BITS Pilani
Pilani Campus

Blockchain Technology and Systems

(SEZG569/SSZG569)

Dr. Ashutosh Bhatia
Department of Computer Science and Information Systems

BITS Pilani
Pilani Campus

QUIZ, HYPE & FACTS

innovate achieve lead

BITS Pilani
Pilani Campus

QUIZ

Q0

What is BITCOIN

a) A Cryptocurrency
b) A decentralized peer-to-peer network
c) A public transaction ledger
d) All

Q1

Who created Bitcoin?

Satoshi Nakamoto

Satoshi Nakamoto is the name used by the presumed pseudonymous person or persons who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation. As part of the implementation, Nakamoto also devised the first blockchain database. Nakamoto was active in the development of bitcoin up until December 2010. Many people have claimed, or have been claimed, to be Nakamoto.

source: https://en.wikipedia.org/wiki/Satoshi_Nakamoto

Q2

Where do you store your cryptocurrency?

Crypto Wallets

In the cryptocurrency ecosystem, the term “wallet” refers to software, online or offline, that allows a cryptocurrency owner to access their cryptocurrency holdings.

Q3

What is a miner?

Computers that validate and
process blockchain transactions

Q4

Where can you buy cryptocurrency?

- A private transaction
- An exchange
- A Bitcoin ATM

Q5

What is a blockchain?

a) A distributed ledger on a peer to peer network
b) A type of cryptocurrency
c) An exchange
d) A centralized ledger

Q6

What is a DApp?

A decentralized application that is developed over blockchain platform

Q7

What is the term for when a blockchain splits?

Fork

A bitcoin hard fork refers to a radical change to the protocol of bitcoin's blockchain that effectively results in two branches, one that follows the previous protocol and one that follows the new version. It is through this forking process that various digital currencies with names similar to bitcoin have been created, including bitcoin cash and bitcoin gold. Bitcoin cash remains the most successful hard fork of the primary cryptocurrency; as of June 2021, it is the eleventh-largest digital currency by market cap.

Q8

What incentivizes the miners to give correct validation of transactions?

A block Reward in form of Bitcoins

Q9

What is a hash function?

Takes an input of any length and returns a fixed-length string of numbers and letters

Q10

What does IPFS stand for?

Interplanetary File System

The **InterPlanetary File System** (**IPFS**) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices.[4]

InterPlanetary File System - Wikipedia

Q11

What is the maximum number of bitcoins that can be created?

21 million

Q12

What was the highest the Bitcoin price ever reached?

₹ 54,404,923

Q13

What is Altcoin?

Altcoins are cryptocurrencies other than Bitcoin.

Altcoin - Bitcoin Wiki

- Binance Coin (BNB)
- Cardano (ADA)
- Chainlink (LINK)
- Ether (ETH)
- Litecoin (LTC)

As of today, **over 5000** of these "alternative" currencies have been created worldwide.

Q14

What is meme coin?

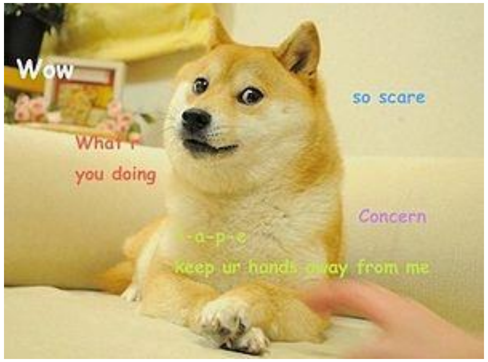
A **meme coin** (also spelled **memecoin**) is a cryptocurrency that originated from an Internet meme or has some other humorous characteristic.[1] It may be used in the broadest sense as a critique of the cryptocurrency.

In late 2013, Dogecoin was released after being created as a joke on the Doge meme by software engineers. This sparkled the creation of several subsequent meme coins. In October 2021, there were about 124 meme coins circulating in the market. Notable examples include Dogecoin and Shiba Inu,[2]

Meme coin - Wikipedia

Q15

What is This?



Dogecoin (/ˈdoʊ(d)ʒkɔɪn/ *DOHJ-koyn* or *DOHZH-koyn*,[2] code: **DOGE**, symbol: **Ð**) is a cryptocurrency created by software engineers Billy Markus and Jackson Palmer, who decided to create a payment system as a "joke", making fun of the wild speculation in cryptocurrencies at the time.[3] It is considered both the first "meme coin", and, more specifically, the first "dog coin". Despite its satirical nature, some consider it a legitimate investment prospect.

Doge (meme) - Wikipedia

Q16

What is Stablecoins?

Cryptocurrency but usually centralized and
pegged with some fiat money or asset class

Stablecoins are cryptocurrencies where the price is designed to be pegged to a cryptocurrency, fiat money, or to exchange-traded commodities (such as precious metals or industrial metals).[1]

Stablecoin - Wikipedia

Q17

What is Token?

Token is a unit of value issued by a tech or crypto start-up, intended to be a piece in the ecosystem of their technology platform or project. Tokens are supported by blockchains. They only physically exist in the form of registry entries in said blockchain. Initially, most tokens were based on the ERC20 protocol by Ethereum.

Tokens are different from bitcoins and altcoins in that they are not mined by their owners nor primarily meant to be traded (although they may be traded on exchanges if the company that issued them becomes valuable enough in the eyes of the public), but to be sold for fiat or cryptocurrency in order to fund the start-up's tech project.

Token Definition – Cryptocurrency – BitcoinWiki

Q18

What is MetaVerse and Omniverse?

Facebook is changing its name to Metaverse to highlight the vision of a future that will be lived in the cyberspace (along with life in the physical space). Augmented Reality and Virtual Reality, along with sensors, displays, artificial intelligence and Digital Twins, are the enabling technologies.

Metaverse vs Omniverse – IEEE Future Directions

Q19

What is Sandbox and Dreamland

The Sandbox is a sandbox game for mobile phones and Microsoft Windows, developed by gamestudio Pixowl and released on May 15, 2012. It was released for PC on Steam on 29 June 2015. The brand was acquired by Animoca Brands in 2018, and its name used for a blockchain-based 3D open world game.

SAND is an ERC-20 Ethereum-powered utility token that will be the medium of exchange within **The Sandbox**. Facilitates the purchase or sale of LANDs or game ASSETs (LANDs are portions of the Metaverse open to player ownership, while ASSETs are tokens created by players).

