# ITU Asia-Pacific Centre of Excellence Training On "Distributed Ledger Technologies (Blockchain) Ecosystem and Decentralization"

3-6 September 2018,
Bangkok, Thailand

Dr. Jean-Marc Seigneur, jean-marc.seigneur@reputaction.com

# Dr. Jean-Marc Seigneur

- 100+ Scientific Publications Worldwide
  - Online Reputation Management (ORM)
  - Computational Trust Expert
  - Attack-resistant Consensus Algorithms
- Academic Member of the ITU
- Director of the Certificate of Advanced Studies (CAS) in Decentralized App Development with Blockchain & DLT at University of Geneva
  - https://www.cas-blockchain-certification.com
- President of Reputaction SAS
- Google Award of Excellent Research in Academia received in 2016

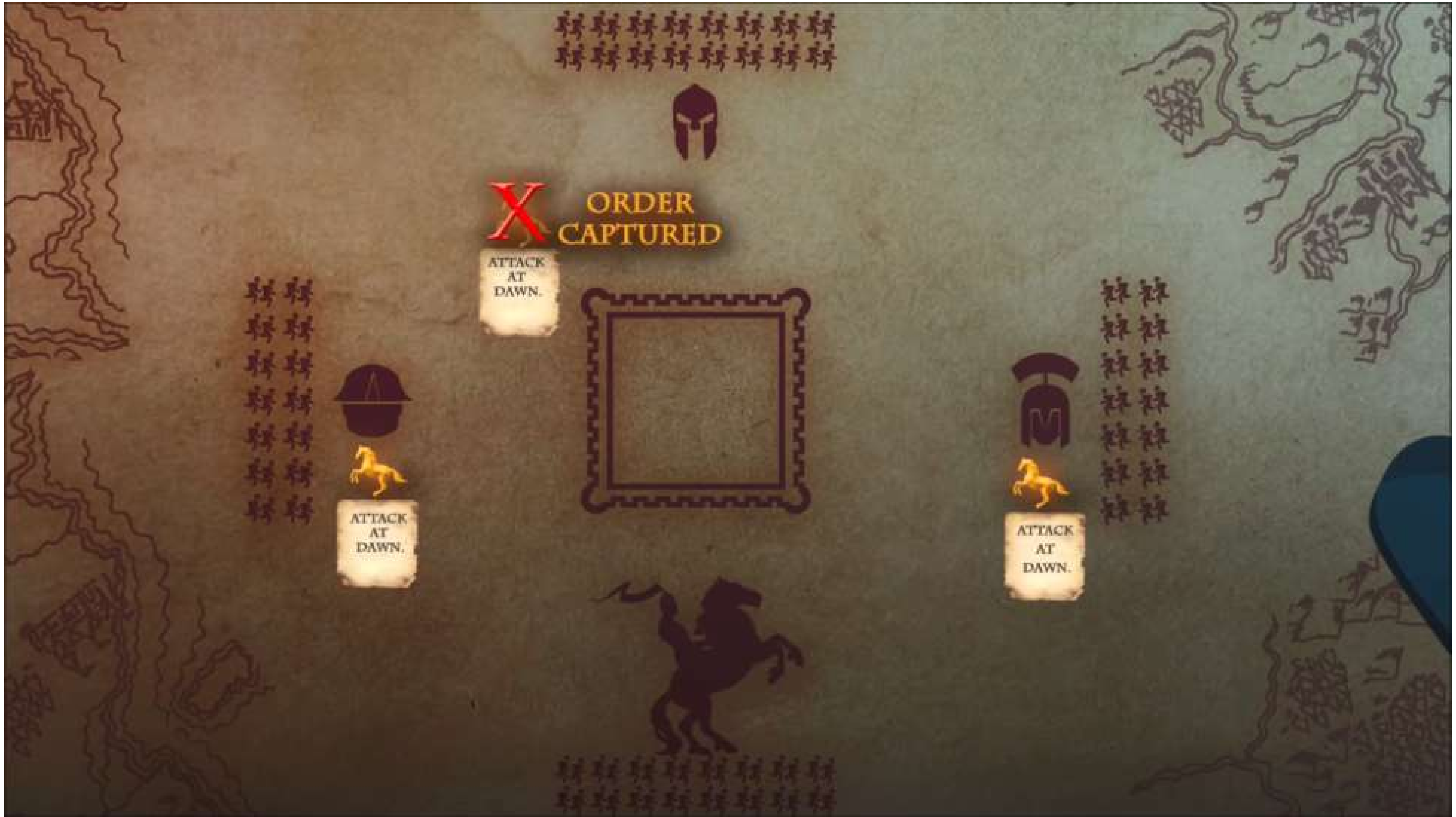
# Bibliography

- “The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order”, Paul Vigna and Michael J. Casey
- “Blockchain: Blueprint for a New Economy”, Melanie Swan
- “Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money”, Mark Gates
- “Blockchain Technology Explained: The Ultimate Beginner’s Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts”, Alan T. Norman
- “Mastering Bitcoin: Programming the Open Blockchain”, Andreas M. Antonopoulos
- “Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners”, Chris Dannen
- “Hasgraph vs Blockchain: The Future of Cryptocurrency”, Stephen Keller

# Agenda

- Understanding the technology behind DLT
- Overview of current DLT development platforms
- How to select the most appropriate DLT for a specific dApp
- Overview of current cryptocurrencies and tools
- Initial Coin Offering (ICO), Token Generation Event (TGE) and tokenomics
- DLT trends

# Byzantine Generals Consensus Problem



[Mike Maloney, Hidden Secrets of Money]

# Exercise with 2 Generals

[Pixabay, Bungie]

# Byzantine Generals Solutions

- Lamport et al.'s Byzantine Generals Problem publication, 1982
- Solutions may exist under various assumptions but they are expensive in amount of time and messages required
  - Oral messages: No solution with fewer than 3f+1 generals can cope with more than f traitors (no solution for 3 generals including 1 traitor)
  - Signed message: No solution with fewer than f+2 generals can cope with more than f traitors
- One potential implemented solution is called Practical Byzantine Fault Tolerance (PBFT) by Castro et Likov in 1999. It requires to have a membership list and selection of a leader in a round-robin fashion, thus it isn't fully permissionless. Each party maintains an internal state. When a party receives a message, they use the message with their internal state to run a computation. This computation will lead to this party's decision about the message. Then, the party will share the decision with all other parties in the network. The final decision is determined based on the total decisions from all parties. A high hashrate is not required in this process because PBFT relies on the number of nodes to confirm trust. Once enough responses are reached, e.g., more than two-third, the transaction is verified to be a valid transaction: there is no need to wait for confirmations.

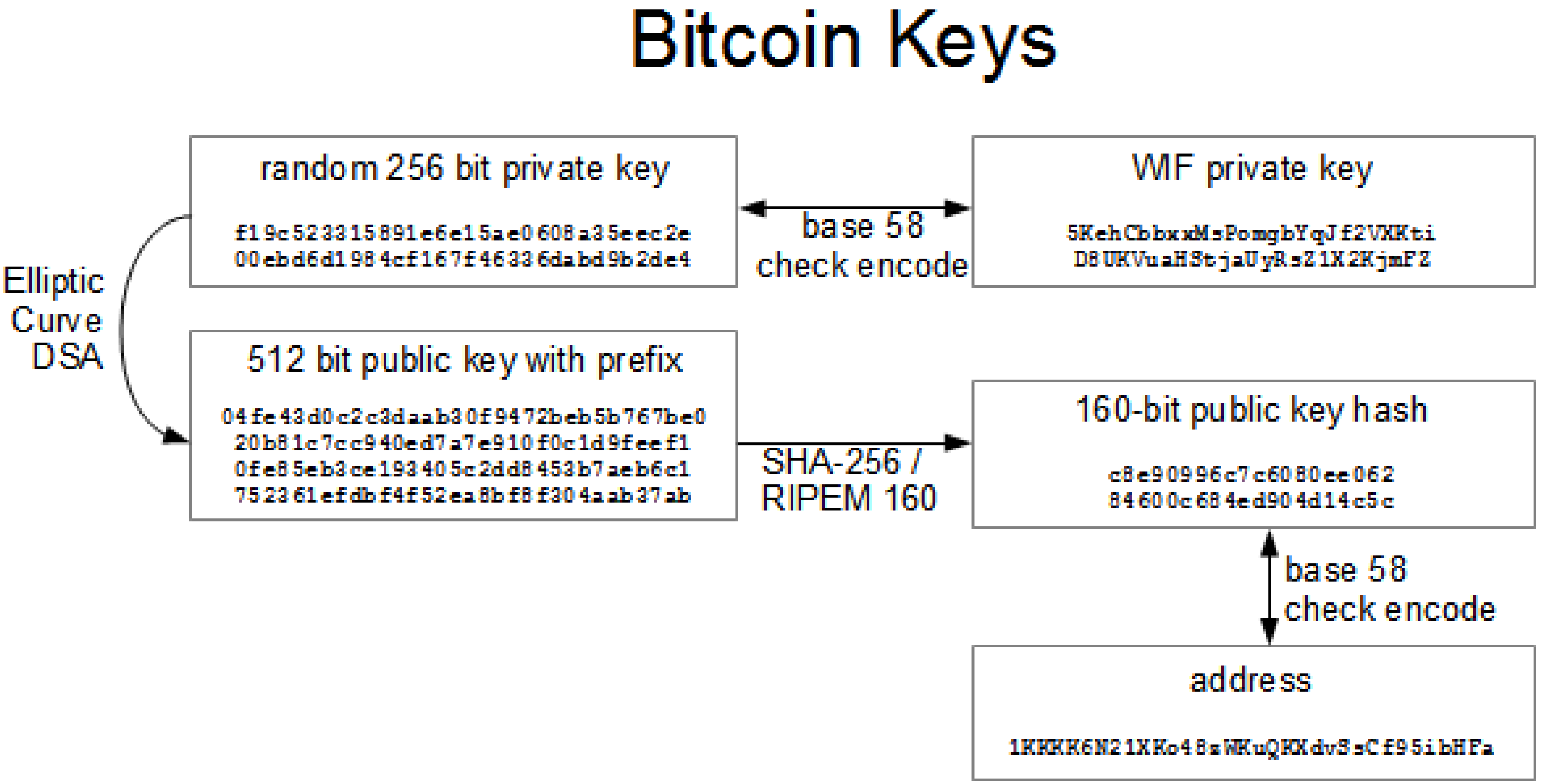
# Asymmetric Cryptography

- 1973: Cocks' Implementation of Asymmetric Cryptography
- Random generation of a key pair:
  - The private must be kept secret
  - The public key can be released publicly to verify a message signed by the private key or to encrypt a message that only the owner of the private key can decrypt
- A crypto wallet can be used to easily create key pairs
  - Be careful of not losing the generated files and keep them secure as well as your recovery passwords
  - Hardware wallets are better against unmaintained daily used computers
  - Exercise with https://www.myetherwallet.com/
- Usually a cryptocurrency account address is derived from hashing the public key

# Hash

- A hash function is any function that can be used to map data of arbitrary size to data of a fixed size.
- Some hash function are said to be secure when they are collision-resistant, which means that it is very hard to find data that will generate the same hash value.
- Secure Hash Algorithms (SHA) are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)
  - SHA-0: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.
  - SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.
  - SHA-2: A family of two similar hash functions, with different block sizes, known as *SHA-256* and *SHA-512*. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.
- The SHA-256 hash function is used within the Bitcoin network in two main ways: mining and creation of Bitcoin addresses

# Relation between Bitcoin Keys and Address



Bitcoin Keys

random 256 bit private key

f19c523315891e6e15ae0608a35eec2e00ebd6d1984cf167f46336dabd9b2de4

WIF private key

5KehCbbxxMsPomgbYqJf2VXKtiD8UKVuaHStjaUyRsZ1X2KjmFZ

512 bit public key with prefix

04fe43d0c2c3daab30f9472beb5b767be020b81c7cc940ed7a7e910f0c1d9feef10fe85eb3ce193405c2dd8453b7aeb6c1752361efdbf4f52ea8bf8f304aab37ab

160-bit public key hash

c8e90996c7c6080ee06284600c684ed904d14c5c

address

1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa

[Ken Shirriff]

# Proof-Of-Work (PoW)

- 1993: Cynthia Dwork and Moni Naor’s Proof-of-Work against SPAM
- Given some data, find a nonce that will generate a hash starting with X zeros
- The higher X is, the higher difficulty
- Many combinations must be tried before the nonce is found and it requires computing power, also known as hash power
- Bitcoin tries to maintain a difficulty leading to a solution found in around 10 minutes

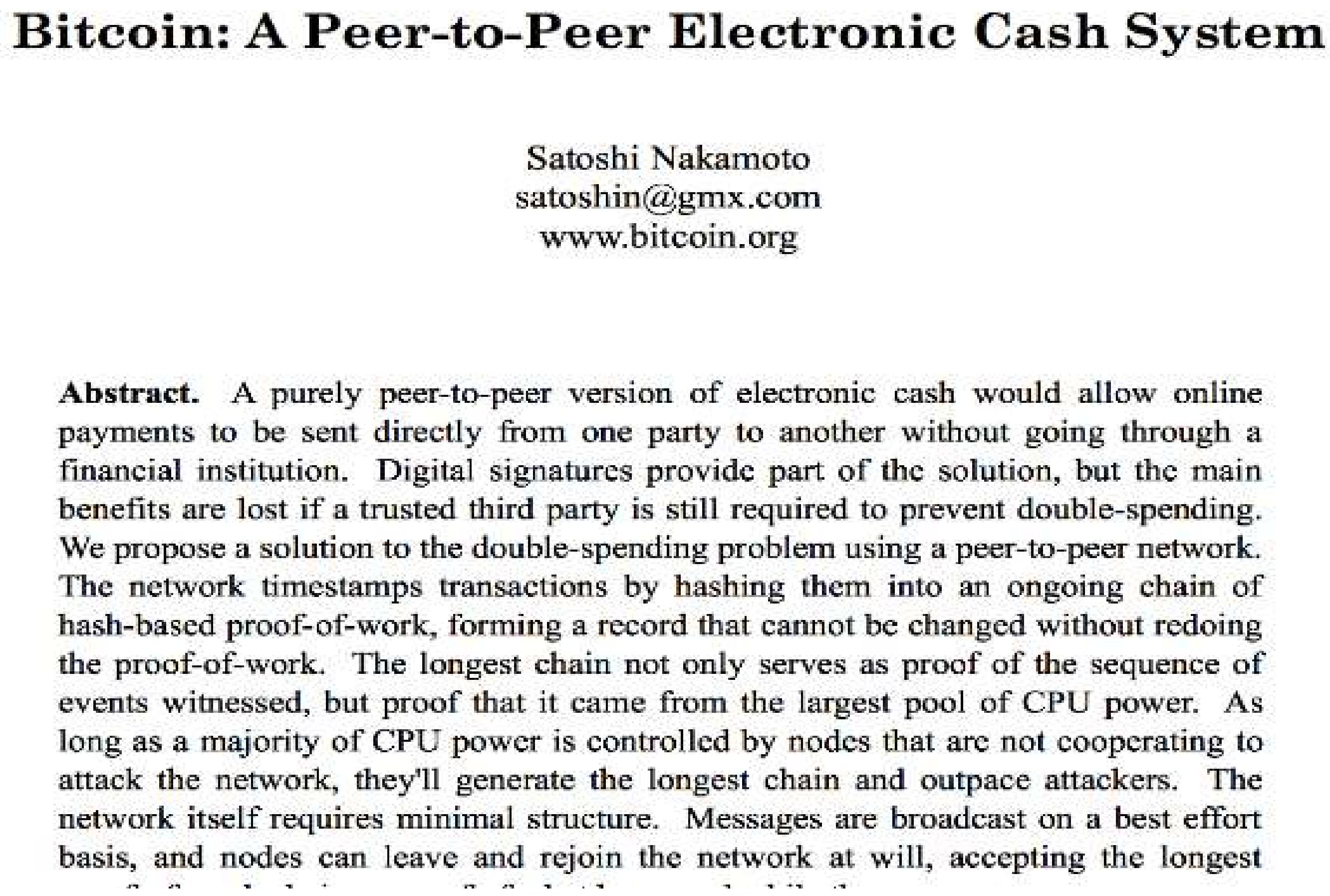
# Peer-to-Peer (P2P)

- 1999: Napster music sharing application
- P2P system is a distributed system where tasks or workloads are provided by peers or nodes.
- An attack-resistant incentive mechanism must exist to avoid the “tragedy of the commons”, a situation in a shared-resource system where individual users acting independently according to their own self-interest behave contrary to the common good of all users by depleting or spoiling that resource through their collective action.
- There are different types of P2P systems.
- BitTorrent has been acquired by TRON cryptocurrency and DLT

# Bitcoin Main Building Blocks

- The first combination of existing building blocks to solve distributed consensus and double-spending without a central authority thanks to a blockchain with PoW
- 31/10/2008, Satoshi Nakamoto's Bitcoin solution publication using several major building blocks:
  - 1973: Cocks' Implementation of Asymmetric Cryptography
  - 1982: Leslie Lamport et al.'s Byzantine Generals Problem
  - 1991: Linked cryptographic timestamps
  - 1993: Cynthia Dwork and Moni Naor's Proof-of-Work against SPAM
  - 1994: Nick Szabo's Smart Contract
  - 1997: Adam Back's HashCash
  - 1998: Nick Szabo's BitGold and Wei Dai's B-Money
  - 1999: Peer-to-Peer Networks (Shawn Fanning's Napster)
  - 2001: SHA-256
- January 12th 2009, first Bitcoin transaction from Satoshi Nakamoto to Hal Finney

# Bitcoin Whitepaper



## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

[bitcoin.org, 10/31/2008]

# Bitcoin “Ideology”

- Born in 2008 amid the turmoil of the 2008 financial crisis
- Satoshi Nakamoto (unknown identity)
  - “The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.”

[Satoshi Nakamoto, Feb. 2009]

[Mashable.com]

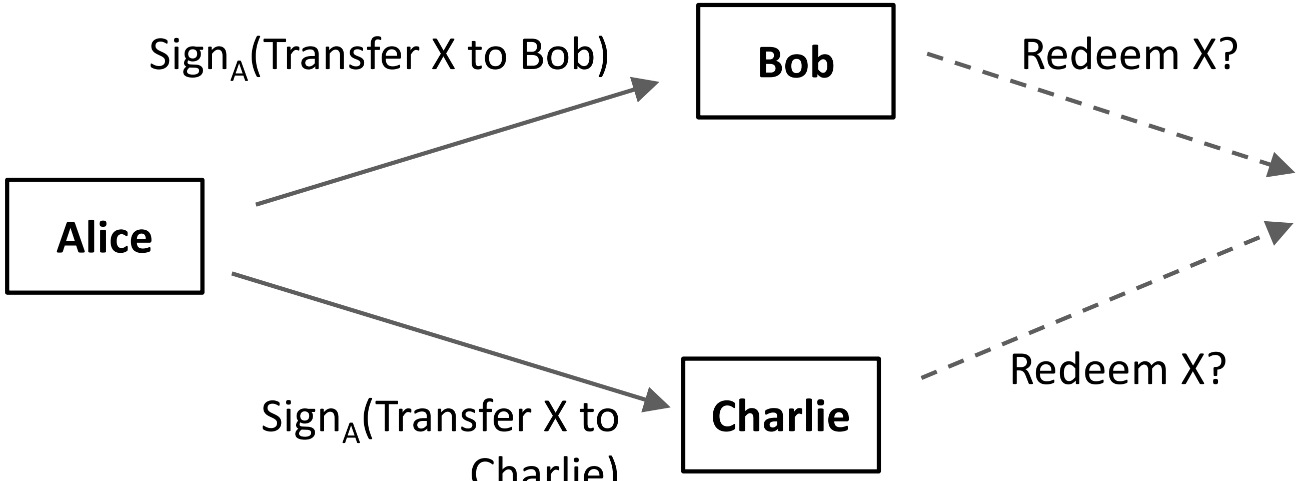
# Satoshi Solution Vision

- “What if I could turn a bank inside out? Instead of one central party controlling the ledger, what if every user were recruited to maintain a constantly updated copy?”
- Copy *instantly* the ledger on all participating nodes and exclude the one that doesn’t agree with the masses

ixabay]

# Double Spending Problem of Digital Currencies

- Digital resources are easy to copy
- Networks are noisy and transmission across networks is far from instantaneous
- Fraudsters may give several times the same digital coin before all ledgers are updated



Alice

Sign$_A$(Transfer X to Bob)

Bob

Sign$_A$(Transfer X to Charlie)

Charlie

Redeem X?

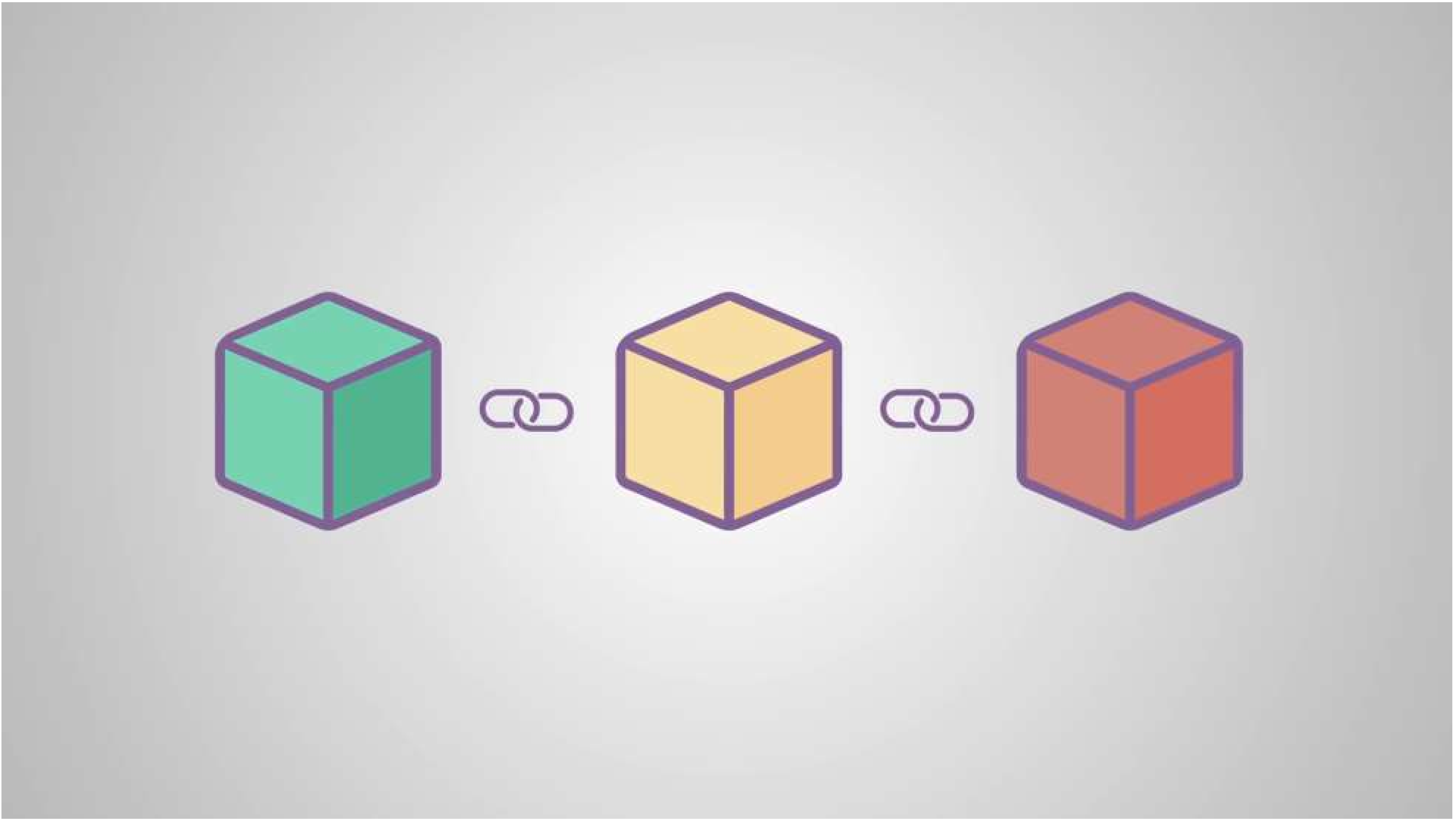
Redeem X?

[Pixabay]

# Blockchain

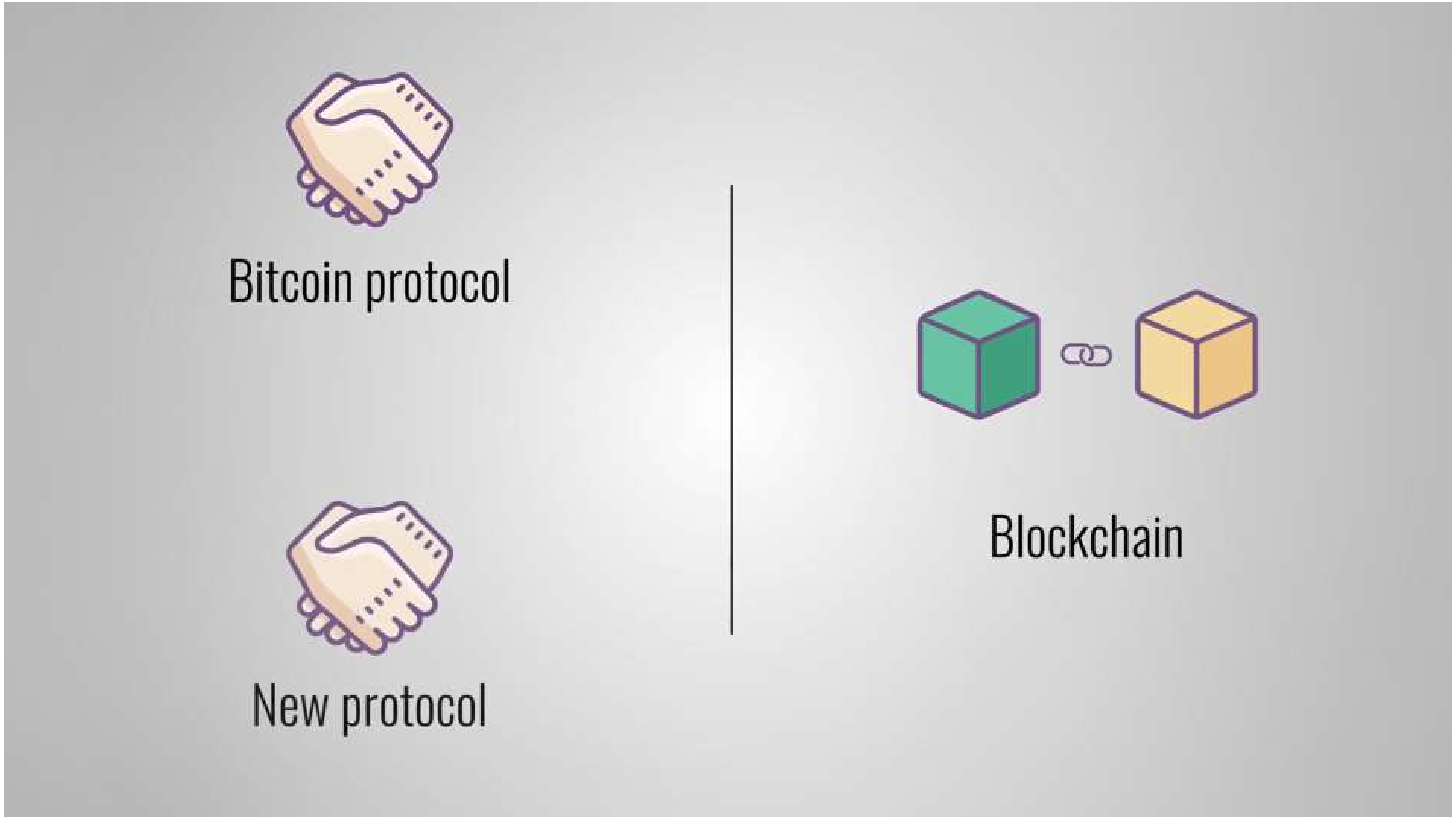
- A block usually contains several signed transactions
- The block also contains the hash of the previous block
- The miner or validator must check that the transactions signatures are valid as well as their content, e.g., the payer signer has still enough cryptocurrencies to pay
- When PoW is used, as in Bitcoin, the miner has to spend resources to find the nonce that will generate a hash of the current difficulty required by the distributed system
  - When the nonce is found, the block is submitted to other peers for inclusion in the blockchain after their validation and usually considered confirmed after a number of future blocks have been added, e.g., usually 6 blocks for Bitcoin
  - Several computers may find valid nonces at similar times and may propagate their new block to other peers. Thus, some peers may end up with different new blocks due to network delays creating a so called “soft fork” of the blockchain. The hash difficulty helps slowing down the number of potential soft forks and gives time for the peers to reach a consensus on the blockchain with most blocks.
  - The miner may be rewarded by an agreed number of cryptocurrencies and/or fees specified in the transactions
- Other consensus algorithms may be used such as Proof-of-Stake (PoS) or ones based on Byzantine Fault Tolerance (BFT)…
  - All have their own advantages and disadvantages: faster but more centralized, prone to some attacks…

# Bitcoin Blockchain Overview



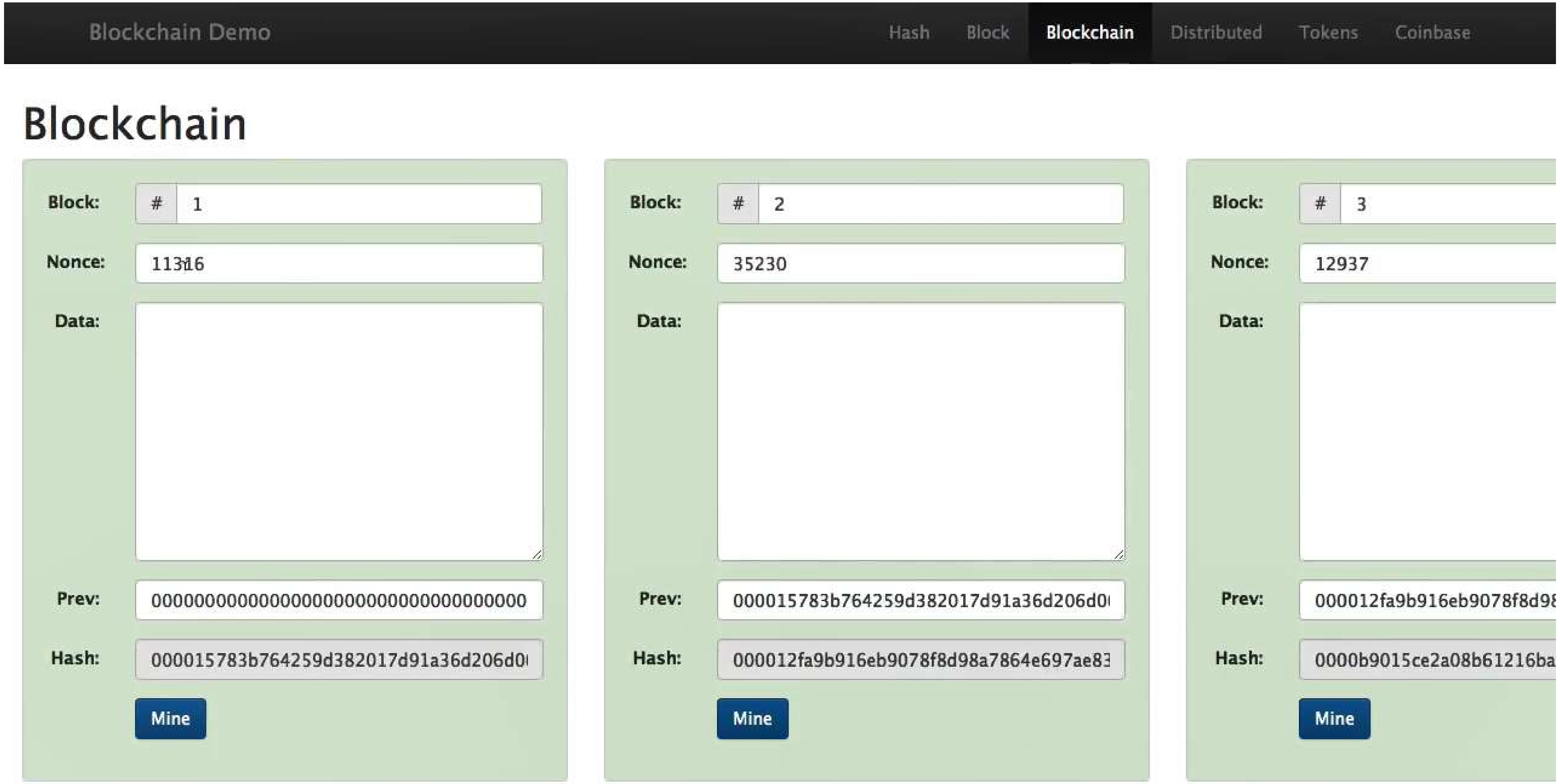
[Simply Explained Savjee]

# Hardfork Overview



[Simply Explained Savjee]

# Blockchain Exercise with https://anders.com/blockchain/



## Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 00000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0
Hash: 000012fa9b916eb9078f8d98a7864e697ae83

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98
Hash: 0000b9015ce2a08b61216ba

[anders.com]

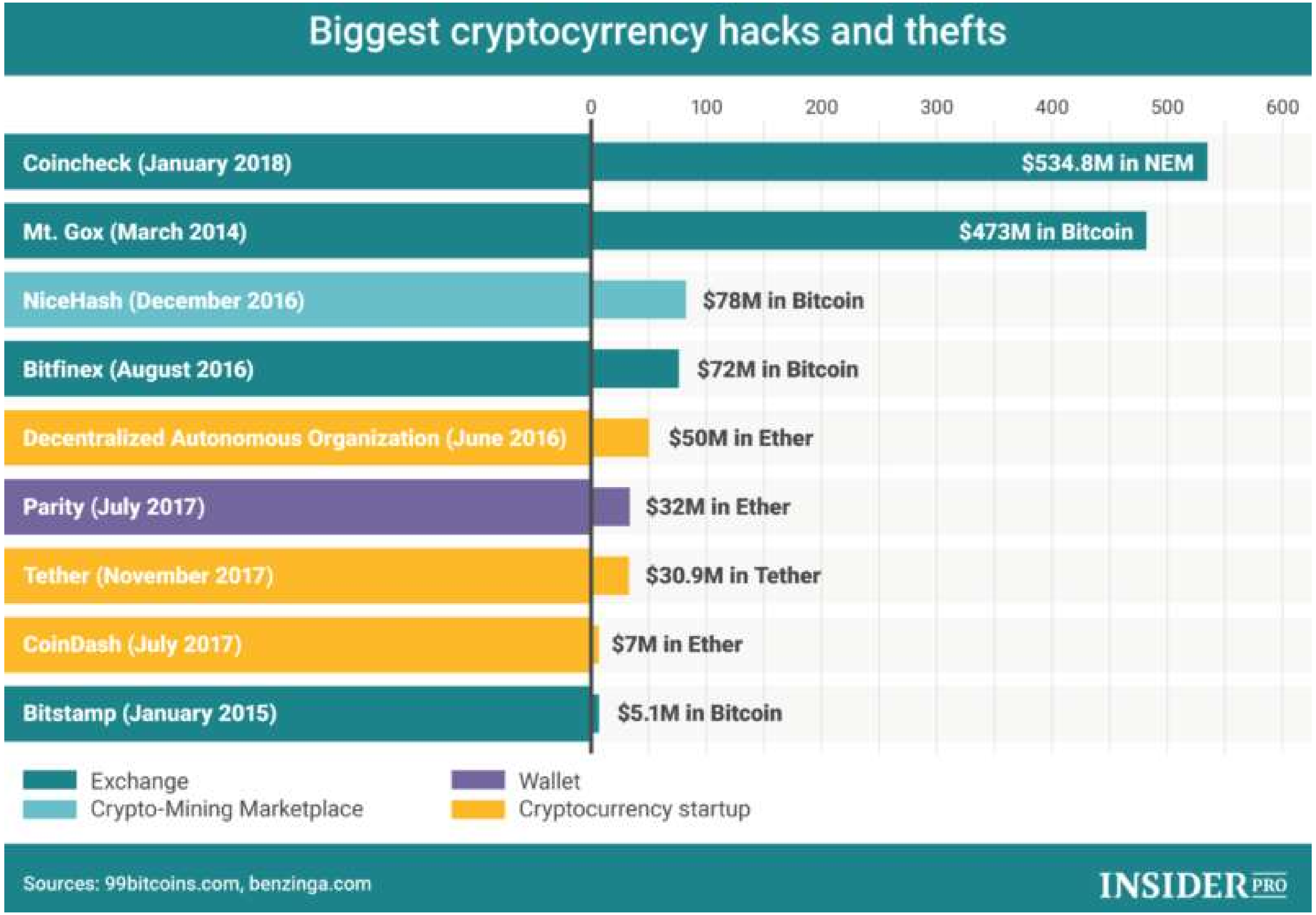
# Bitcoin Theoretical 51% Attack

- “A majority attack (usually labeled 51% attack or >50% attack) is an attack on the network. This attack has a chance to work even if the merchant waits for some confirmations, but requires extremely high relative hashrate.
- The attacker submits to the merchant/network a transaction which pays the merchant, while privately mining a blockchain fork in which a double-spending transaction is included instead. After waiting for n confirmations, the merchant sends the product. If the attacker happened to find more than n blocks at this point, he releases his fork and regains his coins; otherwise, he can try to continue extending his fork with the hope of being able to catch up with the network. If he never manages to do this, the attack fails, the payment to the merchant will go through, and the work done mining will also go to waste, as any new bitcoins would be overwritten by the longest chain.
- The probability of success is a function of the attacker's hashrate (as a proportion of the total network hashrate) and the number of confirmations the merchant waits for. For example, if the attacker controls 10% of the network hashrate but the merchant waits for 6 confirmations, the success probability is on the order of 0.1%. If the attacker controls more than half of the network hashrate, this has a probability of 100% to succeed. Since the attacker can generate blocks faster than the rest of the network, he can simply persevere with his private fork until it becomes longer than the branch built by the honest network, from whatever disadvantage.
- No amount of confirmations can prevent this attack; however, waiting for confirmations does increase the aggregate resource cost of performing the attack, which could make it unprofitable or delay it long enough for the circumstances to change or slower-acting synchronization methods to kick in. A majority attack was more feasible in the past when most transactions were worth significantly more than the block reward and when the network hashrate was much lower and prone to reorganization with the advent of new mining technologies.
- A majority attack has never been successfully executed on the Bitcoin network, but it has been demonstrated to work on some small altcoins.”

[https://en.bitcoin.it]

# Other Public Blockchain Attack-Resistance

- The following altcoins are known to have been successfully attacked with the 51% attack: NEM, Verge, Bitcoin Gold, ZenCash…
- As we have seen, with a Byzantine Fault Tolerance (BFT) approach, no more than 33% of the network participants can be malevolent to maintain the system's integrity.
  - NEO, which uses delegated BFT, has been down several times



Biggest cryptocyrrency hacks and thefts

Sources: 99bitcoins.com, benzinga.com

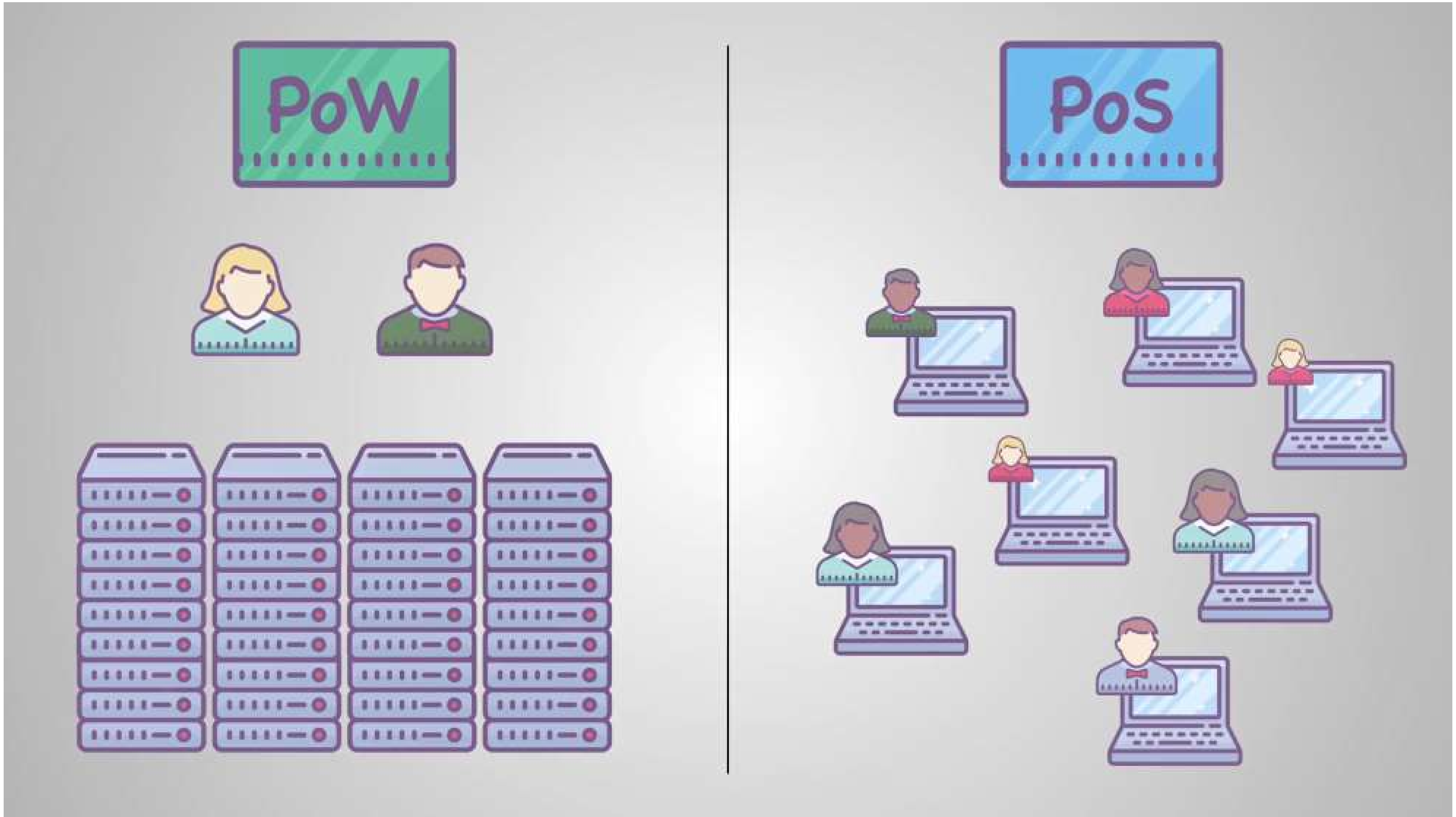
# Bitcoin Issues (at time of writing)

- Fears that Bitmain may be close to approach 51% of total Bitcoin hashrate
- Risk of other hardforks due to divergence in the Bitcoin developers community
- Consensus is only confirmed probabilistically with increased probability as new blocks are added
- Concentration of wealth
  - 97% Bitcoins are only held by 4% of addresses
  - Satoshi Nakamoto may have at time of writing 1 million Bitcoins (6 billion $) over the maximum 21 million Bitcoins
- No enforced Know Your Customer (KYC) for Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) (although not anonymous)
- Used at best as store of value or worse as a speculation tool instead of “electronic cash”
- Performance doesn’t scale as its use increases in contrast to (theoretically) IOTA and Cardano
  - Only around 7 transactions per second and it has already been congested
  - Lightning networks (offchain sidechains) help in this regard
- Alex de Vries’ study found that Bitcoin mining uses roughly the same amount of electricity as the entire nation of Ireland

# Proof-of-Stake (PoS) and Delegated PoS

- Alternative consensus to Proof-of-Work (PoW) without mining.
- In PoS, users may stake some of their coins to be able to become the peer who will be selected as next block validator and potentially earn the transaction fees
- Selection by account balance would result in undesirable centralization because the single richest member would have a permanent advantage as it gets richer.
- Different versions: random selection, stake age-based selection (number of coins stake multiply by the time they have been staked, when selected, time reset to 0)…
- PoS alternatives consume less energy and reach higher TPS but they have also still to prove their attack-resistance in real open public settings like PoW so far.
    - Ethereum is trying to move from PoW to PoS with its Casper protocol.
- In Delegated PoS (DPOS), as in EOS, token holders don't vote on the validity of the blocks themselves, but vote to elect delegates to do the validation on their behalf.

