Blockchain Introductory Workshop – Powered by AI

Chainlink

Edwin Liava’a

Chainlink Developer Expert

edwin.liavaa@proton.me

@EdwinLiavaa

Edwin.Liavaa

Chainlink

Schedule

Time	Activity
5:00 PM - 5:15 PM	Introduction to the workshop
5:15 PM - 5:30 PM	Session 1: What is Blockchain?
5:30 PM - 5:45 PM	Coffee Break (15 minutes)
5:45 PM - 6:15 PM	Session 2: How does Blockchain work?
6:15 PM - 6:30 PM	Coffee Break (15 minutes)
6:30 PM - 7:00 PM	Session 3: Applications of Blockchain
7:00 PM - 7:15 PM	Session 4: Conclusion

Export to Sheets

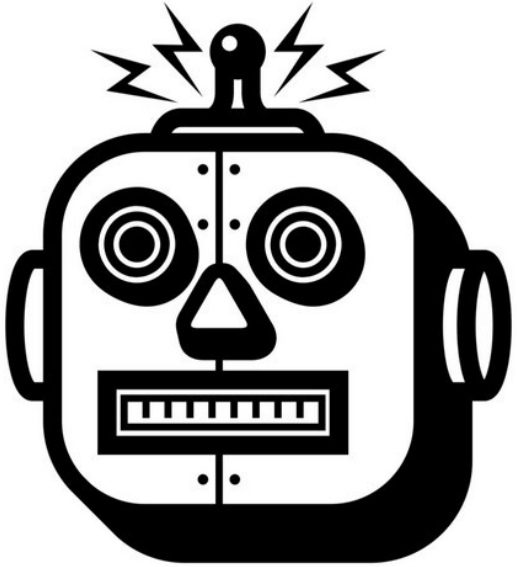
AI – Assistants, Blockchain Tools and Resources

- ChatGPT https://openai.com/blog/chatgpt
- Bing Chat https://www.bing.com/search
- FreedomGPT https://chat.freedomgpt.com
- Google Bart https://bard.google.com
- Anthropic's Claude https://claude.ai
- Opera Aria https://www.opera.com/features/aria
- Metamask https://metamask.io
- Alchemy Sepolia Faucet https://sepoliafaucet.com
- Infura Sepolia Faucet https://www.infura.io/faucet/sepolia
- Chainlink Faucets https://faucets.chain.link
- Chainlink Education https://chain.link/education
- Consensys Academy https://courses.consensys.net
- Alchemy University https://university.alchemy.com
- Web3 University https://www.web3.university

Chainlink

Introduction

- Blockchain, as a distributed ledger technology (DLT), has an interesting history that spans several decades.
  - So, let's ask AI?
    - **Prompt>** Hello AI, what is a Distributed Ledger Technology (DLT)? Step by Step
    - **Prompt>** Thank you AI, can you explain the history of the evolution of Blockchain as a Distributed Ledger Technology (DLT)? Step by Step
    - **Prompt>** Thank you AI, can you give me a definition of Blockchain?



Let's Talk **AI**

Distributed Ledger Technology

"Blockchain"

PERMISSIONLESS, PUBLIC, SHARED SYSTEMS

PERMISSIONED, PUBLIC, SHARED SYSTEMS

PERMISSIONED, PRIVATE, SHARED SYSTEMS

DATABASES

Cross Stakeholder Decentralization

Imperial College London

Chainlink

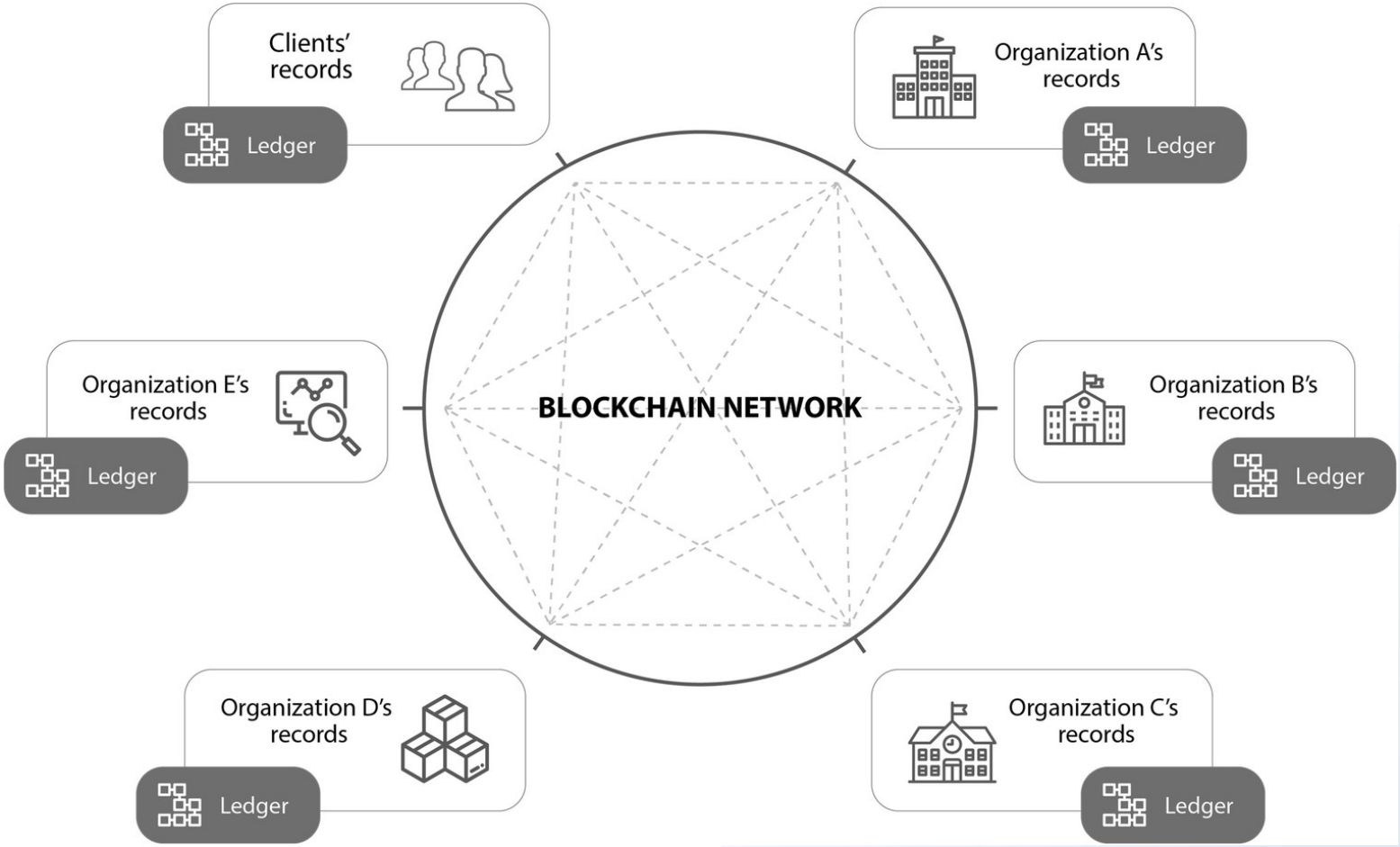
What is Blockchain?

DEFINITION

A blockchain is a highly secure and reliable network that records data in a distributed ledger that is not controlled by a central authority.

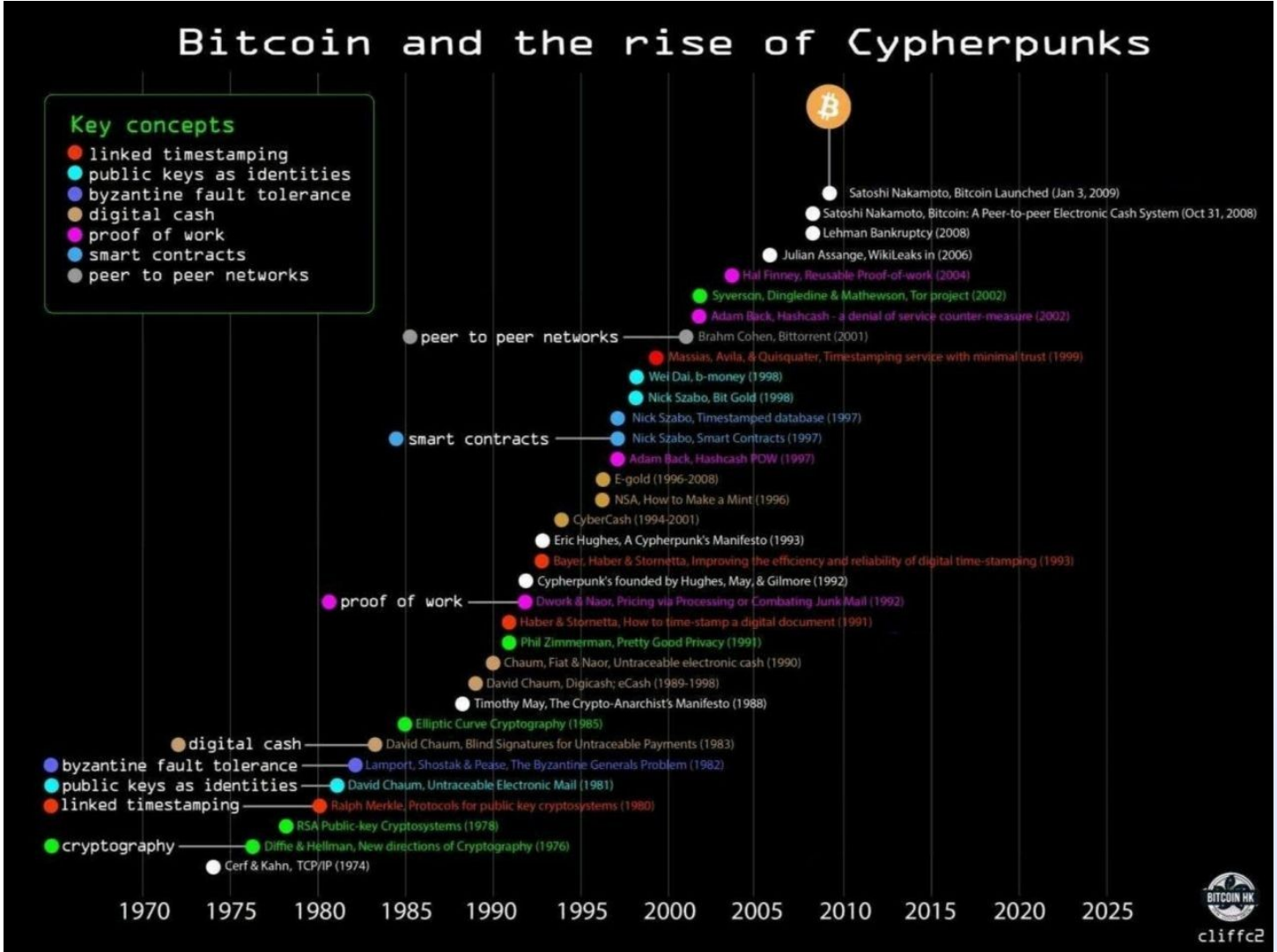
Source: https://chain.link/education-hub/blockchain

Chainlink



Source: https://link.springer.com/article/10.1007/s11036-020-01649-6/figures/1

Chainlink


Bitcoin and the rise of Cypherpunks
Key concepts
linked timestamping
public keys as identities
byzantine fault tolerance
digital cash
proof of work
smart contracts
peer to peer networks
Satoshi Nakamoto, Bitcoin Launched (Jan 3, 2009)
Satoshi Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System (Oct 31, 2008)
Lehman Bankruptcy (2008)
Julian Assange, WikiLeaks in (2006)
Hal Finney, Reusable Proof-of-work (2004)
Syverson, Dingledine & Mathewson, Tor project (2002)
Adam Back, Hashcash - a denial of service counter-measure (2002)
peer to peer networks
Brahm Cohen, Bittorrent (2001)
Massias, Avila, & Quisquater, Timestamping service with minimal trust (1999)
Wei Dai, b-money (1998)
Nick Szabo, Bit Gold (1998)
Nick Szabo, Timestamped database (1997)
smart contracts
Nick Szabo, Smart Contracts (1997)
Adam Back, Hashcash POW (1997)
E-gold (1996-2008)
NSA, How to Make a Mint (1996)
CyberCash (1994-2001)
Eric Hughes, A Cypherpunk's Manifesto (1993)
Bayer, Haber & Stornetta, Improving the efficiency and reliability of digital time-stamping (1993)
Cypherpunk's founded by Hughes, May, & Gilmore (1992)
proof of work
Dwork & Naor, Pricing via Processing or Combating Junk Mail (1992)
Haber & Stornetta, How to time-stamp a digital document (1991)
Phil Zimmerman, Pretty Good Privacy (1991)
Chaum, Fiat & Naor, Untraceable electronic cash (1990)
David Chaum, Digicash; eCash (1989-1998)
Timothy May, The Crypto-Anarchist's Manifesto (1988)
Elliptic Curve Cryptography (1985)
digital cash
David Chaum, Blind Signatures for Untraceable Payments (1983)
byzantine fault tolerance
Lamport, Shostak & Pease, The Byzantine Generals Problem (1982)
public keys as identities
David Chaum, Untraceable Electronic Mail (1981)
linked timestamping
Ralph Merkle, Protocols for public key cryptosystems (1980)
RSA Public-key Cryptosystems (1978)
cryptography
Diffie & Hellman, New directions of Cryptography (1976)
Cerf & Kahn, TCP/IP (1974)
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
cliffc2

Chainlink

What is the purpose of Blockchain?