Metaverse vs Omniverse – IEEE Future Directions

Q20

What is NFT?

A non-fungible token (NFT) is a and non-interchangeable unit of data stored on a blockchain, a form of digital ledger. NFTs can be associated with reproducible digital files such as photos, videos, and audio. NFTs use a digital ledger to provide a public certificate of authenticity or proof of ownership, but do not restrict the sharing or copying of the underlying digital files. The lack of interchangeability (fungibility) distinguishes NFTs from blockchain cryptocurrencies, such as Bitcoin.

Non-fungible token - Wikipedia

Q21

What is (DAO) ?

A company or group of like-minded entities that operate based on the rules set forth in a smart contract. DAOs are used to transform business logic into software logic recorded on a blockchain. A company whose funds are locked in a multisignature wallet that is controlled by a smart contract is an example of a DAO. In that same example, board of directors decisions might be voted on, recorded, and effected through a smart contract rather than by holding physical board meetings.

Q22

What is ETHEREUM ?

Ethereum is a decentralized Blockchain 2.0 chain. It was the first major smart contract platform and has widespread support from Fortune 500 companies through the Ethereum Enterprise Alliance (EEA).

Ethereum currently uses a Proof-of-Work (PoW) consensus algorithm, but future changes to the protocol will update it to a more scalable algorithm, most likely based on Proof-of-Stake (PoS).

Q23

What is HASHRATE ?

The rate at which a particular machine can perform a specific hashing function. Hashrate is similar to general CPU speed, but where processor speed is measured based on the number of arbitrary instructions a machine can carry out per second, hashrate is measured based on the number of times a machine can perform that specific function per second, allowing application-specific integrated circuits (ASIC) to have a much higher hashrate than a processor with the same clock speed.

Q24

What is MAINNET ?

The largest blockchain network a specific protocol runs, or the most valuable chain as decided by the community. Mainnets are typically where real value is derived and represent the truest intent of the core developers.

Q25

What is ORACLE ?

Services that connect real-world data with blockchain applications. Oracles are necessary to provide input that cannot be independently verified, such as temperature measurements. Oracles typically rely on the security of a trusted source rather than the security of trustlessness.

Q26

What is SOLIDITY ?

A smart contract programming language built for the Ethereum Virtual Machine. Syntactically it resembles C++ and Javascript and compiles to eWASM.

Q27

What is SOLIDITY ?

A smart contract programming language built for the Ethereum Virtual Machine. Syntactically it resembles C++ and Javascript and compiles to eWASM.

Q28

What is TOKENIZATION ?

The concept of translating business strategies, goods, or services into discrete, tradeable units that are recorded on a blockchain or other system.

Physical goods can be tokenized by associating their unique identifiers with on-chain references.

Q29

What is TOKENIZATION ?

The concept of translating business strategies, goods, or services into discrete, tradeable units that are recorded on a blockchain or other system.

Physical goods can be tokenized by associating their unique identifiers with on-chain references.

Q30

What Is a "51% Attack"?

A 51% attack refers to a malicious actor (or group acting in concert), controlling over 50% of the total mining power of the blockchain network and disrupting the integrity of the blockchain.

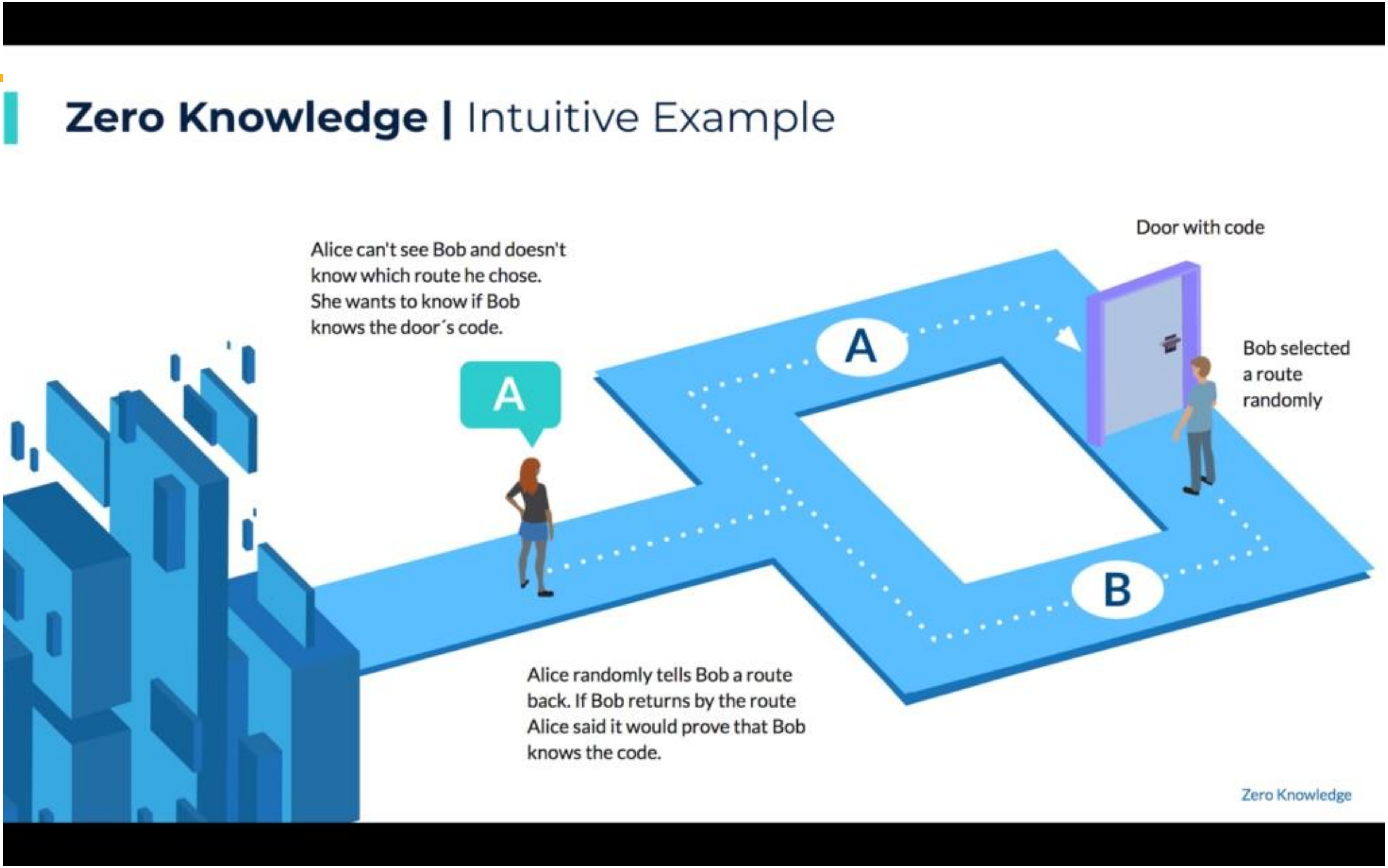
An example of a 51% attack happened in January 2019 on the Ethereum Classic blockchain.

