Blockchain and Digital Assets

Alan Tobin, PhD

First draft: 2018-10-30
This draft: 2024-06-19

Contents

Blockchain

Blockchain is world's first **immutable database** technology.
A blockchain database is resistant to modification by design.

Blockchain is a **distributed ledger** that can record transactions between parties in a verifiable and permanent way. Transactions are irreversible (unlike in the traditional financial system). One revolutionary consequence of this is that businesses need not keep separate ledgers of transactions, but can use a common database that no one controls. Neither trust between participants nor external authority/regulator is required. Huge savings result because of the high costs of resolving discrepancies between separate ledgers.

A blockchain system works by each participating computer (node) running software which adheres to the same protocol for inter-node communication and validating new blocks of data. Thus, blockchain is typically managed by a peer-to-peer network, hence it is decentralized. One key benefit of this is no single point of failure.

Data is added to the blockchain database as a time-stamped sequence (chain) of standardized blocks. The blocks of transactions are stacked on top of each other indefinitely. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

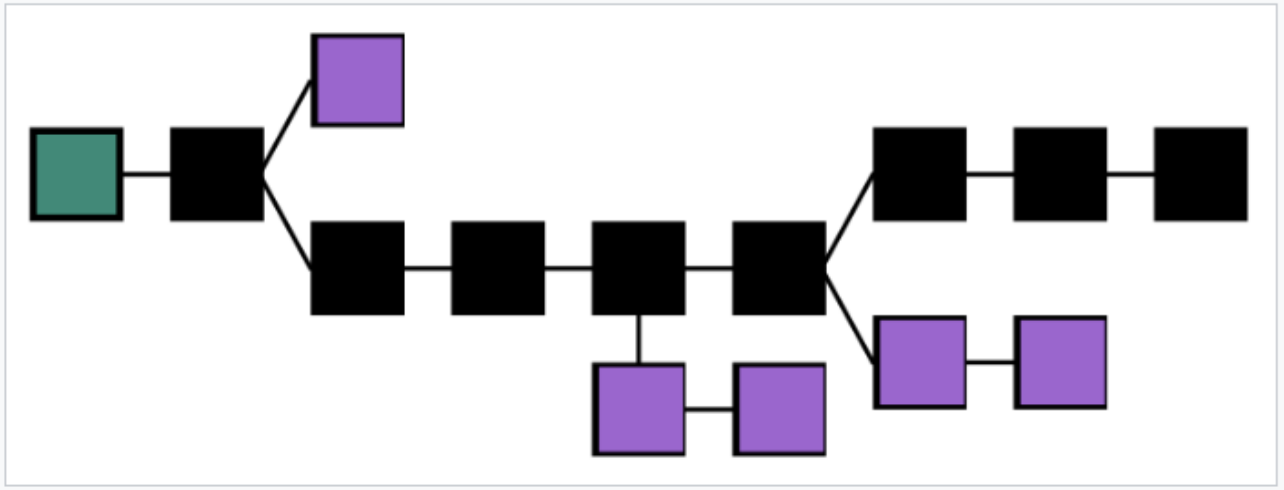


Figure: **Blockchain formation.**
The **main chain** (black) consists of the longest series of blocks
from the **genesis block** (green) to the current block.
Orphan blocks (purple) exist outside of the main chain.

A wide variety of blockchain designs exists.
Examples of architectural differences between blockchains include:

- Public / private / semi-private blockchains (permissioning).
- Consensus mechanisms: Proof-of-work, proof-of-stake, delegated, federated, etc.
- Inter-block time (e.g., 10 min for Bitcoin, 15 sec for Ethereum, 0.4 sec for Solana).

Requirements to blockchain systems that serve enterprise-scale or planet-scale needs are similar to those typically seen in "big data" distributed databases:
Throughput ~1M tx/s, capacity >1 Petabyte, latency <1 second.
For comparison:
Stock exchanges and ad networks run 100k-500k tx/s.
Visa handles 2k tx/s on average, with a peak rate of 56k tx/s.
For **scalability**, blockchain must have high **thruput**, high **capacity**, low **latency**.

Another revolutionary impact is that the blockchain technology allows building decentralized applications (Dapps) which can serve a wide range of areas from fintech and governments to healthcare and supply chain management. Decentralization will, in particular, completely redesign the internet through the so called decentralized web (aka web 3.0).

Blockchain can also serve a timestamping function because each block is timestamped.
If you record something into an immutable blockchain, you can later prove that the information or even a physical object / characteristic existed at a certain point in time.

Blockchains are a way of ordering and verifying transactions in a distributed ledger, where a network of computers maintains and validates a record of consensus of those transactions with a cryptographic audit trail.

Initiate the transaction.

- Multiple parties transact.
- All transactions are recorded, including the transaction's date, time, parties, and amount wants to do a transaction.

Post and record the transaction to the network.

- The transaction is added in order into a network's 'block' and presented.
- Entries can be added but not deleted.
- Each node in the network owns a full copy of the ledger.

Broadcast.

- The 'block' is broadcast to every party and their nodes in the network.
- The network of computer nodes verify and, validate by running a software that continuously replicates the ledger.

Validate via consensus and confirm.

- The network verifies, validates, and approves; the confirmation is broadcast to the other nodes.
- Consensus (agreed mathematical mechanism) is recorded and provides the basis for the trust mechanism.