In all our agreements today, we have this issue of trust and promises.

All these have trust assumptions

Source: https://patrickalphac.medium.com/why-we-web3-bd21a5570019

Chainlink

What is the purpose of Blockchain?

- “Unbreakable Promises”
  - Blockchain technology allows us to create agreements and promises that are effectively unbreakable, similar to the childhood ritual of the pinky swear.
  - Just as the pinky swear signified an unbreakable vow between friends, blockchain provides the tools to make trusted, permanent agreements.
  - Blockchain gives us the capability to establish commitments that do not require absolute trust between parties.
  - In a sense, we now have the technology to make pinky swears - symbolic unbreakable promises - actually binding and permanent.
  - Blockchain enables “**trust-minimized agreements**” that were not feasible before.

Source: https://en.wikipedia.org/wiki/Pinky_swear

Chainlink

What is the purpose of Blockchain?

- “Trust. Minimized. Agreements”
  - **Nick Szabo:** The man, the myth the legend.
  - His paper on Bit Gold and his conception of smart contracts. Bit Gold is seen as the precursor to bitcoin, which **Satoshi Nakamoto (pseudonym)** would go on to refine in **his/her/they** bitcoin whitepaper.
  - **Smart contracts**, Szabo first wrote about back in 1996, enable the execution of cryptocurrency transactions and underpin the viability of the entire field.
  - His philosophy as a whole – is the concept of ‘**trust-minimisation.**’ This posits the theory that, as a species which is optimised to best function in groups of no more than 150 individuals, we need to develop ways in which the need to trust strangers is kept to a minimum.
  - Quite simply, there wouldn’t be crypto without Nick Szabo’s work.

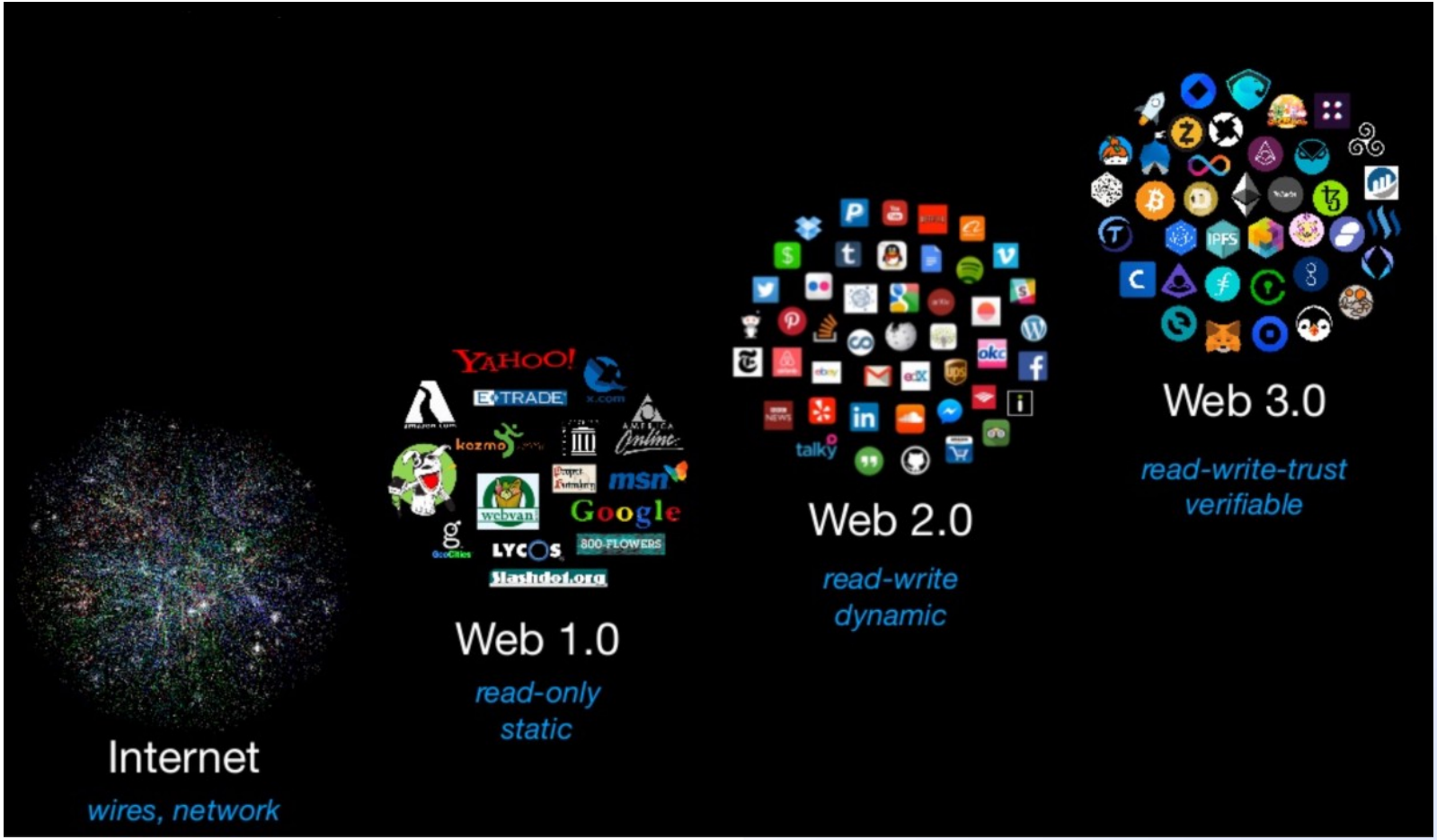
Source: https://www.coinbureau.com/analysis/who-is-nick-szabo/

What is the purpose of Blockchain?

- “Cryptographic Truth”
  - **Sergey Nazarov:** co-founder of Chainlink, a leading decentralized oracle network.
  - His thesis: Cryptographic truth will reshape societal agreements.
  - Blockchain technology creates a tamper-proof ledger.
  - Cryptographic truth can revolutionize trust and enforcement of agreements.
  - Benefits: Increased security, efficiency, transparency and accessibility.
  - Applicable to various domains: finance, supply chains, voting systems, legal contracts.
  - The 4 pillars of good goverance.
  - Sergey Nazarov and former Google CEO Eric Schmidt discussing the future of **Web3**.

Source: https://blog.chain.link/smartcon-2022-recap/

Chainlink



Source: https://www.linkedin.com/pulse/evolution-web-how-web3-changing-internet-we-know-ryan-kirkley/

Chainlink

What is a Smart Contract?

DEFINITION

A smart contract is a tamper-proof program that runs on a blockchain network when certain predefined conditions are satisfied.

- A smart contract is an agreement that is deployed to a decentralized blockchain, and unlike traditional agreements, once a smart contract is deployed, it:
  - Cannot be altered (is immutable)
  - Automatically executes
  - Everyone can see the terms of agreement

Source: https://chain.link/education/smart-contracts

Chainlink

What is SHA-256?

A secure hashing algorithm or commonly referred to as SHA-256, is an unkeyed cryptographic hashing function that takes an input of variable length and produces a 256-bit long hash output.

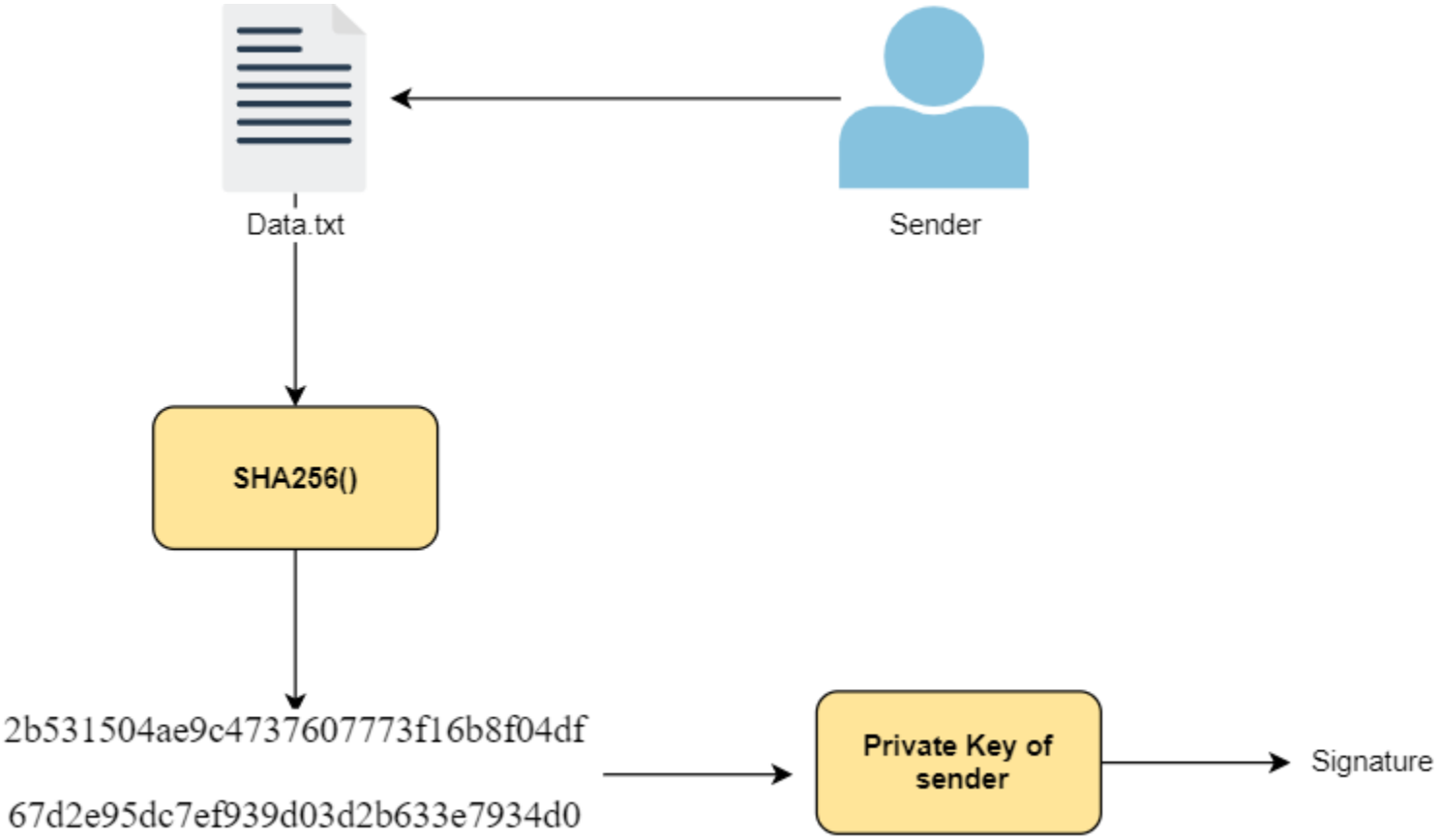
Uses of SHA-256 in blockchain

SHA-256 is one of the first and most prominently used hashing algorithms in blockchains like Bitcoin, Bitcoin Cash, and Bitcoin SV. SHA-256 is used in various stages in a blockchain, most prominently:

- **Consensus mechanism:** Miners calculate the hash of new blocks to be created using SHA-256 by varying the value of nonce in a bitcoin block until they reach the hash below the threshold. Then that block can be accepted into the ledger.
- **Chains of blocks:** Each block in the ledger contains a hash generated by SHA-256 referring to the preceding block in the chain.
- **Digital signatures:** Transactions use digital signatures to maintain integrity, the information used in the transaction is hashed using SHA-256, and then it is encrypted with the sender's private key to generate a signature. The miner then verifies this signature to validate the transaction.