# Proof of Stake (PoS) vs. Proof of Work (PoW)



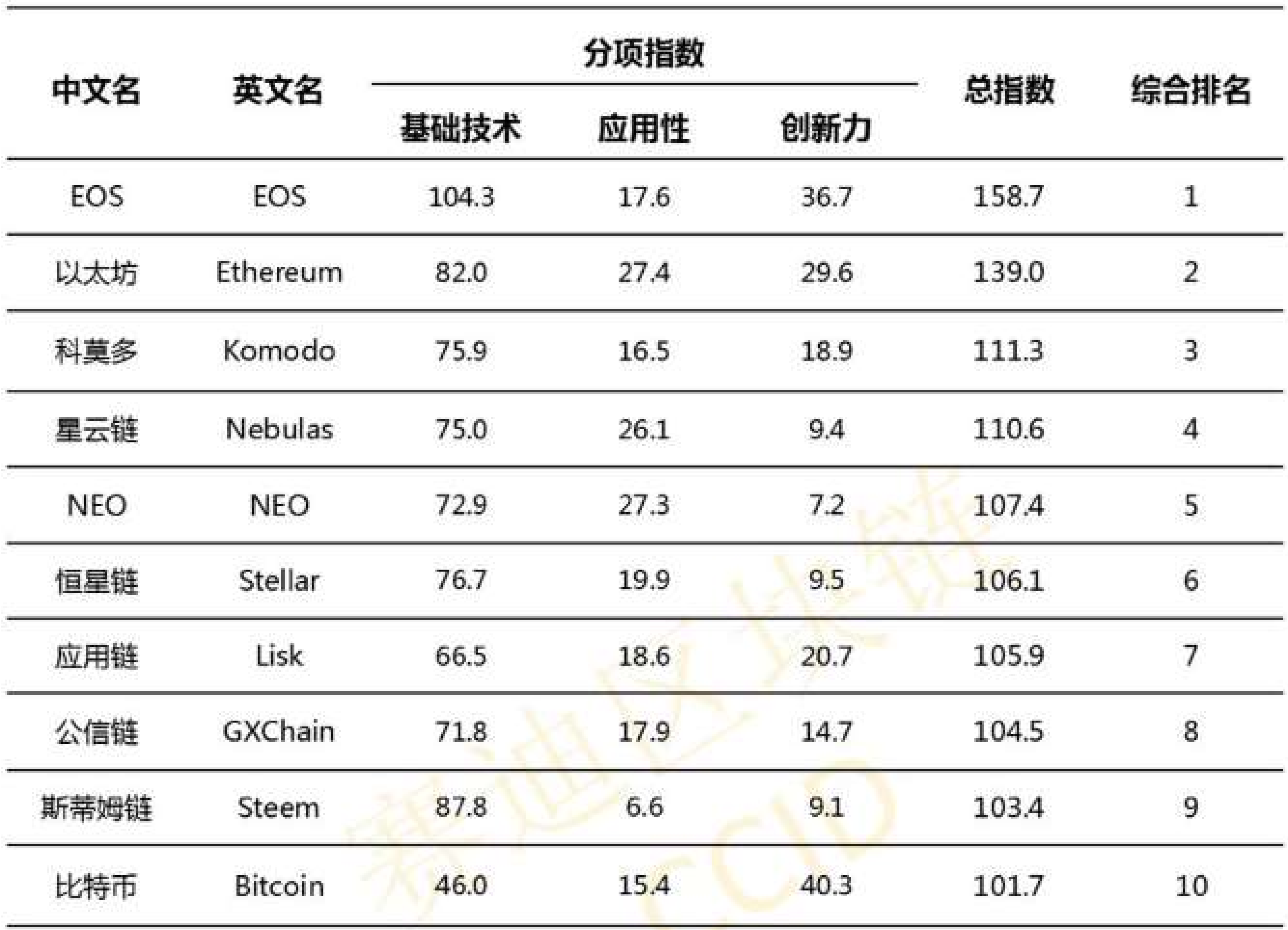
[Simply Explained Savjee]

# Agenda

- Understanding the technology behind DLT
- **Overview of current DLT development platforms**
- How to select the most appropriate DLT for a specific dApp
- Overview of current cryptocurrencies and tools
- Initial Coin Offering (ICO), Token Generation Event (TGE) and tokenomics
- DLT trends

# Chinese Permissionless Blockchain Ranking

- CCID is a research institute working for the Chinese Ministry of Industry and Information Technology
- Ranking based on:
  - Technology
  - Application
  - Innovation
- August 2018 example:



| 中文名 | 英文名 | 分项指数 | | | 总指数 | 综合排名 |
|---|---|---|---|---|---|---|
| | | 基础技术 | 应用性 | 创新力 | | |
| EOS | EOS | 104.3 | 17.6 | 36.7 | 158.7 | 1 |
| 以太坊 | Ethereum | 82.0 | 27.4 | 29.6 | 139.0 | 2 |
| 科莫多 | Komodo | 75.9 | 16.5 | 18.9 | 111.3 | 3 |
| 星云链 | Nebulas | 75.0 | 26.1 | 9.4 | 110.6 | 4 |
| NEO | NEO | 72.9 | 27.3 | 7.2 | 107.4 | 5 |
| 恒星链 | Stellar | 76.7 | 19.9 | 9.5 | 106.1 | 6 |
| 应用链 | Lisk | 66.5 | 18.6 | 20.7 | 105.9 | 7 |
| 公信链 | GXChain | 71.8 | 17.9 | 14.7 | 104.5 | 8 |
| 斯蒂姆链 | Steem | 87.8 | 6.6 | 9.1 | 103.4 | 9 |
| 比特币 | Bitcoin | 46.0 | 15.4 | 40.3 | 101.7 | 10 |

# Stellar vs. Ripple

- Both oriented towards payment/financial transactions
  - Limited set of methods possible compared to Ethereum but less chance for bugs with limited possibilities
- Ripple, more centralized with chosen validators and coins controlled by a company looking for profit, 1500 TPS to upgraded to Visa 50000 TPS (although much use under 2000 TPS)
- Stellar, more decentralized validators and non-profit vision to end poverty , still 1000 TPS
  - Its consensus is based on federated BFT

# Stellar consensus

[Lumenauts]

# Smart contracts beyond payments: Ethereum

- Although Bitcoin has some possibilities for scripts, it has been focused on payment transactions smart contracts and are Turing-incomplete
- A Turing-complete language means that it can approximately simulate the computational aspects of any other real-world general-purpose computer or computer language.
- In 1994, Nick Szabo coined the term "smart contract", a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract, with the aim to provide superior security to traditional contract law and to reduce other transaction costs associated with contracting: "code is law" (although it is not true because smart contracts aren't part of current laws and the cost of lawyers with knowledge in DLT is pretty high)
- In 2013, Vitalik Buterin et al.'s Ethereum has been the first DLT to propose a new DLT for Turing-complete smart contracts and any decentralized applications beyond payments. A co-founder of Ethereum, Charles Hoskinson created later Cardano.
- Although it is generally assumed that transactions and smart contracts once deployed in the blockchain are immutable, other DLTs like EOS keep the option to mutate them and hardforks may happen even in Ethereum because current Ethereum is a fork of Ethereum Classic that reversed the results of the DAO hack.

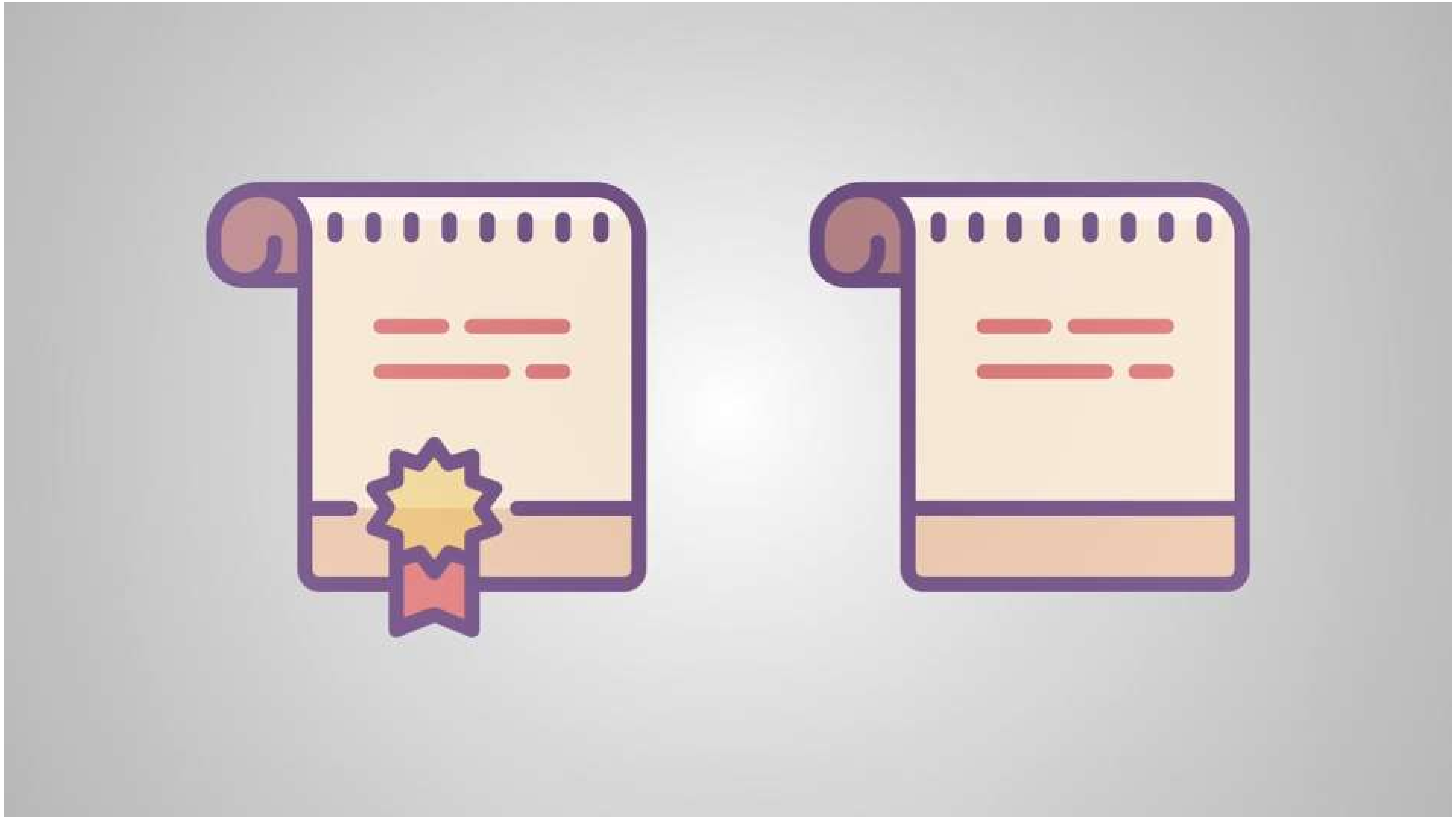
# DAO

- A decentralized autonomous organization (DAO) is an organization that is run through rules encoded as computer programs called smart contracts.
  - For example, token holders may vote to influence the decisions made by the computer program.
- The DAO, which launched with $150 million in crowdfunding in June 2016, and was immediately hacked and drained of US$50 million in cryptocurrency. This hack was reversed in the following weeks, and the money restored, via a hardfork of the Ethereum blockchain. This decentralized bailout was made possible by a majority vote of the blockchain's hash rate.
- The precise legal status of this type of business organization is unclear, which means potentially unlimited legal liability for participants, even if the smart contract code or the DAO's promoters say otherwise.
- Malta is the first country that has voted laws in 2018 to give a legal personality to DAO but other countries, e.g., the USA, have considered DAO tokens as illegal offers of unregistered securities.

# Tokens

- There are 3 main types of crypto tokens.
- Payment token: cryptocurrencies as means of payments such as Bitcoin, although it has become a store of value or means of speculation, as stablecoins or as digital version of fiat money (inconvertible paper money made legal tender by a government decree)
- Utility token: tokens that are needed to use the functionalities of a DLT or dApp (decentralized application) such as Ether
- Security token: tokens that represent assets such as participations in real physical underlyings (stock, commodity, financial product…), companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives.

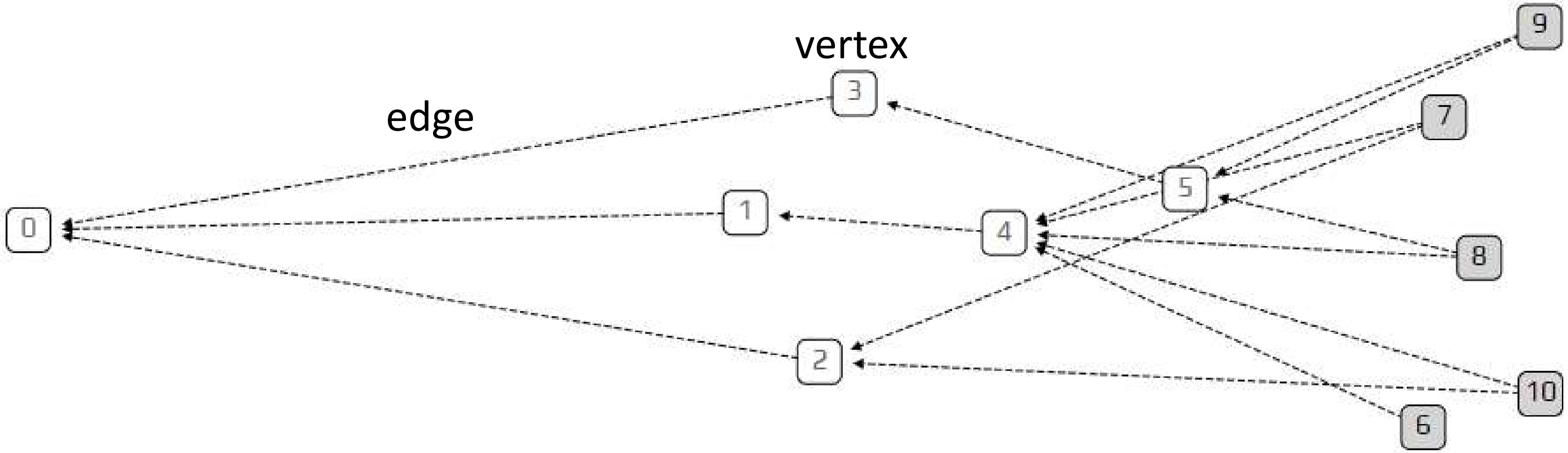
# Smart Contracts Overview



[Simply Explained Savjee]

# Directed Acyclic Graph (DAG)

- Blockchains are only a subset of Distributed Ledger Technologies (DLT).
- Another type of DLT are solutions relying on DAG rather than blockchain: IOTA, Hashgraph, Constellation, Fantom…

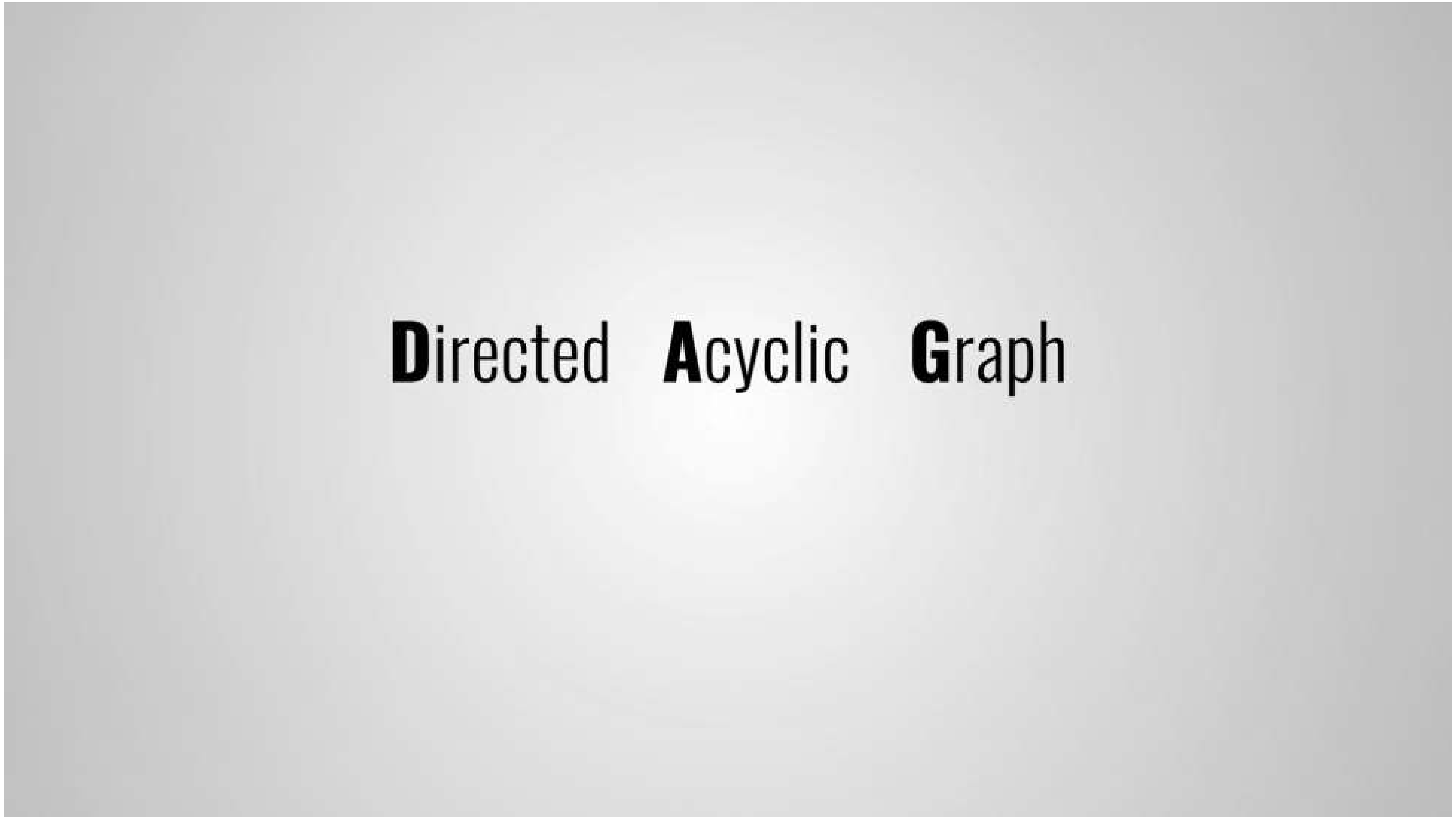


# IOTA

[redacted]

- Launched via an ICO in 2015, IOTA DAG is called tangle
- Advantages:
  - No transaction fee but a new transaction must verify two older transactions (checking there is no conflict and finding the right hash)
  - Performance improves as more transactions are added: it scales with the number of nodes in the network (in contrast to Bitcoin)
- Same as in Bitcoin, there is confirmation confidence as the branch confirming the transaction grows
- Remaining issues:
  - Closed source coordinator to prevent subtangle generation but unknown when the network will be big enough and if it will be resistant to
  - Have used proprietary cryptography rather than peer-reviewed ones
  - Small Internet of Things (IoT) nodes may not be able to hash although IOTA initial targeted IoT
  - Turing-incomplete
  - Low probability of accepting dishonest transaction, which may be an issue, especially for payment use-cases
- Exercise with Vaibhav Saini's simulator here: https://hackernoon.com/a-beginners-ultimate-guide-to-dags-7fc0dd7f39a2

# IOTA Overview



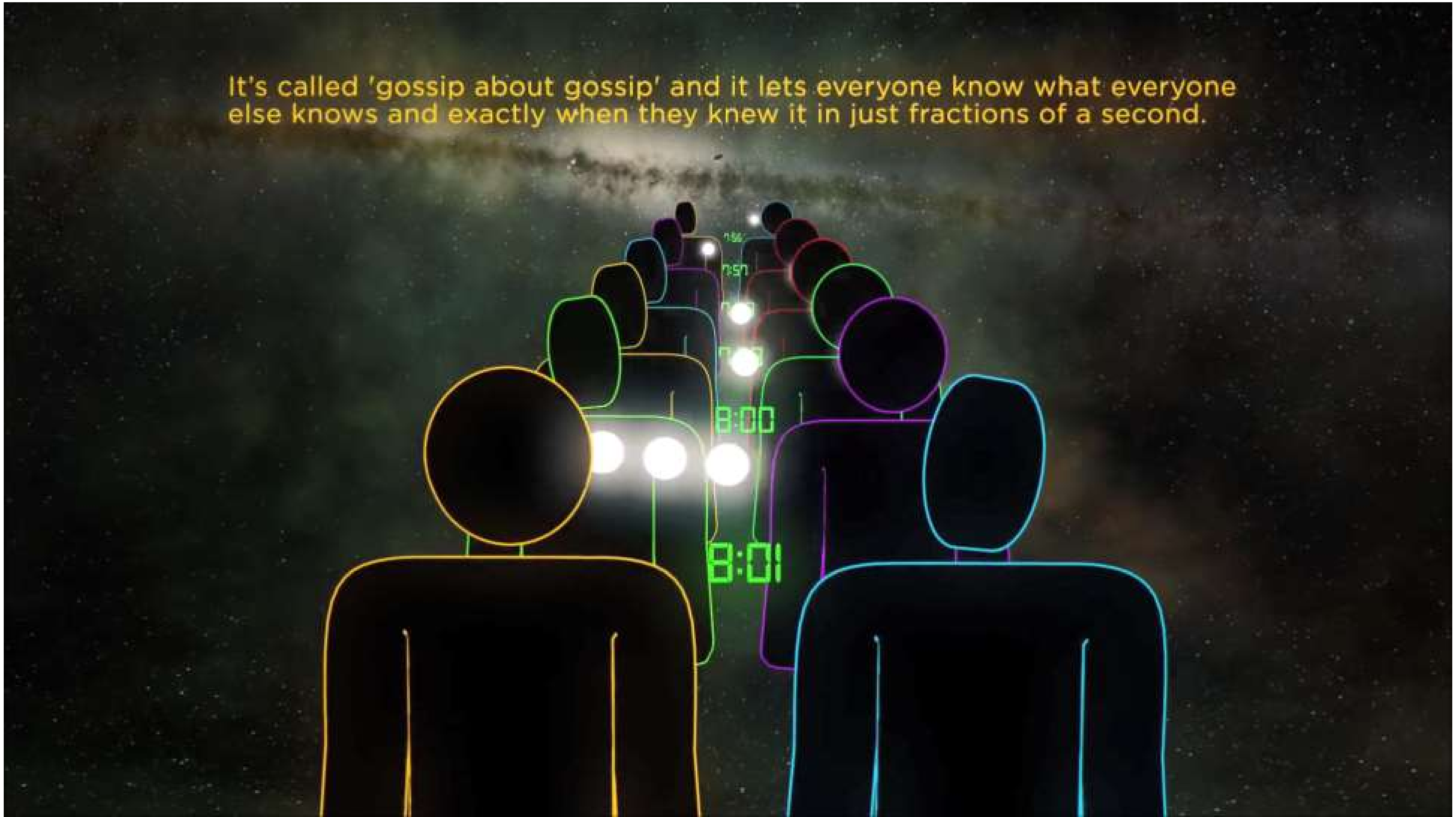
**D**irected **A**cyclic **G**raph

[Simply Explained Savjee]

# Hashgraph

- Hashgraph is a DAG approach relying on a “gossip about gossip” protocol patented by Swirlds and invented by Leemon Baird
- Every node can spread signed information, called events, on new owned transactions and transactions received from others to its randomly chosen neighbors.
- Neighbors aggregate received events with information received from other nodes (including when and from whom) into a new event, and then send it on to other randomly chosen neighbors. This process continues until all the nodes are aware of the information created or received at the beginning. Due to the rapid convergence property of the gossip protocol, every piece of new information can reach each node in the network in a fast manner.
- The history of the gossip protocol can be illustrated by a directed graph, i.e., each node maintains a graph representing sequences of forwarders/witnesses for each transaction.
- By performing virtual voting, each node can determine if a transaction is valid based on whether it has over two-thirds of nodes in the network as witnesses. The assumption is that less than a third of nodes are Byzantine (nodes that can behave badly by forging, delaying, replaying and dropping incoming/outgoing messages).
- Advantages: It works well in permissioned settings reaching over 100000 TPS with mathematically-proven fairness via consensus time stamping instead of blockchain consensus, whose confirmation probability only increases as blocks are added
- Disadvantages: Its attack-resistance in permissionless settings based on PoS has still to be proven.
- It has successfully done its ICO in 2018 in order to move to permissionless use-cases with a platform called Hedera.

# Hashgraph Overview



It's called 'gossip about gossip' and it lets everyone know what everyone else knows and exactly when they knew it in just fractions of a second.

[Mike Maloney, Hidden Secrets of Money]

# Agenda

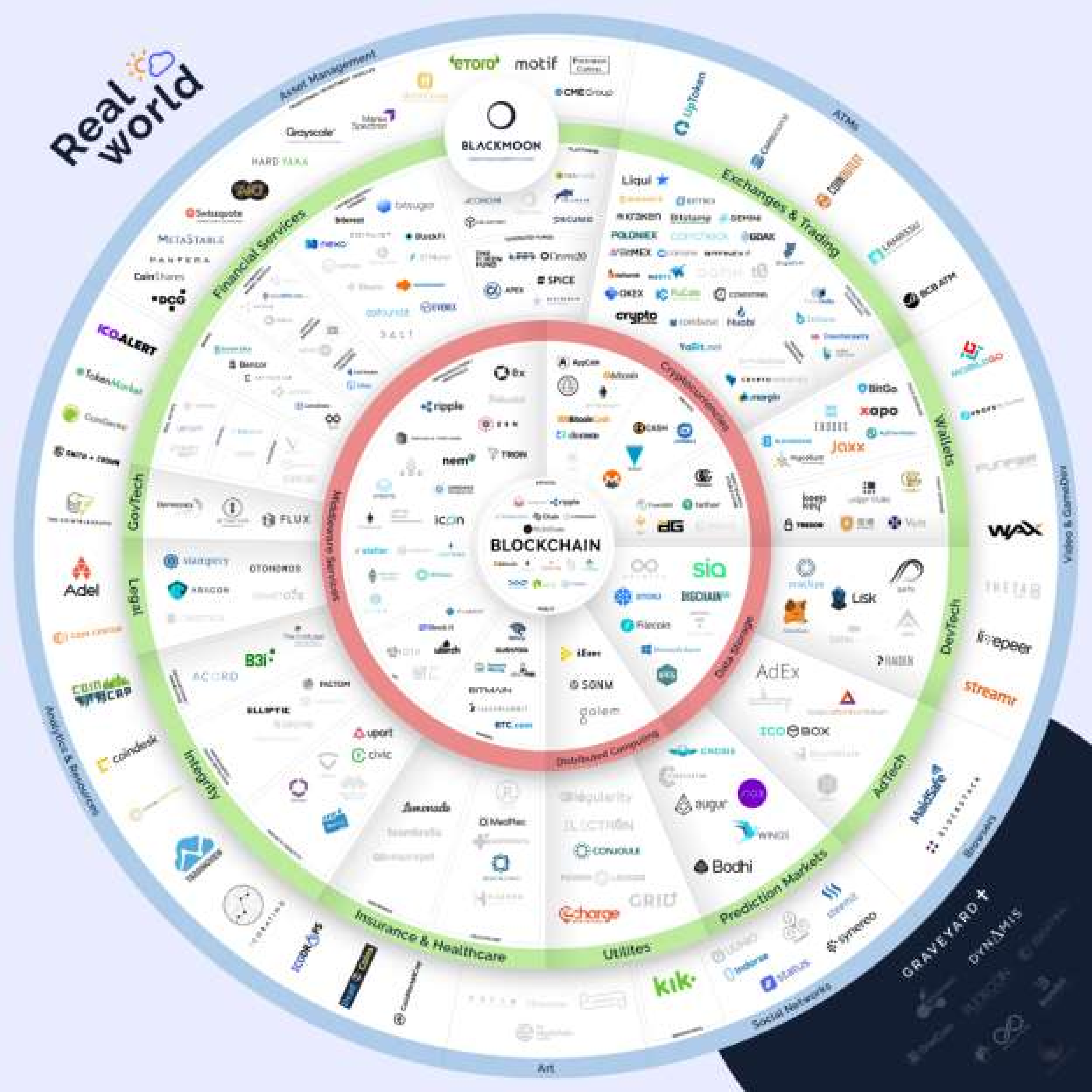
- Understanding the technology behind DLT
- Overview of current DLT development platforms
- **How to select the most appropriate DLT for a specific dApp**
- Overview of current cryptocurrencies and tools
- Initial Coin Offering (ICO), Token Generation Event (TGE) and tokenomics
- DLT trends

# Decentralize Applications (dApp) Requirements

- As presented previously, different DLT platforms have different advantages and disadvantages for dApp development and production:
  - Peer-reviewed
  - Transaction per seconds (TPS)
  - Attack-resistance
  - Turing completeness
  - Permissioned or permissionless
  - Programmability
  - Popularity
  - Sustainability
  - Interoperability
- However, the first requirement to check is to know whether a DLT is needed or not!

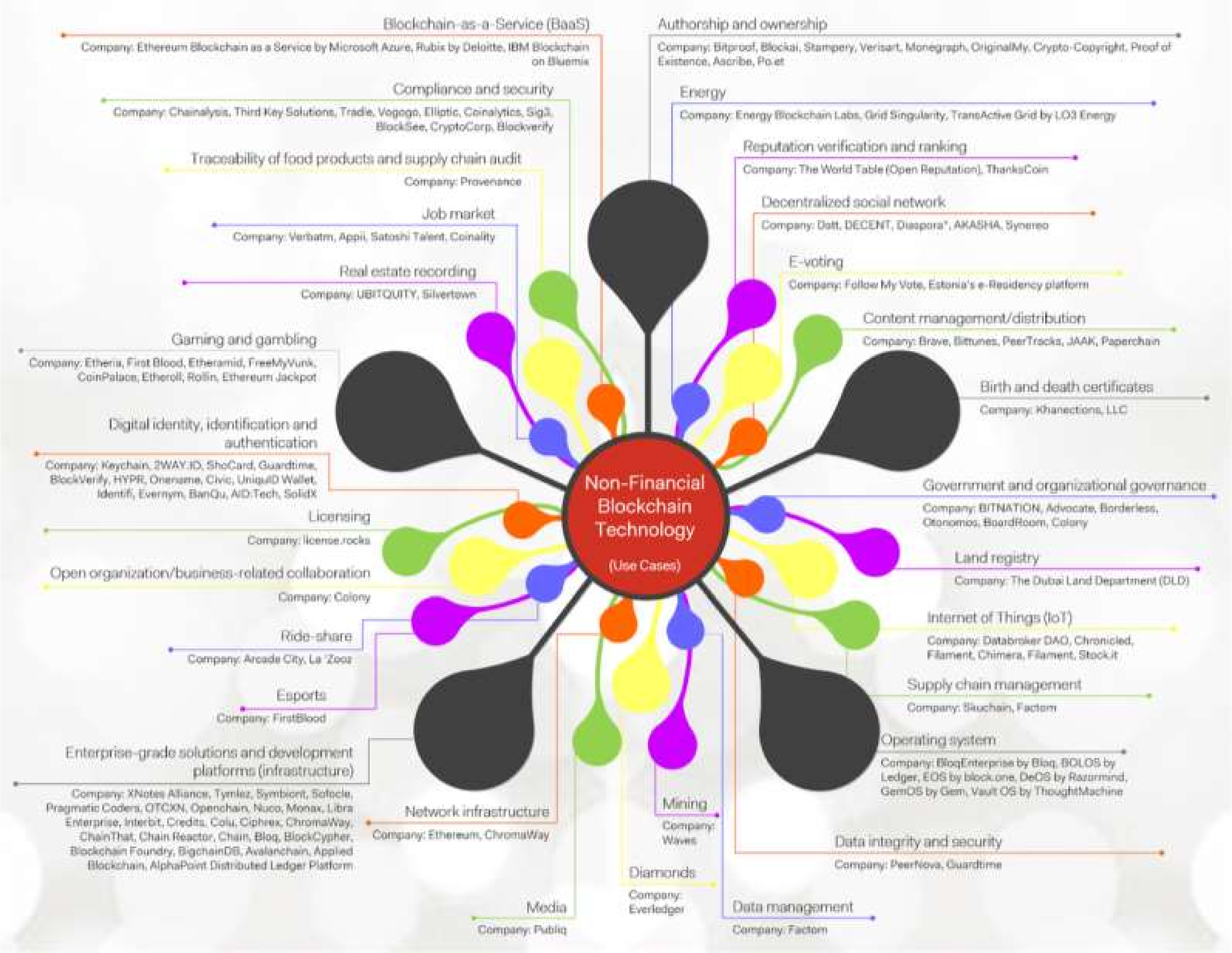
# DLT Business Ecosystem

- [Blackmooncrypto.com]



# Non-financial Use-Cases of Blockchain

- [Medici]



Non-Financial Blockchain Technology

(Use Cases)

Blockchain-as-a-Service (BaaS)
Company: Ethereum Blockchain as a Service by Microsoft Azure, Rubix by Deloitte, IBM Blockchain on Bluemix

Compliance and security
Company: Chainalysis, Third Key Solutions, Tradle, Vogogo, Elliptic, Coinalytics, Sig3, BlockSee, CryptoCorp, Blockverify

Traceability of food products and supply chain audit
Company: Provenance

Job market
Company: Verbatm, Appii, Satoshi Talent, Coinality

Real estate recording
Company: UBITQUITY, Silvertown

Gaming and gambling
Company: Etheria, First Blood, Etheramid, FreeMyVunk, CoinPalace, Etheroll, Rollin, Ethereum Jackpot

Digital identity, identification and authentication
Company: Keychain, 2WAY.IO, ShoCard, Guardtime, BlockVerify, HYPR, Onename, Civic, UniquID Wallet, Identifi, Evernym, BanQu, AID:Tech, SolidX

Licensing
Company: license.rocks

Open organization/business-related collaboration
Company: Colony

Ride-share
Company: Arcade City, La 'Zooz

Esports
Company: FirstBlood

Enterprise-grade solutions and development platforms (infrastructure)
Company: XNotes Alliance, Tymlez, Symbiont, Sofocle, Pragmatic Coders, OTCXN, Openchain, Nuco, Monax, Libra Enterprise, Interbit, Credits, Colu, Ciphrex, ChromaWay, ChainThat, Chain Reactor, Chain, Bloq, BlockCypher, Blockchain Foundry, BigchainDB, Avalanchain, Applied Blockchain, AlphaPoint Distributed Ledger Platform

Network infrastructure
Company: Ethereum, ChromaWay

Media
Company: Publiq

Diamonds
Company: Everledger

Mining
Company: Waves

Data management
Company: Factom

Authorship and ownership
Company: Bitproof, Blockai, Stampery, Verisart, Monegraph, OriginalMy, Crypto-Copyright, Proof of Existence, Ascribe, Po.et

Energy
Company: Energy Blockchain Labs, Grid Singularity, TransActive Grid by LO3 Energy

Reputation verification and ranking
Company: The World Table (Open Reputation), ThanksCoin

Decentralized social network
Company: Dott, DECENT, Diaspora*, AKASHA, Synereo

E-voting
Company: Follow My Vote, Estonia's e-Residency platform

Content management/distribution
Company: Brave, Bittunes, PeerTracks, JAAK, Paperchain

Birth and death certificates
Company: Khanections, LLC

Government and organizational governance
Company: BITNATION, Advocate, Borderless, Otonomos, BoardRoom, Colony

Land registry
Company: The Dubai Land Department (DLD)

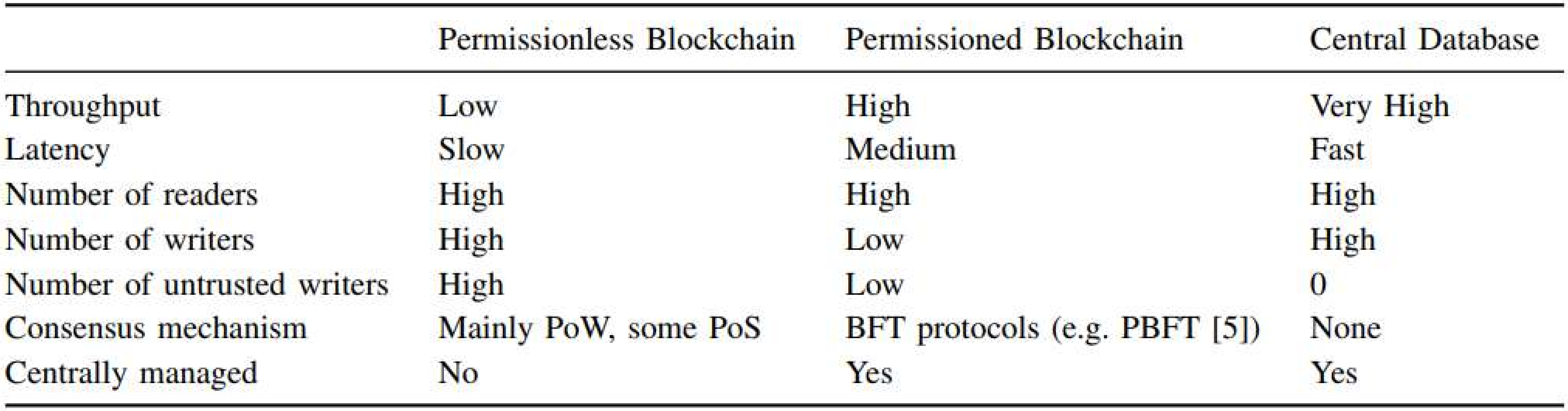
Internet of Things (IoT)
Company: Databroker DAO, Chronicled, Filament, Chimera, Filament, Stock.it

Supply chain management
Company: Skuchain, Factom

Operating system
Company: BloqEnterprise by Bloq, BOLOS by Ledger, EOS by block.one, DeOS by Razormind, GemOS by Gem, Vault OS by ThoughtMachine

Data integrity and security
Company: PeerNova, Guardtime

# Blockchain versus Database

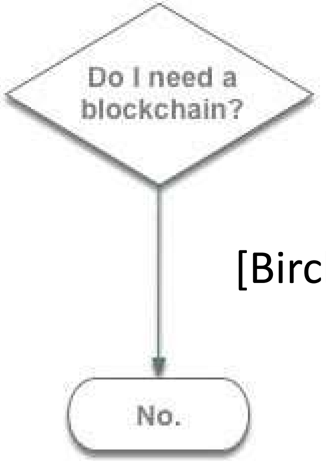


| | Permissionless Blockchain | Permissioned Blockchain | Central Database |
|---|---|---|---|
| Throughput | Low | High | Very High |
| Latency | Slow | Medium | Fast |
| Number of readers | High | High | High |
| Number of writers | High | Low | High |
| Number of untrusted writers | High | Low | 0 |
| Consensus mechanism | Mainly PoW, some PoS | BFT protocols (e.g. PBFT [5]) | None |
| Centrally managed | No | Yes | Yes |

[Wüst and Gervais]

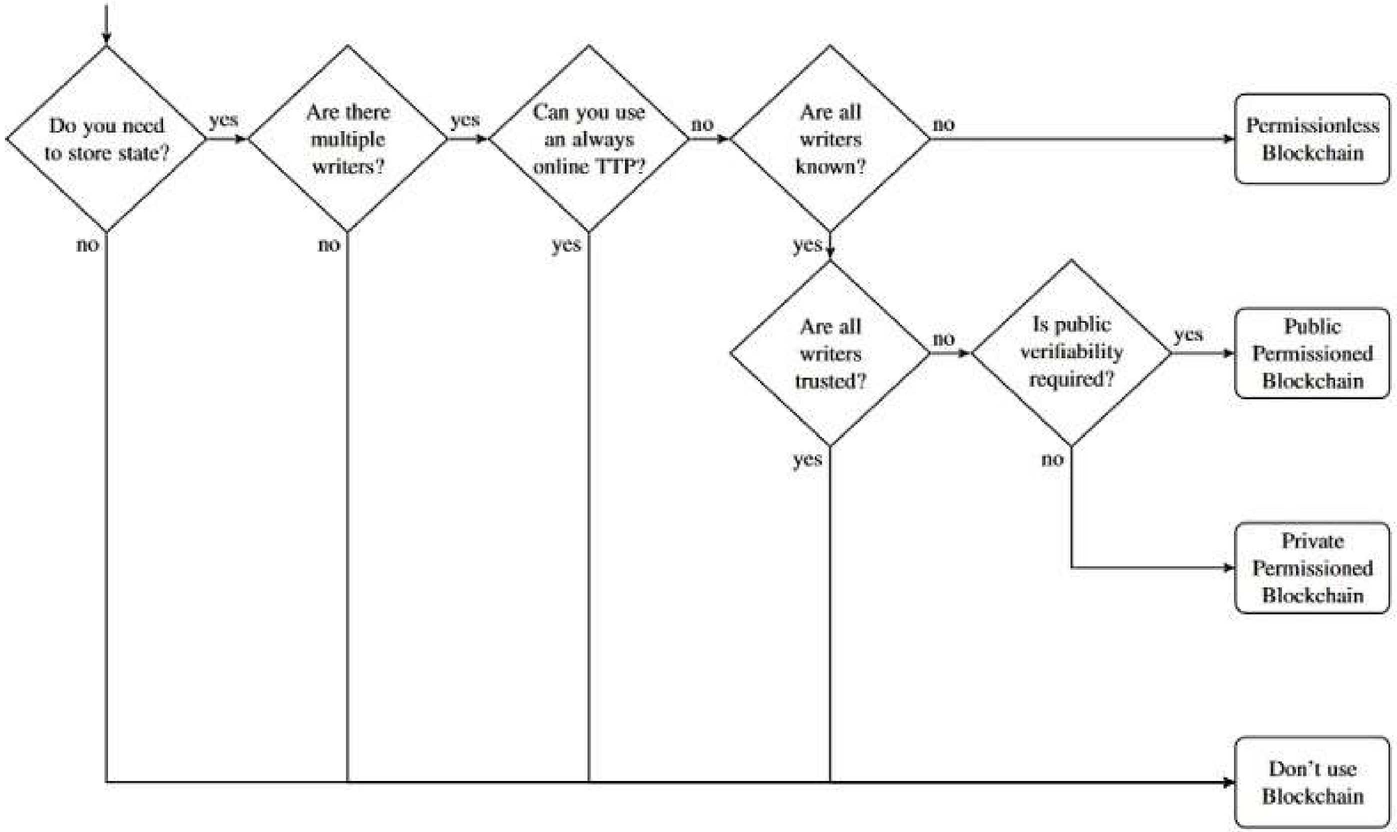
# DLT Decision Flowchart Exercise

- There are several flowcharts to help deciding if the use-case under consideration would benefit from a blockchain. Although we have already seen above that blockchain is only a subset of DLT, we assume that the following blockchain decision flowcharts can also be mainly applied to DLT.
- Which one seems the most appropriate to you?

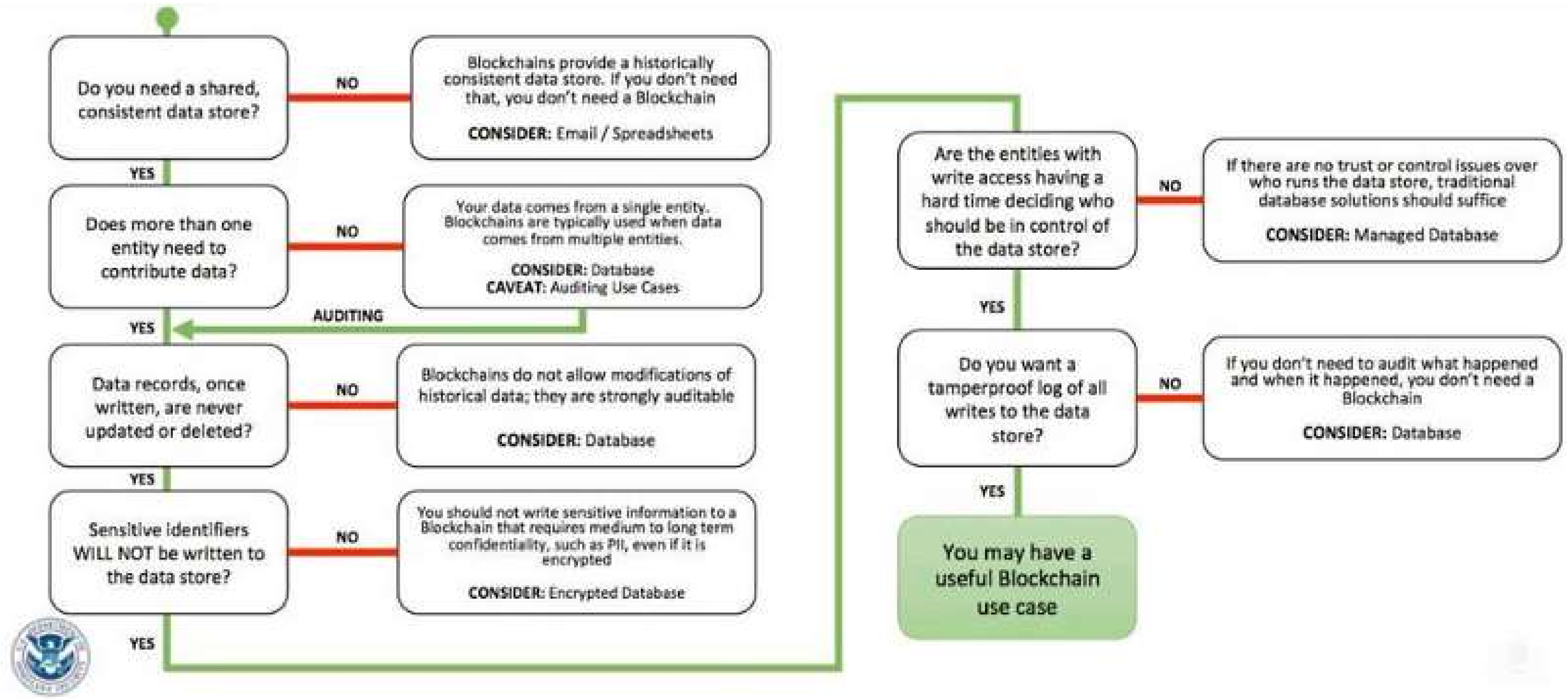


[Birch]

[Wüstl and Gervais]


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

# US DHS DLT Decision Flow Chart



Do you need a shared, consistent data store?