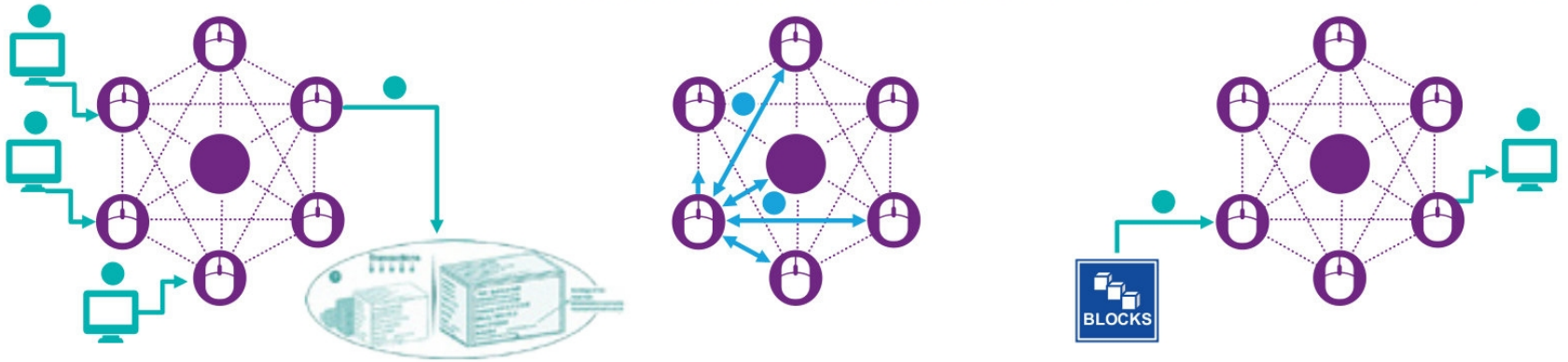
Consensus mechanism applied

Immutable, encrypted block

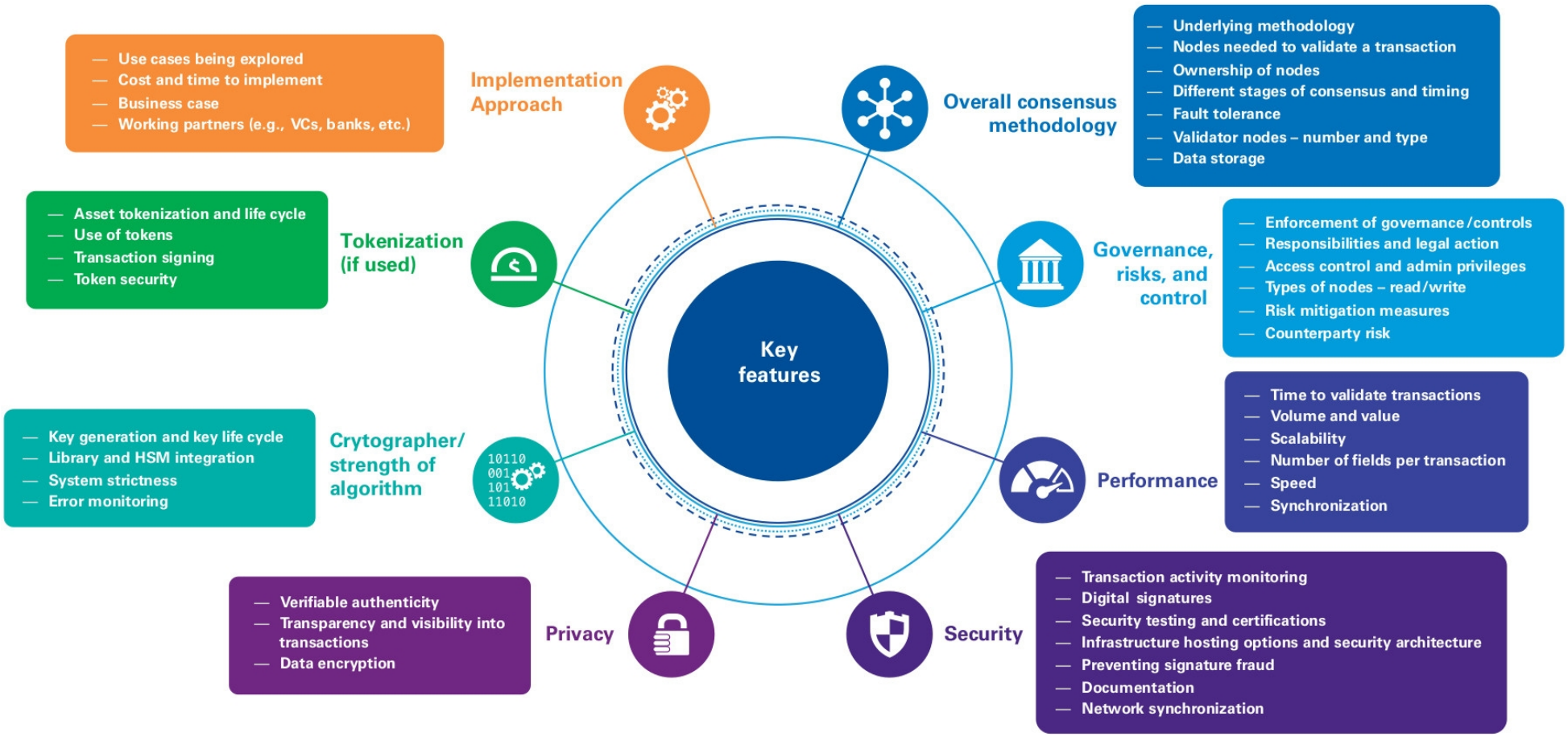
- The confirmed block is added in a linear and chronological order to the chain.
- This provides a transparent record of transactions, audit trail, and traceable digital fingerprint.
- Data is pervasive and persistent and creates a reliable transaction record.

Transaction completed.

- Nodes have access to a shared single source of truth.
- A completed block gives way to the next block in the blockchain.



Distributed Consensus Evaluation Framework



Consensus mechanism - a method to authenticate and validate a transaction without the need to trust a centralized authority. Can be constructed on and off a blockchain. A variety of approaches exist.

Authentication - proving counterparty identities and existence of assets via cryptographic private/public keys.

Cryptocurrencies

Among the many blockchain applications, money (cryptocurrencies) is notable for its impact and robustness. Bitcoin was the first and is still the dominant implementation. Thousands of cryptocurrencies exist with various purposes, use cases, and target audiences.

- A **Cryptocurrency** is 2-in-1: **Money + Payment System**
- It operates 24/7.
- It is global, borderless, jurisdiction-agnostic.
- Its design can be permissionless - anyone can use such cryptocurrency with full rights equal to those of any other entity's.
- Cryptocurrencies are referred to as "cash for the Internet".

What the internet has done for information exchange - irrelevance of national borders, fast, near-costless communication - cryptocurrencies have done for payments.

Transaction irreversibility in cryptocurrencies makes it practical to use **micropayments** (fractions of a penny). These can be useful in a variety of applications, e.g. for online or mobile billing per usage in tiny amounts. The traditional financial system cannot handle micropayments because the cost of dispute resolution makes them uneconomical. Traditional financial transactions are always reversible, except cash.

Top Blockchain-based assets by market cap, 2024-06-13:

#	Asset	Market Cap, $B	Daily Volume, $B
1	Bitcoin	1,340	34
2	Ethereum	426	17
3	USD Tether	112	67
4	Binance coin	90	2
5	Solana	71	3
6	USDC	32	7
7	Ripple	27	1.2
8	Dogecoin	21	1.3
9	Toncoin	18	0.4
10	Cardano	15	0.4
Top 5000 assets		2,480	*88*

Smart Contracts and Smart Property

A blockchain system can be viewed as a distributed computer. The computer code executed on the network makes it possible to form agreements via blockchain. Such agreements are called smart contracts. They are self-executing, typically with automatic payments. Execution of a smart contract cannot be stopped or altered by any authority.

Smart contracts enable **smart property** - the property that is controlled, traded, loaned via blockchain using smart contracts. It can be physical (car, house, phone) or non-physical (shares in a company, access rights to a remote computer, etc.)

Making property smart allows it to be traded with significantly less trust. This reduces fraud, mediation fees and allows trades to take place that otherwise would have never happened. For example, it allows strangers to loan you money over the internet taking your smart property as collateral. This makes lending more competitive and thus credit cheaper.

Primitive forms of smart property are already common. For example, cars come with immobilizers, which augment the physical key with a cryptographic protocol, ensuring that only the holders of the correct token (private key) can activate the engine. They have dramatically reduced car theft.

Nowadays, a cryptographic private key is usually held in a physical container (e.g., SIM card) and cannot be easily transferred or manipulated. Smart property changes this, allowing ownership to be intermediated by blockchain miners.

Tokenization is pairing a unique physical item with a corresponding digital token. Physical objects thus can have a digital twin or representation, which can change ownership, etc. Tokens are used in many areas, e.g. supply chain management, intellectual property, anti-counterfeiting, etc.

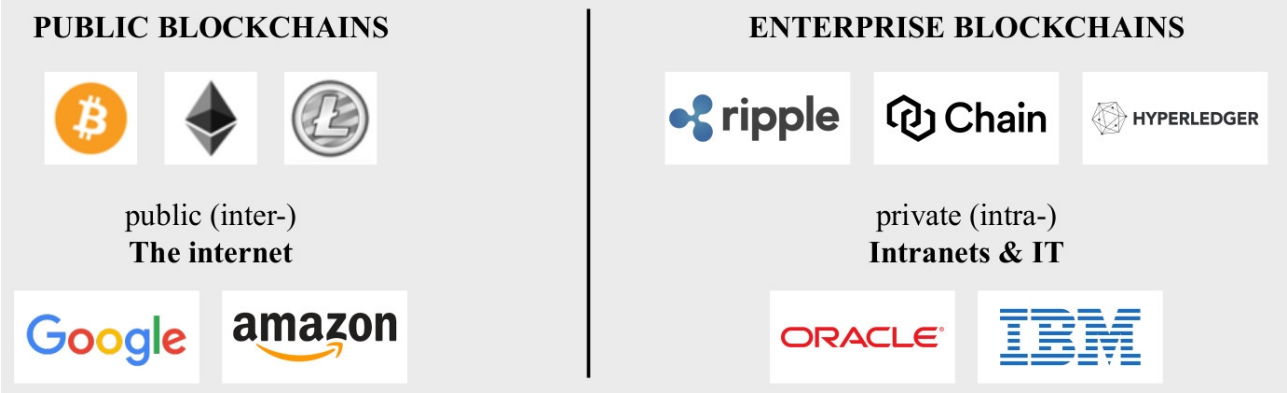
Distributed markets is a P2P implementation for securities trading (bonds, stocks, etc.)
It relies heavily on smart contracts.