Q31

ZERO-KNOWLEDGE (ZK) PROOF

A mathematical representation of an assertion whose output value can be determined without the input information.

Zero-knowledge proofs are used to prove that an actor is in possession of certain information without actually revealing that information. They are especially useful in cryptocurrencies because they can be used to show that a transaction is valid without revealing the sender, recipient, or amount of the transaction. ZK research is still in its infancy.



Zero Knowledge | Intuitive Example

Alice can't see Bob and doesn't know which route he chose. She wants to know if Bob knows the door´s code.

Door with code

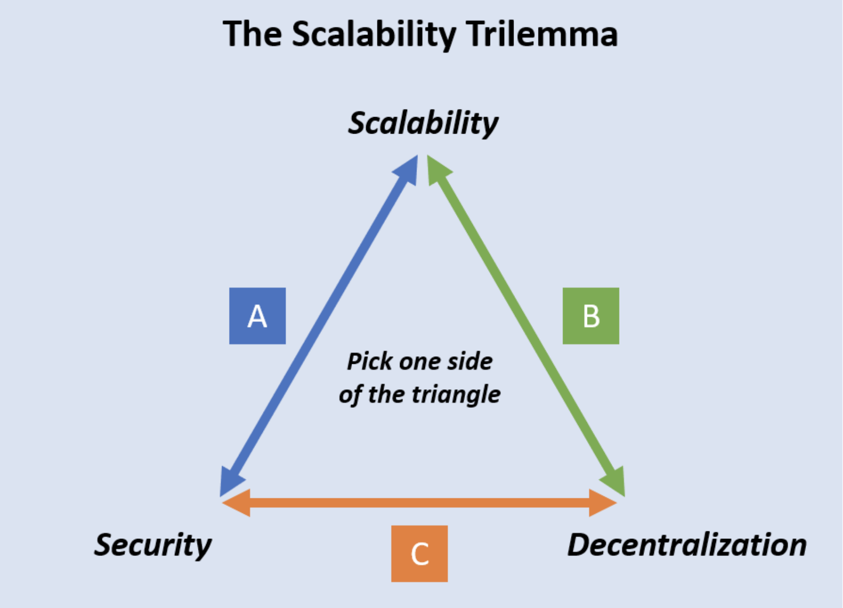
Bob selected a route randomly

Alice randomly tells Bob a route back. If Bob returns by the route Alice said it would prove that Bob knows the code.

Q32

What Is the Blockchain Trilemma?

The blockchain trilemma is a concept coined by Vitalik Buterin that proposes a set of three main issues — decentralization, security and scalability — that developers encounter when building blockchains, forcing them to ultimately sacrifice one "aspect" for as a trade-off to accommodate the other two.



Beeple's, *Everydays " The First 5000 Days"* – $69 Million

Beeple's *Everydays, the First 5000 days* is basically one of the most iconic NFT sales that ever happened in the history of the NFT world. It not only broke the world record but also made. ***Beeple, one of the richest artists in the world.***

The artwork was auctioned at NFT platform, Christies on March 11, 2021. Bascially, the Everydays 5000 consists of Beeple's entire collection of 5000 artworks that he created since May 1, 2007. The bid on this artwork started with $100 but it soon rose to millions ultimately settling for $69 Million dollars.

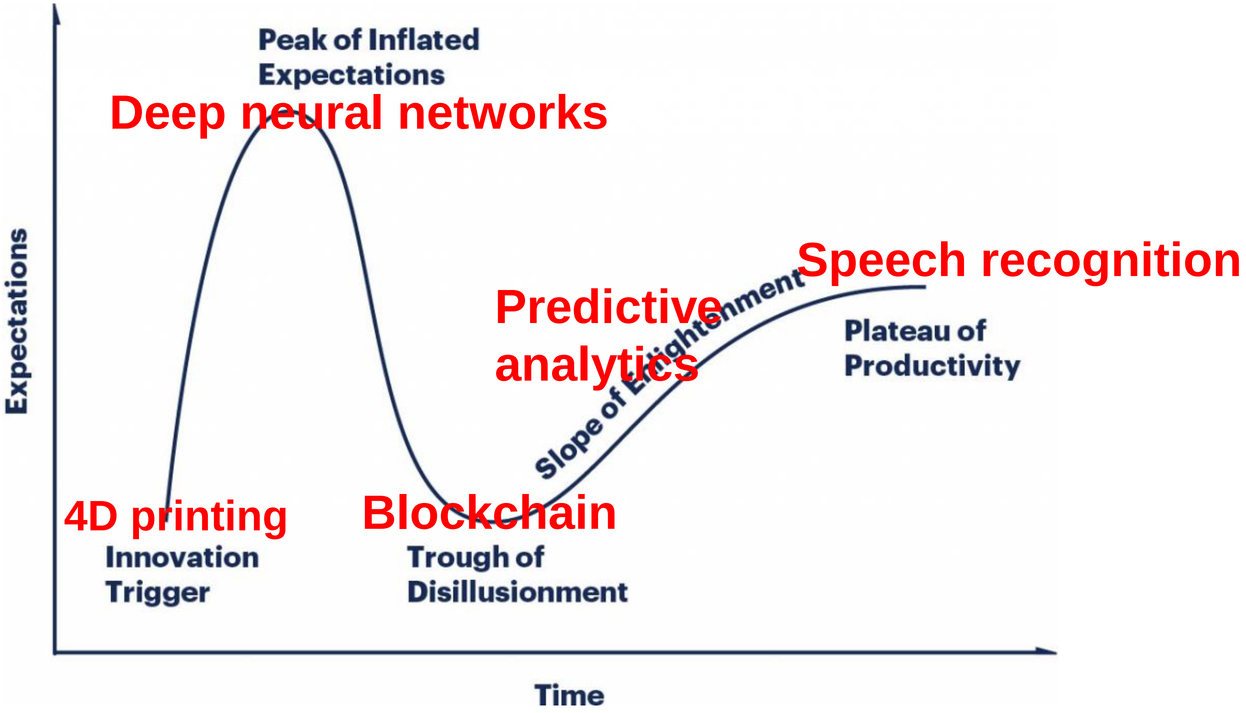
36 MOST EXPENSIVE NFTs EVER SOLD (Ranked) - NFT's Street (nftsstreet.com)

