An Introduction to Blockchain Technology

Ramesh Ramadoss, PhD
Co-chair, IEEE Blockchain Initiative

April 28, 2022

IEEE BLOCKCHAIN™

https://blockchain.ieee.org/

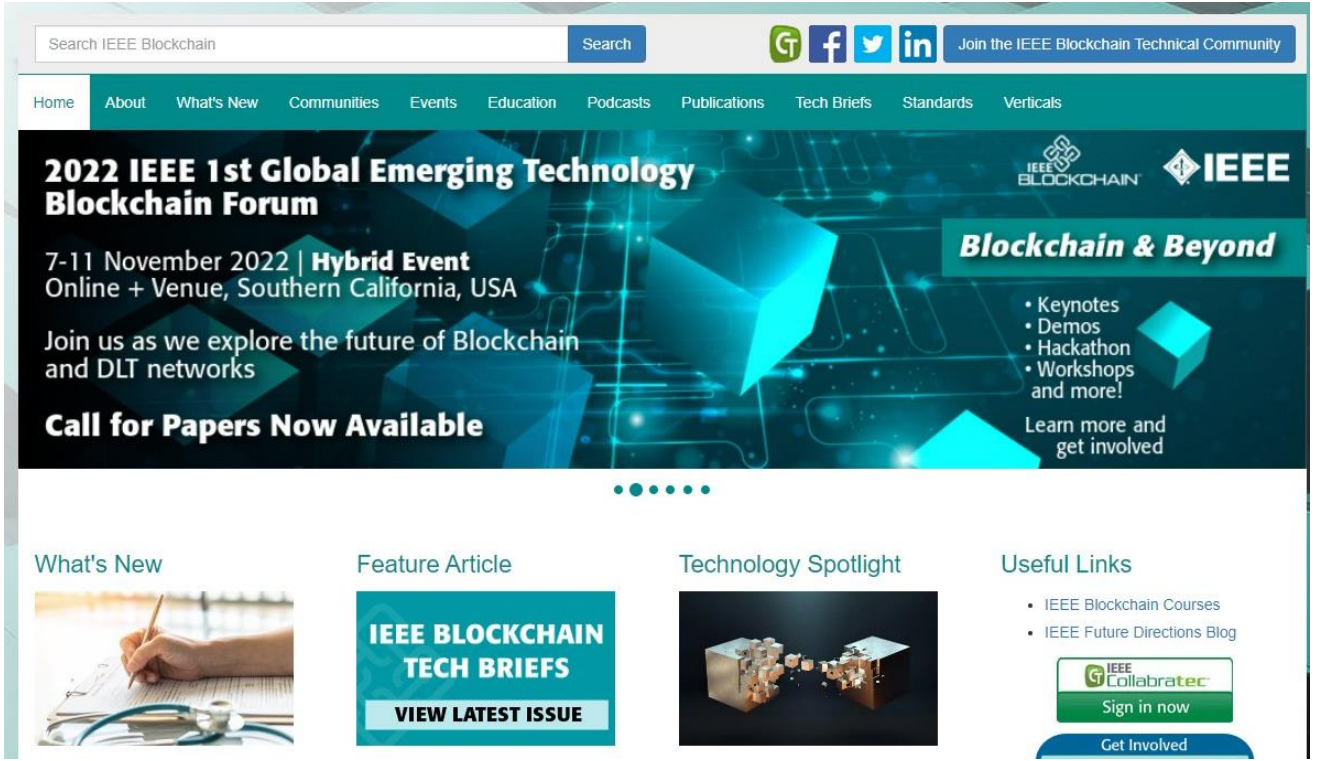
IEEE Advancing Technology for Humanity

IEEE Blockchain Initiative

https://get.blockchain.ieee.org/

IEEE BLOCKCHAIN™

https://blockchain.ieee.org/



IEEE

Community Development - Blockchain Local Groups

Americas:
IEEE Boston Blockchain Group
IEEE North-Central Brazil Blockchain Group
IEEE Cleveland Blockchain Group
IEEE Dallas Blockchain Group
IEEE Denver Blockchain Group
IEEE Kitchener-Waterloo Blockchain Group
IEEE Coastal Los Angeles Blockchain Group
IEEE Memphis Blockchain Group
IEEE New York Blockchain Group
IEEE Orlando Blockchain Group
IEEE Puerto Rico & Caribbean Group
IEEE San Diego Blockchain Group
IEEE Seattle Blockchain Group
IEEE Silicon Valley Blockchain Group
IEEE Toronto Blockchain Group

Europe:
IEEE Benelux Blockchain Group
IEEE Estonia Blockchain Group
IEEE France Blockchain Group
IEEE Italy Blockchain Group
IEEE Latvia Blockchain Group
IEEE Luxembourg Blockchain Group
IEEE Portugal Blockchain Group
IEEE Romania Blockchain Group
IEEE Spain Blockchain Group
IEEE Switzerland Decentralised Systems
IEEE Ukraine Blockchain Group
IEEE UK & Ireland Blockchain Group

Africa
IEEE Morocco Blockchain Group
IEEE Nigeria Blockchain Group
IEEE Tunisia Blockchain Group

Middle East
IEEE Dubai Blockchain Group
IEEE Egypt Blockchain Group
IEEE Israel Blockchain Group
IEEE Kuwait Blockchain Group
IEEE Oman Blockchain Group
IEEE Qatar Blockchain Group
IEEE Turkey Blockchain Group

Asia-Pacific:
IEEE Bangalore Blockchain Group
IEEE Beijing Blockchain Group
IEEE Gujarat Blockchain Group
IEEE Hangzhou Blockchain Group
IEEE Hong Kong Blockchain Group
IEEE Indonesia Blockchain Group
IEEE Japan Blockchain Group
IEEE Macau/Guangzhou Blockchain Group
IEEE Malaysia Blockchain Group
IEEE Shanghai Blockchain Group
IEEE Shenzhen Blockchain Group
IEEE Singapore Blockchain Group
IEEE South Korea Blockchain Group
IEEE Victorian Blockchain Group

Blockchain Standards Working Groups

See https://blockchain.ieee.org/standards

Horizontal Topics: Data, Interoperability, Governance, Identity, Smart Contracts etc.
Vertical Topics: Energy, IoT, Healthcare, FinTech, Cryptocurrency, Digital Asset etc.

IEEE Industry Connections Program: 6

Standards Under Development: 49

Approved/Published Standards: 9

2140.1-2020 - IEEE Standard for General Requirements for Cryptocurrency Exchanges
2140.2-2021 - IEEE Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges
2140.5-2020 - IEEE Standard for a Custodian Framework of Cryptocurrency
2142.1-2021 - IEEE Approved Draft Recommended Practice for E-Invoice Business Using Blockchain Technology
2143.1-2020 - IEEE Standard for General Process of Cryptocurrency Payment
2144.1-2020 - IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management
2418.2-2020 - IEEE Approved Draft Standard Data Format for Blockchain Systems
2418.7-2021 - IEEE Standard for the Use of Blockchain in Supply Chain Finance
2418.10 - IEEE Approved Draft Standard for Blockchain-based Digital Asset Management

Project: Blockchain Transactive Energy (BCTE)

https://blockchain.ieee.org/verticals

BCTE Committee:

- Claudio Lima, PhD, BEC
- Farrokh Rahimi, PhD, OATI
- Hunter Albright, PhD, Curve10
- Paul Heitman, Businovation

BCTE Activities:

- Position Paper
- Workshops at PES GM and CIGRE
- 5 Demonstrations Selected for POCs
- Architecture documentation in draft

Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

Digital Cash/Money/Currency

Digital cash (money or currency) refers to any means of payment that exists purely in electronic form.

Digital cash does not have a physical and tangible form, such as a dollar bill or a coin.

Digital cash is accounted for and transferred using computer systems.

Since the late 1980's, there have been several attempts to create digital cash.

Several Attempts:
1989: DigiCash by David Chaum
1996: E-Gold by Gold & Silver Reserve
1997: HashCash by Adam Back
1998: B-Money by Wei Dai (Theoretical)
2005: Bit Gold by Nick Szabo (Theoretical)
2008: Bitcoin by Satoshi Nakamoto (More on Next Slide)

Bitcoin – A Peer-to-Peer Digital Cash

Bitcoin is the first successful digital cash deployed on a peer-to-peer computer network.

- Oct 2008: Satoshi Nakamoto (An anonymous person) published the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System".

- Jan 2009: The bitcoin software was launched, and the first "Genesis Block" was mined.

Bitcoin is a recipe based on several key ideas developed in the fields of cryptography, consensus protocols, and peer-to-peer networks.

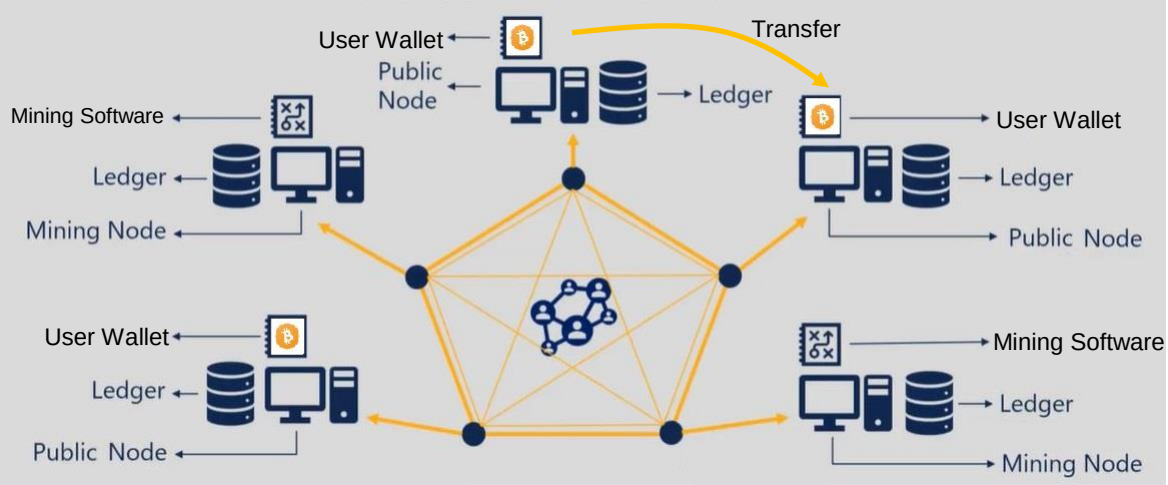
Key Ideas/Ingredients

1976: Public-key cryptography (Whitfield Diffie and Martin Hellman)
1979: Merkle Trees (Ralph C. Merkle)
1991: Time-Stamp (Stuart Haber and W. Scott Stornetta)
1997: Proof-of-Work Algorithm / HashCash (Adam Back)
2001: Secure Hash Algorithm 2 (SHA-2) (NSA)

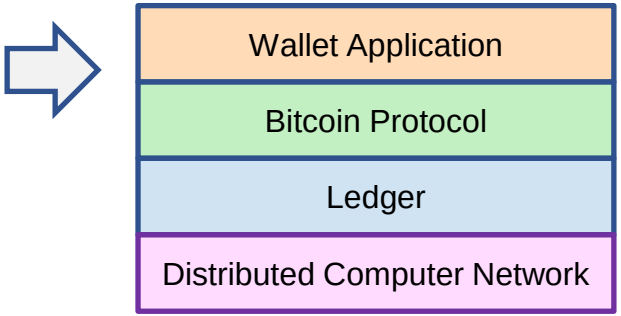
Bitcoin Architecture

Bitcoin is a software that runs on a peer-to-peer computer network and consists of the following components:
- Ledger
- Protocol (Proof-of-Work)
- Wallet

Bitcoin: An Electronic Cash on a Peer-to-Peer Network



Bitcoin Architecture



Bitcoin Fundamentals – Account & Keys

Account: An account is an asymmetric key pair (public key and private key).

- Private Key is kept secret by the owner/entity.
- Public Key can be made available to anyone.
- An account address is generated from the public key.

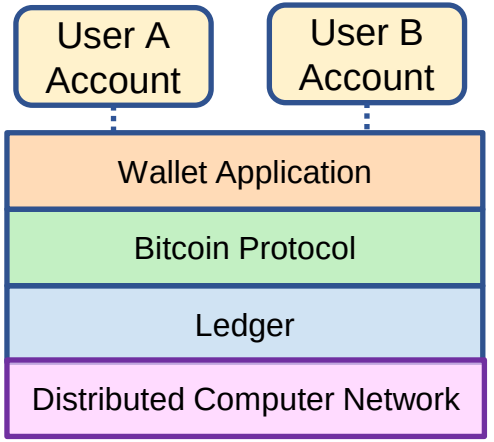
Bitcoin Example: Keys & Account Address (Hexadecimal)

Private Key
6JCG34xv2a040op1BfSwPicBNUNCuk9Ht1qWMgWoMJWJpownAAi

Public Key
0798694TR67C50Z680FVRD54SX9L833137Y30K70062CCEF18L5213I9R471P0107

Bitcoin Address
1E1144JY6R7TCmj3BGzjpofqf9EqP9vLKJm

Bitcoin Architecture



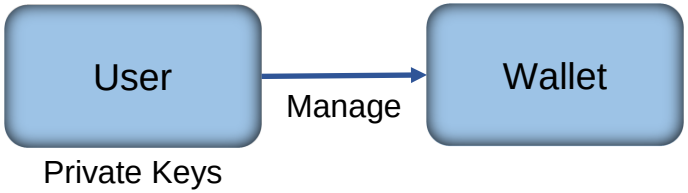
IEEE

Bitcoin Fundamentals – Wallet

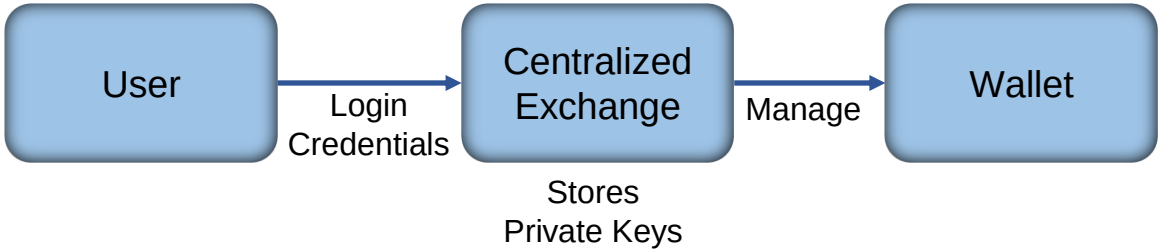
Wallet: An application used to generate, manage, and store private and public keys.

Wallet Custody Type:

Non-Custodial Wallet: Users are in complete control of their private keys and manage their wallet (e.g., MetaMask, Trust, Atomic)

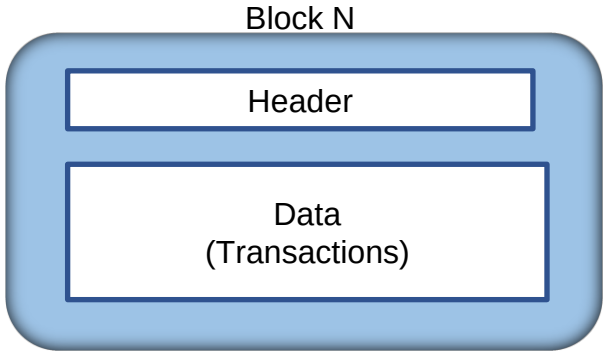


Custodial Wallet: A trusted entity (e.g., a centralized exchanges) stores users' private keys and manages their wallet.