Agent is an autonomous computer program that **maintains its own wallet**.
Agent buys any resources it needs, e.g. server time. It can potentially even hire/fire humans. Money is obtained by the agent selling services. If demand exceeds supply, agents can spawn children that either survive or die depending on whether they can get enough business.

Comparison with the Internet

It can be helpful to think of the blockchain industry by analogy with the internet industry in mid-to-late 1990's. The internet evolution back then can be used as a basis for gauging the current state and forecasting future developments in the blockchain arena.

The Internet-Intranet Comparison:



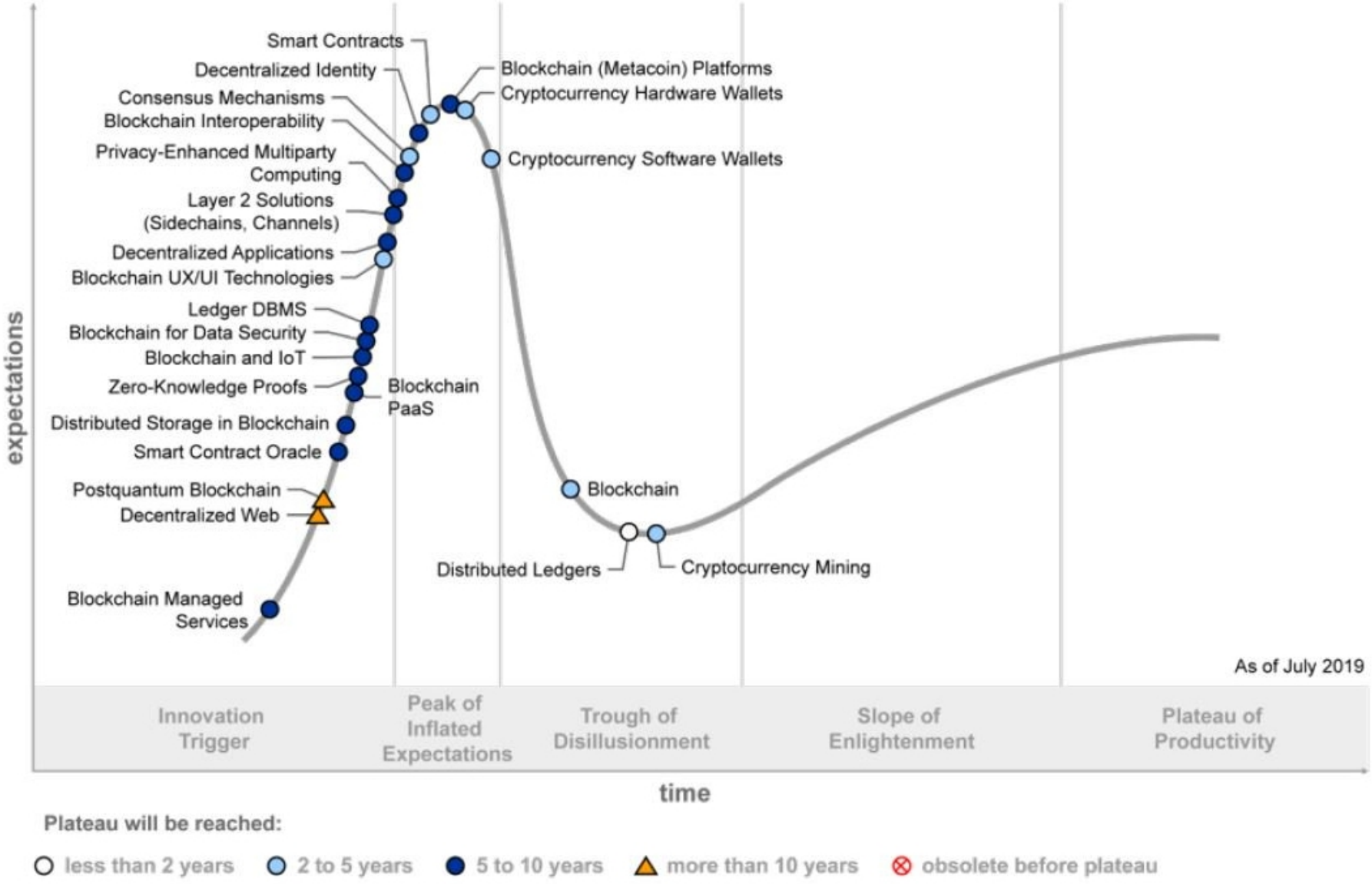
Both public and enterprise blockchains have useful applications, much like the Internet and corporate intranets.

'Public' (Open) vs 'Enterprise' (Permissioned) Blockchains: Features Comparison:

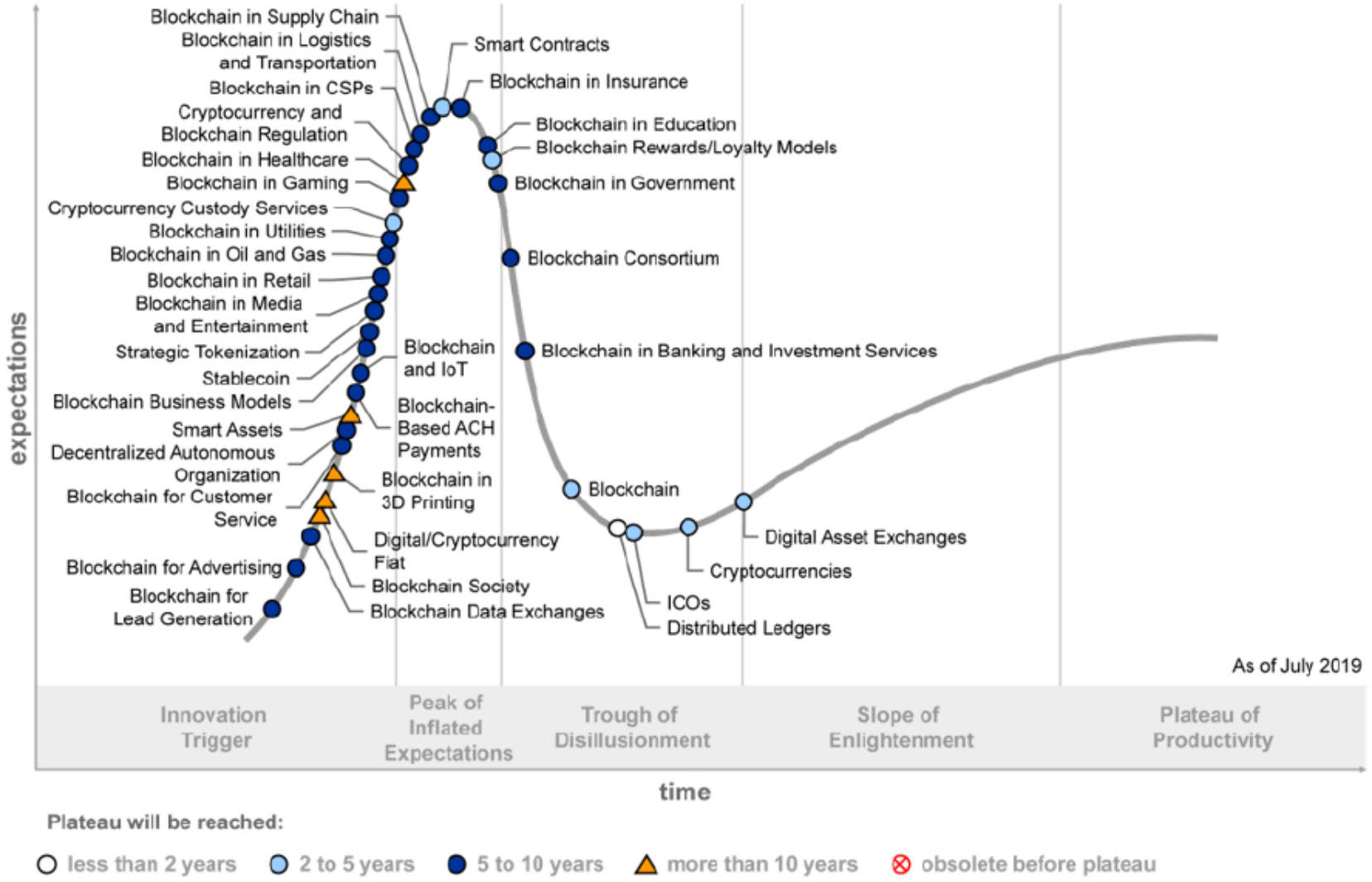
	PUBLIC	ENTERPRISE
ACCESS	Open read and write	Permissioned write and/or read
SPEED	Slower	Faster
SECURITY	Open network	Approved participants
IDENTITY	Anonymous or pseudonymous	Known identities
ASSET	Native assets	Any asset

