

Blockchain Introductory Workshop

- Powered by AI



Edwin Liava'a

Chainlink Developer Expert

@EdwinLiavaa

n <u>Edwin.Liavaa</u>



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



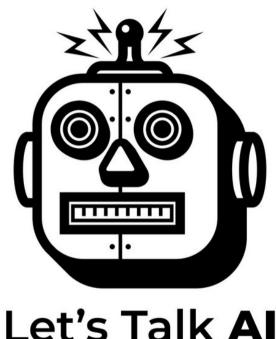
AI – Assistants, Blockchain Tools and Resources

- My GitHub Repo https://github.com/EdwinLiavaa/TWICT-Blockchain-Powered-by-Al-Workshop
- 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



Introduction

- Blockchain, as a distributed ledger technology (DLT), has an interesting history that spans several decades.
 - So, let's ask Al?
 - Prompt> Hello Al, 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 Al, 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



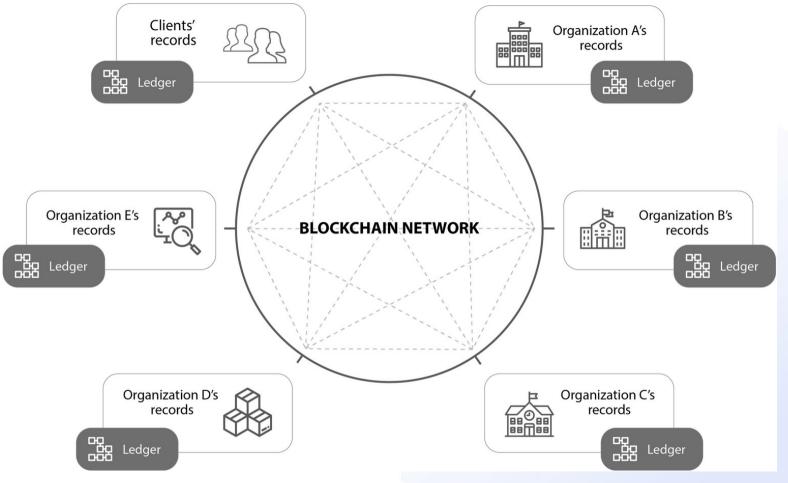
What is Blockchain?

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





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



Bitcoin and the rise of Cypherpunks Key concepts linked timestamping public keys as identities byzantine fault tolerance Satoshi Nakamoto, Bitcoin Launched (Jan 3, 2009) digital cash Satoshi Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System (Oct 31, 2008) proof of work Lehman Bankruptcy (2008) smart contracts Julian Assange, WikiLeaks in (2006) Hal Finney, Reusable Proof-of-work (2004) peer to peer networks 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) Nick Szabo, Smart Contracts (1997) smart contracts — 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) Ocypherpunk's founded by Hughes, May, & Gilmore (1992) Owork & Naor, Pricing via Processing or Combating Junk Mail (1992) proof of work — 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) Iinked timestamping — Balph Merkle, Protocols for public key cryptosystems (1980) RSA Public-key Cryptosystems (1978) Cryptography — Olffie & Hellman, New directions of Cryptography (1976) Cerf & Kahn, TCP/IP (1974) 1970 2015 2020 2025 1975 1980 1985 1990 1995 2000 2005 2010



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



- "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



- "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/



"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.











Web 1.0

read-only static



Web 2.0

read-write dynamic



Web 3.0

read-write-trust verifiable

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



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





What is SHA-256?