BITS Pilani
Pilani Campus

HYPE

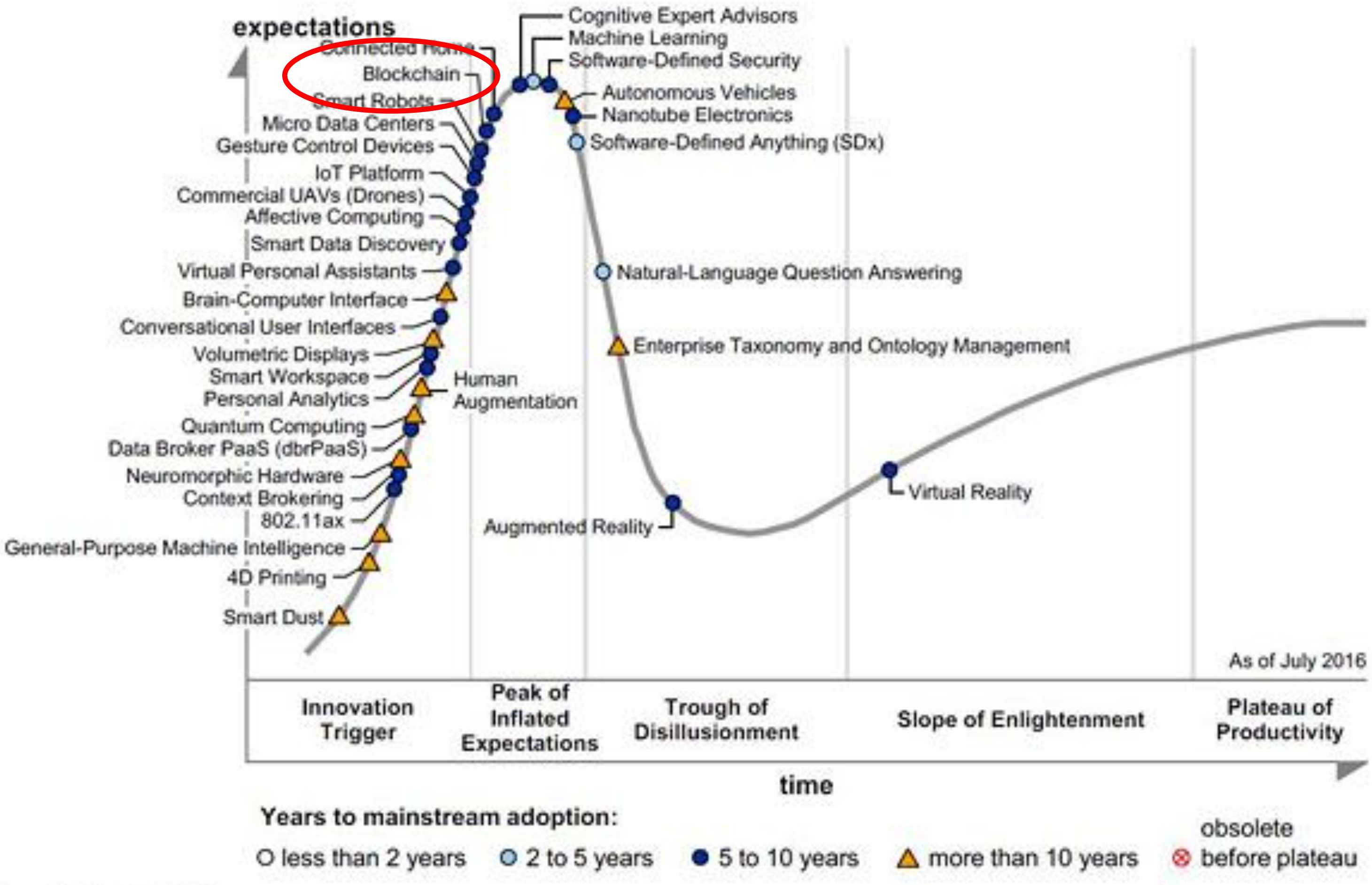
Gartner Hype Cycle

- The Gartner Hype Cycle is a graphical representation of the perceived value of a technology trend or innovation—and its relative market promotion.
- The cycle can help you understand how the perceived value of a given technology evolves over the course of its maturity lifecycle.



[Introduction to the Gartner Hype Cycle – BMC Software | Blogs]

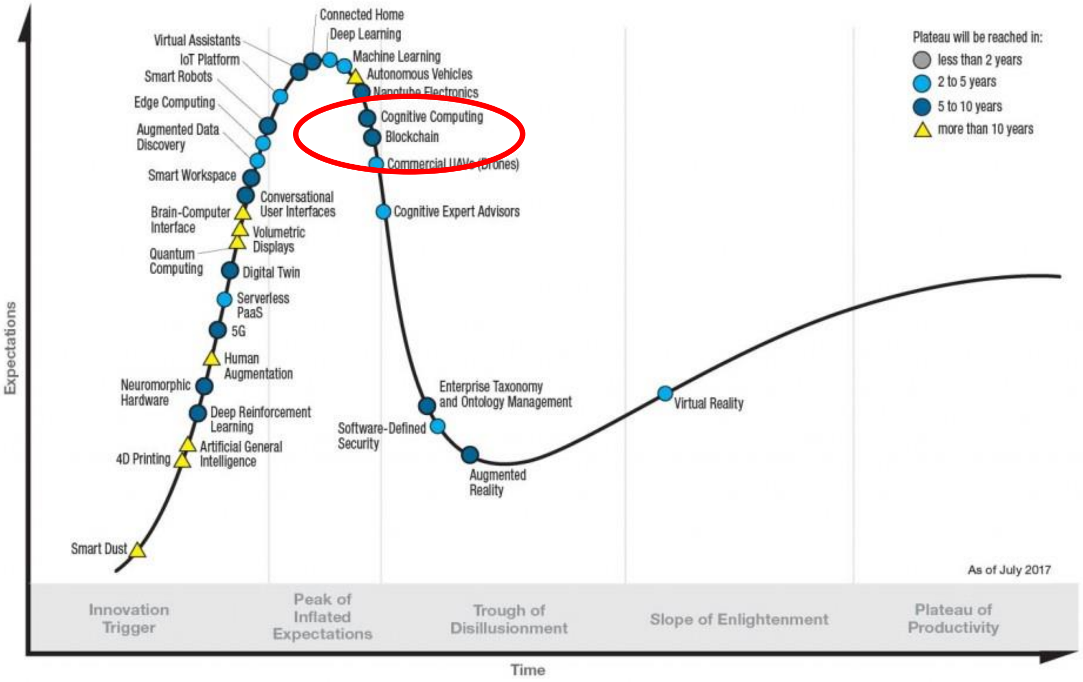
Hype Cycle for Emerging Technologies, 2016



