INTRODUCTION:

CRYPTO CURRENCIES, BLOCK CHAIN TECHNOLOGY, VIRTUAL DIGITAL ASSETS & SMART CONTRACTS

Dr.G.S.Phani Kishore IRS
INDIA

DIGITAL CURRENCY (E-Rupee):

{Central Bank Digital Currencies (CBDC)}

- Digital format of fiat currency (Found in wallet/ATM).
- Backed by a Central authority.
  (E-rupee to be launched in Dec-23)
- Value decided by RBI /Govt
- Digital currencies are essentially e-cash

CRYPTO CURRENCY (Virtual Currency)

- Not backed by a central Agency/authority
- Derives its purchasing power from its community of users.
- They are pieces of code created by 'mining'
- Held and managed through a digital ledger called as **blockchain**
- Stored in '**wallets**'
- Transparent procedure from mining to ownership to transfer.
- They have higher degree of cyber security.

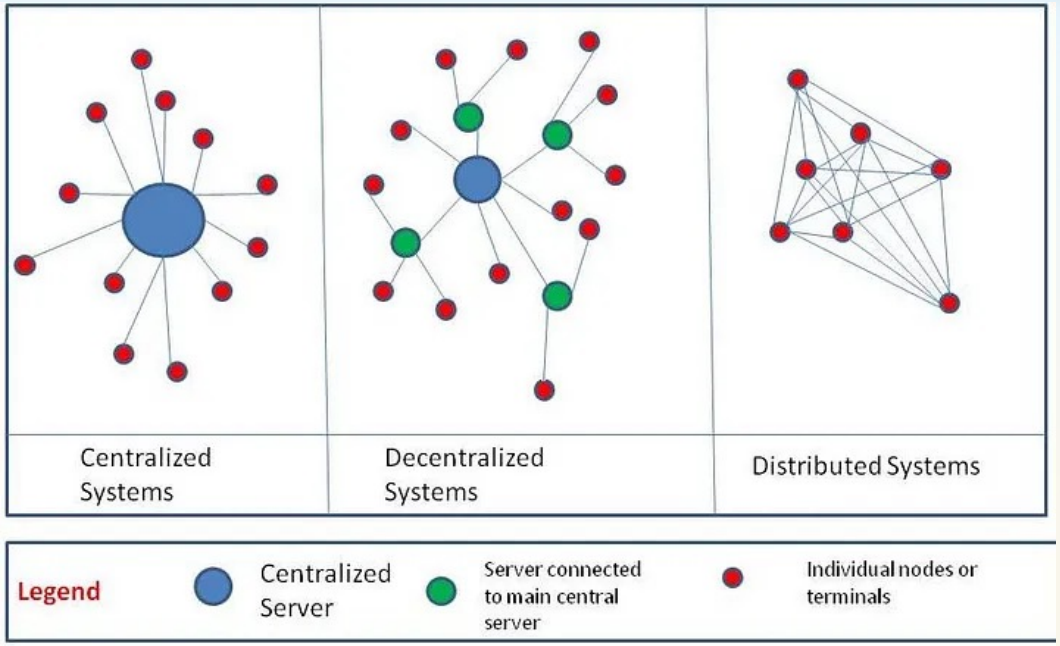
DEFINITION OF CRYPTO CURRENCY

- It is decentralized **virtual money**
- that is based on **blockchain technology**
- secured by **cryptography**.
- They are **not controlled by the government or central regulatory authorities**.
- It works **outside of the banking system** using different brands or types of coins – Like Bitcoin.
- **In 2008**, a person name **Satoshi Nakamoto** published a proposal to create a cash-like electronic payment system that would cut out the middlemen. That's the origin of **Bitcoin.**

What is a BLOCKCHAIN

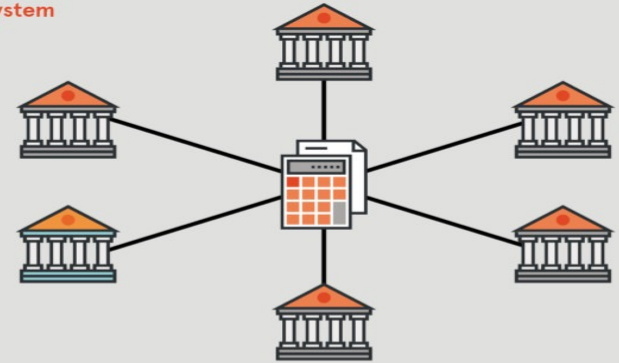
- **BLOCKCHAIN** is a sequence of **BLOCKS** **(data /transactions)** chained together **cryptographically** linking each block to the previous block**.**
- All the transactions coming onto the network are grouped into **blocks of data** and then chained together using sophisticated math.
- **BLOCKCHAIN** is a **digital ledger** of transactions maintained by a network of computers in a way that makes it difficult to hack or alter.
- This digital ledger **records transactions** related to a range of assets - tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).
- The digital Ledger is **distributed** and is shared between its users.
- All information shared is " **time stamped,public,verifiable,transparent, immediate, and immutable".**

DECENTRALISED & DISTRIBUTED SYSTEMS



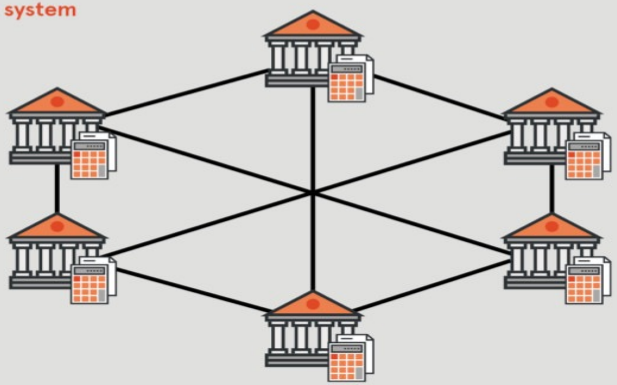
TRADITIONAL & DISTRIBUTED LEDGER

Current system



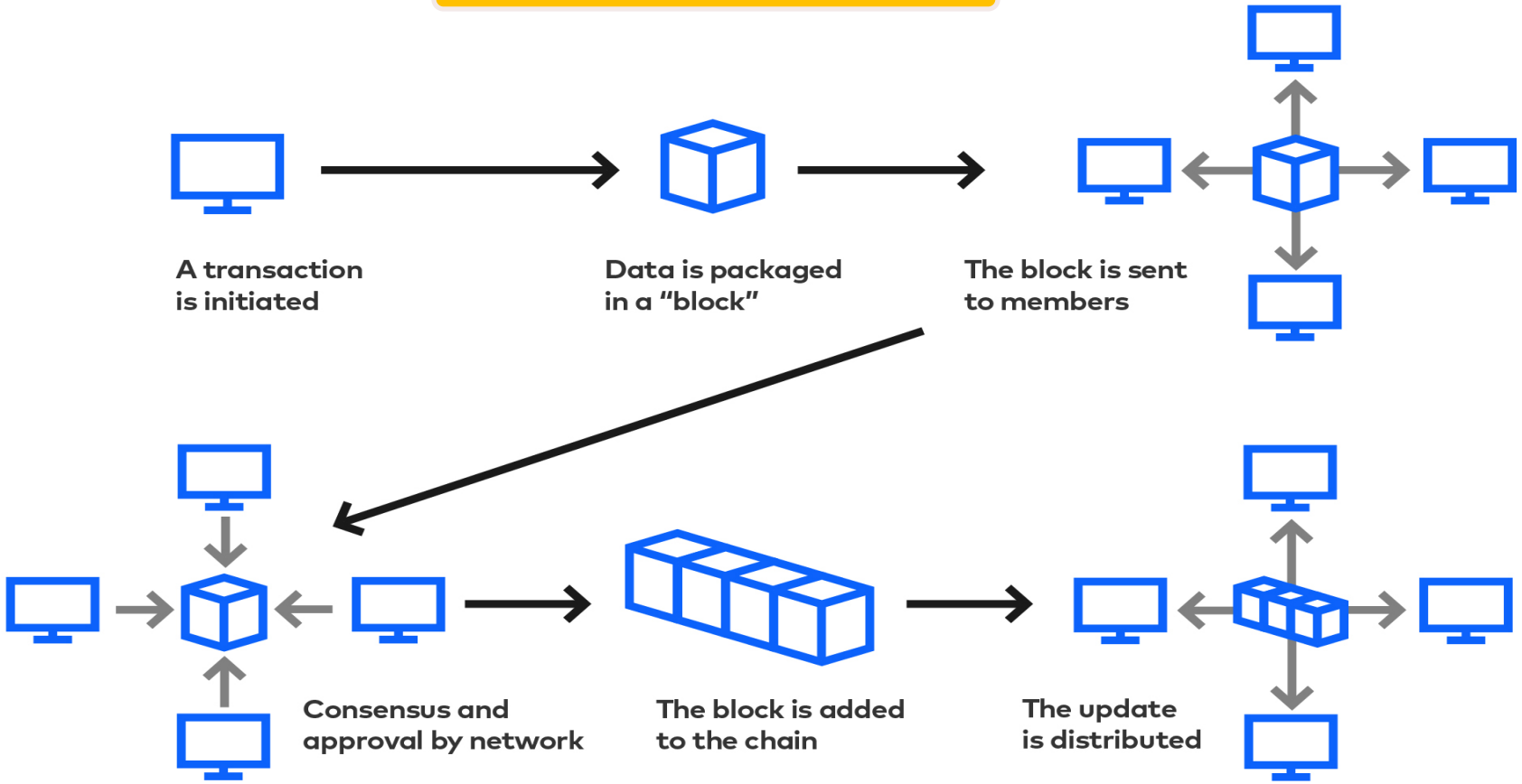
All banks check with central electronic ledger