NO

Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain

**CONSIDER:** Email / Spreadsheets

YES

Does more than one entity need to contribute data?

NO

Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities.

**CONSIDER:** Database
**CAVEAT:** Auditing Use Cases

AUDITING

YES

Data records, once written, are never updated or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

**CONSIDER:** Database

YES

Sensitive identifiers WILL NOT be written to the data store?

NO

You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

**CONSIDER:** Encrypted Database

YES

Are the entities with write access having a hard time deciding who should be in control of the data store?

NO

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

**CONSIDER:** Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

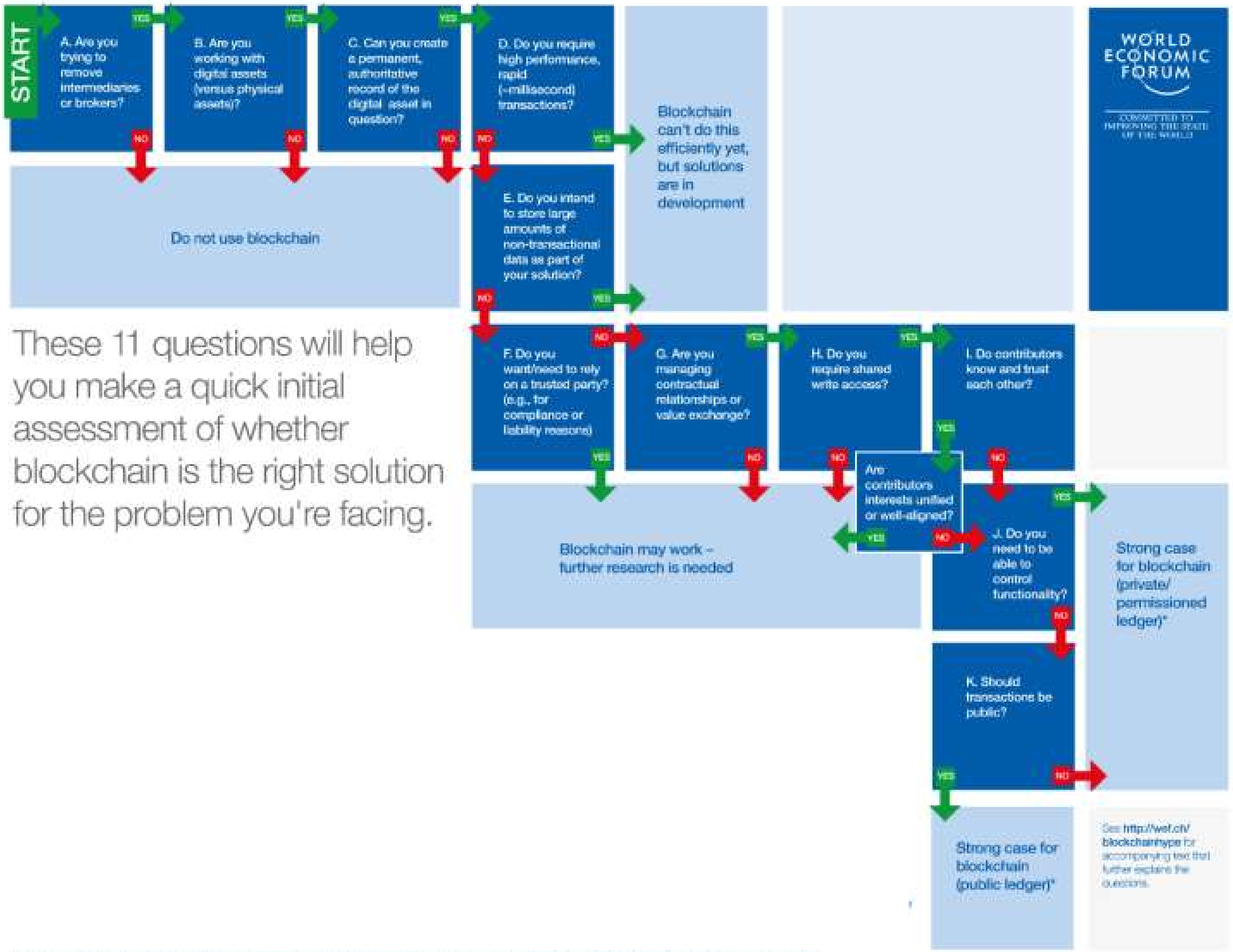
If you don't need to audit what happened and when it happened, you don't need a Blockchain

**CONSIDER:** Database

YES

You may have a useful Blockchain use case

# WEF DLT Decision Flow Chart



START

A. Are you trying to remove intermediaries or brokers?

B. Are you working with digital assets (versus physical assets)?

C. Can you create a permanent, authoritative record of the digital asset in question?

D. Do you require high performance, rapid (~millisecond) transactions?

E. Do you intend to store large amounts of non-transactional data as part of your solution?

F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)

G. Are you managing contractual relationships or value exchange?

H. Do you require shared write access?

I. Do contributors know and trust each other?

Are contributors interests unified or well-aligned?

J. Do you need to be able to control functionality?

K. Should transactions be public?

Do not use blockchain

Blockchain can't do this efficiently yet, but solutions are in development

Blockchain may work – further research is needed

Strong case for blockchain (private/ permissioned ledger)*

Strong case for blockchain (public ledger)*

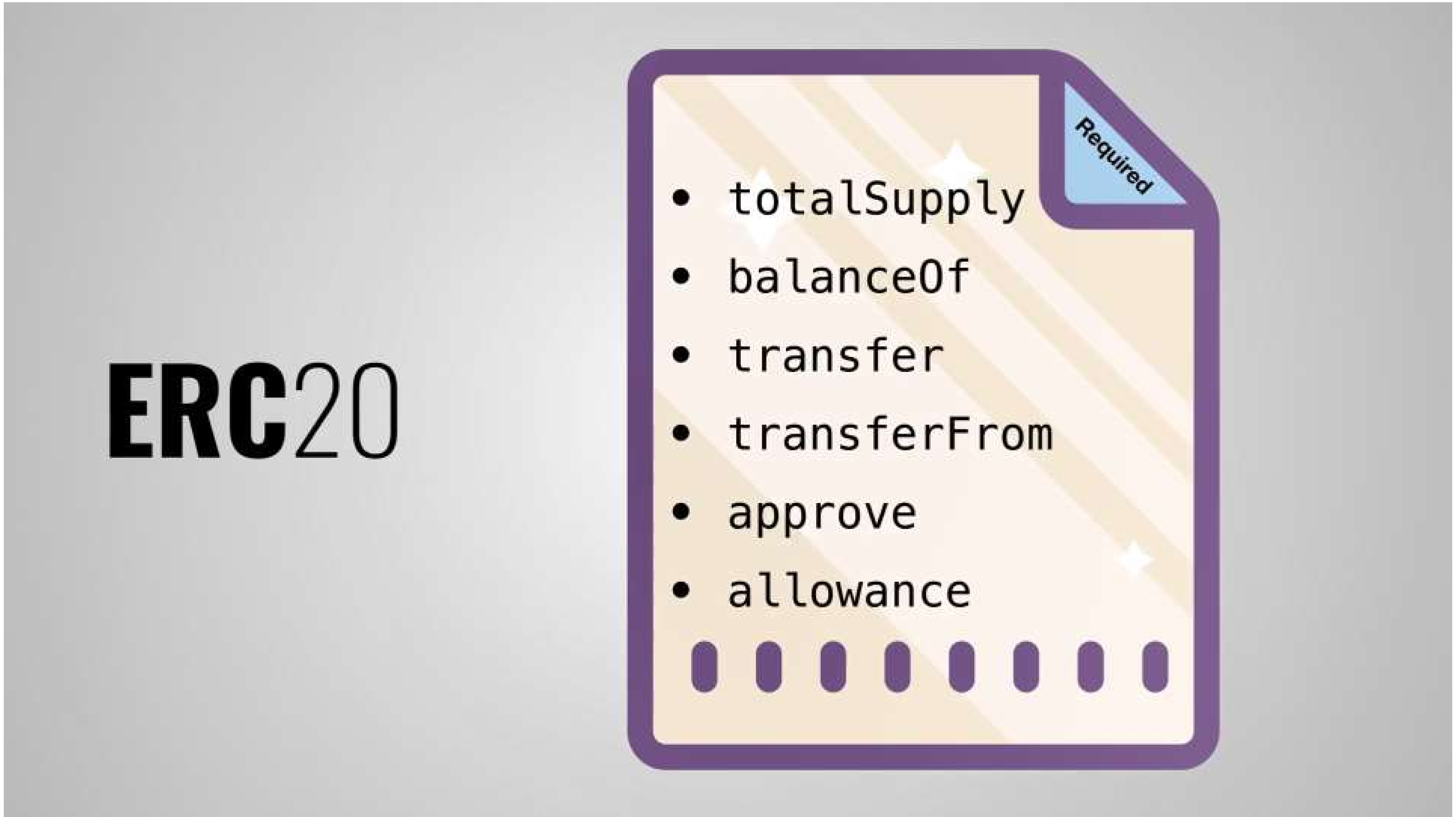
See http://wef.ch/blockchaintype for accompanying text that further explains the questions.

These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

# Programmability

- The following questions may be asked when selecting a DLT:
  - Does the DLT uses a well-known programming level with high-level bug and security checks?
  - Does the DLT provides an Integrated Development Environment (IDE)?
  - How big is the developers community?
  - Are all the DLT components open-source?
  - Are there any restricting patents?
  - Does the DLT use peer-reviewed cryptography?
  - How many other projects/dApp have successfully used the DLT?
  - How many projects/dApps built with the DLT have been successfully attacked due to bugs or security holes?
  - Does the DLT have a testnet separated from the mainnet?
    - Is it easy to use the testnet?
  - Does the DLT have a detailed blocks/transactions explorer?
  - Does the DLT provide an open-source wallet?
  - Is it possible to create privatenets for testing purposes?
  - Does the DLT have an emulator?
  - Does the DLT have an active open-source repository?
    - Including a test suite (unit tests…)?
    - Including active bugs treatments?
    - Including detailed documentation, at least in English?
    - Including tested templates, e.g., ICO smart contracts or tokens generation templates (ERC20, NEP-5…)?

# ERC20 Overview



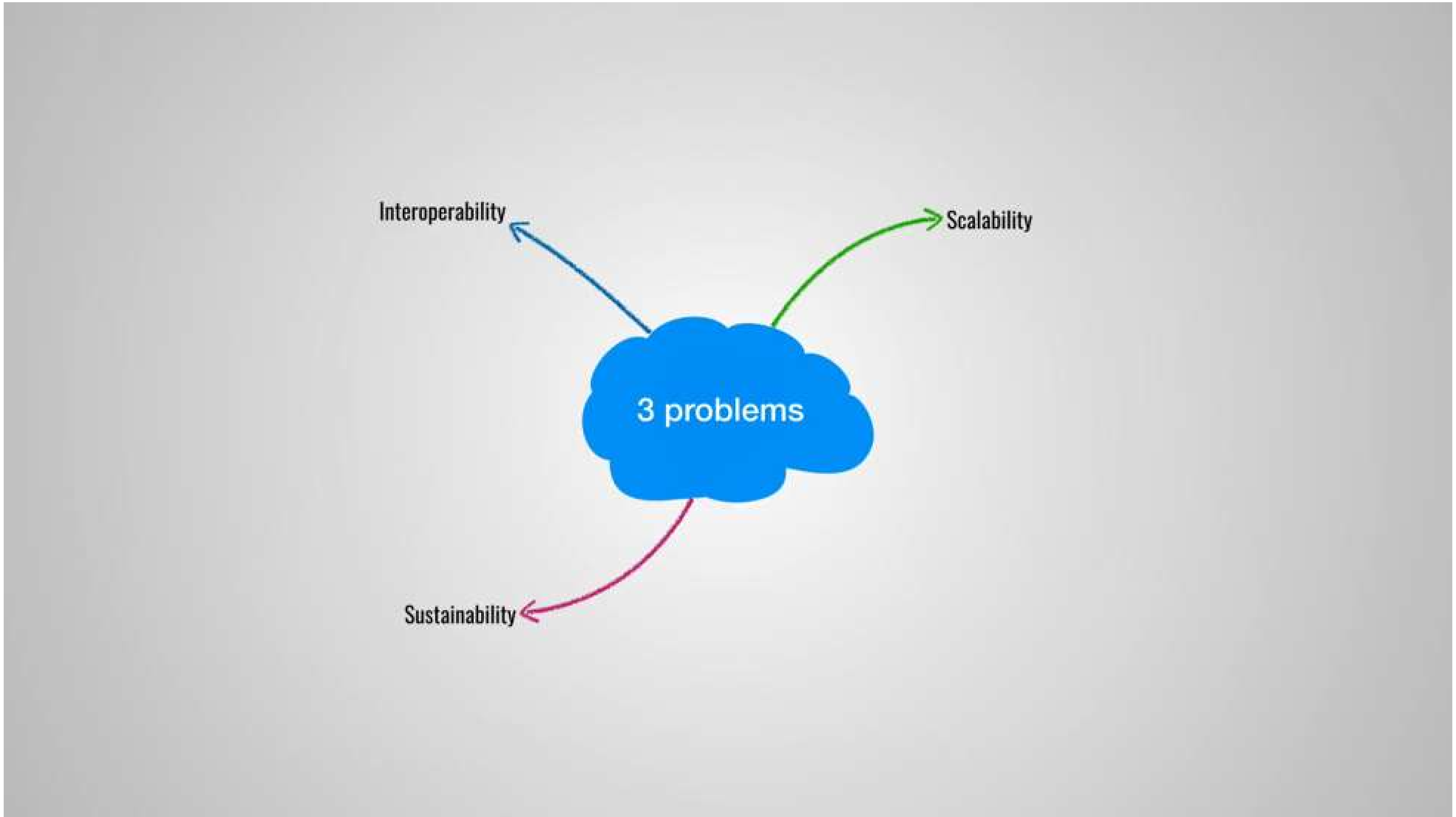
ERC20

Required

- totalSupply
- balanceOf
- transfer
- transferFrom
- approve
- allowance

[Simply Explained Savjee]

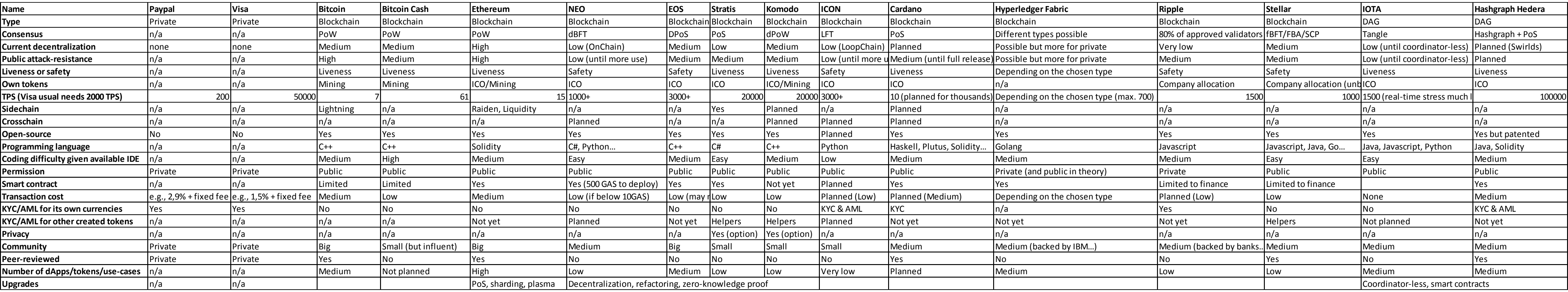
# Cardano Overview



[Simply Explained Savjee]

# Main DLT Overall Comparison

- Checkout the table in the Excel file annex



| Name | Paypal | Visa | Bitcoin | Bitcoin Cash | Ethereum | NEO | EOS | Stratis | Komodo | ICON | Cardano | Hyperledger Fabric | Ripple | Stellar | IOTA | Hashgraph Hedera |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Type | Private | Private | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | Blockchain | DAG | DAG |
| Consensus | n/a | n/a | PoW | PoW | PoW | dBFT | DPoS | PoS | dPoW | LFT | PoS | Different types possible | 80% of approved validators | fBFT/FBA/SCP | Tangle | Hashgraph + PoS |
| Current decentralization | none | none | Medium | Medium | High | Low (OnChain) | Medium | Low | Medium | Low (LoopChain) | Planned | Possible but more for private | Very low | Medium | Low (until coordinator-less) | Planned (Swirlds) |
| Public attack-resistance | n/a | n/a | High | Medium | High | Low (until more use) | Medium | Medium | Medium | Low (until more u | Medium (until full release) | Possible but more for private | Medium | Medium | Low (until coordinator-less) | Planned |
| Liveness or safety | n/a | n/a | Liveness | Liveness | Liveness | Safety | Safety | Liveness | Liveness | Safety | Liveness | Depending on the chosen type | Safety | Safety | Liveness | Liveness |
| Own tokens | n/a | n/a | Mining | Mining | ICO/Mining | ICO | ICO | ICO | ICO/Mining | ICO | ICO | n/a | Company allocation | Company allocation (unb | ICO | ICO |
| TPS (Visa usual needs 2000 TPS) | 200 | 50000 | 7 | 61 | 15 | 1000+ | 3000+ | 20000 | 20000 | 3000+ | 10 (planned for thousands) | Depending on the chosen type (max. 700) | 1500 | 1000 | 1500 (real-time stress much l | 100000 |
| Sidechain | n/a | n/a | Lightning | n/a | Raiden, Liquidity | n/a | n/a | Yes | Planned | n/a | Planned | n/a | n/a | n/a | n/a | n/a |
| Crosschain | n/a | n/a | n/a | n/a | n/a | Planned | n/a | n/a | Planned | Planned | Planned | n/a | n/a | n/a | n/a | n/a |
| Open-source | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Planned | Yes | Yes | Yes | Yes | Yes | Yes but patented |
| Programming language | n/a | n/a | C++ | C++ | Solidity | C#, Python… | C++ | C# | C++ | Python | Haskell, Plutus, Solidity… | Golang | Javascript | Javascript, Java, Go… | Java, Javascript, Python | Java, Solidity |
| Coding difficulty given available IDE | n/a | n/a | Medium | High | Medium | Easy | Medium | Easy | Medium | Low | Medium | Medium | Medium | Easy | Easy | Medium |
| Permission | Private | Private | Public | Public | Public | Public | Public | Public | Public | Public | Public | Private (and public in theory) | Private | Public | Public | Public |
| Smart contract | n/a | n/a | Limited | Limited | Yes | Yes (500 GAS to deploy) | Yes | Yes | Not yet | Planned | Yes | Yes | Limited to finance | Limited to finance |  | Yes |
| Transaction cost | e.g., 2,9% + fixed fee | e.g., 1,5% + fixed fee | Medium | Low | Medium | Low (if below 10GAS) | Low (may r | Low | Low | Planned (Low) | Planned (Medium) | Depending on the chosen type | Planned (Low) | Low | None | Medium |
| KYC/AML for its own currencies | Yes | Yes | No | No | No | No | No | No | No | KYC & AML | KYC | n/a | Yes | No | No | KYC & AML |
| KYC/AML for other created tokens | n/a | n/a | n/a | n/a | Not yet | Planned | Not yet | Helpers | Helpers | Planned | Not yet | Not yet | Not yet | Helpers | Not planned | Not yet |
| Privacy | n/a | n/a | n/a | n/a | n/a | n/a | n/a | Yes (option) | Yes (option) | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Community | Private | Private | Big | Small (but influent) | Big | Medium | Big | Small | Small | Small | Medium | Medium (backed by IBM…) | Medium (backed by banks.. | Medium | Medium | Medium |
| Peer-reviewed | Private | Private | Yes | No | Yes | No | No | No | No | No | Yes | No | No | Yes | No | Yes |
| Number of dApps/tokens/use-cases | n/a | n/a | Medium | Not planned | High | Low | Medium | Low | Low | Very low | Planned | Medium | Low | Low | Medium | Medium |
| Upgrades | n/a | n/a |  |  | PoS, sharding, plasma | Decentralization, refactoring, zero-knowledge proof |  |  |  |  |  |  |  |  | Coordinator-less, smart contracts |  |

# DLT Recommendation Summary

- Permission-based
  - If to be tied to a company isn't an issue:
    - If relations with legacy banks is important: Ripple
    - else: Hashgraph
  - else for an open-source customized blockchain: Hyperledger Fabric
- Permission-less
  - If it concerns payment transactions: Stellar
  - For Turing-complete smart contracts:
    - If Transactions Per Second (TPS) matter now: EOS
    - If own tokens generation and ecosystem matter more than TPS: Ethereum
    - Good candidates when ready:
      - Cardano
      - Hashgraph Hedera (if its attack-resistance get scientific peer-review and its patent constraints are non-blocking)
  - If it concerns rapid prototyping: NEO
  - If privacy features are needed: Stratis or Komodo

# DLT Evaluation Exercise

- Pick a token that hasn’t been evaluated in the slides and prepare a short evaluation presentation

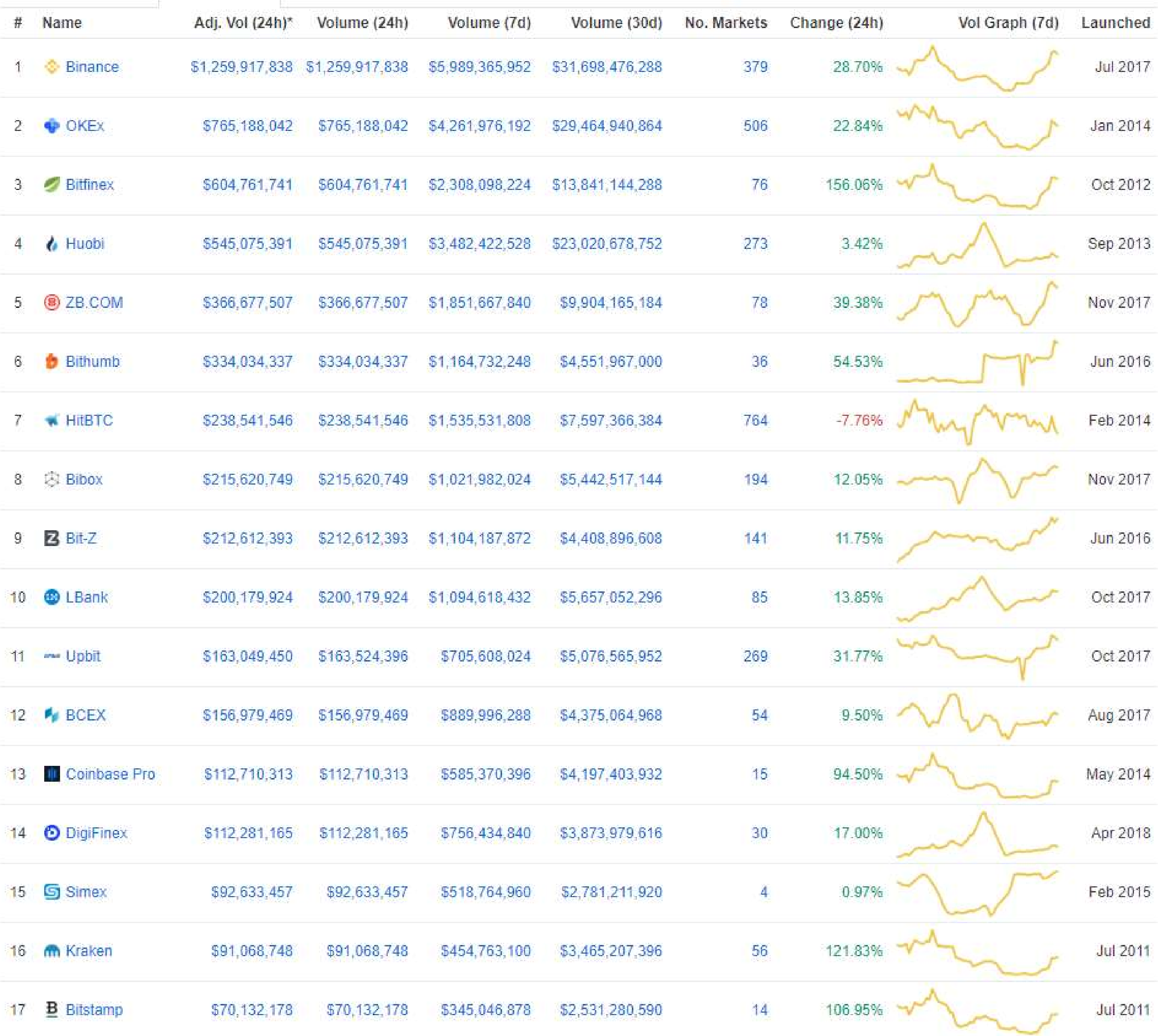
# dApp/project Exercise

- Think of a project that would benefit from be being built with a DLT
- Prepare a presentation arguing why the project would benefit form being built with a DLT and which DLT development platform would be the most appropriate
- Depict the overall technical architecture of the project and its main Application Programming Interface (API)

# Agenda

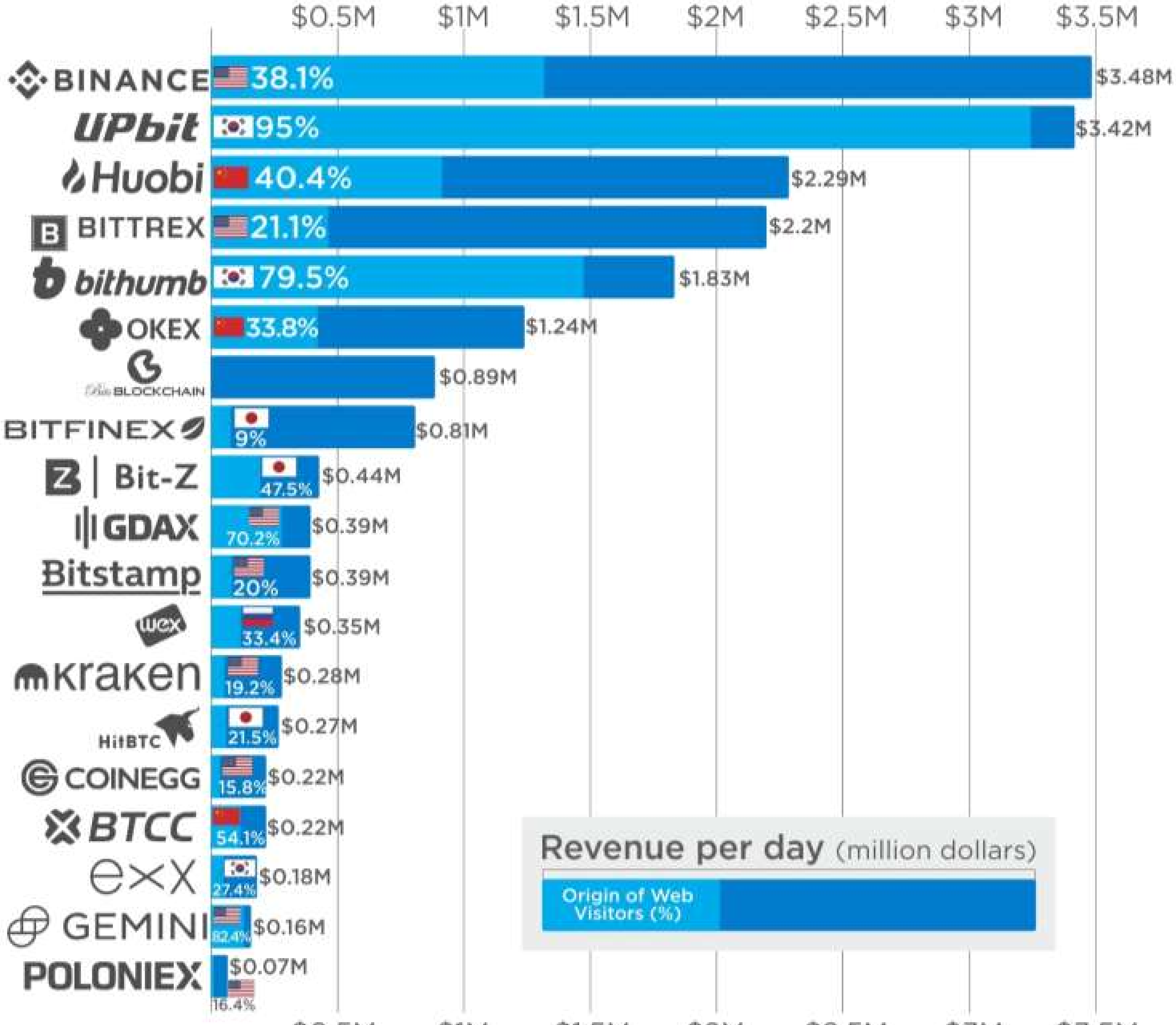
- Understanding the technology behind DLT
- Overview of current DLT development platforms
- How to select the most appropriate DLT for a specific dApp
- **Overview of current cryptocurrencies and tools**
- Initial Coin Offering (ICO), Token Generation Event (TGE) and tokenomics
- DLT trends

# CoinMarketCap Top Exchanges



| # | Name | Adj. Vol (24h)* | Volume (24h) | Volume (7d) | Volume (30d) | No. Markets | Change (24h) | Vol Graph (7d) | Launched |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Binance | $1,259,917,838 | $1,259,917,838 | $5,989,365,952 | $31,698,476,288 | 379 | 28.70% | | Jul 2017 |
| 2 | OKEx | $765,188,042 | $765,188,042 | $4,261,976,192 | $29,464,940,864 | 506 | 22.84% | | Jan 2014 |
| 3 | Bitfinex | $604,761,741 | $604,761,741 | $2,308,098,224 | $13,841,144,288 | 76 | 156.06% | | Oct 2012 |
| 4 | Huobi | $545,075,391 | $545,075,391 | $3,482,422,528 | $23,020,678,752 | 273 | 3.42% | | Sep 2013 |
| 5 | ZB.COM | $366,677,507 | $366,677,507 | $1,851,667,840 | $9,904,165,184 | 78 | 39.38% | | Nov 2017 |
| 6 | Bithumb | $334,034,337 | $334,034,337 | $1,164,732,248 | $4,551,967,000 | 36 | 54.53% | | Jun 2016 |
| 7 | HitBTC | $238,541,546 | $238,541,546 | $1,535,531,808 | $7,597,366,384 | 764 | -7.76% | | Feb 2014 |
| 8 | Bibox | $215,620,749 | $215,620,749 | $1,021,982,024 | $5,442,517,144 | 194 | 12.05% | | Nov 2017 |
| 9 | Bit-Z | $212,612,393 | $212,612,393 | $1,104,187,872 | $4,408,896,608 | 141 | 11.75% | | Jun 2016 |
| 10 | LBank | $200,179,924 | $200,179,924 | $1,094,618,432 | $5,657,052,296 | 85 | 13.85% | | Oct 2017 |
| 11 | Upbit | $163,049,450 | $163,524,396 | $705,608,024 | $5,076,565,952 | 269 | 31.77% | | Oct 2017 |
| 12 | BCEX | $156,979,469 | $156,979,469 | $889,996,288 | $4,375,064,968 | 54 | 9.50% | | Aug 2017 |
| 13 | Coinbase Pro | $112,710,313 | $112,710,313 | $585,370,396 | $4,197,403,932 | 15 | 94.50% | | May 2014 |
| 14 | DigiFinex | $112,281,165 | $112,281,165 | $756,434,840 | $3,873,979,616 | 30 | 17.00% | | Apr 2018 |
| 15 | Simex | $92,633,457 | $92,633,457 | $518,764,960 | $2,781,211,920 | 4 | 0.97% | | Feb 2015 |
| 16 | Kraken | $91,068,748 | $91,068,748 | $454,763,100 | $3,465,207,396 | 56 | 121.83% | | Jul 2011 |
| 17 | Bitstamp | $70,132,178 | $70,132,178 | $345,046,878 | $2,531,280,590 | 14 | 106.95% | | Jul 2011 |

# Crypto Exchanges Trading Revenues Per Day



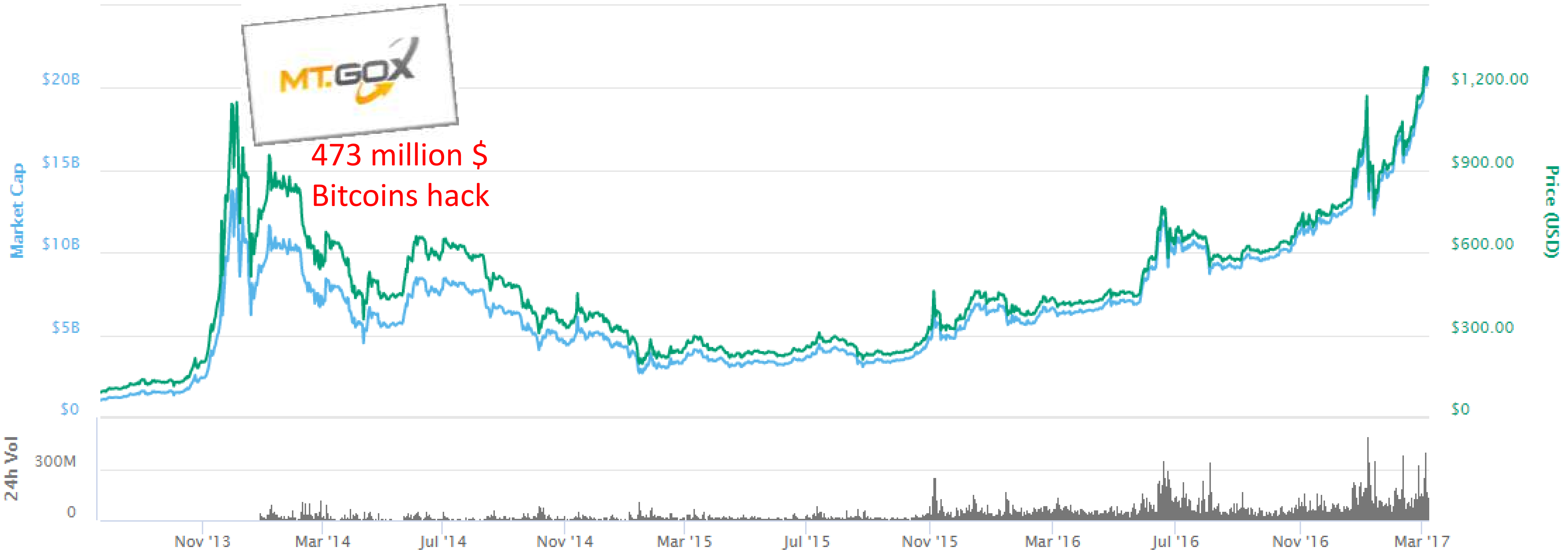
* Daily revenue estimated with CoinMarketCap reported 24Hr volume and fees listed on exchanges' websites.

** Percent of visitors estimated by Alexa.com. It does not necessarily represents the % of revenue but only the % of web visitors.

**Article & Sources:**
https://howmuch.net/articles/crypto-exchanges-revenue
https://www.bloomberg.com
https://www.alexa.com

howmuch net

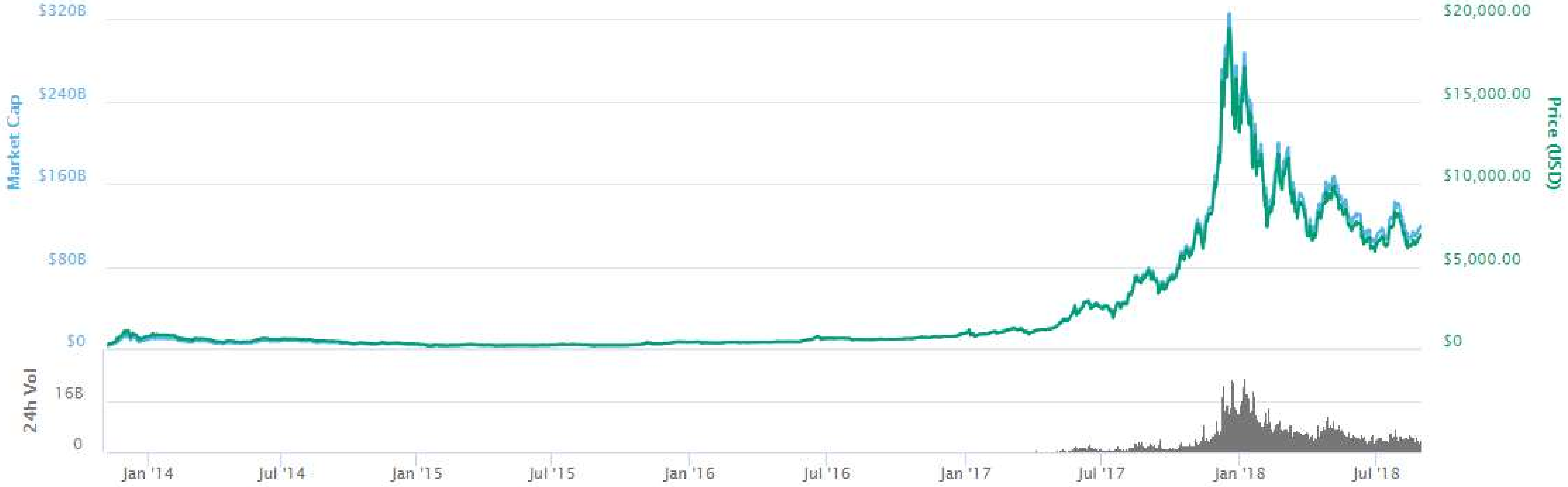
# CoinMarketCap 2013-2017



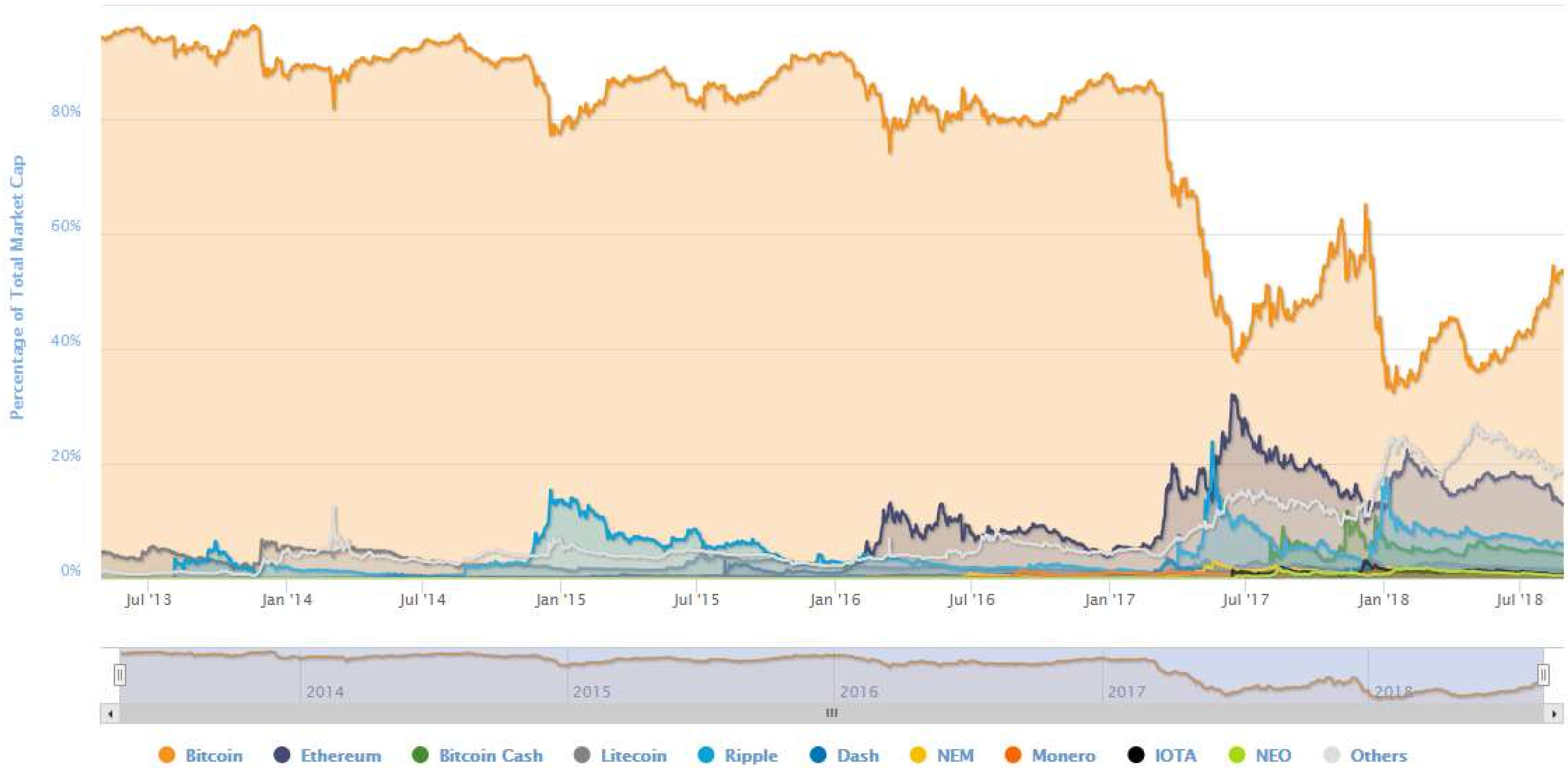
473 million $
Bitcoins hack

# CoinMarketCap 2014-2018

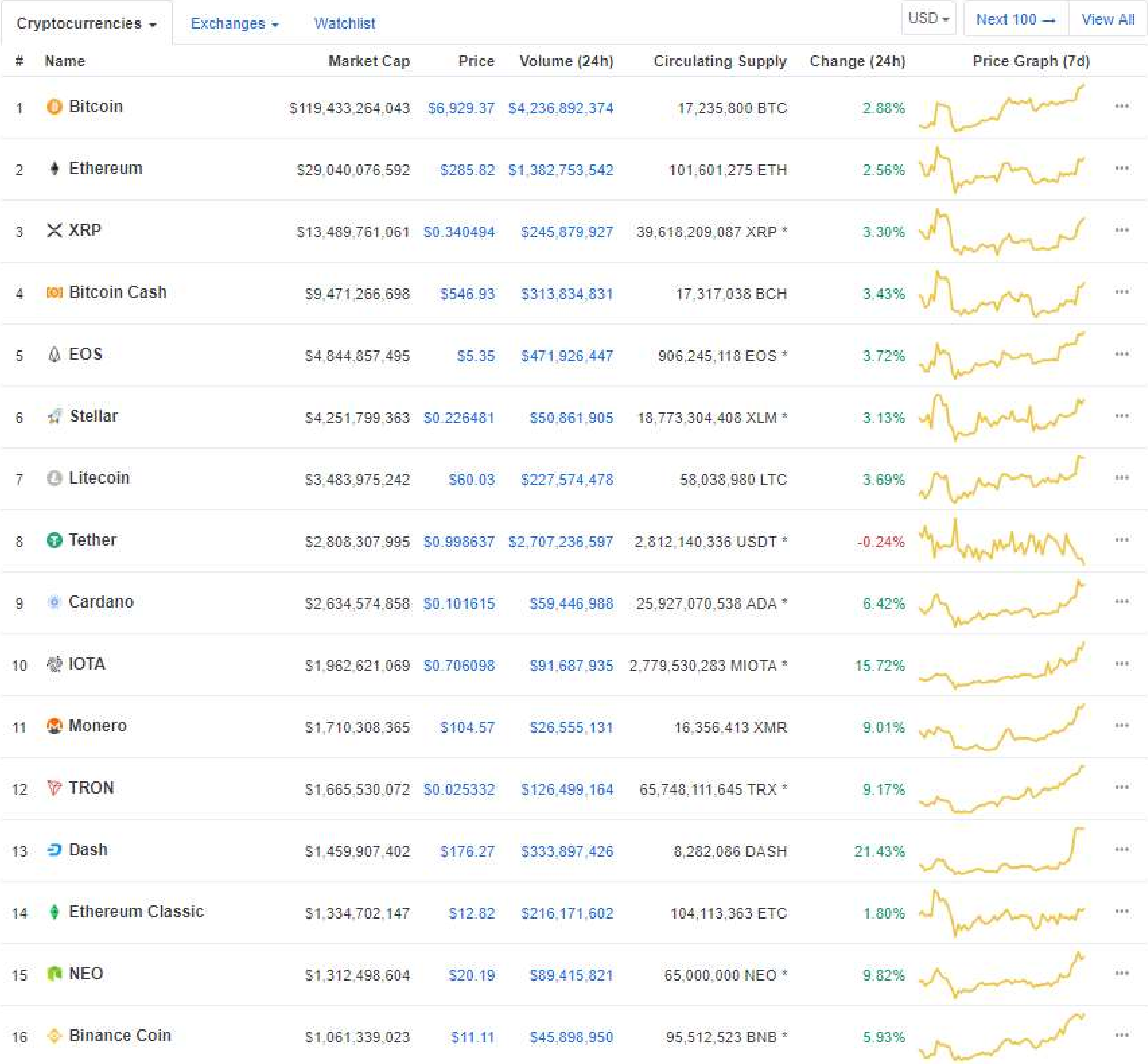
South Korea
crackdown on its major
crypto exchanges