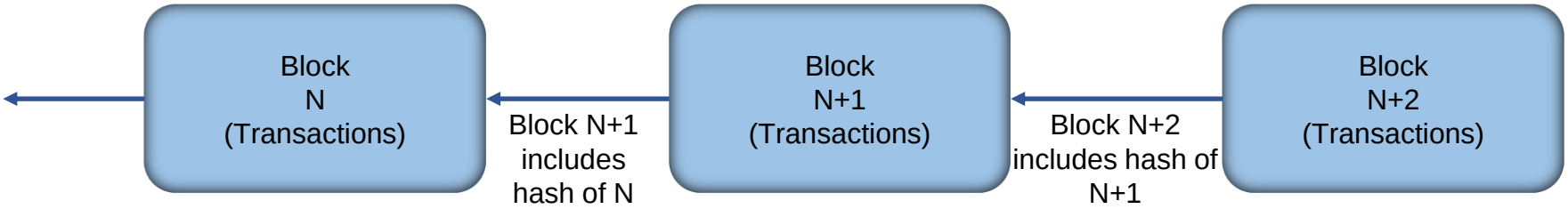
IEEE

Bitcoin Fundamentals - Ledger



Block: A block is a data structure comprising
- a block header, and
- block data (a batch of transactions).

Ledger: A chain of blocks is called a ledger or blockchain. Each block is cryptographically linked (thru hashing) to the previous block.
- Append-only
- Immutable



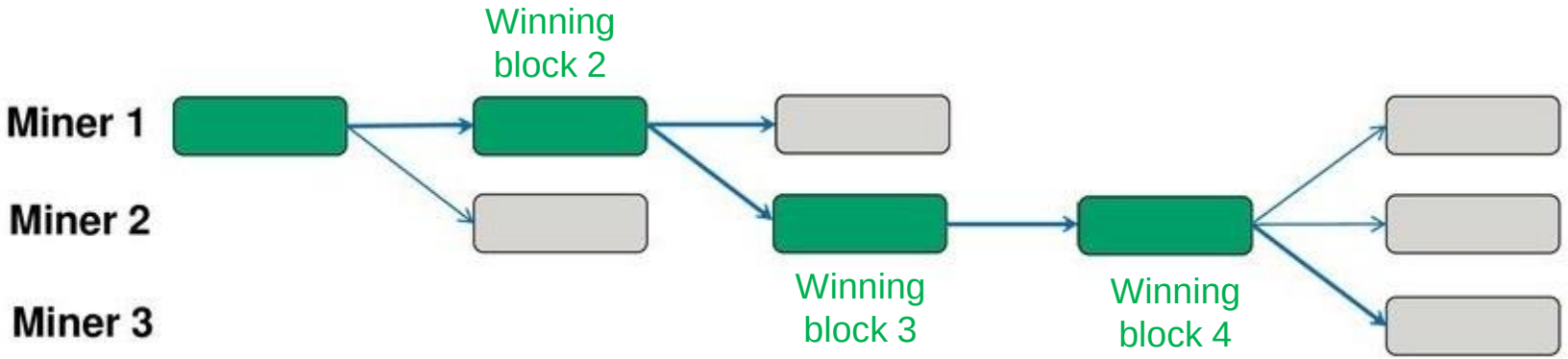
Visual Demo: https://andersbrownworth.com/blockchain/

Bitcoin Fundamentals – Protocol (Proof-of-Work Algorithm)

New Block: A new block (containing new transactions) is added to the blockchain every 10 minutes. Miners propose new blocks and compete to earn the reward.

Proof-of-Work: The competition involves solving a mathematical puzzle using the Proof-of-Work algorithm

Reward: The miner who proposed a winning block receives rewards (new coins + transaction fees).



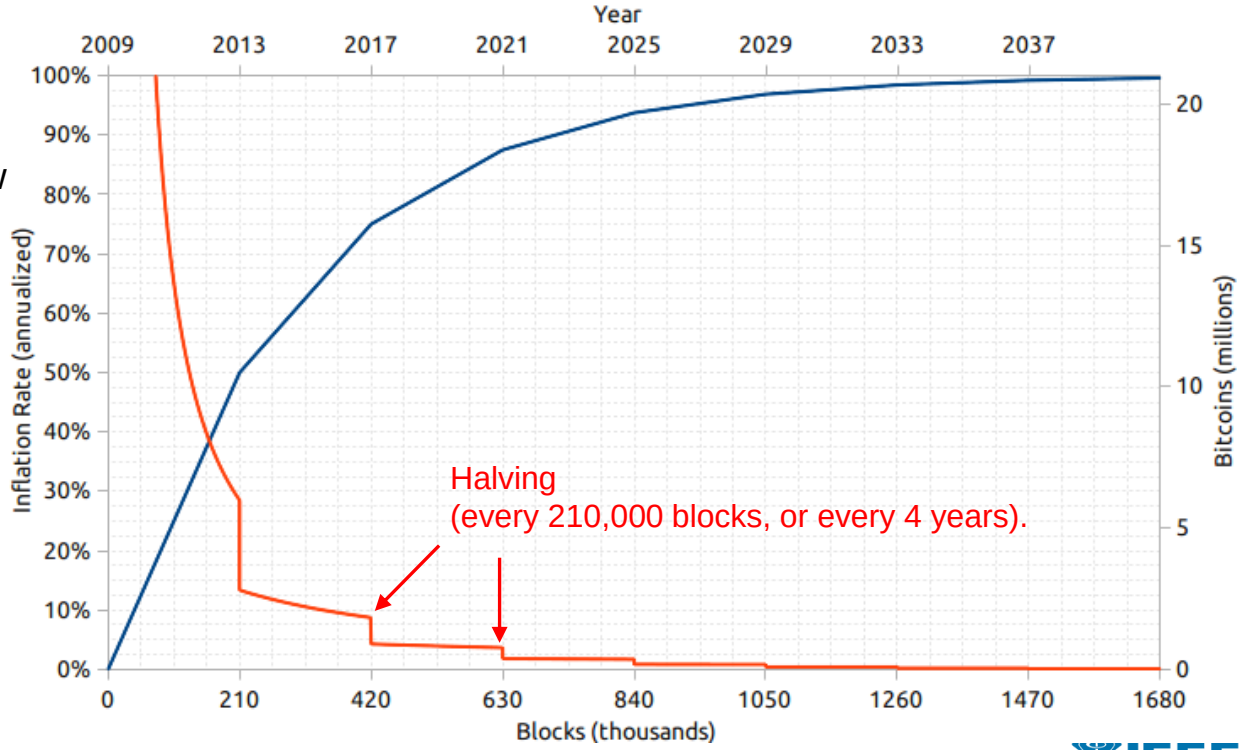
Longest Chain: The longest chain becomes the valid chain and miners work on adding new blocks to it.

Bitcoin – Supply and Mining

The total supply of BTC is limited and pre-defined in the Bitcoin protocol at 21 million.

How are new bitcoins created?
Mining is the process by which new bitcoin is added to the circulating supply.

The mining reward decreases over time (halving every 210,000 blocks or approx. every 4 years).

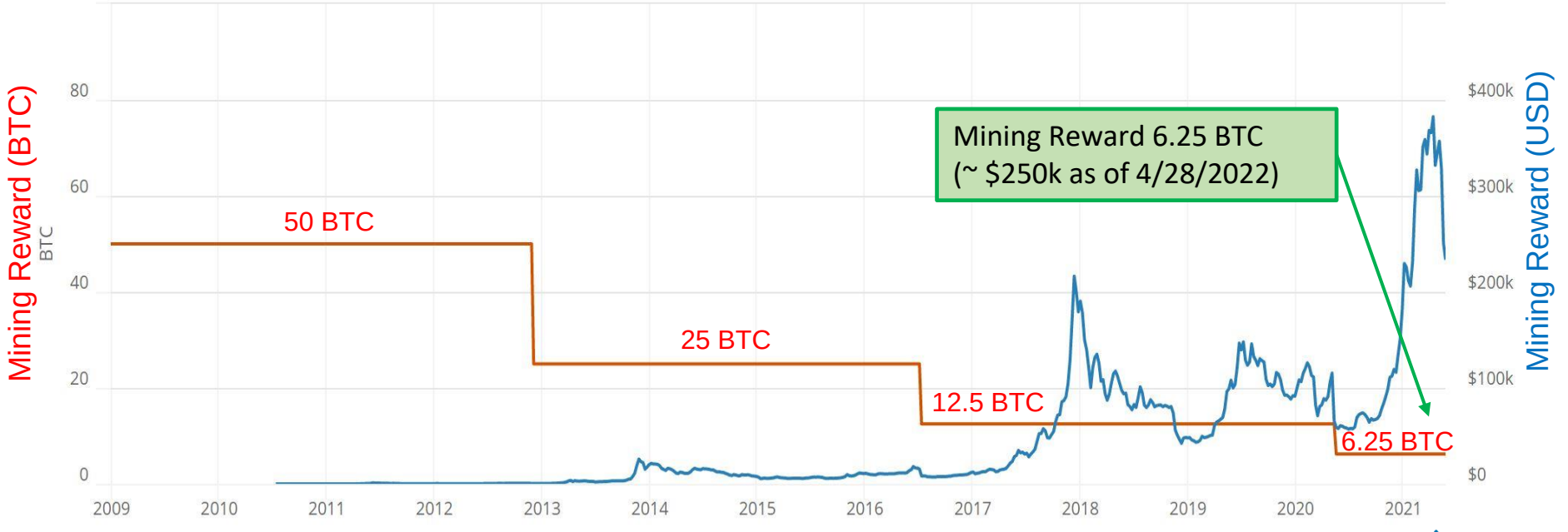


Source: https://www.bitcoinblockhalf.com/

Bitcoin – Mining Reward

Mining reward started at 50 BTC and halves continually every halving event until it reaches 0 (approx. by 2140).

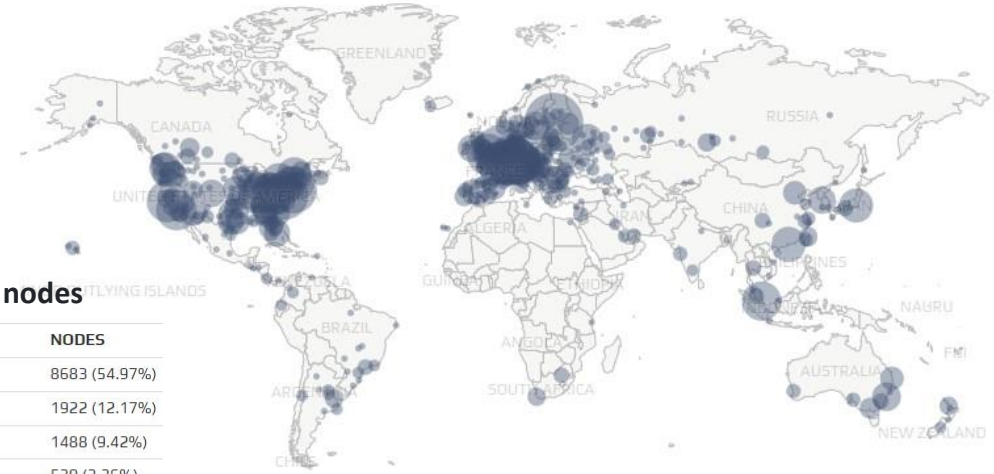
Currently, the mining reward is 6.25 BTC for adding a winning block.



Bitcoin – Mining Pools

Mining pools (centralized computing warehouses) located in parts of the world with low-cost electricity have emerged as new businesses.

Bitcoin Node Distribution (As of 4/28/22)



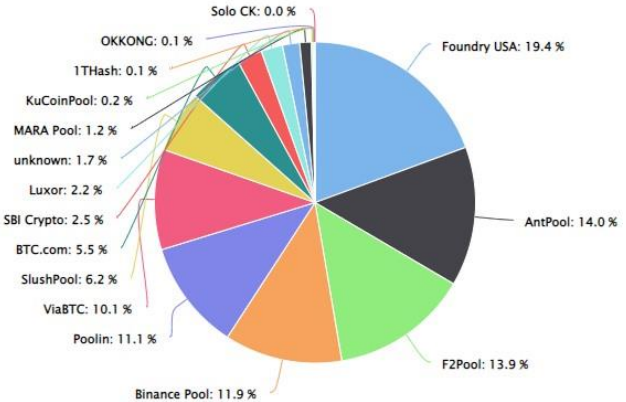
15796 nodes

RANK	COUNTRY	NODES
1	n/a	8683 (54.97%)
2	United States	1922 (12.17%)
3	Germany	1488 (9.42%)
4	France	530 (3.36%)
5	Netherlands	348 (2.20%)
6	Canada	304 (1.92%)
7	Russian Federation	226 (1.43%)
8	Finland	225 (1.42%)
9	United Kingdom	222 (1.41%)
10	Switzerland	128 (0.81%)

Source: https://bitnodes.io

Bitmain Mining Warehouse (IEEE Spectrum)

Mining Pools (30 days)