Source: https://www.educative.io/

Chainlink


Data.txt
Sender
SHA256()
2b531504ae9c4737607773f16b8f04df
67d2e95dc7ef939d03d2b633e7934d0
Private Key of sender
Signature

Chainlink

Cryptographic Truth is Strictly Better than “Just Trust Us”

”Just Trust Us” Paper Promises

- Control is completely given away
- Counterparty risk is high and opaque
- Transparency is purposefully removed

Cryptographic Truth Guarantees

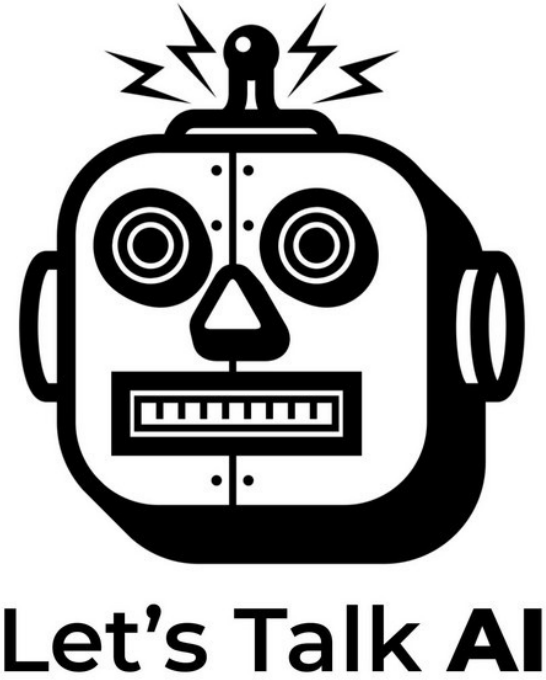
- Control is in the user’s hands
- Counterparty risk is low and transparent
- Transparency is unavoidably built-in

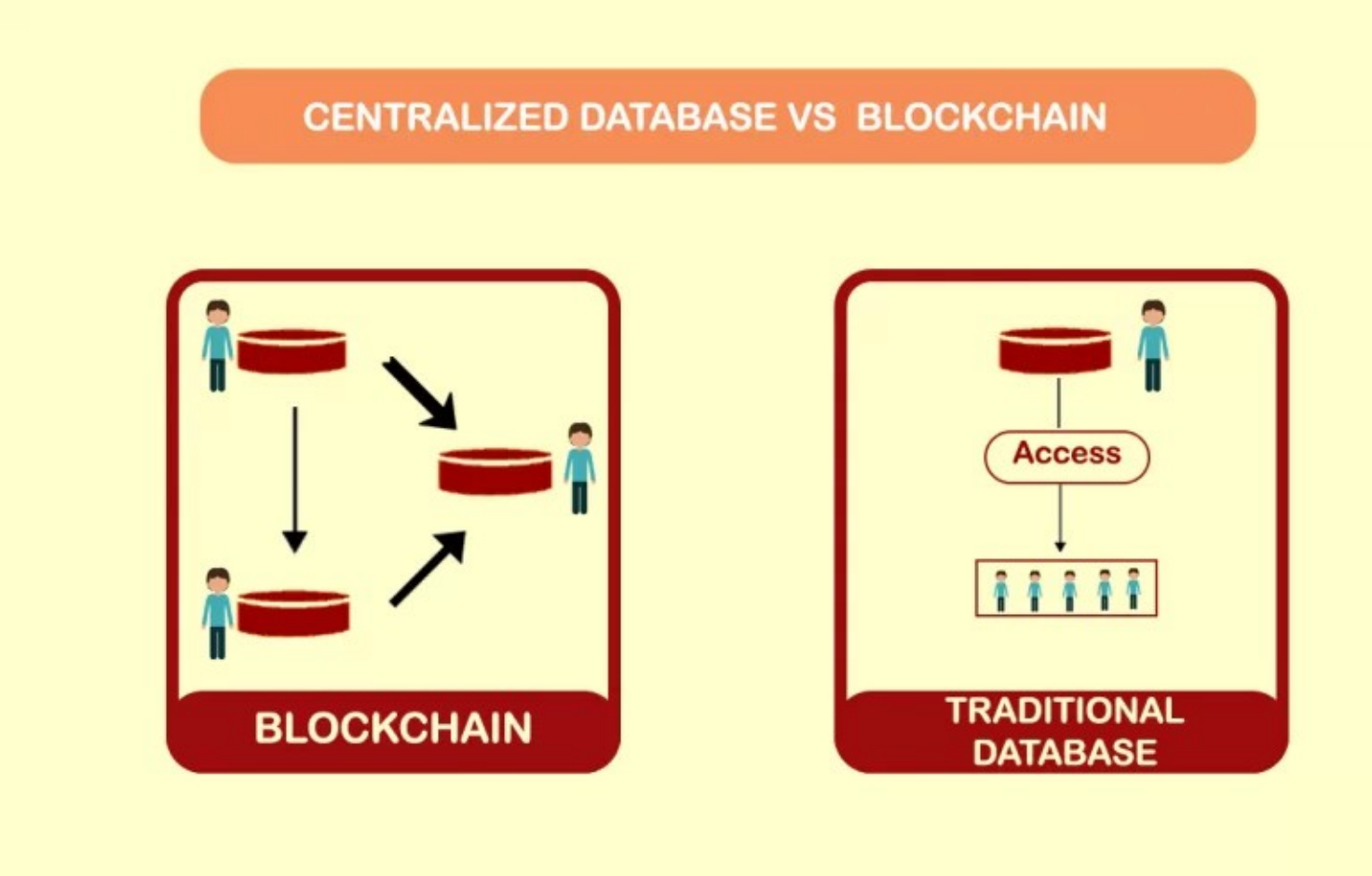
Chainlink

Chainlink

How does Blockchain work?

- The 4 Generals Problem and Byzantine Fault Tolerance are two concepts related to distributed systems and consensus algorithms.
  - So, let’s ask AI?
    - **Prompt>** Hello AI, can you explain the relativity of the 4 generals problem and Byzantine Fault Tolerance to how Blockchain works? Step by Step
    - **Prompt>** Thank you AI, can you give me a breakdown of how blockchain works? Step by step



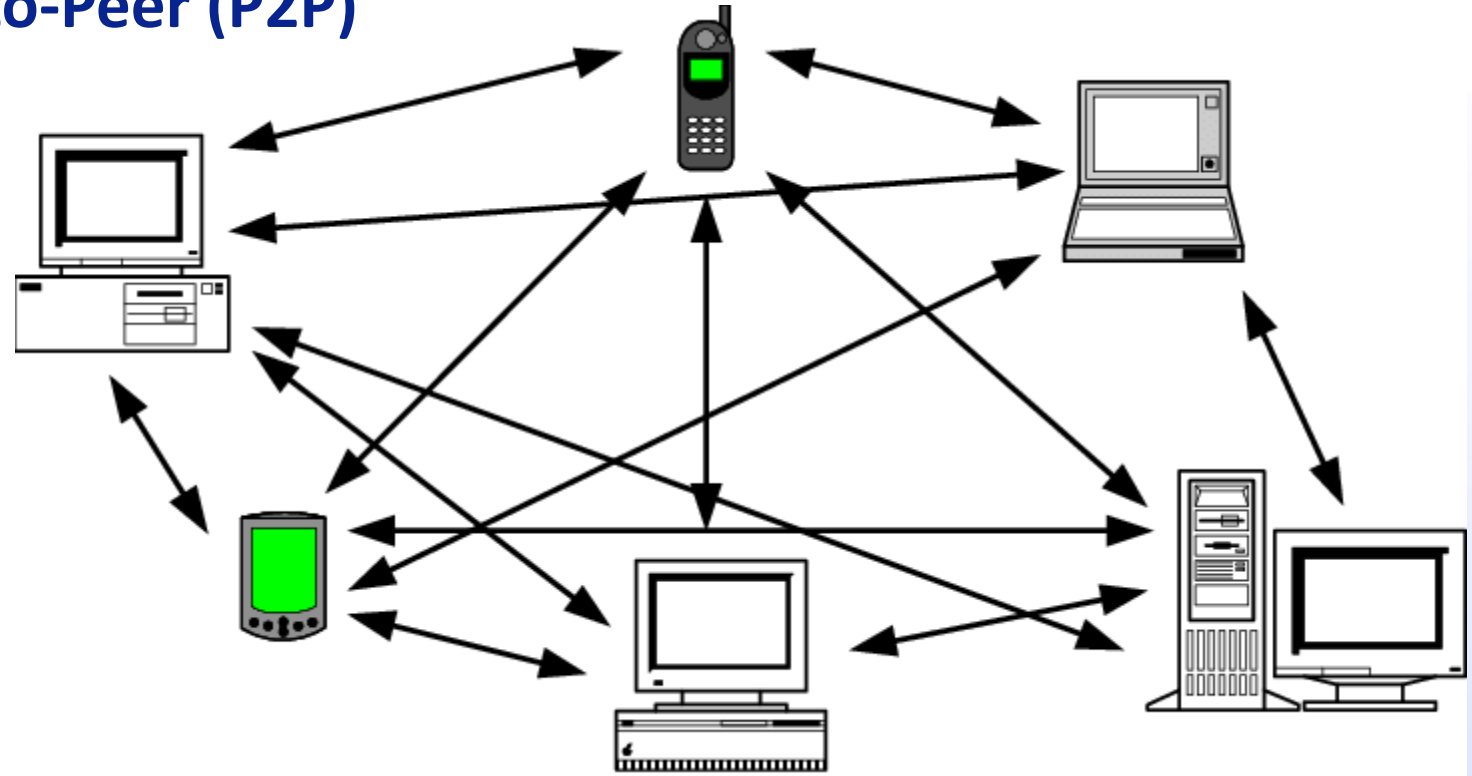


Source: https://hashstudioz.com/blog/what-should-a-startup-choose-between-blockchain-and-a-traditional-database/

Chainlink

How does Blockchain work?