# CoinMarketCap Bitcoin Dominance

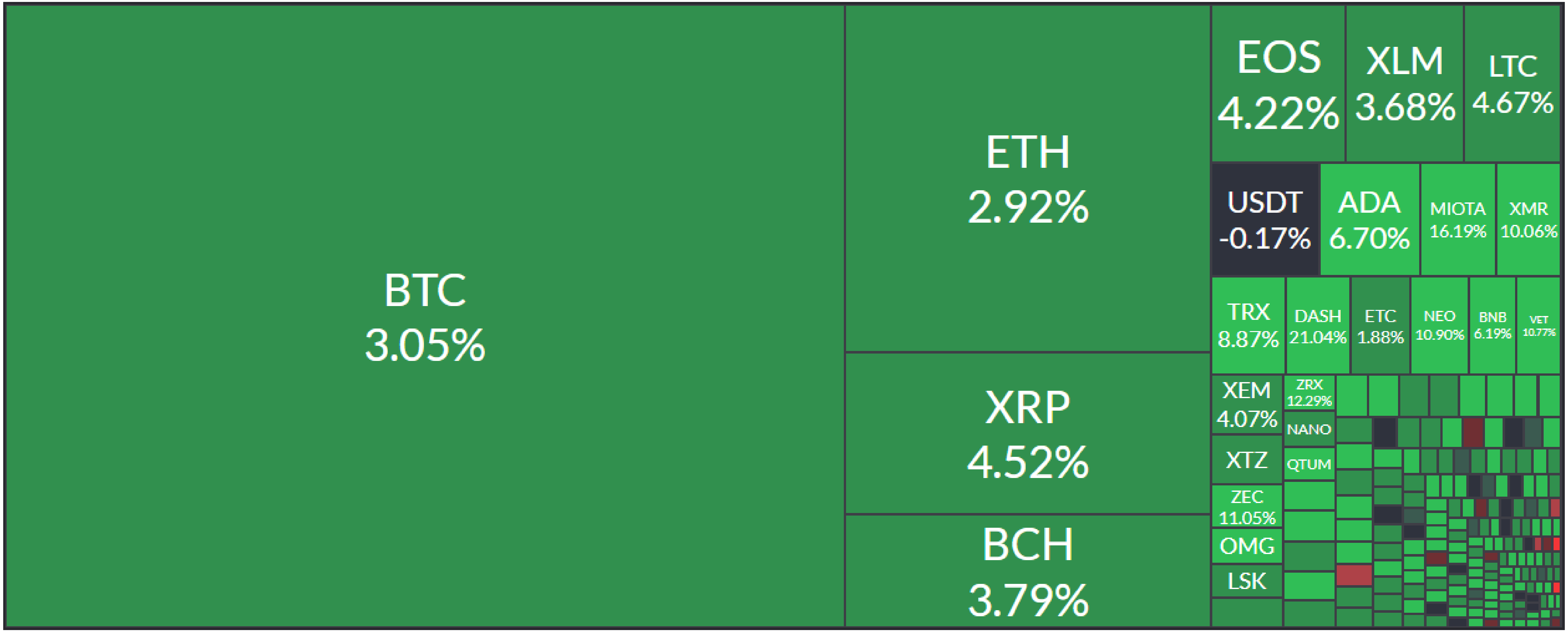


# CoinMarketCap Top Tokens



| # | Name | Market Cap | Price | Volume (24h) | Circulating Supply | Change (24h) | Price Graph (7d) |
|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | $119,433,264,043 | $6,929.37 | $4,236,892,374 | 17,235,800 BTC | 2.88% | |
| 2 | Ethereum | $29,040,076,592 | $285.82 | $1,382,753,542 | 101,601,275 ETH | 2.56% | |
| 3 | XRP | $13,489,761,061 | $0.340494 | $245,879,927 | 39,618,209,087 XRP * | 3.30% | |
| 4 | Bitcoin Cash | $9,471,266,698 | $546.93 | $313,834,831 | 17,317,038 BCH | 3.43% | |
| 5 | EOS | $4,844,857,495 | $5.35 | $471,926,447 | 906,245,118 EOS * | 3.72% | |
| 6 | Stellar | $4,251,799,363 | $0.226481 | $50,861,905 | 18,773,304,408 XLM * | 3.13% | |
| 7 | Litecoin | $3,483,975,242 | $60.03 | $227,574,478 | 58,038,980 LTC | 3.69% | |
| 8 | Tether | $2,808,307,995 | $0.998637 | $2,707,236,597 | 2,812,140,336 USDT * | -0.24% | |
| 9 | Cardano | $2,634,574,858 | $0.101615 | $59,446,988 | 25,927,070,538 ADA * | 6.42% | |
| 10 | IOTA | $1,962,621,069 | $0.706098 | $91,687,935 | 2,779,530,283 MIOTA * | 15.72% | |
| 11 | Monero | $1,710,308,365 | $104.57 | $26,555,131 | 16,356,413 XMR | 9.01% | |
| 12 | TRON | $1,665,530,072 | $0.025332 | $126,499,164 | 65,748,111,645 TRX * | 9.17% | |
| 13 | Dash | $1,459,907,402 | $176.27 | $333,897,426 | 8,282,086 DASH | 21.43% | |
| 14 | Ethereum Classic | $1,334,702,147 | $12.82 | $216,171,602 | 104,113,363 ETC | 1.80% | |
| 15 | NEO | $1,312,498,604 | $20.19 | $89,415,821 | 65,000,000 NEO * | 9.82% | |
| 16 | Binance Coin | $1,061,339,023 | $11.11 | $45,898,950 | 95,512,523 BNB * | 5.93% | |

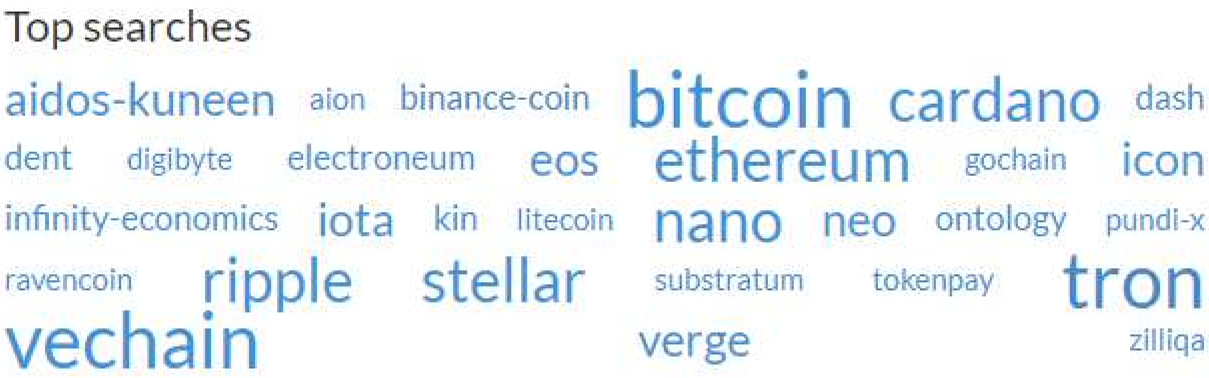
# BitScreener Crypto Market Heatmap



Size: market capitalization. Color: 24h performance

# Cryptocurrencies Search Volume and Traffic

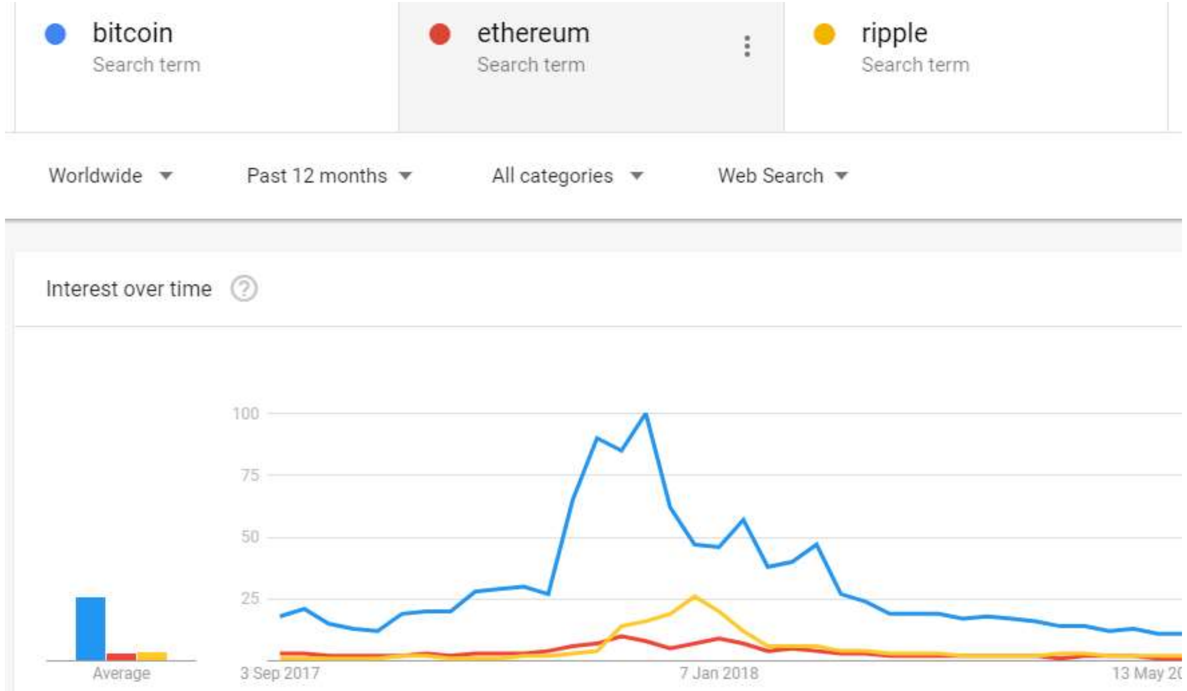
- Bitscreener Top Searches



Top searches

aidos-kuneen aion binance-coin bitcoin cardano dash dent digibyte electroneum eos ethereum gochain icon infinity-economics iota kin litecoin nano neo ontology pundi-x ravencoin ripple stellar substratum tokenpay tron vechain verge zilliqa

- Google Trends



● bitcoin
Search term

● ethereum
Search term

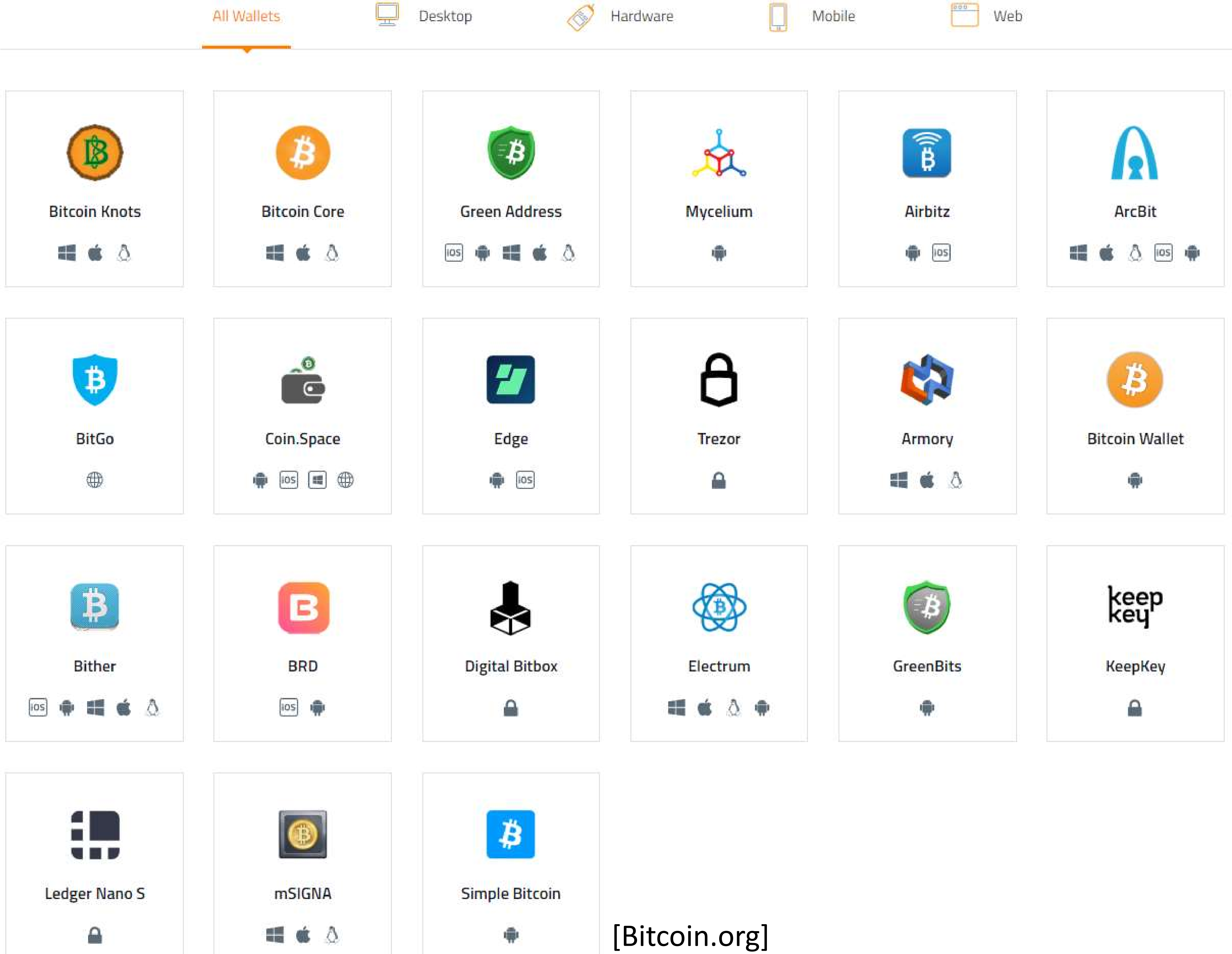
● ripple
Search term

Worldwide ▾ Past 12 months ▾ All categories ▾ Web Search ▾

Interest over time

- SimilarWeb

# Crypto Wallets



All Wallets

Desktop

Hardware

Mobile

Web

Bitcoin Knots

Bitcoin Core

Green Address

Mycelium

Airbitz

ArcBit

BitGo

Coin.Space

Edge

Trezor

Armory

Bitcoin Wallet

Bither

BRD

Digital Bitbox

Electrum

GreenBits

KeepKey

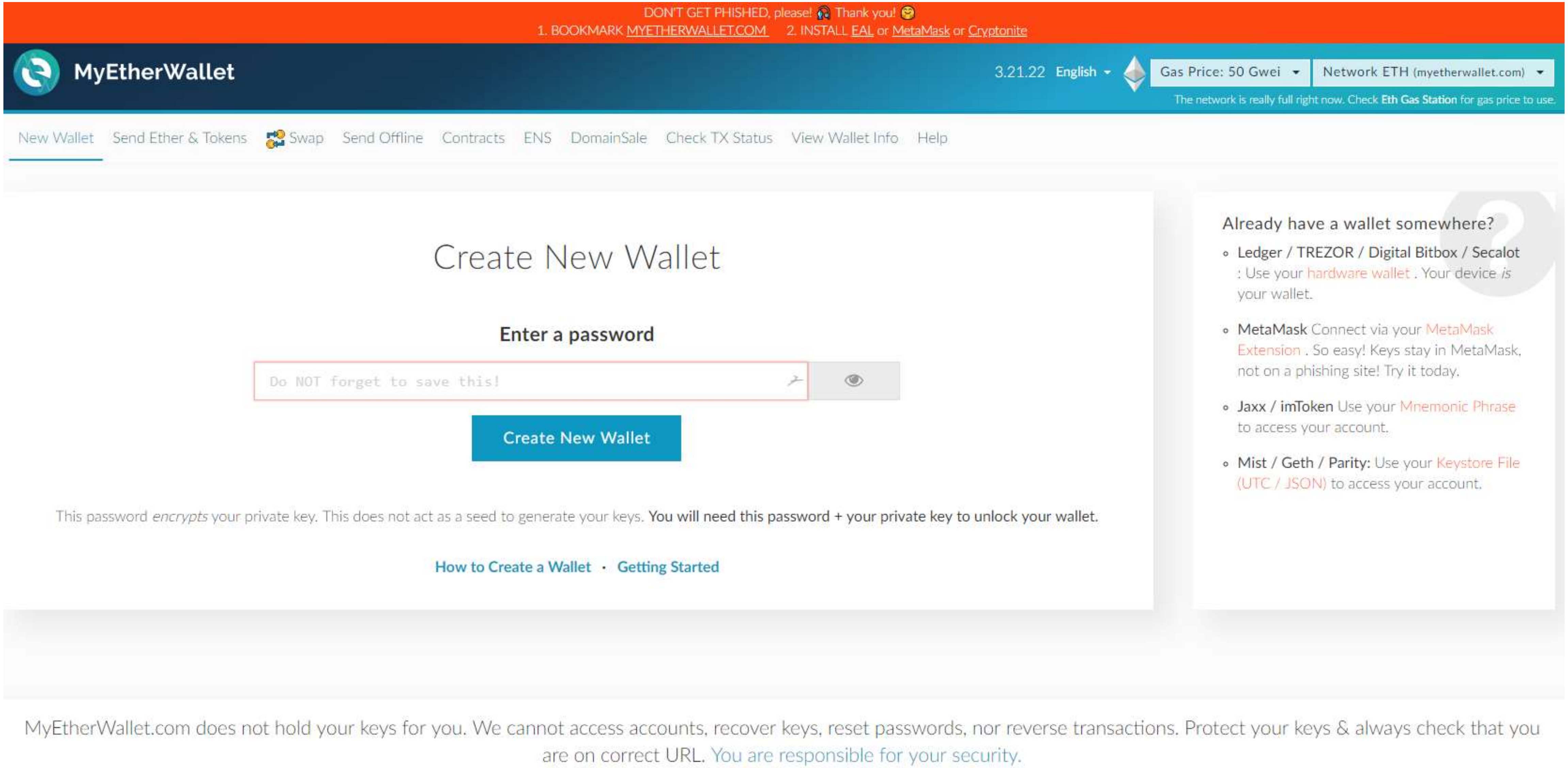
Ledger Nano S

mSIGNA

Simple Bitcoin

[Bitcoin.org]

# Exercise with My Ether Wallet (MEW)



DON'T GET PHISHED, please! Thank you!

1. BOOKMARK MYETHERWALLET.COM 2. INSTALL EAL or MetaMask or Cryptonite

The network is really full right now. Check **Eth Gas Station** for gas price to use.

Create New Wallet

**Enter a password**

Do NOT forget to save this!

This password *encrypts* your private key. This does not act as a seed to generate your keys. **You will need this password + your private key to unlock your wallet.**

How to Create a Wallet · Getting Started

Already have a wallet somewhere?

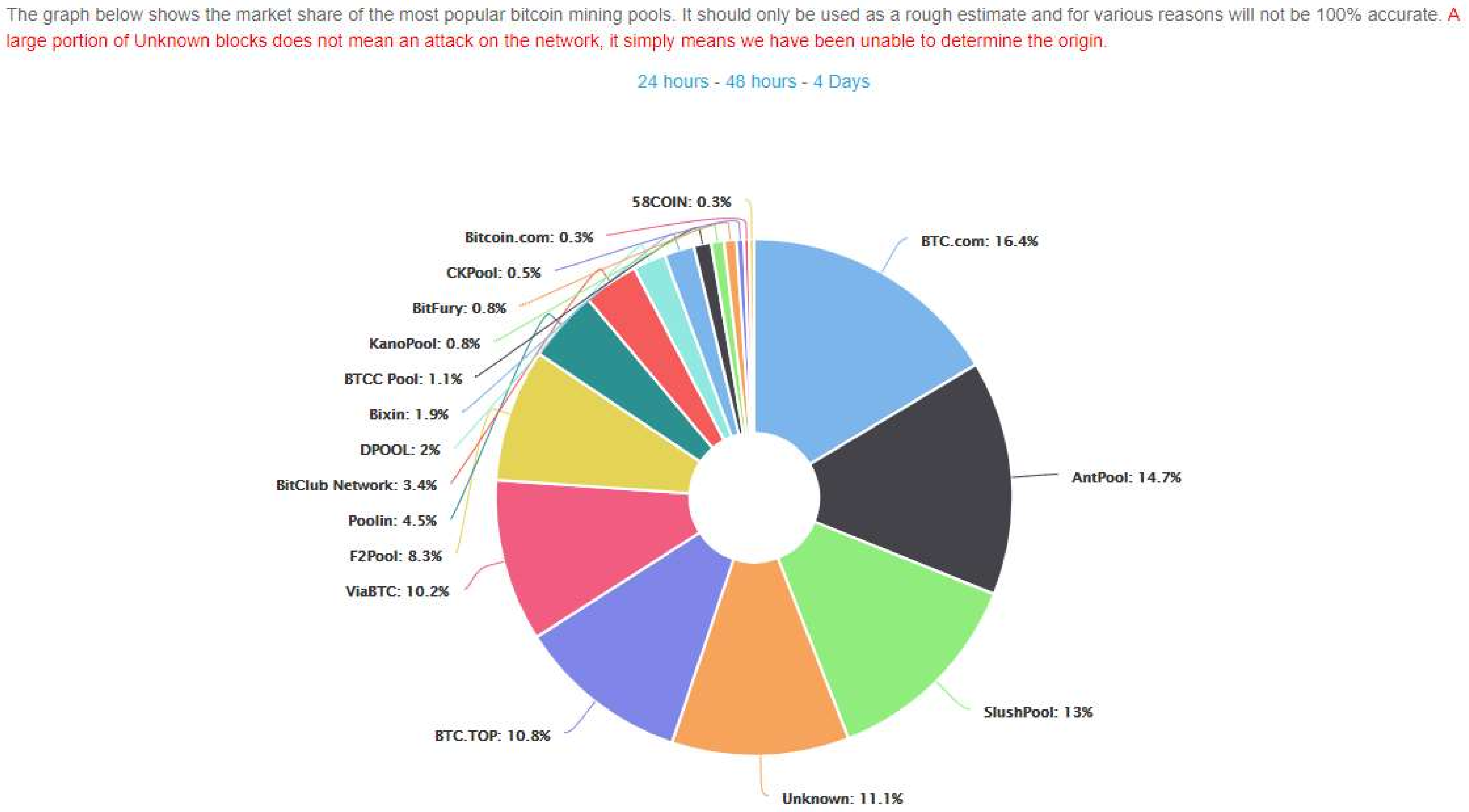
- Ledger / TREZOR / Digital Bitbox / Secalot : Use your hardware wallet . Your device *is* your wallet.
- MetaMask Connect via your MetaMask Extension . So easy! Keys stay in MetaMask, not on a phishing site! Try it today.
- Jaxx / imToken Use your Mnemonic Phrase to access your account.
- Mist / Geth / Parity: Use your Keystore File (UTC / JSON) to access your account.

MyEtherWallet.com does not hold your keys for you. We cannot access accounts, recover keys, reset passwords, nor reverse transactions. Protect your keys & always check that you are on correct URL. You are responsible for your security.

# Blockchain/DLT Explorers

- Each DLT should have has its own explorer to:
  - Watch the block/transaction feed
  - See transaction history of a given address
  - See input and output of transactions
  - Check the current utility token fee for transactions
  - …
- Bitcoin Explorers:
  - https://live.blockcypher.com/btc/ with current fees estimates
  - https://www.blocktrail.com/BTC
- Ethereum Explorers:
  - https://etherscan.io/
  - https://ethplorer.io/ especially if interested by the ERC20 tokens of an address
- Other explorers:
  - https://neotracker.io/ NEO
  - https://eostracker.io/ EOS
  - https://www.coinfirm.io/ risk explorer for Bitcoin and Ethereum addresses

# Blockchain.com Bitcoin Hashrate Distribution



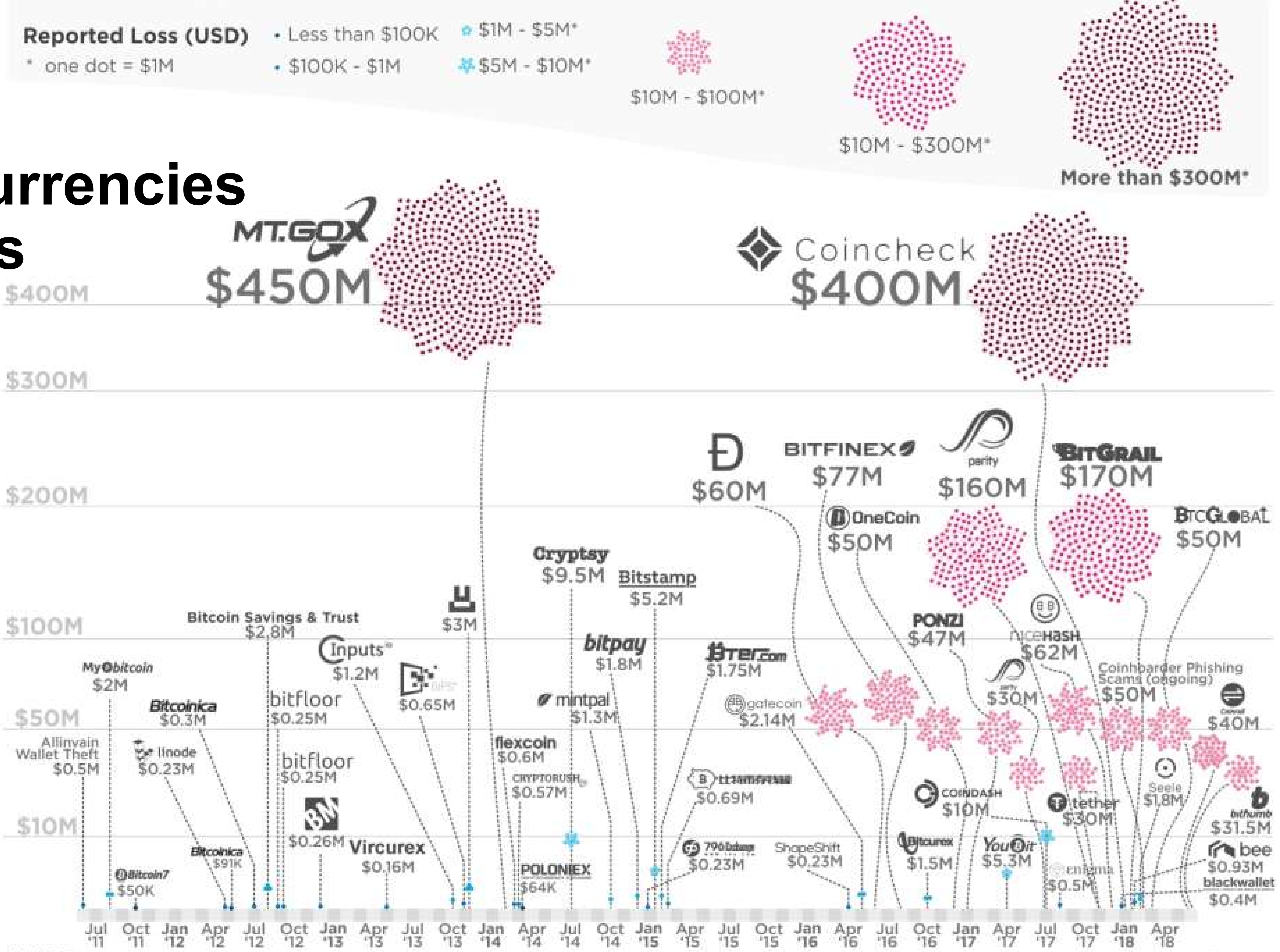
The graph below shows the market share of the most popular bitcoin mining pools. It should only be used as a rough estimate and for various reasons will not be 100% accurate. A large portion of Unknown blocks does not mean an attack on the network, it simply means we have been unable to determine the origin.

24 hours - 48 hours - 4 Days

# Risks of Crypto Trading

- Centralized exchanges own the private keys and may be hacked or disappear (it has happened several times)
  - They have to carry out KYC and AML on your profile and the identity information that you give them may be used for identity theft
- Person-to-person trading, also known as Over The Counter (OTC), is risky because the trader may try to cheat or steal you
  - https://localbitcoins.com/ may help regarding OTC
- In some countries, such trading may involve high and complicated taxes or may even be forbidden.
- Cryptocurrencies are highly volatile and periods of large gains have already happened
- ICOs are even riskier because there have been lots of scams and a lot of marketing is spent to make them appealing
- Due to lack of regulations, laws and use of remote locations for exchanges and ICOs, legal recourses may be impossible.

# Biggest Cryptocurrencies Hacks and Scams



Article & Sources:
https://howmuch.net/articles/biggest-cryptocurrency-hacks-scams
https://howmuch.net/sources/biggest-cryptocurrency-hacks-scams

howmuch net

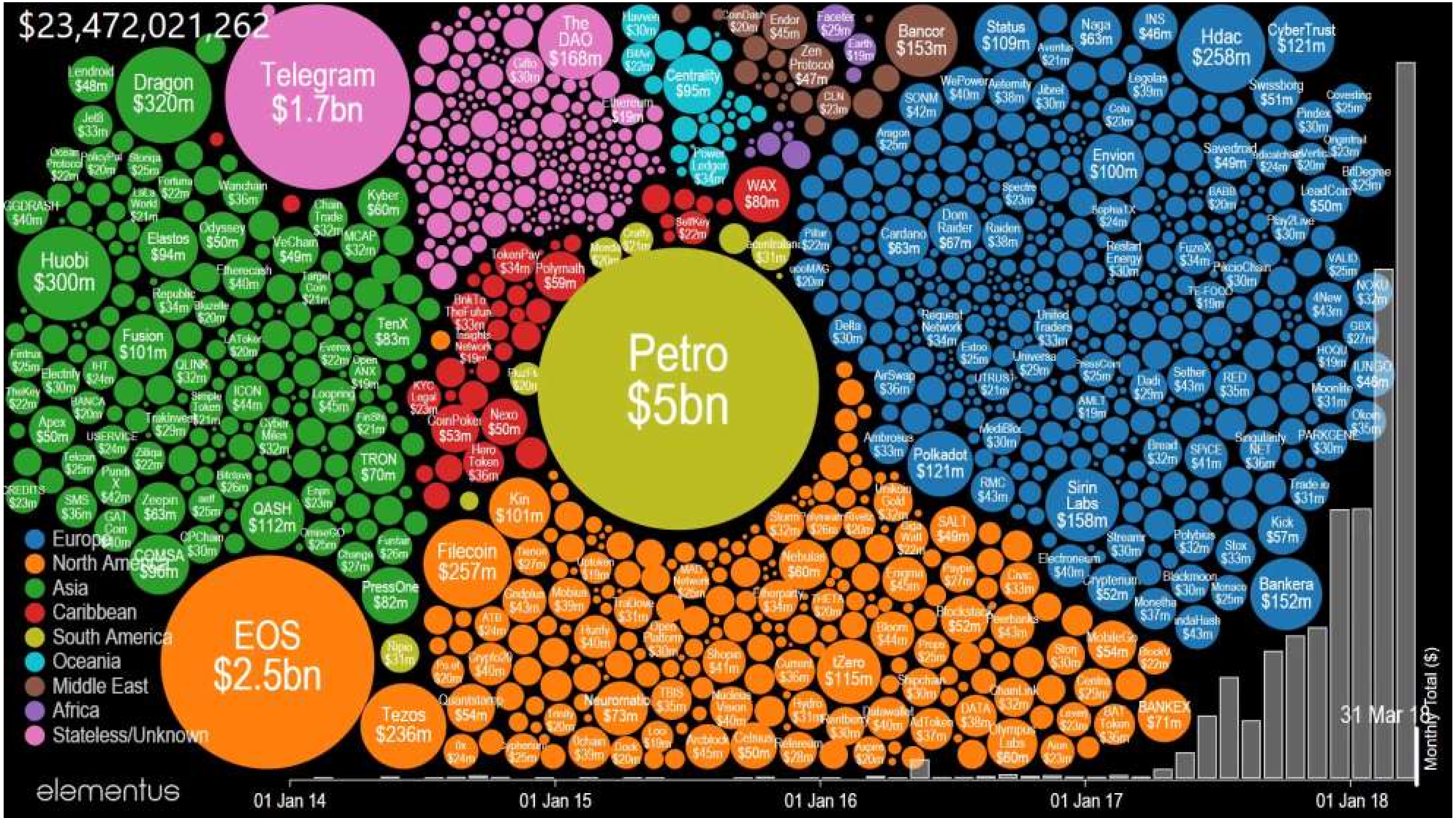
# Agenda

- Understanding the technology behind DLT
- Overview of current DLT development platforms
- How to select the most appropriate DLT for a specific dApp
- Overview of current cryptocurrencies and tools
- **Initial Coin Offering (ICO), Token Generation Event (TGE) and tokenomics**
- DLT trends

# Difference between ICO and TGE

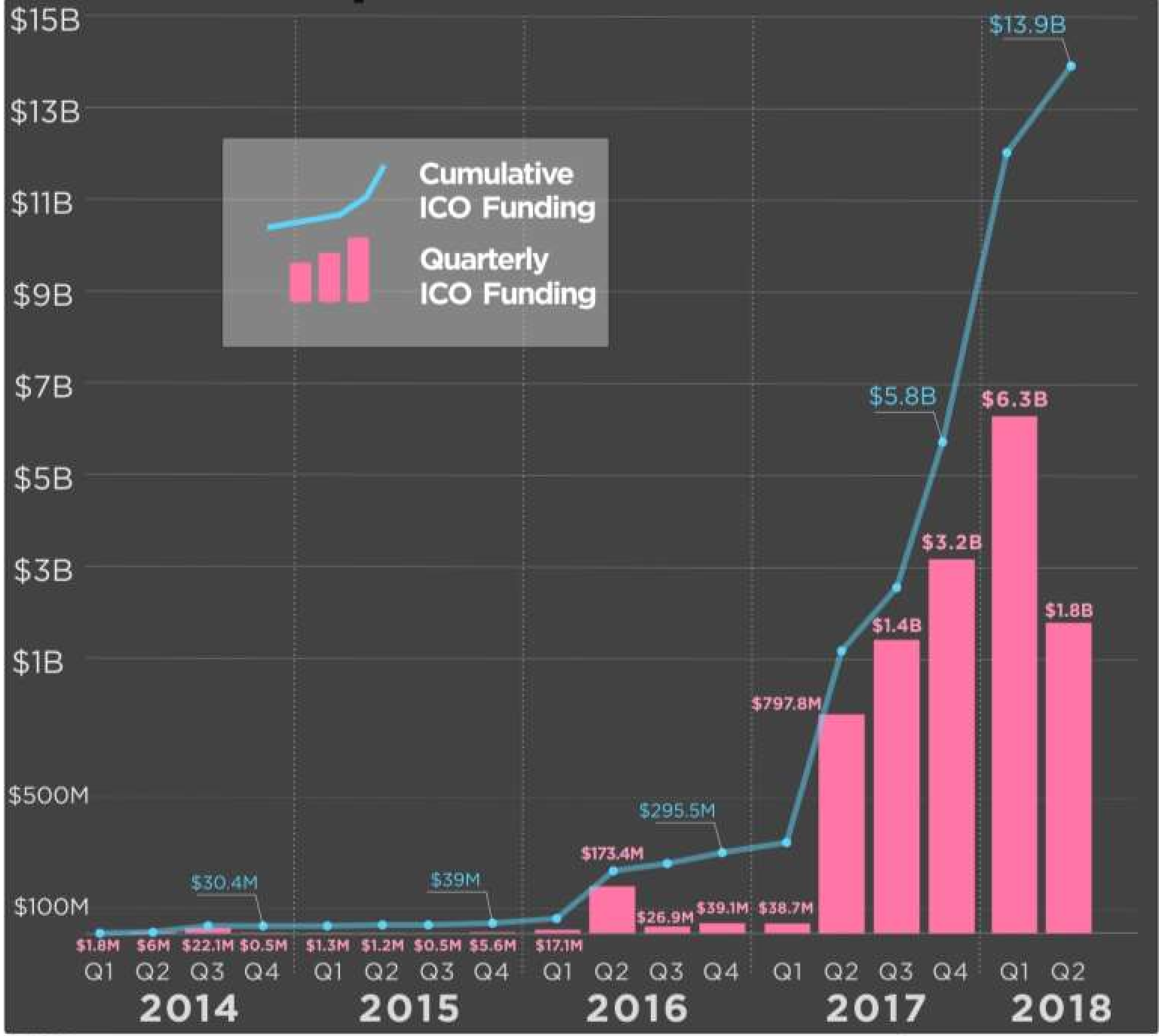
- Initial Coin Offerings (ICO) are associated to projects proposing a way to profit to the tokens buyers who are therefore more considered as investors
  - The generated tokens are most likely considered as security tokens
  - In many countries, selling securities require to comply to laws and regulations, sometime including how it should be publicly communicated
- Token Generation Events (TGE) concern tokens that are generated to use the functionalities of the system
  - The generated tokens are most likely considered as utility tokens, especially if the system where they can be used already exists at time of the TGE
  - There are many legal aspects to take into account to minimize the risks of having a TGE be reclassified as an illegal sale of securities and in each country where the tokens are sold.
- Thus, having legal advice from lawyers specialized in ICOs/TGEs is mandatory anyway

# History of ICOs



[elementus.io]

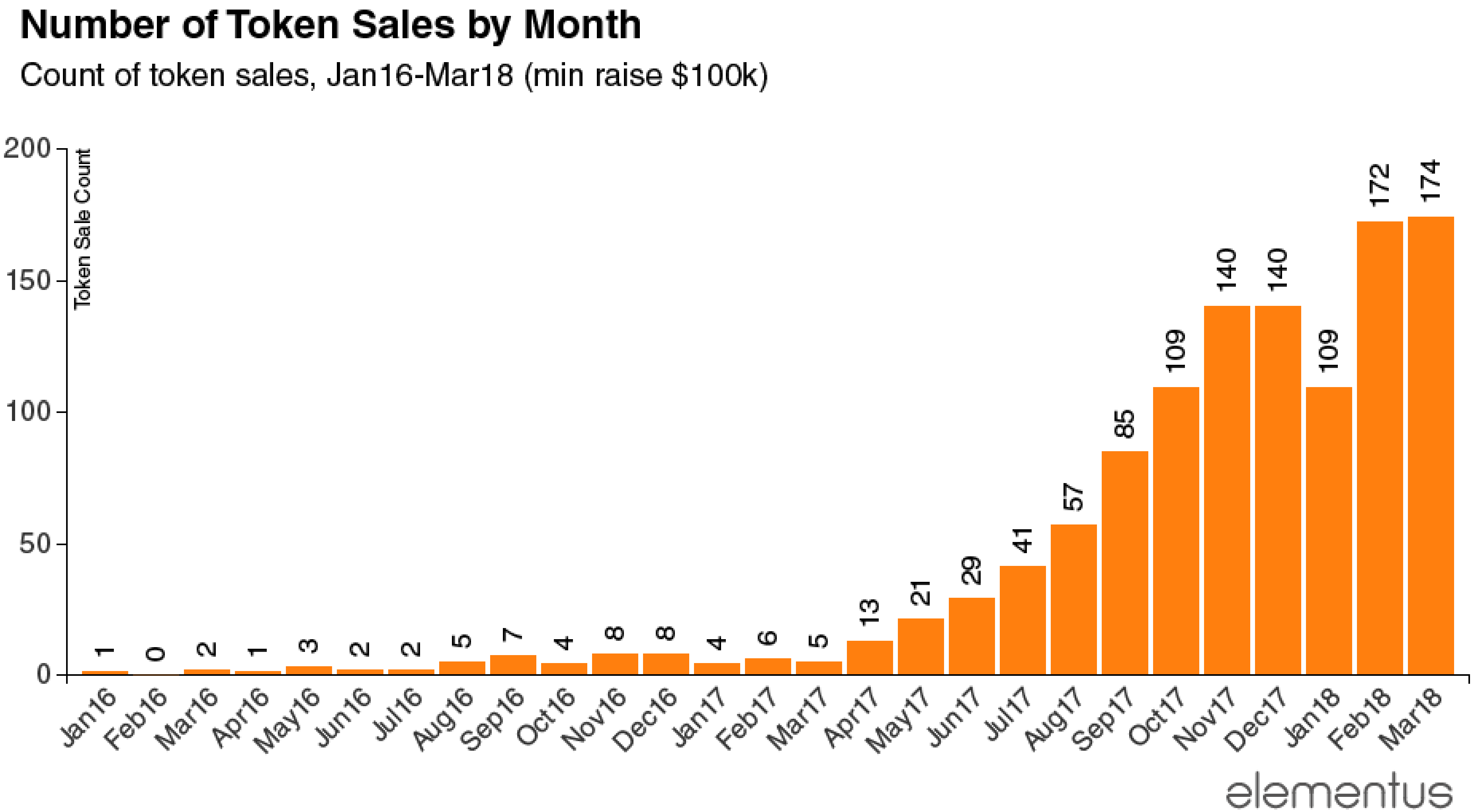
# Cumulative ICOs Funding



Article & Sources:
https://howmuch.net/articles/the-ico-explosion-in-the-past-5-years
https://www.coindesk.com/ico-tracker/

howmuch net

# Token Sales Evolution



# Tokenomics

- The tokenomics concern the economics of the generated tokens.
  - What will they be used for (utility, voting rights, shares…)?
  - What will be their initial price?
    - Are there any discounts based on time, quantity bought…?
  - How many will be generated?
    - Is there a maxcap (maximum money raised when the event is stopped)? a softcap (minimum money raised for the project to continue, otherwise refund)?
    - Depending on whether or not the maxcap will be reached at the end of the generation event, what will happen to the remaining tokens (burnt, reallocated proportionally to the existing token buyers, kept for another TGE…)?
  - How and when will they be generated (auction type, by smart contract…)?
  - Are there any fees kept (for account creation, transaction fees in case of refund…)?
  - What will be their distribution?
    - How many for the team? Any vesting periods? How many reserved for the company, private sale, pre-sale, crowdsale…?
    - How many given as bounty (online marketing tasks, security holes…) and airdrop (sent to a selection of crypto addresses)?
  - Are there interests or more tokens generated via mining, staking, masternodes or other contributions to the system?
  - What will be the use of proceeds of the TGE and roadmap?