Blockchain system

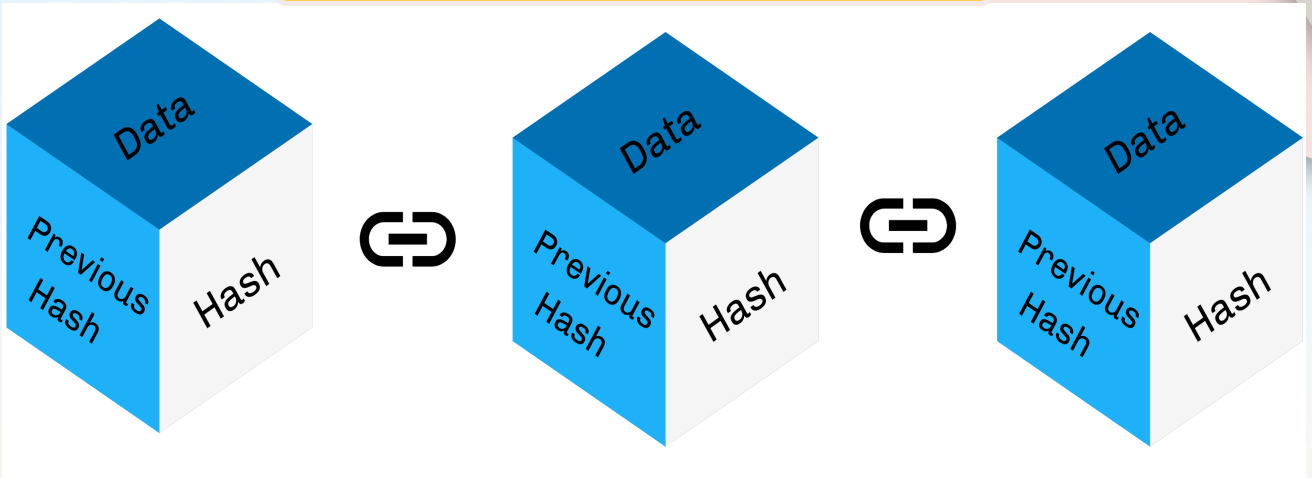


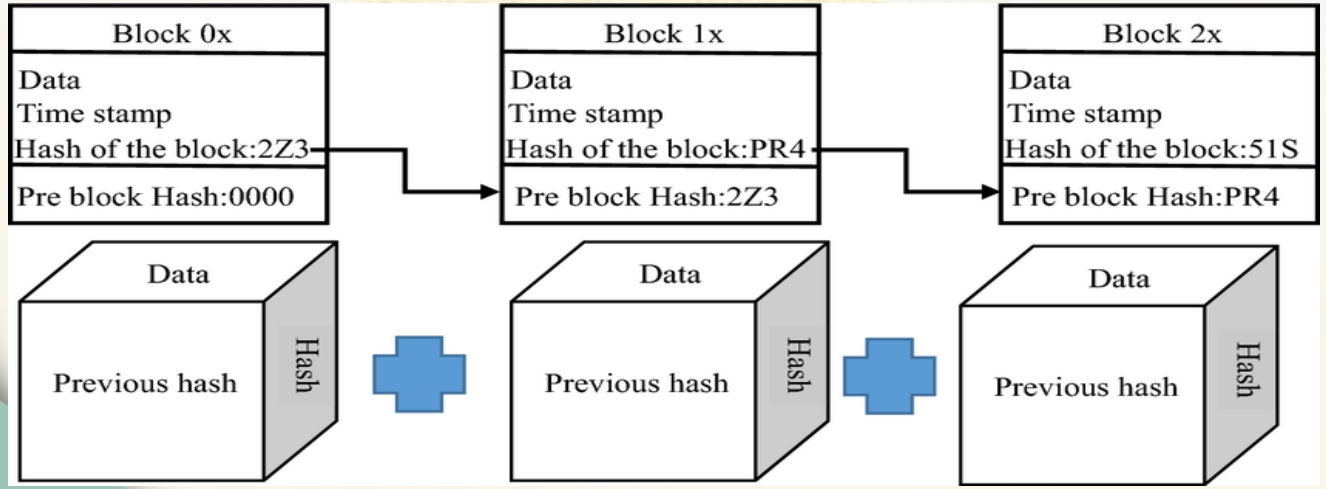
All banks have their own replicated copy of the ledger

