200/1*fTOSBJmdallpvikk89jl-w.png

Tangle



source: https://steemit-production-imageproxy-thumbnail.s3.amazonaws.com/U5dtyqUWreuU2qioSuThYEewccKwp8w_1680x8400

- The transactions issued by nodes constitute the site set of the Tangle i.e. the DAG used as the ledger for storing transactions
- There is also the genesis transaction, which is approved either directly or indirectly by all other transactions

- To issue a transaction, users must work to validate and approve other transactions. Therefore, users who issue a transaction are contributing to the network's security
- This referencing of transactions is seen as an attestation: with a single transaction a user attests directly that two transactions, and indirectly that a subsection of the Tangle are valid and conform to the protocols rules
- A sent transaction must be validated a sufficient number of times by other users in order to be accepted as confirmed by its recipient
- IOTA currently works with a single administrator called the Coordinator which confirms all transactions at regular intervals

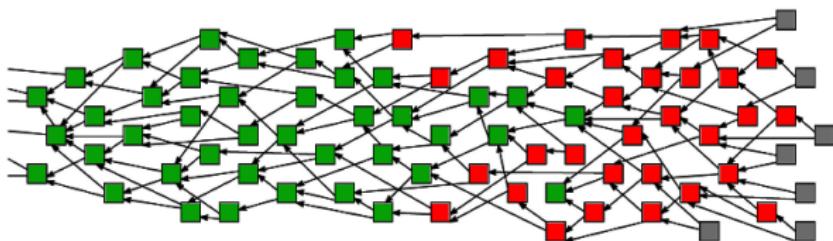
Coordinator

- Every minute the Coordinator makes a normal transaction called a Milestone, with its signature on it
- The coordinator decides where the tangle needs to grow and where to coordinate the next steps. This is the reason why IOTA is not distributed yet per definition, but decentralized
- Milestones exist because if transactions are picked at random, there is the possibility that a malicious node will try to trick others into verifying its fraudulent transactions
- Without the Coordinator, the IOTA DAG is not considered sufficiently secured in its early stages. This Coordinator is meant to be removed when the network is sufficiently large
- Once the coordinator is switched off, transactions will be validated probabilistically using Monte-Carlo methods

Transactions in IOTA

- The transaction making process can be summarized in a 3 step process
 - ① Signing - transaction inputs are signed by the user's private keys
 - ② Tip Selection - Markov chain Monte Carlo (MCMC) is used to randomly select two tips (i.e. unconfirmed transactions), which will be referenced by the user's transaction. If the node finds that a transaction is in conflict with the tangle history, the node will not approve the conflicting transaction in either a direct or indirect manner
 - ③ Proof of Work - In order for a transaction to be accepted by the network, the user needs to do some Proof of Work - similar to Hashcash. Nodes must find a nonce such that the hash of that nonce concatenated with some data from the approved transaction has a particular form
- Once these steps are complete, the transaction will be broadcast to the network, for another user to come along and choose the transaction in the tip selection process and validate it

Consensus



source: https://cdn-images-1.medium.com/max/800/1*Co2IBbi8SxWZSJS5_UxkFw.png

Consensus

- Looking at the colored tangle picture in the previous slide:
 - The green blocks are transactions on which consensus has been achieved
 - These blocks have transaction finality with some guarantees, as they are all indirectly referenced by the tips (grey blocks) that represent unconfirmed transactions
 - The red blocks are transactions where there is still uncertainty about their full acceptance
 - The transactions probability of acceptance is therefore M of N , where M is the number of times you land on a tip that has a direct path to your transaction after executing the MCMC algorithm N times

Consensus

- Users come to consensus on the status of the green blocks only, however they retain complete discretion to decide at what probability they start considering the red blocks as confirmed
- The confirmed status makes blocks eligible to be selected as tips, and this is how the tangle grows
- The probability threshold can further be increased for high value transactions to guarantee transaction finality
- As more time passes and more transactions are added, these red blocks eventually turn green as they become referenced by the majority of the tips returned by the Monte Carlo Random Walk

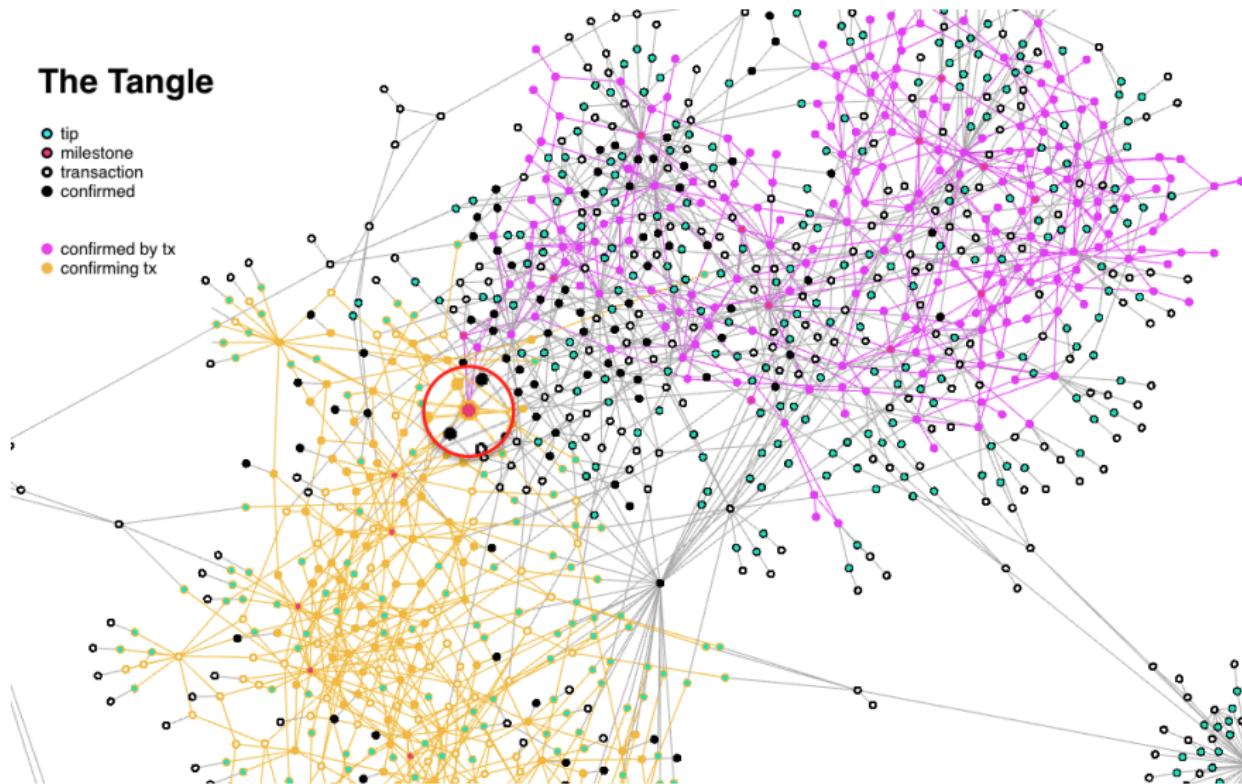
Consensus

- In general, nodes do not necessarily see the same set of transactions, as the network is asynchronous. Therefore there may be conflicting transactions.
- Nodes do not have to achieve consensus on which valid transactions have the right to be in the ledger, meaning all of them can be in the tangle.
- However, in the case where there are conflicting transactions, the nodes need to decide which transactions will become orphaned

Consensus

- As such, consensus is no longer decoupled from the transaction making process (e.g. mining), instead it's an intrinsic part of it, and it's what enables IOTA to scale without any transaction fees
- Since consensus is parallelized, and not done in sequential intervals of batches as with blockchains, the network is able to grow and scale dynamically with the number of transactions
- The more transactions are made, the more secure and the more efficient the Tangle gets
- Tests have already shown Confirmed Transactions Per Second above 100 in smaller networks of less than 250 nodes, with confirmation times of 10 seconds or less

The Tangle



source: <http://tangle.glumb.de>

Cryptography

- IOTA uses the Winternitz One-Time Signature Scheme instead of elliptic curve cryptography to produce signatures
- Hash-based signatures are known to be much faster than ECC
- The Winternitz hash is known as a post-quantum signature because quantum attacks don't significantly lower the security given by this hashes