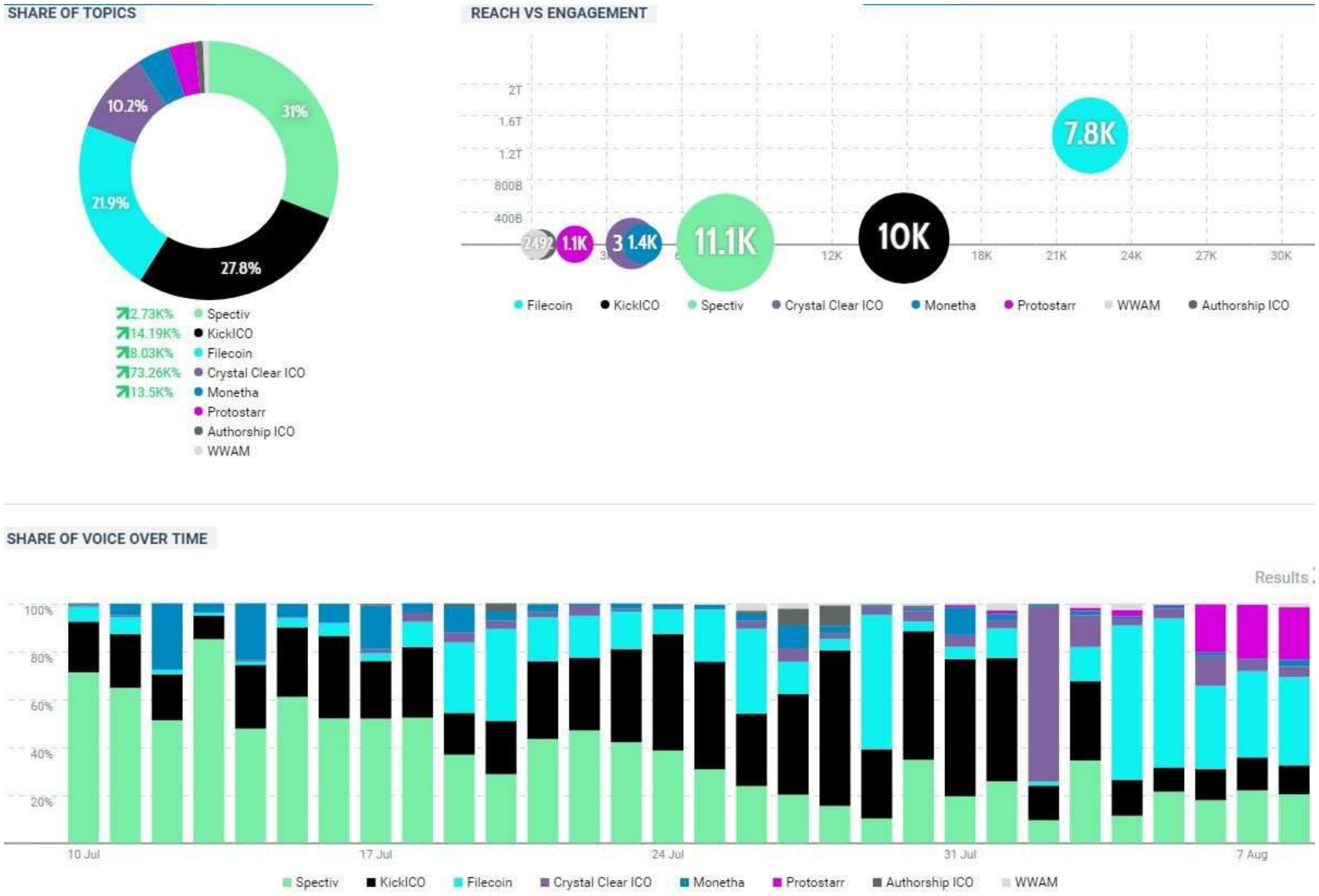
# Main Steps of an ICO/TGE

- Definition of the tokenomics including team and advisors allocation
- Legal aspects validated by a legal partner specialized in ICO/TGE (selection of appropriate countries and nationalities, drafting contracts, legal aid throughout the project…)
- Creation of the whitepaper, other marketing documents, Website and specific online channels
- Selection of the ICO/TGE and smart contract platform most suited to the project according to:
  - functionalities envisaged by the potential decentralized application (dApp) or project
  - clients and investors targeted by the ICO/TGE
- Creation, validation and audit of the smart contract in collaboration with expert DLT developers
- Specialized digital marketing that will attract and convince token buyers with the help of online reputation management (ORM) to select the most influential media whilst respecting regulations communication constraints
  - If allowed, management of the bounty program: from translations to buzz and paid advertising
- Pre-ICO/TGE to contact and convince important investors (private sale, pre-sale…)
- Opening of the ICO/TGE smart contract to the crowdsale with required KYC and AML checks
- Safety and good practices during the ICO/TGE (beware of phishing, denial of service…)
- ICO/TGE ongoing e-reputation monitoring and optimization of investment visits conversions
- After ICO/TGE (release of the tokens, connection with exchanges if allowed…)

# ORM applied to ICO/TGE

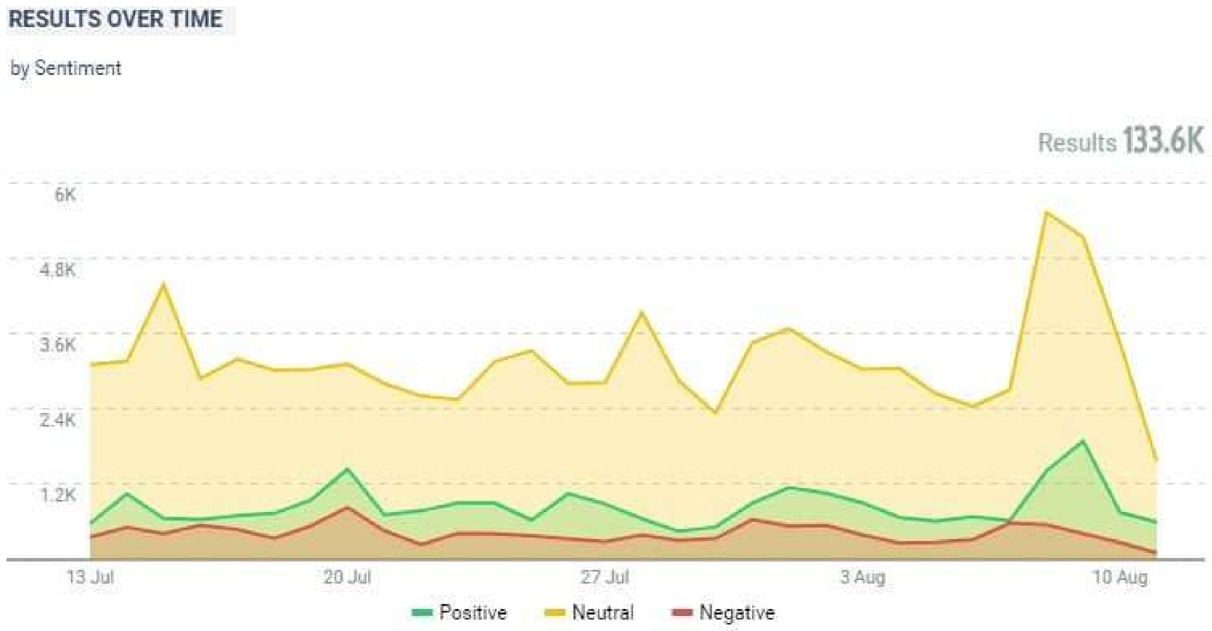
- ICO/TGE and cryptocurrencies value are strongly impacted by the news
  - « Buy the rumor, sell the news »
  - Fear, Uncertainty and Doubt (FUD)
  - SCAM
  - Bounty
  - Fear Of Missing Out (FOMO)
  - Pump & Dump (https://pumpdump.coincheckup.com/)
- Therefore it is an advantage to use Online Reputation Management (ORM) to
  - Know important news before the others in order to buy or sell at the best time
  - Identify fake news
  - Optimize ICO/TGE and cryptocurrencies digital marketing

# ORM Monitoring Example

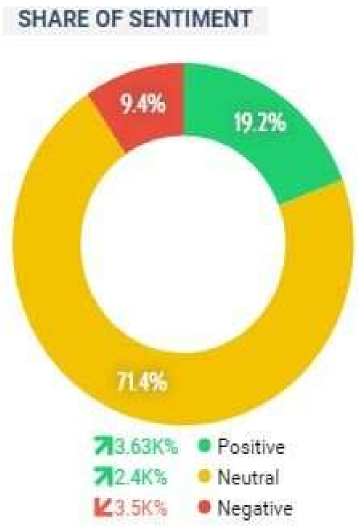


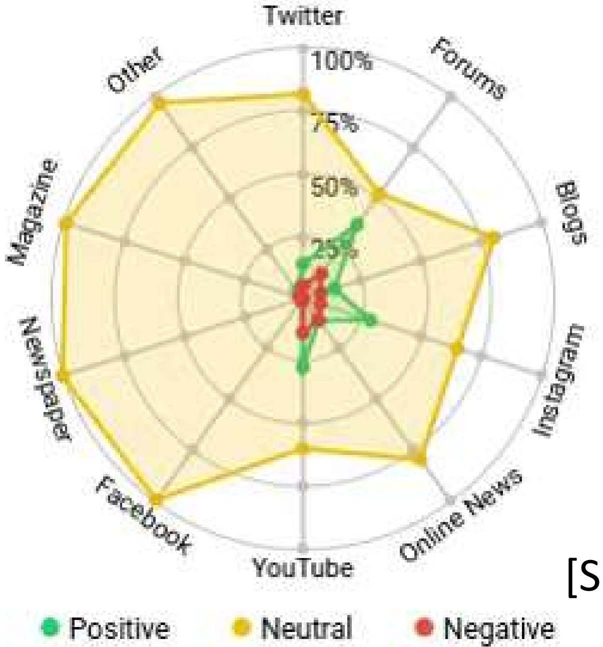
[Seigneur]

# Litecoin ORM Sentiment Analysis Example


RESULTS OVER TIME

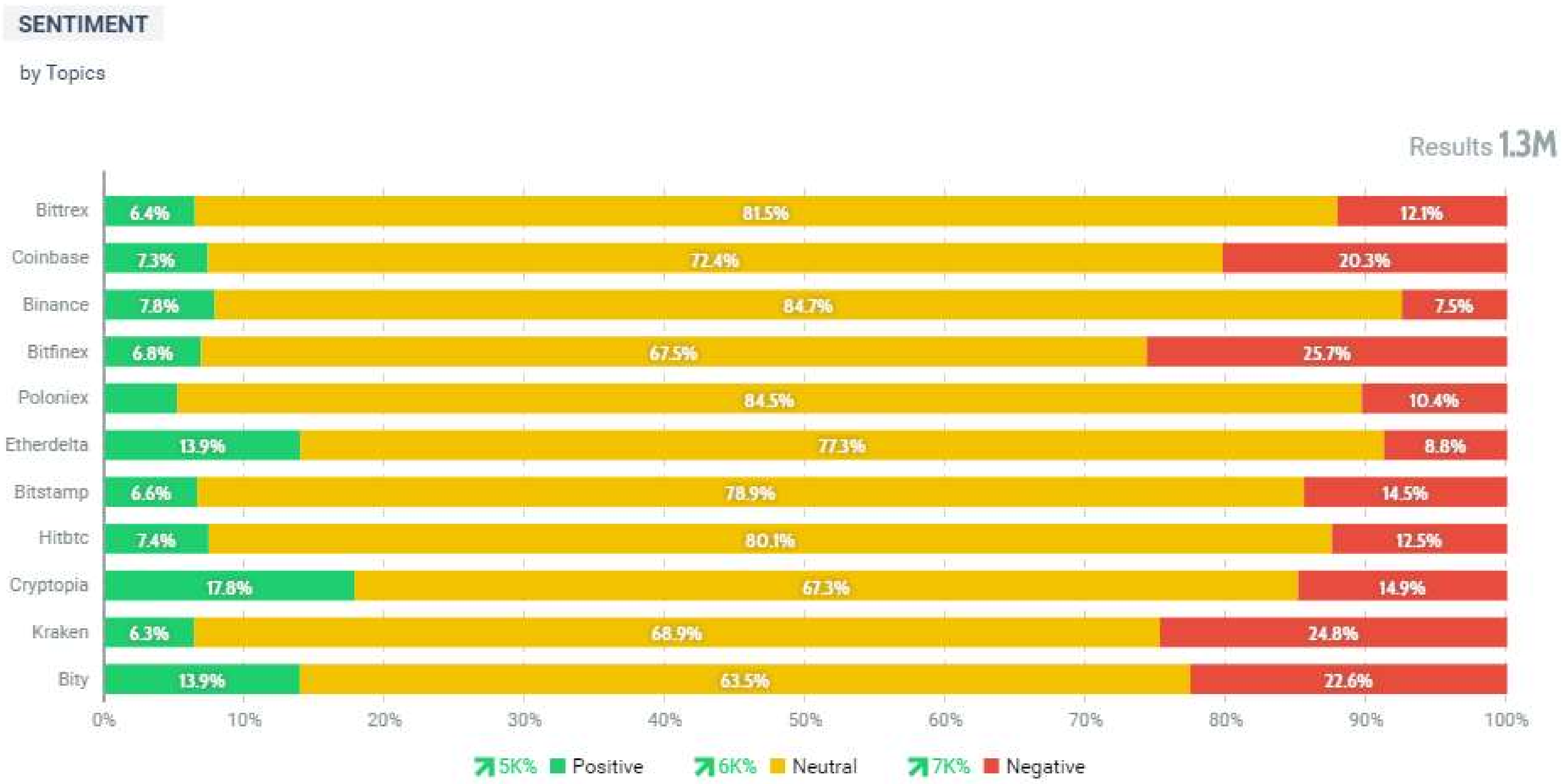
by Sentiment


SHARE OF SENTIMENT



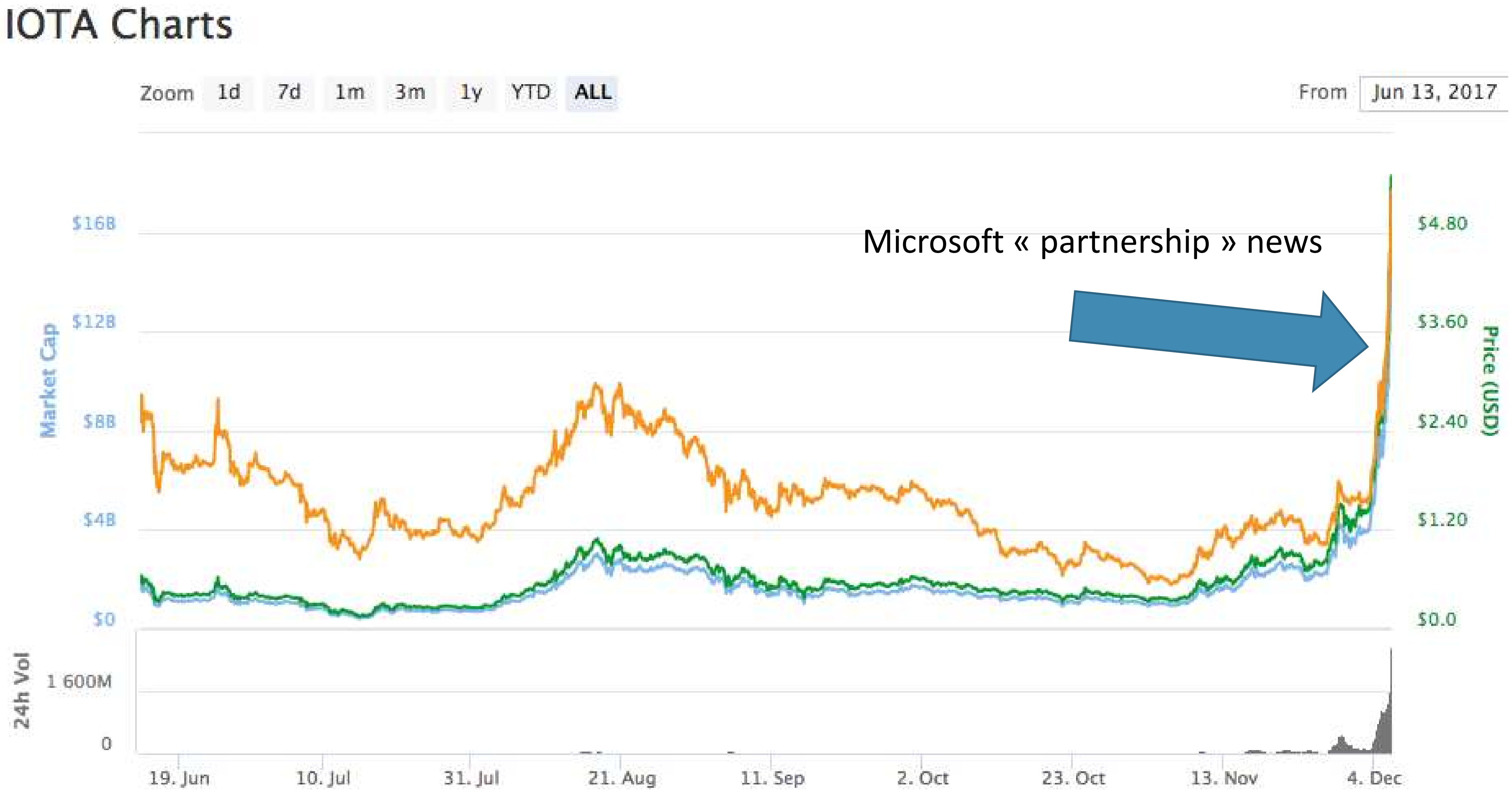
[Seigneur]

# Exchanges ORM Sentiment Analysis



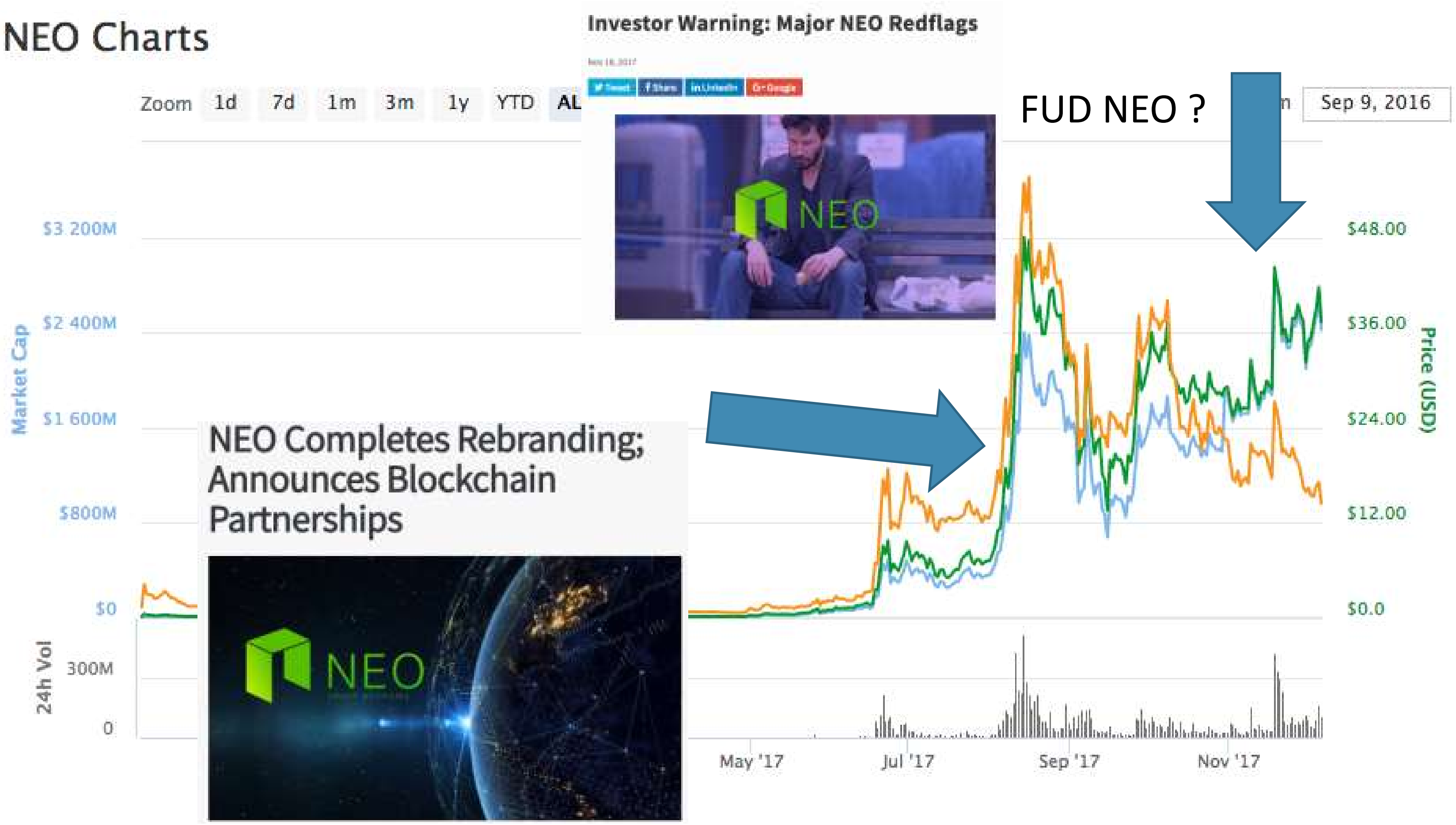
[Seigneur]

# IOTA Breakout Reason?



Microsoft « partnership » news

# NEO Value Evolution Reason?



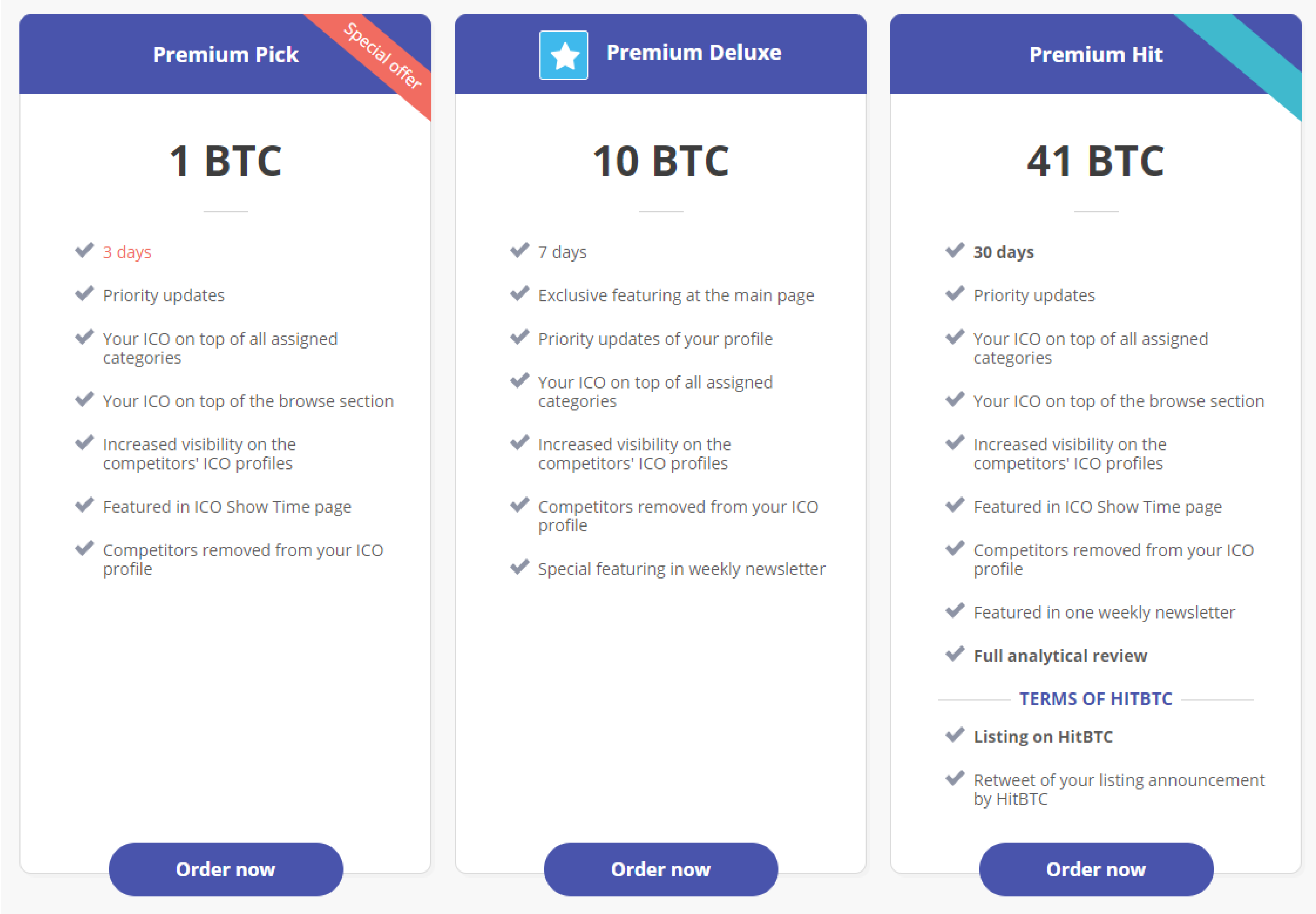
NEO Charts

Investor Warning: Major NEO Redflags

NEO Completes Rebranding; Announces Blockchain Partnerships

FUD NEO ?

# ICOBench Pricing



## Premium Pick

**1 BTC**

- ✓ 3 days
- ✓ Priority updates
- ✓ Your ICO on top of all assigned categories
- ✓ Your ICO on top of the browse section
- ✓ Increased visibility on the competitors' ICO profiles
- ✓ Featured in ICO Show Time page
- ✓ Competitors removed from your ICO profile

## Premium Deluxe

**10 BTC**

- ✓ 7 days
- ✓ Exclusive featuring at the main page
- ✓ Priority updates of your profile
- ✓ Your ICO on top of all assigned categories
- ✓ Increased visibility on the competitors' ICO profiles
- ✓ Competitors removed from your ICO profile
- ✓ Special featuring in weekly newsletter

## Premium Hit

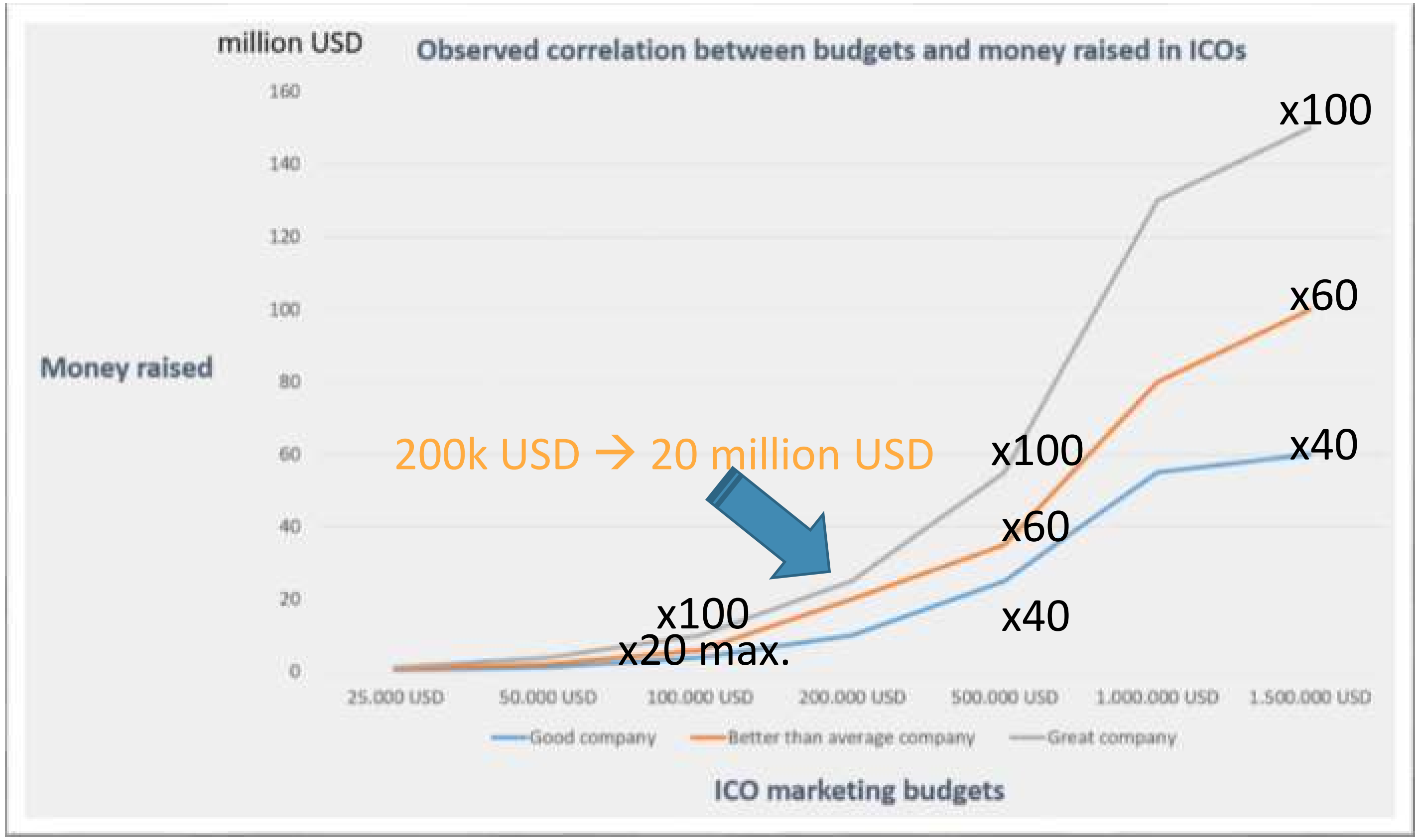
**41 BTC**

- ✓ **30 days**
- ✓ Priority updates
- ✓ Your ICO on top of all assigned categories
- ✓ Your ICO on top of the browse section
- ✓ Increased visibility on the competitors' ICO profiles
- ✓ Featured in ICO Show Time page
- ✓ Competitors removed from your ICO profile
- ✓ Featured in one weekly newsletter
- ✓ **Full analytical review**

**TERMS OF HITBTC**

- ✓ **Listing on HitBTC**
- ✓ Retweet of your listing announcement by HitBTC

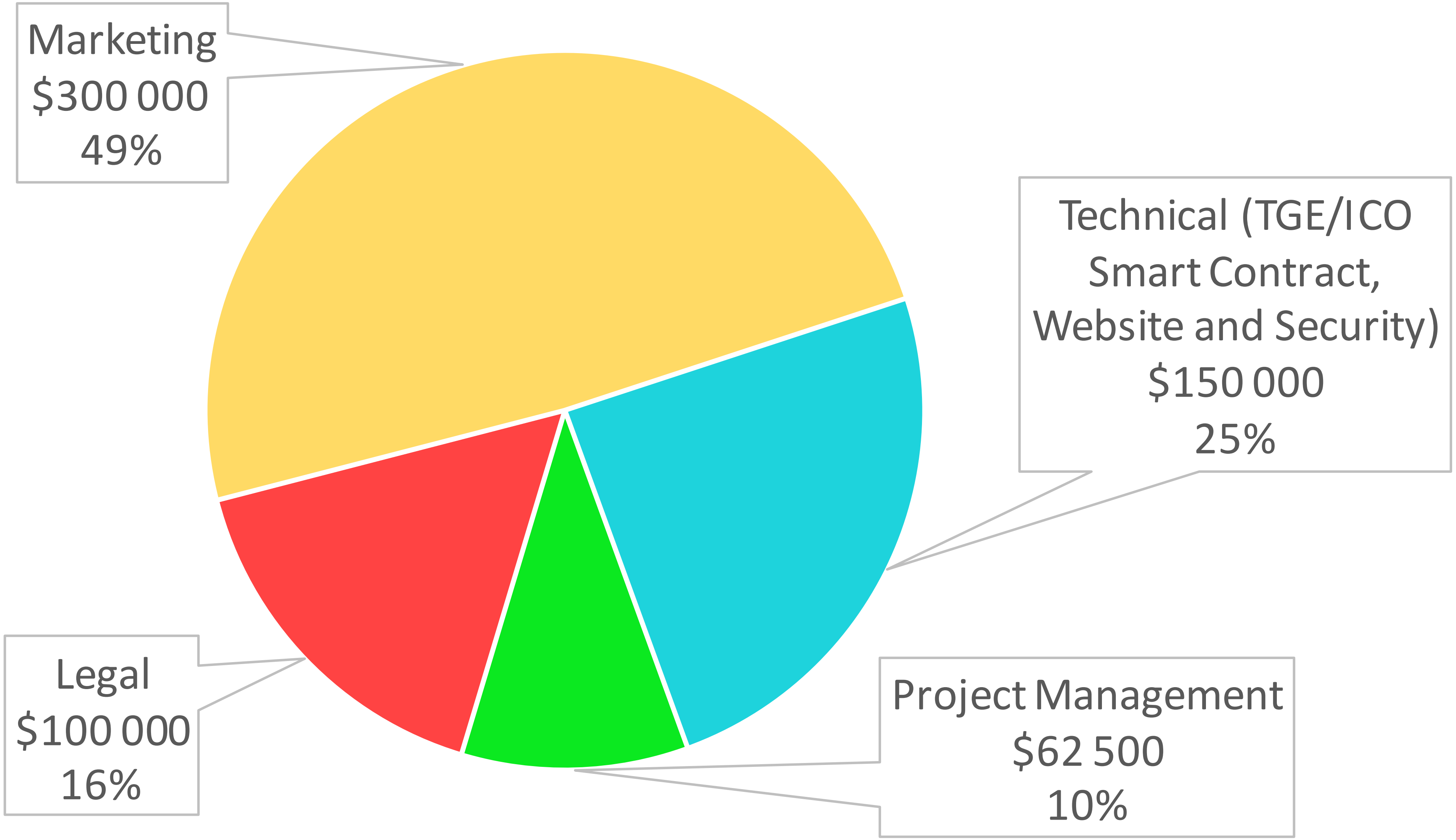
# Significant ICO/TGE Marketing Budgets



200k USD → 20 million USD

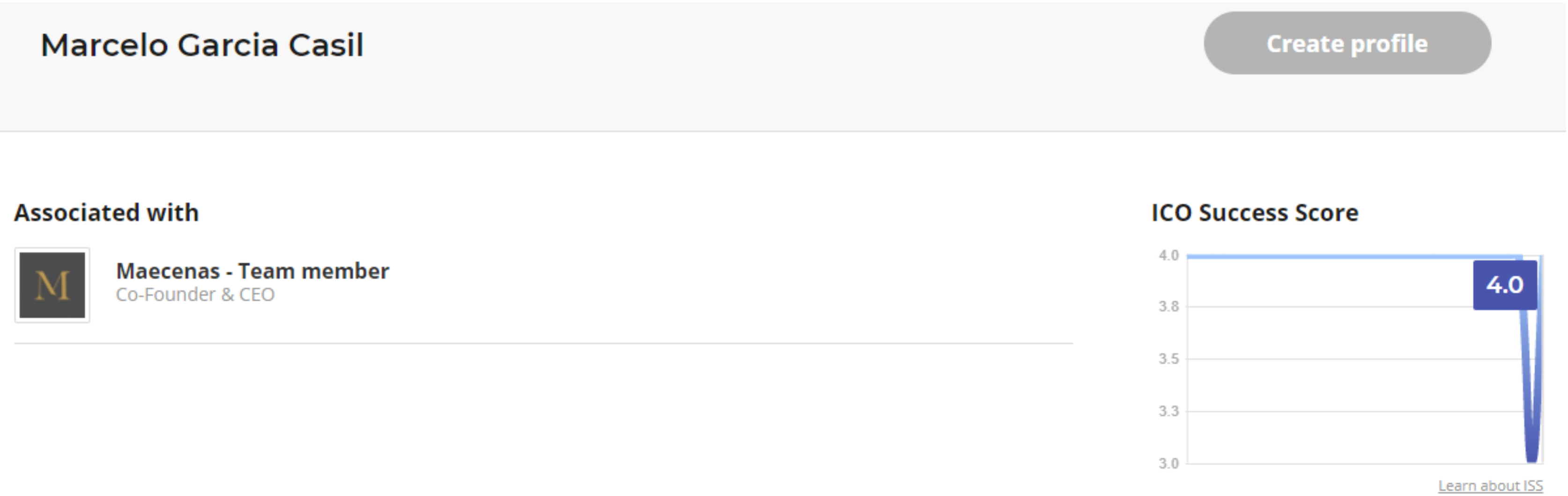
[TSM Global – 20 ICOs reverse engineered (Nov. 17)]

# Overall ICO/TGE Budget (without dApp/MVP)



# ICOBench Success Score (ISS)

- The more the user has participated to successful ICOs in the past, the higher score
- Example https://icobench.com/u/marcelo+garcia+casil



Marcelo Garcia Casil

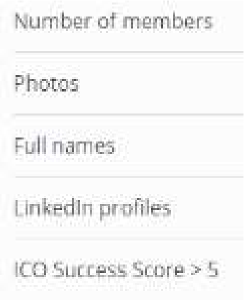
Associated with

Maecenas - Team member
Co-Founder & CEO

ICO Success Score

# ICO Listing Case Study:

- Non-attack resistant score algorithm based on the following criteria and if available manual score by experts evaluators

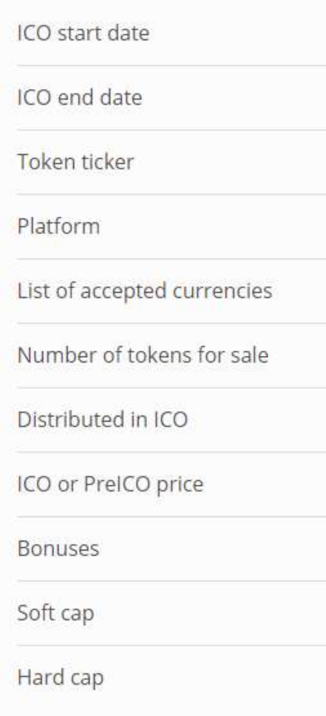

Number of members

Photos

Full names

LinkedIn profiles

ICO Success Score > 5


ICO start date

ICO end date

Token ticker

Platform

List of accepted currencies

Number of tokens for sale

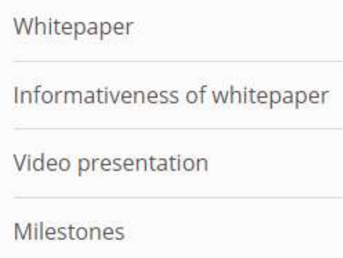
Distributed in ICO

ICO or PreICO price

Bonuses

Soft cap

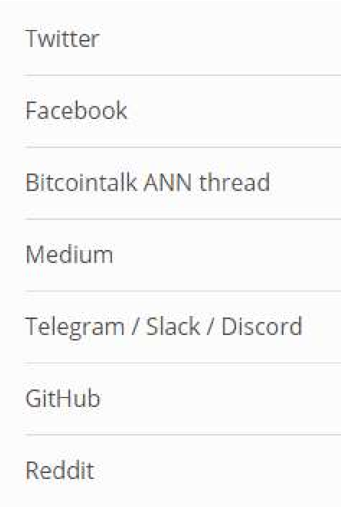
Hard cap


Whitepaper

Informativeness of whitepaper

Video presentation

Milestones


Twitter

Facebook

Bitcointalk ANN thread

Medium

Telegram / Slack / Discord

GitHub

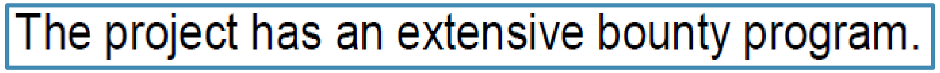
Reddit

# ICO Listing Case Study: SMITH + CROWN

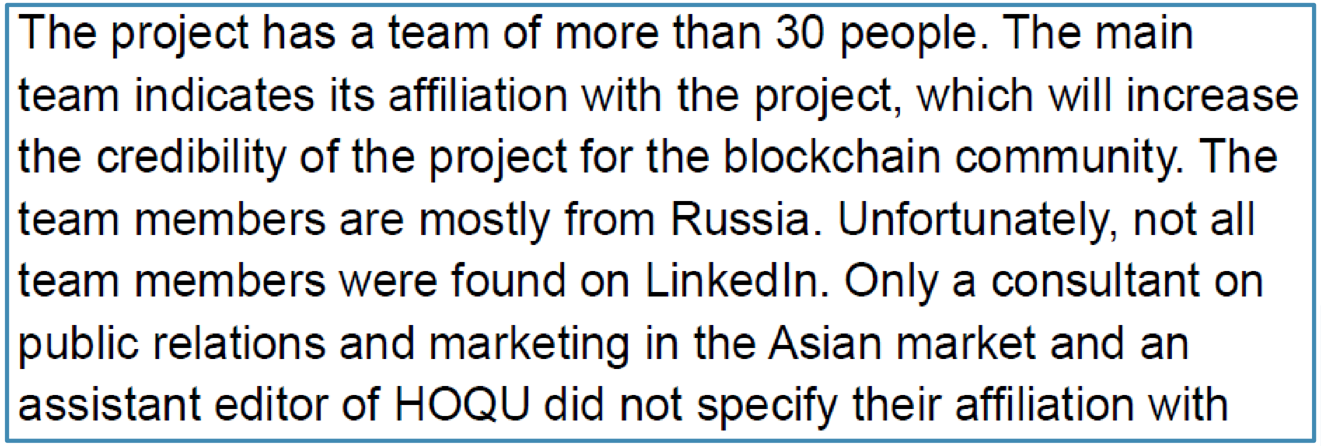
- “Smith + Crown is an independent research firm, not a marketing platform. We do not offer any token sale marketing services. Projects cannot buy their way onto our curated list or pay for published content.”
- Criteria:
  - “Primary team member identity. We are looking for projects that have transparent and verifiable identities.
  - The state of development. We are looking for projects that have public project code or working minimal viable projects. We will also consider pre-product stage projects with detailed white papers and modest raise amounts.
  - The quality of the white paper. We are looking for white papers that provide detailed information about the business plan and the proposed technology. White papers that are primarily marketing or crowdsale documents will likely not qualify.
  - The presence of existing development expertise.”

# ICO Listing Case Study:

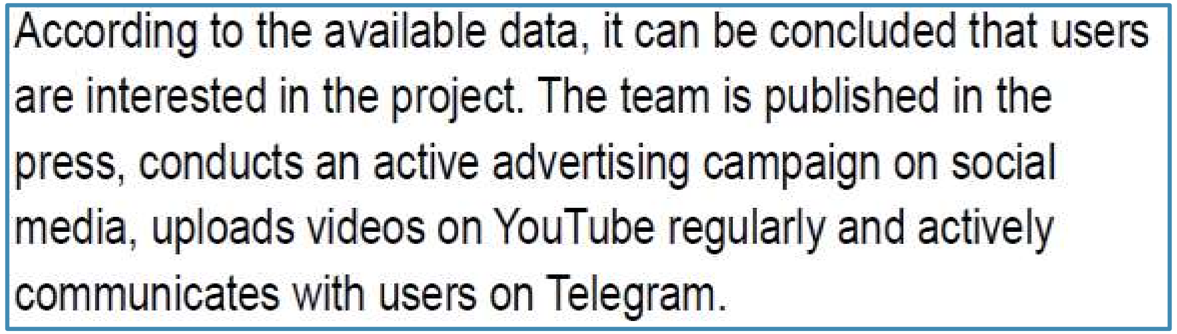
- Paid service, e.g., Basic Review (20 pages for around 7000$)
- Apparently quite unbiased even if paid given the negative aspects found in the reports



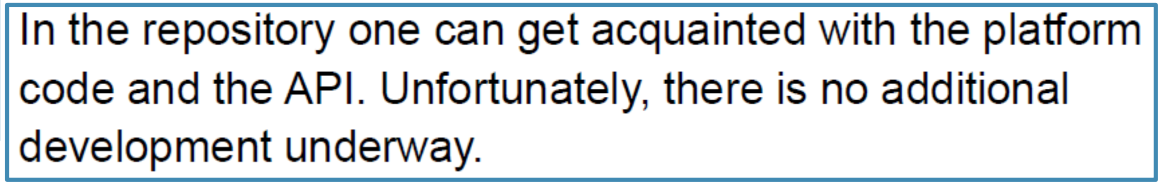
The project has an extensive bounty program.



The project has a team of more than 30 people. The main team indicates its affiliation with the project, which will increase the credibility of the project for the blockchain community. The team members are mostly from Russia. Unfortunately, not all team members were found on LinkedIn. Only a consultant on public relations and marketing in the Asian market and an assistant editor of HOQU did not specify their affiliation with

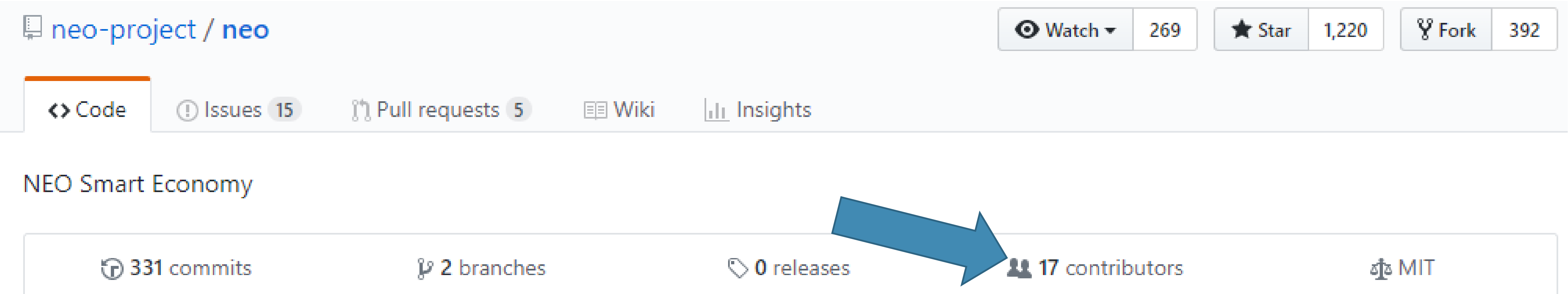


According to the available data, it can be concluded that users are interested in the project. The team is published in the press, conducts an active advertising campaign on social media, uploads videos on YouTube regularly and actively communicates with users on Telegram.