BLOCK CHAIN EXPLAINED



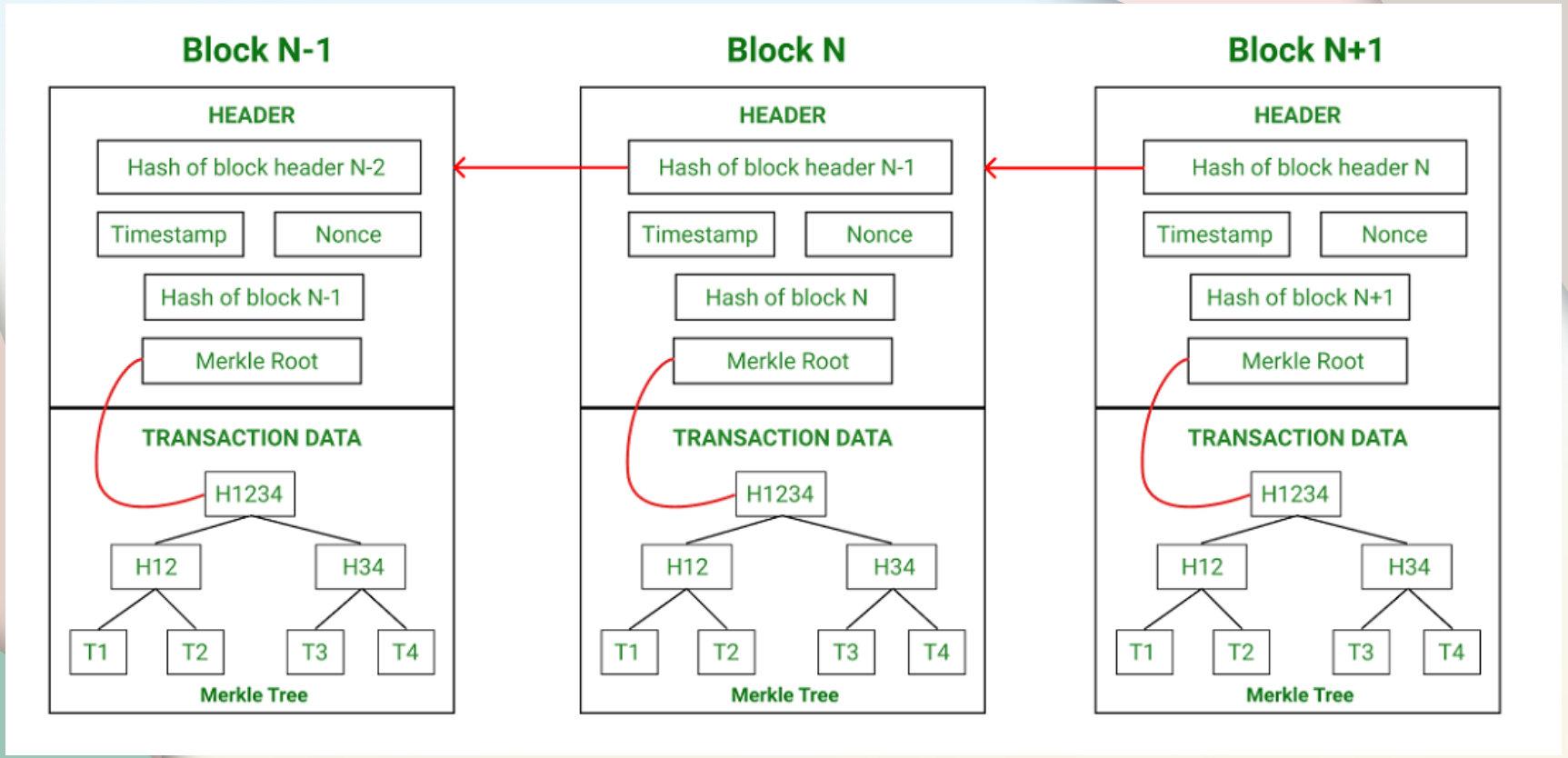
Block Explained





nnn

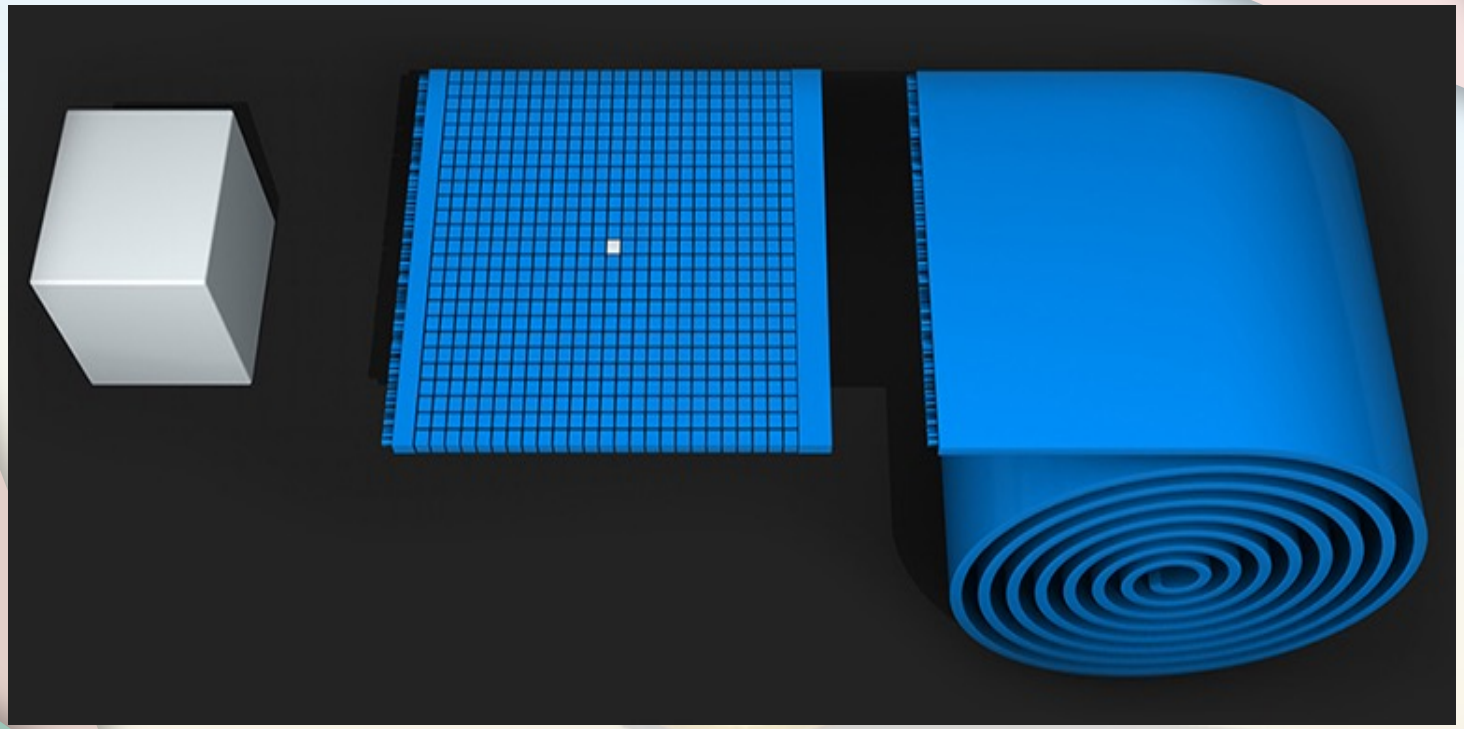
Block Explained



Block Explained

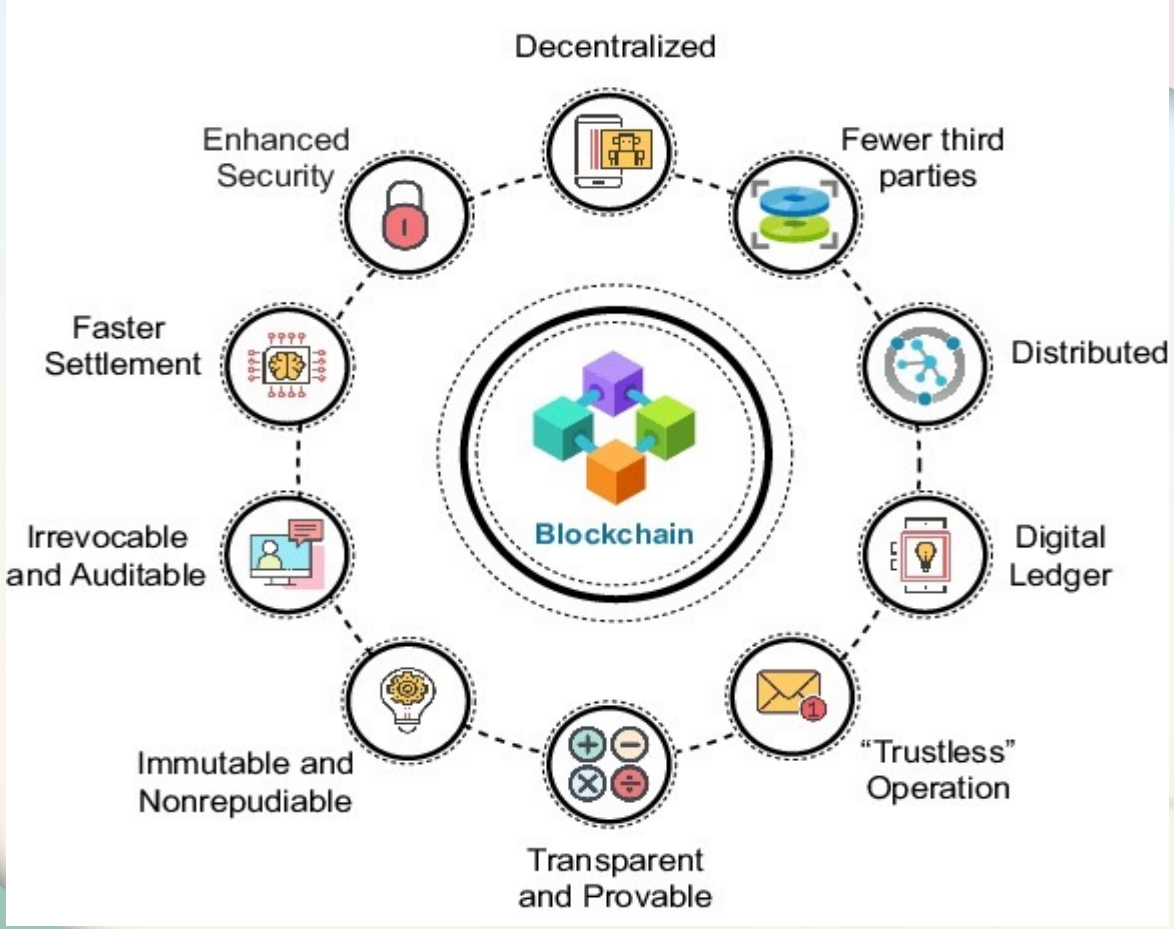
- **Block Header** contains information like - transaction amounts, wallet addresses, time, and date are recorded and encrypted into **a block header**
- **A hash** - a 64-digit encrypted hexadecimal number is created through the blockchain's hashing function. (block hash)
  "0000000000000000057fcc708cf0130d95e27c5819203e9f967ac56e4df598ee"
- The hash from each block is used in the block that follows it when its hash is created.
- This creates **a ledger of chained blocks** that **cannot be altered** because the information from every block is included in the newest block's hash.
- **When a block is closed, the hash must be verified before a new block can be opened**.
- **Miners** do the verification and Validation of **BLOCKS** .This is where **proof of work** comes in.

Block Explained



aaa bbb

Advantages of Block Chain



Some Major Uses of BlockChain

Top Blockchain Use Cases

Cryptocurrencies

Supply Chains

Voting

Insurance

Advertising

Digital IDs

Credit Ratings

Real Estate

Healthcare

Gaming

What is Cryptography

Cryptography is :

- the **process of hiding or coding information** so that **only the person** a message was intended for can read it.
- **a method of sending and receiving messages** that only the intended receiver and sender can read — **to prevent third-party access**.
- **Cryptography is used** in ATM (bank) cards, computer passwords, and shopping on the internet, banking transactions cards, computer passwords, and e- commerce transactions .