Computer protocols (e.g. the TCP/IP suite, which is the foundation of the internet) have been of tremendous value, but **without a meaningful way to *monetize*** their development. The advent of the blockchain technology has changed this. Now, we see an explosion of protocol developments.

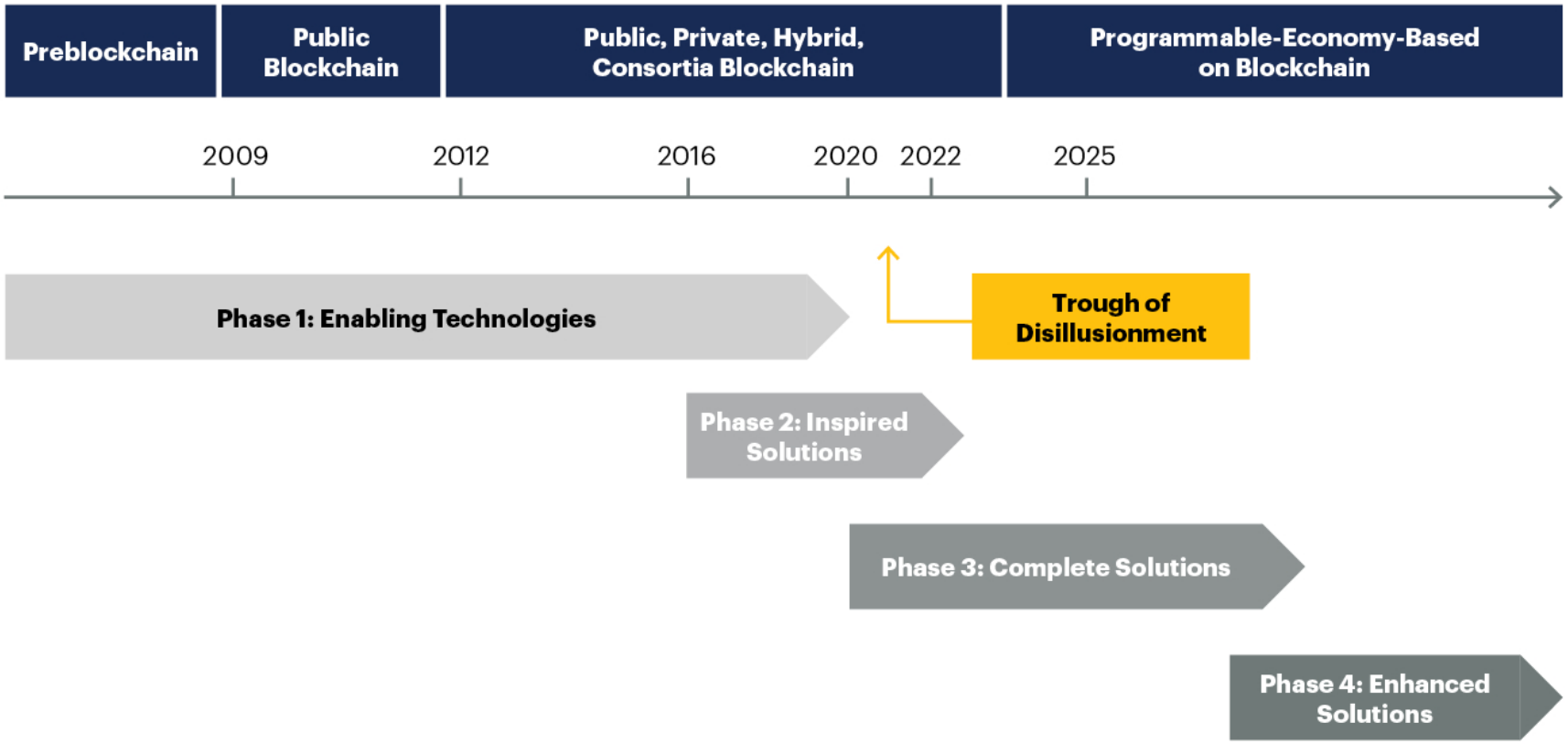
Hype Cycle for Blockchain Technologies 2019



Hype Cycle for Blockchain Business 2019



Blockchain Timeline



[THE FOLLOWING SECTIONS NEED UPDATING]

Blockchain Applications by Industry in 2018

Auditing
Records can be instantly independently verified.

Automotive
Track truthful, full history of vehicle from pre-production to sale.
Supply chain parts management.

Banking, Financial, Fintech
P2P payments and lending.
Currency Exchange and remittance.
Clearing and settlement (T+0 instead of common T+3 in securities trading).
Decentralized markets.

Business Contracts - Set pre-defined rules for transactions between two or more companies engaged in a partnership.

Compliance
Track processes against regulations with pre-defined rules

Donations / Charity
Tracking donation allocation, accountability, integrity.
Reduce overhead and complexity of donation payment processing.
Provide auditable trail for donations to prevent fraud.
Ensure crowdfunded campaigns receive donations and contributors are compensated.

Cloud Storage
Increased security with a shift from centralized data security to decentralized network.
Lower transactional costs within a decentralized network.
Crowdsource unused cloud storage.

Commercial Vehicles & Transportation
Tracking journey stops; paired with IoT to create an immutable ledger of trip data.

Credit History
Make credit reports more accurate, transparent, and accessible.

Cybersecurity
Fight hacking with immutability of ledger.
Guarantee validity with data integrity.
No Single Point of Failure (decrease in IP-based DDoS attack success).

Education
Digitizing, verifying academic credentials.
Federated repository of academic information specific to class, professor, and student.

Energy
Bypass public grids to allow for cheaper, p2p energy transfer. Smart utility metering.

Forecasting
Combined with machine learning algorithms, blockchain can provide a decentralized forecasting tool.

Government & Voting
Reduce voter fraud, inefficiencies with verifiable audit trails.
Minimize government fraud, digitize most processes.
Increase accountability and compliance for government officials.
Identity validation; integrity of citizen registry data.

Human Resources
Background checks: Verification of identity, employment history.
Payment and benefits process validation - smart contracts.

Insurance
Improve multi-party contracts.
Streamline risk contract efficiency.
Streamline claims adjudication.
Reduce disputes with transparency of shared data

IOT
Ability for IoT applications to contribute transactional data to blockchains.

Law enforcement
Integrity of evidence, resistance to falsification of case data.
Documentation of time-stamped, chronological chain of facts.

Legal
Smart contracts with defined rules, expiration, and accessibility for relevant parties.

Marketing - Bypass intermediaries, providing more cost-effective advertising.

Media
Control of ownership rights. Anti-piracy / copyright infringement.
Use of smart contracts for artist compensation/legal proceedings.
Payments processing - secure, anti-3rd party (opens up content availability internationally)

Medical / Healthcare
Drug Supply Chain Integrity.
Patient Databases/Indexes on blockchain.
Claims Adjudication.
Medical Supply Chain Management.
Transparency and Automation within patient-to-hospital or patient-to-doctor transactions.
Clinical trial provenance - integrity with an auditable trail of data exchange.
Efficiency, privacy, and ownership of patient health data.