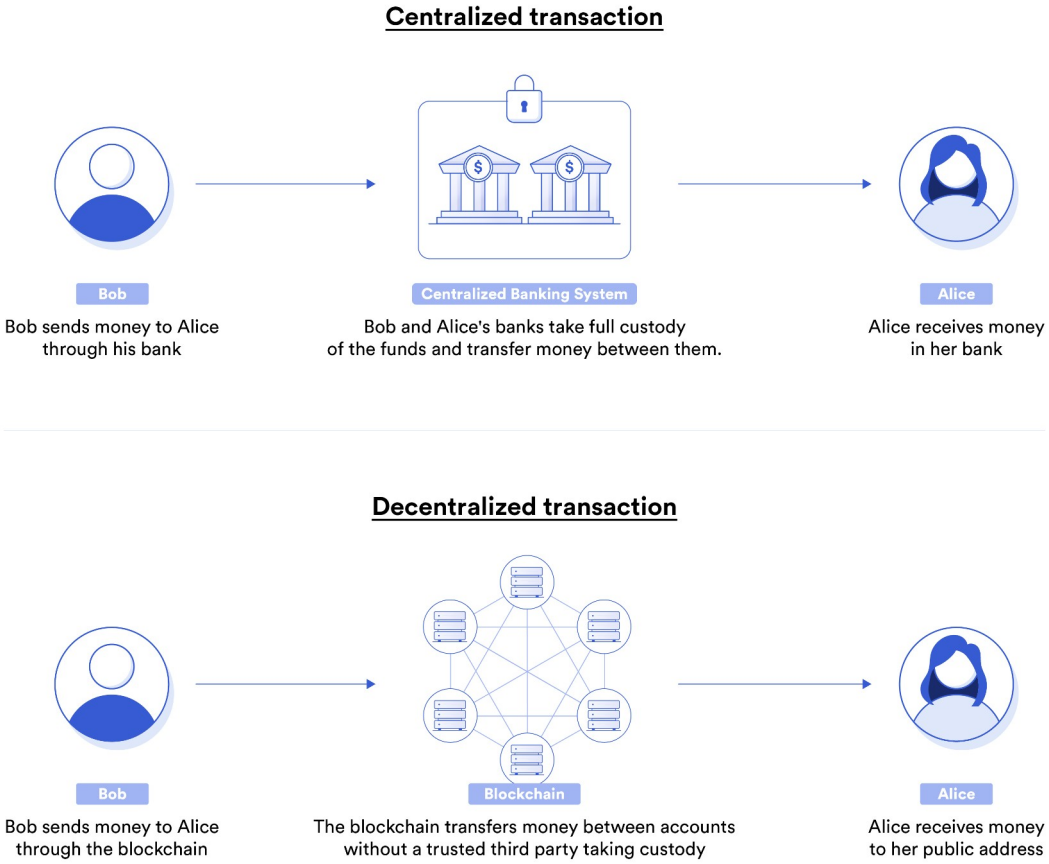
Peer-to-Peer (P2P)



Source: https://www.researchgate.net/publication/2605250_A_distributed_value-oriented_XML_Store

Chainlink

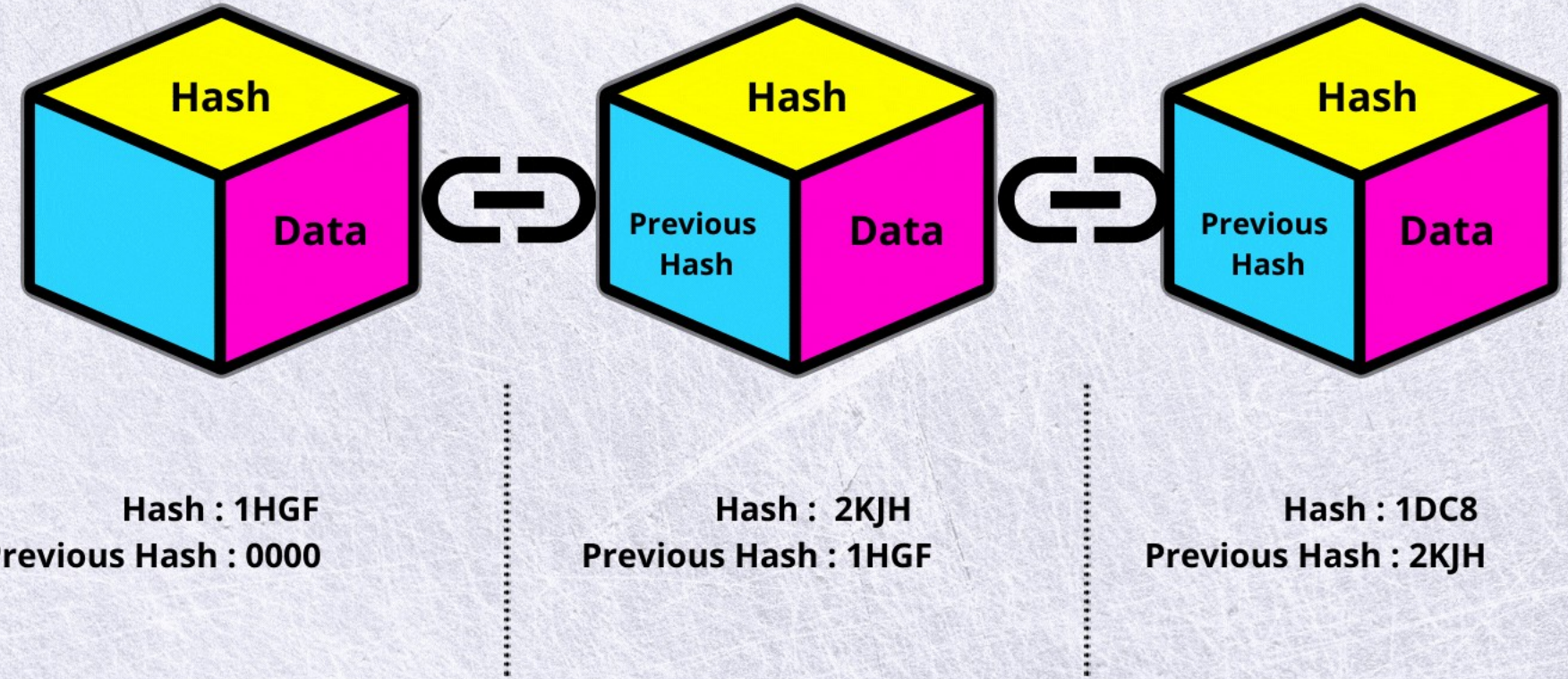
How does Blockchain work?



Source: https://chain.link/education-hub/blockchain

Chainlink

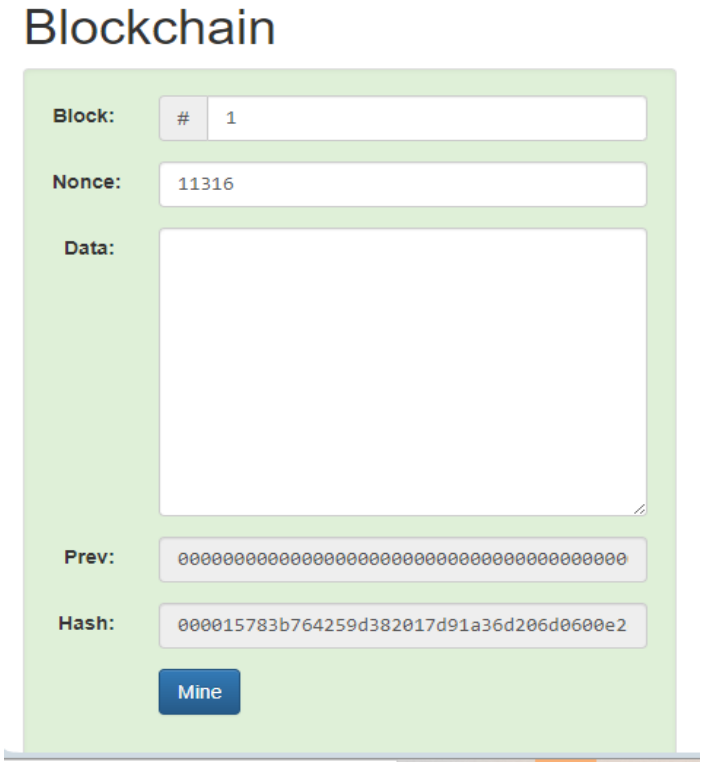
Genesis Block



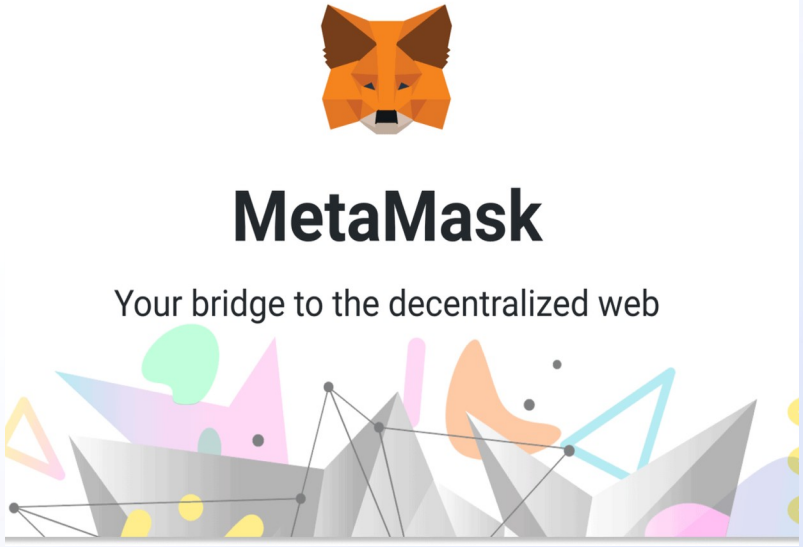
Source: https://medium.com/the-crypto-block/8-concepts-that-will-help-you-understand-blockchain-technology-c51b0941bf19

Practical Session

- Blockchain Demo - https://demoblockchain.org/hash



- MetaMask - https://metamask.io

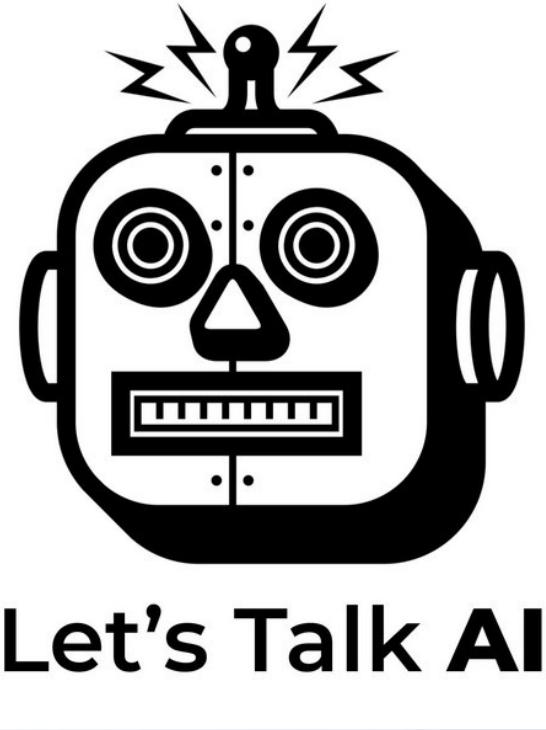


Chainlink

Chainlink

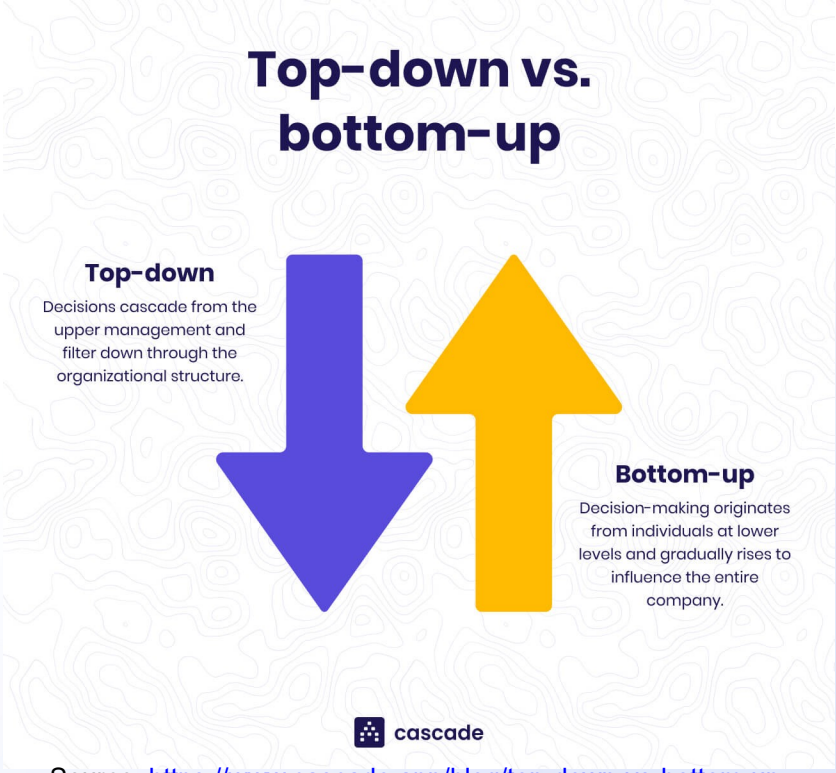
Applications of Blockchain

- What is Adoption?
  - So, let’s ask AI?
    - **Prompt>** Hello AI, can you explain the meaning of “Adoption” in an organisation? Step by Step