Source: Gartner (July 2016)

Hype Cycle for Emerging Technologies, 2017

Gartner Hype Cycle for Emerging Technologies, 2017



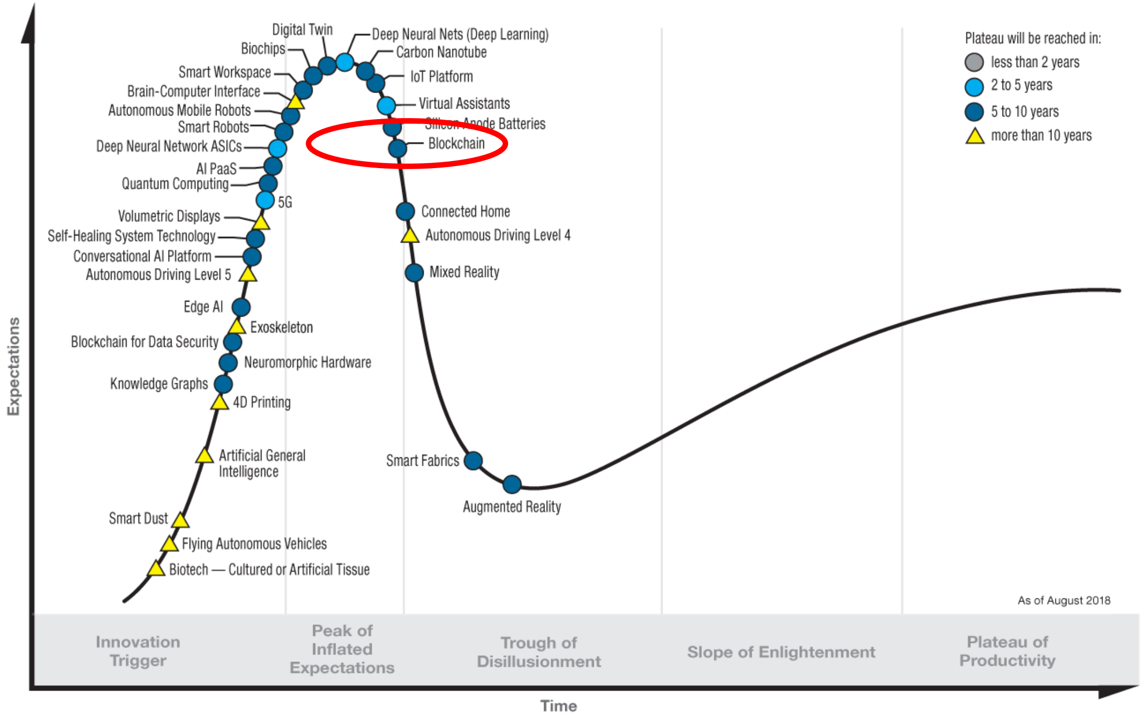
gartner.com/SmarterWithGartner

Source: Gartner (July 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Hype Cycle for Emerging Technologies, 2018

Hype Cycle for Emerging Technologies, 2018



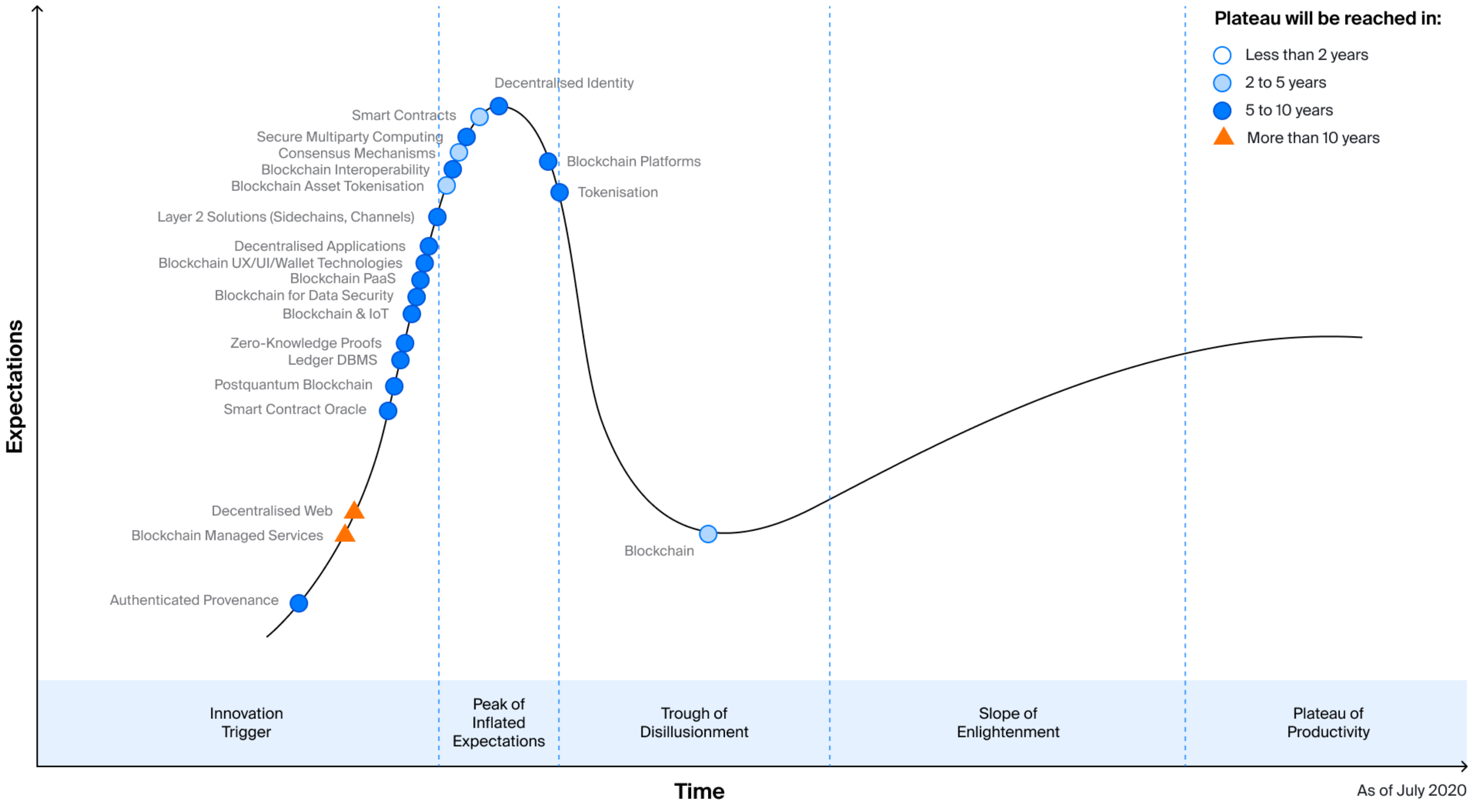
gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner.