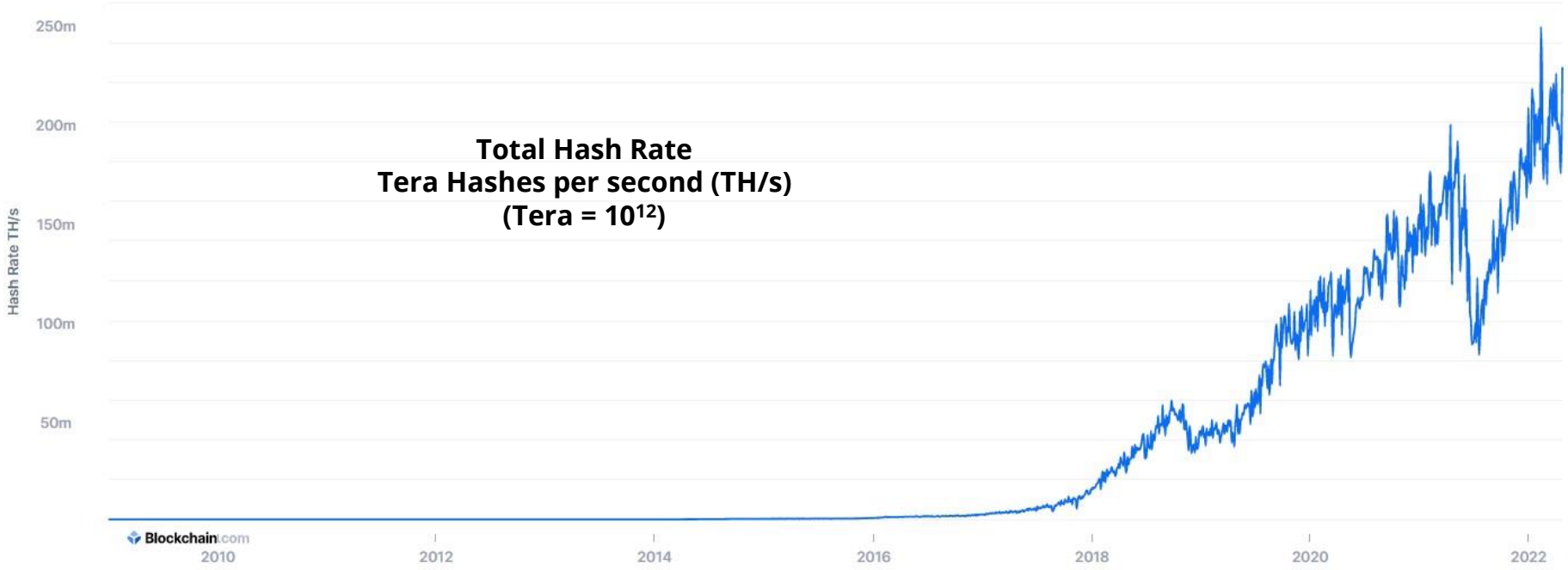


https://btc.com/stats/pool

IEEE

Bitcoin – Hashrate

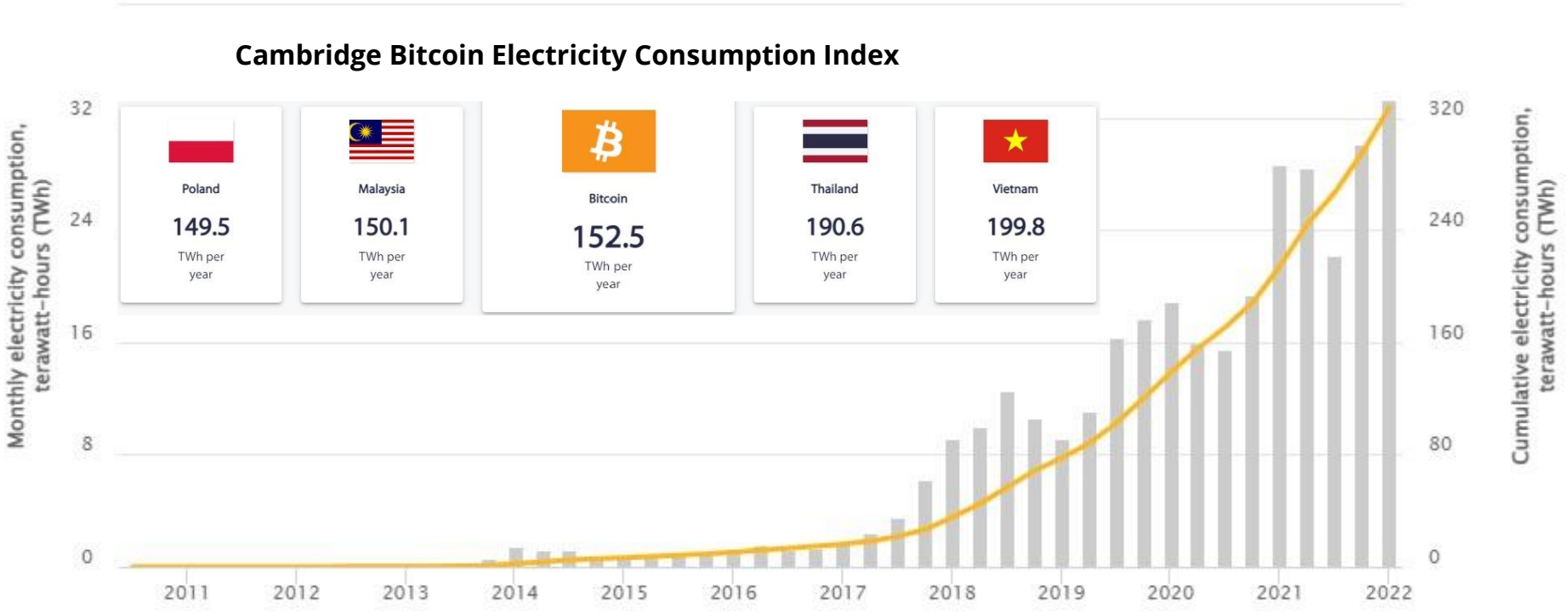
Hashrate refers to the number of total calculations per second needed to mine a new block.



https://www.blockchain.com/charts/hash-rate

Bitcoin – Energy Consumption (Proof-of-Work Computation)

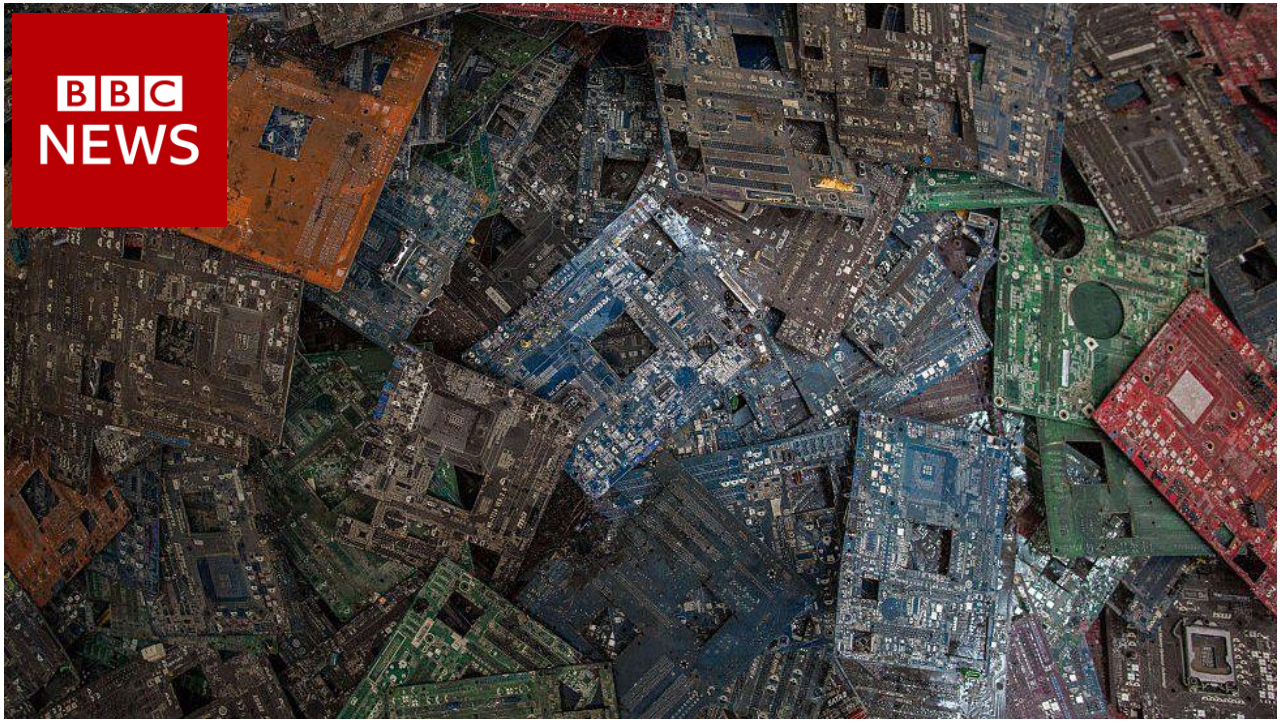
The annual energy consumption of bitcoin has exceeded that of some countries.



https://ccaf.io/cbeci/index

Bitcoin – Environmental Impact (E-Waste)

Bitcoin mining produces electronic waste (e-waste) annually comparable to the small IT equipment waste of a place like the Netherlands.



Further Reading:

de Vries, Alex. "Renewable energy will not solve bitcoin's sustainability problem." Joule 3.4 (2019): 893-898.

IEEE

Bitcoin Drawbacks!

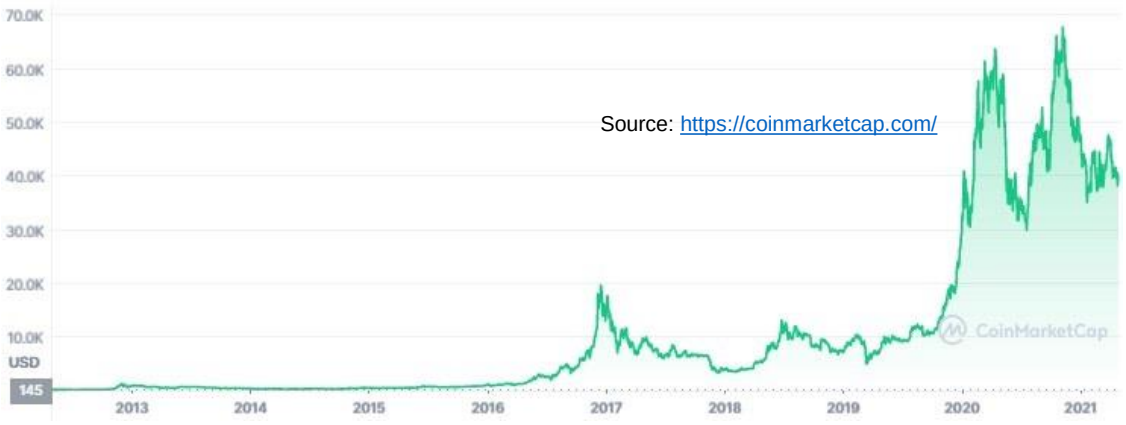
The original idea of Bitcoin was to serve as Digital Cash on a decentralized peer-to-peer network.

However, some of the drawbacks include:

1) Highly volatile: Bitcoin has become a highly speculative digital asset and not stable like cash.

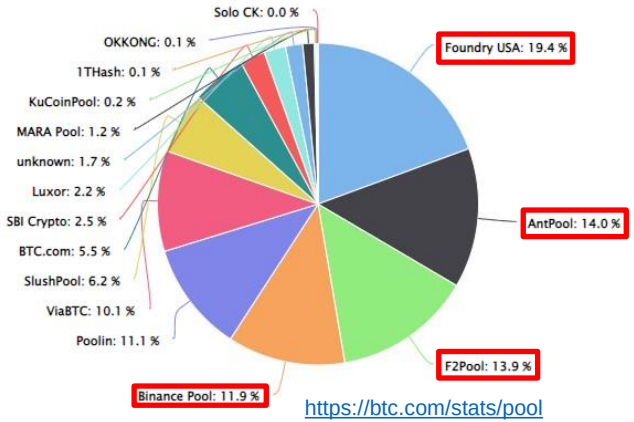
2) Centralized mining pools: Initially peer-to-peer but overtime bitcoin has come under the control of mining pools.

3) High energy consumption: POW algorithm based mining.

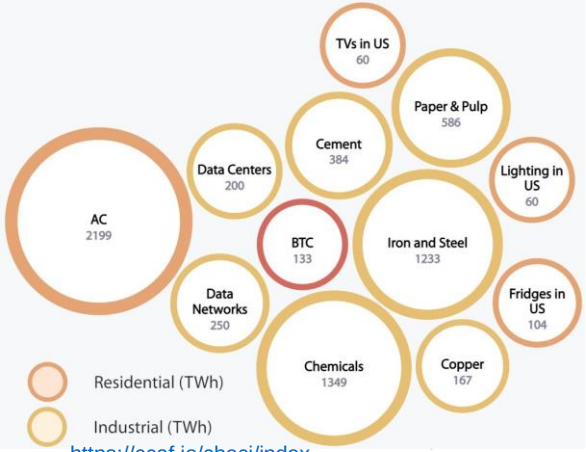


Source: https://coinmarketcap.com/

Top 4 mining pools ~ 59%

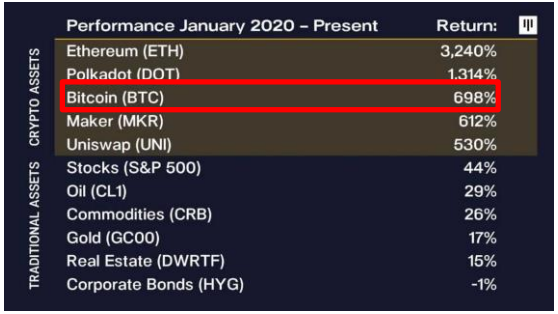


https://btc.com/stats/pool



https://ccaf.io/cbeci/index

Bitcoin – Digital Asset!



	Performance January 2020 – Present	Return:
CRYPTO ASSETS	Ethereum (ETH)	3,240%
	Polkadot (DOT)	1,314%
	Bitcoin (BTC)	698%
	Maker (MKR)	612%
	Uniswap (UNI)	530%
TRADITIONAL ASSETS	Stocks (S&P 500)	44%
	Oil (CL1)	29%
	Commodities (CRB)	26%
	Gold (GC00)	17%
	Real Estate (DWRTF)	15%
	Corporate Bonds (HYG)	-1%

Join TechCrunch+

Fidelity says it will offer crypto in retirement accounts this year

Anita Ramaswamy @anitaramaswamy / 12:09 PM GMT-4 • April 26, 2022

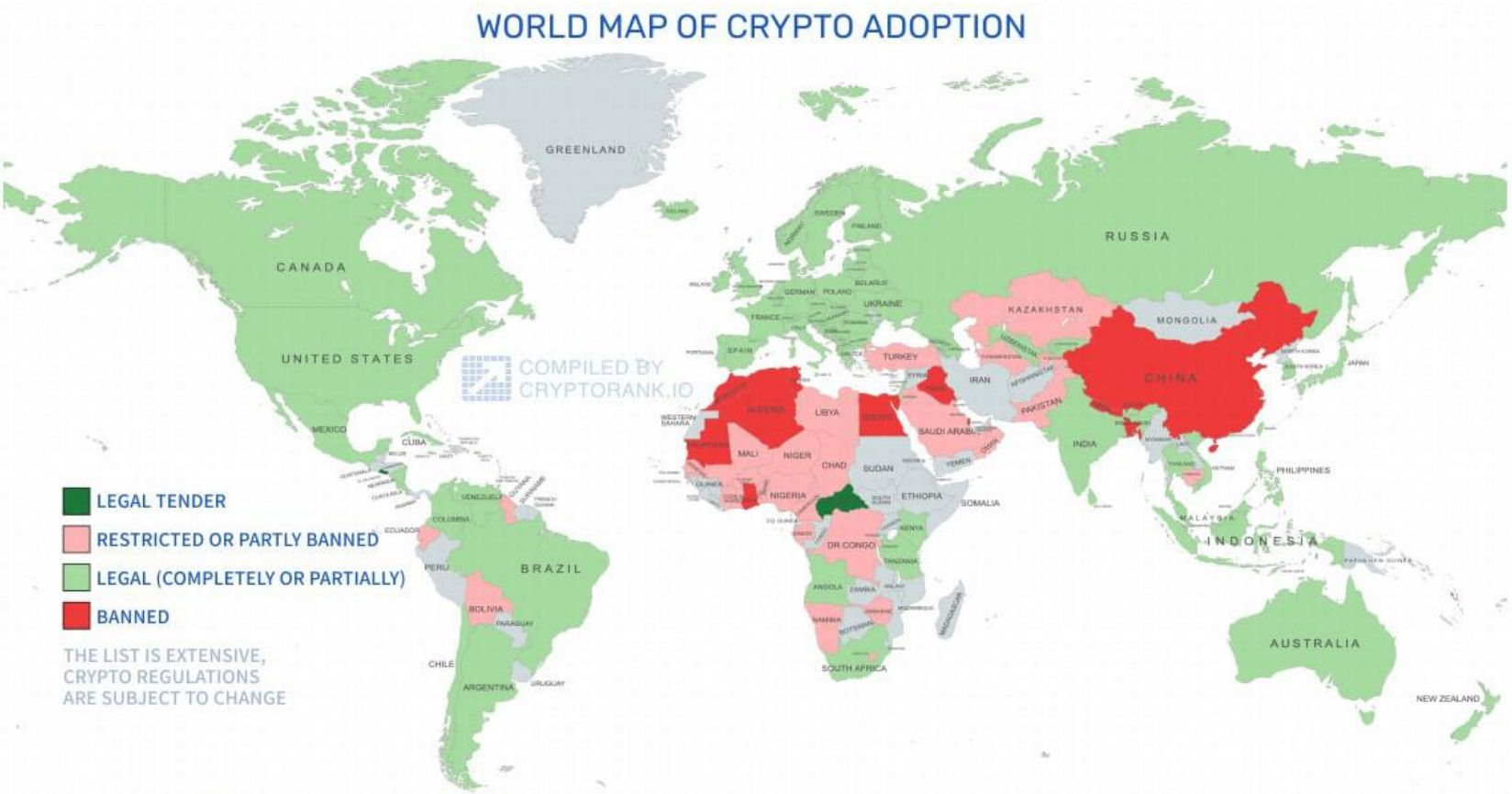
Fidelity, the largest retirement plan provider in the United States, announced plans to offer bitcoin in 401(k) retirement accounts to its account holders later this year. The company is set to allow investors to allocate up to 20% of their 401(k) accounts to bitcoin, though employers will have the ability to lower that cap, Dave Gray, head of workplace retirement offerings and platforms at the asset manager, told the Wall Street Journal.