Central Bank Cryptocurrencies

Central Bank Cryptocurrencies

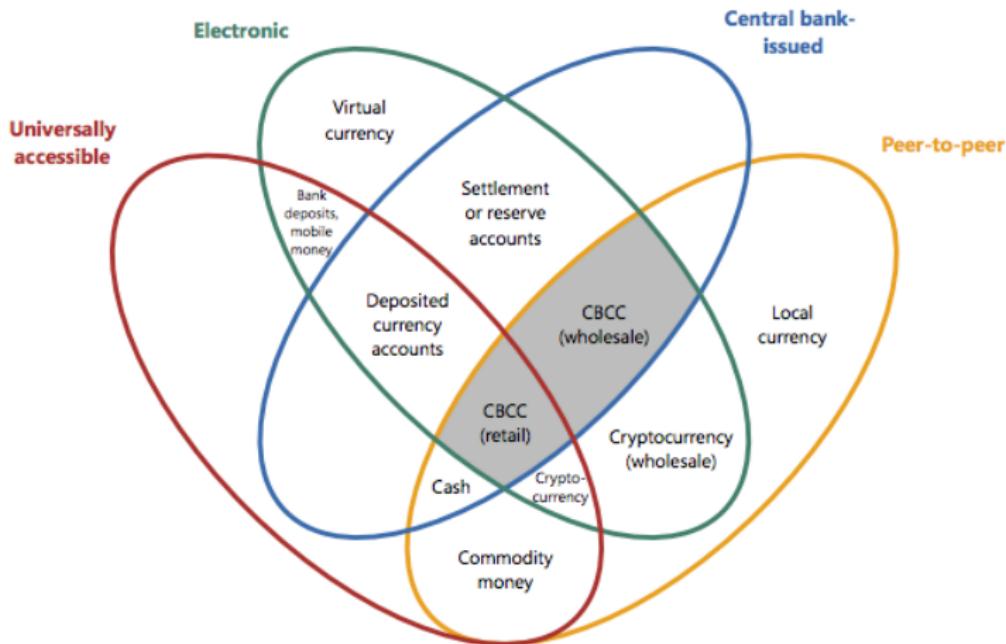
The Bank for International Settlements (BIS) defines a Central Bank Cryptocurrencies (CBCC) as " an electronic form of central bank money that can be exchanged in a decentralized manner known as peer-to-peer"

Their definition distinguishes CBCCs from other existing forms of electronic central bank money, such as reserves, which are exchanged in a centralized fashion across accounts at the central bank

The definition also distinguishes between two possible forms of CBCC

- ① A widely available, consumer-facing payment instrument targeted at retail transactions
- ② A restricted-access, digital settlement token for wholesale payment applications

Central Bank Cryptocurrencies



source: Bank of International Settlements

Central Bank Cryptocurrencies

Central banks from across the world are looking into issuing their own virtual currencies

- In March 2017, Vietnam's central bank said it was seriously studying the possibility of using bitcoin
- The People's Bank of China has run trials of its prototype cryptocurrency
- Sweden's central bank, the Riksbank, floated the idea of creating a national digital currency, the e-krona
- Singapore and Canada have tested blockchain-based currency systems for Internet payments

However, Federal Reserve Board Governor Jerome Powell has been quoted saying the U.S. central bank is not considering a digital currency.

Central Bank Cryptocurrencies

Sweden has seen physical cash circulation drop by 40% since 2009 as the population turns to cards and digital payments for transactions

The demand for cash continues to drop rapidly, with many stores no longer accepting cash and some bank branches no longer disbursing or collecting cash

Having taken notice of the trend toward a cash-free society, Riksbank's deputy governor publicly revealed plans for a central bank-issued digital currency in November 2016

Central Bank Cryptocurrencies

In an initial partial report, the Riksbank proposes a number of characteristics for the currency

- It is mainly intended for small payments between consumers, companies and authorities
- The currency will be directly connected to the Riksbank's balance sheet and made available in real-time, around the clock
- It will not be interest bearing, but should have a built-in feature whereby interest can be paid out at a later time
- Accounts will be combined with a value-based solution that allows you to pay small amounts offline, which ensures the availability to groups that either can not or do not want to have an account
- The Riksbank will be responsible for the basic features of the e-krona, but is looking into the possibility of using existing digital infrastructure

Project Ubin

The Monetary Authority of Singapore (MAS) announced the successful completion of the first phase of Project Ubin in March 2017

This is a collaborative project with the industry to explore the use of distributed ledger technology for clearing and settlement of payments and securities

The project leveraged on MAS's new MAS Electronic Payment System (MEPS+), a Real Time Gross Settlement (RTGS) system to issue funds on a distributed ledger

An Ethereum-based blockchain was designed to interact with the existing MEPS+ RTGS system, and the prototype was tested for the ability to transact 24/7, resilience against single points of failure, and timeliness of settlements.

Project Ubin

MAS plans to implement Project Ubin in multiple phases starting with the distributed ledger technology for domestic payments

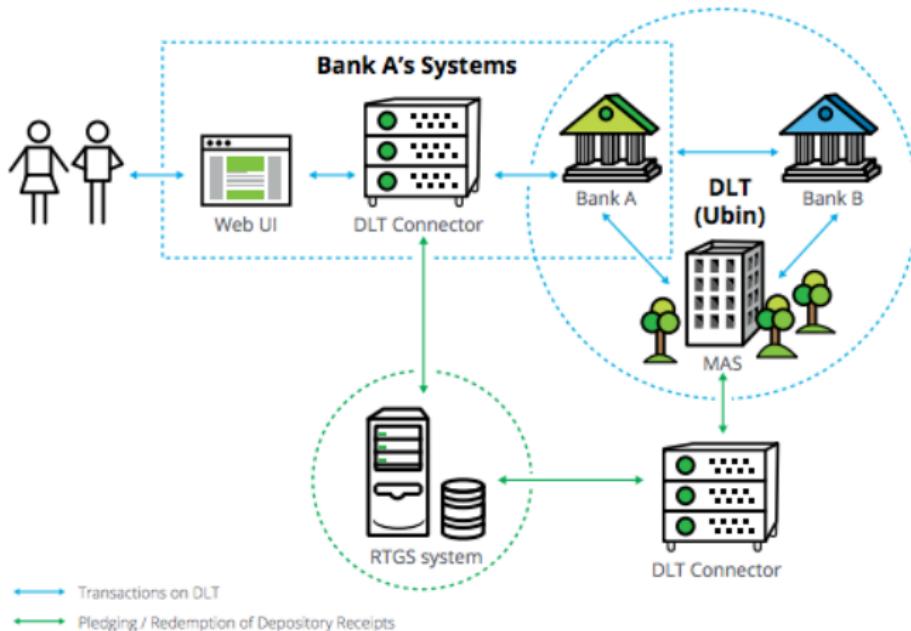
Project Ubin's Phase 1 model was designed so that credit exposures do not arise between participants when payments are transferred

Participants pledge cash into a custody account held at the central bank after which MAS creates an equal value in digital currency on the distributed ledger and sends each bank an amount of digital currency equal to the amount they pledged

Going forward, the second phase plans to focus on securities settlement (led by Singapore Exchange) and cross-border payments (led by MAS)

Project Ubin

High-level architecture of Project Ubin



source: Deloitte

Central Bank Cryptocurrencies

The BIS suggested that central banks should consider introducing their own cryptocurrencies to counter the risks from the explosive growth in bitcoin and other virtual currencies

In contrast to other cryptocurrencies, the value of the central bank's digital currency would be fixed in nominal terms

Moreover, the central bank's digital currency could be implemented using an account-based system, thereby avoiding the resource intensive mining process

Recap

- A cryptocurrency is a decentralized digital currency that uses cryptography to secure transactions
- Depending on the implementation, the blockchain does not store actual coins but rather maintains transactions that can be used to establish records of ownership
- Scalability is widely regarded as one of the biggest problems affecting Bitcoin and other cryptocurrencies
- Either on-chain or off-chain solutions can be used to address challenges surrounding scalability
- Ethereum was designed to function as a Turing complete platform on which decentralized applications and smart contracts are built and deployed

Recap

- Ethereum uses a modified proof of work consensus protocol - Ethash, making it difficult to mine using specialized hardware - which will be replaced by a proof of stake protocol (Casper)
- GHOST protocol distributes mining rewards, to compensate miners of uncle blocks
- Transactions are paid for by using 'gas'
- Ethereum's block difficulty will eventually get to a point where the chain is impossible to mine, encouraging users to switch over to Casper



bitcoin



Concept	Digital currency	Smart contracts
Block time	10mins	12secs
Protocol	Cryprographic	GHOST
Mining	Basic proof of work	Ethash
Turing complete	No	Yes
Market cap	\$4.8 billion	\$1.8 billion

Recap

- Ripple is a RTGS platform that also operates as a asset exchange and remittance network
- The platform functions like the hawala system, where payments occur by transfer of debt
- Not entirely decentralized as most validator nodes are still maintained by Ripple
- IOTA makes use of a DAG to store transactions instead of a blockchain, while still maintaining the advantages of using a blockchain
- The asynchronous nature of the network allows it to grow and scale dynamically with the number of transactions

Recap

- There is no mining, instead transactions are validated through attestation by other transactions
- The only bottleneck for IOTA is availability of bandwidth
- Central banks from across the world are looking into issuing their own virtual currencies as the demand for cash continues to drop
- The BIS suggested that central banks consider introducing their own cryptocurrencies to counter the risks from the explosive growth in Bitcoin and other virtual currencies

Blockchain applications

- Blockchain technology is flexible enough that it can be leveraged for a range of activities in financial markets
- This includes being used as a platform that could support near real time settlement in equity markets
- Another popular use is the ICO, a crowdfunding process that uses smart contract and has been likened to the IPO process
- Investors are given tokens in the ICO process, however these often have no rights attached to them
- Ethereum is the most popular platform used for ICOs
- A standard has been established for the design of these tokens to ensure that tokens perform in a predictable way throughout the ecosystem

Clearing and settlement

Stock exchanges in the modern financial system have come to be a complex entities that can be inefficient, cumbersome, and prone to risks if not designed adequately

Clearing is a process where a trusted entity acts as an intermediary between buyers and sellers. If executed efficiently, this process improves financial markets because:

