Introduction to Blockchain Technology and the Crypto Assets Market

27th, Feb. 2019

Chapters

1. Overview of Blockchain Technology

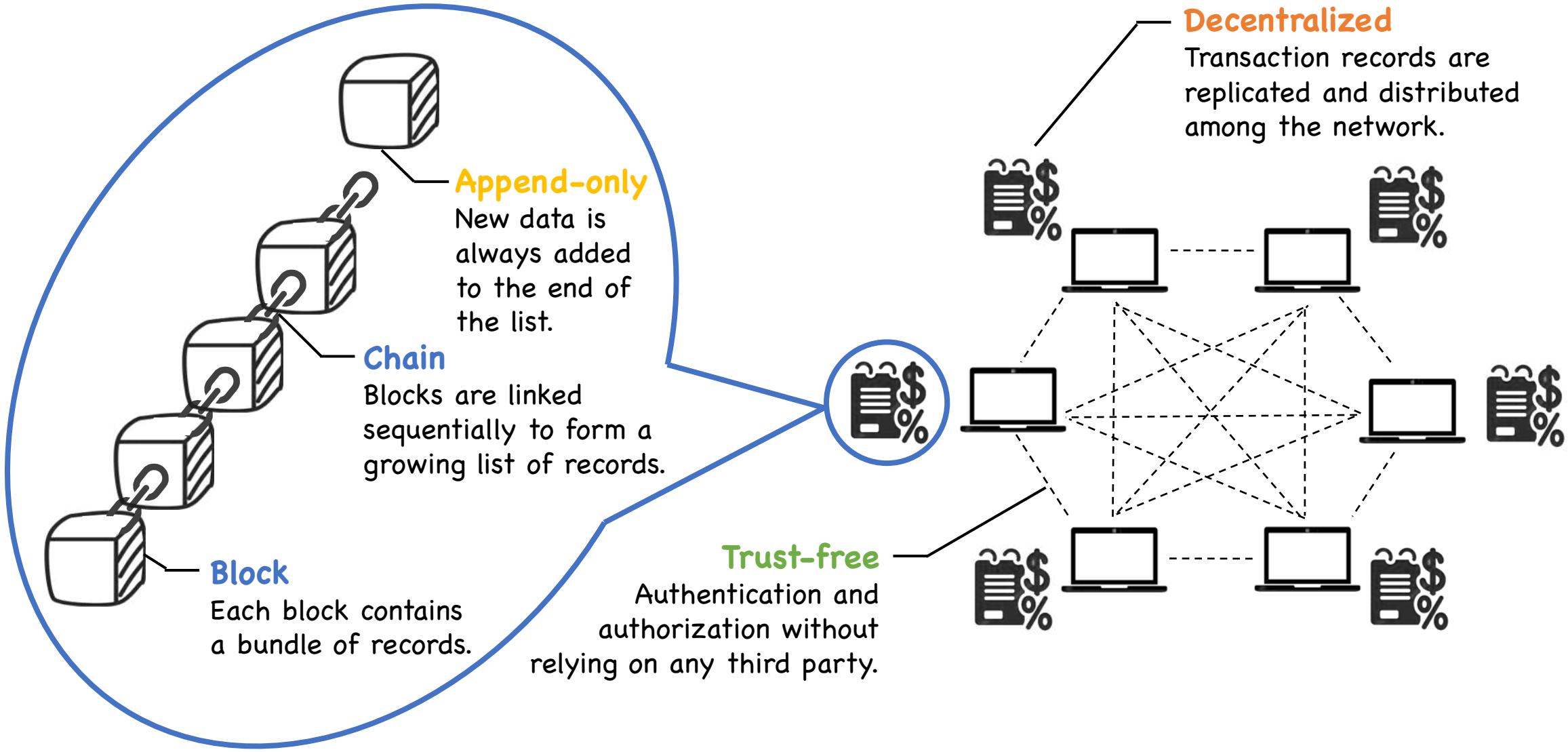
2. Underlying Technology of Blockchain

3. Blockchain Application: Crypto Assets

4. Use in Anti Money Laundering

What is blockchain?

Blockchain, literally "chain of blocks", is a distributed public database that records digital information.



How does blockchain work?

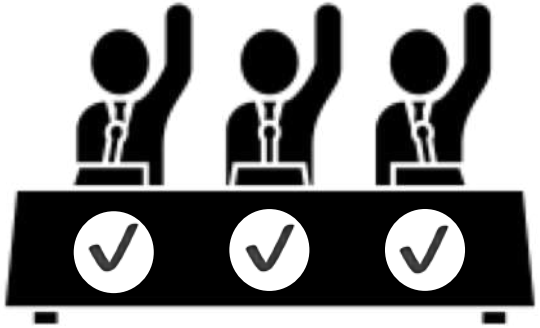
Instead of being a new technology, blockchain is actually an innovative combination of three proven technologies, which are public & private keys encryption, the Internet, and consensus protocols.

Cryptography

Private key provides an identity and ownership certification, whereas public key enables encrypted text to be openly viewed by all the participants in the network.

the Internet (Peer-to-peer Network)

Ledger copies are replicated and distributed through the internet. This kind of distributed structure enhances the anti-hacking ability.



Consensus Protocols (Incentive mechanism)

The independently verified consensus process validates any updates. Decisions are made by the whole network, and participants are rewarded for their contribution to maintain the system.

Several Easily Confused Concepts

Blockchain ≠ Bitcoin

Blockchain is the technology that powers Bitcoin, and Bitcoin is the first and currently the largest application of Blockchain. While this is the original purpose, blockchain is capable of much more and can be utilized to record and track anything of value. (i.e. financial transactions, properties' ownership, supply chain records, etc.)

Blockchain ≠ Initial Coin Offering (ICO)

Initial Coin Offering is a new way of fundraising, where projects utilizes blockchain to issue tokens, distribute them to investors in exchange of funds. Though with a new and fancy name, it is fundamentally a kind of crowdfunding, and again, blockchain is only the technology that support the whole thing.

Blockchain ≠ Anti Government

The true essence of blockchain is to take away the central point as well as intermediaries to realize the Internet of Value, but it doesn't necessarily lead to the conflicts against the government. Rather, Governments can also utilize blockchain technology to improve current systems, personal ID management as an example.