Real Estate
Transparency within agreements.
Verify property information, update and decentralize records.
Reduce paperwork, digitize transactional processes.
Record, track, transfer land titles.

Supply Chain Management
Shared blockchain to coordinate logistics, payments, financial terms, and contract rules.
End-to-End visibility (provenance) and tracking of supply chain process in real-time.

Travel
Passenger identification, boarding, payment, and other documentation digitized & verified.
Loyalty programs digitization and tracking.

Any Industry
Information-sharing across organizations.

Distributed Applications aka ĐApps

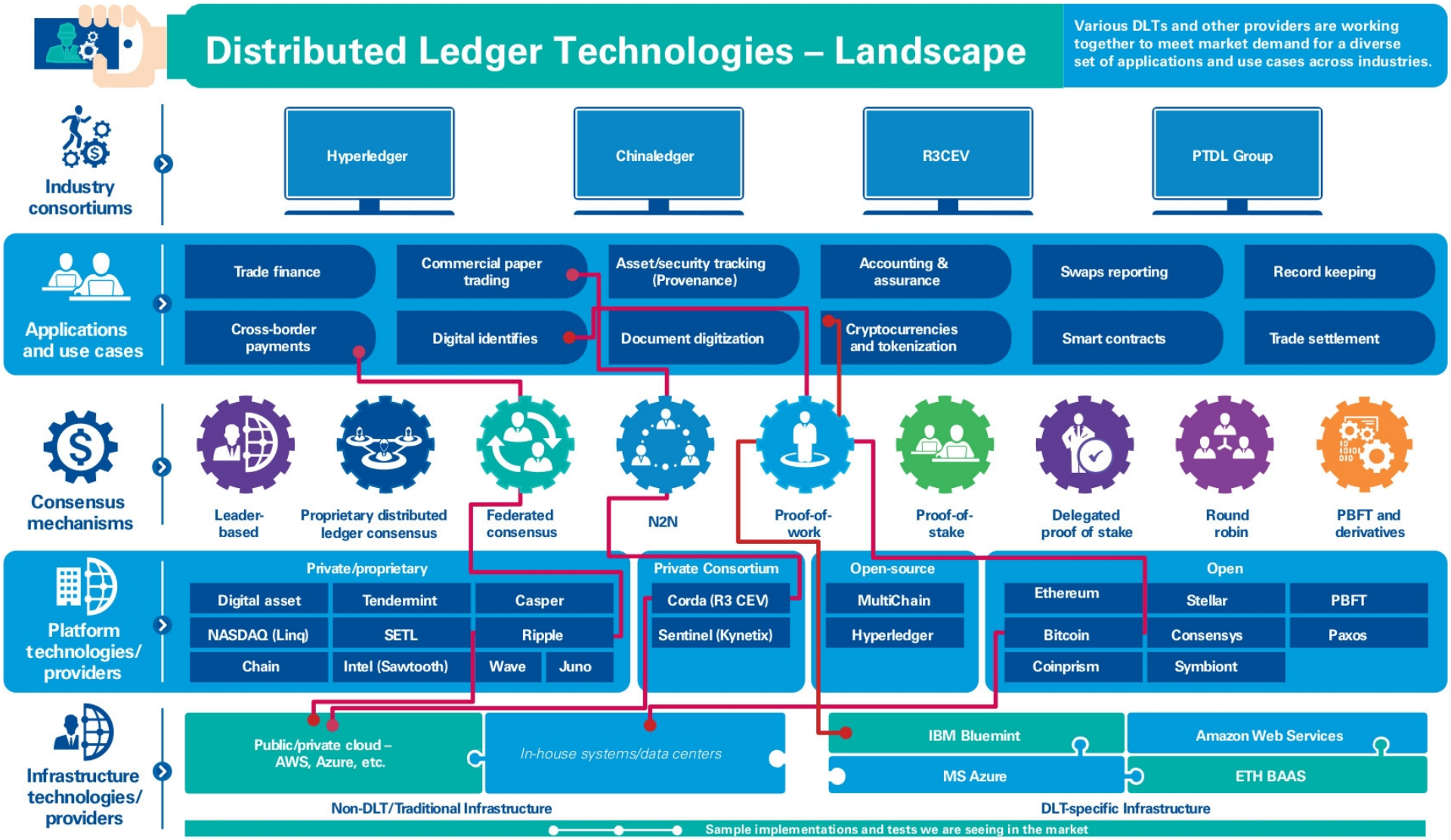
DApps Stats as of 2018-11-25

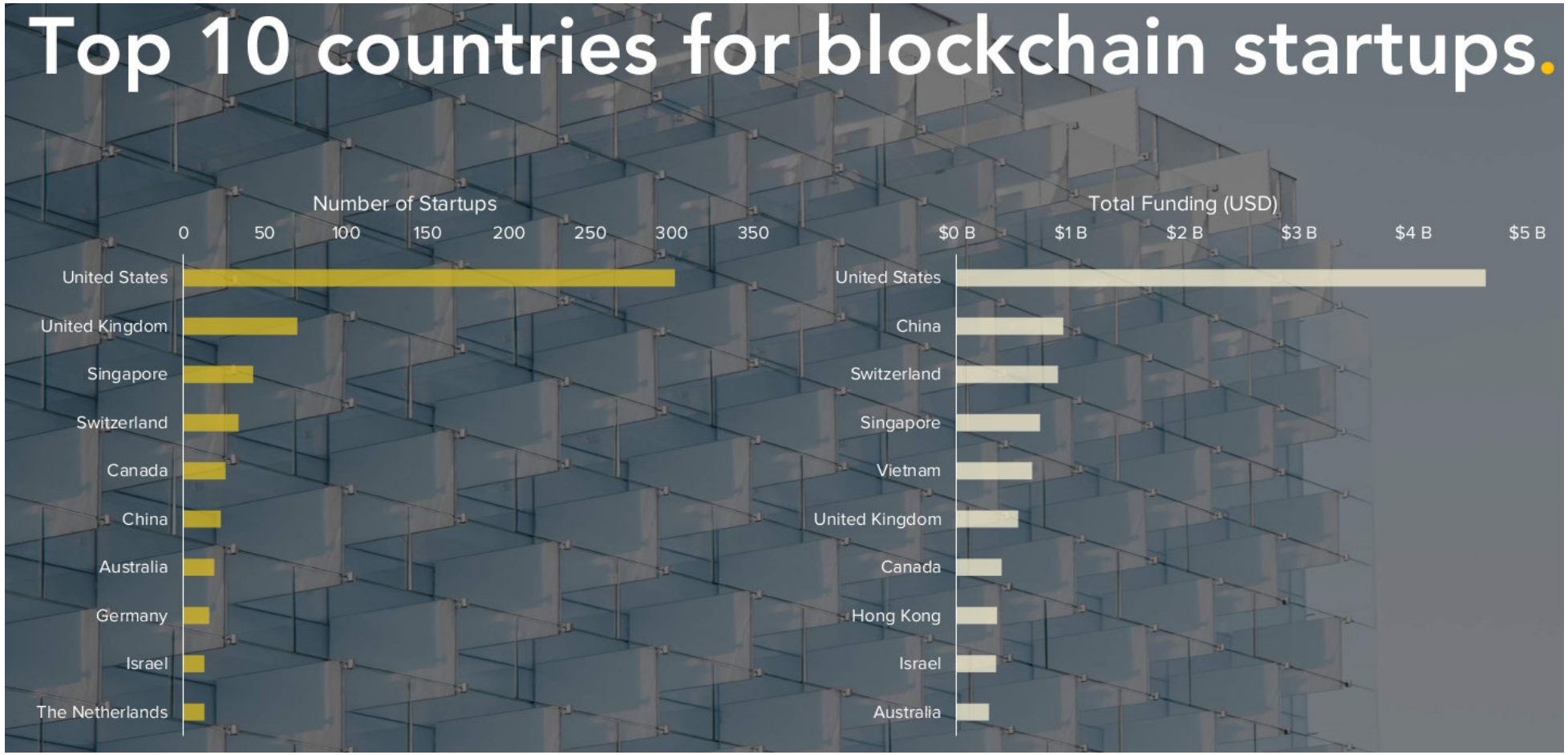
	Category	ĐApps	Users/month	Txs (30d)	# of contracts
	Total	2,255	1.5m	45m	5k
1.	storage	55	53k	70k	19
2.	exchanges	181	50k	773k	463
3.	finance	229	30k	122k	2,030
4.	gambling	492	22k	504k	1,360
5.	wallet	74	19k	47k	23
6.	games	456	12k	477k	985
7.	media	111	6k	11k	84
8.	development	142	6k	14k	26
9.	social	229	5k	17k	116
10.	governance	62	2k	6k	26
11.	identity	27	1k	74k	17
12.	property	62	<1k	6k	60
13.	security	67	<1k	1k	20
14.	insurance	21	12	14	3
15.	energy	26	0	0	3
16.	health	16	0	0	2