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

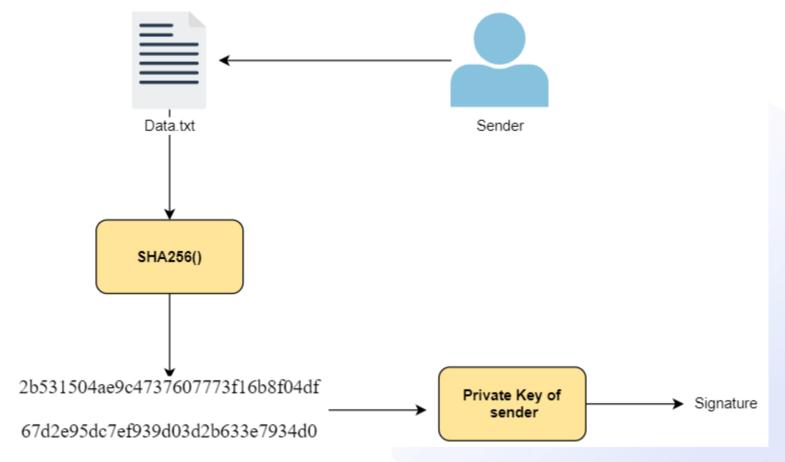
Uses of SHA-256 in blockchain

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/







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

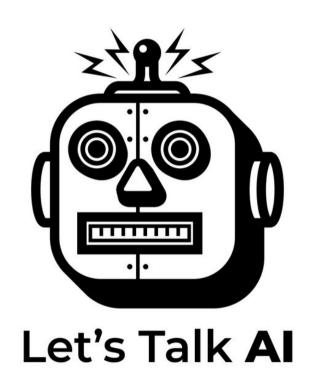






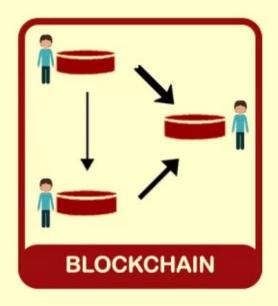
How does Blockchain work?

- The 4 Generals Problem and Byzantine Fault Tolerance are two concepts related to distributed systems and consensus algorithms.
 - So, let's ask Al?
 - Prompt> Hello Al, 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





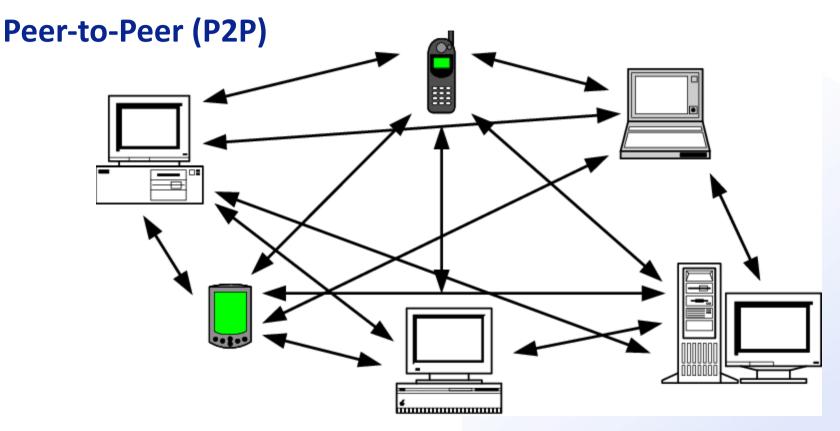
CENTRALIZED DATABASE VS BLOCKCHAIN







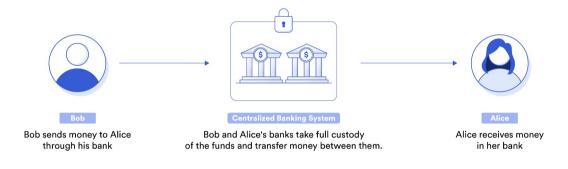
How does Blockchain work?



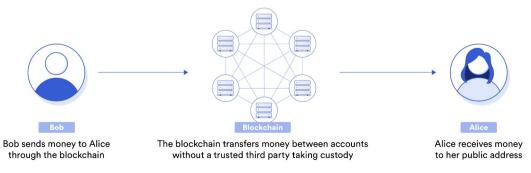


How does Blockchain work?