The Boston-based asset manager, which administers plans covering more than 20 million participants representing $2.7 trillion in assets, said the launch is expected to take place by midyear, debuting at bitcoin supporter Michael Saylor's firm MicroStrategy, which holds billions of dollars of the asset on its balance sheet.

The offering, which Fidelity is calling its Digital Assets Account, will hold bitcoin and short-term money market investments to provide the liquidity investors would need to engage in daily transactions if they choose to do so. The currency will be held in custody with Fidelity Digital Assets to ensure "institutional-grade security," the company said.

IEEE

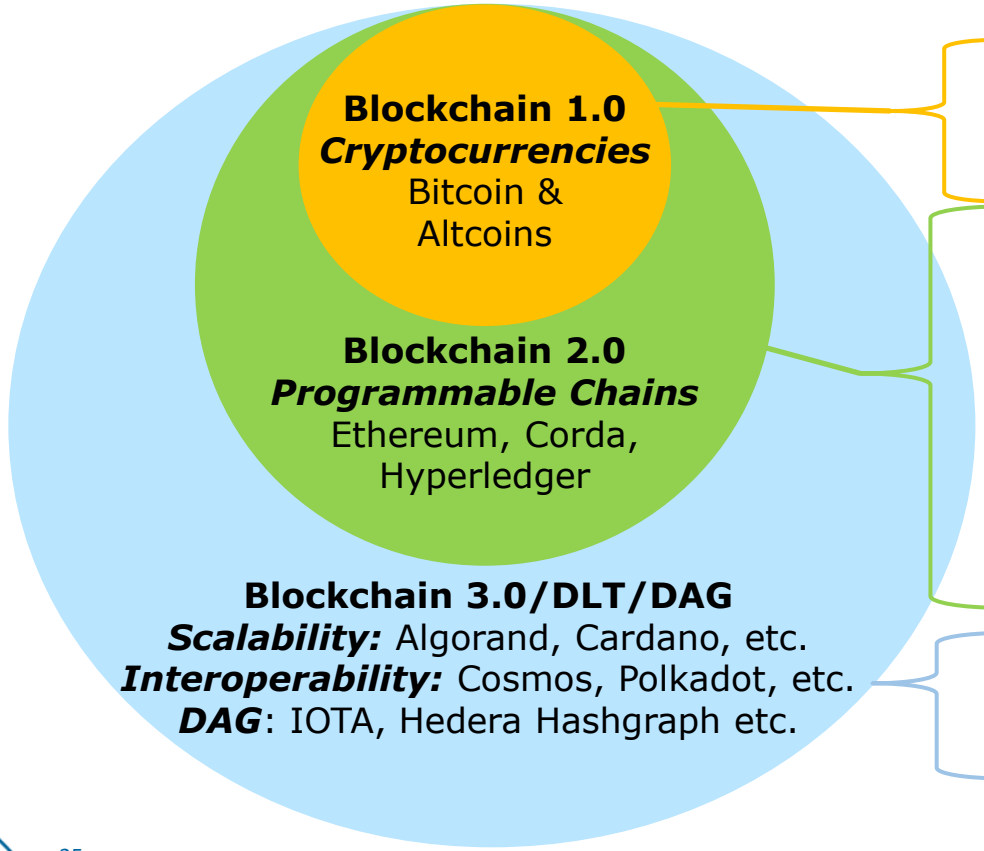
Bitcoin – Legal Status!



Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

Bitcoin/Blockchain/DLT/DAG - Evolution



Jan. 2009: Bitcoin was launched by Satoshi Nakamoto. Bitcoin inspired the launch of several Alternative Coins (AltCoins). The term cryptocurrency refers to a decentralized, digital currency running on a blockchain.

Late 2013: Vitalik Buterin conceived a platform for "Programmable Money" with smart contracts. Gavin Wood largely credited for the thinking behind making Ethereum the general-purpose computing platform. Ethereum (Frontier Version) went live on July 30, 2015.

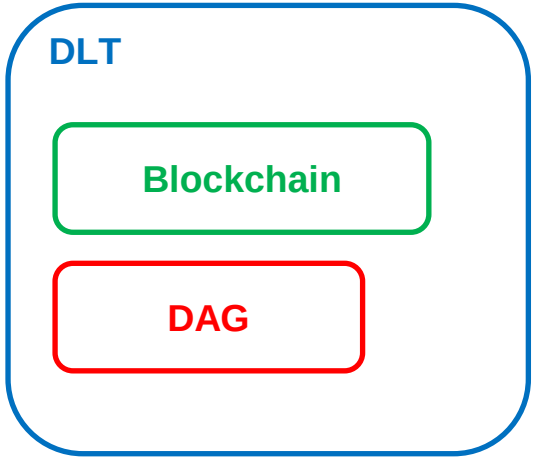
Sept. 2015: R3 was launched to develop Corda, an open-source blockchain platform, for the financial industries.

Dec. 2015: Linux Foundation announced the creation of the hyperledger project for building open-source business blockchain technologies.

Several other blockchains, Distributed Ledger Technology (DLT) and Directed Acyclic Graph (DAG) architectures were launched to address various limitations such as scalability, interoperability, energy efficiency etc.

[25] Blockchain 1.0 & 2.0 inspired by Melanie Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.

Blockchain vs DLT vs DAG



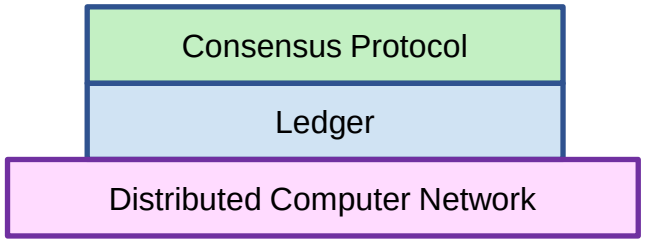
A distributed ledger technology (DLT) is an append-only transactions stored on a distributed computer network.

A blockchain (a sub-set of DLT) is a cryptographically secured chain of blocks. Each block consists of a batch of transactions.

A Directed Acyclic Graph (DAG) is a mathematically interconnected structure that consist of vertices and directed edges that never form a directed cycle. In the case of DAG based DLTs, the vertices often represent transactions (or blocks) and the edges represent "parent-child" references between the transactions (or blocks).

Blockchain/DLT Architecture

Blockchain/DLT Architecture

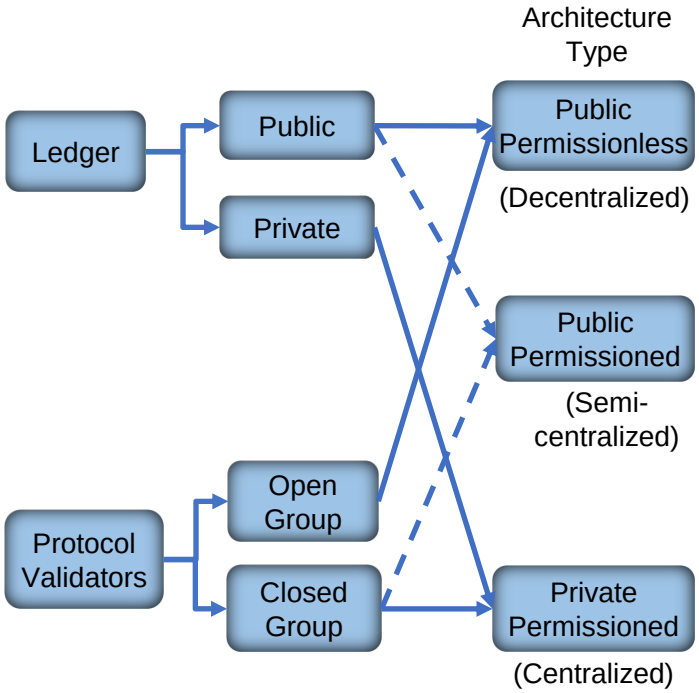


The consensus protocol defines the rules and parameters by which transactions are processed/approved by the validators in the network.

The ledger represents the conceptual layer where transactions are stored in the network.

A distributed computer network is a collection of autonomous computers (nodes) that appears to its users as a single coherent computer.

General Classification - Blockchain & DLT



Public-Permissionless Type: The ledger is visible to the public, and anyone can join the network. Also, the validators (Open Group) can be anyone on the network. These are fully decentralized architectures.

Public-Permissioned Type: The ledger is visible to the public. However, the validators (Closed Group) are selected by a governing body or a consensus algorithm. Typically, these are semi-centralized architectures.

Private-Permissioned Type: The ledger is private (visible to members only). The validators (Closed Group) are selected by a governing body. These are centralized architectures.

Decentralization – Consensus Algorithms & Validator Nodes

Public-Permissionless Type:
(Decentralized)

Public-Permissioned Type:
(Semi-Decentralized)

Public Blockchain	Consensus Algorithm	Validator/ Mining Nodes	Transaction per second (TPS)
Bitcoin	Proof-of-Work (PoW)	15796	10
Ethereum 1.0	Proof-of-Work (PoW)	6041	20
Solana	Byzantine Fault Tolerance (Tower Consensus)	200	65,000
EOS	Delegated POS	21	250

Private-Permissioned Type: Hyperledger Fabric, Corda
(Centralized)

Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

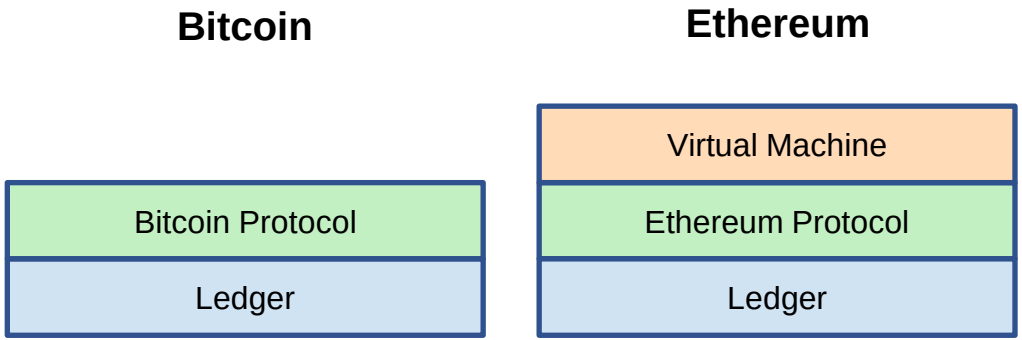
Ethereum Fundamentals – Virtual Machine

Ethereum is a programmable blockchain with an **Ethereum Virtual Machine (EVM)**.

The EVM is a global decentralized computer capable of executing computer instructions/code.

The EVM is a quasi-Turing-complete state machine.

Architecture Comparison

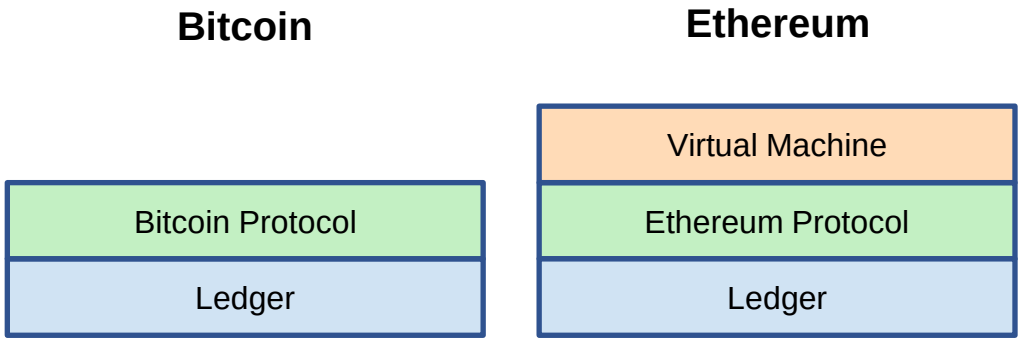


Ethereum Fundamentals - Smart Contracts

Smart Contract: A computer program that runs on (the virtual machine) a blockchain and the outcome of any execution of the program is recorded on the blockchain.

Ethereum: Smart Contracts can be programmed in Solidity, Java, Python etc.

Architecture Comparison



Ethereum Fundamentals - Native Asset

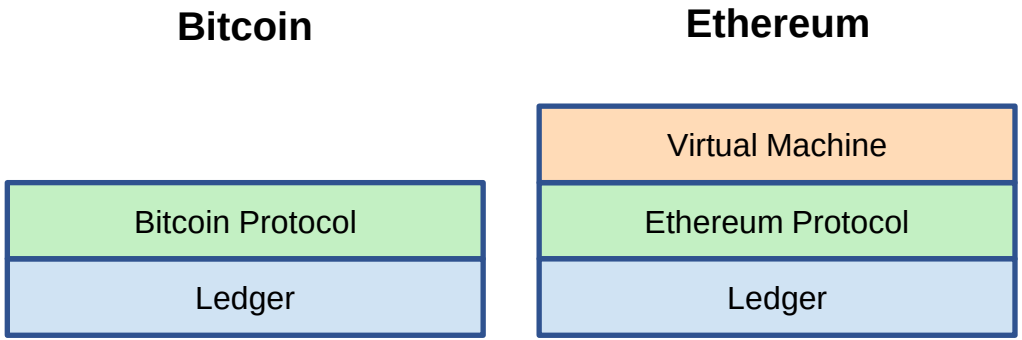
Native Asset: Cryptocurrency programmed at the protocol-level is the “Native Asset”, which is needed to execute transactions on the blockchain.

Transaction Fees:

Bitcoin Protocol: Bitcoin

Ethereum Protocol: Ether*
(*Gas fees paid to miners for validating transactions)

Architecture Comparison



Ethereum Fundamentals - Tokens

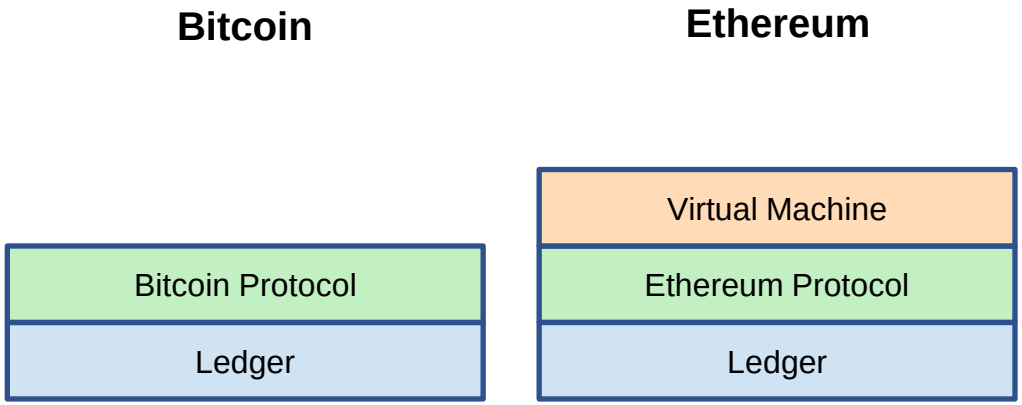
Tokens: A smart contract can be used to create a new type of Digital Asset called “Tokens”.