Applications of Blockchain

- What is Adoption?
  - **Accepting**
  - **Emracing**
  - **Starting to use something (Ultimate Decision)**



Source: https://www.cascade.app/blog/top-down-vs-bottom-up

Meaning of Adoption in an Organisation

Chainlink

Meaning of Adoption in an Organisation

Chainlink

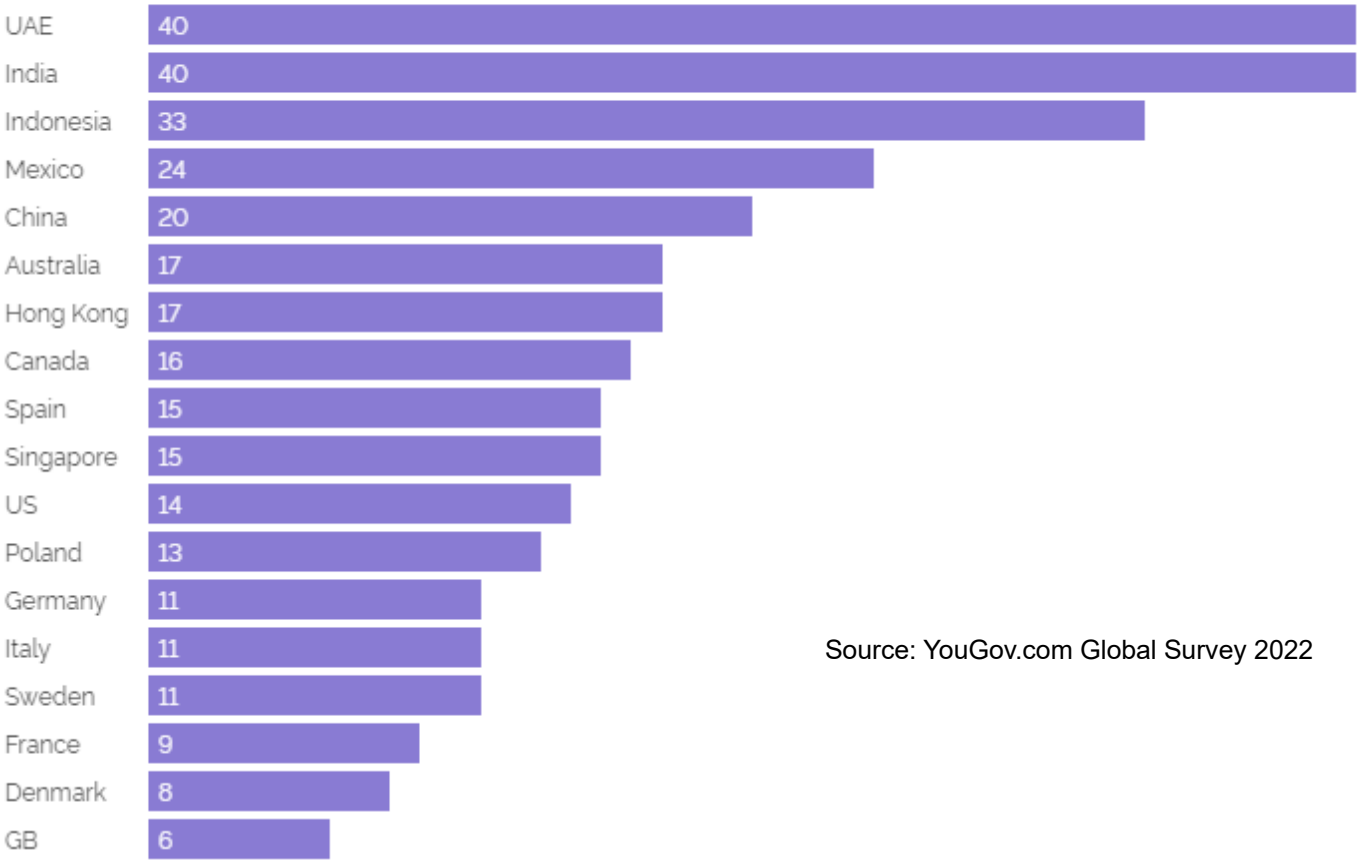
MARCH 30TH, 2022, SONIKA CHOUBEY

Two-thirds of UAE adults are interested in cryptocurrency, with young adults showing most interest

Source: https://business.yougov.com/content/41850-two-thirds-uae-adults-are-interested-cryptocurrenc

UAE leads the globe in terms of trust in cryptocurrencies

To what extent would you say you trust each of the following financial services companies?...% of respondents who said they trust cryptocurrency



Source: YouGov.com Global Survey 2022

Chainlink

Blockchain in the UAE government

Blockchain is a shared immutable real-time ledger for recording the history of financial transactions, contracts, physical assets, supply chain info, etc. The UAE Government adopted blockchain technology in conducting its transactions. To aid this move, it launched the Emirates Blockchain Strategy 2021 and Dubai Blockchain Strategy. Dubai Future Foundation established the Global Blockchain Council to explore, discuss current and future applications and organise transactions through the blockchain platform.

Source: https://u.ae/en/about-the-uae/digital-uae/digital-technology/blockchain-in-the-uae-government

AWARENESS.

"Dubai [will be] the first city fully powered by Blockchain"

3 strategic pillars
Government Efficiency,
Industry Creation,
International Leadership.

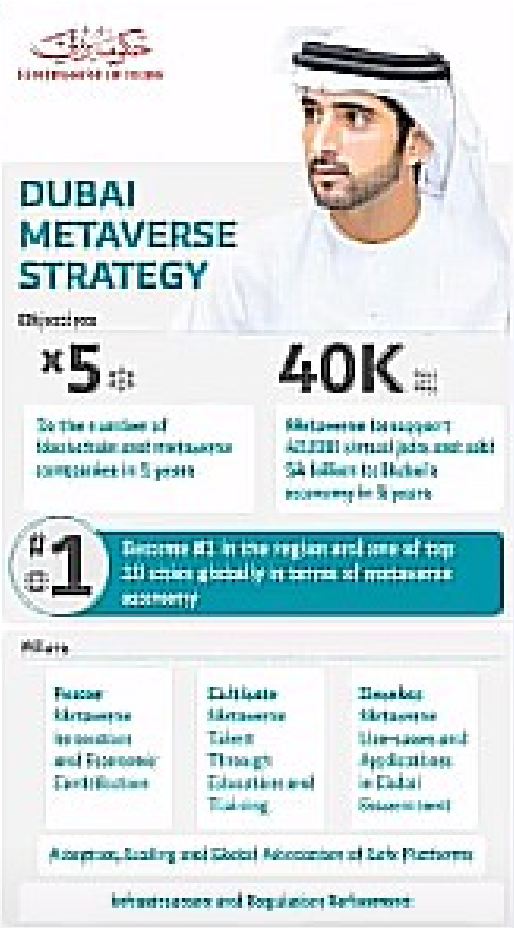
دبـــــي الرقمية
DIGITAL DUBAI

Dubai wants to become a global tech hub – and it's betting on crypto to get it there

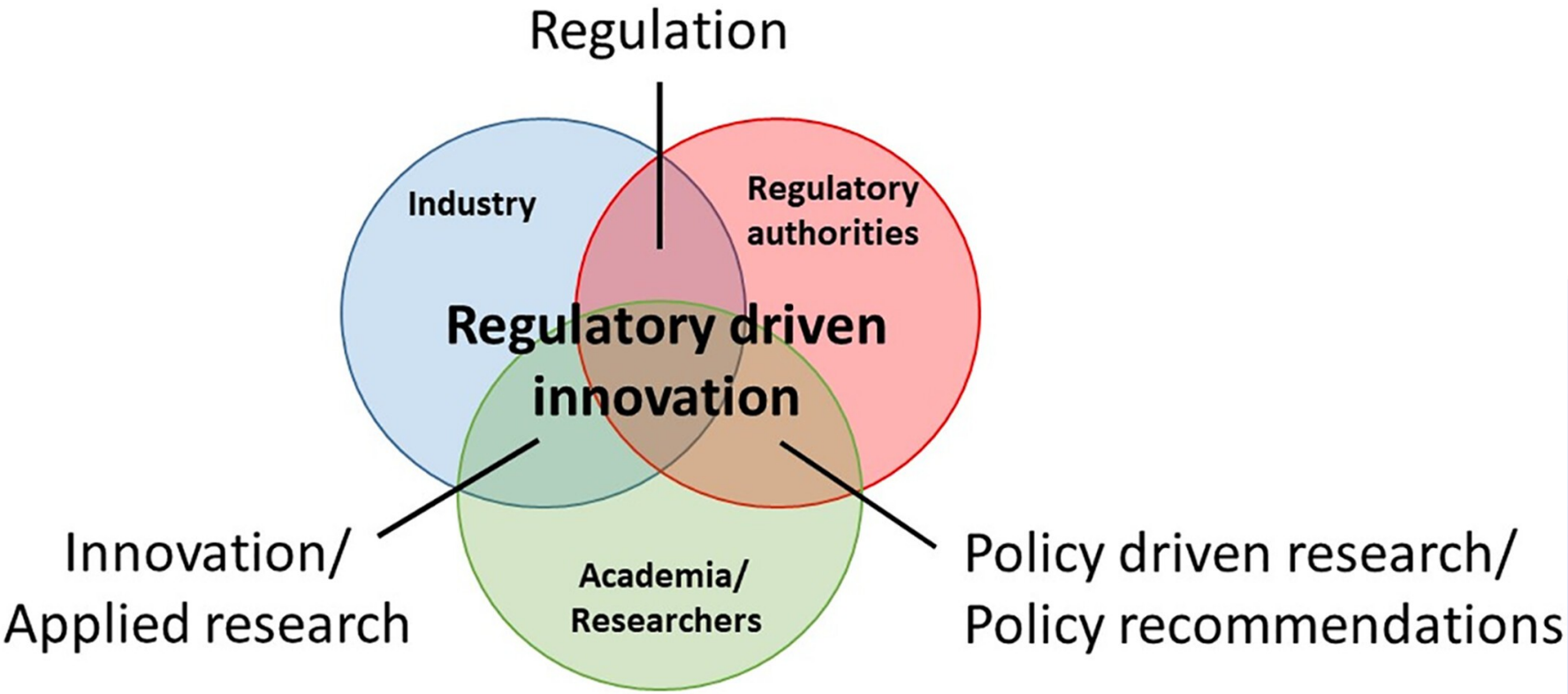
Mena region is 'world's fastest-growing cryptocurrency market'

Dubai's Future Blockchain Summit to create global business opportunities for Web3 innovators

UAE's Future Blockchain Summit to address all things Blockchain in Dubai from tomorrow