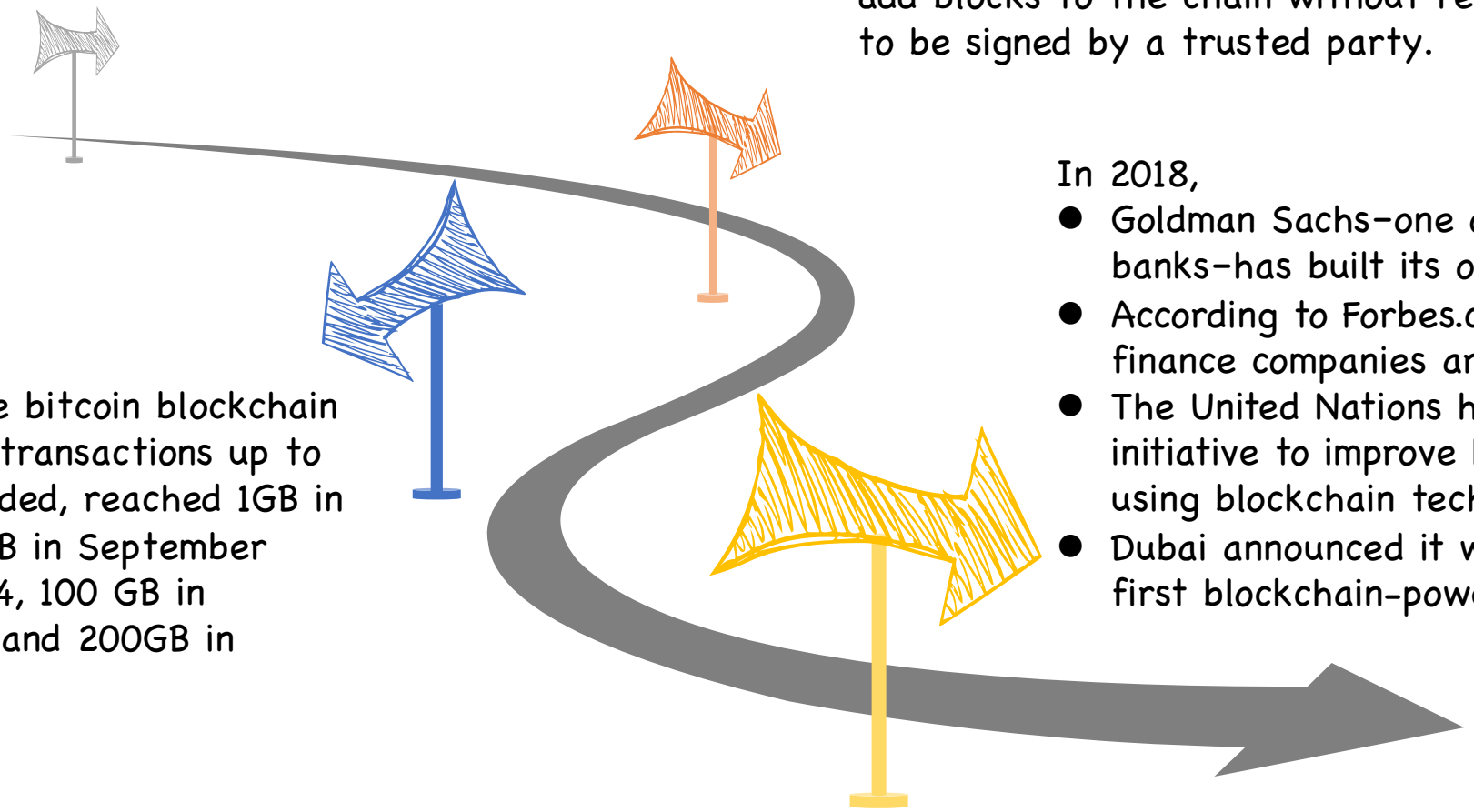
Blockchain ≠ Scam

It is true that in the last two years, the ICO is improperly used by many scammers to defraud the investors of their money, but it doesn't mean that the technology itself is a scam. Rather, blockchain provides us with the possibility of a totally new way to transact with each other in the digital era.

A Brief History of Blockchain

- The concept of a cryptographically secured chain of blocks was first proposed in 1991 by Stuart Haber and W. Scott Stornetta, though they end up with failure.

- The first blockchain was conceptualized by a person (or a group of people) known as Satoshi Nakamoto in 2008 in the invention of Bitcoin. Nakamoto improved the design with hashing to add blocks to the chain without requiring them to be signed by a trusted party.



- The size of the bitcoin blockchain file, where all transactions up to date are recorded, reached 1GB in May 2012, 10GB in September 2013, July 2014, 100 GB in January 2017, and 200GB in January 2019.

In 2018,

- Goldman Sachs–one of the world's largest banks–has built its own blockchain.
- According to Forbes.com, nearly 15% of finance companies are using blockchain.
- The United Nations has launched an initiative to improve humanitarian efforts using blockchain technology.
- Dubai announced it will be the world's first blockchain-powered government.

Use Cases of Blockchain (I)

Global Banking System

Blockchain based crypto assets enable easier, faster and cheaper cross-border money transfer. Also, the new system, along with digital identity verification, offers a solution for billions of people in developing countries who are still unbanked.

Government

Blockchain can store sensitive information, while also allowing view access without compromising the integrity of data. Allowing anyone to inspect government operation will certainly bring a new level of public oversight to governance.

Digital Identity

A single key matched against an immutable ledger enables a self-sovereign ID package that can store all types of information about an individual. These credentials can be utilized in various identity verification situations, alleviating the need to continually reproduce documents.

Personal Data Utilization

The decentralized feature removes the power from IT giants and shifts control of personal data back to the users. The choice to monetize the data and corresponding profits are retrieved, where worries about personal information abuse no longer exist.

Content Distribution

Blockchain can be the architecture for an effective content distribution platform, where intermediaries are eliminated and content creators are directly connected with consumers. Here, creators can truly earn the amount that belongs to them.

Use Cases of Blockchain (II)

Real Estate Transaction

Intermediaries have been necessary for decades to draw up, record and manage lease and purchase contracts, which is a labor-intensive, costly job. Applying blockchain can facilitates the reinvention and digitization of the real estate market.

Asset Tokenization

Blockchain tokens can act as the digital counterpart of assets in the real world, where anything can be tokenized. This kind of tokenization introduces the concept of fractional ownership which can improve the liquidity of costly assets such as real estate.

Energy Market

Blockchain enables the smart metering of electricity generated through an individual's solar panels to be recorded, traded and settled on a ledger. Thus, a less costly and more efficient market without a centralized grid can be realized.

Healthcare

A blockchain platform not only securely stores health records, but they enables different organizations including doctors, researchers and health insurers to request permission to access a patient's record to serve their purpose and record transactions on the distributed ledger.

Supply Chain Management

Blockchain helps solve the issue of transparency by acting as the single and immutable source of truth accessed by all the related parties, which is append-only and provides a time stamped audit trail from the beginning to the end.

Chapters

1. Overview of Blockchain Technology

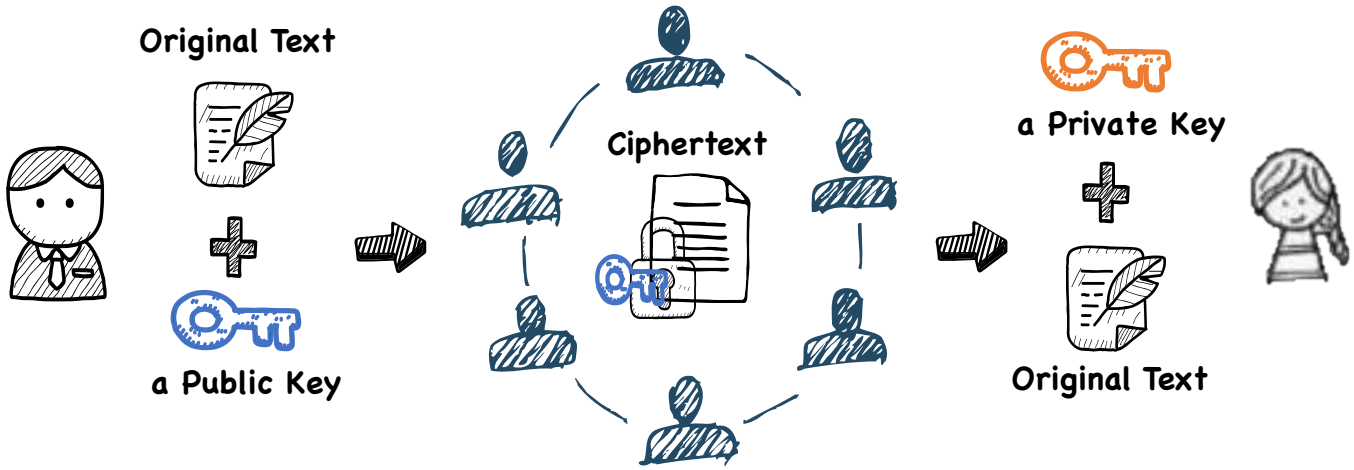
2. Underlying Technology of Blockchain

3. Blockchain Application: Crypto Assets

4. Use in Anti Money Laundering

Underlying Technology: Public & Private Keys Encryption

- Cryptography is the method of encrypting and decrypting the information through complex mathematics. The method involves taking unencrypted data and encrypting it using a mathematical algorithm, known as a cipher. This produces a ciphertext, a piece of information that is completely useless and nonsensical until decrypted.



- Encrypted information is transferred through a public key that can be shared with anyone, while the recipient who possess the only private key paired to the public key can decrypt the original message.
- By design, it is impossible for anyone to work out what the private key is based on the public key. Therefore, a user can send their public key to anyone without worrying that someone will gain access to the private key.

The cryptocurrency transfer using public & private key encryption (I)

A public key, also referred to as a wallet address, can be compared to an email address that anyone in the network could see.