Token Types:

Fungible: interchangeable tokens (e.g., ERC-20 on Ethereum).

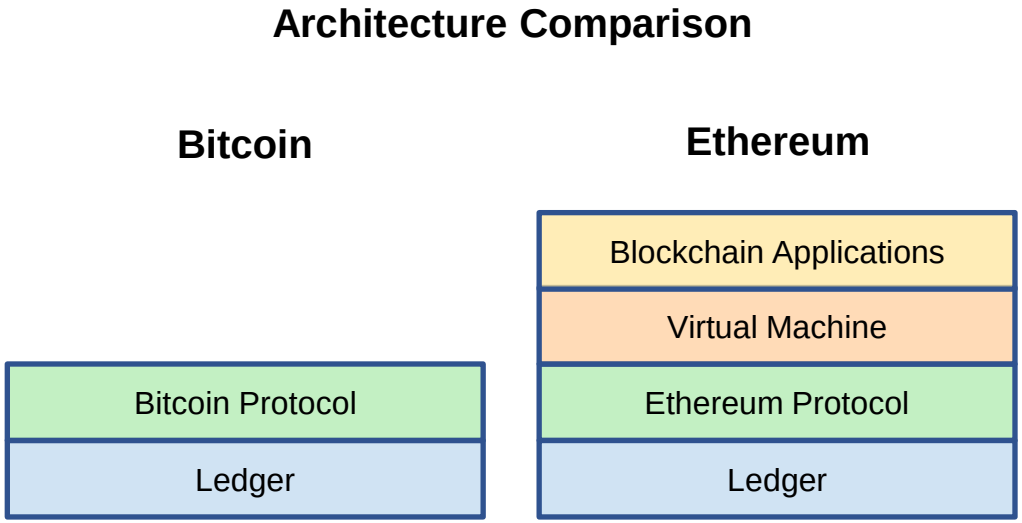
Non-Fungible: Unique and not interchangeable (e.g., ERC-721 on Ethereum).

Architecture Comparison



Ethereum Fundamentals - DApps

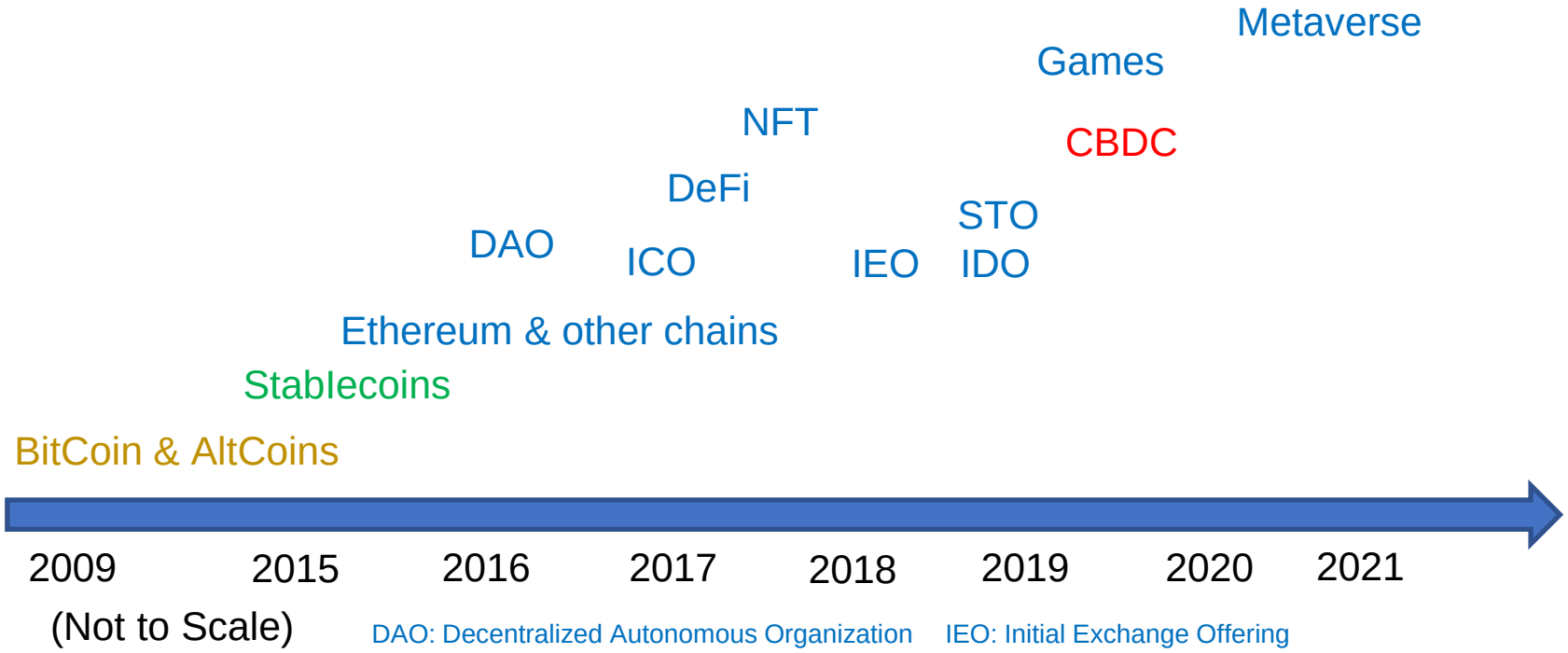
“DApps” are decentralized applications that involve one or more smart contracts and front-end components (Javascript, HTML, CSS).



Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

Cryptocurrencies/Digital Asset Evolution



DAO: Decentralized Autonomous Organization
NFT: Non-Fungible Token
DeFi: Decentralized Exchange
ICO: Initial Coin Offering

IEO: Initial Exchange Offering
IDO: Initial Decentralized Exchange Offering
STO: Security Token Offering
CBDC: Central Bank Digital Currency

IEEE

Cryptocurrency Ecosystem: Total Market Capitalization

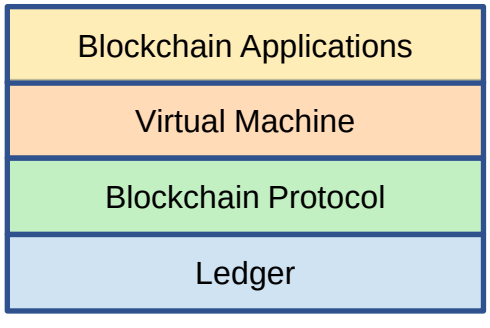
Cryptocurrencies (Coins & Tokens)

Apr 28, 2022
Cryptocurrencies: 19,182
Total Market Cap ~ $1.8 Trillion
(Bitcoin: 42%)

Source: CoinMarketCap

Blockchain Infrastructure

Blockchain Architecture

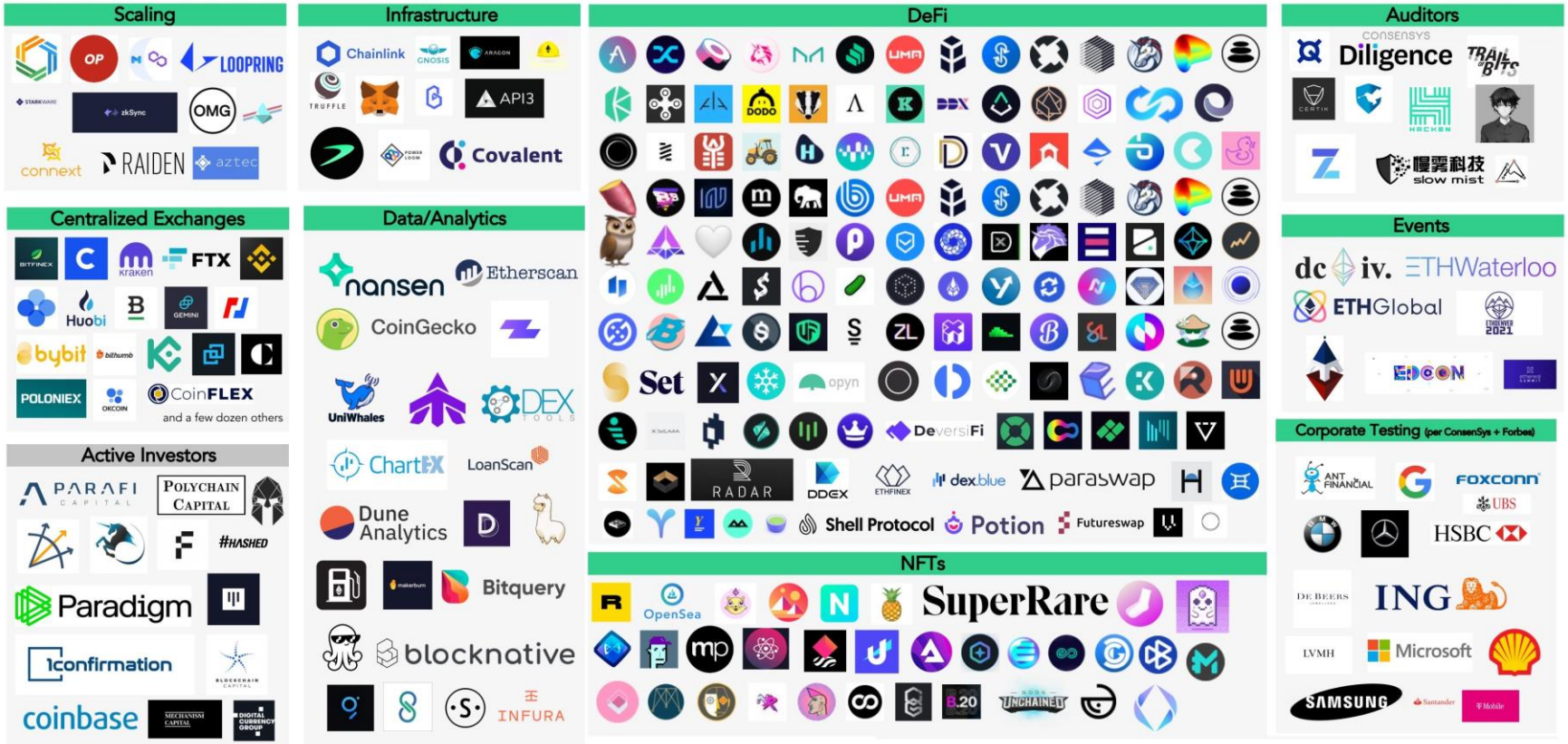


Infrastructure: Public Blockchains

Public-Permissionless Type: The ledger is visible to the public, and anyone can join the network. Also, the validators (Open Group) can be anyone on the network. These are fully decentralized architectures.

Public-Permissioned Type: The ledger is visible to the public. However, the validators (Closed Group) are selected by a governing body or a consensus algorithm. Typically, these are semi-centralized architectures.

Ethereum Blockchain Ecosystem



IEEE

SOLANA ECOSYSTEM

Wallet

Sollet.io
COIN98 WALLET
Trust Wallet
Math Wallet
Atomic Wallet
P2P Wallet
Ledger
EXODUS
swipe
Solflare
MOONLET
zelcore
Solong
Phantom
Blockfolio

Infrastructure

the graph
arweave
MERCURIAL FINANCE
Boring Protocol
Ren
Decentology
hummingbot
Wormhole
fantom
pocket
akash
Magic
Waves
TORUS
VELAS
MoonPay
BSN
parsiq
plasmafinance

Tooling + Explorer

Solana Beach
APE BOARD
MuDao
Sombra
Serum Pulse
SolanaProject
LIQ Protocol
SoproX
aleph.im
Sonar
Sollpay
SOLSCAN
SerumTaxTime
Cappuccino
Salty.ai
SOLANA
Solanascan
SolGSN
validators.app
DEFI COMPARE

Oracle

PYTH
Chainlink
Band Protocol
Switchboard
Gravity

Stablecoin

tether
Terra
USD Coin
UPFI Network
SOTERIA
BRZ TOKEN

DeFi

SERUM
RAYDIUM
COIN98 EXCHANGE
Luna Network
LIDO
Mango Markets
Hedgehog
cyclos
DEXLAB
BONFIDA
DOCE SWAP
Step
NERVE
Popsicle finance
SenSwap
IdentitySwap
RAMP DEFI
OXYGEN
SolFarm
CRYPTOPLEASE
solrise finance
Synthetify
Orca
HXRO
traderdome
PsyOptions
Particle Finance
YMaxDex
twirl finance
FRONTIER
Cappuu
Solaris
Aviata
BURNT FINANCE
Parrot
Saber
Solana Structured Products
Anchor
SOLEON
jet
SolAPE
DTFs Protocol
Apollo
Apricot Finance
DeFi Land
ZETA
Open Serum
Marinade
Solend
Port
LAGUNA
Francium
Slope
staking.io
FUTURE
SYMMETRY
LARIX
HAPI
SOLYARD
CropperFinance
HydraSwap
raydius
Everlend
Moët Finance
Zero Interest
Sendit
PLUTOS NETWORK

Application

Solstarter
コープ|COPE
MAPS.ME
GRAPE
AUDIUS
Solanium
KIN
LAVA
MetaSOL
Crowny
SOLCUBATOR
Polarity
Run Node
civic
Zoints
SOLPAD
HUMAN
SAMOYEDCOIN
Nina
dfuse
BocaChica
Satellite.im
Wum.bo
ROPE
The Media Network

Gaming/NFT

STAR ATLAS
All Art
Solarians
SOLV PROTOCOL
OpenEra
only¹
Kreechures
NFRACTION
AURORY
METAPLEX
SOL Survivor
SOLPUNKS
PROJECT SEED
Solible
Blockasset
SOLANIA
Metamarket
Scallop
Sollectify
KAIJU Cards
Uniforge
CLUB