Chainlink



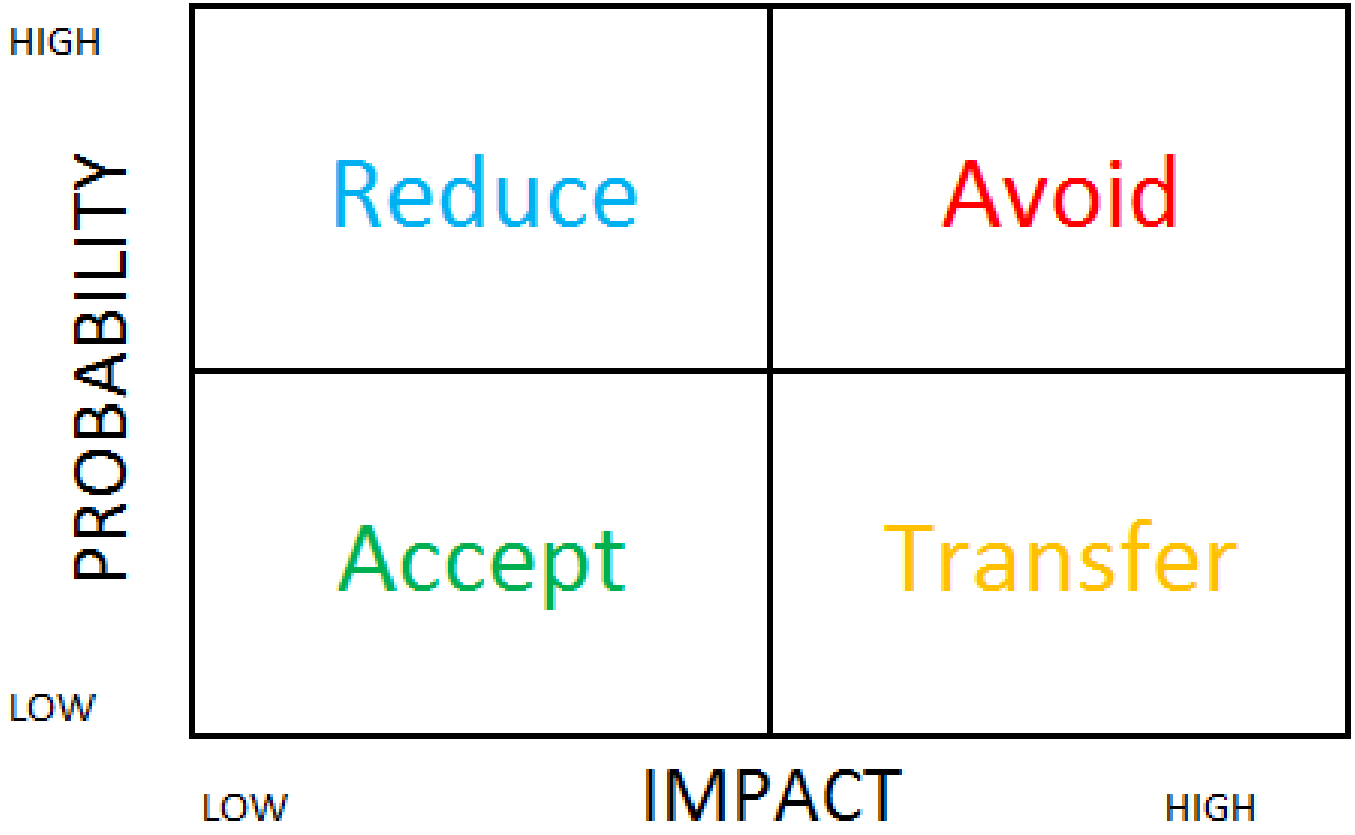
Source: The innovation triple helix depicting the processes of regulatory driven innovation. Modified from Zhou and Etzkowitz (2021)

Chainlink

Meaning of Adoption in an Organisation

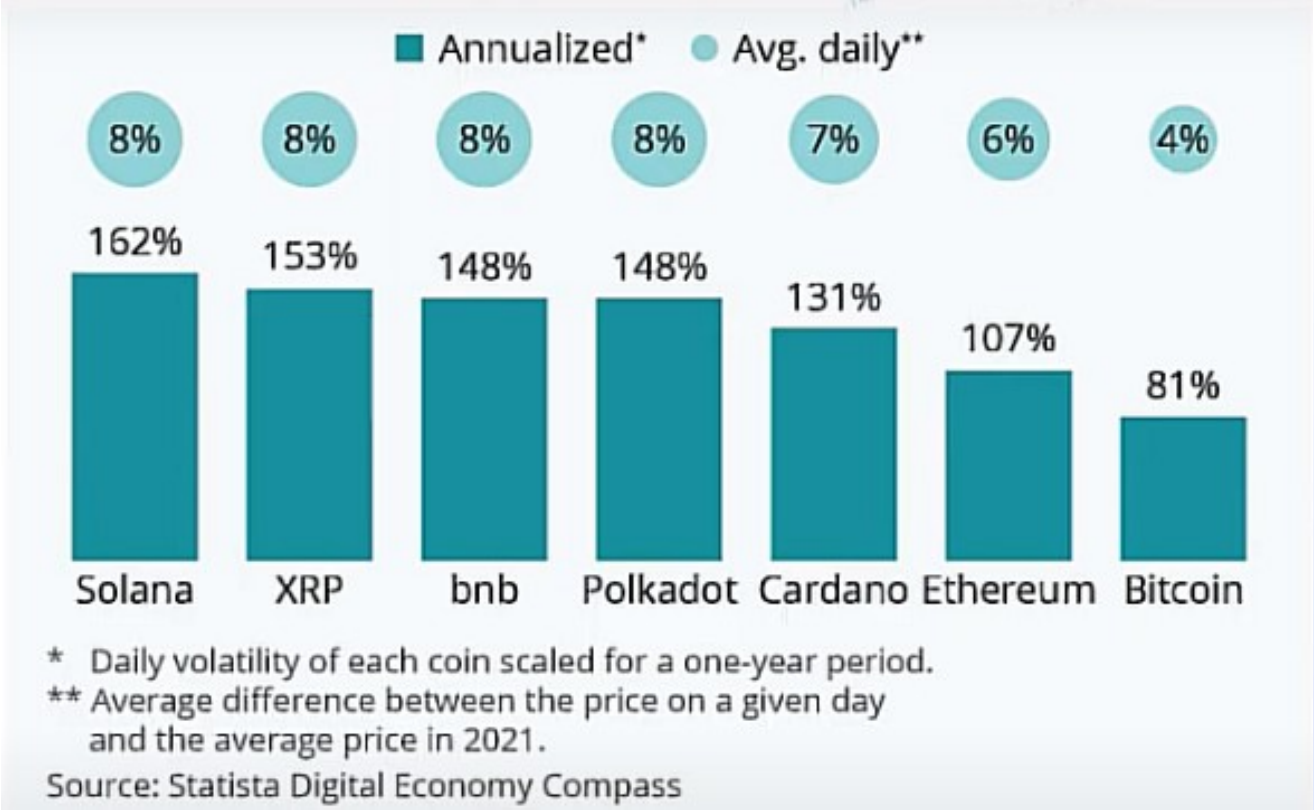
Chainlink

The TARA framework is a tool that can be used to assess and manage risk



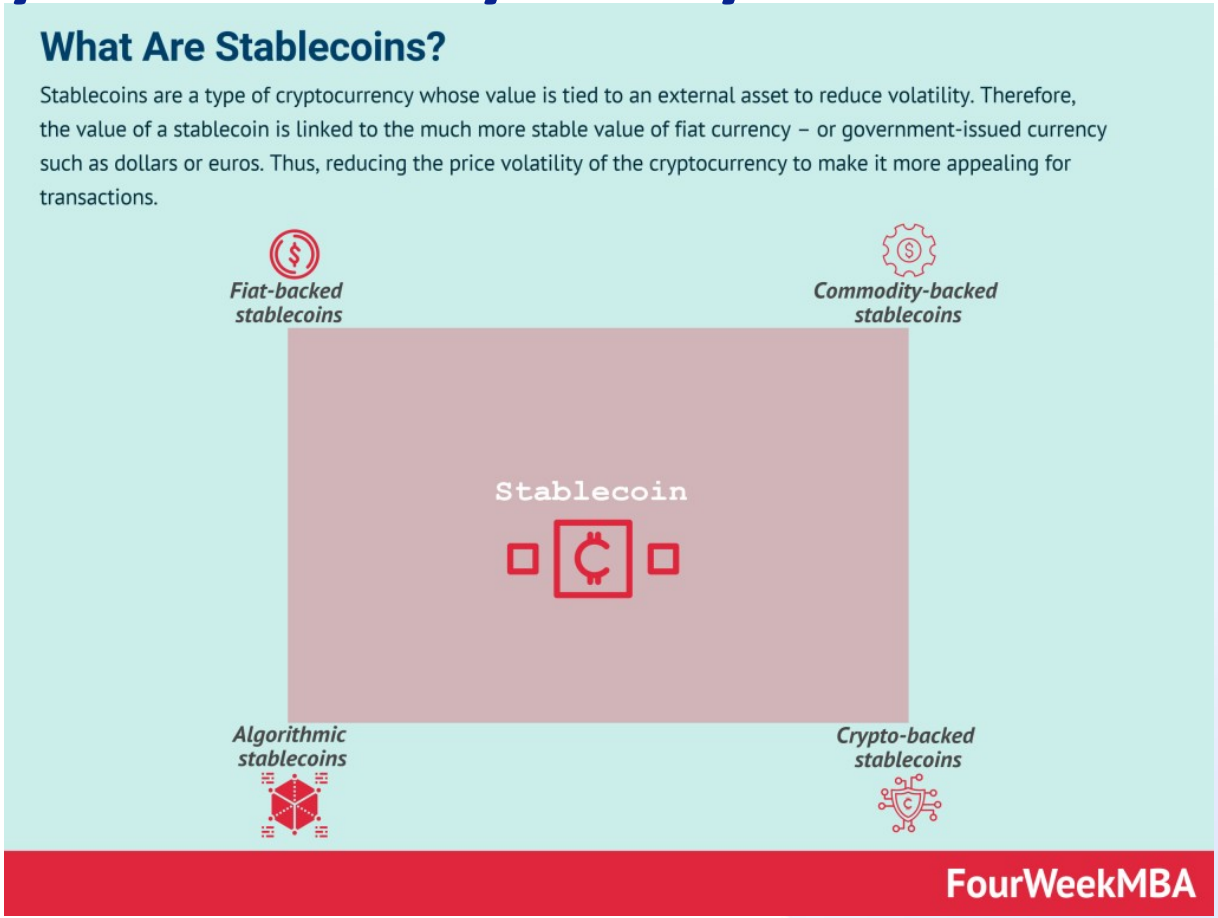
Chainlink

Volatility is the enemy of any business



Chainlink

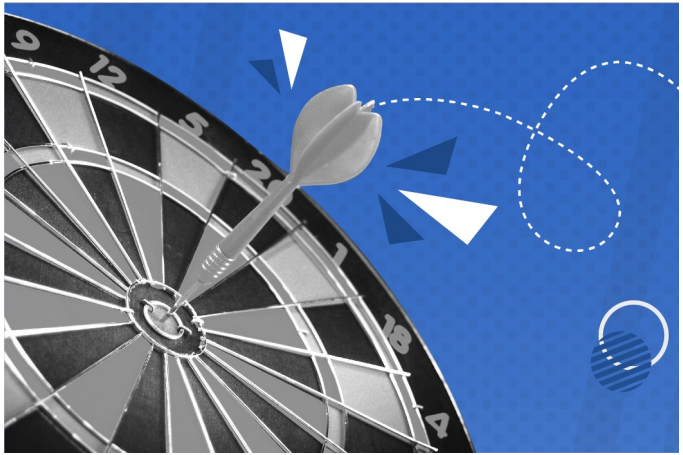
Volatility is the enemy of any business



Chainlink

Avoid High Risky Projects

- Organisations will adopt Blockchain Projects that are:
  - **Low Risk**
  - **Closer to the Core**



Chainlink

Meaning of Adoption in an Organisation

Chainlink

Three Stages of Adoption

precise information on how your operating strategies are working

Discovery

integration and refinement of business processes to drive the generation and protection of profits