In the repository one can get acquainted with the platform code and the API. Unfortunately, there is no additional development underway.

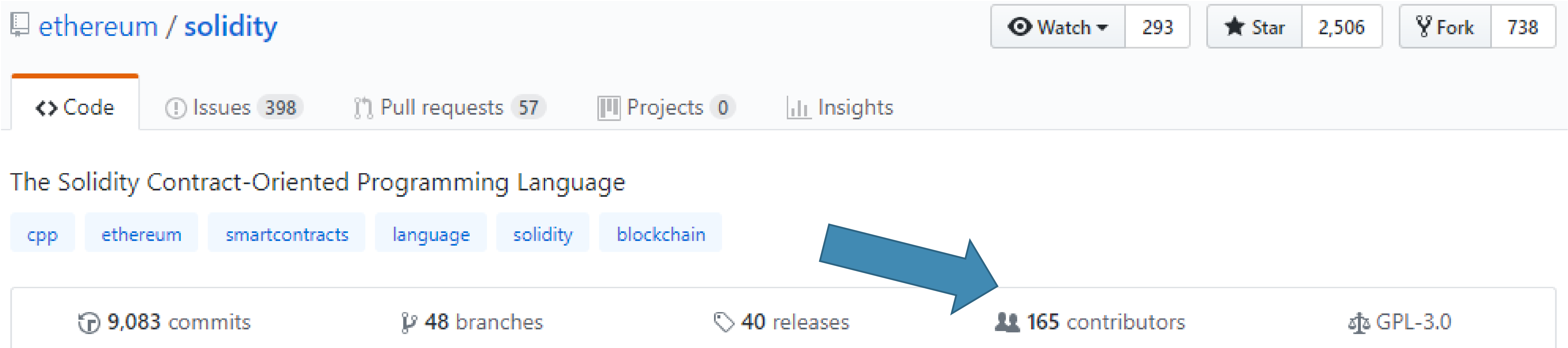
# Token ORM on GitHub



neo-project / neo

NEO Smart Economy

331 commits | 2 branches | 0 releases | 17 contributors | MIT

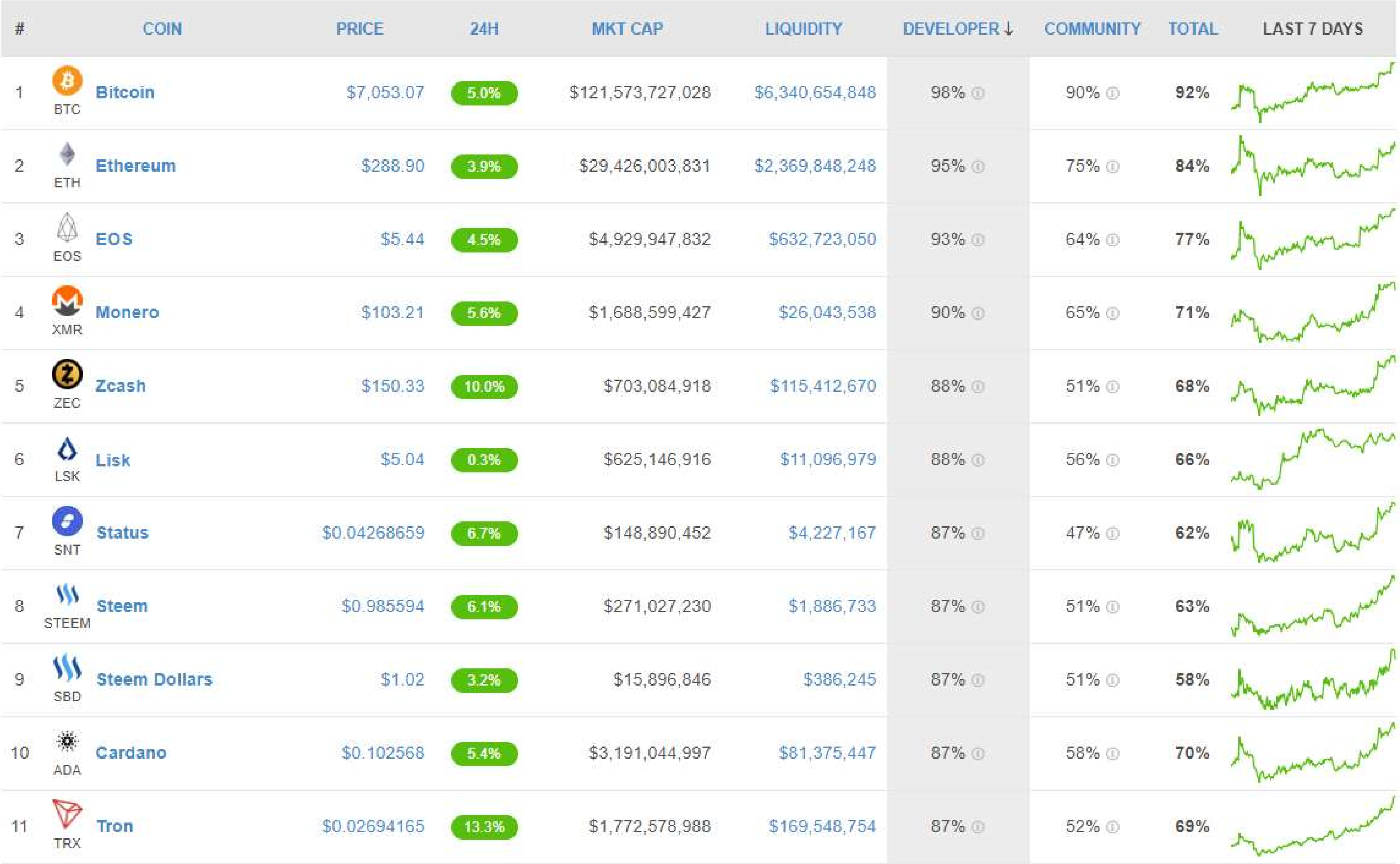


ethereum / solidity

The Solidity Contract-Oriented Programming Language

9,083 commits | 48 branches | 40 releases | 165 contributors | GPL-3.0

# CoinGecko.com

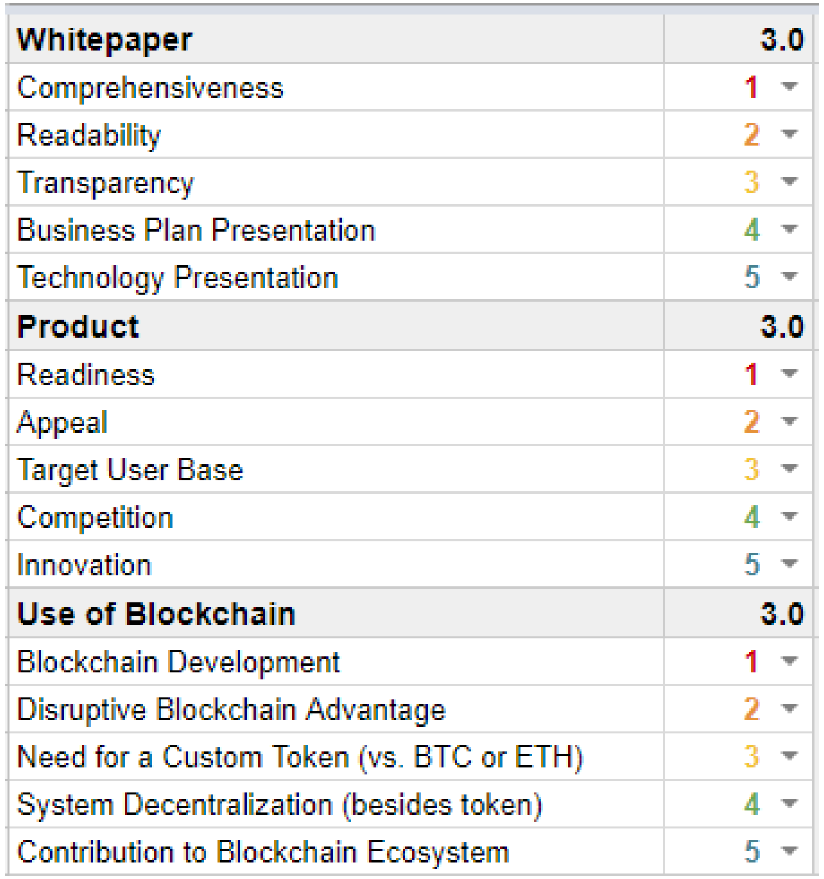


| # | COIN | PRICE | 24H | MKT CAP | LIQUIDITY | DEVELOPER ↓ | COMMUNITY | TOTAL | LAST 7 DAYS |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Bitcoin<br>BTC | $7,053.07 | 5.0% | $121,573,727,028 | $6,340,654,848 | 98% | 90% | 92% | |
| 2 | Ethereum<br>ETH | $288.90 | 3.9% | $29,426,003,831 | $2,369,848,248 | 95% | 75% | 84% | |
| 3 | EOS<br>EOS | $5.44 | 4.5% | $4,929,947,832 | $632,723,050 | 93% | 64% | 77% | |
| 4 | Monero<br>XMR | $103.21 | 5.6% | $1,688,599,427 | $26,043,538 | 90% | 65% | 71% | |
| 5 | Zcash<br>ZEC | $150.33 | 10.0% | $703,084,918 | $115,412,670 | 88% | 51% | 68% | |
| 6 | Lisk<br>LSK | $5.04 | 0.3% | $625,146,916 | $11,096,979 | 88% | 56% | 66% | |
| 7 | Status<br>SNT | $0.04268659 | 6.7% | $148,890,452 | $4,227,167 | 87% | 47% | 62% | |
| 8 | Steem<br>STEEM | $0.985594 | 6.1% | $271,027,230 | $1,886,733 | 87% | 51% | 63% | |
| 9 | Steem Dollars<br>SBD | $1.02 | 3.2% | $15,896,846 | $386,245 | 87% | 51% | 58% | |
| 10 | Cardano<br>ADA | $0.102568 | 5.4% | $3,191,044,997 | $81,375,447 | 87% | 58% | 70% | |
| 11 | Tron<br>TRX | $0.02694165 | 13.3% | $1,772,578,988 | $169,548,754 | 87% | 52% | 69% | |

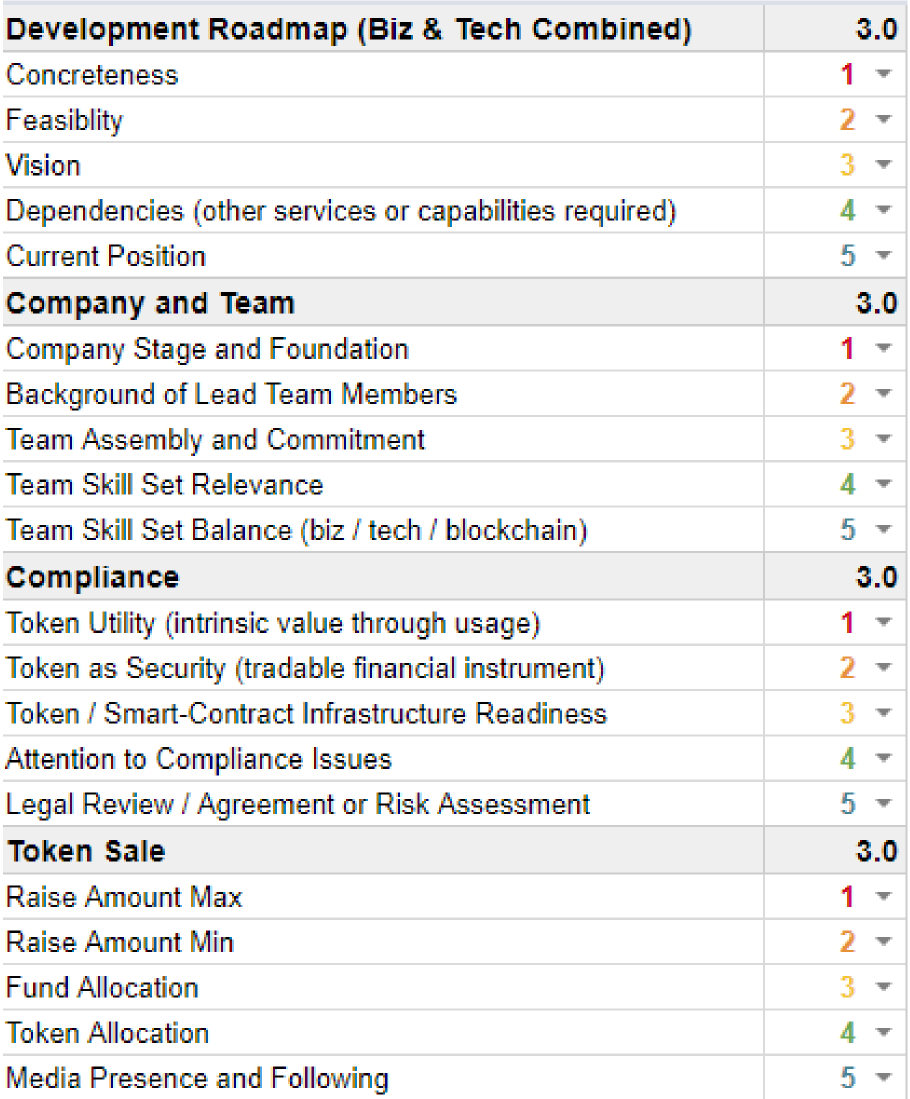
# ICO Listing Case Study:

CRYPTORATED
ICO Reviews, Ratings & Analysis

- Interesting scorecard: https://goo.gl/ssKWT6



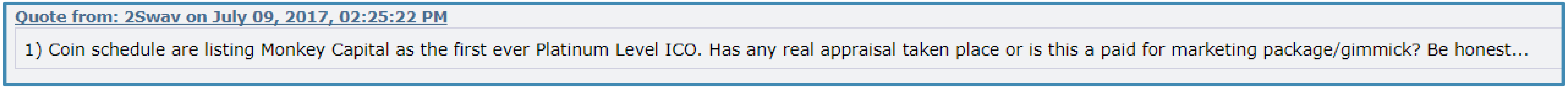
| Whitepaper | 3.0 |
|---|---|
| Comprehensiveness | 1 |
| Readability | 2 |
| Transparency | 3 |
| Business Plan Presentation | 4 |
| Technology Presentation | 5 |
| **Product** | **3.0** |
| Readiness | 1 |
| Appeal | 2 |
| Target User Base | 3 |
| Competition | 4 |
| Innovation | 5 |
| **Use of Blockchain** | **3.0** |
| Blockchain Development | 1 |
| Disruptive Blockchain Advantage | 2 |
| Need for a Custom Token (vs. BTC or ETH) | 3 |
| System Decentralization (besides token) | 4 |
| Contribution to Blockchain Ecosystem | 5 |



| Development Roadmap (Biz & Tech Combined) | 3.0 |
|---|---|
| Concreteness | 1 |
| Feasiblity | 2 |
| Vision | 3 |
| Dependencies (other services or capabilities required) | 4 |
| Current Position | 5 |
| **Company and Team** | **3.0** |
| Company Stage and Foundation | 1 |
| Background of Lead Team Members | 2 |
| Team Assembly and Commitment | 3 |
| Team Skill Set Relevance | 4 |
| Team Skill Set Balance (biz / tech / blockchain) | 5 |
| **Compliance** | **3.0** |
| Token Utility (intrinsic value through usage) | 1 |
| Token as Security (tradable financial instrument) | 2 |
| Token / Smart-Contract Infrastructure Readiness | 3 |
| Attention to Compliance Issues | 4 |
| Legal Review / Agreement or Risk Assessment | 5 |
| **Token Sale** | **3.0** |
| Raise Amount Max | 1 |
| Raise Amount Min | 2 |
| Fund Allocation | 3 |
| Token Allocation | 4 |
| Media Presence and Following | 5 |

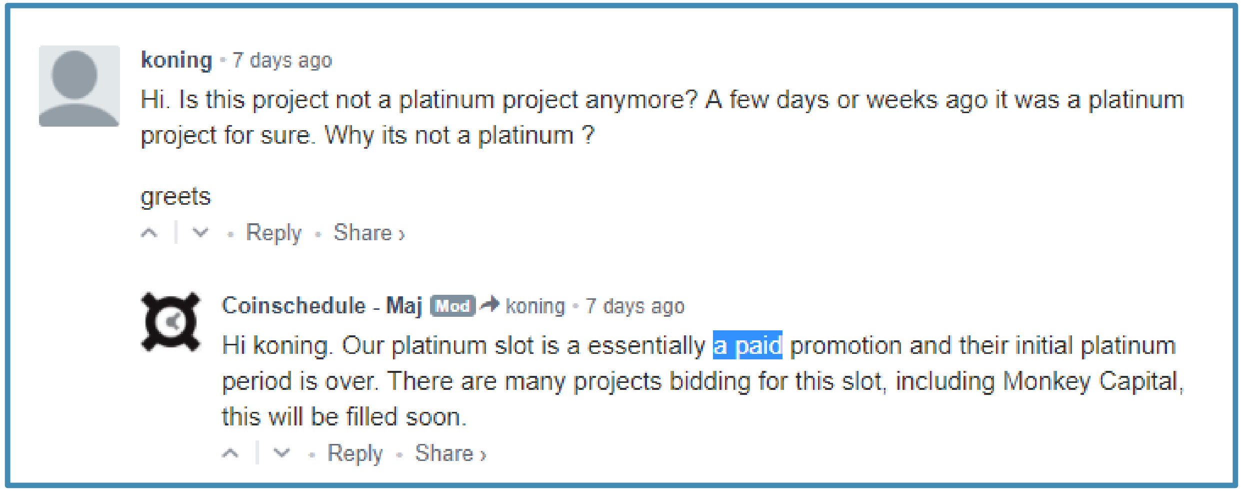
# ICO Listing Case Study:

- No clear indication on their Website that their badges (Platinum, Gold…) are only paid features without further evaluation
- Their first Platinum badge was given to the Monkey Capital ICO considered as “SCAM”



Quote from: 2Swav on July 09, 2017, 02:25:22 PM

1) Coin schedule are listing Monkey Capital as the first ever Platinum Level ICO. Has any real appraisal taken place or is this a paid for marketing package/gimmick? Be honest...



koning • 7 days ago

Hi. Is this project not a platinum project anymore? A few days or weeks ago it was a platinum project for sure. Why its not a platinum ?

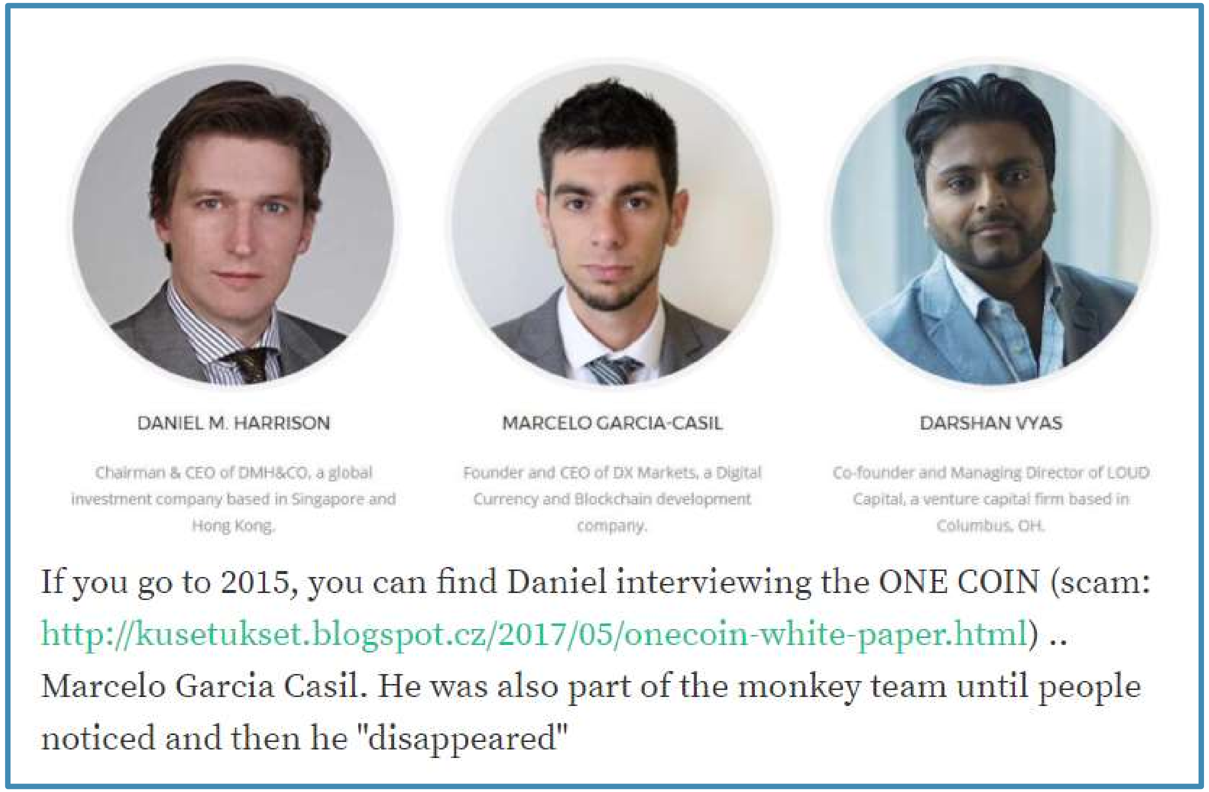
greets

Coinschedule - Maj Mod → koning • 7 days ago

Hi koning. Our platinum slot is a essentially a paid promotion and their initial platinum period is over. There are many projects bidding for this slot, including Monkey Capital, this will be filled soon.

# Monkey Capital ICO SCAM

- https://steemit.com/cryptocurrency/@goldseek/beware-of-monkey-capital-and-its-monkey-daniel-harrison



DANIEL M. HARRISON

Chairman & CEO of DMH&CO, a global investment company based in Singapore and Hong Kong.

MARCELO GARCIA-CASIL

Founder and CEO of DX Markets, a Digital Currency and Blockchain development company.

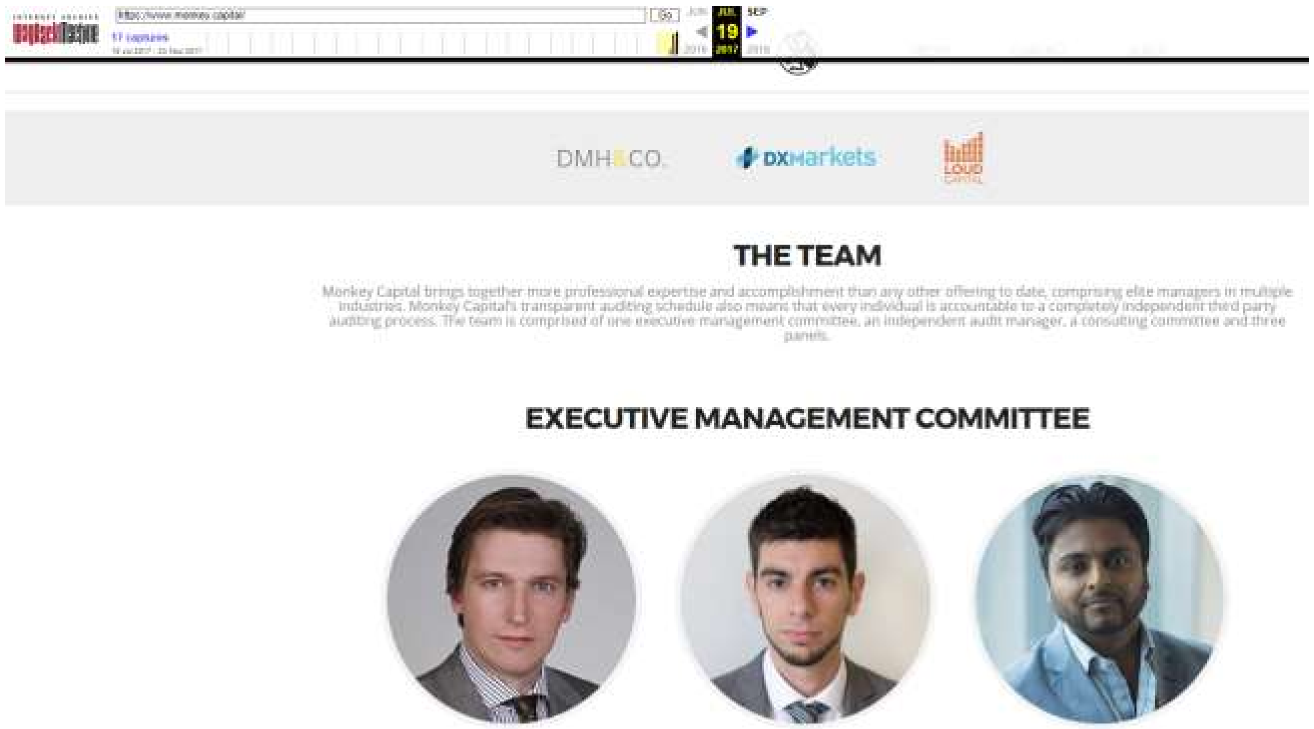
DARSHAN VYAS

Co-founder and Managing Director of LOUD Capital, a venture capital firm based in Columbus, OH.

If you go to 2015, you can find Daniel interviewing the ONE COIN (scam: http://kusetukset.blogspot.cz/2017/05/onecoin-white-paper.html) .. Marcelo Garcia Casil. He was also part of the monkey team until people noticed and then he "disappeared"

# Archive.org

- Tool used to retrieve old versions of Websites

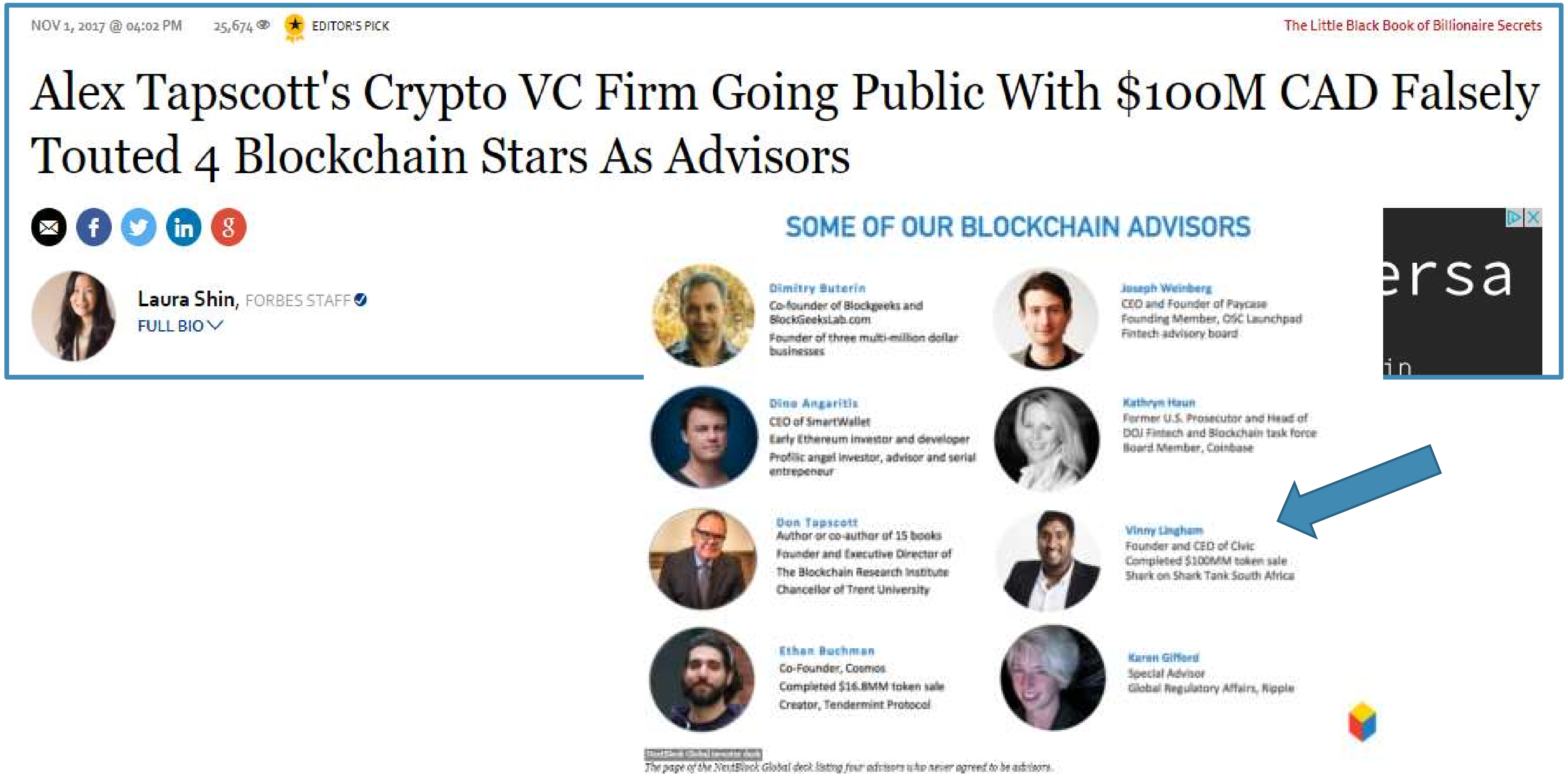


## THE TEAM

Monkey Capital brings together more professional expertise and accomplishment than any other offering to date, comprising elite managers in multiple industries. Monkey Capital's transparent auditing schedule also means that every individual is accountable to a completely independent third party auditing process. The team is comprised of one executive management committee, an independent audit manager, a consulting committee and three panels.

## EXECUTIVE MANAGEMENT COMMITTEE

# Always double-check team and advisor profiles



NOV 1, 2017 @ 04:02 PM 25,674 EDITOR'S PICK

## Alex Tapscott's Crypto VC Firm Going Public With $100M CAD Falsely Touted 4 Blockchain Stars As Advisors

Laura Shin, FORBES STAFF
FULL BIO

### SOME OF OUR BLOCKCHAIN ADVISORS

**Dimitry Buterin**
Co-founder of Blockgeeks and BlockGeeksLab.com
Founder of three multi-million dollar businesses

**Joseph Weinberg**
CEO and Founder of Paycase
Founding Member, OSC Launchpad Fintech advisory board

**Dino Angaritis**
CEO of SmartWallet
Early Ethereum investor and developer
Prolific angel investor, advisor and serial entrepeneur

**Kathryn Haun**
Former U.S. Prosecutor and Head of DOJ Fintech and Blockchain task force
Board Member, Coinbase

**Don Tapscott**
Author or co-author of 15 books
Founder and Executive Director of The Blockchain Research Institute
Chancellor of Trent University

**Vinny Lingham**
Founder and CEO of Civic
Completed $100MM token sale
Shark on Shark Tank South Africa

**Ethan Buchman**
Co-Founder, Cosmos
Completed $16.8MM token sale
Creator, Tendermint Protocol

**Karen Gifford**
Special Advisor
Global Regulatory Affairs, Ripple

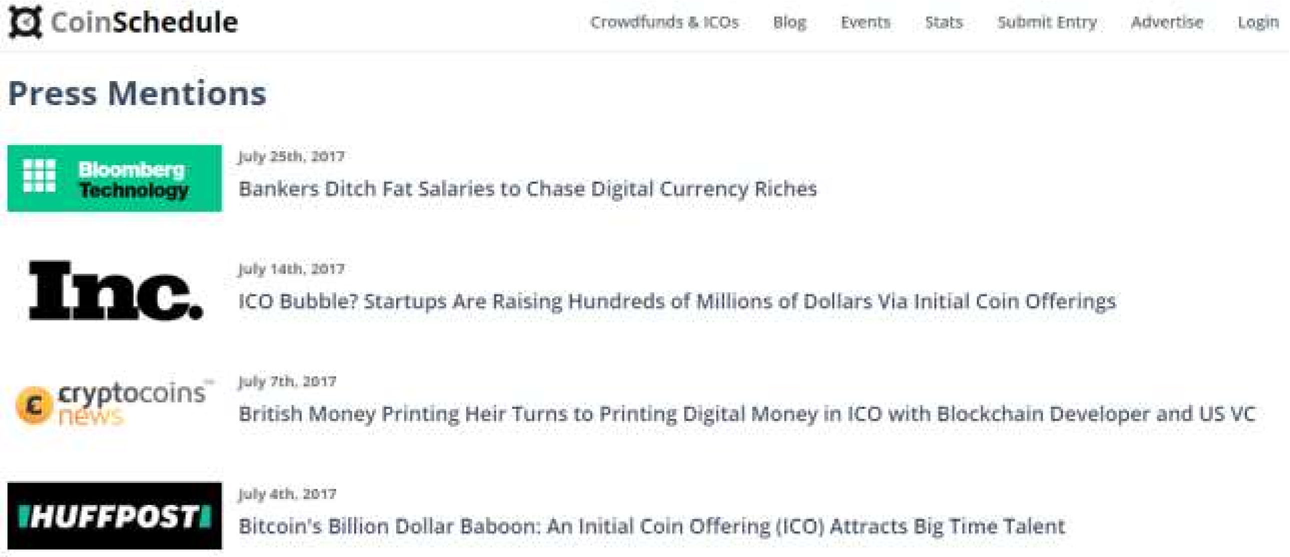
NextBlock Global investor deck
*The page of the NextBlock Global deck listing four advisors who never agreed to be advisors.*

# Summary of influential sources listing ICO/TGE

- In-depth reports that seem unbiased
  - Smith + Crown
  - CryptoBriefing
  - CoinCheckup
  - CoinGecko
  - Picolo Research (Astronaut.Capital)
  - Hacked.com
  - ICORating (even if paid reports)
- On YouTube:
  - Crush Crypto
  - The Crypto Lark
  - Chico Crypto
- Sources that cover more ICO/TGEs but less reliable than the above ones
  - Listing sites: TokenMarket, ICOBench, ICOAlert, CoinSchedule
  - On YouTube: Ian Balina

# Traditional Media for ICO/TGE/Cryptocurrencies

- The well-known traditional media (Forbes, The Wall Street Journal, The New York Times, Bloomberg Technology, Huffington Post…) or digital media (Twitter, YouTube, Medium, The Verge, TechCrunch…) are important for ICO/TGE online reputation but the application domain has its own specific media
- Not all traditional media mention ”Sponsored Article”
- For example, 100$ may be paid to get an article posted on the Huffington Post



CoinSchedule

Crowdfunds & ICOs | Blog | Events | Stats | Submit Entry | Advertise | Login

## Press Mentions

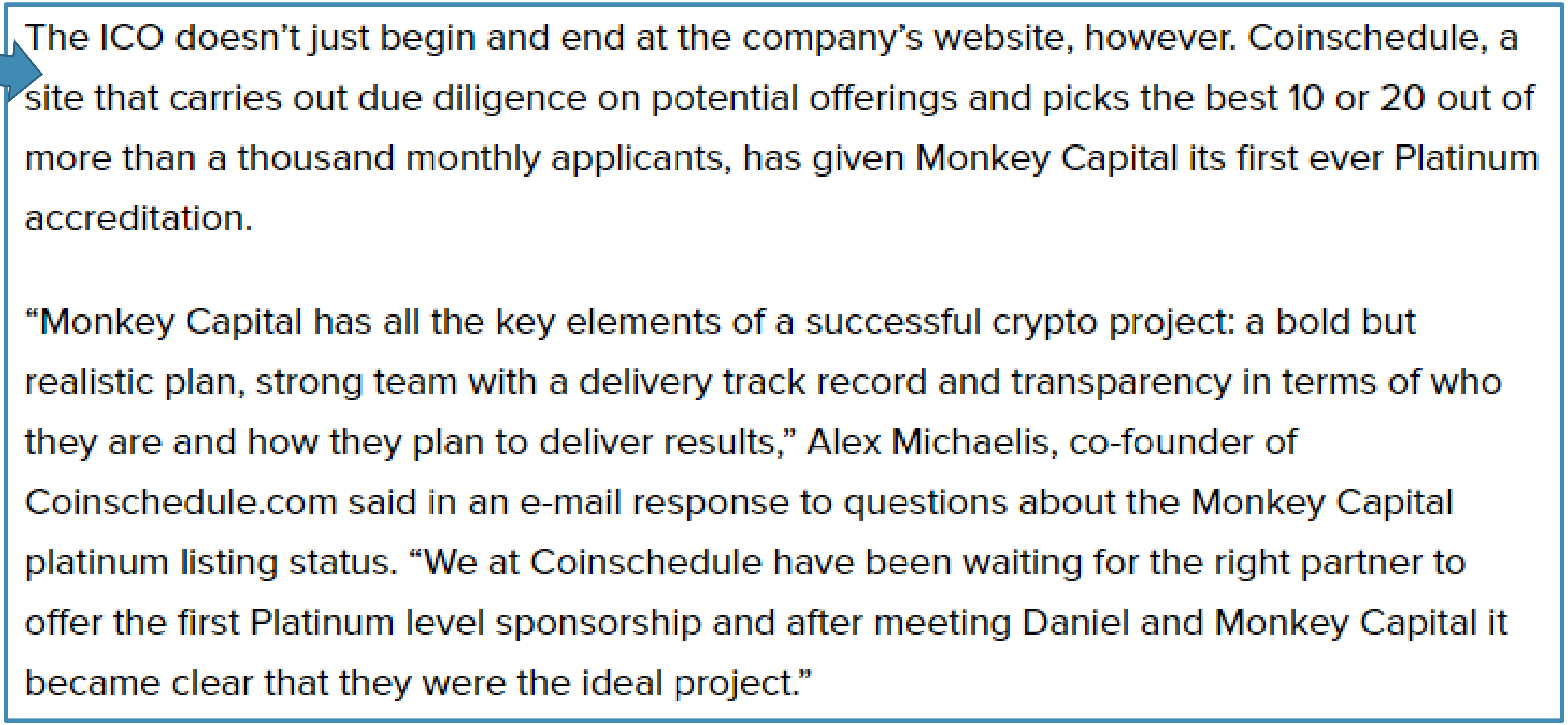
Bloomberg Technology
July 25th, 2017
Bankers Ditch Fat Salaries to Chase Digital Currency Riches

Inc.
July 14th, 2017
ICO Bubble? Startups Are Raising Hundreds of Millions of Dollars Via Initial Coin Offerings

cryptocoins news
July 7th, 2017
British Money Printing Heir Turns to Printing Digital Money in ICO with Blockchain Developer and US VC

HUFFPOST
July 4th, 2017
Bitcoin's Billion Dollar Baboon: An Initial Coin Offering (ICO) Attracts Big Time Talent

# « Monkey Capital » Huffington Post Article



The ICO doesn't just begin and end at the company's website, however. Coinschedule, a site that carries out due diligence on potential offerings and picks the best 10 or 20 out of more than a thousand monthly applicants, has given Monkey Capital its first ever Platinum accreditation.

"Monkey Capital has all the key elements of a successful crypto project: a bold but realistic plan, strong team with a delivery track record and transparency in terms of who they are and how they plan to deliver results," Alex Michaelis, co-founder of Coinschedule.com said in an e-mail response to questions about the Monkey Capital platinum listing status. "We at Coinschedule have been waiting for the right partner to offer the first Platinum level sponsorship and after meeting Daniel and Monkey Capital it became clear that they were the ideal project."