SOLANIANS

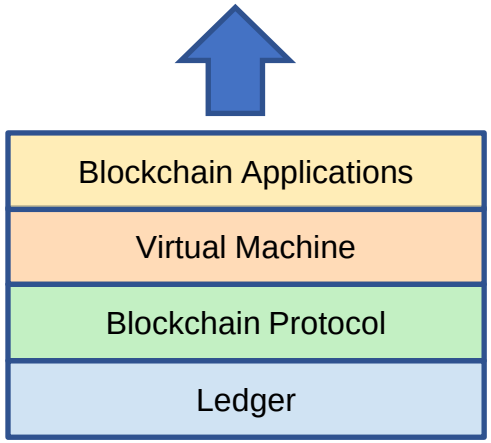
Updated: Jun 15th, 2021

@Solanians_

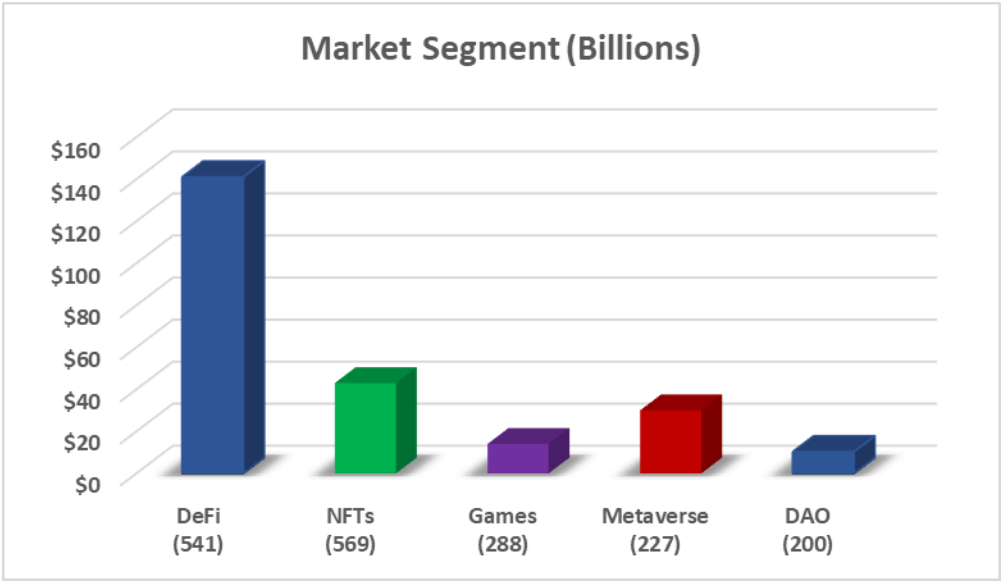
Decentralized Applications & Emerging Use Cases

Some applications and new uses enabled by the blockchain infrastructure include:

1) Decentralized Finance (DeFi)
2) Non-Fungible Tokens (NFTs)
3) Games (Play-to-Earn)
4) Metaverse



As of Apr 28, 2022



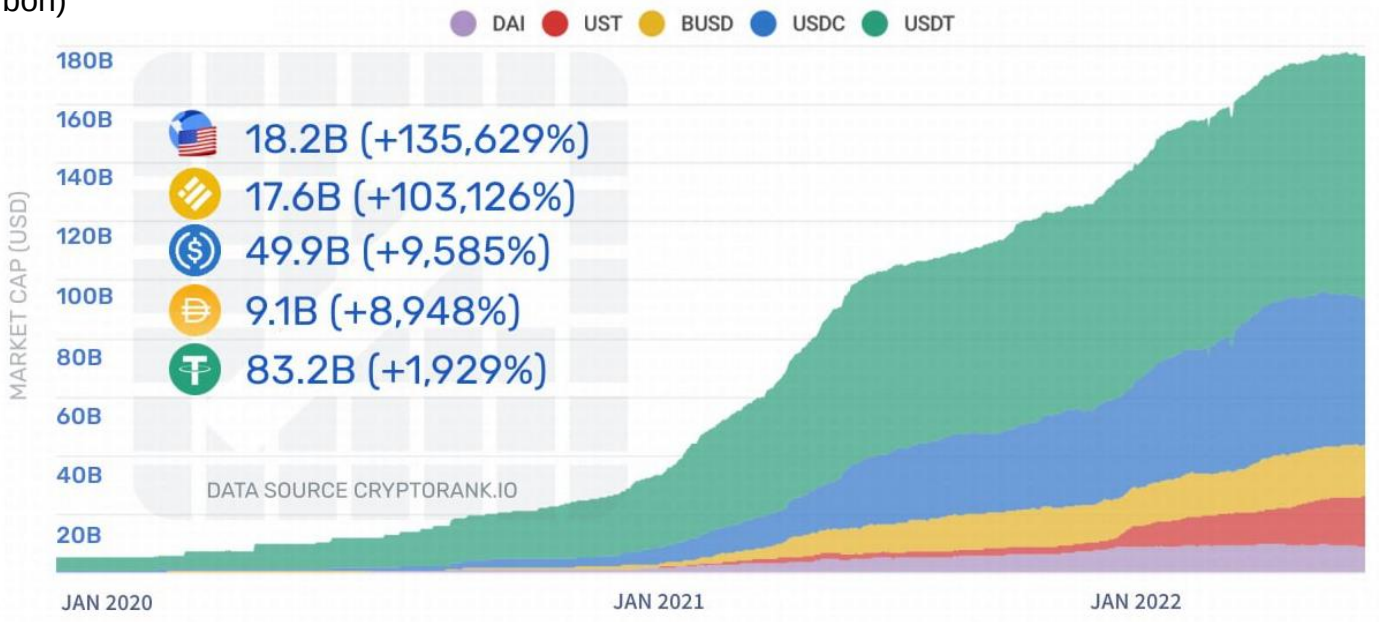
Source: https://coinmarketcap.com/

Stablecoins

Stablecoin is a type of cryptocurrency that has a stable price.

The value of a stable coin is pegged to a
- Fiat currency (e.g., US dollar backed USDC),
- Commodity (e.g., gold-backed Digix),
- Crypto (e.g., DAI by MakerDAO),
- Algorithmic supply (e.g., Carbon)

Total Market Cap ~ $180 Billion!

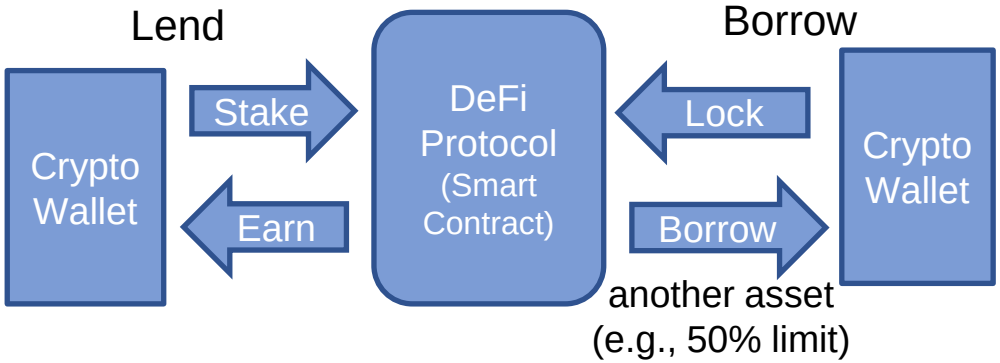


Decentralized Finance (DeFi)

Decentralized Finance (DeFi) is a peer-to-peer financial system that is built entirely on (public) blockchains.

Services similar to the legacy financial system (Exchange, Lending, Borrowing, Derivates etc.) are carried out using Crypto assets.

For example, you could get a loan on your crypto assets (or) you can receive interest income from your idle crypto assets.

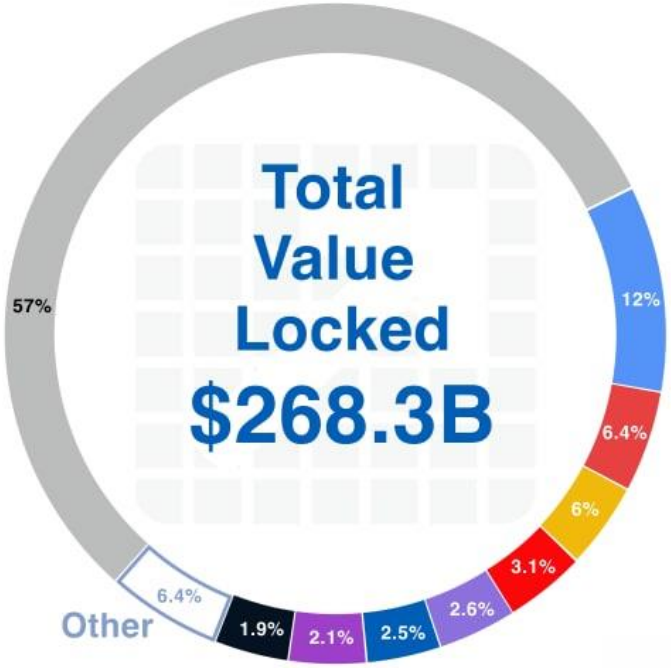


#	NAME	CHAIN	SECTOR	TVL (USD)
1	Maker	Ethereum	Lending	$14.52B
2	Aave	Multichain	Lending	$11.25B
3	Curve Finance	Ethereum	DEXes	$9.89B
4	Convex Finance	Ethereum	Assets	$9.83B
5	Uniswap	Ethereum	DEXes	$7.04B
6	Compound	Ethereum	Lending	$6.14B
7	InstaDApp	Ethereum	Lending	$4.61B
8	yearn.finance	Ethereum	Assets	$2.39B
9	Balancer	Ethereum	DEXes	$2.19B
10	Bancor	Ethereum	DEXes	$1.84B

Source: https://defipulse.com/

DEFI TOTAL VALUE LOCKED OVERVIEW

- Total value locked in decentralized finance increased by 20.7% in the last 30 days: $222.2B —> 268.3B



TVL IN DEFI FOR LAST YEAR

TVL ON MULTIPLE BLOCKCHAINS

Ethereum — TVL $153.7B
Market Cap $371B
Volume $16B

Terra — TVL $32.5B
Market Cap $33.3B
Volume $2.1B

Avalanche — TVL $17.3B
Market Cap $21B
Volume $589M

BNB — TVL $16.2B
Market Cap $70.3B
Volume $2.07B

Tron — TVL $8.38B
Market Cap $6.38B
Volume $961M

Solana — TVL $6.93B
Market Cap $35.3B
Volume $1.66B

Fantom — TVL $6.8B
Market Cap $2.99B
Volume $361M

Polygon — TVL $5.57B
Market Cap $11.1B
Volume $602M

Cronos — TVL $5.12B
Market Cap $10.6B
Volume $48M

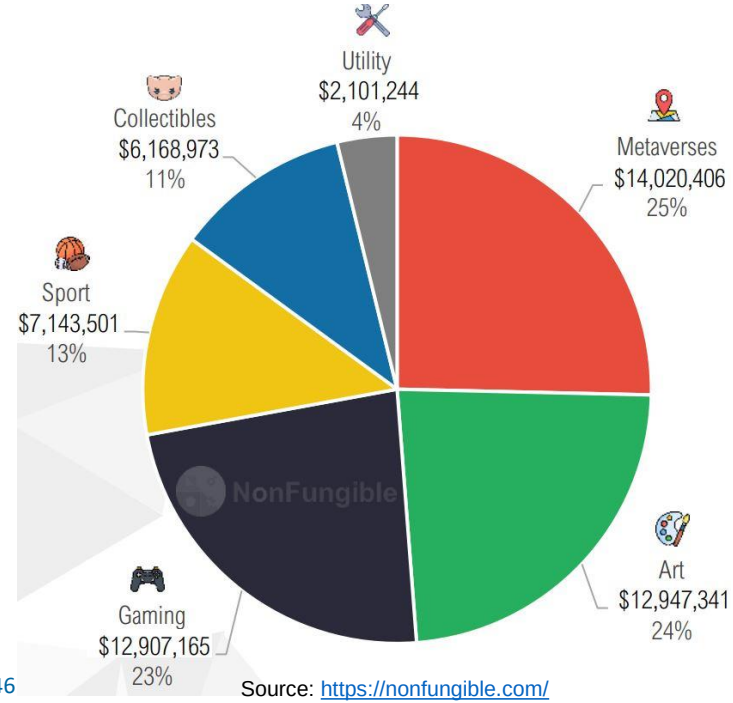
CryptoRank.io @CryptoRank_io @CryptoRankNews

April 21,2022

Non-Fungible Tokens (NFTs)

NFTs are unique and non-interchangeable (e.g., ERC-721 token standard on Ethereum) digital asset programmed on blockchain.

NFTs can be used to represent digital files such as photos, audio, or videos.



Source: https://nonfungible.com/

Digital Art (JPEG file!)

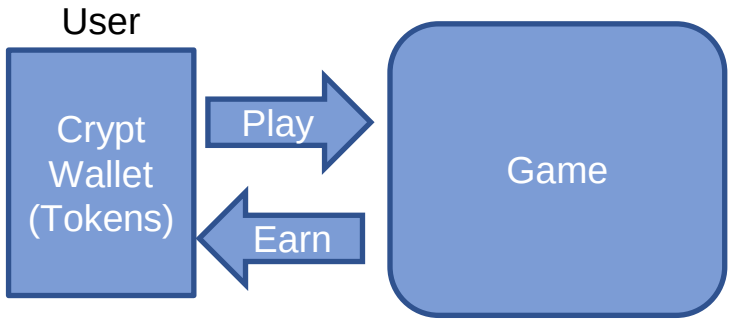
NFT – Market Cap & Trade Volume

	2019	2020	2021
Market capitalisation	$123,999,573	$372,203,300 +200%	$16,898,362,987 +4.440%
Volume of dollars traded	$24,532,783	$82,492,916 +236%	$17,694,851,721 +21.350%
Volume of sales	1,619,516	1,415,638 -13%	27,414,477 +1.836%
Buyers	44,324	75,144 +70%	2,301,544 +2.962%
Sellers	25,036	31,774 +27%	1,197,796 +3.669%
Total active wallets	55,330	89,061 +61%	2,574,302 +1.822%

Games

In Play-to-Earn (P2E) games, the players can earn rewards in the form of tokens in games that they play.

The P2E movement has attracted millions of users across several blockchains.



Name	Genre
Axie Infinity Battle and collect fantasy creatures called Axie	BREEDING CARD PVP
The Sandbox User generated Blockchain Gaming Metaverse	MINIGAME OPEN-WORLD VIRTUAL-WORLD
Undead Blocks Kill Zombies & Earn	ACTION ADVENTURE SHOOTER
Rogue West: Crypto TCG The Online Trading Card Game You Really Own	CARD COLLECTIBLE PVP
Avarik Saga The journey of the 8,888 generative personas.	COLLECTIBLE PVP RPG

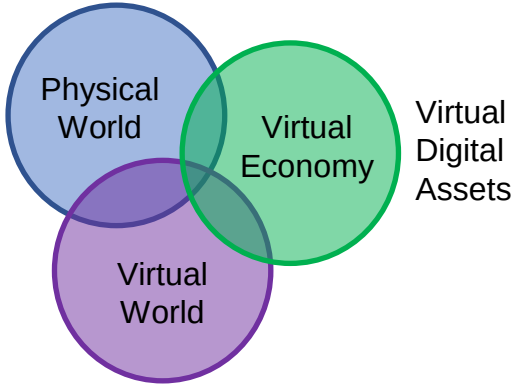
Source: https://playtoearn.net/blockchaingames

Metaverse

Metaverse is considered to be the next iteration/evolution of the internet (Web3.0). 3-D virtual environments enabled by personal or mobile computing with virtual and augmented reality headsets.

The metaverse is described as a means of creating immersive digital spaces for a range of human activity.

NFTs allow users to take ownership of virtual items such as plots of land, avatars and artifacts, and enable them to move those items between different virtual worlds.