Dapps by Platform, 2018-11-25:

Platform	ĐApps	Daily_users	Txs (24hr)	Volume (24hr)	#contracts
eos	96	35k	1,420k	8m	142
ethereum	2,146	14k	74k	0.2m	5,040
poa	13	29	2k	2m	42

Ecosystem in 2018

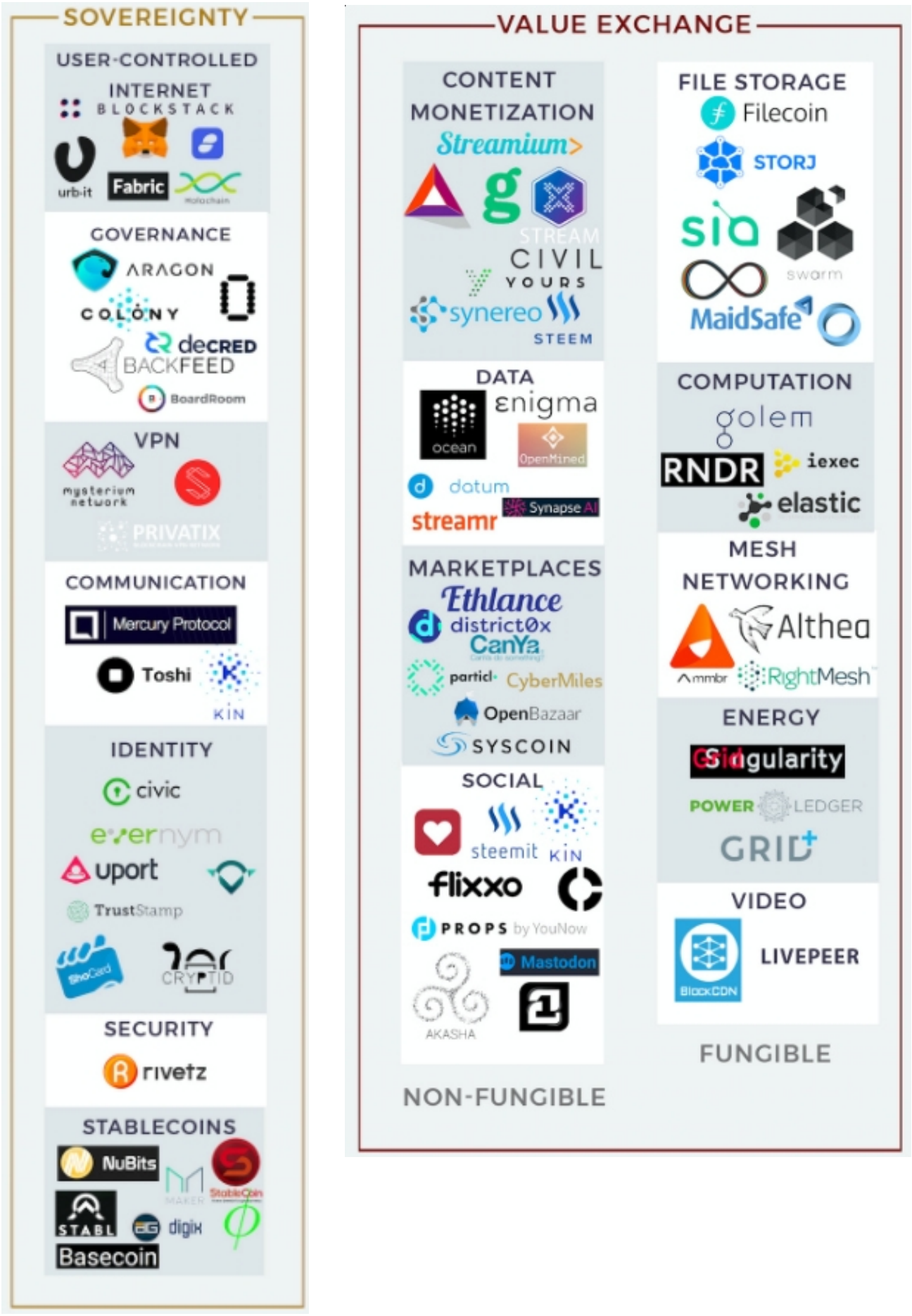



Top 10 countries for blockchain startups.
Number of Startups
0
50
100
150
200
250
300
350
United States
United Kingdom
Singapore
Switzerland
Canada
China
Australia
Germany
Israel
The Netherlands
Total Funding (USD)
$0 B
$1 B
$2 B
$3 B
$4 B
$5 B
United States
China
Switzerland
Singapore
Vietnam
United Kingdom
Canada
Hong Kong
Israel
Australia

2018

Blockchain Projects Ecosystem in 2018


FINTECH
TRADING/DEX
0x
omise
Bancor
AIRSWAP
Counterparty
bitShares
raidEX
EverMarkets
kyber. network
EtherDelta
INSURANCE
INSUREX
ai gang
ChainThat
Blockchain Innovation
ETHERISC
LENDING
SALT
MICRO MONEY
ripio
dharma
WeTrust
ETHLend
FUNDS/INVESTMENT MANAGEMENT
NUMERAI
ICONOMI
CINDICATOR
BLOCKCHAIN CAPITAL
DEVELOPER TOOLS
SMART CONTRACTS
EOS
LISK
ethereum
NEO
RSK
BOScoin
SCALING
TrueBit
RAIDEN
LIGHTNING NETWORK
PLASMA
ORACLES
oraclize
SECURITY
ZEPPELIN
Gladius
LEGAL
CODELEGIT
AGRELLO
COALA IP
INTEROPERABILITY
Polkadot
COSMOS
BTC RELAY
AION
OpenZeppelin
Simple Token
PRIVACY
NUCYPHER
ROCKCHAIN
DAGs
Byteball
IOTA


SOVEREIGNTY
USER-CONTROLLED
INTERNET
BLOCKSTACK
urb-it
Fabric
GOVERNANCE
ARAGON
COLONY
decRED
BACKFEED
BoardRoom
VPN
mysterium network
PRIVATIX
COMMUNICATION
Mercury Protocol
Toshi
KIN
IDENTITY
civic
evernym
uport
TrustStamp
CRYPTID
SECURITY
rivetz
STABLECOINS
NuBits
StableCoin
STABL
digix
Basecoin
VALUE EXCHANGE
CONTENT MONETIZATION
Streamium
STREAM
CIVIL
YOURS
synereo
STEEM
DATA
ocean
enigma
OpenMined
datum
streamr
Synapse AI
MARKETPLACES
Ethlance
district0x
CanYa
particl
CyberMiles
OpenBazaar
SYSCOIN
SOCIAL
steemit
KIN
flixxo
PROPS by YouNow
Mastodon
AKASHA
NON-FUNGIBLE
FILE STORAGE
Filecoin
STORJ
sia
swarm
MaidSafe
COMPUTATION
golem
RNDR
iexec
elastic
MESH NETWORKING
Althea
Ammbr
RightMesh
ENERGY
Singularity
POWER LEDGER
GRID+
VIDEO
BlockCDN
LIVEPEER
FUNGIBLE