Centralized transaction



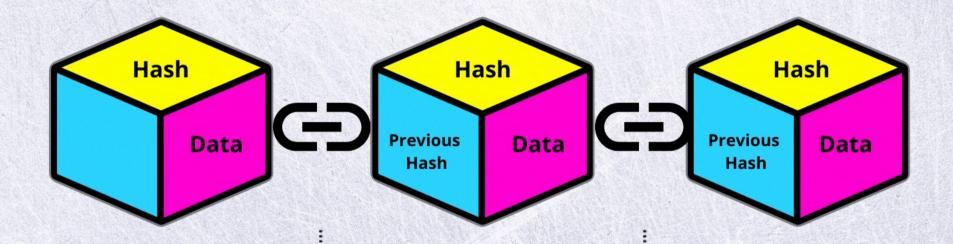
Decentralized transaction



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



Genesis Block



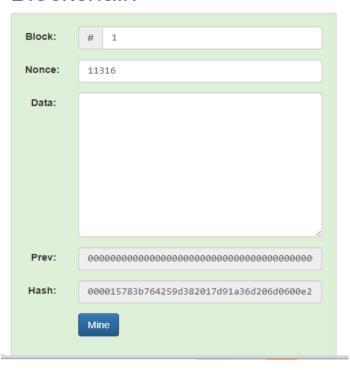
Hash: 1HGF Previous Hash: 0000 Hash: 2KJH Previous Hash: 1HGF Hash: 1DC8 Previous Hash: 2KJH

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

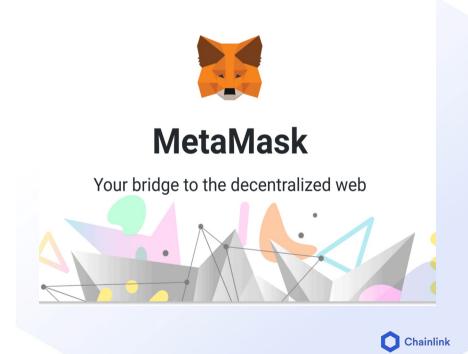
Practical Session

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

Blockchain



• MetaMask - https://metamask.io

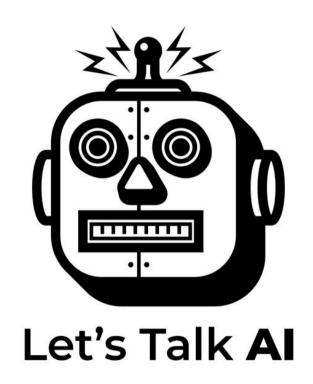






Applications of Blockchain

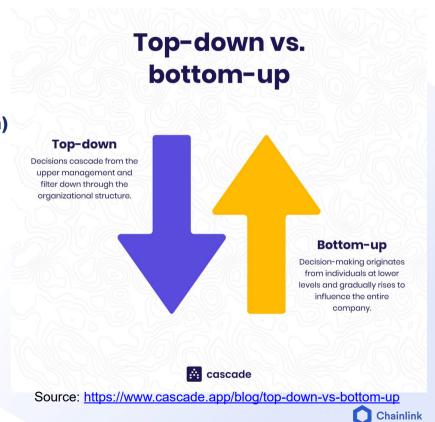
- What is Adoption?
 - So, let's ask Al?
 - Prompt> Hello AI, can you explain the meaning of "Adoption" in an organisation? Step by Step





Applications of Blockchain

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



Meaning of Adoption in an Organisation





Meaning of Adoption in an Organisation





MARCH 30TH, 2022, SONIKA CHOUBEY

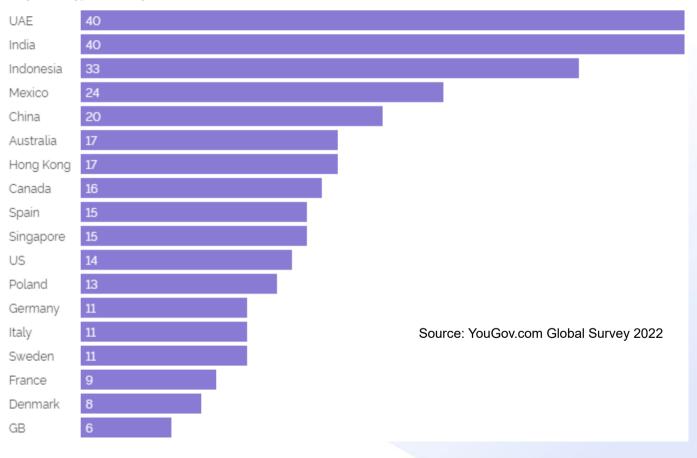
Two-thirds of UAE adults are interested in cryptocurrency, with young adults showing most interest

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







About the UAE > Digital UAE > Digital technology > Blockchain in the UAE government

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.