Virtual Digital Assets

Augmented reality (AR)
Virtual reality (VR)
Mixed Reality (MR)

Top 3 Projects

DECENTRALAND

AXIE INFINITY

THE SANDBOX

Virtual Land Sale

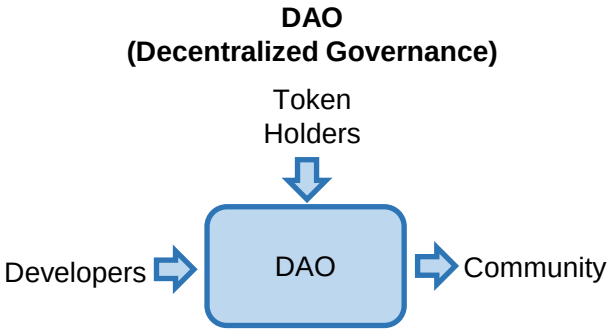
Fashion Street Estate $2.42M
Decentraland 618k MANA

Source: https://dappradar.com/

IEEE

Decentralized Autonomous Organizations (DAOs)

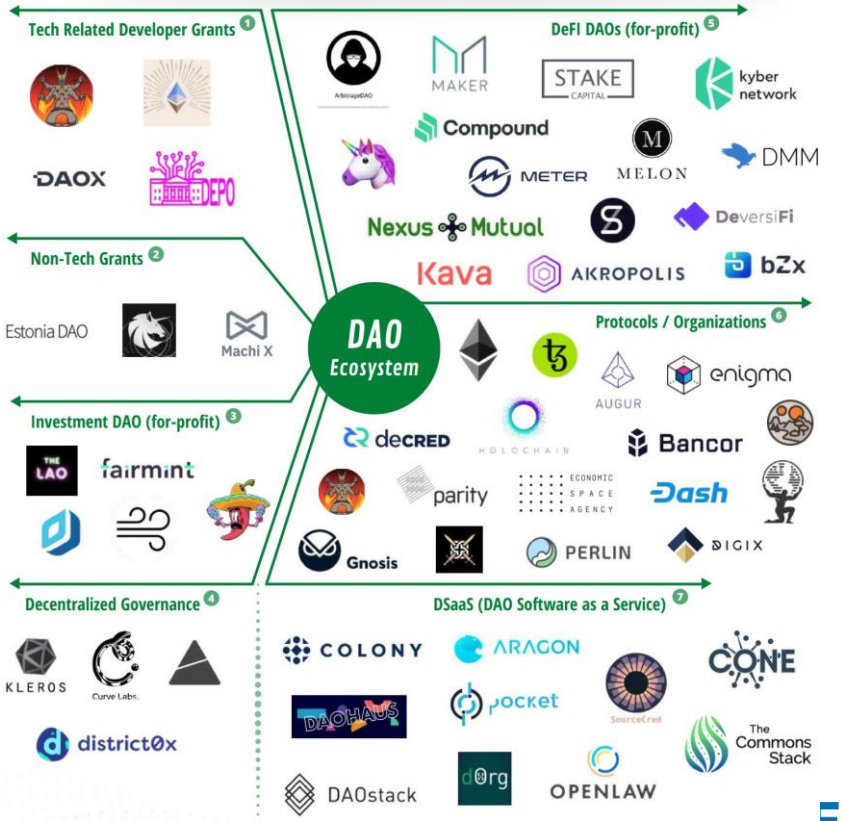
A decentralized autonomous organization (DAO) is an organization represented by rules encoded as smart contract(s) on blockchain.



The collective management of common goods/assets via decentralized governance.

No central authority regulates a DAO. However, this might change soon!

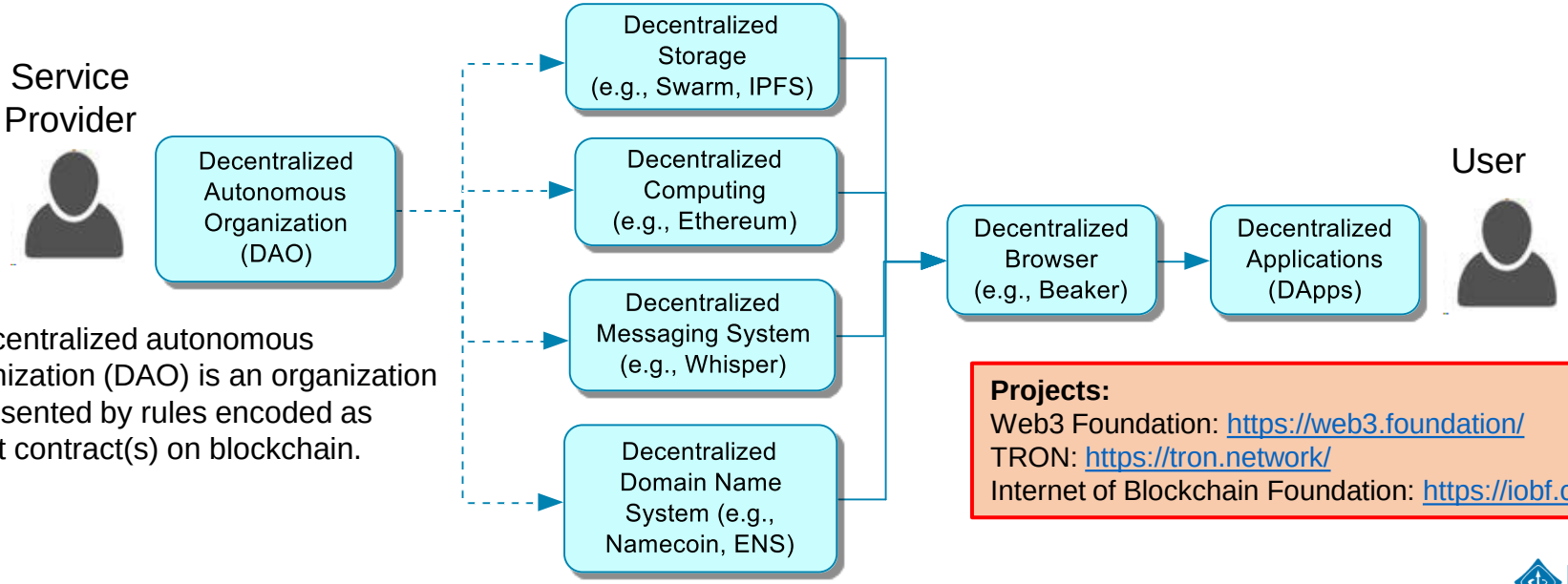
Note: Effective July 1, 2021, the State of Wyoming (USA) to recognize DAO as a limited liability company (LLC).



Decentralized Internet Architecture (or Web 3.0)

Advantages:

- Decentralized Governance (No single authority, Censorship Resistant)
- Immutability (Trust & Transparency)
- Distributed Data Storage (No single point of failure, Resiliency)
- No intermediaries



A decentralized autonomous organization (DAO) is an organization represented by rules encoded as smart contract(s) on blockchain.

Projects:
Web3 Foundation: https://web3.foundation/
TRON: https://tron.network/
Internet of Blockchain Foundation: https://iobf.co/

Decentralized Storage

In a decentralized storage system, the data is broken up into pieces through sharding and stored on multiple computers (called nodes) on a decentralized computer network.

As of Nov 17th, 2021, there are about 37 Projects/Coins with a total market capitalization of $17B.

https://coinmarketcap.com/view/storage/

Decentralized Messaging Protocol & Apps

Whisper is a simple, privacy-first, low-level messaging protocol for decentralized applications built on top of the Ethereum blockchain

Waku (a fork of Whisper) is a decentralized peer-to-peer messaging protocol on Ethereum.

Sylo is a decentralized communication and data exchange network powered by a layer 2 micropayments infrastructure and the $SYLO token.

Secretum is a decentralized, encrypted messaging app, built on the Ethereum and Solana Blockchains.

Decentralized Domain Naming System (DNS)

Domain Naming System (DNS) is managed by Internet Corporation for Assigned Names and Numbers (ICANN). ICANN oversees the allocation of top-level domains like .com, .org, .net, and most two-letter country codes (.ca, .pk).

Several projects are working on blockchain-based decentralized version of DNS. Top-level domains (TLDs) allowed by some projects include:

***Ethereum Naming Service (ENS)*:** .xyz, .kred, .luxe, .club, .art
***Unstoppable Domains*:** .zil, .crypto, .coin, .wallet, .bitoin, .x, .888, .nft, .dao, .blockchain
namecoin: .bit

Decentralized Browser

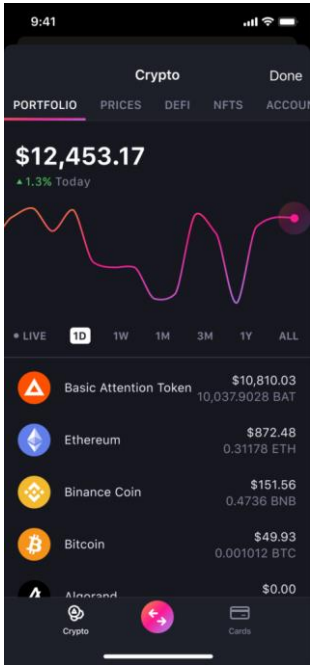
Brave is a privacy-focused, fast, and secure web browser (PC, Mac and mobile).

The Basic Attention Token (BAT), an Ethereum-based native utility token is used to reward users for their attention. BAT is also used for compensating content creators and advertisers.

Brave browser provides native integration with InterPlanetary File System (IPFS), which is a decentralized storage network.

Now, “Brave Search (beta)” with privacy search feature is available in Brave browser .

Brave Crypto Wallet



Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

Enterprise Use Case: Blockchain for Supply Chain

Harvard Business Review

How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenges

by Kate Vitasek, John Bayliss, Loudon Owen, and Neeraj Srivastava

January 05, 2022

Unilever pursues supply chain sustainability with blockchain

Unilever deploys blockchain-enabled GreenToken by SAP to help ensure the palm oil used in its products comes from responsible sources and doesn't contribute to rainforest loss.

By Jim O'Donnell, News Writer

Published: 30 Mar 2022

Blockchain could solve pharma's supply chain challenges, says Zuellig Pharma

Daniel Laverick at Zuellig Pharma tells us how blockchain can solve the most common challenges in pharmaceutical supply chains

04/08/2022

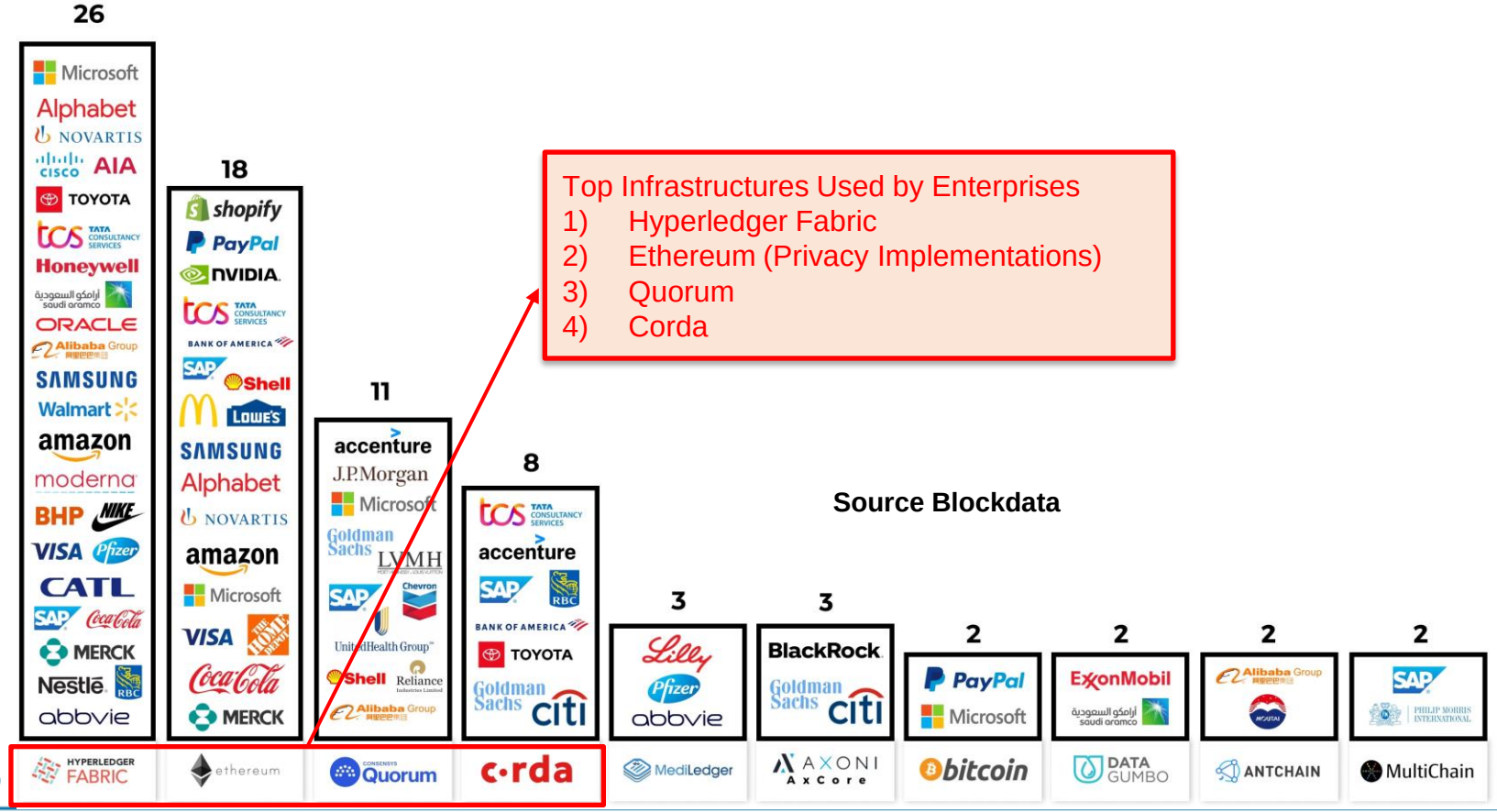
IEEE

Enterprise Blockchain: Players & Use Cases

81 of top 100 companies use blockchain technology!

(Source: Blockdata)

Enterprise Blockchain/DLT: Infrastructure Used



Enterprise Ecosystem: Alliances & Consortia

Enterprise alliances and consortia build private blockchain infrastructure, clients, tools, industry standards and specifications.

Enterprise Blockchains

Sept 2015

r3.