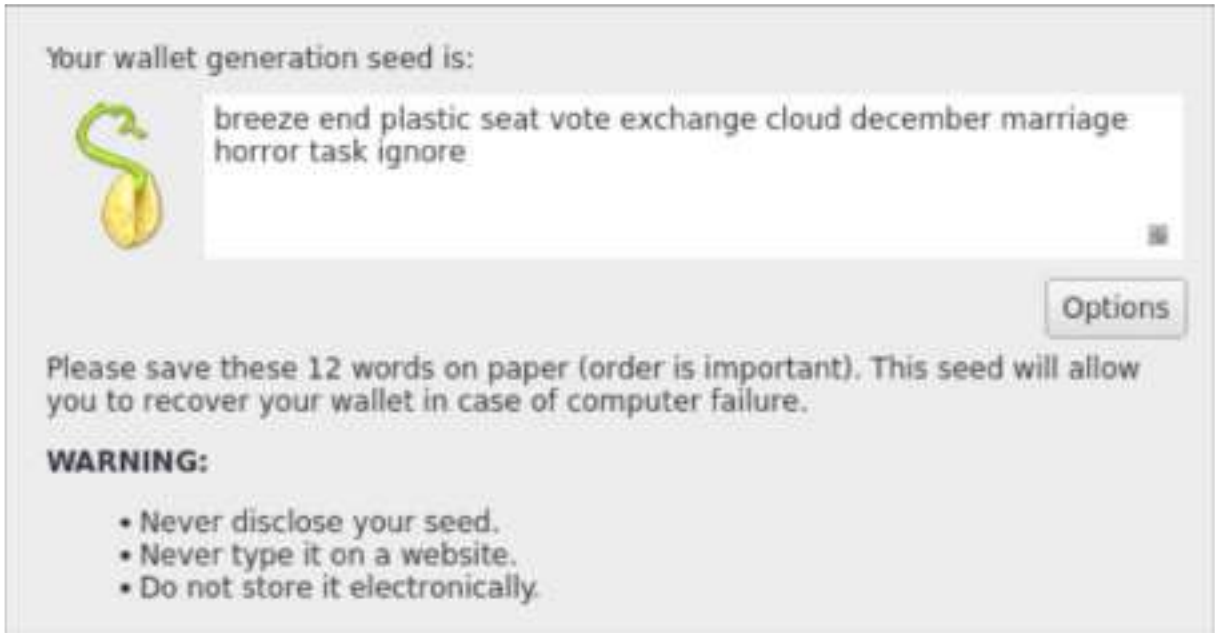
This Is Your Bitcoin Address

19emjx4vqHPn6ZTsh1ZNbBD7uFZFqWA5Cq

Share this with anyone and they can send you payments.

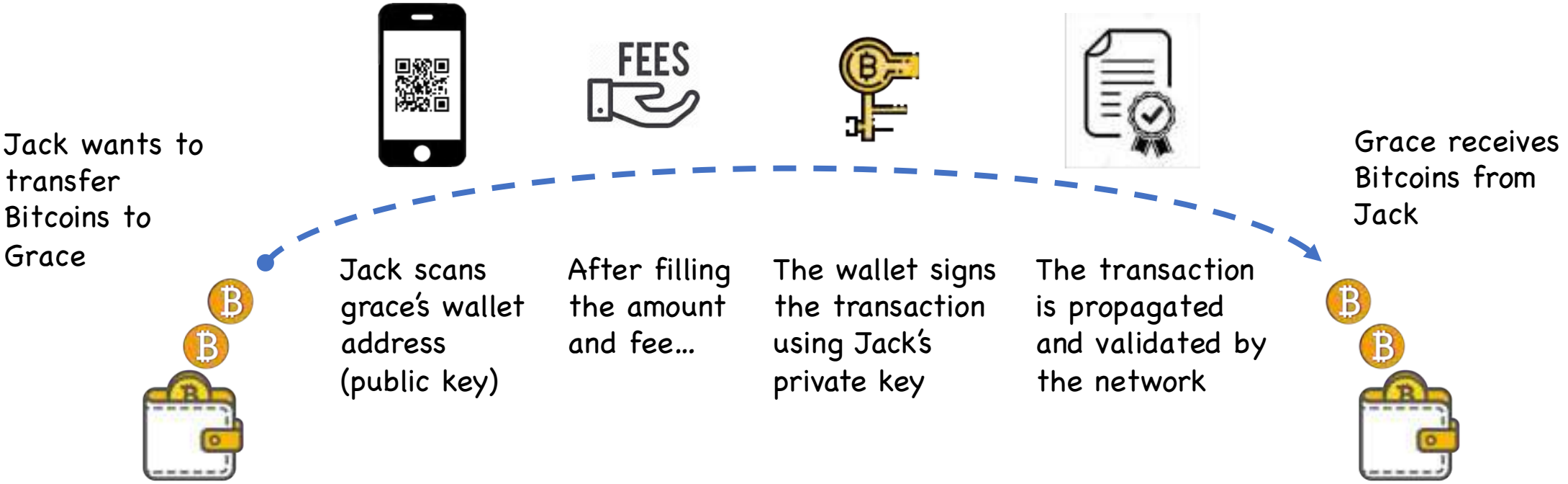
※ Only for demonstration purpose. Doesn't necessarily represent anything in reality.

A private key, often in the form of a combination of several irrelevant words in a certain order, is the password to this address. This password is only known by its holder and cannot be retrieved by anyone once forgotten.



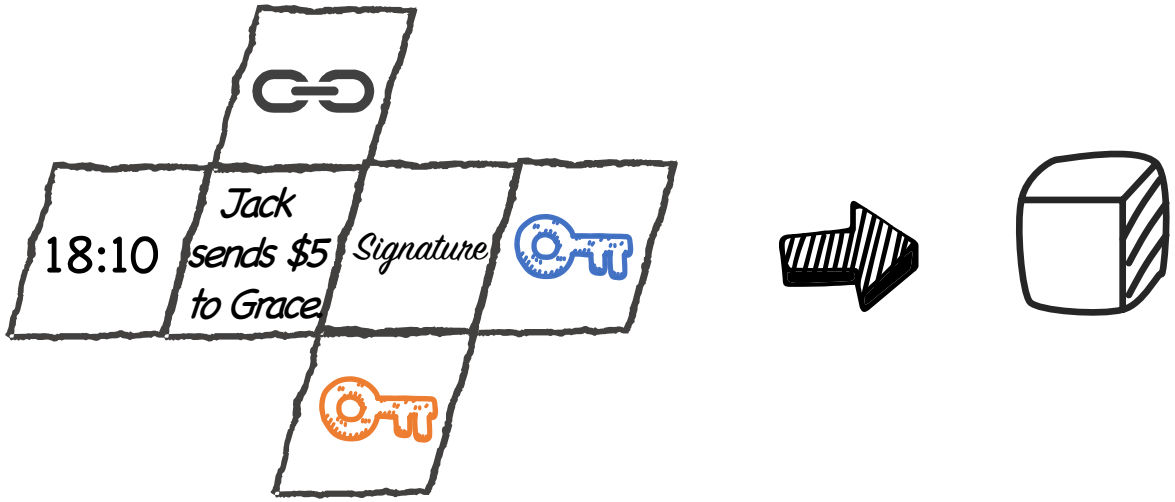
※ Only for demonstration purpose. Doesn't necessarily represent anything in reality.