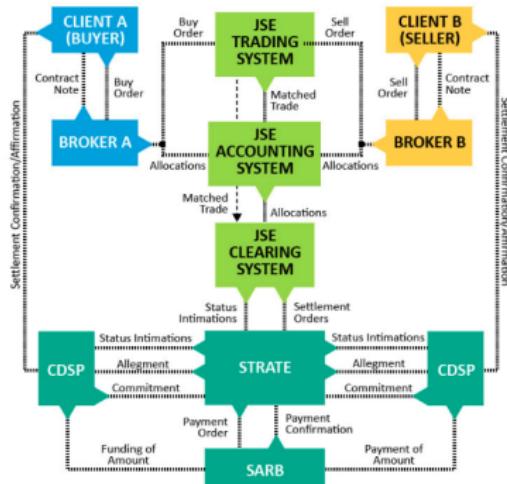
- It makes them smoother and more efficient
- It ensures that trades are settled in accordance with market rules by managing post-trade and pre-settlement credit exposures

Clearing and settlement

Settlement takes place once the clearing process has been completed

- The intermediary receives cash from the buyers and securities from the sellers and at the end of the process gives the securities to the buyers and cash to the sellers
- Typically settlement takes place three days after the transaction ($T+3$), however this differs in some jurisdictions
- This time is needed to efficiently deal with high volumes of trades and minimize the number of failed trades

Clearing and settlement on the Johannesburg Stock Exchange



source:

https://www.jse.co.za/Publishing/Images/Pages/clearingandsettlement/equitymarket/Clearing-and-Settlements_Equity-Market.jpg

Equity markets

Although technology has improved the efficiency of the equity markets over time, certain problems still persist

- Centralization means depositories and transfer agents are a single point of failure, making counter-party risk systemic
- The involvement of intermediaries generates significant administrative costs
- Limited transparency results in information asymmetry
- Legal ownership rests with the transfer agent in most jurisdictions, however this does not affect beneficial ownership (e.g. Cede & Co. in the U.S)
- Short selling may result in the appearance of two legitimate owners of a stock at any given time, otherwise known as 'phantom shares'

Blockchains are expected to reduce or even eliminate operational and financial inefficiencies with current methods of record keeping and transfer of assets in the financial markets

Blockchains in equity markets

A report by the European Central Bank highlights the potential impact of blockchains in the equities market

- The need for an intermediary to assume counter-party risk is eliminated as blockchains can be used to directly transfer share ownership between investors
- Blockchains have the potential to allow trading and settlement of securities to take place in almost real time (e.g. JSE has a t+3 settlement cycle)
- Being able to require the availability of securities and cash to transact would eliminate liquidity and credit risk from any trade executed for immediate delivery
- The report identifies that the need for a central authority does not disappear, it just takes on a different role, as a reliable institution will be required to verify that the number of securities recorded in the distributed ledger corresponds to the description of the issuance given
- The report also raises concerns regarding transparency and confidentiality which were previously discussed

Blockchains in equity markets

In 2016, online retailer Overstock.com became the first publicly traded company to issue stocks over the internet, distributing more than 126,000 shares on a proprietary blockchain through a subsidiary called t-zero, raising \$10.9m in capital

In Feb 2017, Northern Trust Corp deployed a blockchain-based system built with IBM to record information on transactions involving private equity funds

IBM also revealed that they are working with London Stock exchange to build a blockchain solution to digitize the issuance of securities for small and medium sized enterprises

In each instance, blockchains are used to facilitate the use and transfer of asset backed tokens

Blockchains in equity markets

Nasdaq - In 2015, Nasdaq unveiled the use of its Nasdaq Linq blockchain ledger technology to successfully complete and record private securities transactions for Chain.com

Australian Stock Exchange - Began to evaluate replacement options for the Clearing House Electronic Subregister System (CHESS) in 2015. This project is expected to end in 2017

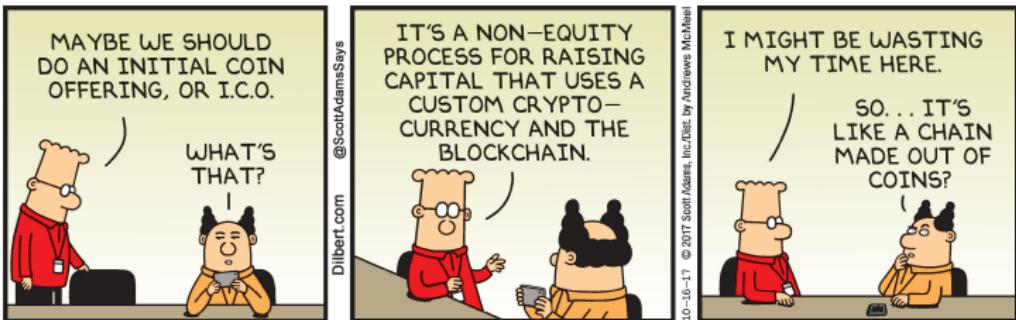
Japan Exchange Group - Working with IBM towards testing the potential of blockchain technology for use in trading in low transaction markets.

Korea Exchange - Launched Korea Startup Market (KSM) with Blocko's blockchain technology to enable equity shares of startup companies to be traded in the open market.

Dole stock crisis

- In 2015, a class action lawsuit revealed that there were 12 million more shares of Dole Food outstanding than the company thought existed
- This anomaly is thought to have been caused by the 'chill' period instituted by the Depository Trust & Clearing Corporation (DTCC). When there is a merger or acquisition about to close, the DTCC will place a chill on the stock and not record any tradees for the three days leading up to the closure due to high activity that will be difficult to keep track of
- When Dole Food transitioned from a public to a private company, trades under the terms of a chill were allowed to continue, but DTCC ownership records did not reflect any changes over this period
- This, coupled along with short selling may have contributed to the existence of the phantom shares

Incidents like this would become near impossible if blockchains are used to record stock ownership as the markets would benefit from improved transparency and auditability of records



source: <http://dilbert.com/strip/2017-10-16>

ICO

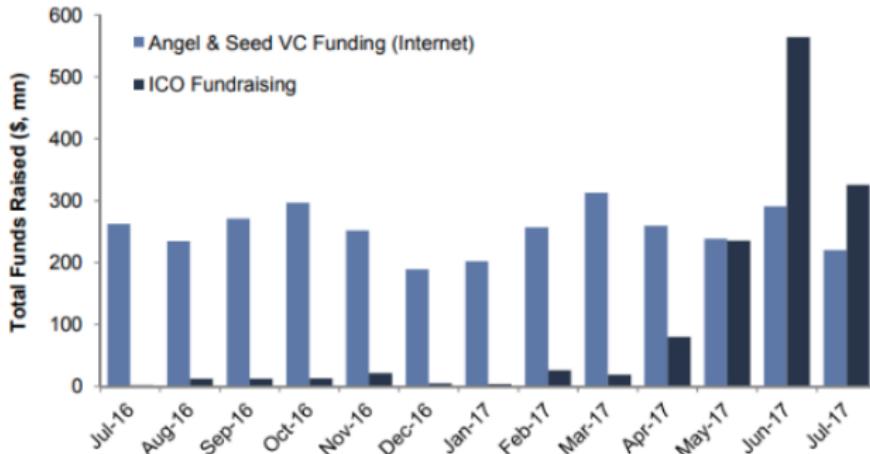
Initial Coin Offerings (ICO) are a hybrid between the Initial Public Offerings (IPO) of the equity markets, crowd-funding and venture capital, allowing start-ups to raise funds denominated in cryptocurrency

Investors purchase tokens that represent ownership in an underlying company that will undertake a particular technology project starting at a later date

According to the CoinDesk ICO tracker, an excess of \$12.83 billion has been raised through ICOs worldwide since 2014

ICOs have since become a primary means of fundraising for projects built on blockchain technology

The pace of ICO fundraising has now surpassed Angel & Seed stage Internet VC funding globally
Total Funds Raised by month (\$, millions)



Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.

Goldman Sachs

ICO



source: <https://media.blockchainhub.net/wp-content/uploads/2017/04/History-of-ICOs-1.jpg>

ICO

- ICOs have gained popularity among startups as this method allows them to raise capital without having to promise to pay dividends or sell any equity
- Ideally, the token sold at ICO should be an integral part of the system or application
- Tokens can have some voting rights for investors
- In such cases, this may lead to the tokens being classified as securities under the laws of the jurisdiction

ICO

Generally, there are three different ways in which to conduct an ICO

- ① Developing and launching your own blockchain - this method is typically used by startups looking to create their own cryptocurrency. This has the advantage of having more control over characteristics like security and additional features
- ② Launching a second layer token on top of an existing one - this is the most popular method used. Ethereum's Turing complete language allows users to build custom tokens through the use of smart contracts
- ③ Using a purpose built ICO platform - Platforms such as Waves or ICONOMI have been created specifically for the purpose of easing the process of launching and conducting an ICO as much as possible, allowing the startups to begin their ICOs in just a few clicks

ICOs - Step by step guide

- ① Present a white paper to describe the idea in greater technical depth for the cryptocurrency community to review
- ② Lay out project specification as well as terms of token distribution
- ③ Start the crowdfunding campaign