Enhancement

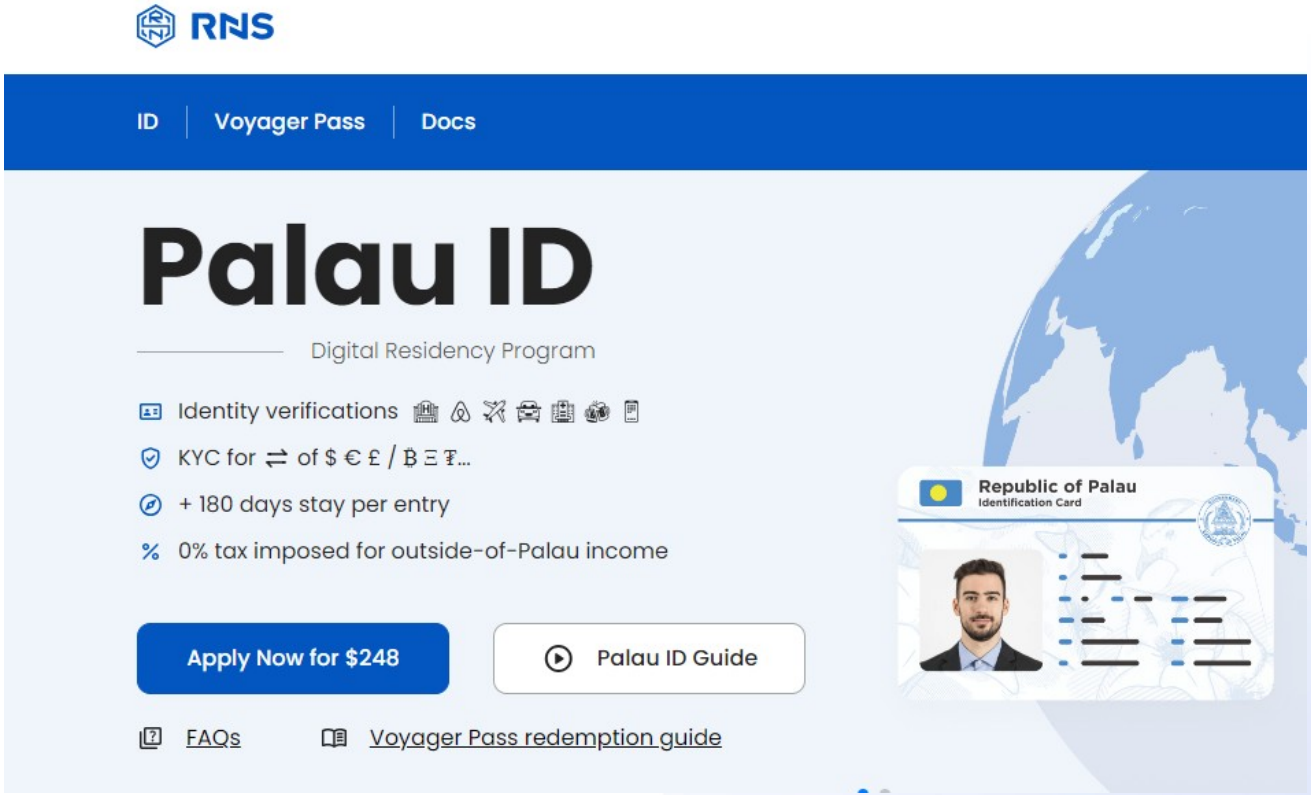
analyzing and measuring the impact of possible changes to the future operation

Innovation

Source: https://blogs.dcvelocity.com/big_data/2014/08/the-journey-understanding-the-path-of-adoption.html

Chainlink

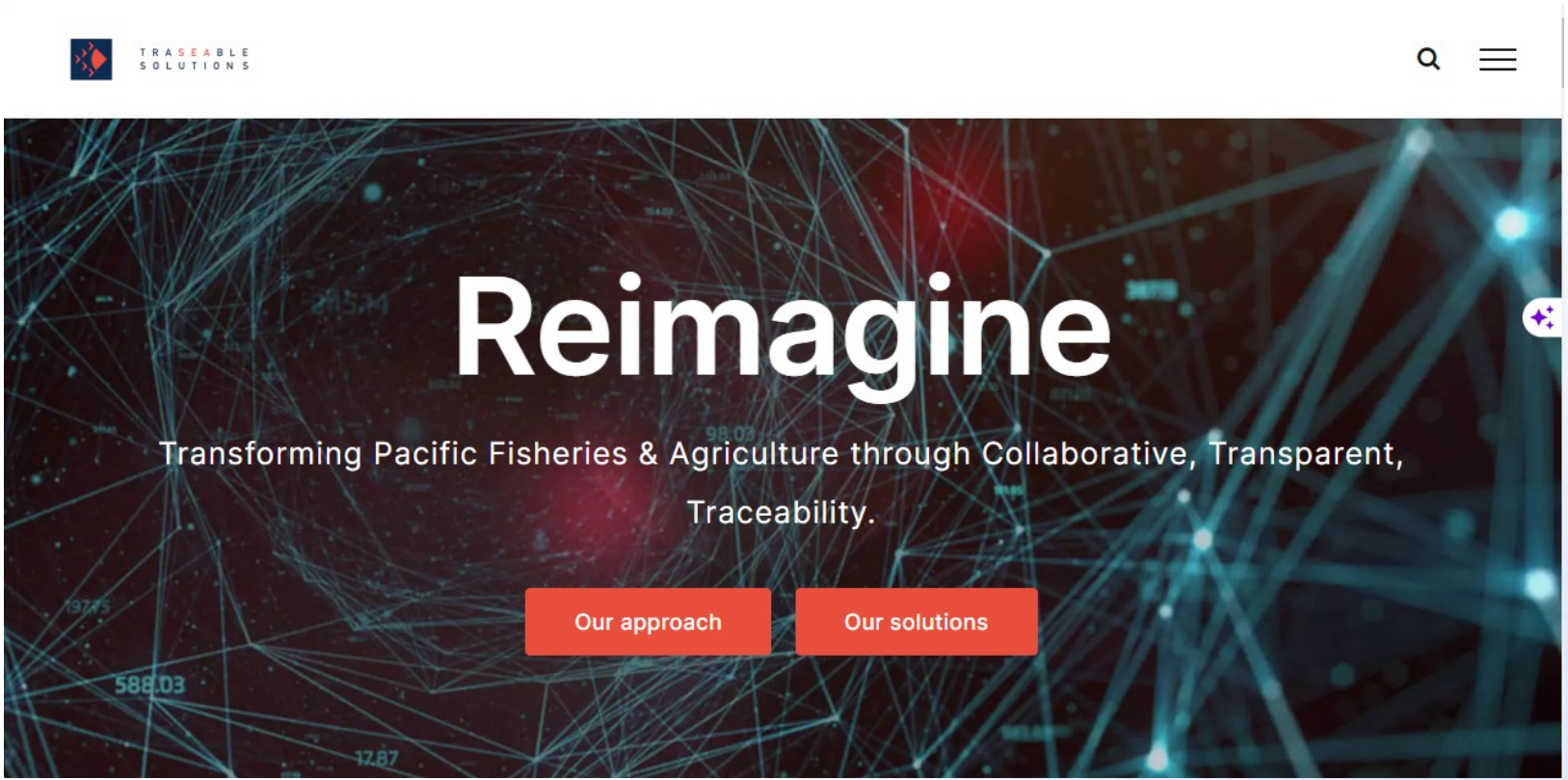
Applications of Blockchain in the Pacific Islands



Source: https://rns.id

Chainlink

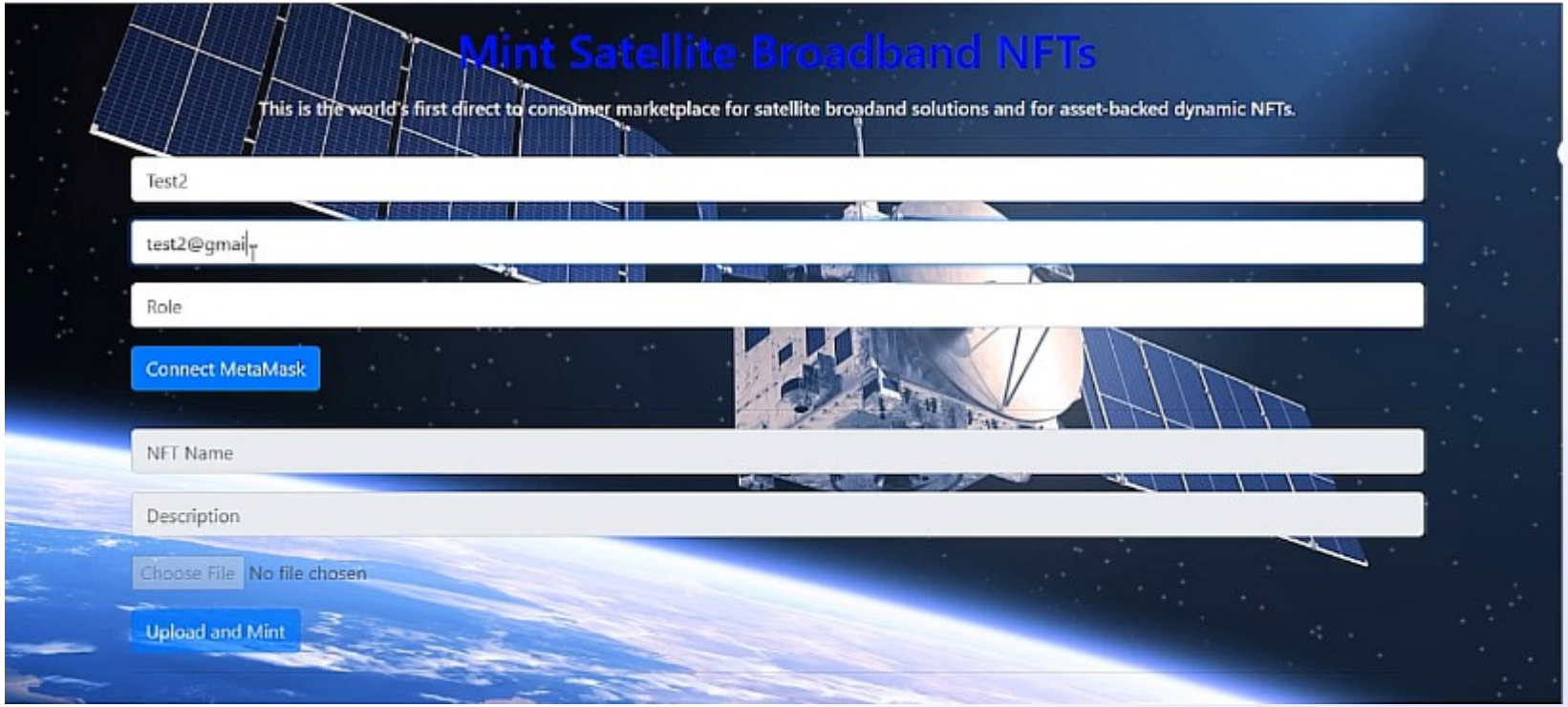
Applications of Blockchain in the Pacific Islands



Source: https://www.traseable.com

Chainlink

Applications of Blockchain in the Pacific Islands

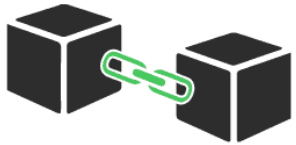


Source: https://devpost.com/software/blockchain-chainlink-satellite-broadband-supply-chain

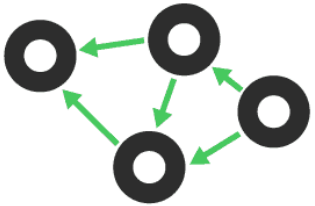
Chainlink

Conclusion

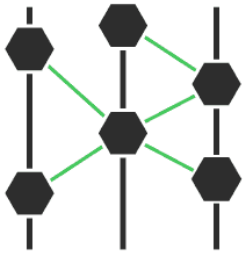
Types Of Distributed Ledger Technologies



Blockchain



Directed Acyclic Graph



Hashgraph

CryptoManiaks
Master the Crypto World

Chainlink

Distributed Ledger Technologies Compared

	Blockchain	DAG	Hashgraph
Transactions per second	7	Potentially unlimited	250,000+
dApps support	Yes	No	No
Tested under real market conditions	Yes	Yes	No
Patented	No	No	Yes

CryptoManiaks
Master the Crypto World

Chainlink

The Properties of Distributed Ledger Technology (DLT)

Programmable
A blockchain is programmable (i.e. Smart Contracts)

Distributed
All network participants have a copy of the ledger for complete transparency