The cryptocurrency transfer using public & private key encryption (II)



Underlying Technology: Digital Signature

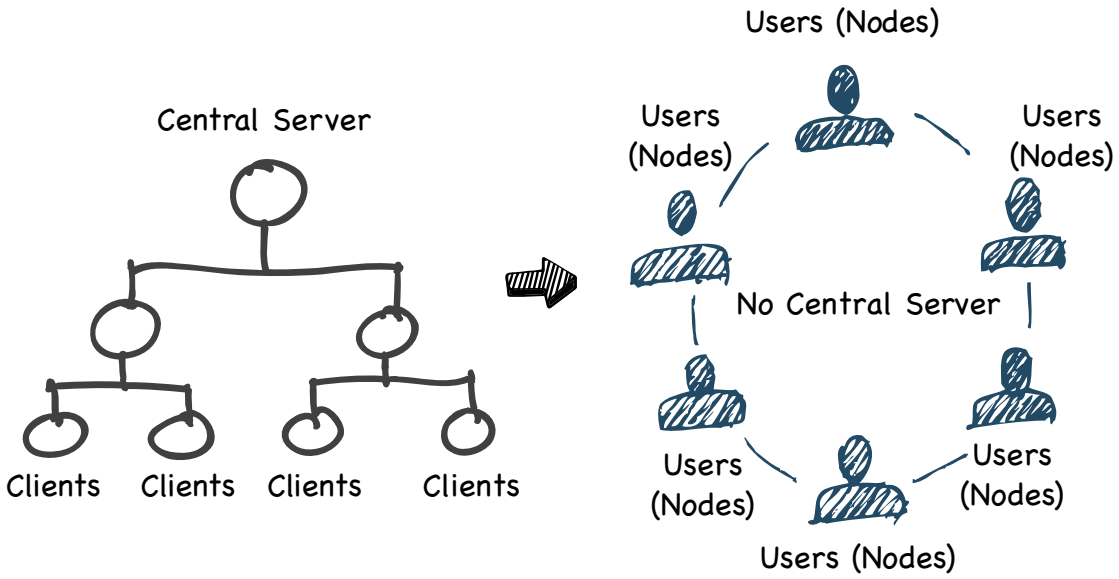
- Then, by combining the user's private key with the data that they wish to sign through a mathematical algorithm, a digital signature is produced. A digital signature stands for the ownership, thus guarantees one is communicating with whom he intends to, with only the least necessary personal information provided.
- Also, since the actual data itself is part of the digital signature, the network will not recognize it as valid if any part of it is tampered with, for unlawfully editing even the slightest aspect of the data will reshape the whole signature, making it false and obsolete. Through this, blockchain technology is capable of guaranteeing that any data being recorded onto it is true, accurate and untampered with.



- Furthermore, blockchain introduces multi-signature, which means that in order to approve a transaction a majority of parties are required to be in agreement to do so. Digital signatures are a key component in securing data on a blockchain, whereas nodes are the very foundations upon which the network itself is built.

Underlying Technology: Peer-to-peer Network & Decentralized Structure

- In a P2P network, the user utilizes and provides the foundation of the network simultaneously and voluntarily. Compared to the traditional client-server models that are common today, information is constantly recorded and interchanged between all of the participants on the network. Trust in all powerful third parties is no longer needed as users can rather deal directly with one another across a secure and distributed and decentralized network.



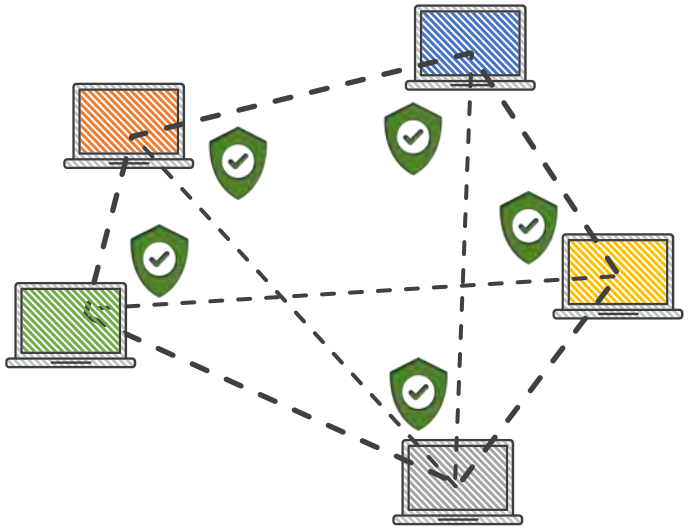
Advantages over Traditional Client-server Model

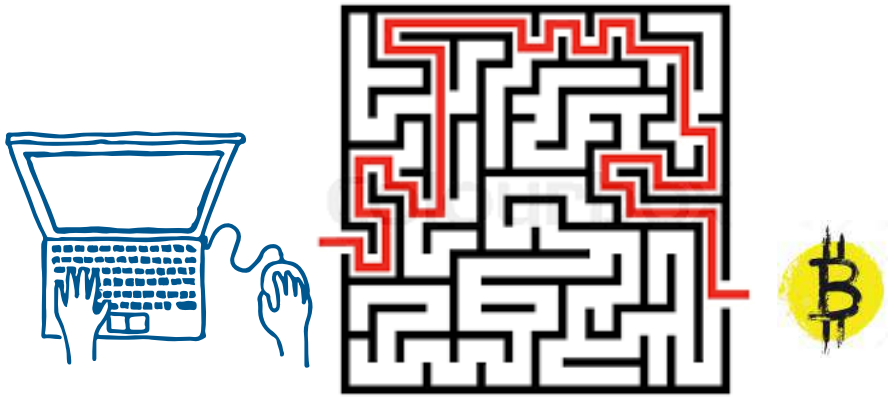
1. Data is less vulnerable to being hacked, exploited or lost
2. No need for a dominant authority, therefore no single party can control and use the network on own behalf
3. Users become the true owner of their personal data, which is controlled by service providers today
4. A centralized server model inevitably slows down when more users join it, while a P2P network actually improve its power with more devices joining the network

- A peer (often referred to as a node) makes a portion of its computing resources available to other participants without the need for any central server to coordinate. The role of a node is to support the network by maintaining a copy of a blockchain and, in some cases, to process transactions. In return, they have the chance to collect the transaction fees and earn a reward in the underlying cryptocurrency for doing so, which is known as mining.

Underlying Technology: Consensus Protocol & Rewarding Mechanism

- A consensus protocol is one of the most important and revolutionary aspects of blockchain. It creates an irrefutable system of agreement between various devices in a distributed network to make it a constantly updated self-auditing ecosystem, whilst prevents any single entity from controlling or derailing the whole system. The aim of consensus rules is to guarantee a single chain is used and followed.
- The most famous consensus protocol is called Proof of work (abbreviated to PoW) which was first introduced by Bitcoin. It comes in the form of an answer to a mathematical problem, one that requires considerable work to arrive at, but is easily verified to be correct once the answer has been reached.
- The process to find the answer is known as mining and the nodes on the network are known as "miners". Miners run a long and random process of presenting answers on a trial and error basis, and the miner who manages to solve the riddle mines the next block, adding it to the chain and validating the transactions within it, and receiving the reward associated with the block in the form of Bitcoin. Keeping these miners incentivized is a key function of a protocol as they are in a sense the foundation that keeps the system running.

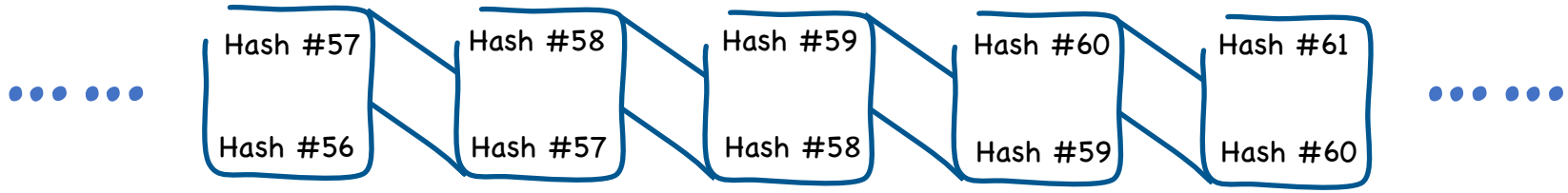




Underlying Technology: Hashing

- Hashing is the process of taking an input of any length and turning it into a cryptographic fixed output through a mathematical algorithm. It is what realizes the irrefutable security of blockchain, with its major functions directly associated with the features of blockchain as a whole:

1. The same message will always produce the same hash value, and it is impossible to produce the same hash value for differing inputs. Each new block contains the hash of itself as well as the hash of the block before it, thus blocks are linked one after another to form a chain. In other words, the latest state of blockchain is based on and authenticated by all previous transactions.
2. Impossible to determine input based on hash value. This is the prerequisite for the transparent nature as well as the consensus protocol of blockchain. Since all participants have a copy of the entire blockchain, they can detect any tampering. So when the hashes match up across the chain, all parties know that they can trust their records.
3. Even the slightest change to an input completely alters the hash. If a hacker wants to change the data on a existing block, he has to update all the block afterwards in order to cover the track of manipulation.
4. Quick to produce a hash for any given message, but finding the only target hash requires considerable power input. It is considered theoretically impossible for a hacker to acquire more computational power than the rest of the network combined. Thus, data on blockchain is considered immutable.