ICOs - Step by step guide

- ① The Issuing company presents a whitepaper describing the business model and the technical specifications of a project
 - This is typically advertised on cryptocurrency forums and supported by a prototype
 - Whitepapers are aimed at experts and opinion leaders, professionals who are able to understand the technical essence of the product
 - Among other things, it should outline the relevance of the project and the market it operates on, the economics of the project and token and the team involved
 - However there is no need to explicitly start with a working product. Sometimes an ICO is just that - a fundraising campaign solely for the purpose of securing money for the production of the actual solution
 - More sophisticated projects will offer a Yellow paper, that will present the technology and the innovations that they have created, or propose to create in scientific detail

ICOs - Step by step guide

- ② A project timeline, target budget detailing expected costs until launch (marketing, R&D, etc.), and a plan for the token distribution are set
 - This stage also includes marketing efforts in the form of websites, banner advertisements, press releases, and collaboration with media outlets
 - Token supply can either be static or dynamic depending on whether there is a specific goal or limit on the funds to be raised
 - A static supply with a set goal will mean that tokens have pre-designated price that will not change during the process
 - A dynamic supply with a dynamic goal would mean that a new token is created every time funds are received

ICOs - Step by step guide

- ③ The token is then offered to investors in exchange for cryptocurrency
 - Investors participate through the use of token compatible wallets; examples are provided [here](#)
 - Due to strict regulations, US residents are in theory not allowed to participate in ICOs as only accredited investors can partake in private placements of securities
 - Although the issuer can not guarantee it, they are expected to take the necessary steps to prevent most US citizens from investing
 - A time limit for participation is determined either by a set time frame or by the funding goals
 - Best practices dictate that all funds raised ultimately be kept in a multi-signature wallet (i.e. requires multiple signatures to authorize transactions) that is made public

ICO tokens

A token is a smart contract (or script) running on a blockchain

This script describes the behavior of the token i.e. token generation, units of measurement or any other functions necessary for the token to remain functional

Operations are executed by when users or other smart contracts send a valid message to that token's contract in the form of 'transactions' that execute the functions defined in the contract

All allocations of tokens are done through the token contract in question, and still, the owner of the tokens has to sign and execute any transfers

ICO tokens

The process is conducted entirely on the blockchain; Ethereum has become the platform preferred by many developers

Ethereum has simplified ICOs as one of its main capabilities is that it allows users to create their own tokens

Tokens are non-dilutive, (usually) possess no voting power, and have very little, if any, rights attached to them

They are neither debt, which enjoys mandatory repayment in the event of a default, nor are they equity, which grants the holder some preferential rights vis-a-vis ordinary shareholders

ERC-20 Token standard

The Ethereum developers created the ERC-20 'Token Standard' to standardize token creation

The standard establishes a common set of rules for tokens issued, and currently serves as the basis for the many tokens that have been released through ICOs

The standard ensures that ethereum-based tokens perform in a predictable way throughout the ecosystem, such that decentralized applications and smart contracts are interoperable across the platform, and that all tokens follow a fixed standard of security

Other token standards exist, like

ERC-20 Token standard

- Until September 2017 ERC-20 was unenforced, but it had been already adopted by token developers since its introduction in late 2015
- The standard defines a set of six functions that other smart contracts within the ethereum ecosystem will understand and recognize, such that decentralized applications and smart contracts are interoperable across the platform
- These include, for instance, how to transfer a token (by the owner or on behalf of the owner) and how to access data (name, symbol, supply, balance) about the token.
- The standard also describes two events - signals that a smart contract can execute and that other smart contracts 'listen' for
- Before ERC-20, every ICO token implemented its own versions of these basic functions
- This standard allows for the tokenization of other features, including voting rights

ERC-20 Token standard

```
1 // 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 }
```

A sample token contract is available here

Token standards

Multiple token standards exist, however ERC-20 is the most well known and used of them all

- ERC-233: Very similar to the ERC-20 standard, but it solves the problem where tokens can get stuck inside a contract due to human error
- ERC-621: ERC-20 only allows a single token issuance event, which restricts the supply to a certain amount which can't be changed. This standard solves this by using the functions `increaseSupply` and `decreaseSupply` which can increase and decrease the token supply in circulation
- ERC-721: Can be used to issue non-fungible tokens i.e. each token is totally different and each one can have a different value to different users
- ERC-827: An extension of the ERC-20 standard that allows for the token holder to nominate a third party that can spend the token

ICO pricing

Due to the lack of regulation, developers have had free reign on how to run an ICO so far

The price of a token during ICO period typically runs through different stages depending on the pricing mechanism:

- ① Increasing Price: ICO runs in stages where the team sets a fixed exchange rate for the tokens and the rate increases incrementally with time. This way, early investors who take the biggest risk get the best price per coin ratio
- ② Decreasing Price: A dutch auction. The sale starts at the highest price per token proportionally decreases until the end of the auction to get each investors reservation price
- ③ Fixed price: This mechanism is appealing to large investors because they don't have to worry about influencing the price by purchasing a big number of tokens
- ④ Price not determined: Investors are given tokens in proportion to their part of total investments

How to participate in an ICO

1 Buy Cryptocurrency

- Find an exchange from which you can purchase a traded cryptocurrency
- Bitcoin and some other alt-coins may be accepted, depending on the ICO
- Once the funds have been acquired, they are used to buy the tokens by transferring them to the ERC-20 compatible wallet
- The address that sends Ether to the ERC-20 compatible wallet gets credited with the equivalent amount of the token in the ERC-20 token contract
- The following are the most popular wallets that support Ethereum ICOs: MyEtherwallet, Mist, Parity, MetaMask, imToken

How to participate in an ICO

2 Contribute to the ICO

- The ICO whitepaper will contain all information regarding the project, including the price of a token, start date, and the duration of the token sale
- Send a deposit to the ICO contract address with correct data and gas limit values
- The project will generally announce the recommended Gas Limit for their smart contract once the contract address is publicly known
- Setting a value less than this runs the risk of running out of gas and failing to complete the transaction
- Once the transaction successfully completes, you will receive the token

How to participate in an ICO

Send Ether & Tokens

To Address
0x7cB57B5A97eAbe94205C07890BE4c1aD31E486A8

Amount to Send
Amount ETH ▾
Send Entire Balance

Gas Limit
21000
+Advanced: Add Data

Data
0x6d79657468657277616c6c65742e636f6d20697320746865206265737421

Generate Transaction

Figure: Sending ether with MyEtherwallet

How to participate in an ICO

A comprehensive list of the upcoming and past ICos is available at ICO Watch List

ICO WATCHLIST

Welcome to the ICO Watch List!

Discover the best ICO (initial coin offering) opportunities. Review this list daily to stay on top of the exponentially growing cryptocurrency & blockchain ecosystem. The projects on the ICO list are scanned and updated daily, to help crypto investors make better investment decisions.

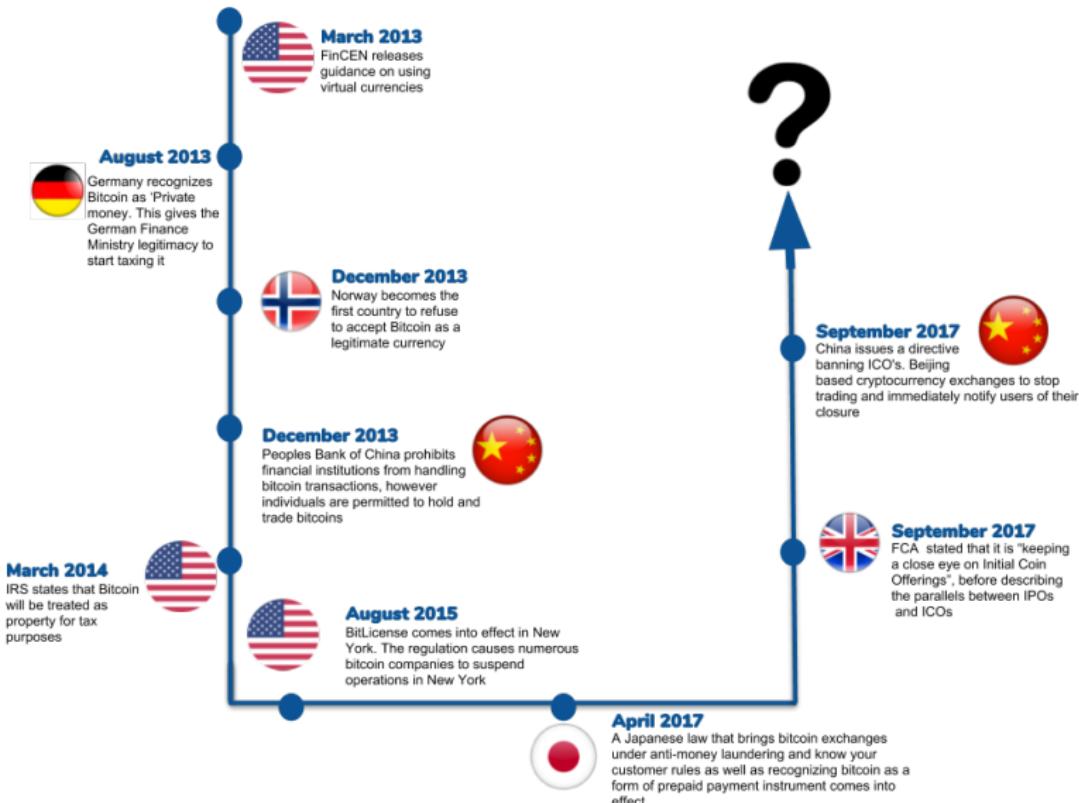
LIVE ICOs UPCOMING ICOs FINISHED ICOs

PROJECT	INFO	TIME	PROGRESS	
 REGA INSURANCE	We reinvent insurance.	ENDS IN: 30 07 55 Days Hours Minutes	<div style="width: 3%;"><div style="width: 3%;">3%</div></div>	ICO Details 
 VERIFYUNION SECURITY IDENTITY	Decentralized Platform for Digital Identification and Social Scoring Engine.	ENDS IN: 46 17 54 Days Hours Minutes	<div style="width: 21%;"><div style="width: 21%;">21%</div></div>	ICO Details 
 UCASH FINANCE	Cash meets digital currencies.	ENDS IN: 81 13 55 Days Hours Minutes	<div style="width: 31%;"><div style="width: 31%;">31%</div></div>	ICO Details 