Cryptographic Techniques

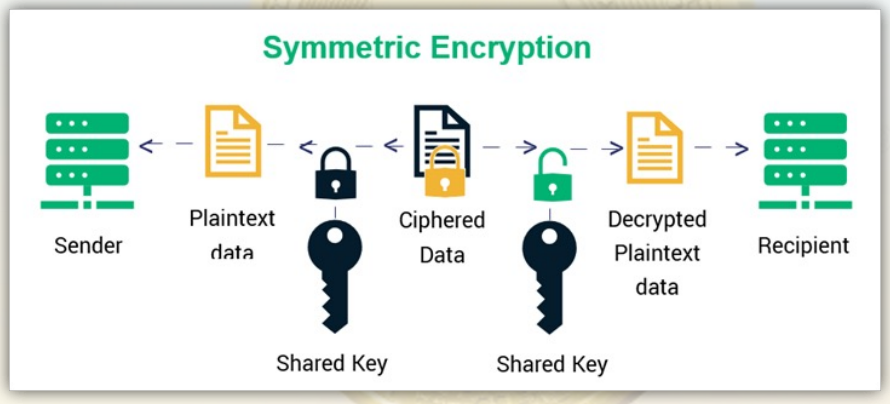
Three types of cryptographic techniques:

1. Symmetric-key cryptography
2. Public-key cryptography
3. Hash functions.

Modern cryptography Techniques

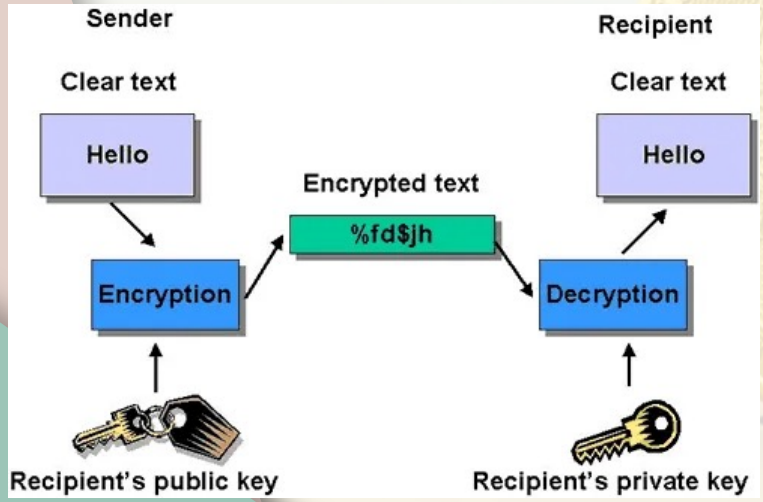
Symmetric-key Cryptography:

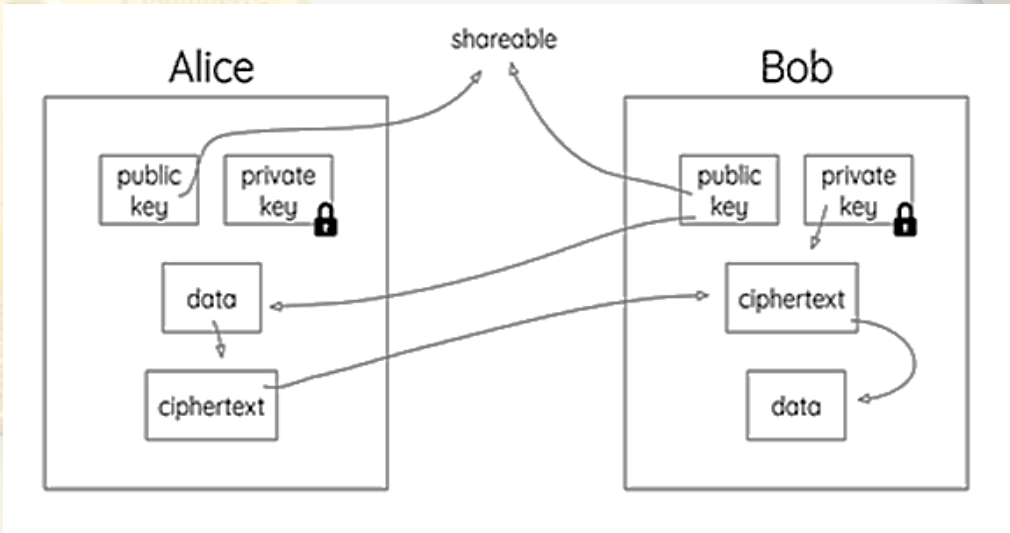
- Both the sender and receiver share a single key.
- The sender uses this key to encrypt plaintext and send the cipher text to the receiver.
- On the other side the receiver applies the same key to decrypt the message and recover the plain text.



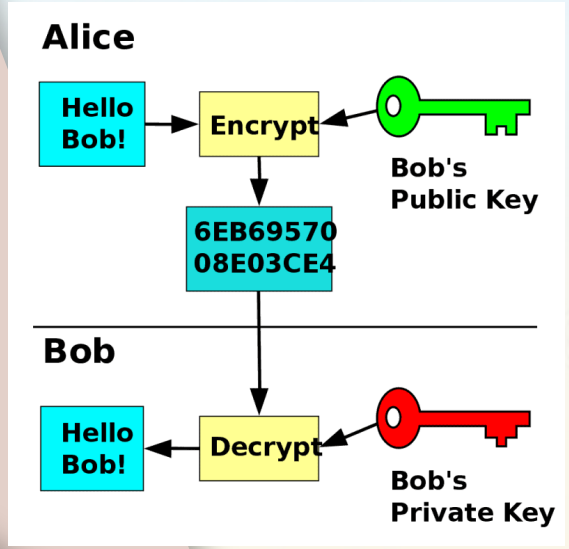
Public-Key Cryptography: This is the most revolutionary concept:-

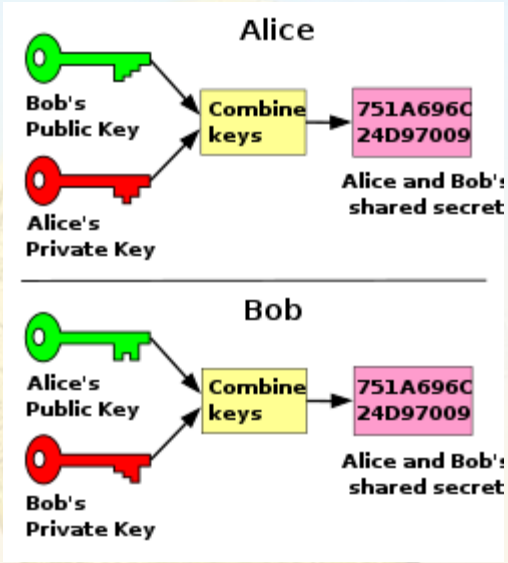
- In Public-Key Cryptography two related keys (public and private key) are used.
- Public key may be freely distributed, while its paired private key, remains a secret.
- The public key is used for encryption and for decryption private key is used.

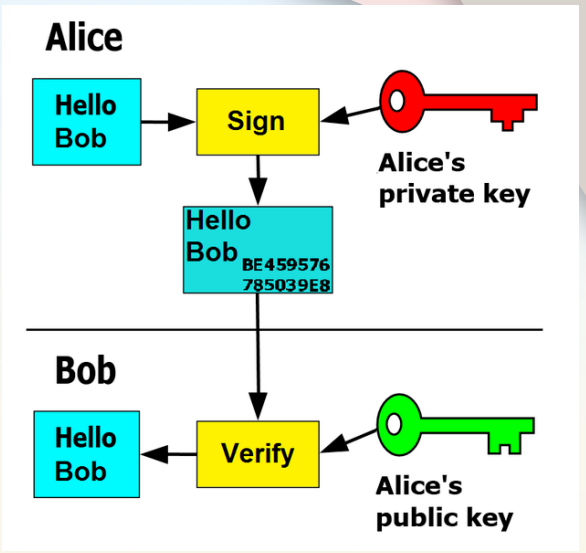




Different Use Of Keys







RSA means Rivest, Shamir, Adleman.

These are the inventors of the popular RSA Algorithm.

The RSA algorithm is based on **public-key encryption technology** which is a public-key cryptosystem for reliable data transmission.

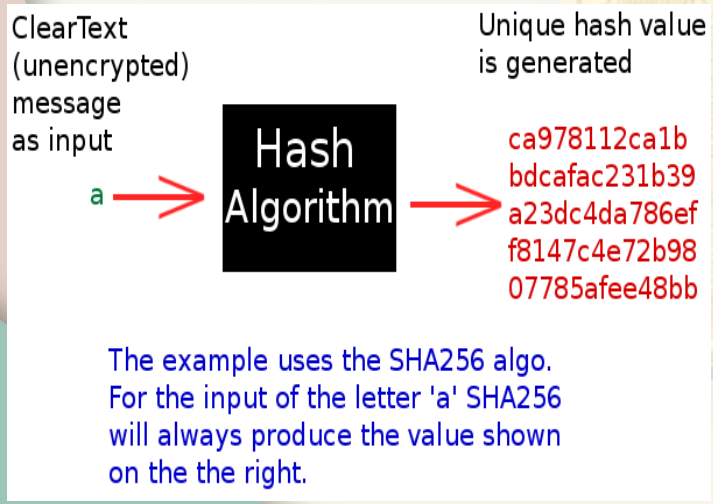
film

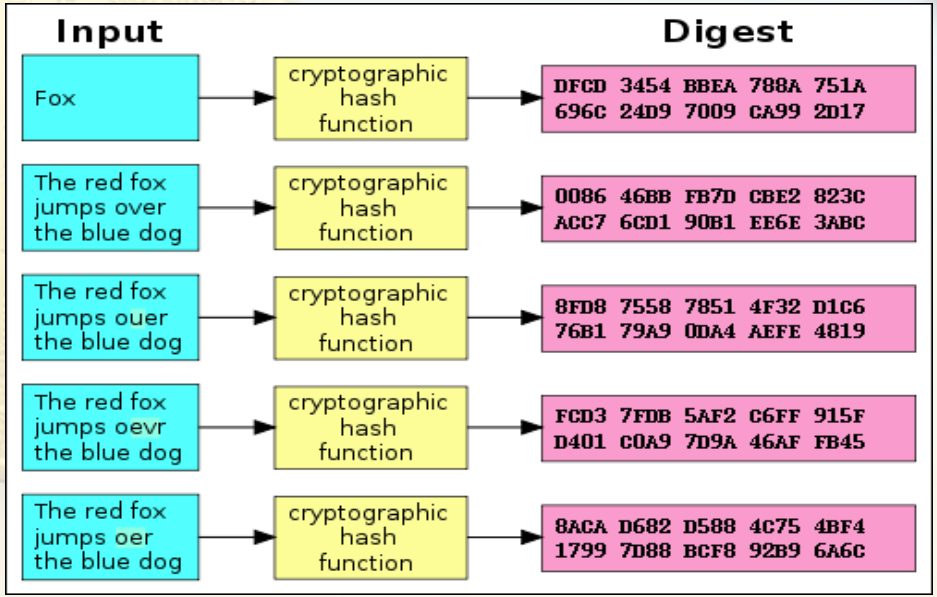
Hash Function

Hash Functions: No key is used in this algorithm.