Chapters

1. Overview of Blockchain Technology

2. Underlying Technology of Blockchain

3. Blockchain Application: Crypto Assets

4. Use in Anti Money Laundering

Cryptocurrency Market at a Glance

Today's Cryptocurrency Market Total Capitalization ⇒ 121 Billion USD [1]

(Peak Value on Jan. 7th, 2018 ⇒ 814 Billion USD)

Which means that it accounts for ……

Total U.S. Currency in Circulation [2]
by the end of Jan. 2019
⇒ 1.7 Trillion USD $\frac{1}{15}$

World's Total Gold Reserve [3]
by the end of 2017
⇒ 8 Trillion USD $\frac{1}{70}$

World's Stock of Narrow Money (M1) [4]
by the end of 2017
⇒ 43 Trillion USD $\frac{1}{350}$

World's Stock Market Capitalization [5]
by the end of 2018
⇒ 69 Trillion USD $\frac{1}{600}$

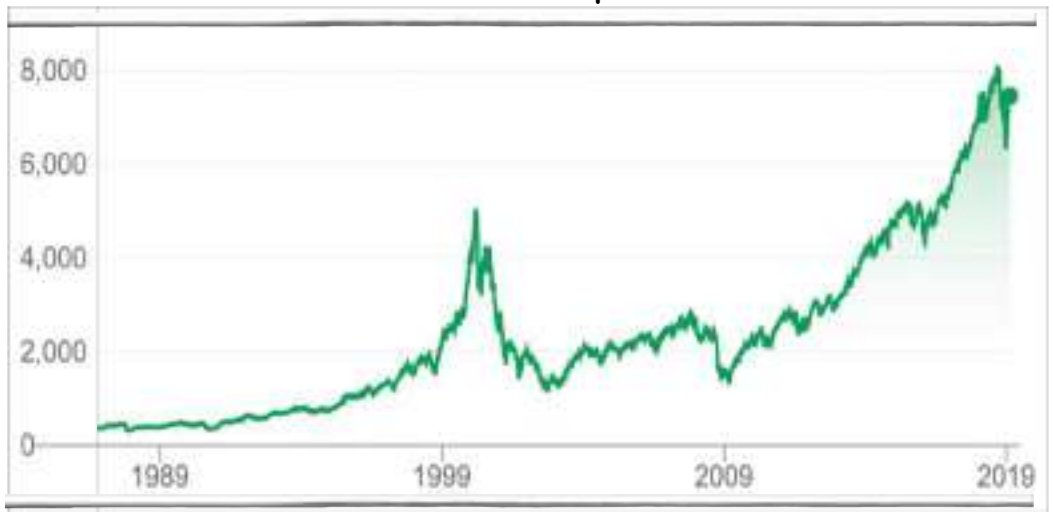
World's Total GDP [6]
by the end of 2018
⇒ 84 Trillion USD $\frac{1}{700}$

World's Total Value of Real Estate [7]
by the end of 2017
⇒ 280 Trillion USD $\frac{1}{2300}$

1. **CoinMarketCap:** https://coinmarketcap.com/charts/
2. **Federal Reserve:** https://www.federalreserve.gov/faqs/currency_12773.htm
3. **World Gold Council:** https://en.wikipedia.org/wiki/Gold_reserve; https://www.gold.org/goldhub/data/gold-prices
4. **Central Intelligence Agency:** https://www.cia.gov/LIBRARY/publications/the-world-factbook/rankorder/2214rank.html
5. **ET Intelligence Group:** https://economictimes.indiatimes.com/markets/stocks/news/world-stocks-lost-13-trillion-in-2018/articleshow/67280681.cms
6. **World Bank & International Monetary Fund:** https://data.worldbank.org/indicator/NY.GDP.MKTP.CD; https://www.imf.org/en/Publications/WEO/Issues/2019/01/11/weo-update-january-2019
7. **Savils:** https://en.crimerussia.com/gromkie-dela/cost-of-all-real-estate-in-the-world-reaches-280-trillion-dollars/

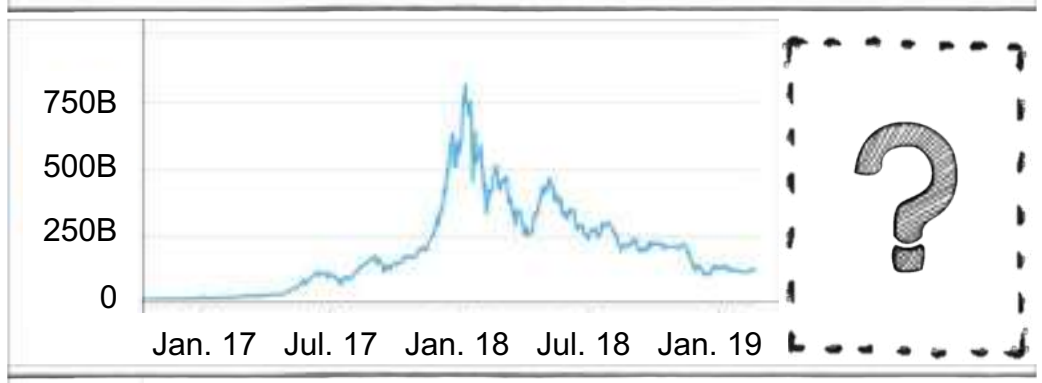
DotCom Bubble VS. Today's Cryptocurrency Market

NASDAQ Composite



Source: Yahoo Finance

Cryptocurrency Total Market Capitalization (US$)