SHARED DATA

INTERNET OF THINGS

FOAM
IOTA
OAKEN INNOVATIONS
SIKORKA
ethereum meets the great outdoors

SUPPLY CHAIN/LOGISTICS

T-MINING BLOCKCHAIN LOGISTICS
walton
Kouvola.innovation
Sweetbridge
MONAX
origintrail

ATTRIBUTION

ujo
po.et
JAAK
MYCELIA
POEX.IO

REPUTATION

ink
bitconnect
Bloom
monetha

CONTENT CURATION

userfeeds
CURATION MARKETS

AUTHENTICITY

DATA

FACTOM
TIERION

TICKETING

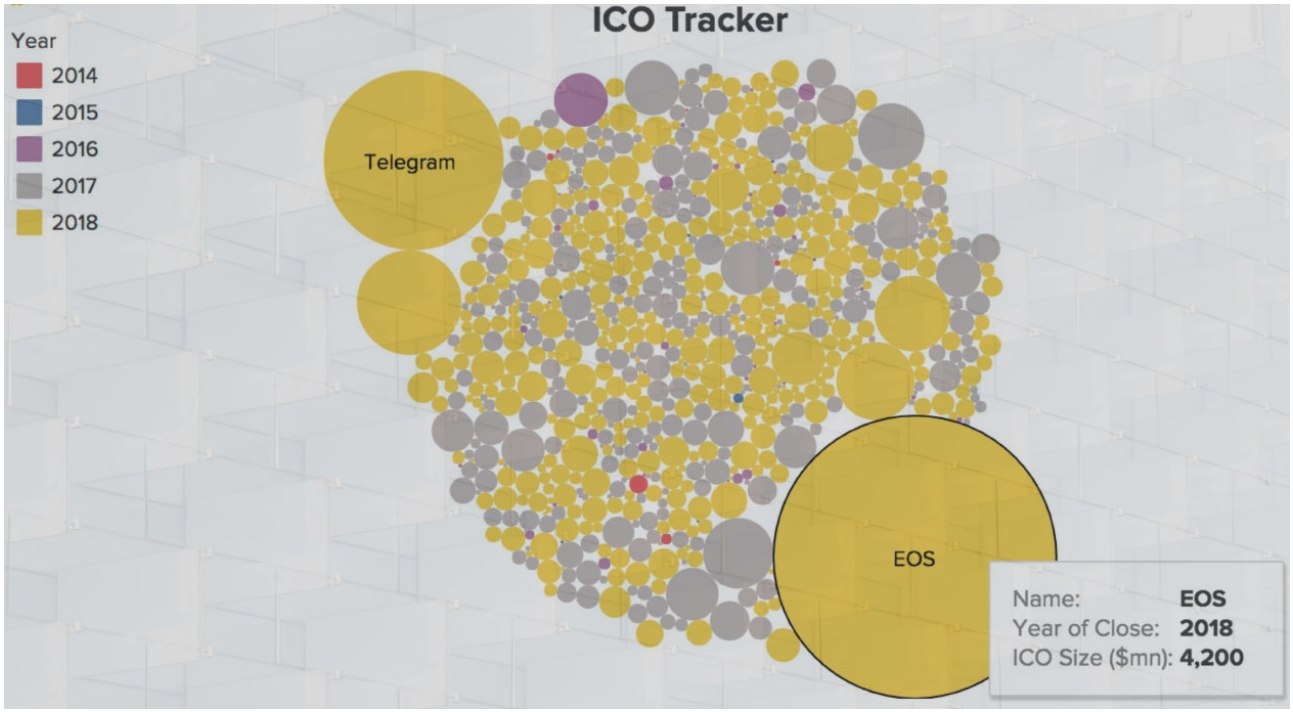
GUTS
aventus
BT BLOCKTIX
TicketChain

Blockchain Project Funding in 2018

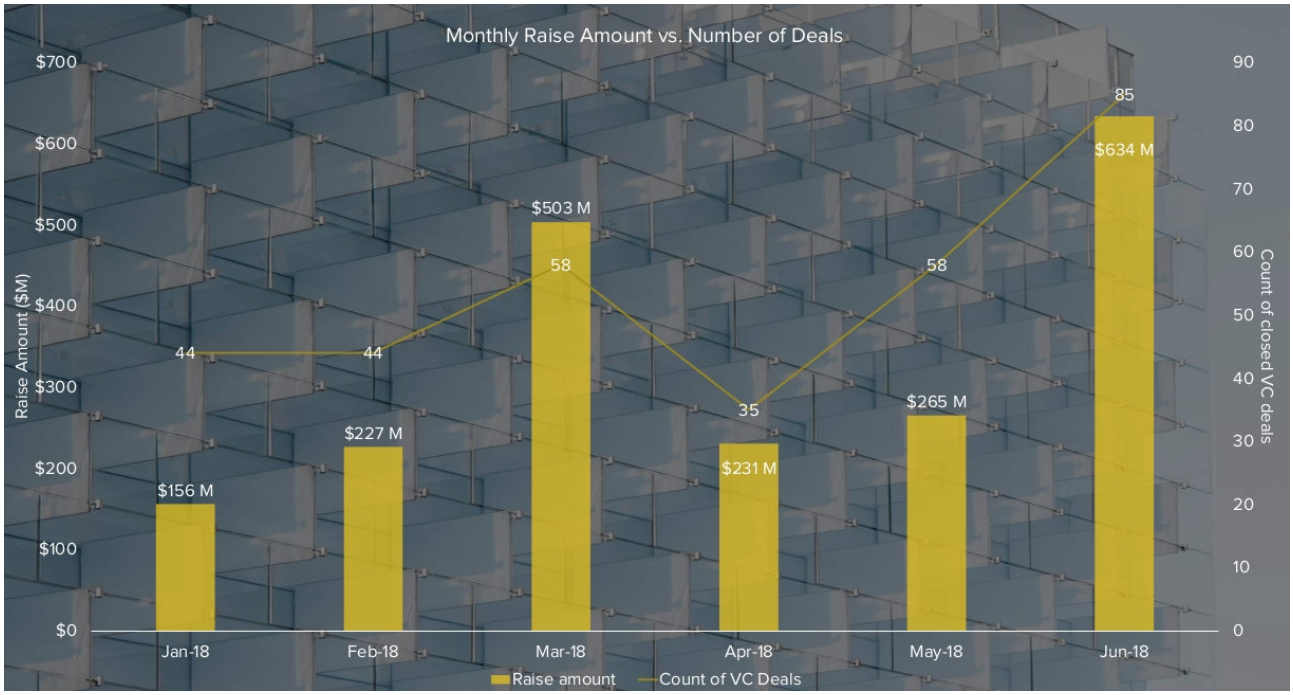
ICO (Initial Coin Offering) is a type of funding using cryptocurrencies.
It is mostly done by crowdfunding, but private ICO's are becoming more common.
In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" ("coins") to speculators or investors, in exchange for legal tender or other cryptocurrencies.
The tokens sold are promoted as future functional units of currency when the ICO's funding goal is met and the project launches.

An ICO can be a source of capital for startups, which allows them to avoid regulatory compliance and intermediaries such as venture capitalists, banks and stock exchanges. ICOs may fall outside of existing regulations, depending on the nature of the project, or be banned altogether in some jurisdictions.