Hype Cycle for Blochchain Technologies 2020

Hype Cycle for Blockchain Technologies, 2020

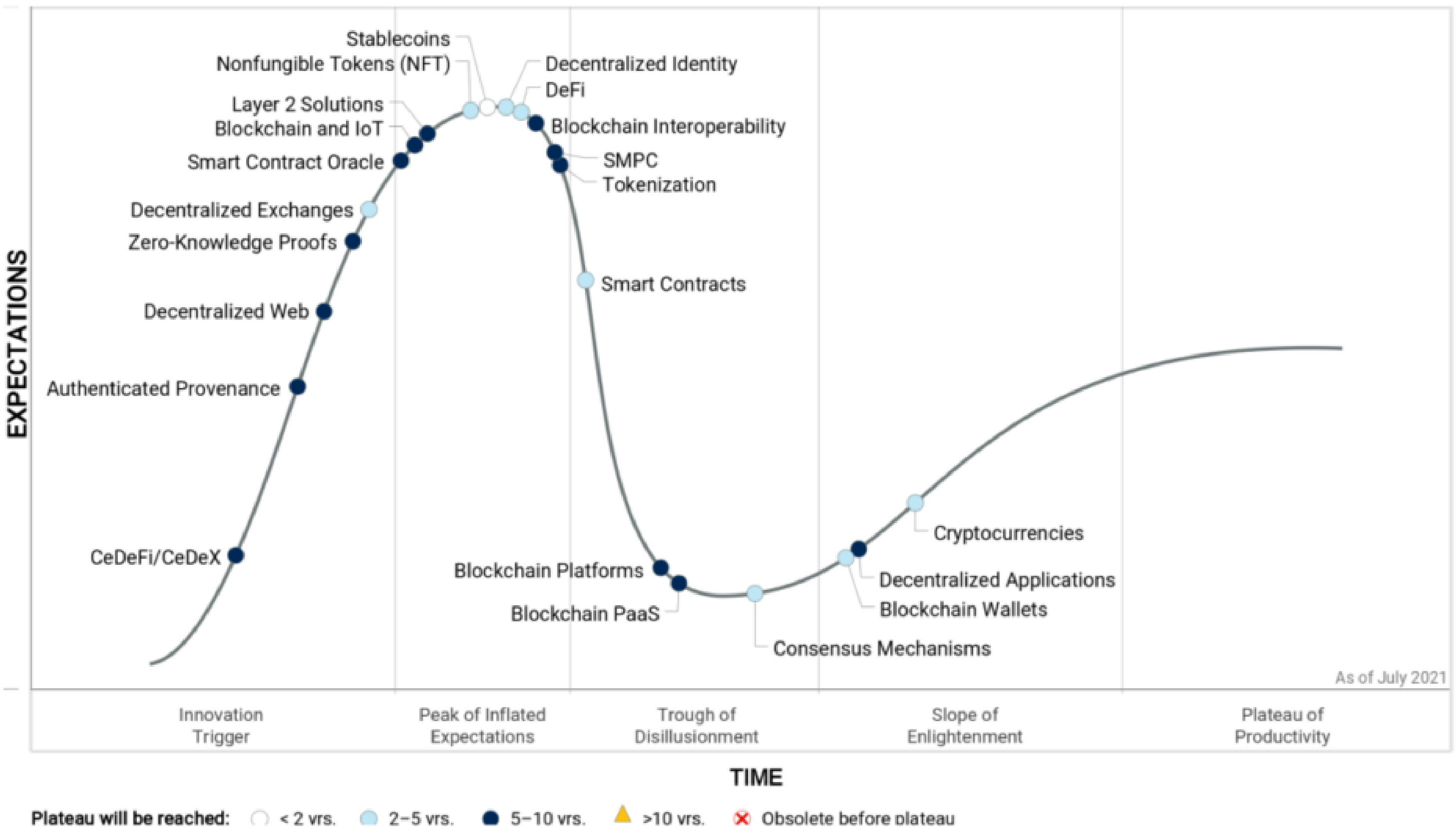


Source: Gartner (2020)