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

have an extracting a street end and the street and

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

 Advance private in the region assists that is a popular receivable for ED in the SEC country in The research

Duba's Future Blockshain Summit to create global business apportunities for Web I innovators

Contract Contract

UAE's Future Blockcisain Summit to address all things Blockshain in Dubai ham tamonaw

The CDI politicised the Fullian Resolution & second grant to have an imaginary theory of the building best and

-

Depart to Deck







Objects you

×5.

40K

So the number of blocks train and metassyna companies in Signm Alletamente teranggarit Alletti sirrani judis andruski SA lellere terillerbeik populare in Supara

#1)

Encourse #1 in the region and one of top 20 when globally in terms of metaverse expensive

Millery

Editions Measure Edent Through

Education and

The street

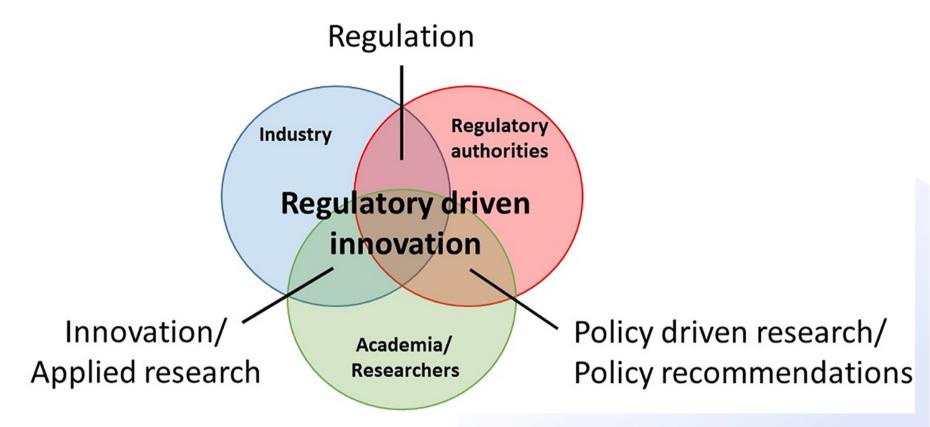
tikrasense Ure-sasen end Appdications in Endai Entonalised

Bear ker

Adoption, Scaling and Christ Management of Link Plantonns

behavioracons and Regulation Refusement.





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

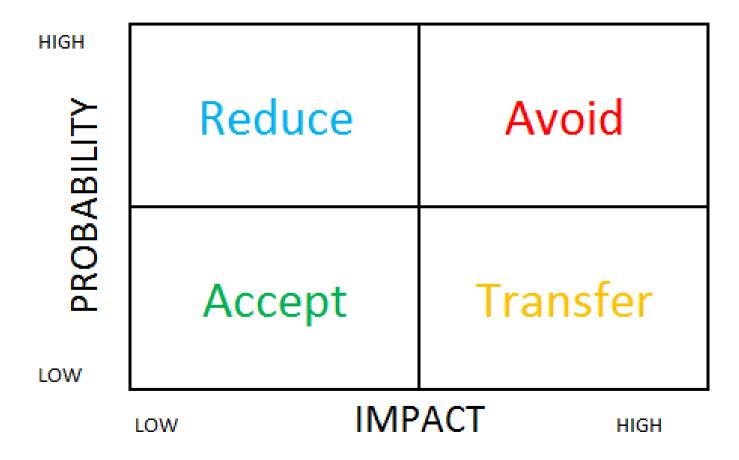


Meaning of Adoption in an Organisation



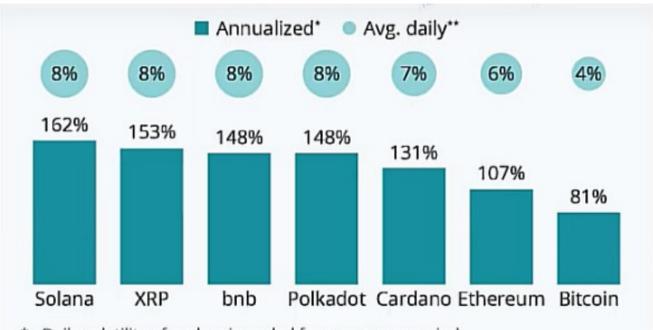


The TARA framework is a tool that can be used to assess and manage risk





Volatility is the enemy of any business



Daily volatility of each coin scaled for a one-year period.