- A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered.
- Hash functions are also used by many operating systems to encrypt passwords.

@@@





Role Miners in Cryptography

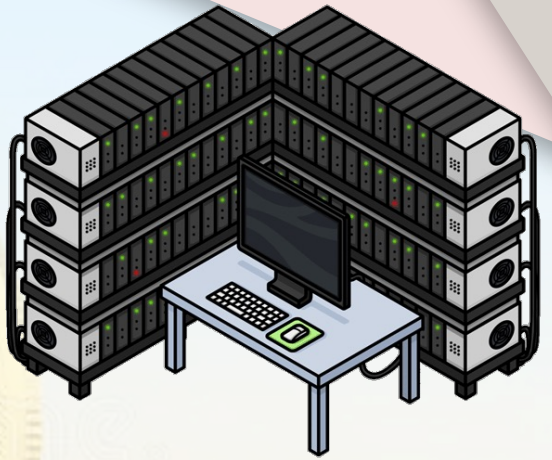
1. A miner **collects a group of unconfirmed transactions** into a block.
2. The miner **adds a block header** to the block. The block header contains information about the block, such as the previous block hash, the timestamp, and the merkle root.
3. The miner **hashes the block header** to generate the **block hash**.
4. The miner **compares the block hash to the target hash**. If the block hash is less than or equal to the target hash, the block is valid. (NONCE)
5. The miner **broadcasts the valid block** to the network.
6. Other nodes on the network **verify the block** by recalculating the block hash and comparing it to the target hash.
7. **If the block is valid**, it is added to the blockchain and the miner is awarded a block reward.
8. **Hash functions play an essential role in cryptocurrency mining**.
9. They help to **secure the blockchain and to generate new cryptocurrency.**

What is NONCE

- A nonce is **an arbitrary value** that can be only used once.
- It is the **random variable** added as input to the SHA-256 crypto engine to create the unique hash value.
- **The miners don't know the nonce value**, but do have the block contents. Miners will take the block contents, pick a nonce, and input them into the SHA-256 crypto engine.
- **If the hash value is the "correct" hash value** (Target Hash), awesome — they have solved it !.
- Otherwise, they pick a new nonce, input the same block contents and run it through the SHA-256 crypto engine again.
- **This loop iteration may take thousands or hundreds of thousands of iterations** to find the correct nonce.

Power Consumption by Cryptocurrencies

In 2009, you could mine one Bitcoin using a setup like this in your living room.

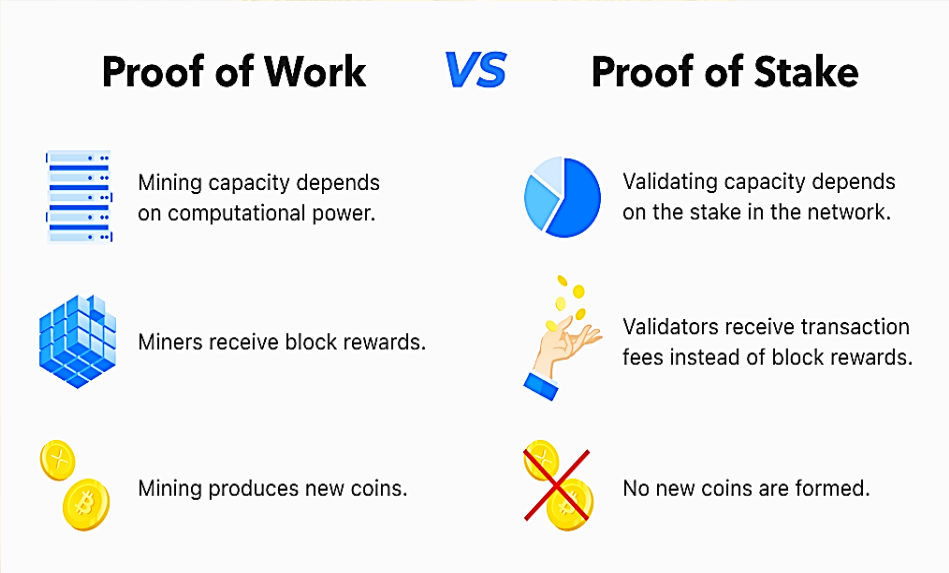


Today, you'd need a room full of specialized machines, each costing thousands of dollars.

- The process of creating Bitcoin to spend or trade consumes around **91 terawatt-hours** of electricity annually, **more than is used by Finland**- a nation of about 5.5 million.
- The Bitcoin network **consumes 1,708% more electricity than Google**, but **39% less than all of the world's data centers**

What is POW and POS

- **PoW (Proof of Work)** may be **a way of verifying current and past transactions**.
- **POW is an algorithm** that's designed to verify transactions and obtain new blocks added to blockchain. (Bitcoin).
- POS (Proof-of-stake) is a consensus algorithm that decides on **who validates next block**, **according to how many coins you hold**.{EOS (EOS), Tezos (XTZ), Cardano (ADA), Cosmos (ATOM), Lisk (LSK)}.



Mining of Bitcoin

Miners connect to other nodes and perform six tasks:

1. Listen for transactions (and validate them by checking that signatures are correct and outputs being spent haven`t been spent before.)

2. Maintain block chains and listen for new blocks (Start by asking nodes for historical blocks before you joined. Listen for new ones, by validating the transaction and valid nonce)

3. Assemble a candidate block (Most difficult part)

4. Find a nonce that makes your block valid (hitting target)

5. Hope your block is accepted(Hope that others accept your block on the consensus chain, instead of others)

= Profit (Transaction fees, if applies, given to miners.)

Miners do :

- Book keeping
- Network Guardian
- Settlement and clearing
- Creation of new Bitcoins

Through

- validating transactions and blocks, and
- Compete to find blocks and profit.

The so called incentive to keep it as a currency.

Types of Cryptocurrencies

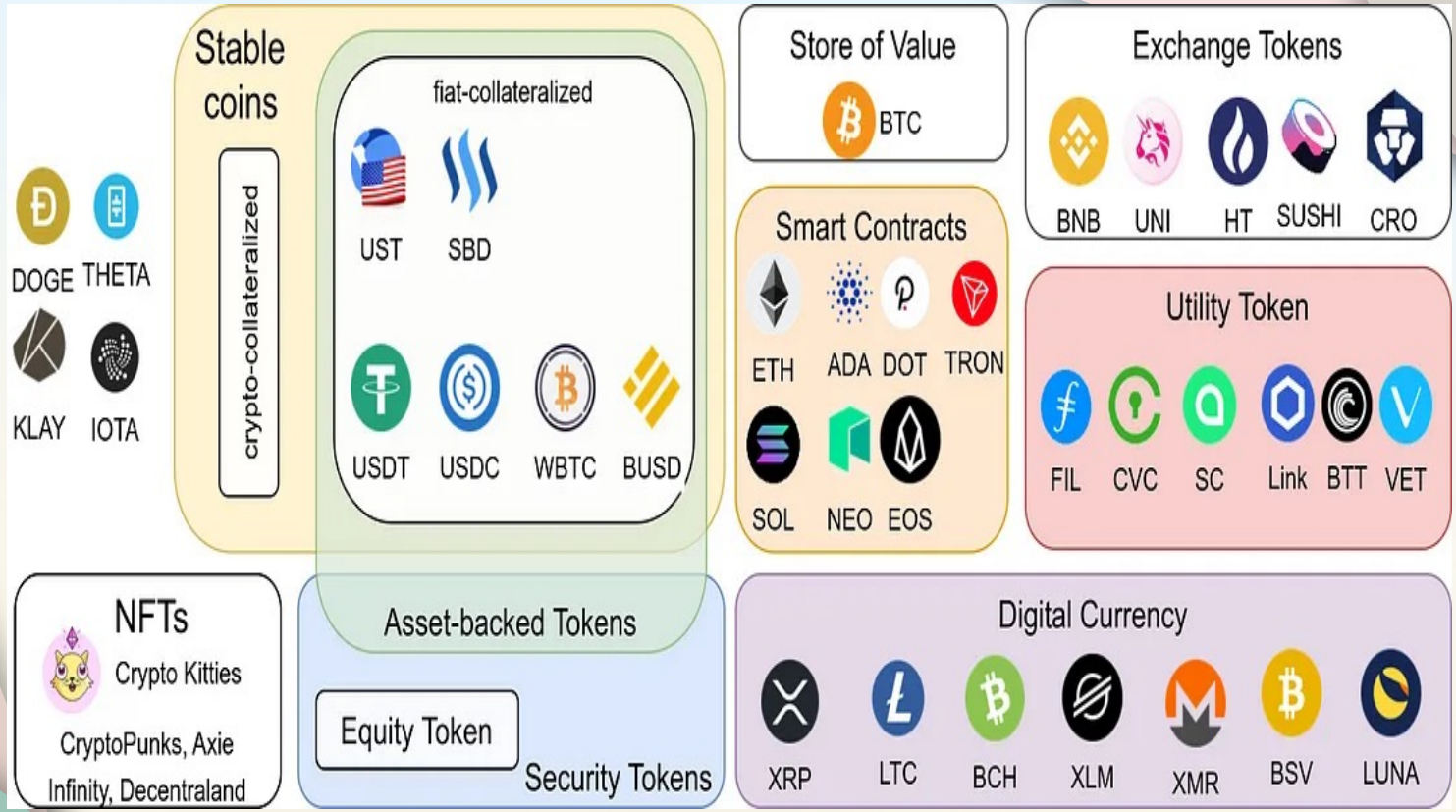
Over 9,000 available types - • Different uses • Different features• Total market capitalization and trading volume is enormous