# Other Influential ICO/Crypto Media

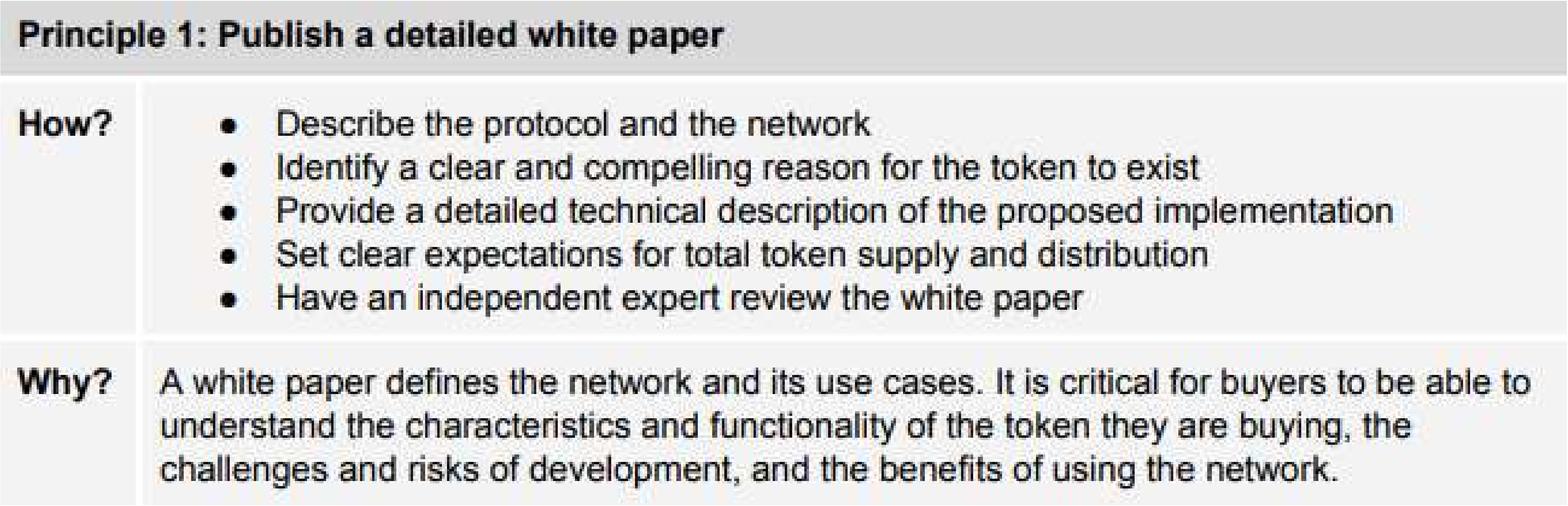
- Short news articles
  - CoinDesk, CoinTelegraph, CryptoCoinsNews
- Exchanges
  - Ascending influence for the occidental market:
    - EtherDelta, HitBTC, Binance (paid marketing options available), Bittrex, CoinBase (GDAX)
- Blogs platforms
  - Steemit (with its own blockchain and cryptocurrencies: STEEM…)
- Messengers
  - Telegram
  - Discord
- Full magazine
  - ICOCrowd
- Forums and social networks
  - BitcoinTalk
  - Reddit (subreddits specialized on cryptocurrencies)
  - Github

# CoinBase Security Law Framework for Tokens

coinbase

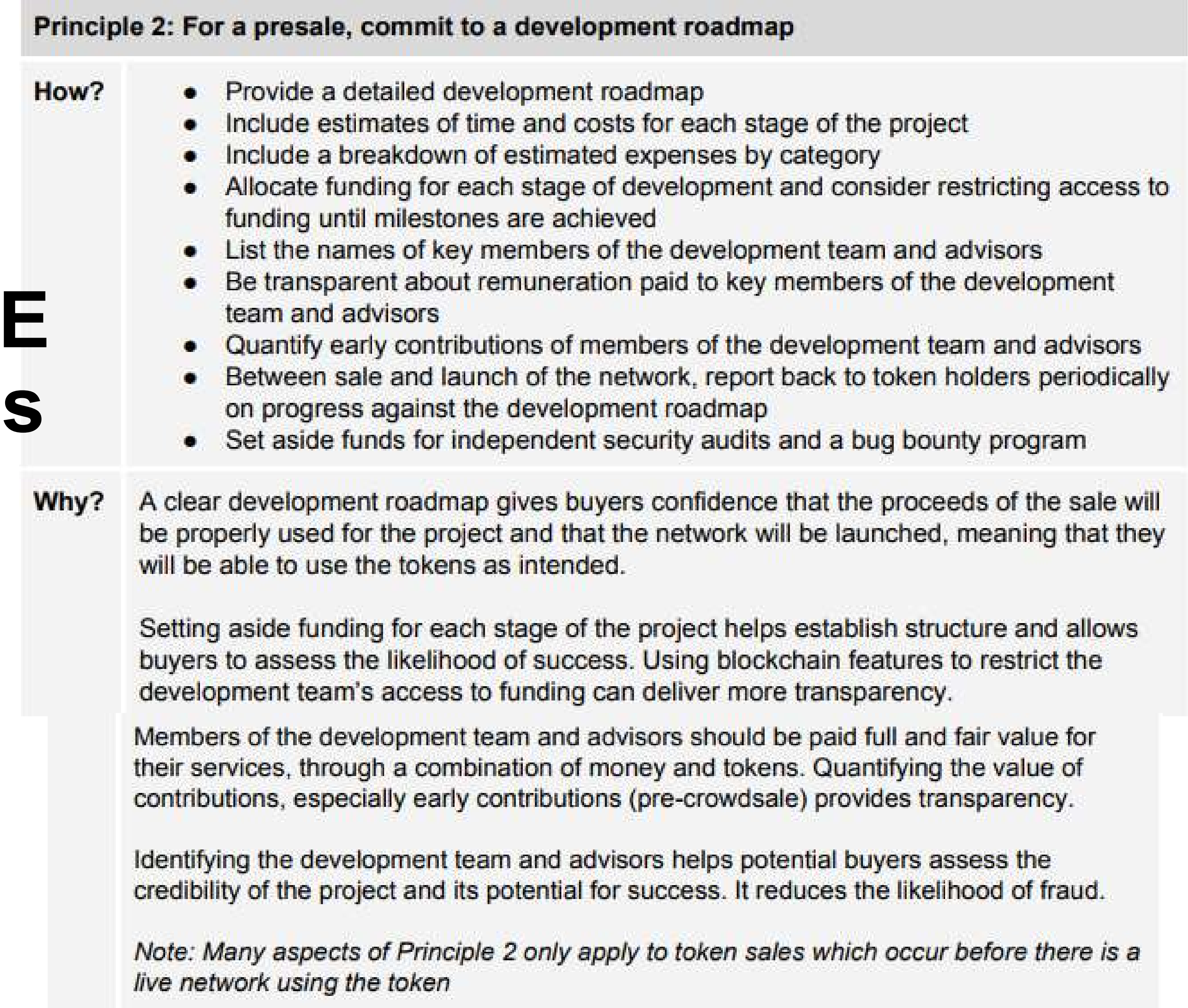
- CoinBase lists few tokens but gives high visibility to them being the most well-known exchange in the USA
- Being based in the USA, CoinBase doesn’t want to list illegal securities tokens and provide interesting resources to assess the likelihood of a coin to be considered as a security (although legally outdate because written in 2016)
  - An online form: https://goo.gl/WhKn1x
  - and a recommendation report: https://www.coinbase.com/legal/securities-law-framework.pdf

# CoinBase ICO/TGE Recommendations



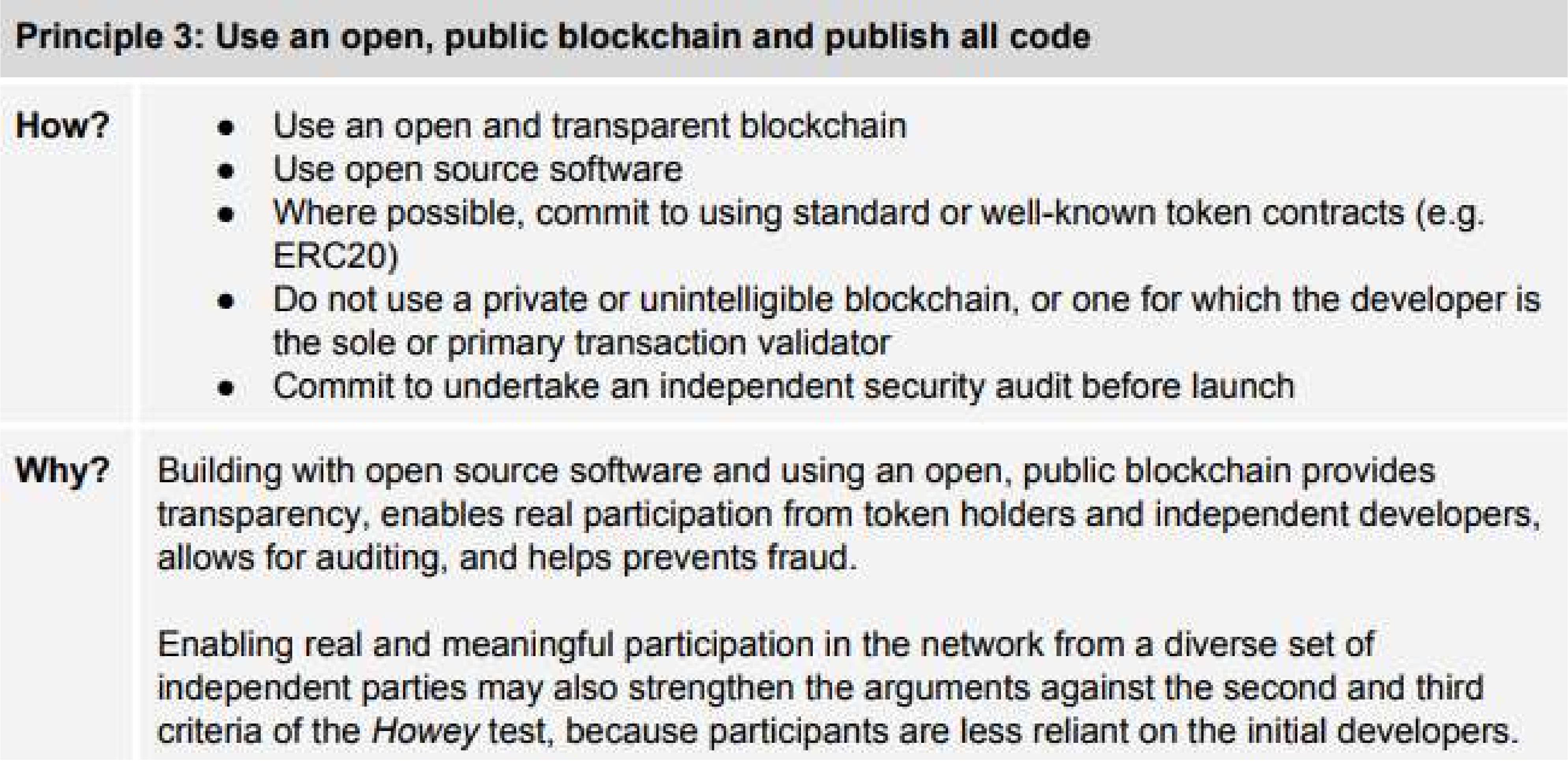
| Principle 1: Publish a detailed white paper | |
|---|---|
| How? | • Describe the protocol and the network<br>• Identify a clear and compelling reason for the token to exist<br>• Provide a detailed technical description of the proposed implementation<br>• Set clear expectations for total token supply and distribution<br>• Have an independent expert review the white paper |
| Why? | A white paper defines the network and its use cases. It is critical for buyers to be able to understand the characteristics and functionality of the token they are buying, the challenges and risks of development, and the benefits of using the network. |

# CoinBase ICO/TGE Recommendations (2)



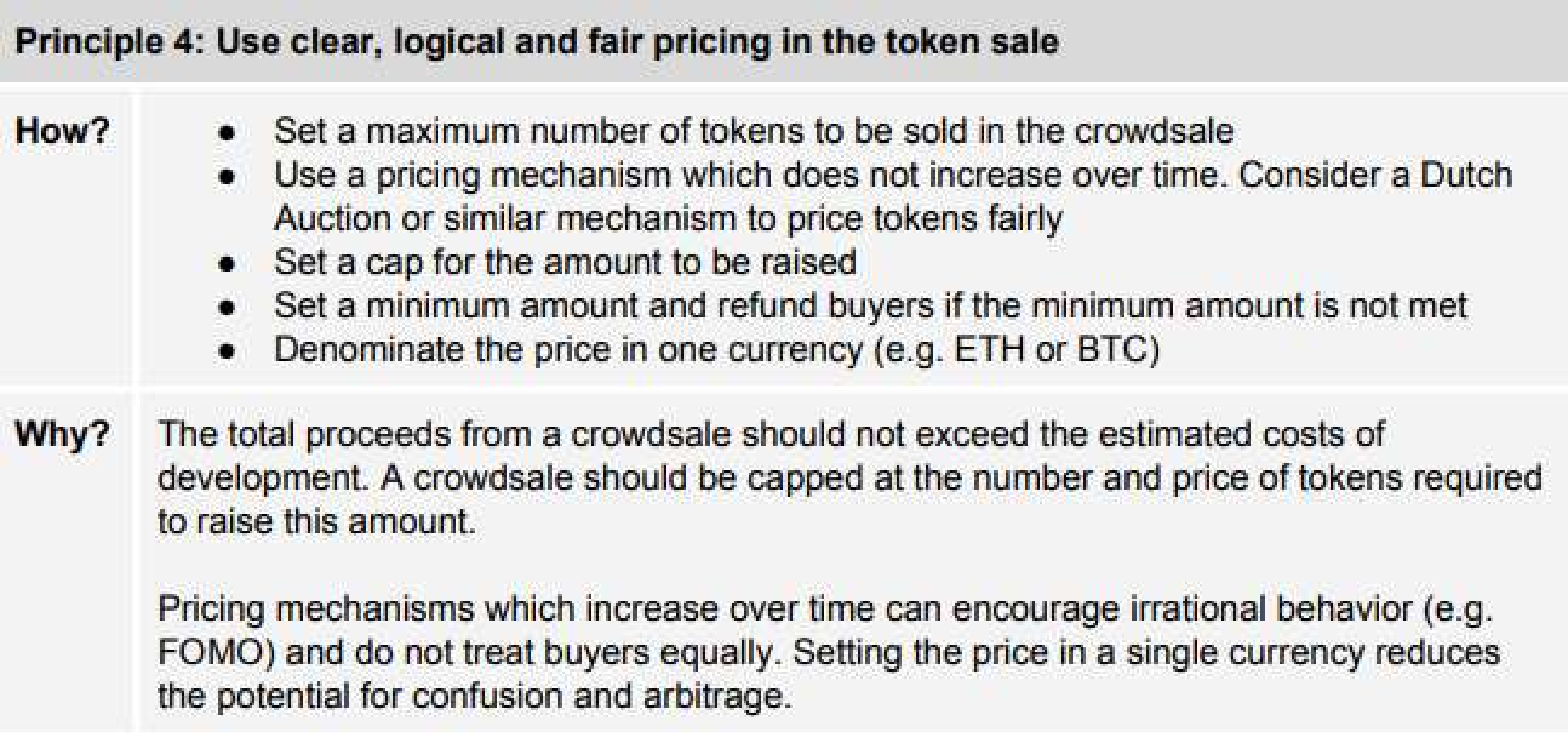
| Principle 2: For a presale, commit to a development roadmap | |
|---|---|
| **How?** | ● Provide a detailed development roadmap<br>● Include estimates of time and costs for each stage of the project<br>● Include a breakdown of estimated expenses by category<br>● Allocate funding for each stage of development and consider restricting access to funding until milestones are achieved<br>● List the names of key members of the development team and advisors<br>● Be transparent about remuneration paid to key members of the development team and advisors<br>● Quantify early contributions of members of the development team and advisors<br>● Between sale and launch of the network, report back to token holders periodically on progress against the development roadmap<br>● Set aside funds for independent security audits and a bug bounty program |
| **Why?** | A clear development roadmap gives buyers confidence that the proceeds of the sale will be properly used for the project and that the network will be launched, meaning that they will be able to use the tokens as intended.<br>Setting aside funding for each stage of the project helps establish structure and allows buyers to assess the likelihood of success. Using blockchain features to restrict the development team's access to funding can deliver more transparency.<br>Members of the development team and advisors should be paid full and fair value for their services, through a combination of money and tokens. Quantifying the value of contributions, especially early contributions (pre-crowdsale) provides transparency.<br>Identifying the development team and advisors helps potential buyers assess the credibility of the project and its potential for success. It reduces the likelihood of fraud.<br>*Note: Many aspects of Principle 2 only apply to token sales which occur before there is a live network using the token* |

# CoinBase ICO/TGE Recommendations (3)



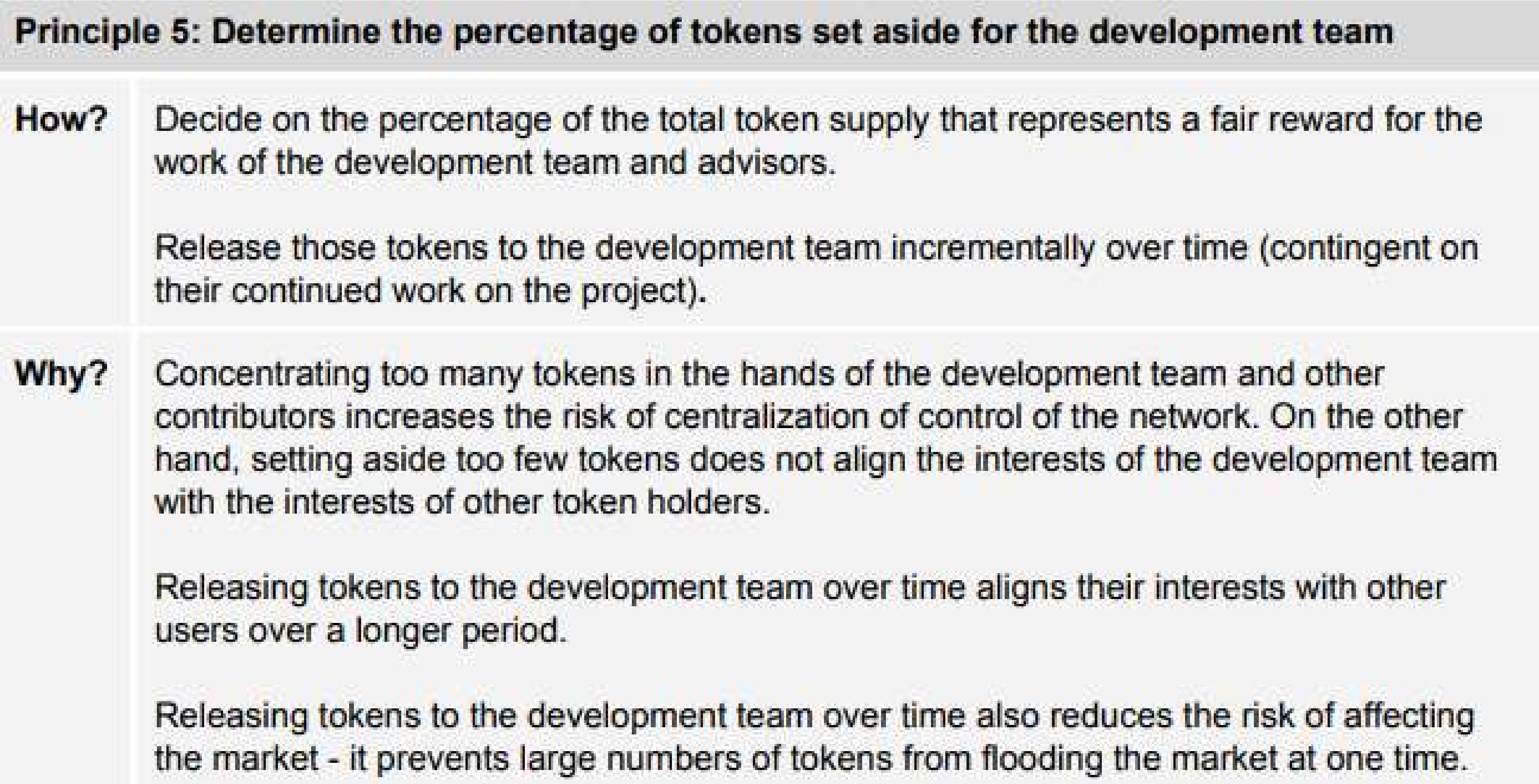
| **Principle 3: Use an open, public blockchain and publish all code** | |
|---|---|
| **How?** | • Use an open and transparent blockchain<br>• Use open source software<br>• Where possible, commit to using standard or well-known token contracts (e.g. ERC20)<br>• Do not use a private or unintelligible blockchain, or one for which the developer is the sole or primary transaction validator<br>• Commit to undertake an independent security audit before launch |
| **Why?** | Building with open source software and using an open, public blockchain provides transparency, enables real participation from token holders and independent developers, allows for auditing, and helps prevents fraud.<br>Enabling real and meaningful participation in the network from a diverse set of independent parties may also strengthen the arguments against the second and third criteria of the *Howey* test, because participants are less reliant on the initial developers. |

# CoinBase ICO/TGE Recommendations (4)



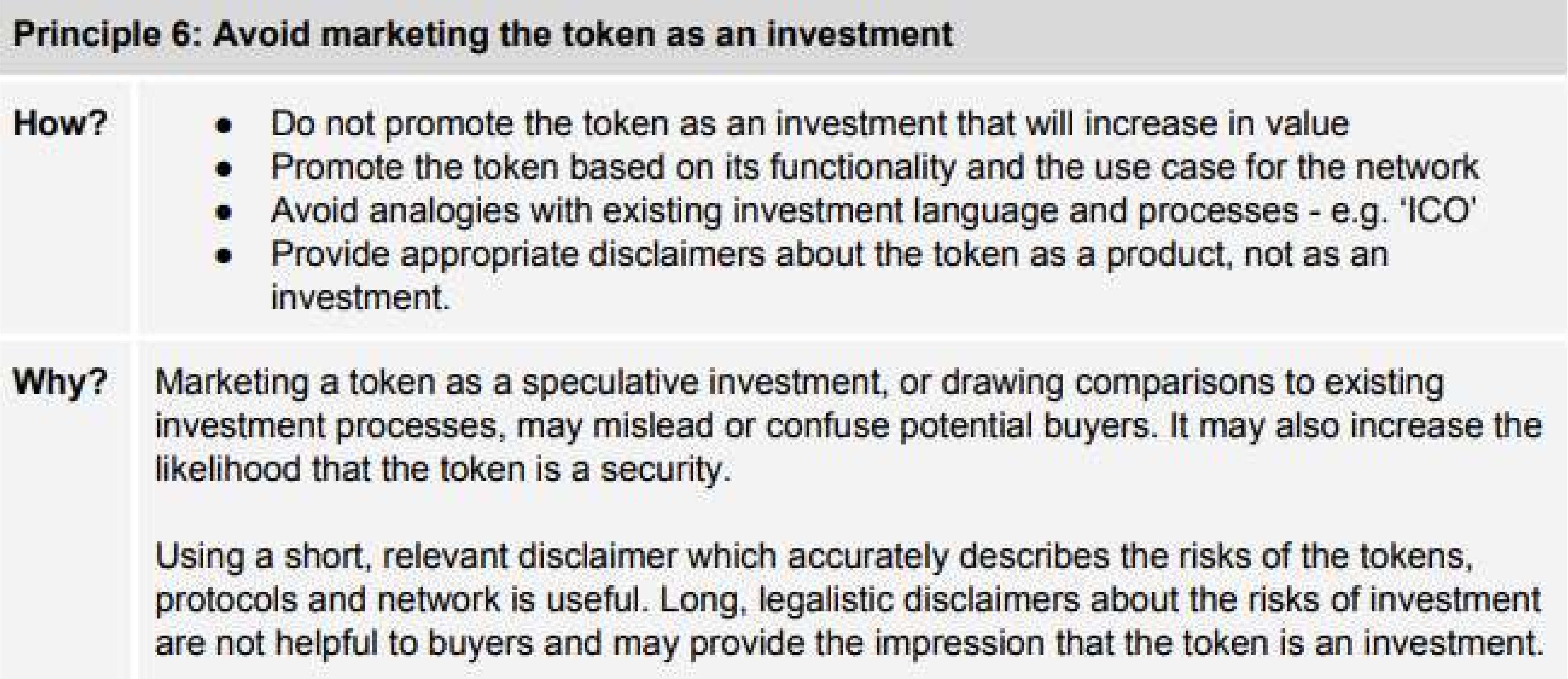
| Principle 4: Use clear, logical and fair pricing in the token sale | |
|---|---|
| How? | • Set a maximum number of tokens to be sold in the crowdsale<br>• Use a pricing mechanism which does not increase over time. Consider a Dutch Auction or similar mechanism to price tokens fairly<br>• Set a cap for the amount to be raised<br>• Set a minimum amount and refund buyers if the minimum amount is not met<br>• Denominate the price in one currency (e.g. ETH or BTC) |
| Why? | The total proceeds from a crowdsale should not exceed the estimated costs of development. A crowdsale should be capped at the number and price of tokens required to raise this amount.<br><br>Pricing mechanisms which increase over time can encourage irrational behavior (e.g. FOMO) and do not treat buyers equally. Setting the price in a single currency reduces the potential for confusion and arbitrage. |

# CoinBase ICO/TGE Recommendations (5)



| **Principle 5: Determine the percentage of tokens set aside for the development team** | |
|---|---|
| **How?** | Decide on the percentage of the total token supply that represents a fair reward for the work of the development team and advisors.<br>Release those tokens to the development team incrementally over time (contingent on their continued work on the project). |
| **Why?** | Concentrating too many tokens in the hands of the development team and other contributors increases the risk of centralization of control of the network. On the other hand, setting aside too few tokens does not align the interests of the development team with the interests of other token holders.<br>Releasing tokens to the development team over time aligns their interests with other users over a longer period.<br>Releasing tokens to the development team over time also reduces the risk of affecting the market - it prevents large numbers of tokens from flooding the market at one time. |

# CoinBase ICO/TGE Recommendations (6)



| Principle 6: Avoid marketing the token as an investment | |
|---|---|
| **How?** | • Do not promote the token as an investment that will increase in value<br>• Promote the token based on its functionality and the use case for the network<br>• Avoid analogies with existing investment language and processes - e.g. 'ICO'<br>• Provide appropriate disclaimers about the token as a product, not as an investment. |
| **Why?** | Marketing a token as a speculative investment, or drawing comparisons to existing investment processes, may mislead or confuse potential buyers. It may also increase the likelihood that the token is a security.<br><br>Using a short, relevant disclaimer which accurately describes the risks of the tokens, protocols and network is useful. Long, legalistic disclaimers about the risks of investment are not helpful to buyers and may provide the impression that the token is an investment. |

# ICO/TGE Exercise

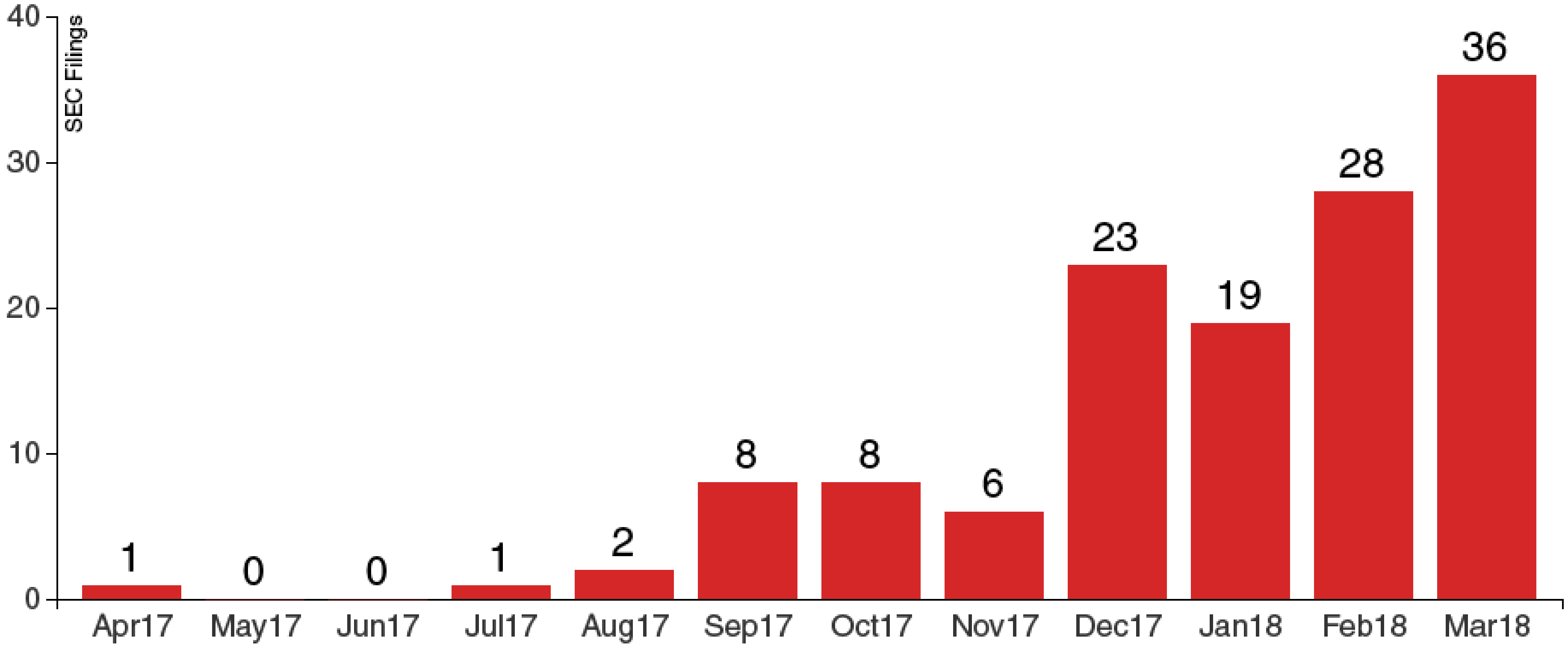
- Prepare a presentation highlighting the main steps of your ICO/TGE
  - Budget and planning
  - Tokenomics
  - Main whitepaper sections
  - Main marketing selling points
  - …

# Agenda

- Understanding the technology behind DLT
- Overview of current DLT development platforms
- How to select the most appropriate DLT for a specific dApp
- Overview of current cryptocurrencies and tools
- Initial Coin Offering (ICO), Token Generation Event (TGE) and tokenomics
- **DLT trends**

# Security Tokens ICOs

- Security tokens and SAFT agreements are growing in popularity



Crypto-Security Registrations

SEC Form D filings for tokens or token convertibles, Apr17-Mar18

# Platforms to Tokenize Assets

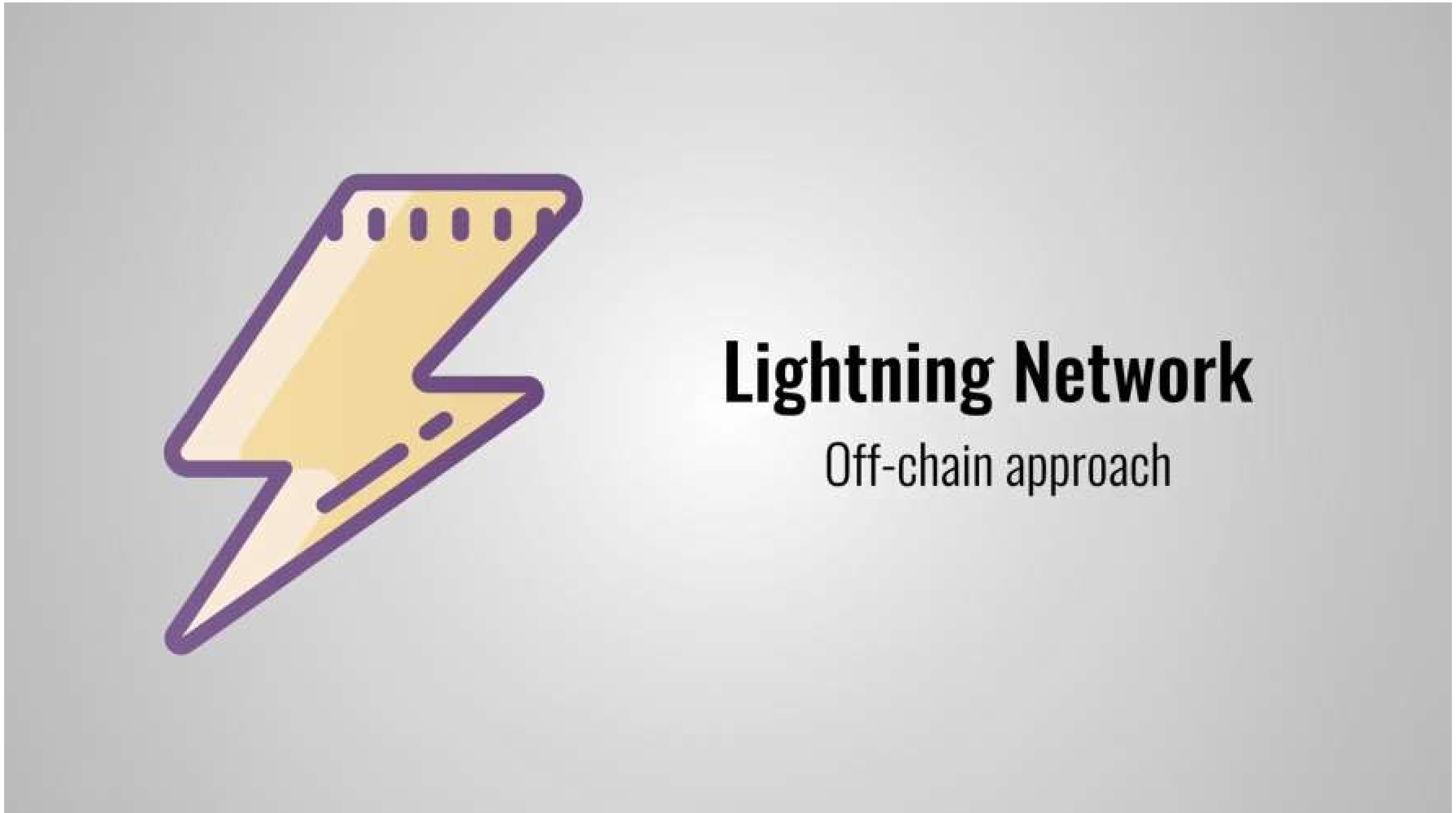
- They argue to frameworks.

POLYMATH
THE SECURITIES TOKEN PLATFORM
HARBOR
TrustToken
OpenFinance
NETWORK
S

# Sidechains and offchain

- Several DLT platforms try to improve their performance by adding mechanisms external to the blockchain.
- When the blockchain is directly used, the action is called onchain. Otherwise it is called offchain.
- Some offchain actions may not be tracked onchain although their end results must still be compatible onchain.
- Sidechains are of different types, e.g., an external smaller chain protected by cryptography may be created to enforce some transactions between 2 or more parties and then its results may be synchronized on the main blockchain. They are called Lightning Networks in the Bitcoin system.
- Another option may be that the external transactions are enforced and protected by Trusted Execution Environments (TEE) or Trusted Platform Modules (TPM) such as done in the Reputaction patent-pending hardened crypto-wallet.

# Lightning Networks



Lightning Network

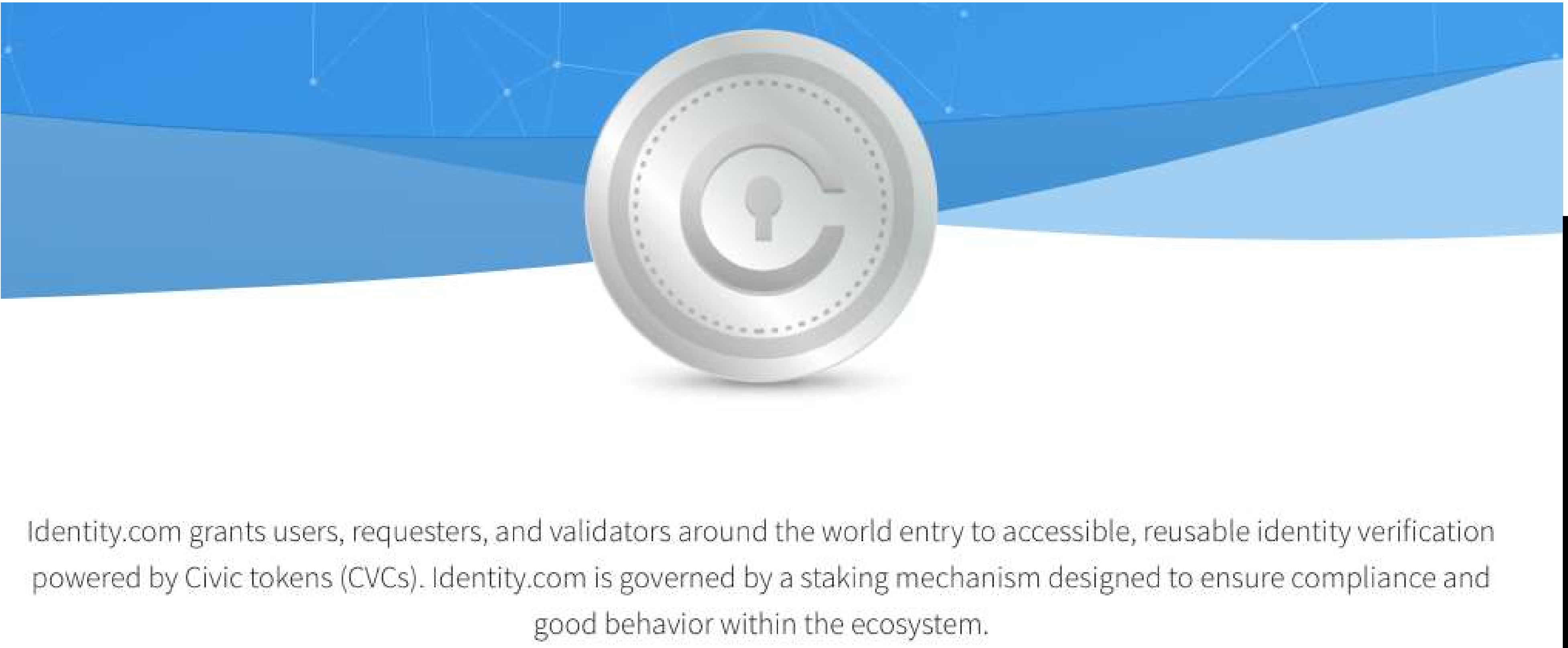
Off-chain approach

[Simply Explained Savjee]

# Beyond ICO-only KYC and AML Checks

- Initially, no KYC/AML checks was done, even at ICO stage
  - Same for mining rewards, any miner without KYC/AML could gain coins
- Thus, some criminals may hold older tokens and coins
- If someone gets coins/tokens from them, they become linked to transactions made with these criminals due to the trackability of most coins/tokens
- We have seen that some services exist to compute the risk in crypto addresses such as CoinFirm
- Due to many countries asking now for KYC/AML and risks of prosecutions, most ICOs enforce KYC/AML before releasing their coins/tokens to their investors/buyers
- The trend is that KYC/AML should be enforced each time tokens/coins are transferred between parties at smart contract level
  - Stellar smart contracts already have the possibility to enforce KYC/AML before any transfer

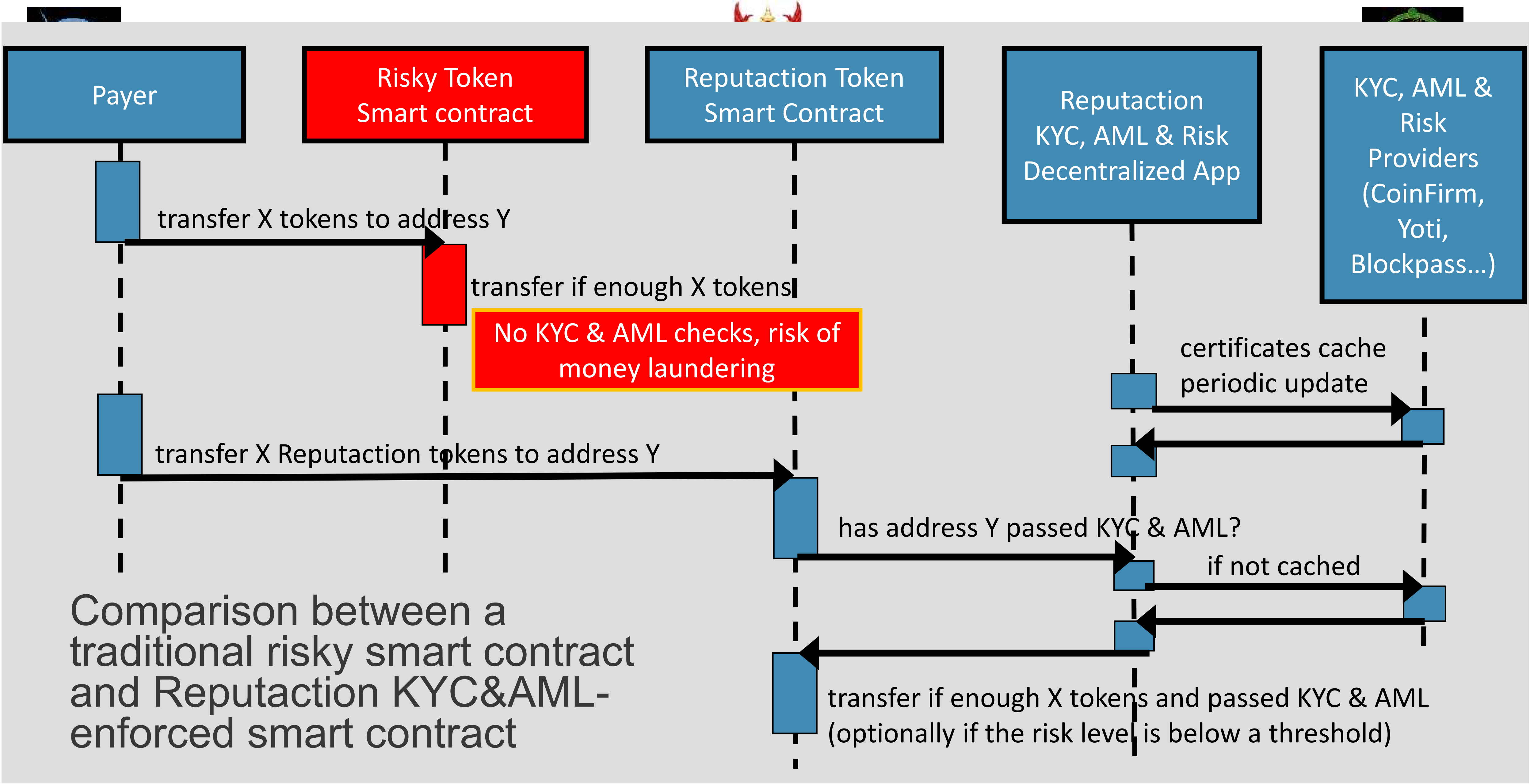
# Decentralized Identity/KYC/AML



Identity.com grants users, requesters, and validators around the world entry to accessible, reusable identity verification powered by Civic tokens (CVCs). Identity.com is governed by a staking mechanism designed to ensure compliance and good behavior within the ecosystem.

BLOCKPASS

civic



Payer

Risky Token Smart contract

Reputaction Token Smart Contract

Reputaction KYC, AML & Risk Decentralized App

KYC, AML & Risk Providers (CoinFirm, Yoti, Blockpass…)

transfer X tokens to address Y

transfer if enough X tokens

No KYC & AML checks, risk of money laundering

certificates cache periodic update

transfer X Reputaction tokens to address Y

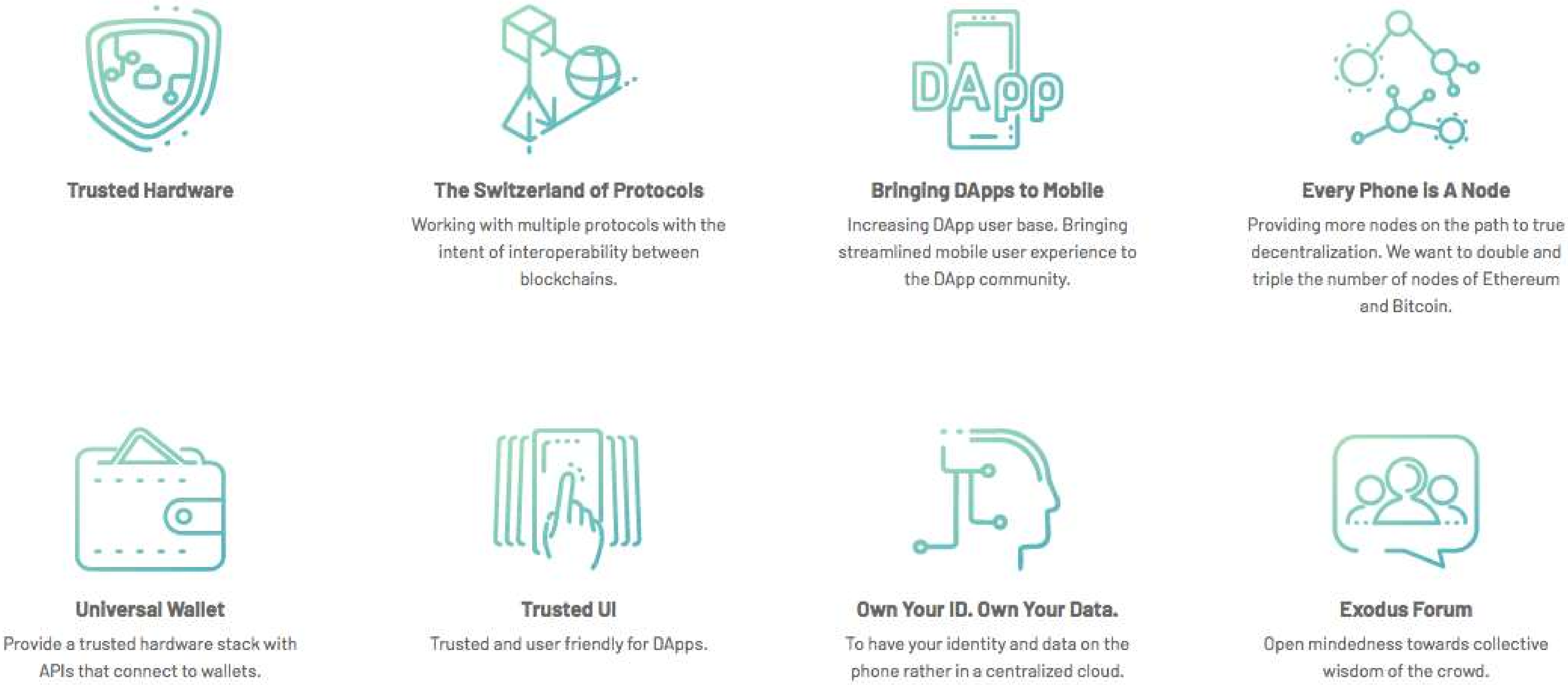
has address Y passed KYC & AML?

if not cached

transfer if enough X tokens and passed KYC & AML (optionally if the risk level is below a threshold)

Comparison between a traditional risky smart contract and Reputaction KYC&AML-enforced smart contract

# HTC Exodus



**Trusted Hardware**

**The Switzerland of Protocols**

Working with multiple protocols with the intent of interoperability between blockchains.

**Bringing DApps to Mobile**

Increasing DApp user base. Bringing streamlined mobile user experience to the DApp community.

**Every Phone Is A Node**

Providing more nodes on the path to true decentralization. We want to double and triple the number of nodes of Ethereum and Bitcoin.

**Universal Wallet**

Provide a trusted hardware stack with APIs that connect to wallets.

**Trusted UI**

Trusted and user friendly for DApps.

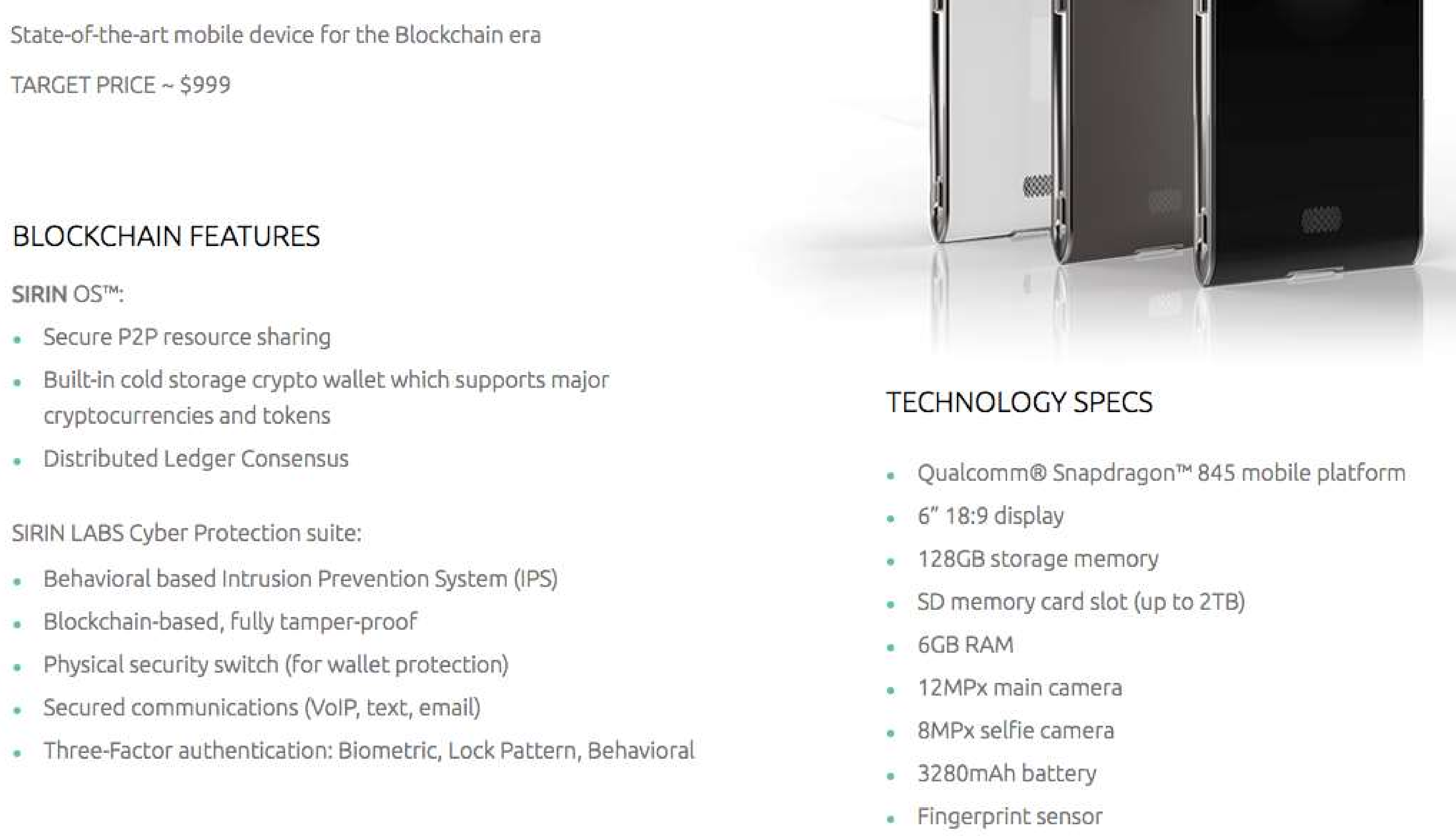
**Own Your ID. Own Your Data.**

To have your identity and data on the phone rather in a centralized cloud.