Source: Statista Digital Economy Compass

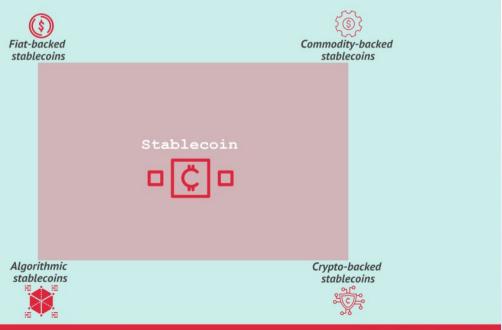


^{**} Average difference between the price on a given day and the average price in 2021.

Volatility is the enemy of any business

What Are Stablecoins?

Stablecoins are a type of cryptocurrency whose value is tied to an external asset to reduce volatility. Therefore, the value of a stablecoin is linked to the much more stable value of fiat currency – or government-issued currency such as dollars or euros. Thus, reducing the price volatility of the cryptocurrency to make it more appealing for transactions.





Avoid High Risky Projects

Organisations will adopt Blockchain Projects that are:

- Low Risk
- Closer to the Core







Meaning of Adoption in an Organisation





Three Stages of Adoption

Value

precise
information on
how your
operating
strategies are
working

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

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

Discovery

Enhancement

Innovation



Applications of Blockchain in the Pacific Islands

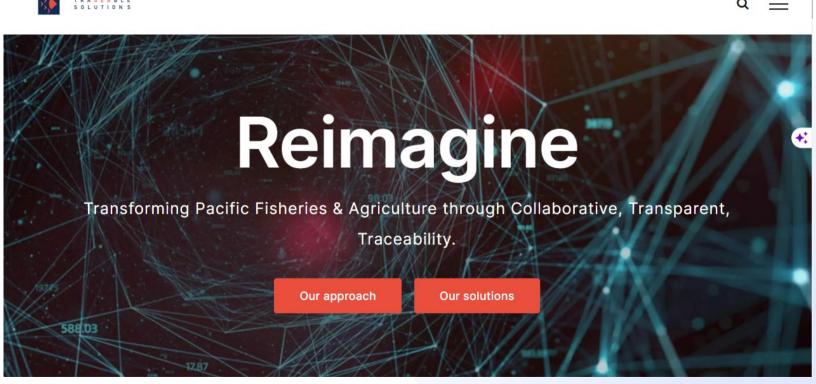
RNS



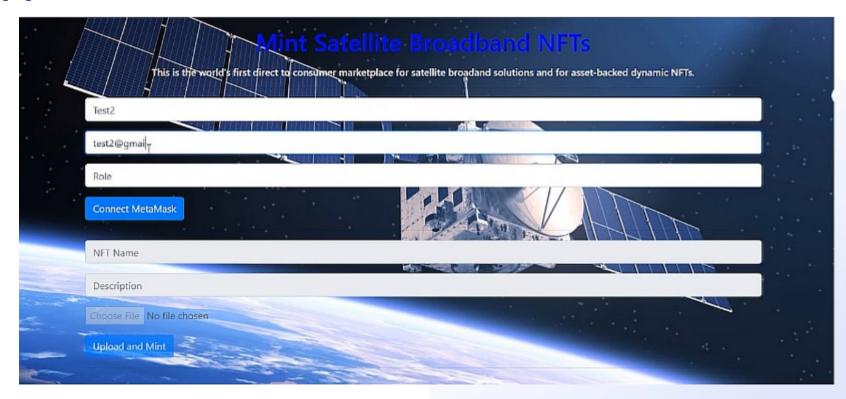




Applications of Blockchain in the Pacific Islands



Applications of Blockchain in the Pacific Islands



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

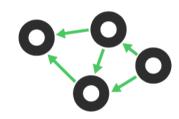


Conclusion

Types Of Distributed Ledger Technologies



Blockchain



Directed Acyclic Graph



Hashgraph





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





The Properties of Distributed Ledger Technology (DLT)