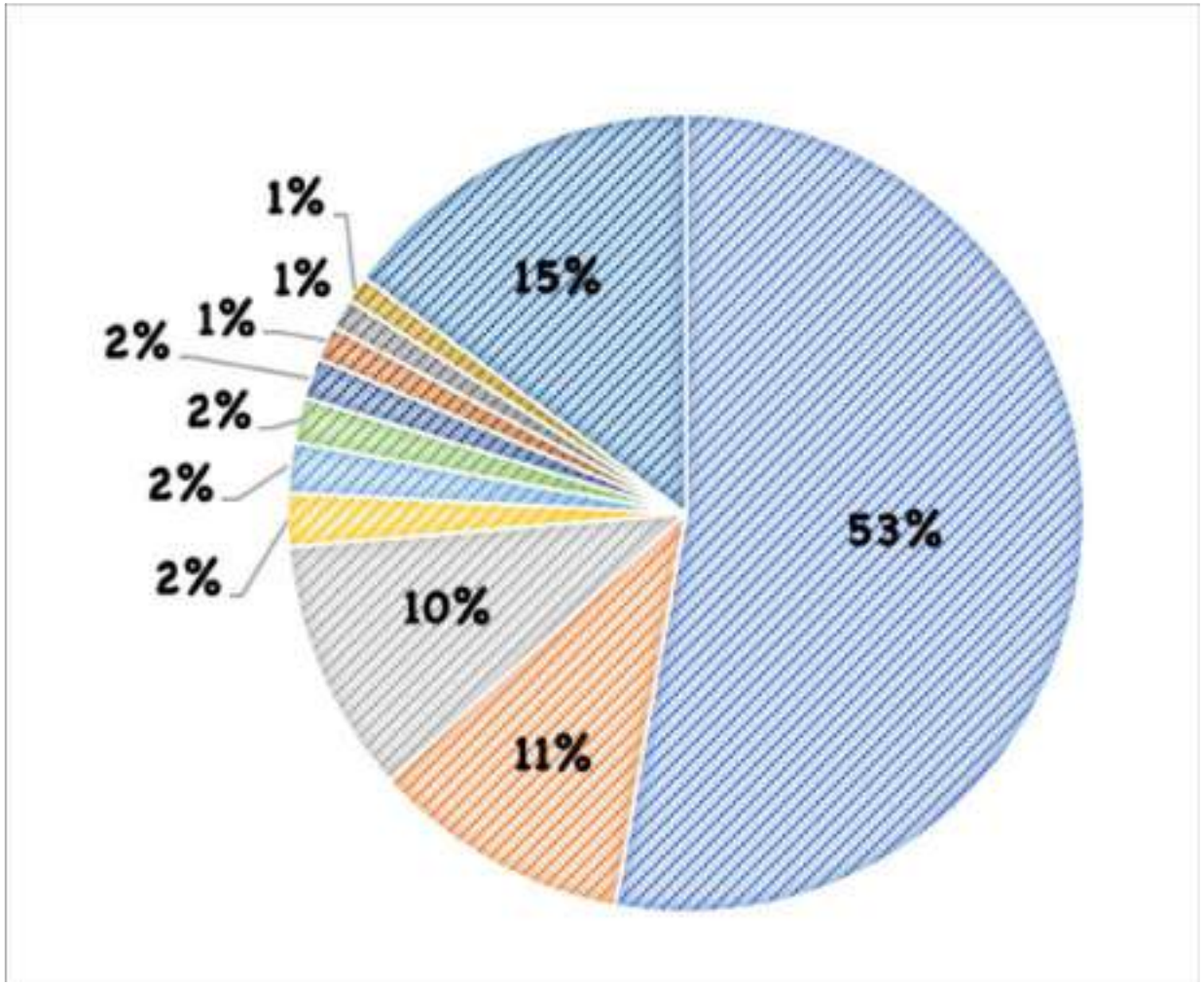
Source: CoinMarketCap

- When the dotcom bubble burst in 2000, the world-changing ideas didn't just float away- rather, they developed and eventually considerably reshaped our lives.
- Amazon is the best fitting example of the long-term recovery process of NASDAQ. It saw its stock price peak in late 1999 at just over $113, and was traded for under $6 in Sep. 2001. Today, its stocks are worth more than $1,600.
- On the contrary, many others such as Pets.com (pet supplies), Geocities (web hosting services), Boo.com (clothing and cosmetics) and Kozmo (fast delivery services), to name a few, are now nothing more than a distant memory.
- The total market capitalization of the cryptocurrency markets has followed a similar path to that of the Dot.com bubble till now. Will the cryptocurrency market go the same way as the recovery and further development of NASDAQ?

⇒ **The rise and fall of the Dot.com bubble illustrates that only those startups with an underlying product or service that offered real-world value would ultimately stand the test of time.**

Cryptocurrencies with Top 10 Market Capitalization

- Bitcoin: 64.0 Billion USD
- Ethereum: 12.7 Billion USD
- XRP: 12.5 Billion USD
- Litecoin: 2.6 Billion USD
- EOS: 2.5 Billion USD
- Bitcoin Cash: 2.2 Billion USD
- Tether: 2.0 Billion USD
- TRON: 1.7 Billion USD
- Stellar: 1.5 Billion USD
- Binance Coin: 1.3 Billion USD
- Others: 18.1 Billion USD



Source: CoinMarketCap, https://coinmarketcap.com

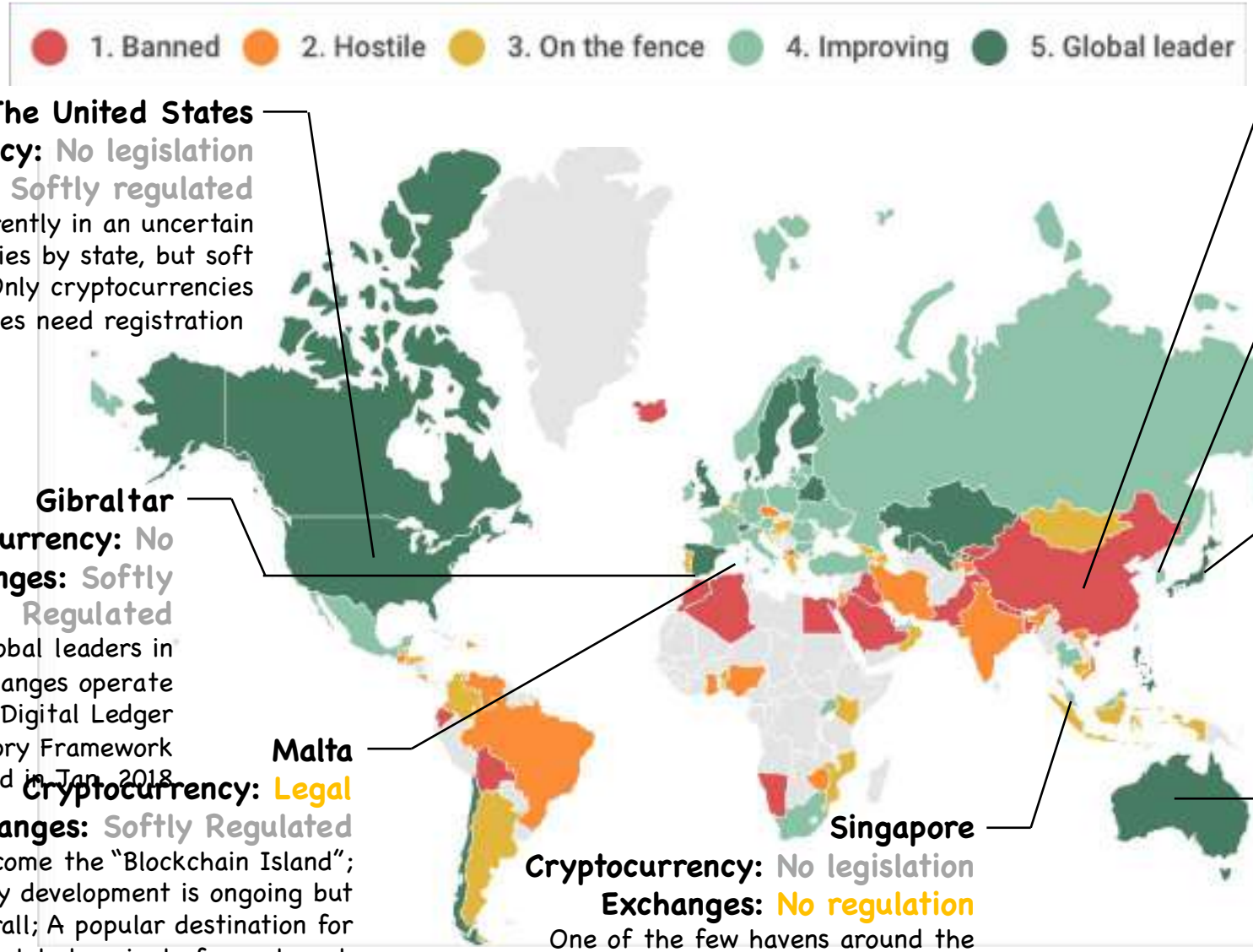
Brief Introduction to Top 10 Cryptocurrencies

bitcoin	Finance	Bitcoin (BTC) is a purely peer-to-peer version of electronic cash, based on a consensus network powered by its users, which requires no central authority to operate and no financial institution to involve in money transfer process.
ethereum	Development Platform	Ethereum (ETH) is the pioneer for blockchain based smart contracts, which is a self-operating computer program that automatically executes when specific conditions are met without any possibility of downtime, censorship, fraud or third-party interference. It is also a platform that enables developers to build decentralized applications (dapps).
ripple	Finance	Ripple (XRP) is an independent digital asset that is native to the Ripple Consensus Ledger. With proven governance and the fastest transaction confirmation of its kind, XRP aims to be the most efficient settlement option for financial institutions and liquidity providers seeking global reach, accessibility and fast settlement finality for interbank flows.
EOS	Development Platform	EOS is a smart contract platform and decentralized operating system intended for the deployment of industrial-scale decentralized applications through a decentralized autonomous corporation model. The EOS software provides accounts, authentication, databases, asynchronous communication and the scheduling of applications.
litecoin	Finance	Litecoin is a peer-to-peer cryptocurrency created based on the Bitcoin protocol but uses a different memory intensive hashing algorithm called Scrypt Proof of Work, which allows consumer-grade hardware such as GPU to mine the coins.