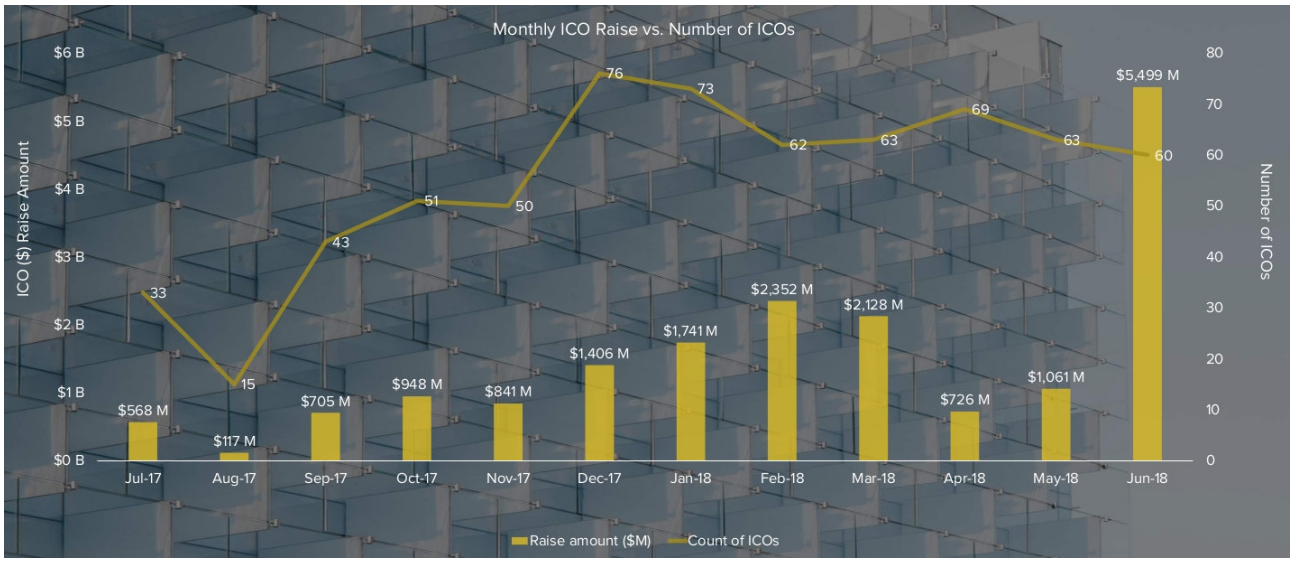
ICOs have been prone to scams and securities law violations.
Despite this, a record $7 billion was raised via ICOs in the first half of 2018.



Venture Capital



ICO



Blockchain in Telecom, 2018

Sim-card will be replaced by software. Phone can switch networks depending on price and available capacity on a minute-by-minute basis, creating a more efficient market.
Consequences:

- Telecom loses its last contact point with the end-user.
- "Virtual" providers go out of business, being outcompeted by Apple, Samsung, etc.
- Network providers see their profits dwindle in a more efficient market dominated by a few professional customers.

Telecom industry is already responding by diversifying into new revenue sources.
This is where blockchain will emerge - not as a disruptor, but as a response to the disruption already on the horizon. It is just one of many tools that telecom could employ.
Blockchain would allow IoT devices to both perform transactions and to be tracked.

Uses of blockchain in Telecom:

- Phones roaming on different networks can be seen as "micro contracts". Roaming and autonomous brokering of prices will happen much more and be machine-to-machine. Blockchain could be essential when Apple and Samsung's smart agents negotiate with network providers in real-time.

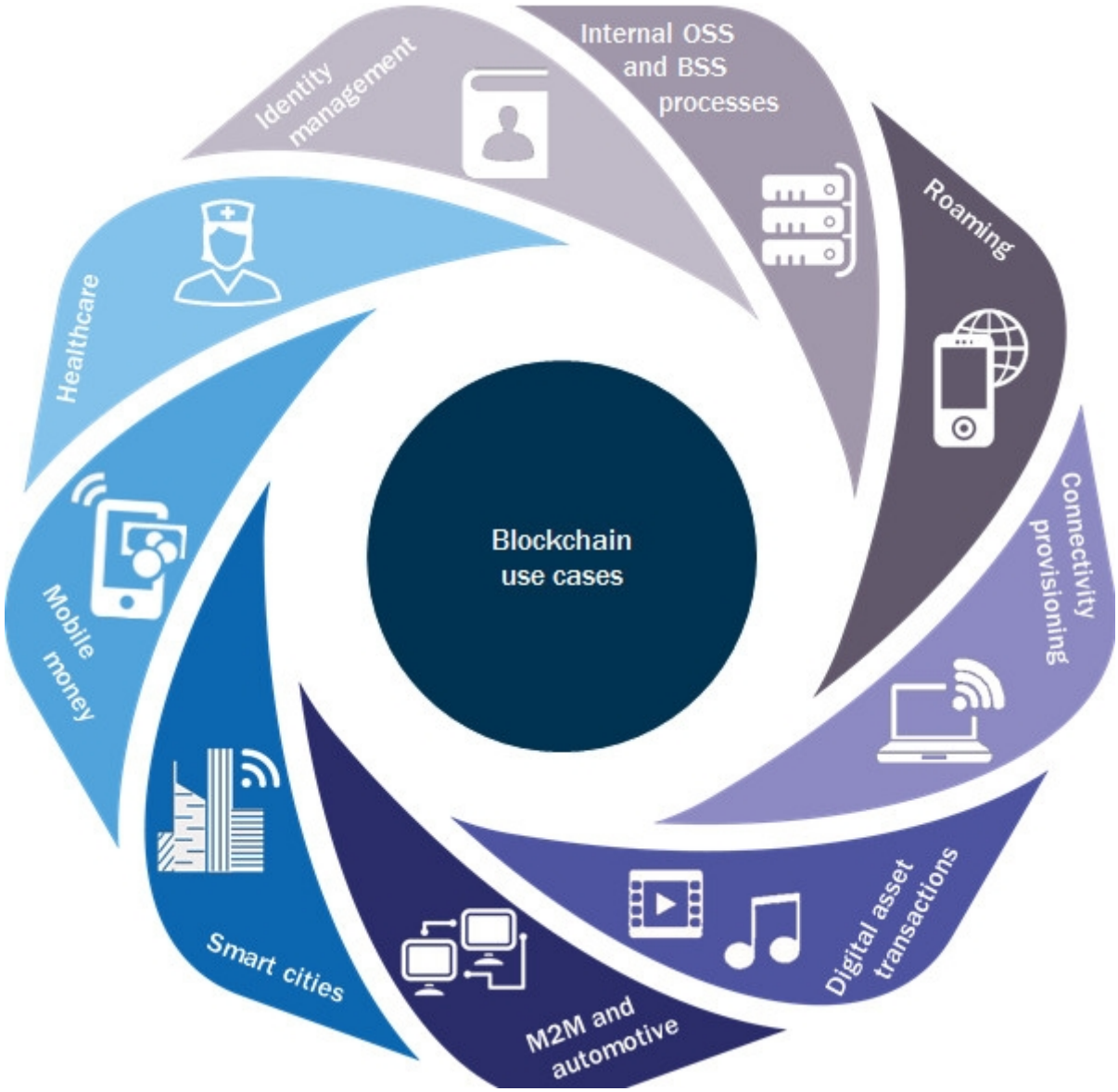
  Roaming agreements as micro-contracts are blockchain's obvious disruption of telecom. But this cannot happen without the network provider being in on it. It is uneconomical for a new "disruptive" provider to set up their own cellphone towers, installation costs being high and frequencies occupied.

  This is why blockchain-use will be a telecom innovation, not a telecom disruption. The "revolution" will not start until we see sim-free phones.

- Blockchain could provide immediate authentication of people and devices. This puts blockchain-wielding telecom providers in the place of authentication providers for all kinds of third-party services. Today's smartphone apps that unlock hotel doors, pay your bus fare and authenticate you toward your bank is just the beginning.

- Telecom industry and phone manufacturers already want micro-transactions and payment, as seen in many payment solutions for smartphones. Blockchain, as a verifyer of transactions, may be a key to let telecom providers disrupt banks.

Blockchain use cases in Telecom



Streamlining internal processes, including interactions with suppliers and other CSPs

Resulting in

- lower costs
- faster throughput
- improved experiences

for all players

Developing services for customers built on blockchain

Services to support e.g.

- identity management
- mobile money
- digital assets transactions

Collaborating in business ecosystems – including the IoT

Providing in ecosystems

- trust
- security
- transparency

for all transactions