Recap

- In the equity markets, blockchains are posited to improve the efficiency of the clearing and settlement processes
- The capacity for almost real time settlement and increased transparency is expected to eliminate operational inefficiencies and reduce costs
- Blockchains are already being used in some transactions involving private equity funds
- ICOs have become a primary means of fundraising for projects built on blockchain technology
- A token is fundamentally a smart contract. Different tokens may represent different rights to holders
- Tokens issued on the Ethereum blockchain generally follow the ERC-20 Token Standard
- Due to the lack of regulation, developers have had carte blanche on how to price ICOs

Fintech Regulation



Regulatory landscape

- Fintech regulation still remains a contentious issue
- very few regulatory authorities have come forward with a definitive stance
- Concerns include the ease with which the technologies can be used for malicious activity
- Regulators around the world are starting to consider tokens issued in ICOs as securities
- The ways in which smart contracts will interact with traditional contracts and the law still remains unclear

Regulatory landscape

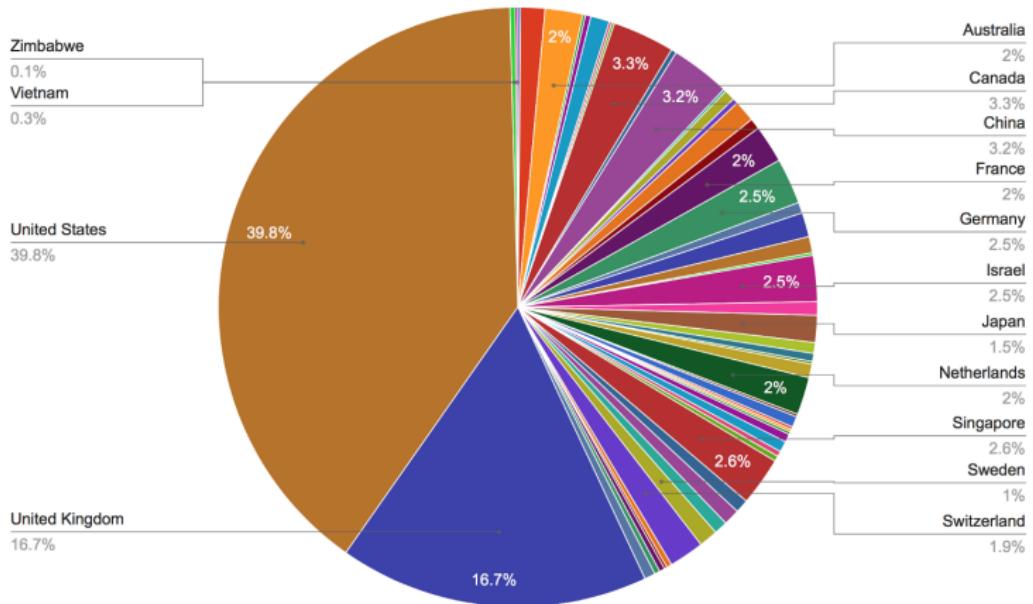
To date, very few authorities have made their stance completely clear by way of issuing regulatory guidance

The regulation of FinTech companies is often a contentious issue, given the need to balance a framework that remains flexible enough to encourage financial innovation, all while maintaining the regulator's commitment to the safety of consumers and the financial markets

The majority of players in the banking industry advocate for regulators to hold FinTech companies that perform banking functions to the same standards as traditional banking institutions

A more evolutionary approach would be adopting a regulatory framework that is unique to these firms in order to encourage innovation

Blockchain Startup Hotspots



source: https://cdn-images-1.medium.com/max/1000/1*ePq2zWVXZUACW5WxclgHfA.png

Regulation in the US

The Office of the Comptroller of the Currency (the "OCC"), the regulator of national and federal savings banks, issued a whitepaper in March 2016 titled "Supporting Responsible Innovation in the Federal Banking System."

The OCC requested comments on a number of areas, including how to facilitate responsible innovation and enhance its process for monitoring and assessing innovation within the federal banking system.

Eight basic principles were established, guiding the development of a framework to evaluate FinTech products and services by national and federal savings banks

Regulation in the US

The principles call for the OCC to

- ① Support responsible innovation
- ② Foster an internal culture receptive to responsible innovation
- ③ Leverage agency experience and expertise
- ④ Encourage responsible innovation that provides fair access to financial services and fair treatment of consumers
- ⑤ Promote safe and sound operation through effective risk management
- ⑥ Encourage all banks to integrate responsible innovation into their strategic planning
- ⑦ Promote dialog through formal outreach
- ⑧ Collaborate with other regulators

Financial Services Innovation Act

- Proposed by Patrick McHenry, vice chairman of the U.S. House of Representatives Financial Services Committee
- Calls for the creation of a Financial Services Innovation Office (a "FSIO") within each federal banking agency as well as a number of other federal agencies that will have jurisdiction over types of financial services
- Fintech companies providing banking services would not be forced into the same mold as traditional banks, which may stifle innovative capacity of small businesses
- Instead, the Act allows for "regulatory beta testing" i.e. a period of time, during which new types of regulation, new openings for innovation, and the measurement tools would be test-driven, and customized before being adopted

BitLicense

- In 2015, the New York State Department of Financial Services (NYDFS) introduced BitLicense, a business license for cryptocurrency activities
- This regulation is primarily targeted at cryptocurrency exchanges and issuers of cryptocurrencies, with an emphasis on consumer protection
- Merchants and consumers that use cryptocurrencies solely for the purchase or sale of goods or services or for investment purposes are excluded under these rules and regulations
- All licensed bitcoin businesses are required to meet capital requirements, that have been determined to sufficiently ensure financial integrity
- They are also required to submit quarterly reports to the NYDFS that include complete financial statements as well as other information at the discretion of state regulators

Regulation in the US

- In 2017, the Securities Exchange Commission (SEC) released an investigative report in which it said some token sales should be categorized as securities, therefore appropriate steps must be taken to comply with the U.S. federal securities laws
- The ruling followed an SEC investigation into a German corporation behind The DAO, that raised \$150 million in an ICO and then was attacked and robbed of 1/3 of their assets due to a flaw in The DAO's source code
- The SEC cited concerns regarding consumer protection
- This possibility of being required to comply to the strict securities laws of the US is the reason why most ICOs will restrict the participation of US citizens

Regulation in the US

- For tax purposes, the US Internal Revenue Service (IRS) treats digital currency as property rather than foreign currency
- Any institution legally formed in the US can therefore expect a combined federal and state tax rate between 35% and 50% for any token related activities
- According to the Financial Crimes Enforcement Network (FinCEN), any administrator or exchanger of virtual currency is a money service business and will be regulated accordingly

Regulation in the US

- In June 2016, Vermont signed into an economic development bill, a provision that recognizes the application of blockchain technology to promote economic development
- The states of California and Florida have proposed amendments to legislation that would formally recognize blockchain signatures and smart contracts
- Similar amendments have already been passed in Arizona and Vermont

Regulation in Singapore

In 2016, the Monetary Authority of Singapore (MAS) announced its plans to merge and simplify money exchange, remittance and payments system law into one legislation that would regulate old and new payments services.