Brief Introduction to Top 10 Cryptocurrencies

Bitcoin Cash	Finance	Bitcoin Cash (BCH) is hard fork, a community-activated update to the protocol or code, of Bitcoin that took effect on August 1st, 2017. It increased the block size limit from 1MB to 8MB to help the scale the underlying technology of Bitcoin. On Nov 16th 2018, BCH was hard forked again and split into Bitcoin ABC and Bitcoin SV, where Bitcoin ABC became the dominant chain and took over the BCH ticker as it had more hash power and majority of the nodes in the network.
tether	Finance	Tether (USDT) is a designed to be stable cryptocurrency with a value equal to 1 USD. It is issued by a private company called Tether Limited instead of any official institution, but it is widely used as if digital dollars in the cryptocurrency market at present.
TRON	Content Platform	TRON (TRX) aims to build an truly decentralized internet and global free content entertainment system that could enable developers to create smart contracts and decentralized applications, freely publish, own, and store data and other content.
STELLAR	Finance	Stellar (XLM) is a payment technology that aims to connect financial institutions, payment systems and people of all income levels and provide a drastically cost-reduced and time-saved cross-border transfers, based on an open source and distributed network.
BINANCE COIN	Finance	Binance Coin (BNB) is the cryptocurrency of the Binance platform, the world's largest cryptocurrency exchange based in Hong Kong, which can be used to enjoy a transaction fee discount. Also, as a incentive mechanism, Binance plans to use 20% of its profits each quarter to buy back and burn BNB, until 50% of the total BNB supply is burned.

Cryptocurrency Regulation around the World



The United States
Cryptocurrency: No legislation
Exchanges: Softly regulated
Regulations are currently in an uncertain legal territory and varies by state, but soft in general; Only cryptocurrencies categorized as securities need registration

Gibraltar
Cryptocurrency: No legislation **Exchanges:** Softly Regulated
One of the global leaders in regulation; Exchanges operate within a well-defined Digital Ledger Technology Regulatory Framework released in Jan. 2018

Malta
Cryptocurrency: Legal
Exchanges: Softly Regulated
Aims to become the "Blockchain Island"; Regulatory development is ongoing but friendly overall; A popular destination for blockchain related projects from abroad.

Source: CryptoFinder, https://www.finder.com/global-cryptocurrency-regulations

Singapore
Cryptocurrency: No legislation
Exchanges: No regulation
One of the few havens around the world for free cryptocurrency trading; Cryptocurrencies are not considered a legal tender yet

China
Cryptocurrency: Illegal
Exchanges: Illegal
World's most harsh regulations; Banned ICOs and domestic exchanges in Sep. 2017

South Korea
Cryptocurrency: No legislation
Exchanges: Softly regulated
Still, the supervision body imposed tighter reporting obligations on bank accounts held by exchanges in 2018

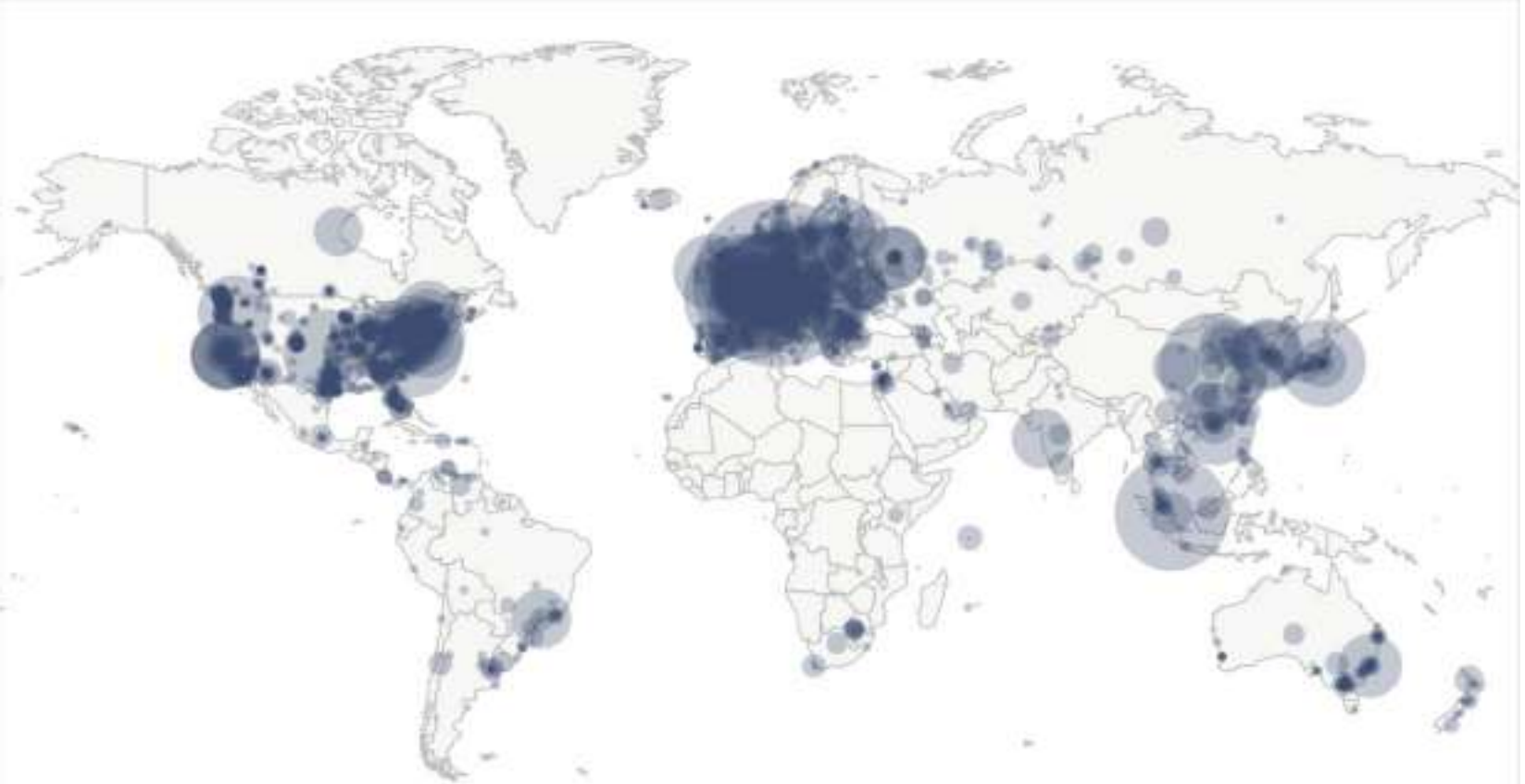
Japan
Cryptocurrency: Legal
Exchanges: Strictly Regulated
World's most progressive regulatory climate, but growing Concerns from the supervision body for AML and security & internal management of exchanges

Australia
Cryptocurrency: Legal
Exchanges: Softly regulated
Stated cryptocurrencies be treated as property; unregistered exchanges will be subject to criminal charges and financial penalties from 2018

Global Bitcoin Nodes Distribution

Reachable nodes around the world as of 24th, Feb 2019: **10356 Nodes**

The US	2531 (24.44%)
Germany	1904 (18.39%)
France	710 (6.86%)
Netherlands	533 (5.15%)
China	412 (3.98%)
Canada	407 (3.93%)
The UK	349 (3.37%)
Singapore	287 (2.77%)
Russia	267 (2.58%)
Others	253 (28.53%)



Source: BitNodes, https://bitnodes.earn.com

Chapters

Cryptocurrencies & Money Laundering

Blockchain-based cryptocurrencies are frequently labelled as a tool for money launderers. However, the facts are:

- The majority of users are investors and technological enthusiasts who wish to support this new technology.
- The real anonymity cannot be achieved since cryptocurrency exchanges, where cryptocurrencies can be exchanged to fiat money and vise versa, conduct KYC (Know Your Customer) verification
- Cryptocurrency transactions do carry a high level of risk being scrutinized retrospectively, for the blockchain ledger is unalterable
- Blockchain actually makes it possible to monitor complex transactions in an automated and effective manner, as well as immutably record audit trails of suspicious transactions across the system.