Broadly we can categorize cryptocurrencies into four broad types:

- **Payment Cryptocurrency**
- **Utility Tokens**
- **Stablecoins**
- **NFT (Non-Fungible Tokens)**

&&& CoinDCX, WazirX, and CoinSwitch Kuber

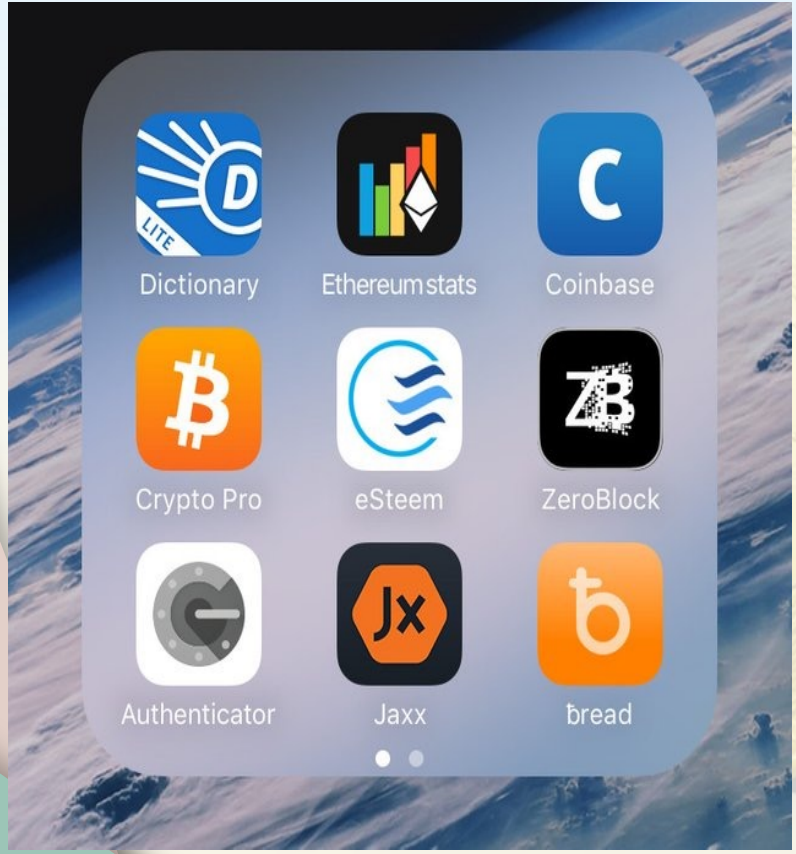
Types of Cryptocurrencies

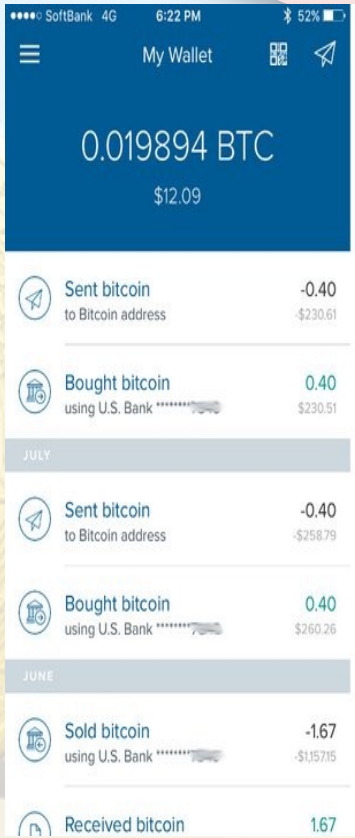


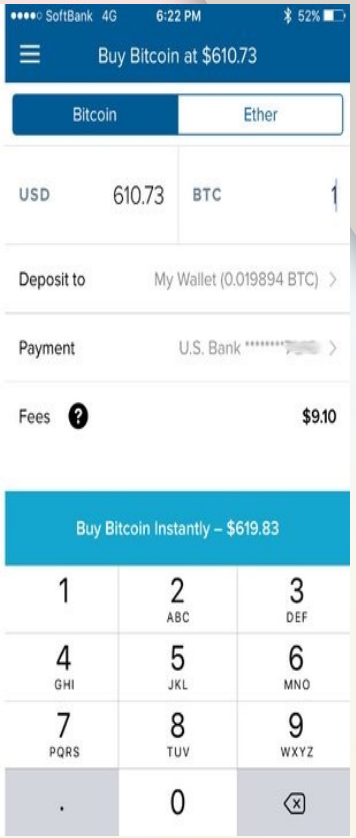
Retail Payment in Crypto

- I present the app on my phone or other device to the retailer.
- The retailer’s Bitcoin app checks my Bitcoin wallet via the blockchain.
- The Bitcoin is transferred from my wallet to the retailer’s wallet via the blockchain.
- The transaction is recorded publicly on the blockchain.
- The transaction involves me, the retailer and the Blockchain.
- No fees are extracted therefore, no one profits other than the retailer.

Typical Wallet for Crypto

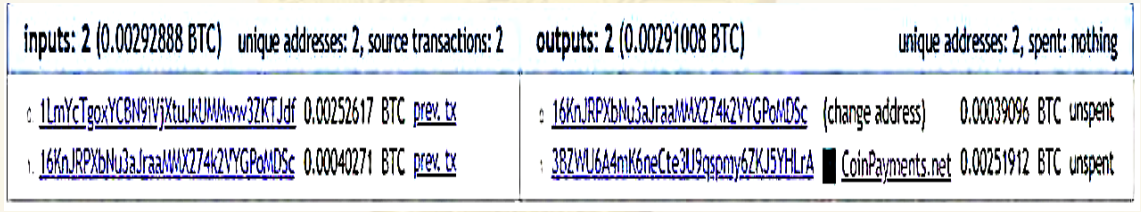






Crypto Transaction Explained

- Bitcoin is transferred from **one address to another.**
- A transaction recorded with a signed date , structure , expressing a transfer of value.
- Transactions are then transmitted over the bitcoin network, included in blocks and made permanent on the blockchain.
- Network is controlled by miners.
- **Each transaction has two sides, inputs and outputs.**
- The inputs show the amount being sent and what sender address is involved.



- The outputs show the amount of bitcoin being credited and the recipients address.
- Importantly the inputs and outputs do not necessarily add up to the same amount. This is because **there is a fee to pay for including a transaction in a block**.

CATMs (Cryptocurrency ATMs)

//coinatmradar.com

Bitcoin ATMs by Country.

Bitcoin ATMs are installed in many countries in the world. The current distribution of installations accross the countries can be found on The Chart of Bitcoin ATM number by Continents and Countries.