Programmable

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

Secure

All records are individually encrypted

Anonymous

The identity of participants is either anonymous or pseudonymous

Distributed

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

Immutable

Any validated records are irreversible and cannot be changed

Unanimous

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

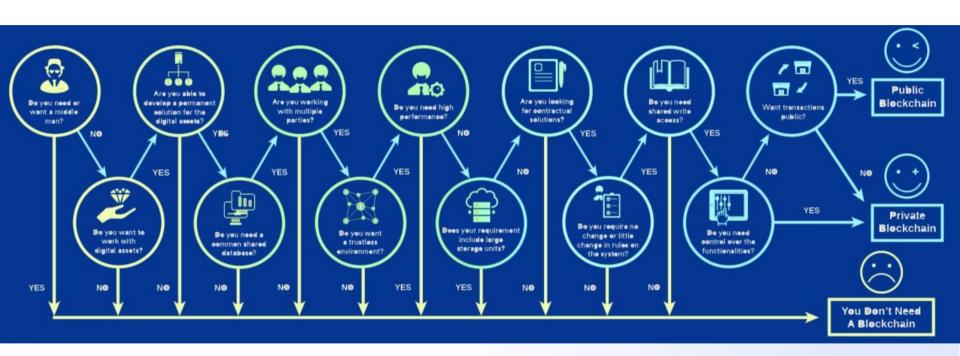
Time-stamped

A transaction timestamp is recorded on a block

© Euromoney Learning 2020

Source: https://phemex.com

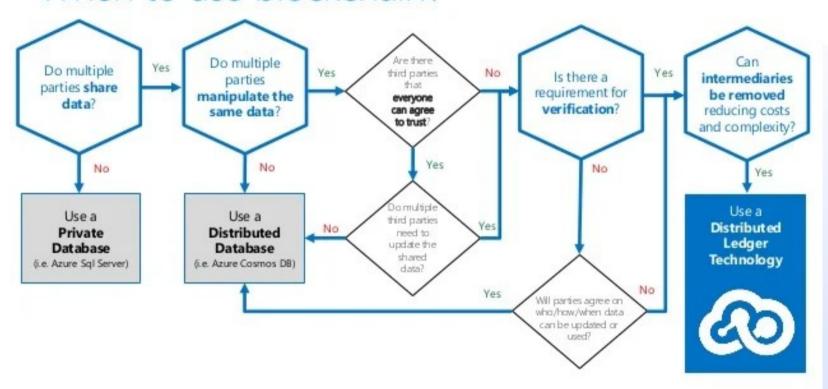




Source: Blockchain Council https://www.blockchain-council.org

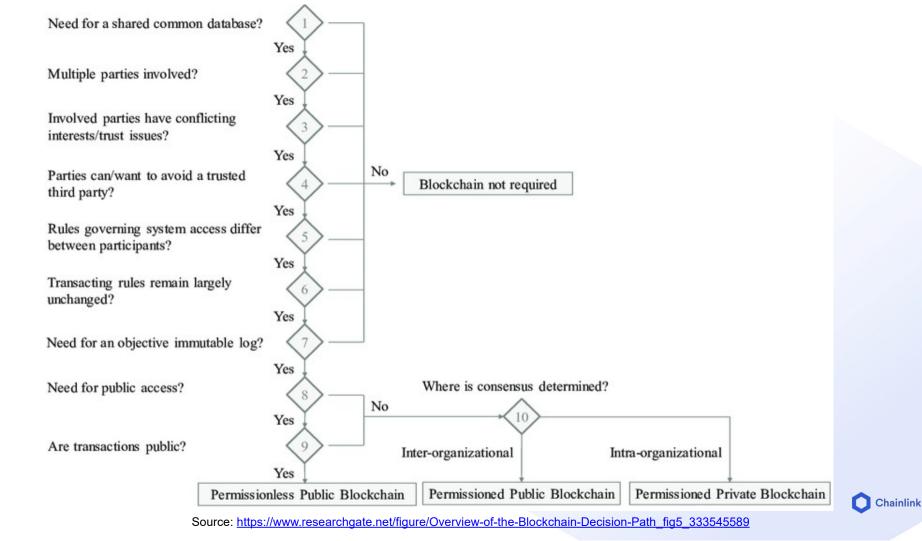


When to use blockchain?



Source: https://www.slideshare.net





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.





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?