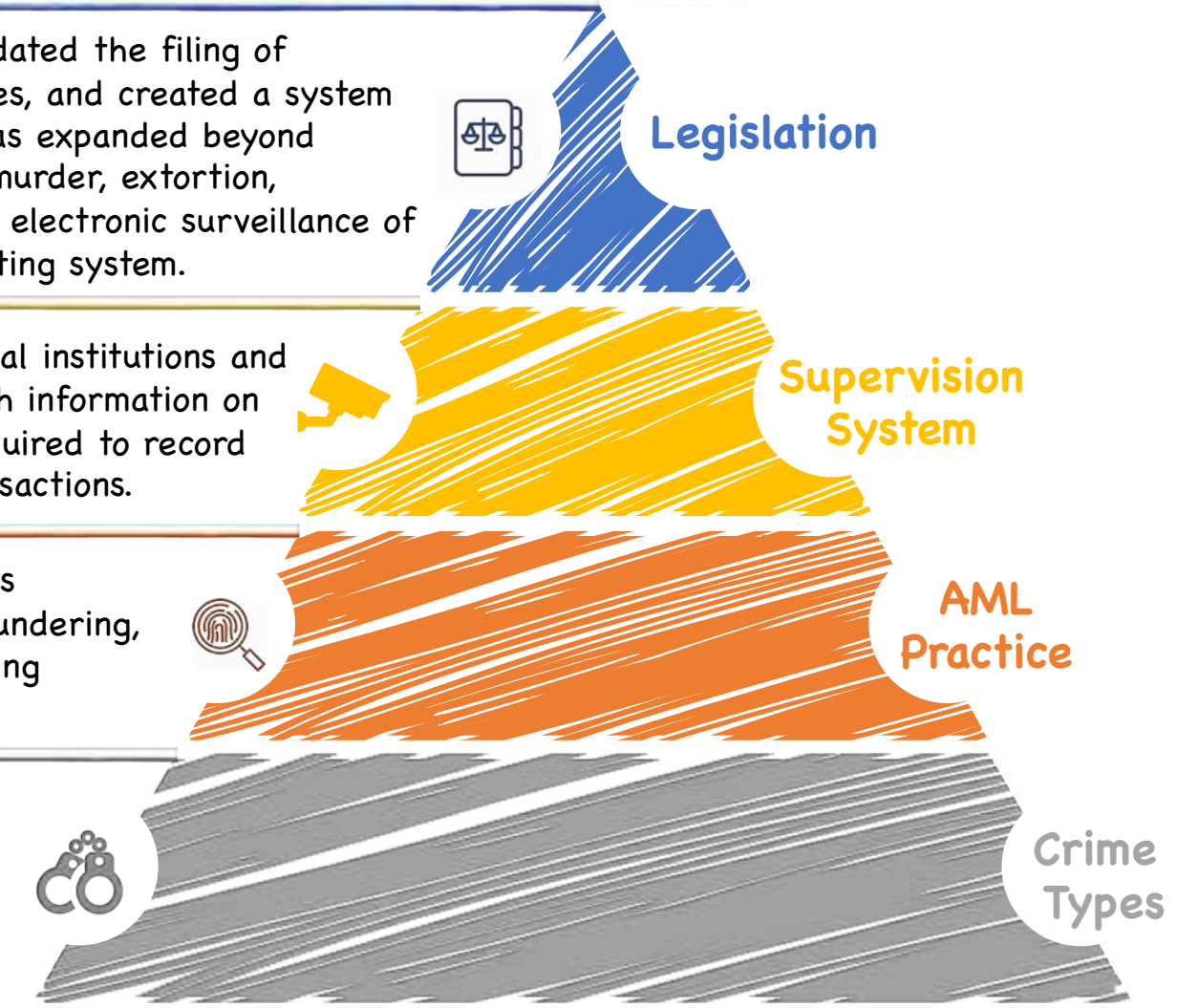
Japan's Current AML Circumstances

The Anti-Drug Special Law first took effect in July 1992, which mandated the filing of suspicious transaction reports for suspected proceeds of drug offenses, and created a system to confiscate illegal profits gained through drug crimes. The range was expanded beyond narcotics trafficking to include money laundering predicates such as murder, extortion, fraud,etc. The 1999 Anti-Organized Crime Law, which also authorized electronic surveillance of organized crime members, enhanced the suspicious transaction reporting system.

Japan's Financial Services Agency (FSA) monitors public-sector financial institutions and securities transactions, and provides law enforcement authorities with information on suspicious transactions reported by financial institutions, who are required to record and report the identity of customers engaged in large currency transactions.

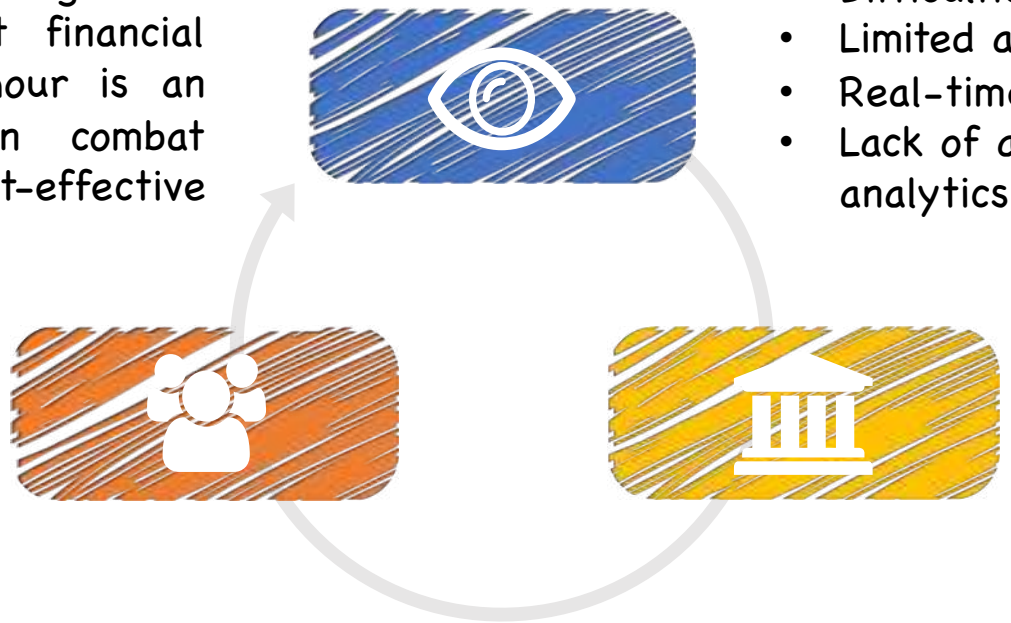
As a member of the Financial Action Task Force (FATF), Japan requires financial institutions to develop programs to combat against money laundering, which include internal policies designs, procedures and controls, ongoing employee training programs, and audit functions to test the system.

The principal sources of laundered funds are narcotics trafficking and financial crimes (illicit gambling, loan-sharking, extortion, abuse of legitimate corporate activities, internet fraud schemes, and all types of property-related crimes), which are often linked to Japan's organized criminal organizations.



Challenges in Current AML System

On the one hand, the existing transaction monitoring systems based on traditional technology are unable to keep pace with the growing volume and complexity of financial transactions; on the other hand, money launderers are constantly discovering more innovative ways to conduct illicit financial transactions. The need of the hour is an innovative technology which can combat money laundering in a scalable, cost-effective and comprehensive manner.



For Regulators & Auditors

- Lack of standardization
- Difficulties in global collaboration
- Limited access to firsthand data
- Real-time monitoring impossible
- Lack of automation, end-to-end analytics and visualization capabilities

For Corporations & Users

- Poor customer experience (same information asked to provide over and over again)
- Long on-boarding time
- Different requirements from bank to bank
- Challenge in meeting the ever-increasing scale and rate of regulatory change

For Financial Institutions

- Costly to carry out
- Time and labor consuming
- Opportunity cost of new revenues
- Redundant documents
- Regulatory risk (fines and even shutdown for non-compliance)
- Reputational risk

Blockchain utilization proposed: what can it bring to all participants?

By having a single integrated system using blockchain as well as smart-contracts with built-in algorithms,

- Financial institutions can securely parse data through an AML engine on the blockchain, with the automation providing high efficiency and ensuring minimum friction. Suspicious activities can be detected and highlighted to all related participants, while alerts can then be issued to stakeholders and the transaction then automatically be flagged and stopped for further investigation.
- The burden of each bank can be significantly reduced, which leads to faster onboarding and better customer experience. Corporations also benefit from reduced paperwork by doing KYC once and sharing it with all relevant financial institutions through a user-controlled consent model, where customers can dictate at which time and with whom they want to share information, without the need of a intermediary to be involved in the middle.

Thanks for your attention!