**Exodus Forum**

Open mindedness towards collective wisdom of the crowd.

# SIRIN Labs (1)



State-of-the-art mobile device for the Blockchain era

TARGET PRICE ~ $999

## BLOCKCHAIN FEATURES

**SIRIN** OS™:

- Secure P2P resource sharing
- Built-in cold storage crypto wallet which supports major cryptocurrencies and tokens
- Distributed Ledger Consensus

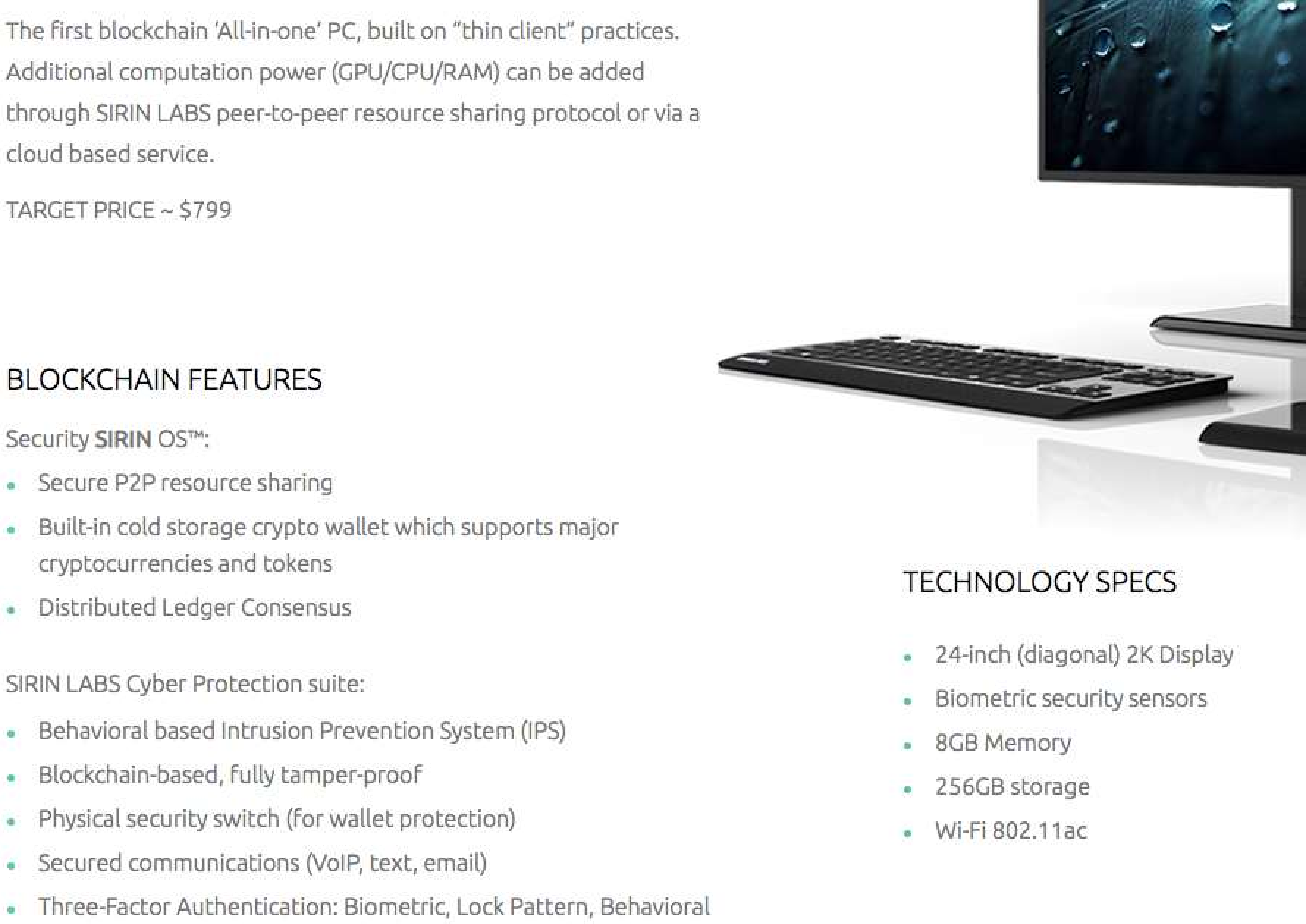
SIRIN LABS Cyber Protection suite:

- Behavioral based Intrusion Prevention System (IPS)
- Blockchain-based, fully tamper-proof
- Physical security switch (for wallet protection)
- Secured communications (VoIP, text, email)
- Three-Factor authentication: Biometric, Lock Pattern, Behavioral

## TECHNOLOGY SPECS

- Qualcomm® Snapdragon™ 845 mobile platform
- 6” 18:9 display
- 128GB storage memory
- SD memory card slot (up to 2TB)
- 6GB RAM
- 12MPx main camera
- 8MPx selfie camera
- 3280mAh battery
- Fingerprint sensor

# SIRIN Labs (2)



The first blockchain 'All-in-one' PC, built on "thin client" practices. Additional computation power (GPU/CPU/RAM) can be added through SIRIN LABS peer-to-peer resource sharing protocol or via a cloud based service.

TARGET PRICE ~ $799

BLOCKCHAIN FEATURES

Security **SIRIN** OS™:

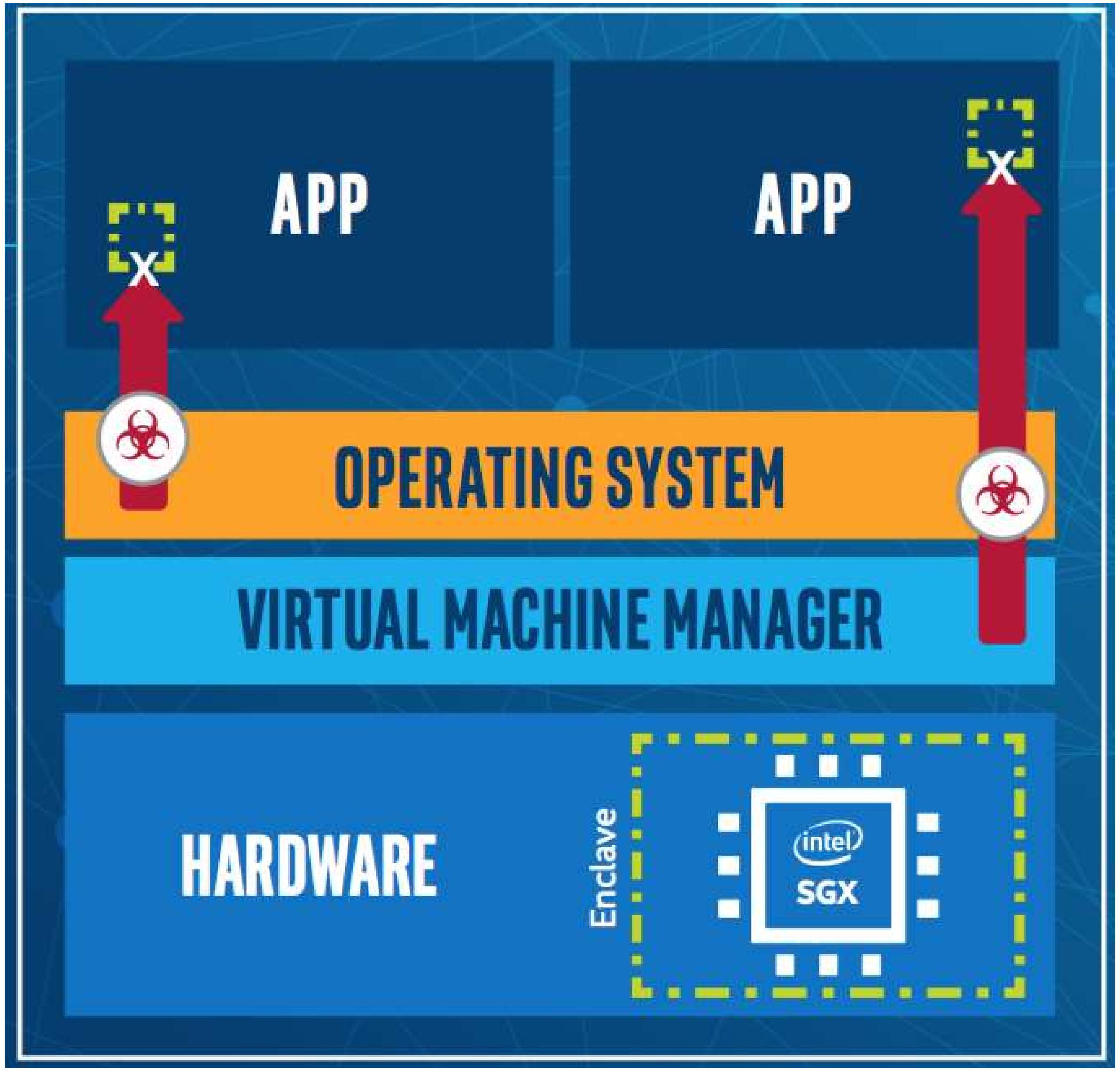
- Secure P2P resource sharing
- Built-in cold storage crypto wallet which supports major cryptocurrencies and tokens
- Distributed Ledger Consensus

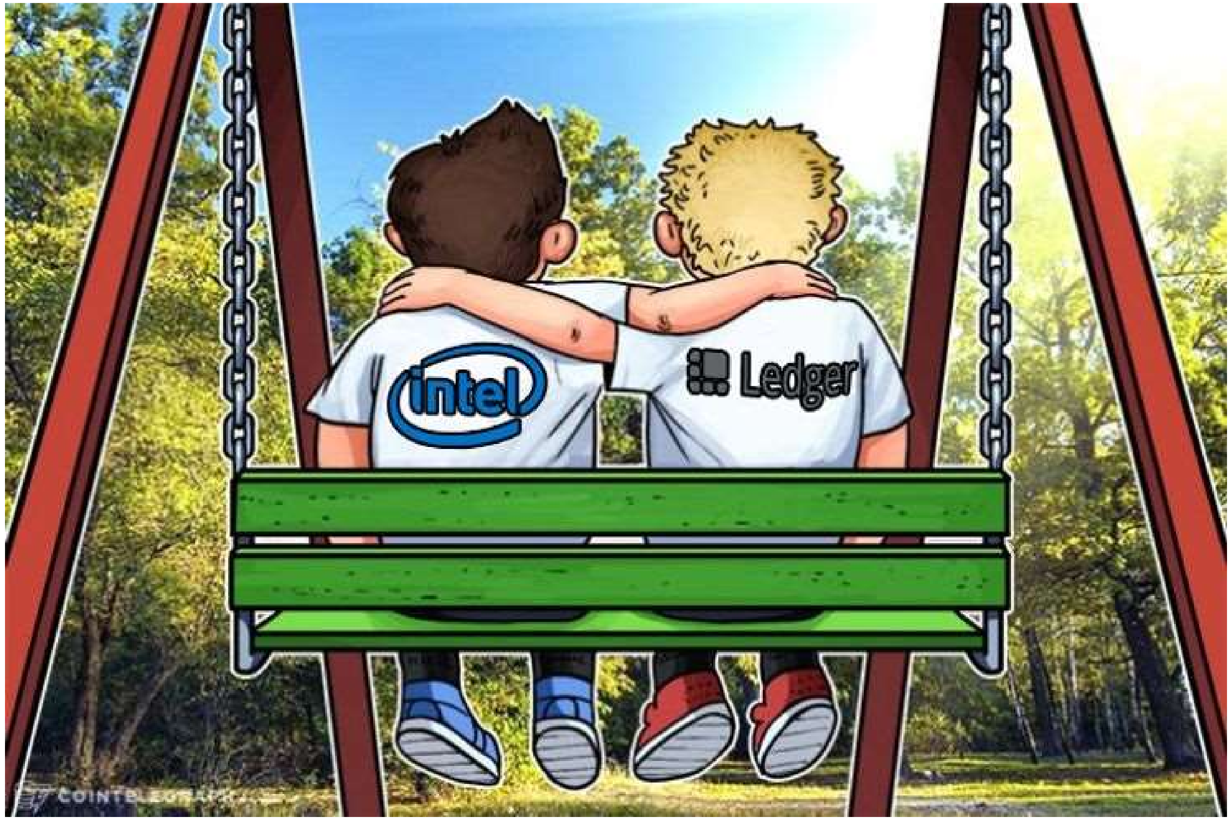
SIRIN LABS Cyber Protection suite:

- Behavioral based Intrusion Prevention System (IPS)
- Blockchain-based, fully tamper-proof
- Physical security switch (for wallet protection)
- Secured communications (VoIP, text, email)
- Three-Factor Authentication: Biometric, Lock Pattern, Behavioral

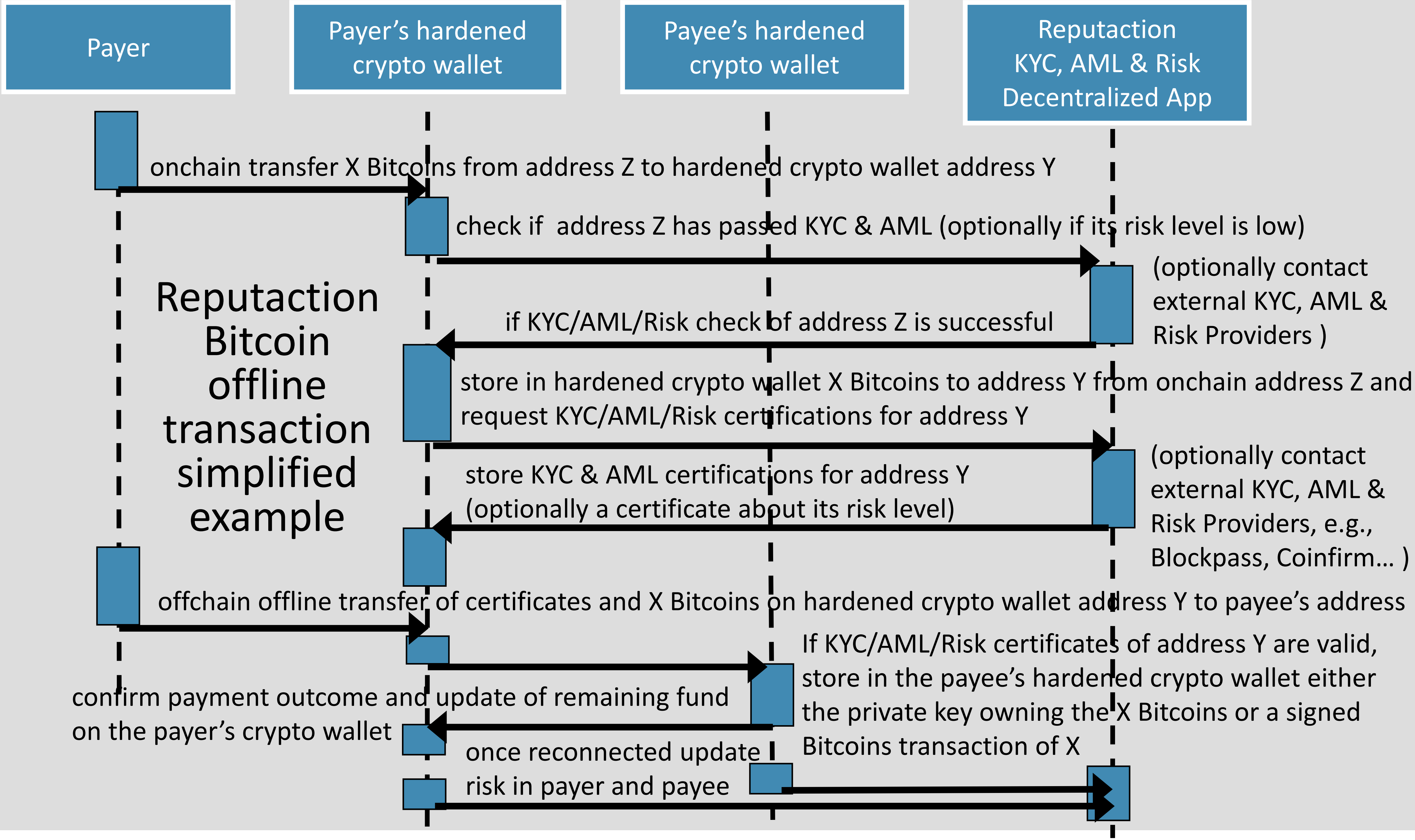
TECHNOLOGY SPECS

- 24-inch (diagonal) 2K Display
- Biometric security sensors
- 8GB Memory
- 256GB storage
- Wi-Fi 802.11ac





[Coin Telegraph]



Reputaction Bitcoin offline transaction simplified example

Payer

Payer’s hardened crypto wallet

Payee’s hardened crypto wallet

Reputaction KYC, AML & Risk Decentralized App

onchain transfer X Bitcoins from address Z to hardened crypto wallet address Y

check if  address Z has passed KYC & AML (optionally if its risk level is low)

(optionally contact external KYC, AML & Risk Providers )

if KYC/AML/Risk check of address Z is successful

store in hardened crypto wallet X Bitcoins to address Y from onchain address Z and request KYC/AML/Risk certifications for address Y

(optionally contact external KYC, AML & Risk Providers, e.g., Blockpass, Coinfirm… )

store KYC & AML certifications for address Y (optionally a certificate about its risk level)

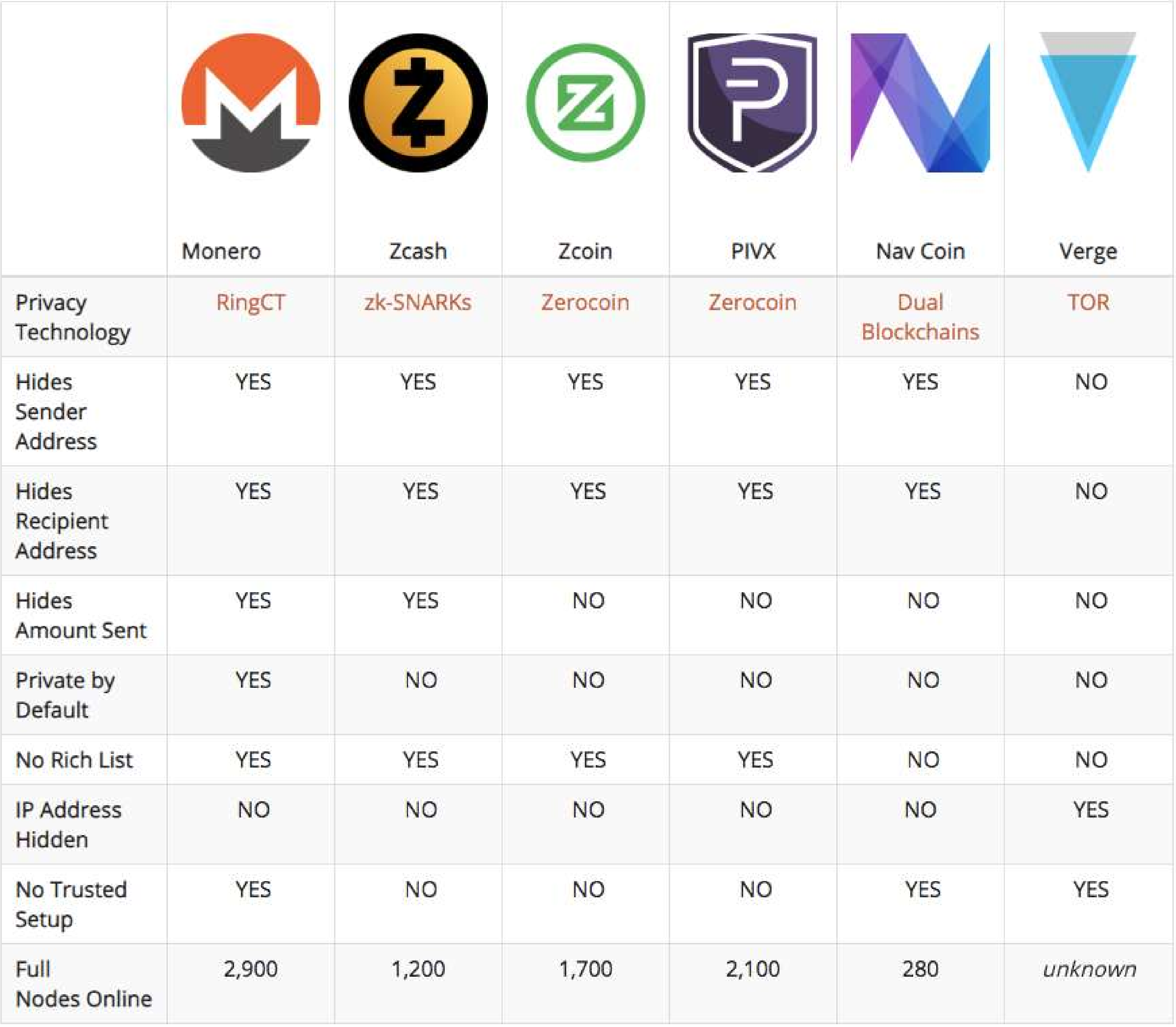
offchain offline transfer of certificates and X Bitcoins on hardened crypto wallet address Y to payee’s address

If KYC/AML/Risk certificates of address Y are valid, store in the payee’s hardened crypto wallet either the private key owning the X Bitcoins or a signed Bitcoins transaction of X

confirm payment outcome and update of remaining fund on the payer’s crypto wallet

once reconnected update risk in payer and payee

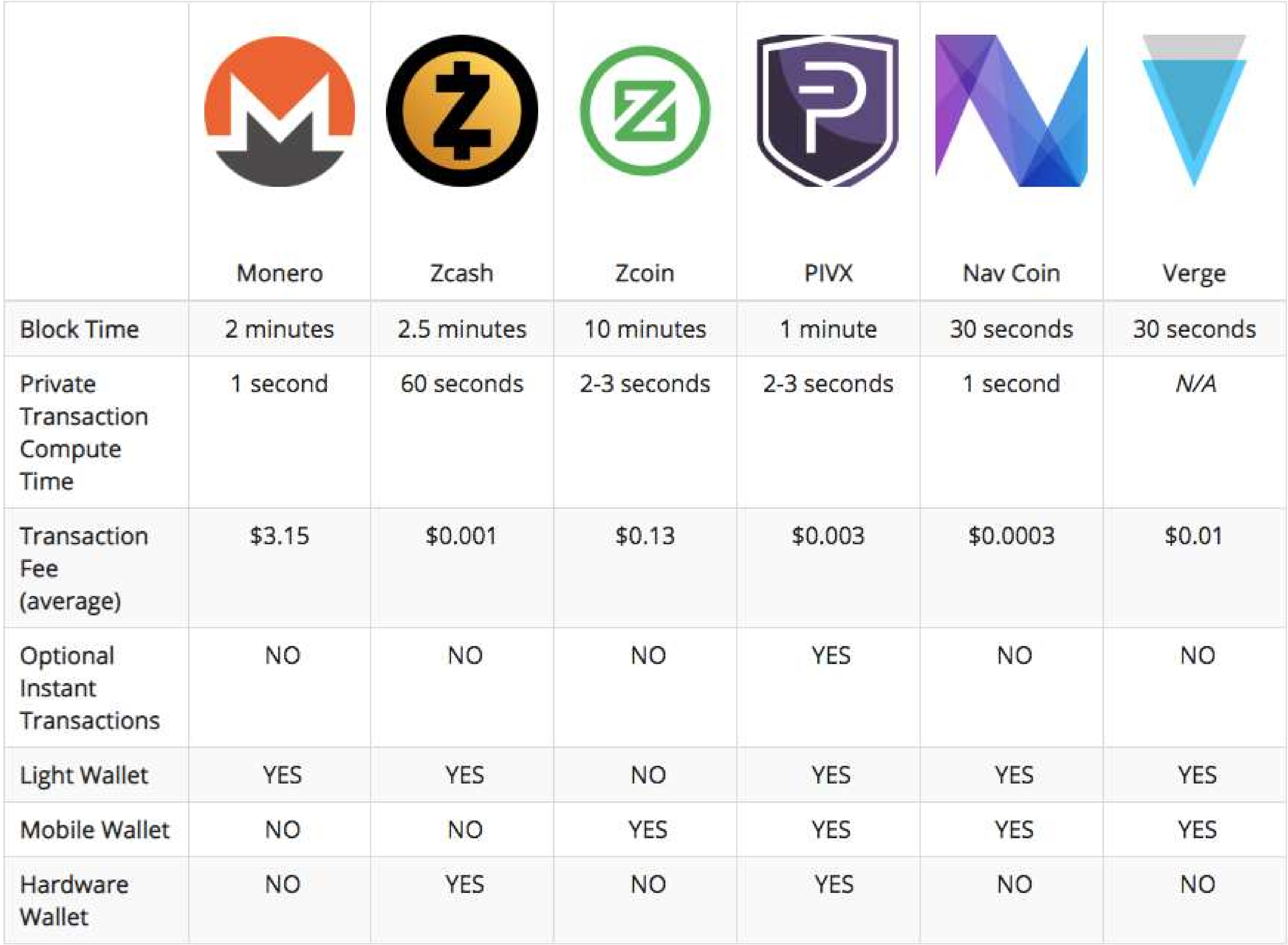
# Privacy Coins Comparison (1)



| | Monero | Zcash | Zcoin | PIVX | Nav Coin | Verge |
|---|---|---|---|---|---|---|
| Privacy Technology | RingCT | zk-SNARKs | Zerocoin | Zerocoin | Dual Blockchains | TOR |
| Hides Sender Address | YES | YES | YES | YES | YES | NO |
| Hides Recipient Address | YES | YES | YES | YES | YES | NO |
| Hides Amount Sent | YES | YES | NO | NO | NO | NO |
| Private by Default | YES | NO | NO | NO | NO | NO |
| No Rich List | YES | YES | YES | YES | NO | NO |
| IP Address Hidden | NO | NO | NO | NO | NO | YES |
| No Trusted Setup | YES | NO | NO | NO | YES | YES |
| Full Nodes Online | 2,900 | 1,200 | 1,700 | 2,100 | 280 | *unknown* |

[xbt.net]

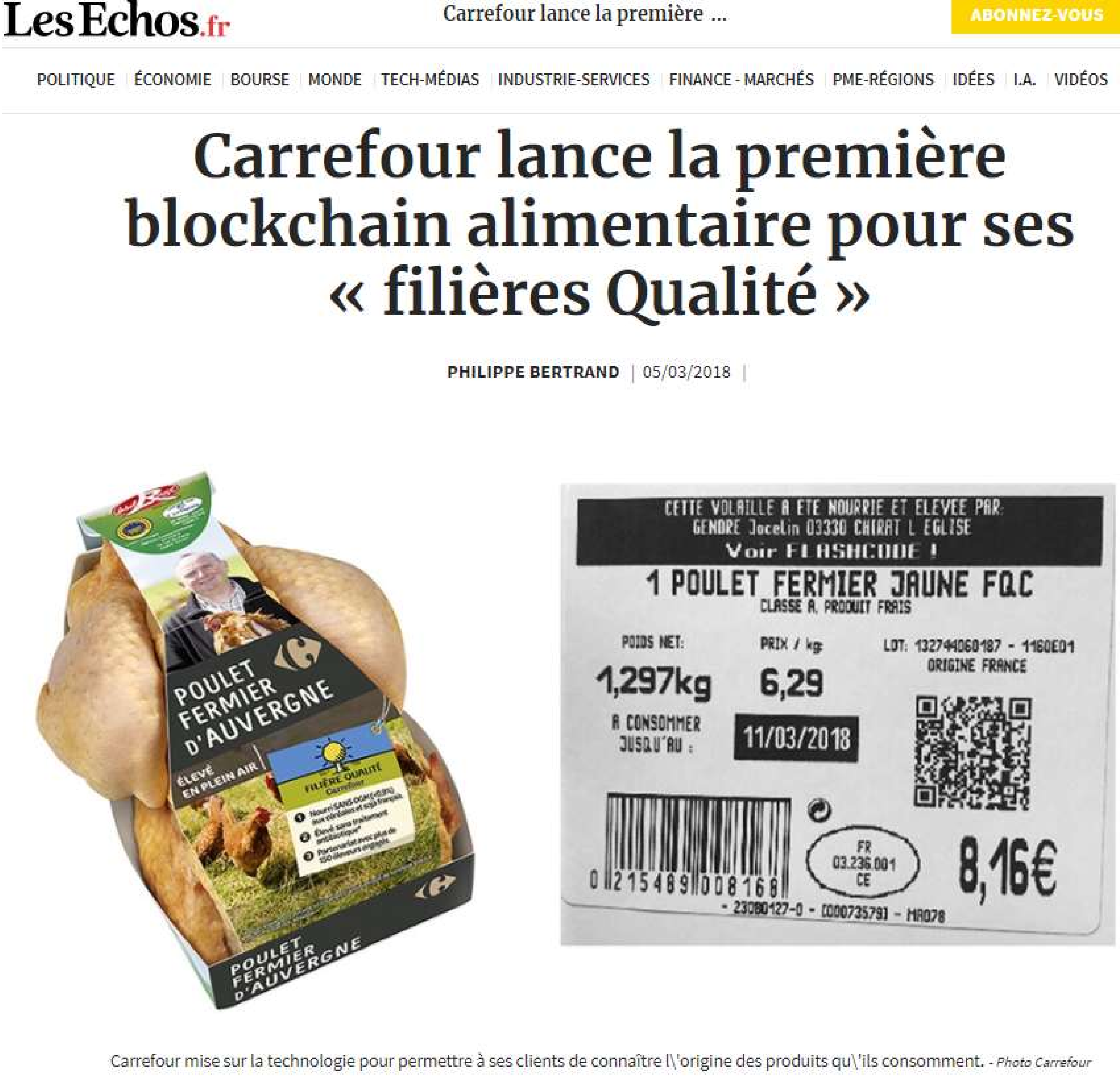
# Privacy Coins Comparison (2)



| | Monero | Zcash | Zcoin | PIVX | Nav Coin | Verge |
|---|---|---|---|---|---|---|
| Block Time | 2 minutes | 2.5 minutes | 10 minutes | 1 minute | 30 seconds | 30 seconds |
| Private Transaction Compute Time | 1 second | 60 seconds | 2-3 seconds | 2-3 seconds | 1 second | *N/A* |
| Transaction Fee (average) | $3.15 | $0.001 | $0.13 | $0.003 | $0.0003 | $0.01 |
| Optional Instant Transactions | NO | NO | NO | YES | NO | NO |
| Light Wallet | YES | YES | NO | YES | YES | YES |
| Mobile Wallet | NO | NO | YES | YES | YES | YES |
| Hardware Wallet | NO | YES | NO | YES | NO | NO |

[xbt.net]

# Blockchain Tracking Food App



LesEchos.fr

Carrefour lance la première ...

ABONNEZ-VOUS

POLITIQUE | ÉCONOMIE | BOURSE | MONDE | TECH-MÉDIAS | INDUSTRIE-SERVICES | FINANCE - MARCHÉS | PME-RÉGIONS | IDÉES | I.A. | VIDÉOS

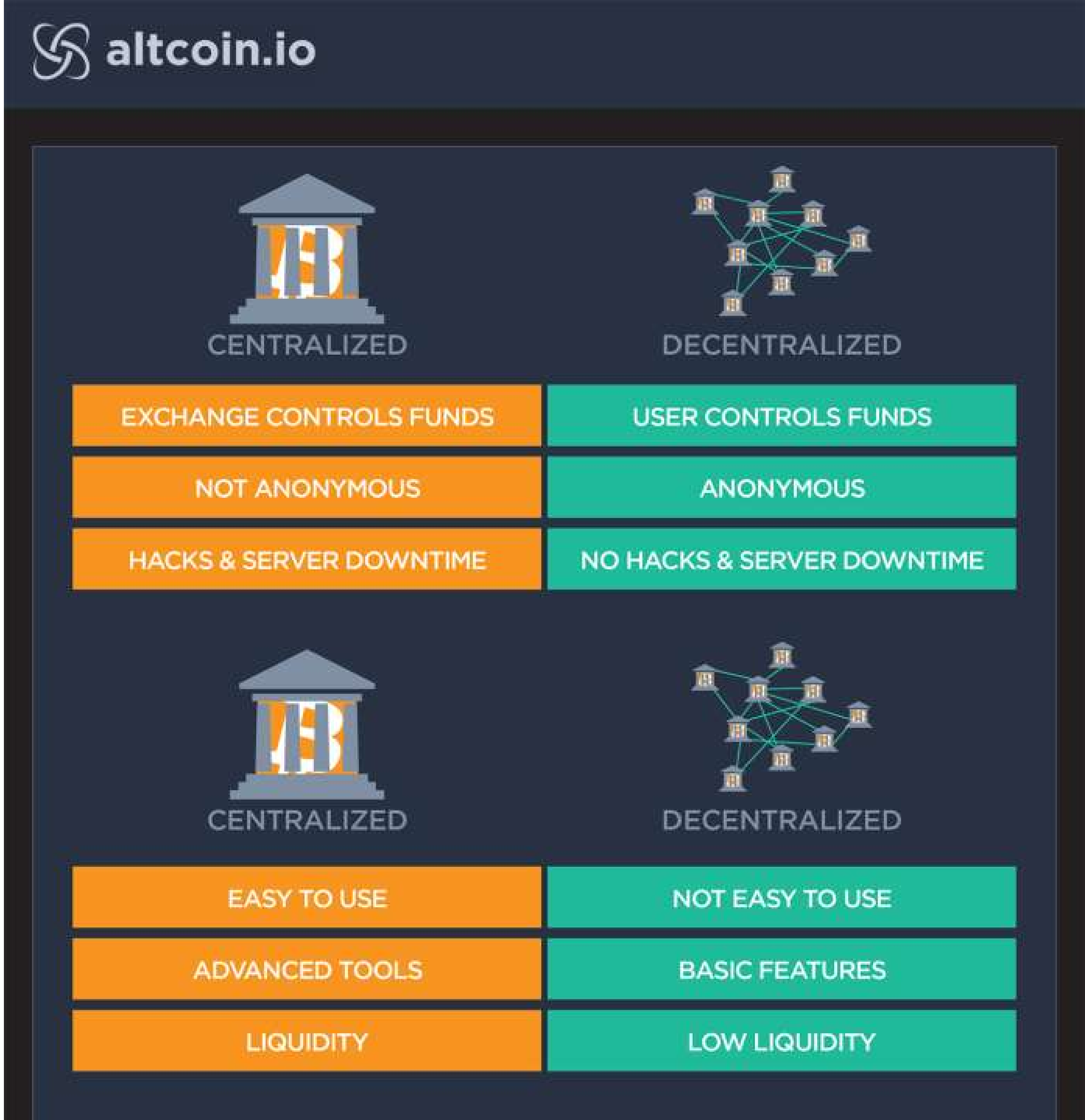
## Carrefour lance la première blockchain alimentaire pour ses « filières Qualité »

PHILIPPE BERTRAND | 05/03/2018 |

POULET FERMIER D'AUVERGNE
ÉLEVÉ EN PLEIN AIR
FILIÈRE QUALITÉ Carrefour
POULET FERMIER D'AUVERGNE
CETTE VOLAILLE A ETE NOURRIE ET ELEVEE PAR:
GENDRE Jocelin 03330 CHIRAT L EGLISE
Voir FLASHCODE !
1 POULET FERMIER JAUNE FQC
CLASSE A, PRODUIT FRAIS
POIDS NET:
1,297kg
PRIX / kg:
6,29
LOT: 13274060187 - 1160E01
ORIGINE FRANCE
A CONSOMMER JUSQU'AU :
11/03/2018
0 215489 008168
FR 03.236.001 CE
8,16€
- 23080127-0 - [00073579] - MA078

Carrefour mise sur la technologie pour permettre à ses clients de connaître l\'origine des produits qu\'ils consomment. - *Photo Carrefour*

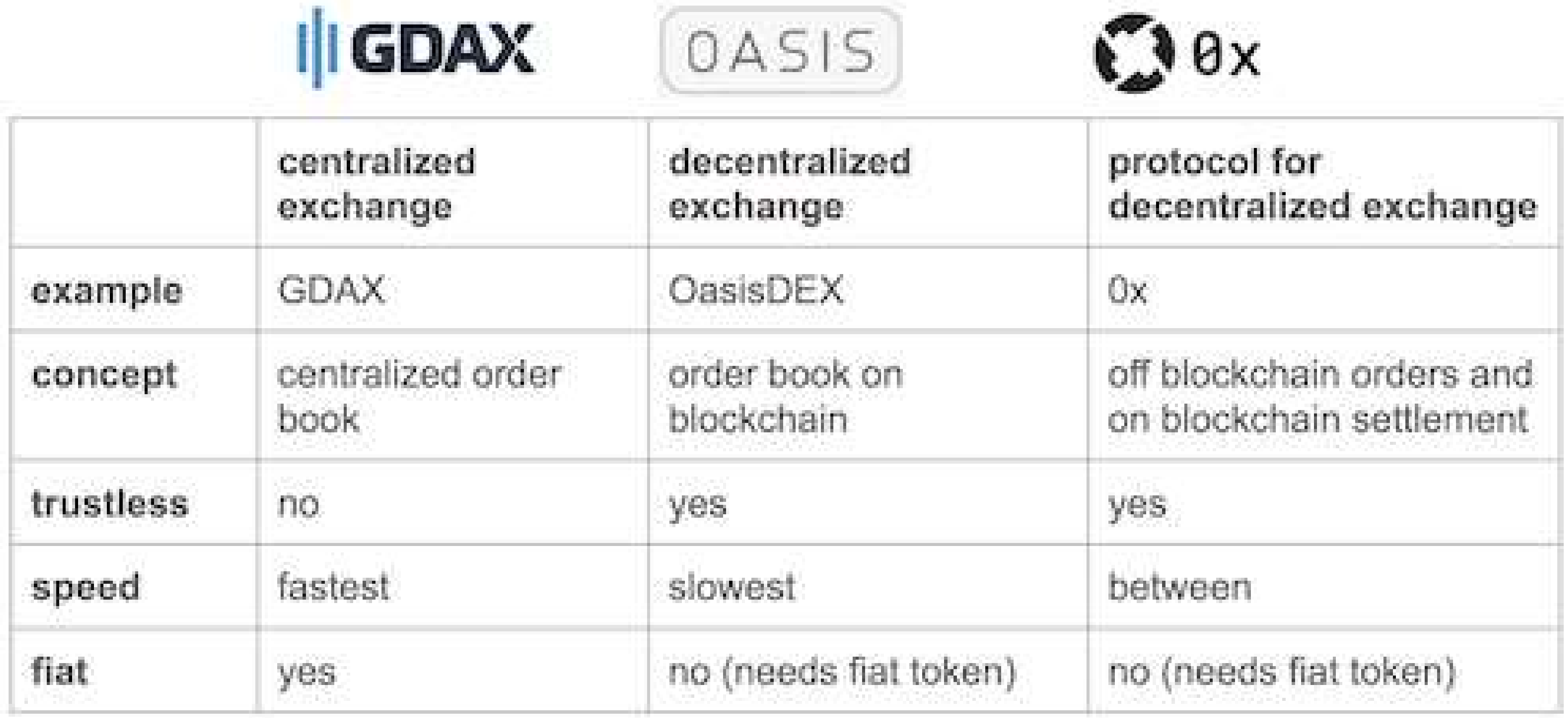
# Centralized vs Decentralized Exchanges



altcoin.io

| CENTRALIZED | DECENTRALIZED |
|---|---|
| EXCHANGE CONTROLS FUNDS | USER CONTROLS FUNDS |
| NOT ANONYMOUS | ANONYMOUS |
| HACKS & SERVER DOWNTIME | NO HACKS & SERVER DOWNTIME |
| CENTRALIZED | DECENTRALIZED |
| EASY TO USE | NOT EASY TO USE |
| ADVANCED TOOLS | BASIC FEATURES |
| LIQUIDITY | LOW LIQUIDITY |

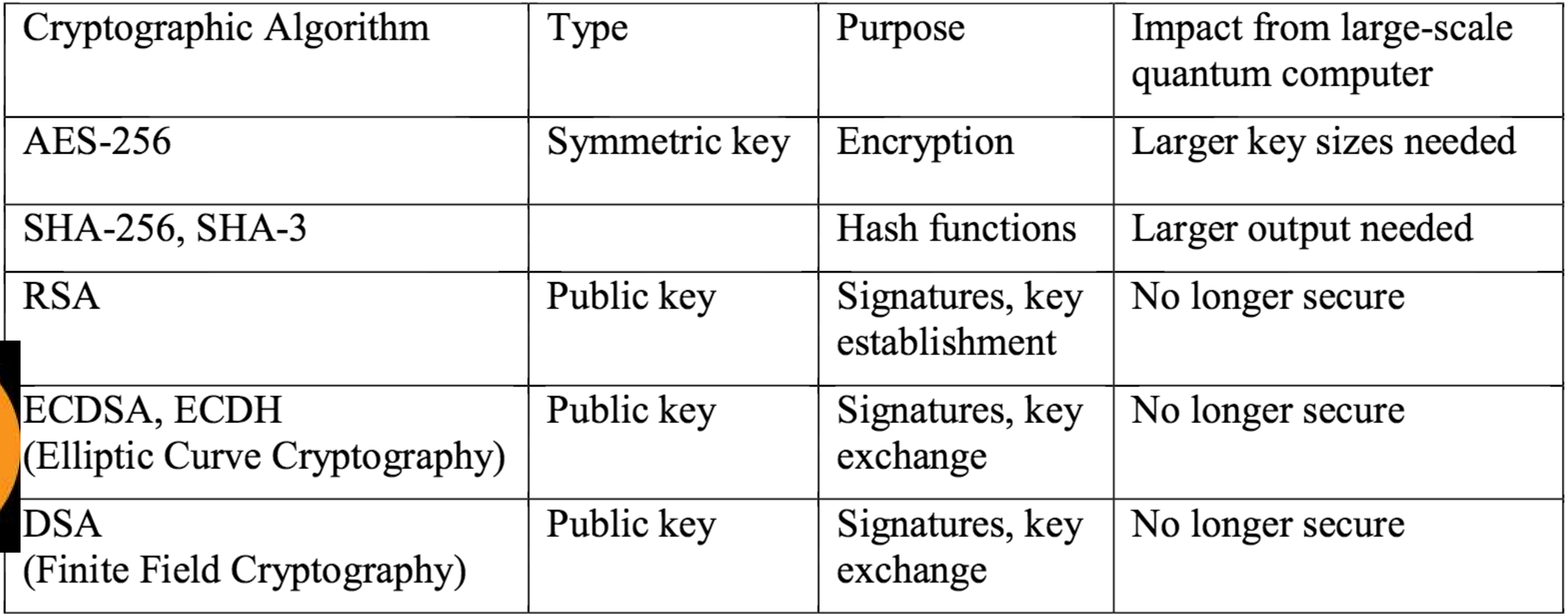
# Decentralized Exchanges Examples


GDAX
OASIS
0x

| | centralized exchange | decentralized exchange | protocol for decentralized exchange |
|---|---|---|---|
| example | GDAX | OasisDEX | 0x |
| concept | centralized order book | order book on blockchain | off blockchain orders and on blockchain settlement |
| trustless | no | yes | yes |
| speed | fastest | slowest | between |
| fiat | yes | no (needs fiat token) | no (needs fiat token) |

[Coin Bureau]

# Quantum Computing Attacks



| Cryptographic Algorithm | Type | Purpose | Impact from large-scale quantum computer |
|---|---|---|---|
| AES-256 | Symmetric key | Encryption | Larger key sizes needed |
| SHA-256, SHA-3 | | Hash functions | Larger output needed |
| RSA | Public key | Signatures, key establishment | No longer secure |
| ECDSA, ECDH (Elliptic Curve Cryptography) | Public key | Signatures, key exchange | No longer secure |
| DSA (Finite Field Cryptography) | Public key | Signatures, key exchange | No longer secure |

**Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms**

[NIST]

## Thanks for your attention!

Jean-Marc.Seigneur@reputaction.com

Follow me on Twitter or Instagram @reputaction