This initiative aims to allocate S\$225m by the end of 2020 to help foster growth and innovation in the domestic FinTech sector

The mandate is to create an environment for the type of innovation that enables the structures in the already existing financial system to improve its efficiency and cost effectiveness, instead of disrupting it

MAS regulatory sandbox

The MAS launched a regulatory sandbox to allow for experimentation with FinTech solutions

In this environment, some regulatory requirements are relaxed and actual products or services are provided to the customers but within a well-defined space and duration

- This includes and is not limited to requirements regarding board composition, compliance with MAS guidelines on technology risk management and outsourcing and requirements on financial soundness
- However, exemptions will not be made for regulations regarding customer confidentiality, AML regulations and the handling of customer assets by intermediaries

Firms are able to conduct small scale experiments and test ideas in a secure, low risk market before exporting to bigger markets

MAS regulatory sandbox

Even if an experiment fails, its impact on consumers and on broader financial stability will be limited

MAS also plans to introduce new rulings that would make it easier for startup and SMEs to raise funds on securities-based crowdfunding (SCF) platforms

- SMEs seeking to raise less than \$5million within a 12month period will be able to do so without having to issue a prospectus
- Financial requirements for SCF platform operators who want to raise funds from accredited and institutional investors will be reduced. Both the base capital requirement and minimum operational risk requirement for such intermediaries will be reduced from \$250,000 to \$50,000, and the requirement for a \$100,000 security deposit will also be removed

In 2017, the MAS joined forces with the French regulators Autorité de Contrôle Prudentiel et de Résolution (ACPR) and the Autorité des Marchés Financiers (AMF) after forming a partnership with the Swiss Financial Market Supervisory Authority (FINMA) in 2016

Regulation in Australia

The Australian Securities and Investments Commission (ASIC) followed suit and set up its own regulatory sandbox targeted at businesses without financial services licenses

Strict limits have been placed on the types and amounts of products that qualify to be a part of the sandbox

- Marketplace lenders and firms working in superannuation or life insurance are prohibited from participating
- The purpose of the limits is to reduce the number of start-ups that can automatically use the sandbox

Those that qualify for the sandbox are only required to notify ASIC that they are using it and do not need to go through any formal approval process unlike in Singapore

Businesses that don't qualify can apply for an individual exemption, but there is no clear guidance on the criteria that ASIC uses to assess such an application

Regulation in Australia

ASIC has issued regulatory guidance to help businesses in specific sectors on multiple occasions

- Regulatory Guide 255 aims to assist industry to understand ASIC's approach to regulating digital advice
- Information Sheet 213 gives guidance to providers of marketplace lending products and related financial services in connection with these products, outlining disclosure requirements, regulatory obligations and good practice examples
- Information Sheet 219 assists those who are considering operating market infrastructure on a blockchain

Regulation in Australia

- The Australian Tax Office does not consider cryptocurrencies money for goods-and-services tax (GST) purposes. Instead, they are considered as a form of intangible property subject to capital gains tax
- In 2017 the Australian government introduced *Treasury Laws Amendment (2017 Measures No. 6) Bill 2017*
- This bill exempts the purchase of bitcoin and other cryptocurrency as taxable supplies, removing double taxation when the currency is used to buy a taxable supply
- The guidance accounts for whether the cryptocurrency is kept for personal use, as an investment or in a profit making scheme

Regulation in the UK

- In 2016, the UK treasury published a report in which it presents a set of recommendations which address blockchains, their governance, security and privacy
- The report recommends that government establishes a regulatory framework flexible enough to evolve parallel with ongoing development, established in collaboration with academia and industry
- The report further calls for government to support and facilitate an increase in the investment in the research required for innovation
- Although bitcoin is not explicitly recognized as a currency, for tax purposes it is effectively treated like any other form of payment

Regulation in South Africa

South African regulators taken a more neutral and reactionary approach to regulating FinTech and other digital innovations

They refer to this as 'back to basics', whereby they focus on risk based principles rather than creating rules based principles aimed at regulating specific technologies or products

Innovations will therefore not be regulated beyond how they may fall within the existing framework

- This lack of clarity and guidance makes navigating South Africa's comprehensive regulatory framework rather difficult due to compliance risk as certain financial functions may be subject to multiple pieces of legislation overseen by different regulators
- As a result, most of the innovation has occurred in the relatively less regulated payments sector

Regulation in South Africa

In 2013, an intergovernmental FinTech working group was established between National Treasury, the Reserve Bank, the Financial Intelligence Centre, and the Financial Services Board

The groups mandate includes determining appropriate FinTech regulatory frameworks that align with government's policy objectives such as financial inclusion and deepening competition in the financial sector

In 2014 the Reserve Bank established an internal working group on virtual currencies and distributed ledger technologies

- The group identified cryptocurrencies as not posing a significant threat to financial stability, price stability or the national payment systems as they are not widely used
- This is why the Reserve Bank has opted not to regulate cryptocurrencies. But they reserve the right to do so in the future

Regulation in South Africa

The Financial Services Board has also created draft amendments to the Financial Advisors and Intermediary Services Act which recognize additional requirements on firms using artificial intelligence to provide automated investment advice

In an effort to take a more proactive approach to regulation, in 2017, the Reserve Bank announced that it had established a three-man FinTech unit to monitor the impact of new technology developments on deposit taking, payments, lending, insurance, and investments

- Responsibilities are expected to include the facilitation of the development of appropriate policy frameworks for the Reserve Bank across the FinTech domain, while working together with the inter-governmental FinTech working group.
- There is also a mandate to collaborate with and take into account the experiences and models of foreign central banks in establishing innovation hubs and regulatory sandboxes

Regulation in China

Historically, Chinese authorities have often taken drastic measures in the regulation of FinTech due to factors that put the Chinese economy at greater risk relative to other countries

- China is one of the world's largest markets for FinTech services
- It has the world's largest online alternative finance markets by transaction volume, and the largest community of Bitcoin miners

To date no other authorities have issued regulatory guidance as comprehensive and restrictive as the Chinese

Regulatory tools used by authorities range from limiting investment by foreigners, to restricting the roles institutions can play in the market, and in some instances prohibition

Regulation in China

Main authorities and the areas they regulate include

- People's Bank of China - online payment services sector
- China Securities Regulatory commission - equity crowdfunding and online sale of funds
- China Insurance Regulatory Commission - internet insurance services
- China Banking Regulatory Commission - online micro-lending and peer-to-peer lending

Regulation in China

People's Bank of China

- Refuse to acknowledge cryptocurrencies as legal tender because they are not issued by monetary authorities
- In 2013, enacted legislation that prevents banks and other financial institutions from using Bitcoin as a currency
- In 2017, banned withdrawals from Chinese cryptocurrency exchanges, citing concerns about capital flight, and then went on to later shut down all exchanges
- Announced plans in early 2018 to block access to all online platforms and mobile applications that offer exchange-like services for cryptocurrencies. Financial institutions were further instructed to stop providing banking or funding to any activity related to cryptocurrencies
- Despite all of this, substantial investments have been made for developing their own central bank issued cryptocurrency

Regulation in China

China Securities Regulatory commission

- Issued a directive in September 2017 banning ICO's with immediate effect
- Token sales were identified to be contravention of securities laws and were labeled as 'illegal and disruptive to economic and financial stability.'
- Fundraising platforms are no longer allowed to provide trading and exchange services, and all financial institutions are prohibited from doing any business related to ICO trading.
- Organizations and individuals who had completed funding through an ICO were instructed to make necessary arrangements to repay investors

Regulation in China

China Banking Regulatory Commission

- Published *The Interim Administrative Measures for the Business Activities of P2P Lending Information Intermediaries* in August 2016. A piece of legislation aimed at regulating the peer-2-peer lending sector
- High entry thresholds for firms were implemented through the use of capital adequacy and information disclosure requirements, along with a ban on unsecured lending
- Firms facilitating lending transactions are prohibited from promising fixed returns, and those directly engaging in lending transactions are prohibited from financing their own projects or related parties' projects with funds solicited via their platforms
- All lending firms are barred from directly or indirectly holding and gathering client money solicited via online portals. This responsibility is left to a nominated third-party depository financial institution

Regulatory challenges

It remains unclear whether the transparency that comes with the use of blockchains in the financial markets will be detrimental or beneficial to overall efficiency

- From a regulatory perspective it is clear how this, coupled along with the ability to perform regulatory functions in real time, will be beneficial
- On the other hand, transparency may bring about the end of dark pool trading. This is a private forum for trading financial instruments where large trades by financial institutions are offered away from public exchanges. This is done for multiple reasons, and one of them includes facilitating large trades without affecting prices

Regulatory challenges

Cryptocurrencies have always been tainted by the fact that the use of bitcoins grew in the market for illegal goods

This showed its potential to be used for money laundering and financing other illicit activities

At a point in time, Silk Road, the infamous online black market, was responsible for half of all bitcoin transactions

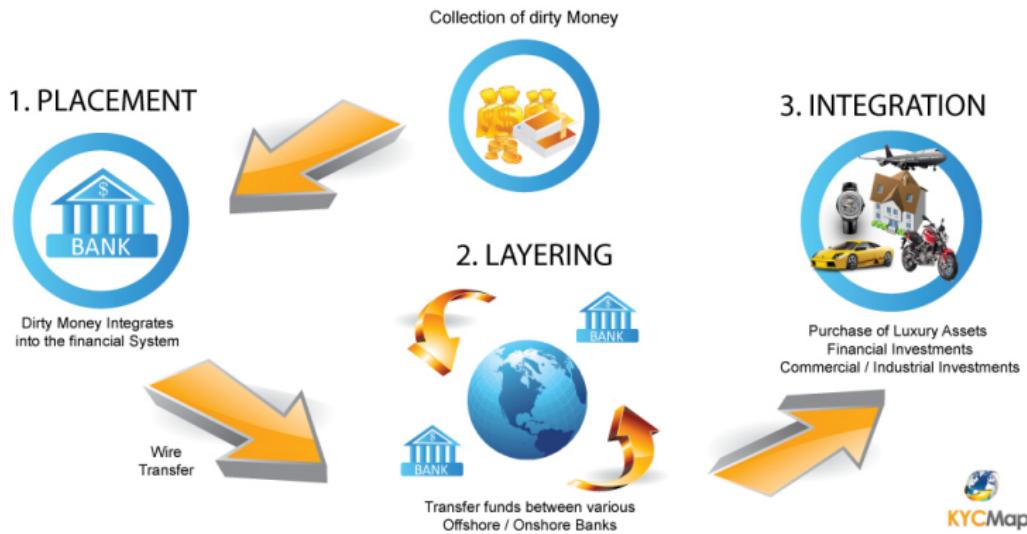
Despite this, several educational and entrepreneurial groups have begun developing ways to legitimize the currency