Dec 2015

HYPERLEDGER

2016

CONSENSYS Quorum

(Aug 2020: Acquired by ConsenSys)

Enterprise Client Specs

Mar 2017

ENTERPRISE ETHEREUM ALLIANCE

Application Areas

Sept 2017

TrustedIoTAlliance

(Now Part of IIC)

Aug 2017

BiTA BLOCKCHAIN IN TRANSPORT ALLIANCE

May 2018

MOBI

(See next slide)

IEEE

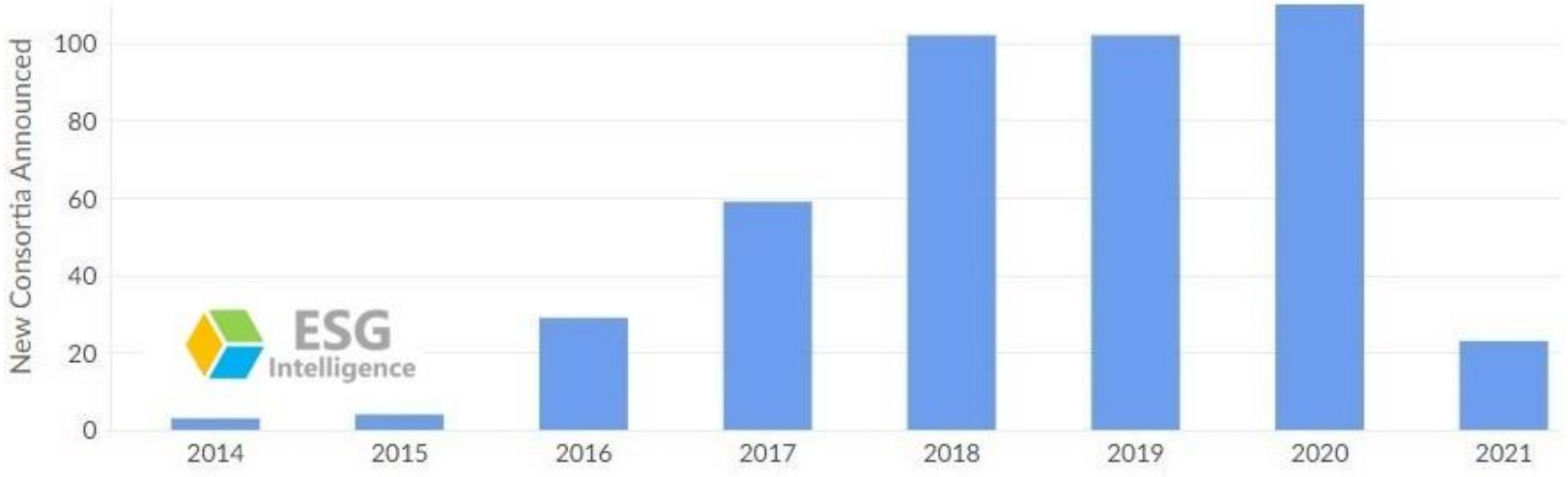
Enterprise Ecosystem: Number of Consortia Formed by Year

433
Blockchain Consortia

8763
Unique Consortia Participants

2855
Key Executives

23
New Consortia in 2021



IEEE

Enterprise: Blockchain-as-a-Service (BaaS)

Leading cloud-service providers have started offering BaaS platforms and solutions.

Mar 2017

IBM

Hyperledger Fabric

https://www.ibm.com/blockchain

Aug 2017

Microsoft

Build Azure
All about the Microsoft Cloud

https://azure.microsoft.com/en-us/solutions/blockchain/

Apr 2018

aws

AWS Blockchain Ethereum & Hyperledger Templates

https://aws.amazon.com/blockchain/templates/

Jul 2018

ORACLE

Oracle Blockchain Platform

https://www.oracle.com/cloud/blockchain/

April 2017

Tencent Cloud

TrustSQL

https://tencentcloud.io/tag/blockchain-technology/

Jan 2018

Baidu 公益

Baidu Trust

https://chain.baidu.com/

Sept 2018

Alibaba Cloud
Worldwide Cloud Services Partner

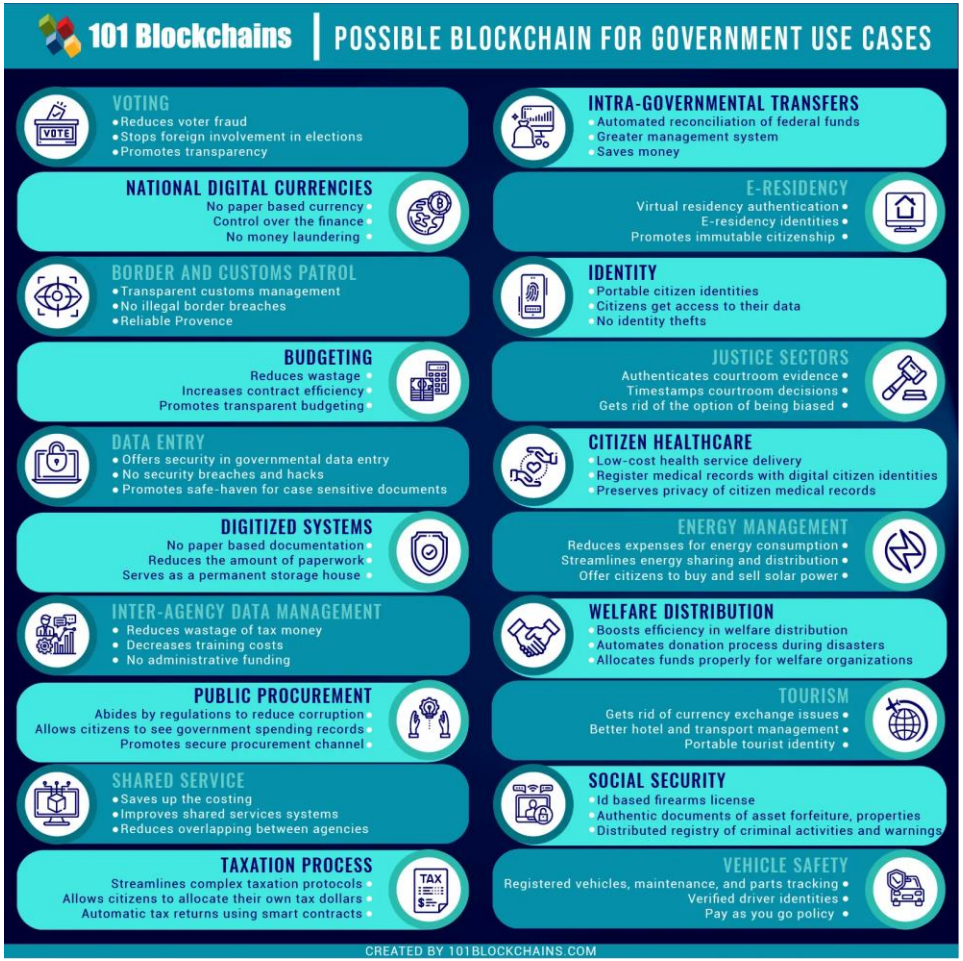
Blockchain as a Service

https://www.alibabacloud.com/products/baas

Outline

- Digital Cash
- Bitcoin
- Blockchain Evolution
- Ethereum
- Cryptocurrencies & Startups
- Enterprise Use Cases
- Government Use Cases

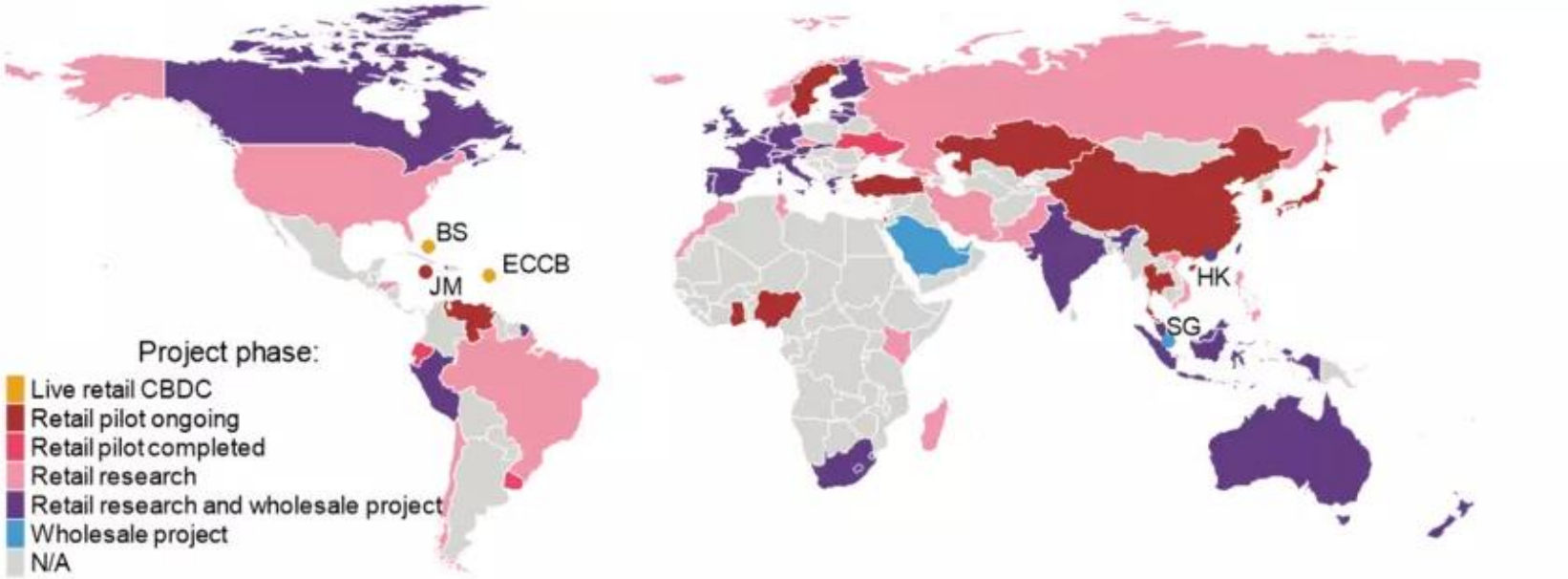
Government Use Cases



IEEE

Central Bank Digital Currencies (CBDCs): Global Landscape

CBDC is a digital currency issued by Central Banks on blockchains/DLT. It will serve as the new digital medium of exchange, settlement, and payment verification.



BS = The Bahamas; ECCB = Eastern Caribbean Central Bank; HK = Hong Kong SAR; JM = Jamaica; SG = Singapore. The use of this map does not constitute, and should not be construed as constituting, an expression of a position by the BIS regarding the legal status of, or sovereignty of any territory or its authorities, to the delimitation of international frontiers and boundaries and/or to the name and designation of any territory, city or area.

Source: R Auer, G Cornelli and J Frost (2020), "Rise of the central bank digital currencies: drivers, approaches and technologies", *BIS working papers*, No 880, August.

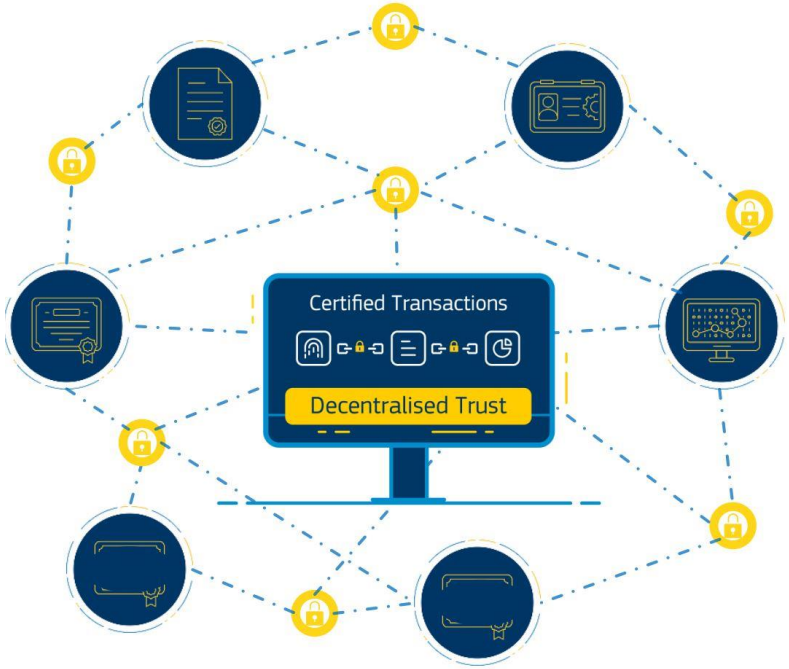
Source: BIS

European Blockchain Services Infrastructure (EBSI)

The EBSI project is building a blockchain infrastructure that will offer cross-border public services for the European Union member states.

The vision is for EBSI to become a network where the members can flexibly use the infrastructure to cooperate via cross-border public services, connect existing solutions or integrate specific services.

EBSI includes 4 initial use cases:
- European Self-Sovereign Identity
- Trusted data sharing
- Diplomas Management
- Notarization of documents



https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734

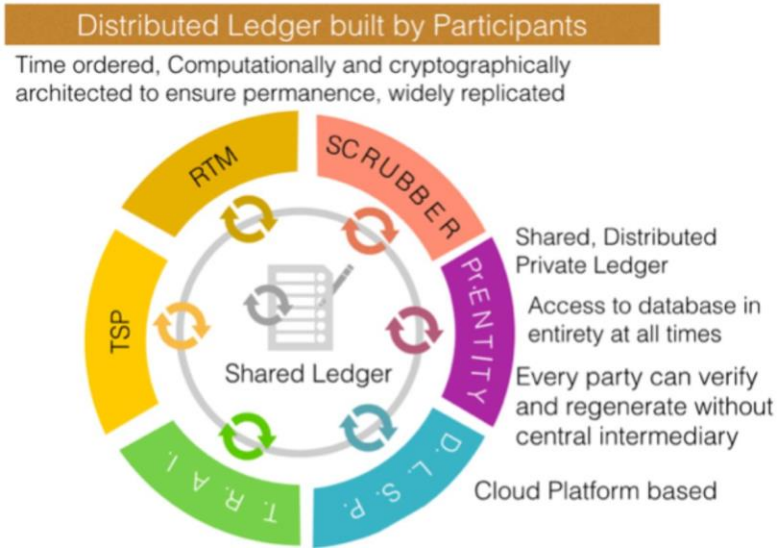
Telecom Regulatory Authority of India (TRAI)

Problem: Unsolicited Commercial Communications (UCC) or “spam” calls are a major cause of disturbance and inconvenience for telecom users in recent times.

Regulation: TRAI mandated telecom providers to adopt Distributed Ledger Technology (DLT) to address this problem.

Solution: Tech Mahindra built a Hyperledger Fabric based solution to manage UCC in compliance with the regulations and guidelines of TRAI.

This solution helps 500 million mobile phone customers manage their consent and preferences to avoid spam calls and text messages!



TSP: Telecom Service Providers.
RTM: Registered Telemarketers.
SCRUBBER: The process of verifying the SMS content.
Pr. ENTITY: The Principal Entities.
DLSP: Digital Locker Service Provider.
TRAI: Telecom Regulatory Authority of India

Source: Pavan Gupta, Jt. Advisor, Telecom Regulatory Authroity of India, “Use of DLT to control Unsolicited Commercial Communication”

United Nations – Practical Guide & Projects

UN published a Practical Guide to give a basic understanding of blockchain and general guidance on how to determine if blockchain could help solve a particular problem.

This guide is meant to serve as a starting point to evaluate blockchain use cases and introduces ways in which the UN is approaching these technologies in a systematic way.

UN showcase projects using blockchain & cryptocurrency:
- Land record management in Afghanistan
- Transparent supply-chain between Djibouti and Ethiopia
- Cash transfers in refugee camps in Jordan
- Tracking chocolate production in Ecuador

Blockchain to Save and Change Lives WFP Innovation Accelerator Initiative

Apply to receive up to US $100,000 in equity-free funding, mentorship and access to the world's largest humanitarian organization

Innovative technologies enable the development of new products and services that can be used to address some of the most critical challenges of our society: for example, saving people affected by natural disasters and conflict and changing their lives to be more resilient and dignified. We believe that decentralized technologies and token-based economics (namely, blockchain, distributed ledger technology, Web 3.0) may deliver a large impact within the context of humanitarian response and food security.

Do you have an idea to help humanity? We are looking for your bold idea in any of the areas described below. Please consider that poor connectivity and limited smartphone penetration are common in many contexts in which WFP works. Furthermore, digital literacy, financial literacy, and inclusive and ethical technology developments need to be appraised as part of your proposed application.

Thank You!

Ramesh Ramadoss, PhD
Dr.Ramesh.Ramadoss@ieee.org

https://blockchain.ieee.org/