Chainstack

Hype Cycle for Blockchain 2021: More Action than Hype

Hype Cycle for Blockchain, 2021

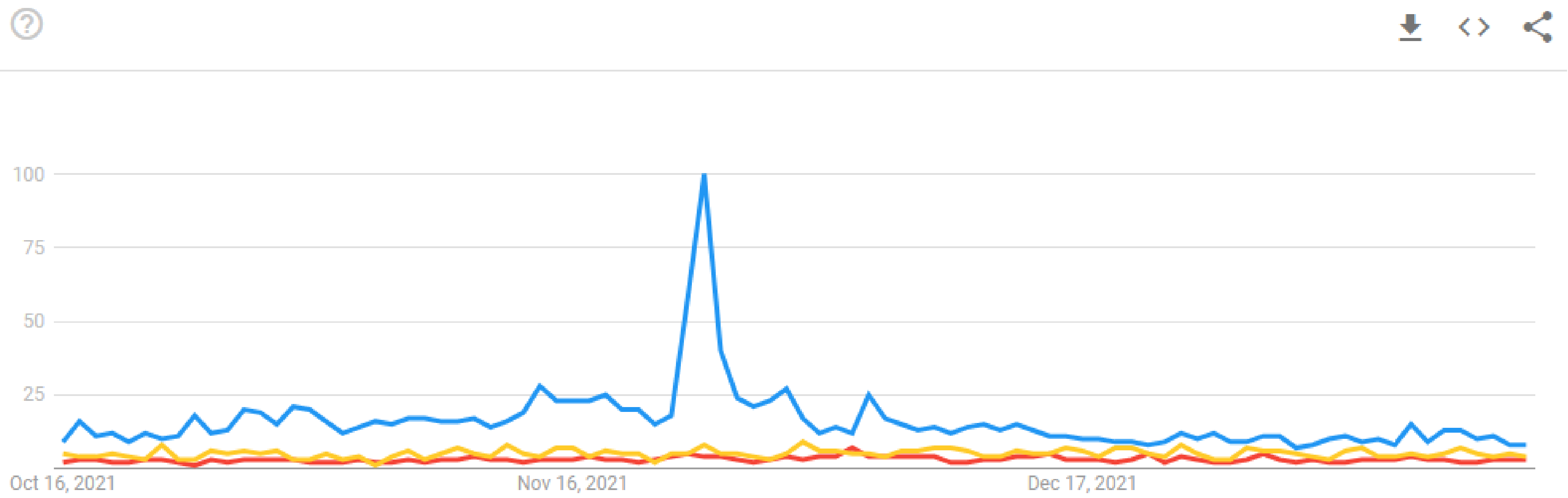


Source: Gartner (July 2021)