Money laundering

- Money laundering is the process of concealing the origins of illegally obtained money by exchanging it into ostensibly legitimate assets
- This is typically by means of transfers involving foreign banks, legitimate cash based businesses or currency exchanges
- Money can be laundered by many methods which vary in complexity and sophistication
- The process involves three fundamental steps
 - ① Placement - introducing the illicit funds into the system
 - ② Layering - concealing the source of the funds by way of a series of complex transactions and bookkeeping tricks
 - ③ Integration - integrating the funds into the financial system through purportedly legitimate transactions

Money laundering

A TYPICAL MONEY LAUNDERING SCHEME



source: <http://kycmap.com/wordpress/wp-content/uploads/2012/12/Paul-Renner-C6-KYC-money-laundering-example.jpg>

Cryptocurrency laundering

- Just like conventional currency, cryptocurrencies are not immune to being laundered
- Full transaction auditability of cryptocurrency can easily be thwarted
- The propensity to use cryptocurrencies to facilitate fraud is further exacerbated by pseudonymity
- In 2017, a cyber criminal who laundered £3bn in bitcoin through a cryptocurrency exchange was arrested in Greece

Cryptocurrency mixing

Mixing/tumbling is a process in which cryptocurrency is 'cleaned'

- Users send their funds to the service provider, pay small commission, and then receive the same sum of untraceable funds less a service fee
- The client's funds are divided into smaller parts. These parts are mixed and exchanged at random with similar parts of other clients from unrelated transactions and then sent back to the client who is now using a new public address, making ownership virtually untraceable.
- The quality of tumbling depends on total number of users and the amount of coins available for mixing
- This process was initially intended to further protect the privacy of bitcoin users. Currently there are several mixers including CryptoMixer and CoinMixer

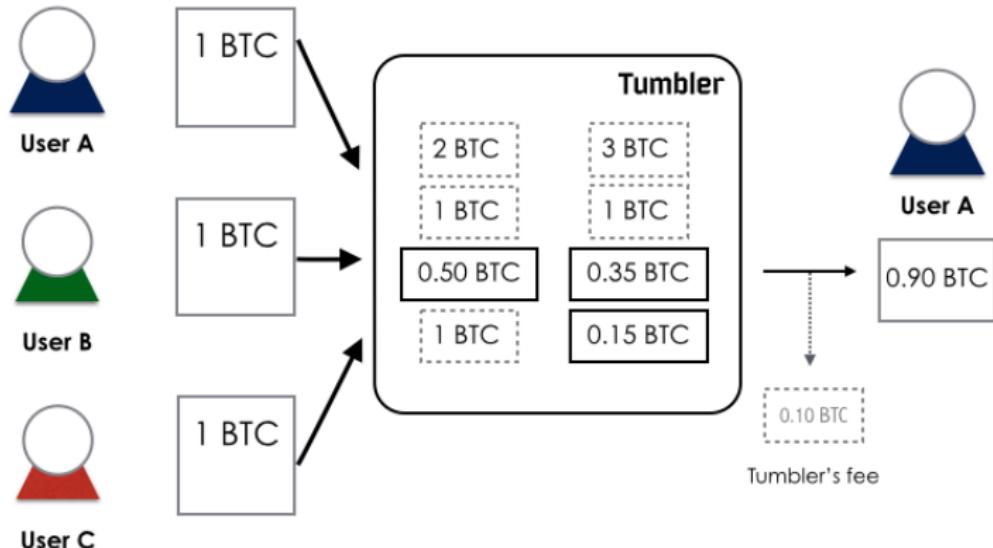


Figure: Bitcoin mixing

source: <http://tech.eu/wp-content/uploads/2014/05/Bitcoin-tumbler-mixer.png>

Cryptocurrency laundering

Cold storage and off-chain transactions

- Cold storage refers to keeping a reserve of cryptocurrency offline
- Methods of cold storage include USB drives or other data storage medium, paper wallets (a document containing all of the data necessary to generate any number of private keys) or a hardware wallet (a secure hardware device which stores the user's private keys)
- This is a common practice among exchanges as a security measure intended to minimize losses in the event of a security breach. The only amount kept on the server is the amount needed to cover anticipated withdrawals

Cryptocurrency laundering

- An off-chain transaction is the movement of value outside of the blockchain
- While a normal transaction modifies the blockchain and depends on it to determine its validity, an off-chain transaction relies on other methods to record and validate the transaction
- Cryptocurrency held in cold storage can just as easily be exchanged for goods or services once the value has been confirmed
- Once a wallet has been used in multiple off chain transactions, ownership becomes virtually untraceable, therefore circumventing the auditability of a blockchain

Anti-Money Laundering

- This refers to legal controls that require financial institutions and other regulated entities to detect, report and prevent the practice of generating income through illegal actions
- Anti-Money Laundering (AML) regulations require financial institutions to complete due-diligence procedures to ensure they are not aiding in money-laundering activities
- The onus to perform these procedures is on the institutions, not on the criminals or the government
- A report by the Financial Action Task Force found that that money remittance and currency exchange businesses have been both willing and unwitting participants in laundering activities, and in certain instances, financing terrorism

AML in cryptocurrencies

- In the US, FinCEN issued guidance regarding *Persons Administering, Exchanging, or Using Virtual Currencies*
- Cryptocurrency exchanges are considered money service businesses and hence are required to comply with Bank Secrecy Act laws and regulations, including AML requirements and KYC (Know Your Customer) rules
- A bill known as "Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017" was introduced to senate
- The bill will allow for civil asset forfeitures of cryptocurrencies, and requires users to declare cryptocurrency assets exceeding \$10,000 whenever they cross the US border

AML in cryptocurrencies

- In Australia, the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill was introduced in 2017
- Under the bill, cryptocurrency exchanges have to enroll in a Digital Currency Exchange Register
- Exchanges will have to implement measures to mitigate the risks of money laundering as well as identify and verify the identity of their customers
- Suspicious transactions will have to be reported, including cash transactions exceeding \$10,000 and seven years worth of records documenting their AML measures have to be kept

AML in cryptocurrencies

- The EU has proposed AML4, legislation that contains numerous articles that directly address cryptocurrencies
- Cryptocurrency exchanges would be required to gain licensed authorization from the nation state in which they are based
- They will also be subject to existing AML and KYC legislation
- The act aims to end the anonymity associated with cryptocurrency transactions

Money laundering through ICOs

- The increasing popularity of ICOs as a primary source for fund raising has increased angst among members of the financial industry, due to the absence of regulatory oversight
- Many have cited fears of widespread money laundering and fraud
- Whereas traditional AML framework requires fund raising companies to do their due diligence like KYC and tracking the sources of an investors wealth, this is not a requirement for ICOs

Money laundering through ICOs

- ① Party A buys into an ICO in the hope that the value of tokens will appreciate
- ② Party B, who is looking to launder money, then offers to buy the tokens from A at a premium on a cryptocurrency exchange that does not strictly adhere to KYC requirements
- ③ Once B has purchased the token, it can then be sold for cryptocurrency on another exchange that has more stringent rules. This in effect 'legitimizes' the funds as ICO tokens tend to have inflated prices therefore nothing will appear out of the ordinary
- ④ The funds can then be withdrawn and integrated into the financial system in exchange for fiat currency

Regulating ICOs

In September 2017, China issued a directive banning ICO's with the authorities citing concerns about "protecting market stability and protecting the interest of investors"

There were 43 ICO platforms in China in July 2017; Sixty-five ICO projects had been completed, raising 2.6 billion yuan (\$398 million)

Then, in July and August alone, Chinese tech firms raised \$766 million worth of cryptocurrencies in local ICOs in just 8 weeks

The MAS, publicly declared that ICOs are "vulnerable to money laundering and terrorist financing risks due to the anonymous nature of the transactions, and the ease with which large sums of monies may be raised in a short period of time."

Federal Securities Laws

- It is illegal to offer or sell securities in the United States unless the offer and sale are exempt under the federal securities laws or a registration statement has been filed with the SEC
- This law is broad enough to capture any contract, transaction or scheme, and in some cases, tokens issued during ICOs may fall within the scope of this law
- The SEC reiterated that "[w]hether or not a particular transaction involves the offer and sale of a security-regardless of the terminology used-will depend on the facts and circumstances, including the economic realities of the transaction."
- One of the types of investments that is listed as a security under the Securities Act is an investment contract

The Howey test

- The Howey Test is a test created by the United States Supreme Court for determining whether certain transactions qualify as investment contracts
- If so, then under the Securities Act, those transactions are considered securities and therefore subject to certain disclosure and registration requirements
- A transaction is considered an investment contract if
 - ① There exists an investment of money
 - ② The investment of money is in a common enterprise
 - ③ There exists an expectation of profits
 - ④ Any profit comes from the efforts of a promoter or third party

Federal Money Services Laws

- Some token sales may be characterized as unlicensed money transmitting businesses and hence may fall under the purview of the Financial Crimes Enforcement Network (FinCEN)
- FinCEN requires the registration of money services businesses, a term that is defined to include money transmitters
- A money transmitter can be either: (i) a person that provides money transmission services, or (ii) any other person engaged in the transfer of funds
- FinCEN published guidance on convertible virtual currencies (CVC) and tokens, stating that users of CVC are not money transmitters, but those who both issue and redeem CVC (administrators) and those who exchange CVC for either fiat or other CVC (exchangers) who accept and transmit funds as a business would be deemed money transmitters