- United States • (27158 locations)
- Canada • (2848 locations)
- Australia • (651 locations)
- Spain • (285 locations)
- Poland • (269 locations)
- El Salvador • (212 locations)
- Hong Kong • (160 locations)
- Romania • (147 locations)
- Germany • (140 locations)
- Switzerland • (139 locations)
- Georgia • (133 locations)
- Austria • (119 locations)
- Italy • (79 locations)
- Czech Republic • (79 locations)
- Russian Federation • (76 locations)
- Slovakia • (75 locations)
- Mexico • (52 locations)
- Puerto Rico • (45 locations)
- Hungary • (44 locations)
- Turkey • (21 locations)
- Taiwan • (20 locations)
- South Africa • (20 locations)
- Croatia • (19 locations)
- France • (17 locations)
- Guatemala • (15 locations)
- Finland • (15 locations)
- Ukraine • (15 locations)
- Dominican Republic • (15 locations)
- Argentina • (13 locations)
- Armenia • (12 locations)
- Israel • (10 locations)
- Portugal • (10 locations)
- New Zealand • (10 locations)
- Lebanon • (7 locations)
- Brazil • (7 locations)
- Costa Rica • (6 locations)
- Kosovo • (6 locations)
- Bosnia and Herzegovina • (3 locations)
- Japan • (3 locations)
- United Kingdom • (2 locations)
- Anguilla • (2 locations)
- India • (2 locations)
- Nigeria • (2 locations)
- Antigua and Barbuda • (2 locations)
- Guam • (1 location)
- Venezuela • (1 location)
- Uruguay • (1 location)
- Botswana • (1 location)
- Djibouti • (1 location)
- Ecuador • (1 location)
- Uganda • (1 location)
- Saint Kitts and Nevis • (1 location)
- Thailand • (1 location)
- San Marino • (1 location)
- Kazakhstan • (1 location)

Operations in Cryptocurrencies

1. **Mining :**
   - ➢Miners are responsible for ensuring the authenticity of information and updating the blockchain with the valid transaction.
   - ➢They solve certain mathematical puzzles over specially equipped computer systems to be rewarded with bitcoins in exchange.
   - ➢Miners save blockchains from block fraud and hacker attacks and guarantee the network's decentralization.

2. **Buying, selling, and storing**:
   - ➢ Cryptocurrencies from central exchanges, brokers, and individual owners or sell it to them.
   - ➢ Exchanges or platforms like Coinbase are the easiest ways to buy or sell
   - ➢ Once bought, cryptocurrencies can be stored in **digital wallets**.
   - ➢ Digital wallets can be "hot" or "cold".

3. **Transacting or investing :**
   - ➢ Easily transferred from one digital wallet to another, using only a smartphone.
   - ➢ Once you own them, your choices are to:
     - a) use them to buy goods or services
     - b) trade in them
     - c) exchange them for cash
     - d) Debit –Card Type /ATM

TOKENS- Utility Token

UTILITY TOKEN :

- **A utility token** is a type of cryptocurrency
- It **provides access to a product or service** within its ecosystem and allows users to perform some action on a certain network.
- Normally created on Ethereum Block Chain
- Utility tokens **are not mineable cryptocurrencies**.
- They are usually **pre-mined**, being created all at once and distributed in a manner chosen by the team behind the project.

Ex: Cronos (CRO), Binance (BNB), Bitcoin.com (Verse),Filecoin (FIL) –(storage), Siacoin (SC)-(network storage), Civic (CVC)-(special features)

TOKENS- Security Token

SECURITY TOKEN:

- Security token **derives value from external, tradeable assets** such as stocks or real estate, bond, or option.
- There are **three common types of security tokens: equity tokens, debt tokens, and real asset tokens.**
- Instead of certifying ownership on paper certificates, equity tokens are recorded on the blockchain.
- **Debt tokens represent a debt or a loan**. It could be for real estate mortgages or corporate bonds .
- **Equity tokens represent the value of the share** issued by a company.
- **Security tokens are similar to stocks, bonds, ETFs, and other securities.**

Ex: tZERO (TZRO), Harbor (HBR), Polymath (POLY)

Stable coins

Stablecoins maintain a stable value, typically **pegged to a specific asset** like a fiat currency (e.g., US dollars), a commodity (e.g., gold), or a basket of assets.

They **serve as a bridge** between the volatile world of cryptocurrencies and the stability of traditional financial systems.

Stablecoins work in one of three primary ways:

Fiat-Collateralized: Some stablecoins are backed by real-world assets, like US dollars, sitting in a bank account.

Crypto-Collateralized: These stablecoins use other cryptocurrencies (like Ethereum or Bitcoin) as collateral.

Algorithmic: These stablecoins use complex algorithms to maintain their value. The algorithm can expand or contract the supply of stablecoins in response to market demand, aiming to keep the value stable.

Stablecoins have various uses:Store Value; Facilitate Trading; Remittances; DeFi (Decentralized Finance):

Smart Contracts

Smart contracts are self-executing contracts :

- The terms of the agreement directly written into code.
- They automatically enforce, facilitate, or verify the negotiation and execution of a contract when predefined conditions or criteria are met.
- They offer a powerful tool for automating and securing agreements in a decentralized and efficient manner.

A computer program (the smart contract) :

- Contains the terms and specifies the conditions and the outcomes.
- It is deployed onto a blockchain, which is a decentralized and tamper-resistant digital ledger.
- The contract is then locked and cannot be altered by any party once deployed.
- As the scenario unfolds, the smart contract continuously monitors the outcome through a trusted data source (e.g., an API –Application Programming Interface provides real-time data).
- At the finality of the event, the smart contract automatically triggers the execution of the award / transfer

Smart contracts are widely used in various fields, including finance (e.g., DeFi protocols), supply chain management, insurance, voting systems, and more.

HOW **SMART CONTRACTS** WORK

Benefits Of Stablecoins For Businesses And Traders

- Exchange your cryptocurrencies to any stablecoin and avoid price fluctuations
- Option to redeem fiat currency for your fiat-pegged stablecoin
- Use stablecoins for settling fast payments globally
- Blockchain-based payment systems eliminate middle-men in the process of transaction

N F T

NFT stands for "Non-Fungible Token.

It is like a special digital certificate or proof of ownership for something unique- like a rare collectible item.

It could be digital art, a video, music, a tweet, a virtual land, or anything else unique that can be digital. Digital version of collectibles like baseball cards, stamps, or rare comic books.

Not Interchangeable: (Non-Fungible)

- "Non-Fungible" means it's not interchangeable with other things.
  For example, one bitcoin is the same as any other bitcoin; they're interchangeable.

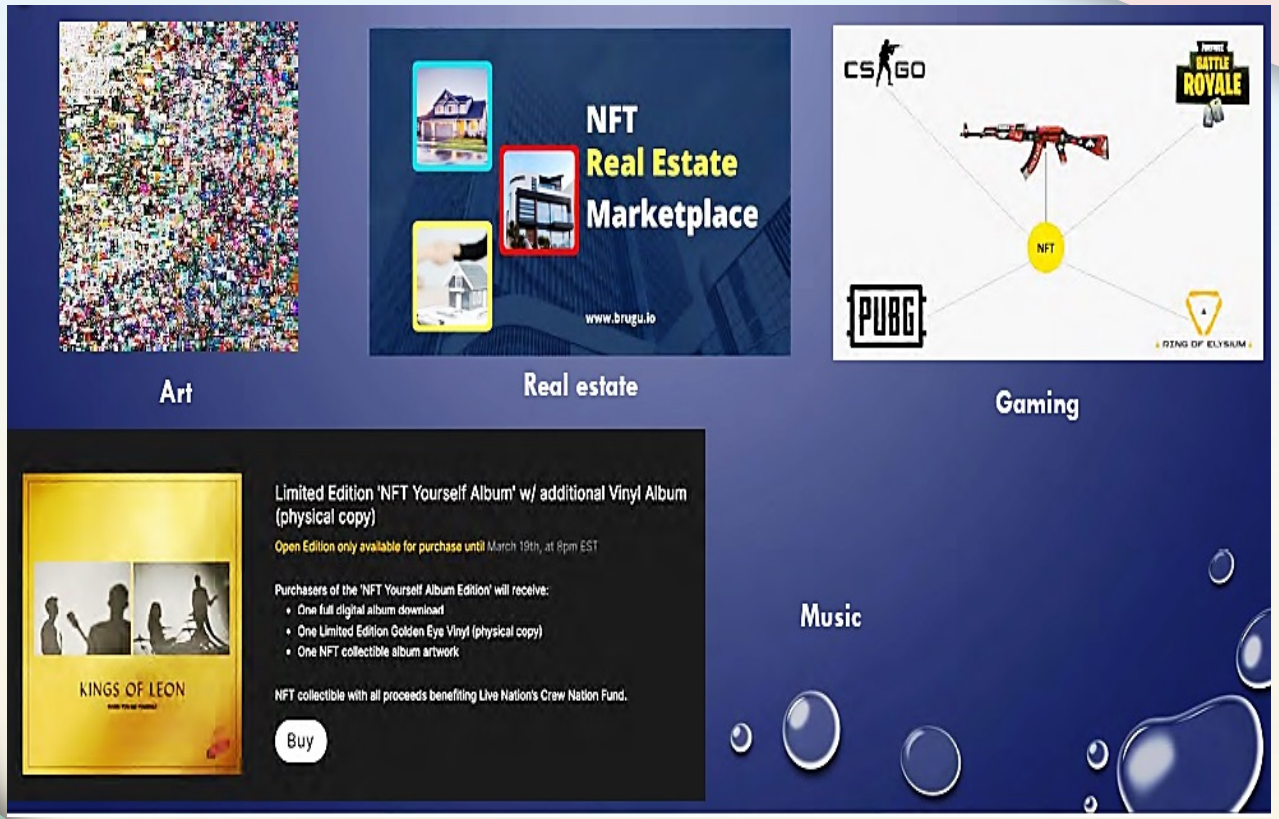
- But NFTs are unique and can't be swapped for something else,

- just like a rare baseball card can't be swapped for a different card.

Blockchain Proof: NFTs use blockchain technology to prove ownership, that you're the official owner.