Secure
All records are individually encrypted

Immutable
Any validated records are irreversible and cannot be changed

Anonymous
The identity of participants is either anonymous or pseudonymous

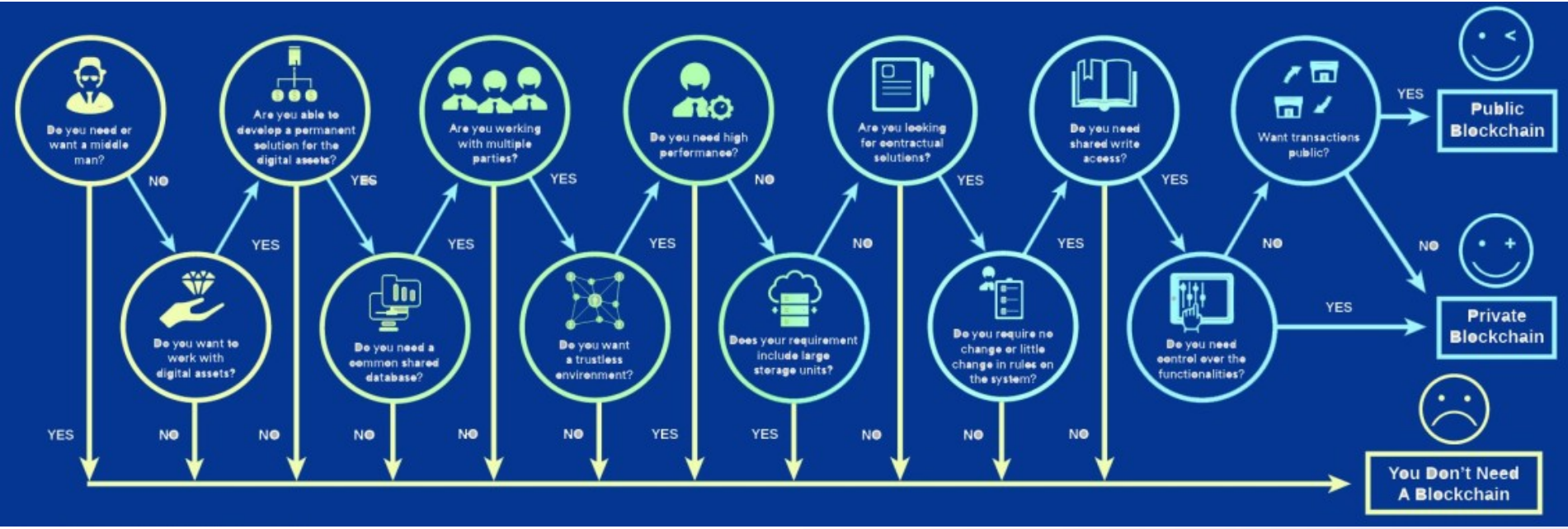
Unanimous
All network participants agree to the validity of each of the records

Time-stamped
A transaction timestamp is recorded on a block

© Euromoney Learning 2020

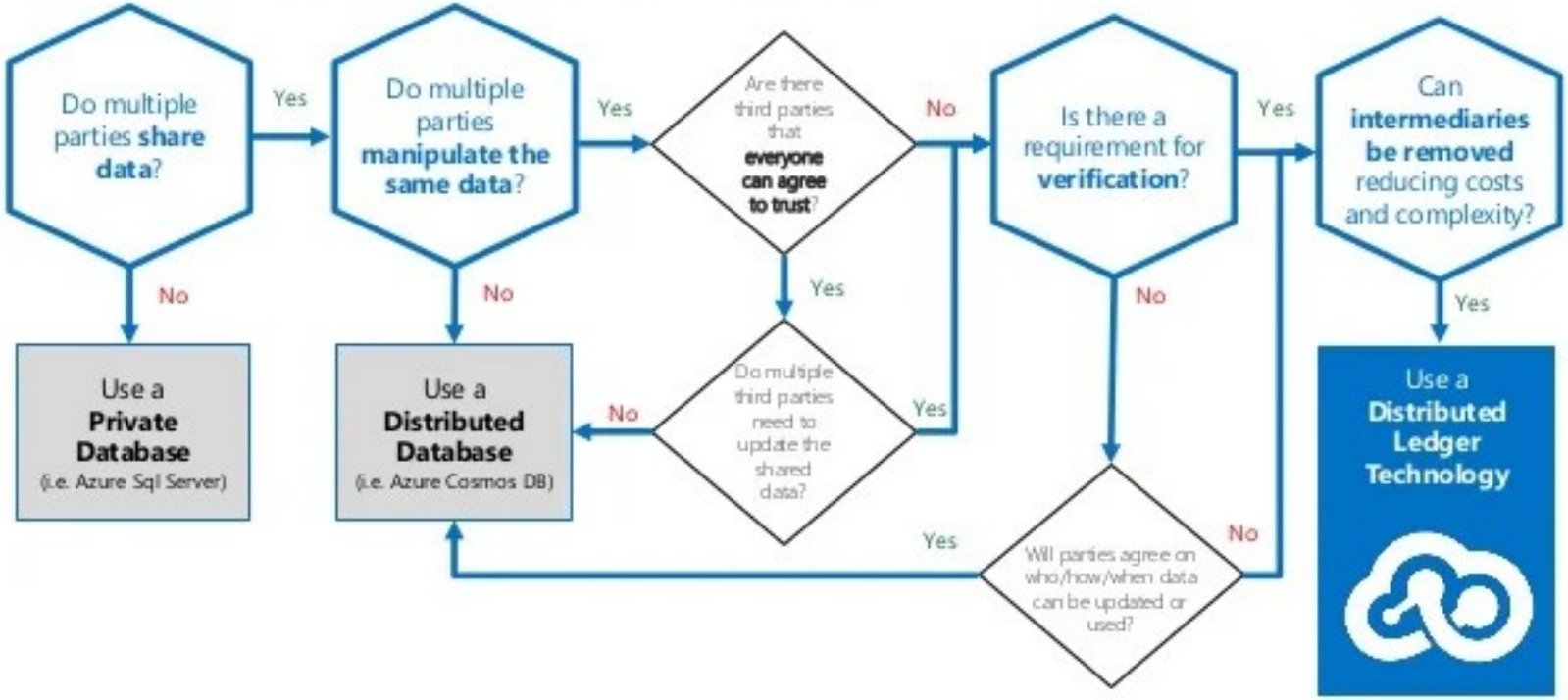
Source: https://phemex.com

Chainlink

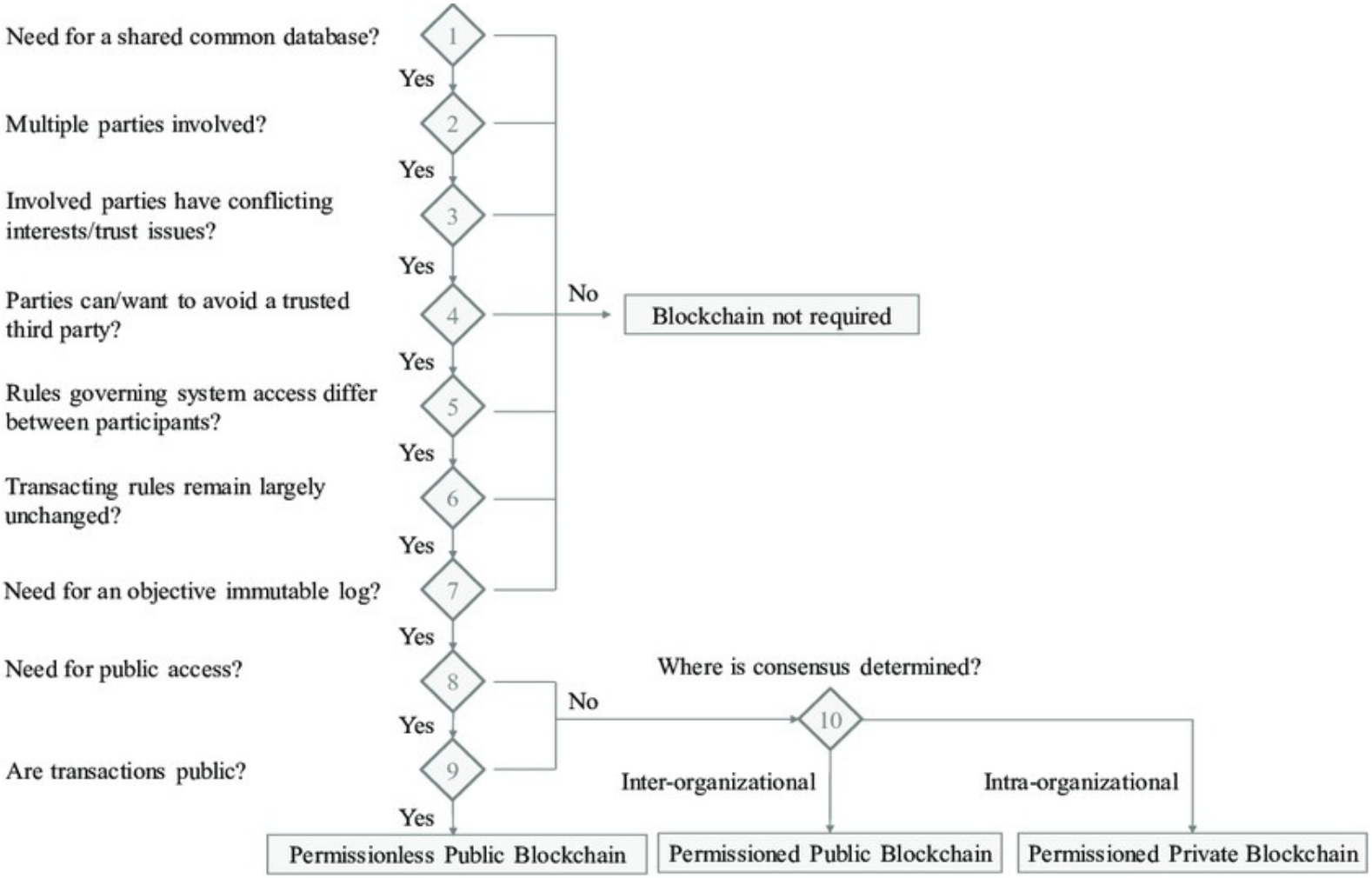


Source: Blockchain Council https://www.blockchain-council.org

When to use blockchain?



Source: https://www.slideshare.net



Source: https://www.researchgate.net/figure/Overview-of-the-Blockchain-Decision-Path_fig5_333545589

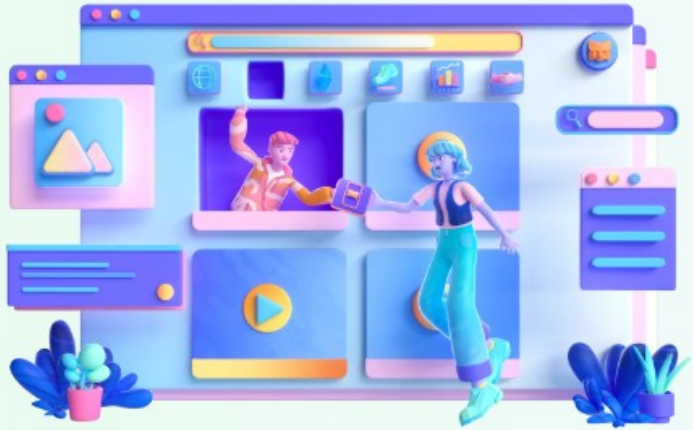
Chainlink

Homework Practical Session – Web3 101

- https://learn.metamask.io/overview

The Web3 101 Course

Our world is increasingly digital and interconnected. It's taking place on devices: our screens are our windows, our data is our identity, and more and more of our lives take place online.

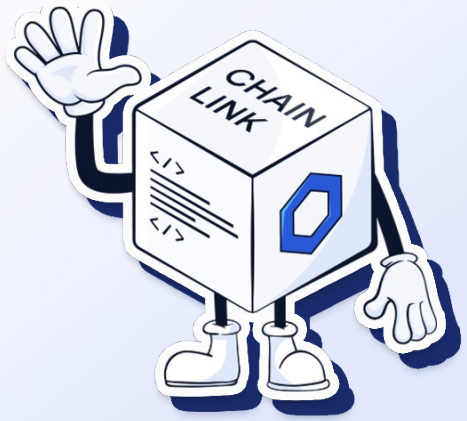


Chainlink

The Genie is out of the bottle

- **Any Web3 Wishes?**

- **Would you like to learn more about Smart Contracts?**
- **Would you like to learn more about Chainlink?**
- **Would you like to learn more about Crypto?**



Chainlink