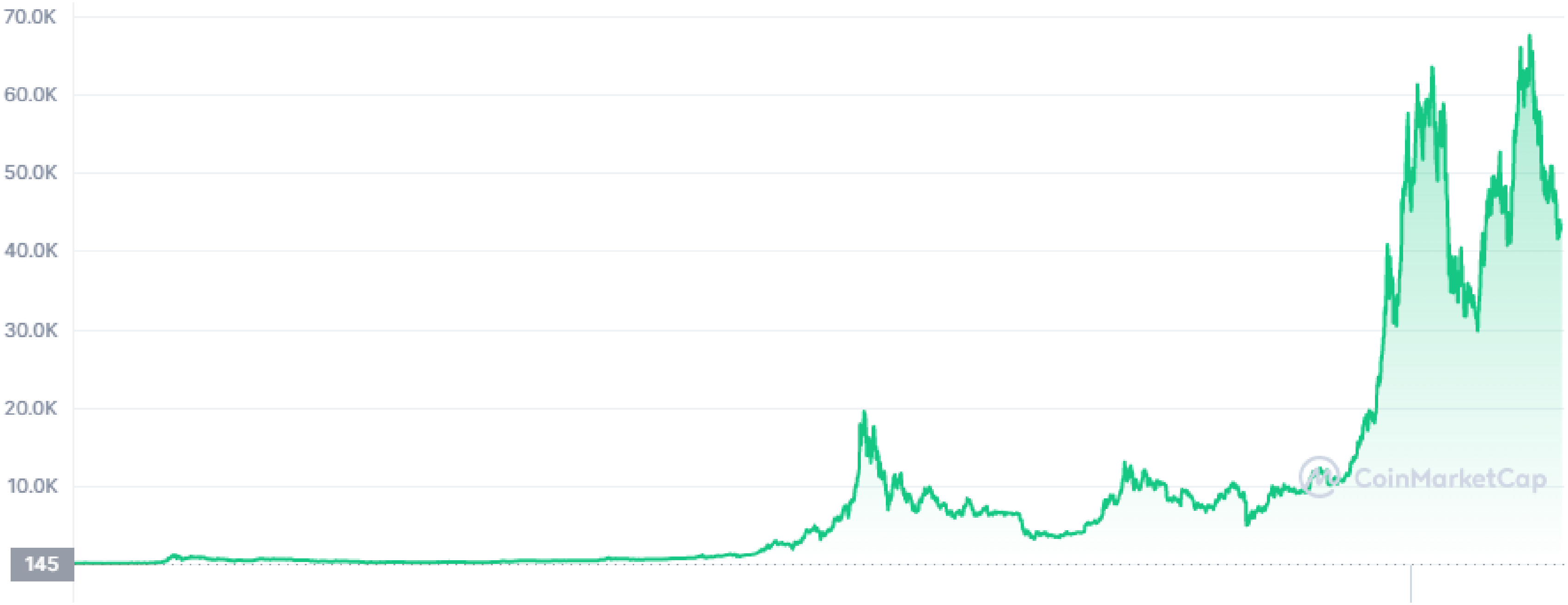
747513

Trends and Facts

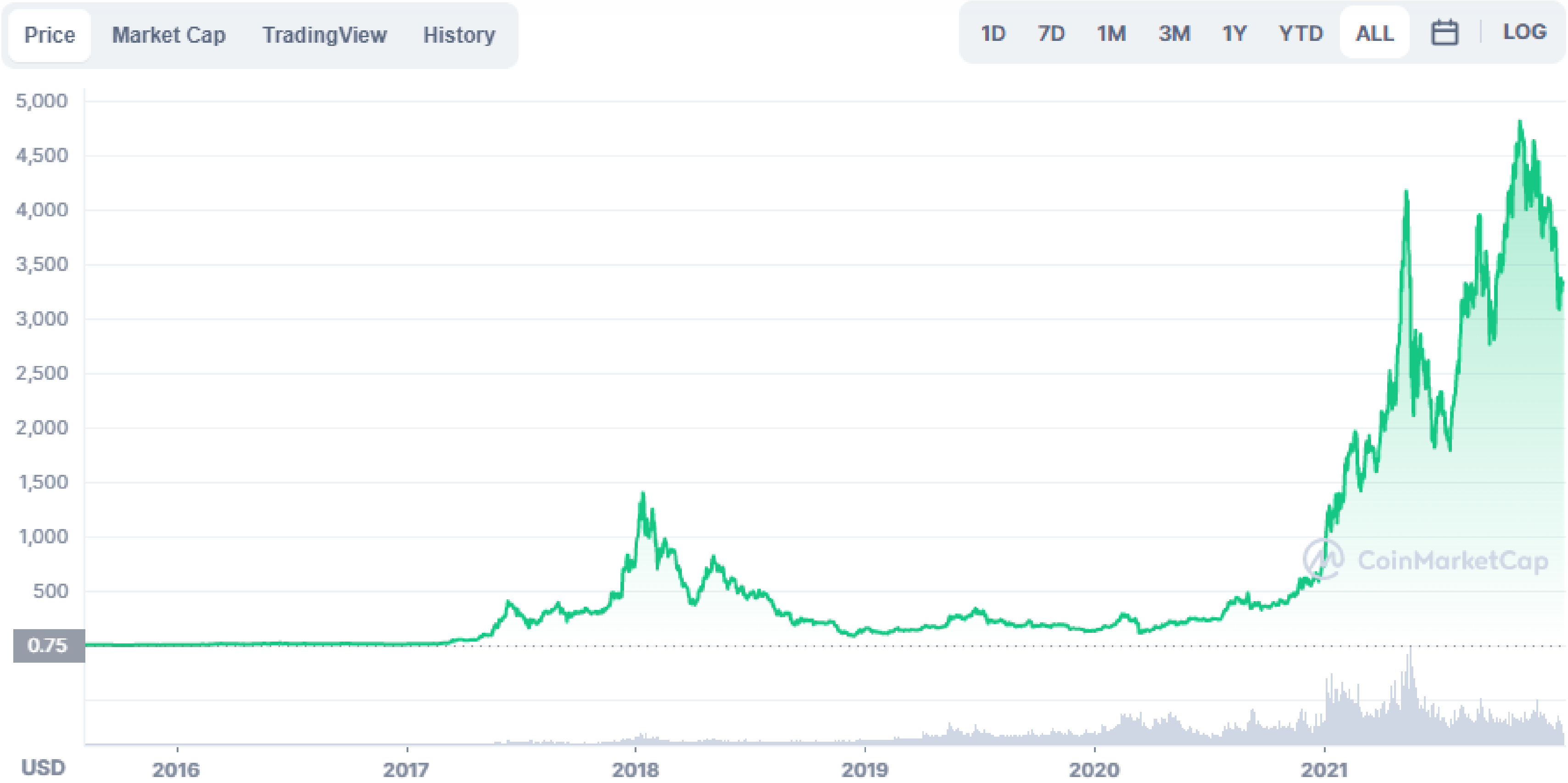
Google Trends: Cryptocurrency, Blockchain ans Machine Learning



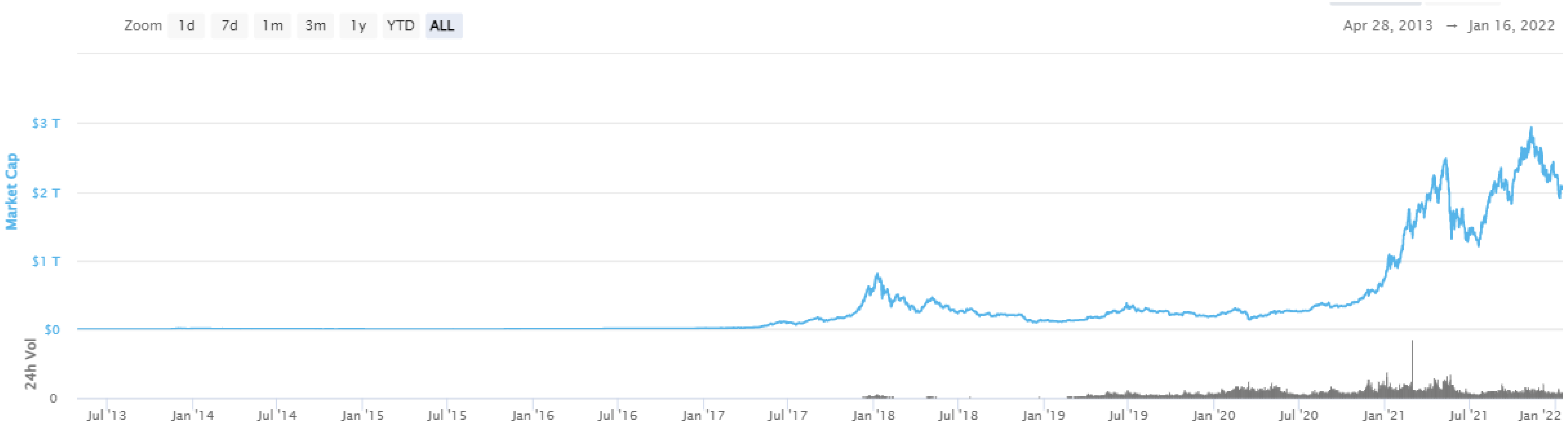
BITCOIN Growth



Etherium Growth



Cryptocurrency Market Cap



Key adoption drivers

- Mainstream adoption of Bitcoin, including El Salvador’s adoption of Bitcoin as legal tender in June 2021.
- Payment network, banking and social network adoption of distributed ledger technologies (DLTs) for money movement, with the expected deployment of central bank digital currencies (CBDCs) being a key influencer.
- Decentralized finance (DeFi) applications offer substantially greater financial rewards than traditional finance. Centralized firms like hedge funds already take advantage of this.
- Tokenization of assets, including explosive growth of NFTs and DeFi tokens, and the promise of tokens linked to physical assets in the future.
- Blockchains such as Binance, Cardano, and Solana offering viable cost-effective alternatives to Ethereum chain transactions.
- Monumental progress in blockchain interoperability, including gateways and abstraction middleware, already used today by DeFi applications.
- Blockchain migration from the proof-of-work (POW) consensus method (still used for Bitcoin) to more energy-efficient consensus methods such as proof of stake (PoS). The ongoing upgrade of Ethereum leads this trend.

Still, the picture is not all rosy. There are plenty of challenges

- Adoption of permissioned blockchains is moving much more slowly. Some use cases — especially around supply chain and authenticated provenance — are benefiting from ledger technology. However, most users are stuck trying to align use cases to the technology.
- Global regulations and accounting standards need clarification before most enterprises adopt cryptocurrency
- China continues to clamp down on crypto activities as they work on making their own CBDC the world's dominant currency.