Federal Tax Laws

- Tokens, whether CVC or other kinds of blockchain tokens, are generally treated as property for U.S. federal income tax purposes
- As a result, proceeds from a token sale are taxable to the entity selling the token
- Entities organized as corporations formed in the US will generally bear a heavy tax burden on the proceeds from the token sale; expect a combined federal and state tax rate between 35% and 50%
- Hence any sellers often incorporate offshore in low tax jurisdictions and exclude US citizens from the sales
- Some even go as far as registering as non-profit foundations, classifying proceeds as donations

The SAFT

- The SAFT is a framework intended to simplify investments in utility tokens by venture capital firms, hedge funds, and large holders of cryptocurrencies by navigating the federal securities and money-transmitter laws, provide greater flexibility for tax management
- It is based on the Simple Agreement for Future Equity (SAFE), which has been widely used to finance early stage companies for many years
- SAFT is intended to be used for ICOs by entities still in the development stage of their product and looking for funding
- The SAFT is designed to qualify as an investment contract divided in two separate events:
 - ① raising of money from institutional or other large investors to fund the development of a token-based platform, and
 - ② delivery of genuinely functional tokens to investors for later resale to the public

SAFT Transaction

- ① Developers publish their whitepaper, incorporate, and secure commitments from accredited investors
- ② Developers enter into a SAFT with the accredited investors relying on the exemption set forth in Rule 506(c) of Regulation D of the Securities Act, and the accredited investors transfer funds
 - Rule 506(c) of the Securities Act allows for general solicitation of investors, but requires that the offering must be limited, only to verified accredited investors
 - The SAFT offers investors a discount on the final token sale and is a security, so the developers file a Form D with the SEC disclosing the sale
- ③ The entity uses the proceeds to develop the network into a product that provides genuine utility to its users
- ④ The network is launched and tokens are delivered to the investors who begin sales of the token to the public, either directly or through exchanges

SAFT Criticism

- The framework assumes that its application will automatically qualify the transaction a security, however the SEC has repeatedly stated that the test for whether a particular instrument will be deemed a security depends only on the relevant facts, circumstances, and economic realities and not a defined set of rules
- Furthermore, SAFT purchasers are required to expressly disclaim any desire to use or consume the tokens for any purpose other than selling the tokens to earn an investment profit
- As a result this may emphasize the speculative, profit-generating aspects of the tokens being developed, in a way that could trigger federal securities law scrutiny well beyond the initial SAFT sale

SAFT Criticism

- SAFT also poses a risk of misaligning incentives among developers, SAFT holders, and other consumers who may own or purchase tokens for consumptive purposes
- The incentives of traditional equity investors are often aligned to support the long-term growth of a company and its valuation and equities are generally subject to robust transfer restrictions
- SAFT purchasers are incentivized to only profit from a short-term token sale event and this may contribute to cultivating an environment that incentivizes investors to push for a successful token sale more than a successful token-based platform
- This framework could therefore potentially make it more expensive for consumers to purchase tokens and participate on these networks and if widely used, could exacerbate speculation

Regulating ICOs

- In the UK, the Financial Conduct Authority (FCA) stated that whether an ICO falls within its regulatory boundaries will be determined on a case by case basis
- The decision ultimately depends on how the process is structured, given the parallels between IPOs and ICOs
- In China, after the ban was enacted, officials came out to explain that the suspension on ICOs and the government's declaration of ICOs as an illegal fund raising method are only temporary
- These measures were only intended to be in place until local financial regulators introduce necessary regulatory frameworks and policies for both ICO investors and projects
- They further explained that Chinese ICOs are likely to continue in a controlled environment, through a licensing program

Regulating ICOs

- The Financial Services Regulatory Authority (FSRA) in Abu Dhabi has released guidelines to bring clarity to its regulatory approach to ICOs
- Under the new guidelines, companies wishing to organize an ICO are now required to approach the FSRA which will determine if the token offering is to be regulated as a security
- If the FSRA determines that the token falls outside the definition of a security, the token offering will remain unregulated
- In Switzerland, the Crypto Valley Association (CVA) has developed an "ICO Code of Conduct"
- The framework is designed to promote self governance models for the ICO industry, taking into account all legal, moral and security obligations
- Furthermore, it aims to assist regulators in clarifying the exact function and legal and tax status of the tokens being issued



Smart contracts and contract law

- How smart contracts will interact with the law still remains unclear
- This uncertainty is partially due to the complexity brought about by the spectrum of possibilities for their use; ranging from contracts that simply automate implementation or performance of natural language contracts to contracts entirely written in code
- As a result, whether a smart contract will give rise to legally binding contractual relations may vary significantly depending on the contracting jurisdiction
- The commercial utility of smart contracts stems from the ability to automatically self-execute transactions in accordance with pre-coded instructions

Smart contracts and contract law

- In 2017, ten law firms and four legal institutions that specialize in blockchain technology joined the Enterprise Ethereum Alliance
- This collective includes the likes of BP, J.P. Morgan and Microsoft, with a focus on finding ways to use blockchain technology to run smart contracts at Fortune 500 companies
- This came weeks after the SEC released its first formal guidance on blockchain based assets that might also be regarded as securities
- These legal firms will be working to find ways that guarantee that smart contracts remain compliant to all current rules and regulations

HB 2417

- In May 2017, The State of Arizona passed HB 2417 into law, with the intention to encourage blockchain
- HB 2417 amends the Arizona Electronic Transactions Act (AETA), which stipulates that records or signatures in electronic form cannot be denied legal effect and enforceability based on the fact that they are in electronic form
- It clarifies that electronic records, electronic signatures and smart contract terms secured through blockchain technology will be considered to be in an electronic form and to be an electronic signature under AETA
- The statute also provides that a traditional contract may not be deemed illegal, invalid or unenforceable solely because that contract contains a "smart contract term"

Smart contracts and contract law

The following characteristics ought to be kept in mind when establishing how smart contracts will interact with the law

- Smart contracts are usually part of an application running on Distributed Ledger Technology (DLT), rather than standing alone as a DLT application
- Smart contracts are autonomous in that the software developer who created them does not actively have to maintain, monitor, or even be in contact with them while they operate
- Smart contracts guarantee execution of the contemplated transaction
- Smart contracts offer event-driven functionality that can be triggered by external data supplied by "oracles" - trusted data sources that send information to smart contracts

Smart contracts and contract law

- To date, most of the available legal analysis focuses on the use of computer code to articulate, verify and execute an agreement between parties
- Under a contract law analysis, key legal issues include notice, consent, and consumer protection
- Even fully self-executing contracts will ultimately need to make reference to legal terms and concepts that will define each party's rights if their relationship leads to litigation
- Enforceability is further complicated by the fact that personal service contracts are not subject to computer control e.g. delivery of physical commodity

Smart contracts and contract law

- With traditional contract law, it is possible to rescind or modify agreements with the assistance of a court, or voluntarily by the relevant parties. A smart contract on the other hand will always perform as it was intended to at the time of deployment due to the immutability of the blockchain
- This would present a significant limitation as it does not account for events that may occur outside the scope of the pre-coded contracting language that would potentially render contracts unenforceable in the legal sense
- This includes unforeseen events like war, a natural catastrophe or even an event occurring after the contract is formed that might make performance illegal
- The only possible remedy for a smart contract to be removed from the blockchain is through the use of the `selfdestruct` function

Smart contracts and contract law

- The legal status of Distributed Autonomous Organisations (DAOs) as entities- which are fundamentally smart contracts - still remains unclear
- DAOs also present challenges in the form of legal issues surrounding the ownership and liability
- There is also the matter of jurisdiction and applicable laws
- Where servers are decentralized and can be spread around the world, pinpointing where a breach or failure occurred may be complex in the event that legal action is required

Smart contracts and contract law

- The ambiguity of the law and subjectivity required in its interpretation means that certain contractual terms may not be fully expressed in code
- As a result, most of the literature is of the opinion that smart contracts will never fully replace natural-language law
- Rather, the emergence of smart contracts will lead to a re-evaluation of common practice, as lawyers and clients discover which types of agreements and terms are best suited to code, which should be left to natural language, and how to combine them to achieve the best of both worlds
- Authors also predict that conducting legal contracts through smart contracting computer code can bring clarity, predictability, auditability, and ease of enforcement to contractual relations

Recap

- Many regulatory authorities have yet to establish a definitive stance regarding the regulation of FinTech
- An emphasis is placed on consumer protection, without stifling innovation
- Authorities are largely concerned with FinTech platforms being used for malicious activity
- In the US, the OCC is responsible for overseeing and adapting the regulatory framework to support the growth of FinTech
- In Singapore, the MAS has set up a regulatory sandbox for developers to test their product

Recap

- The SAFT is a contract intentionally structured to qualify as a security, in order to make ICOs compliant to federal securities and money-transmitter laws and to provide token issuers greater flexibility when it comes to tax management
- Although SAFT appears to have its benefits, it could trigger federal securities law scrutiny well beyond the initial SAFT sale
- How smart contracts will interact with traditional law still remains unclear
- Within the current regulatory framework, smart contracts are best left to simple functions based on rules that are defined mathematically and enforced mechanically