Ownership and Value: People buy and sell NFTs because they want to own a piece of digital history or art, and they believe it has value.

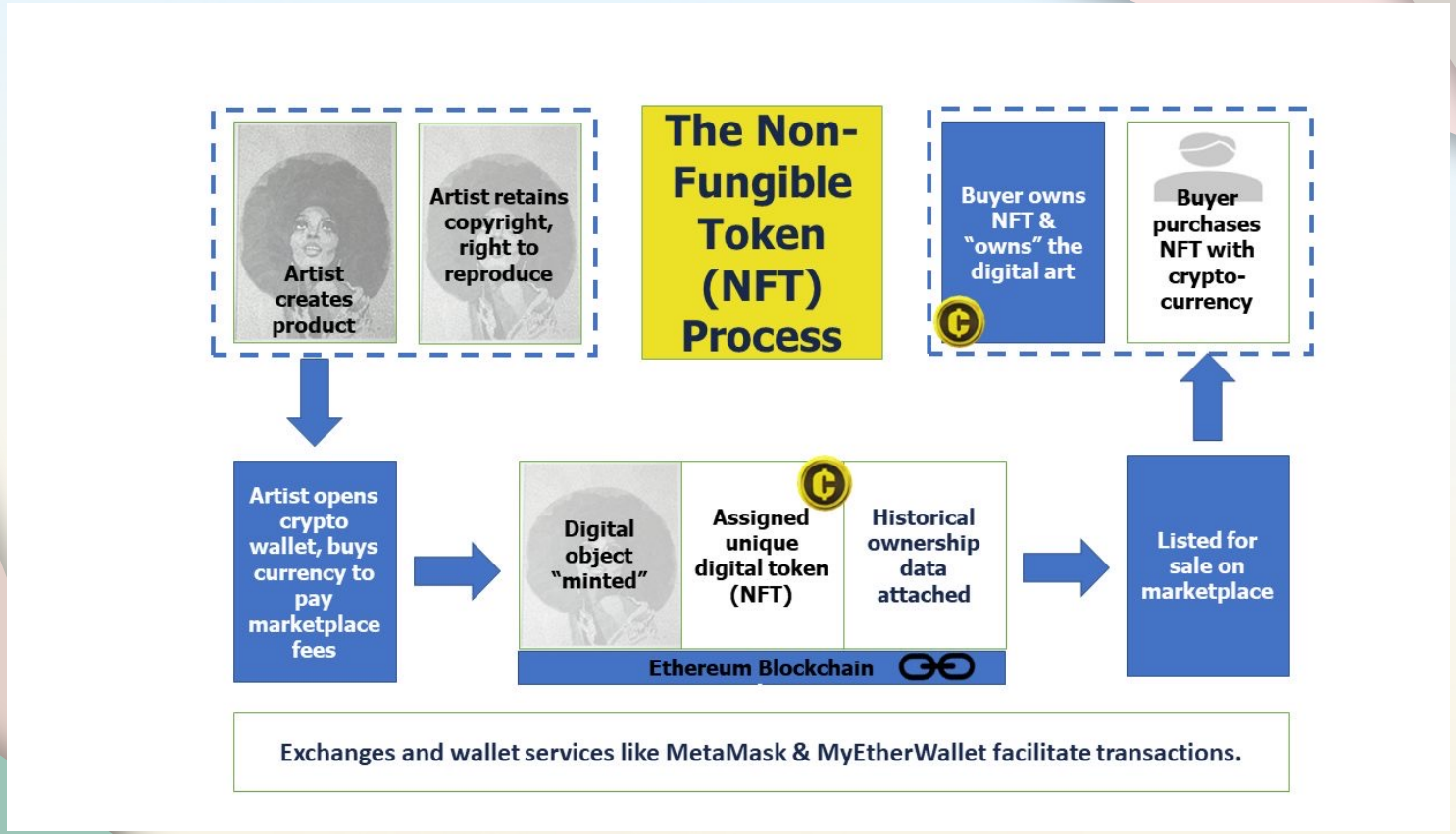
N F T


Art
NFT
Real Estate
Marketplace
www.brugu.io
Real estate
CS GO
BATTLE ROYALE
NFT
PUBG
RING OF ELYSIUM
Gaming
KINGS OF LEON
Limited Edition 'NFT Yourself Album' w/ additional Vinyl Album (physical copy)
Open Edition only available for purchase until March 19th, at 8pm EST
Purchasers of the 'NFT Yourself Album Edition' will receive:
One full digital album download
One Limited Edition Golden Eye Vinyl (physical copy)
One NFT collectible album artwork
NFT collectible with all proceeds benefiting Live Nation's Crew Nation Fund.
Buy
Music

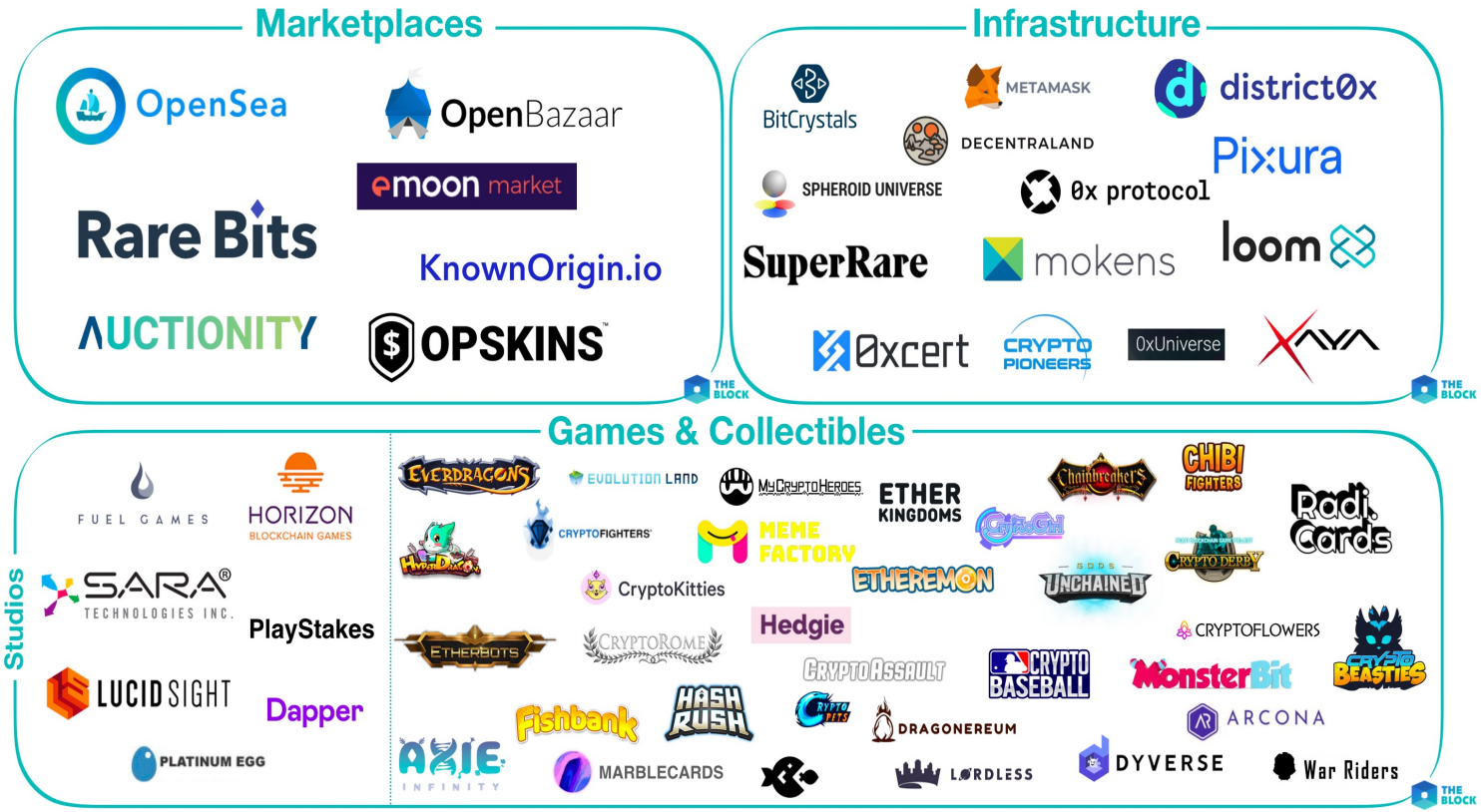
N F T- Platforms

- Artists can offer NFTs for sale on these platforms/markets.
- Buyers can then search the platform and buy the item of their choice.
- This is usually done by bidding.
- “OpenSea” has processed more than 10 billion dollar in transactions since its launch in 2017.

N F T- Process


Artist creates product
Artist retains copyright, right to reproduce
The Non-Fungible Token (NFT) Process
Buyer owns NFT & "owns" the digital art
Buyer purchases NFT with crypto-currency
Artist opens crypto wallet, buys currency to pay marketplace fees
Digital object "minted"
Assigned unique digital token (NFT)
Historical ownership data attached
Ethereum Blockchain
Listed for sale on marketplace
Exchanges and wallet services like MetaMask & MyEtherWallet facilitate transactions.

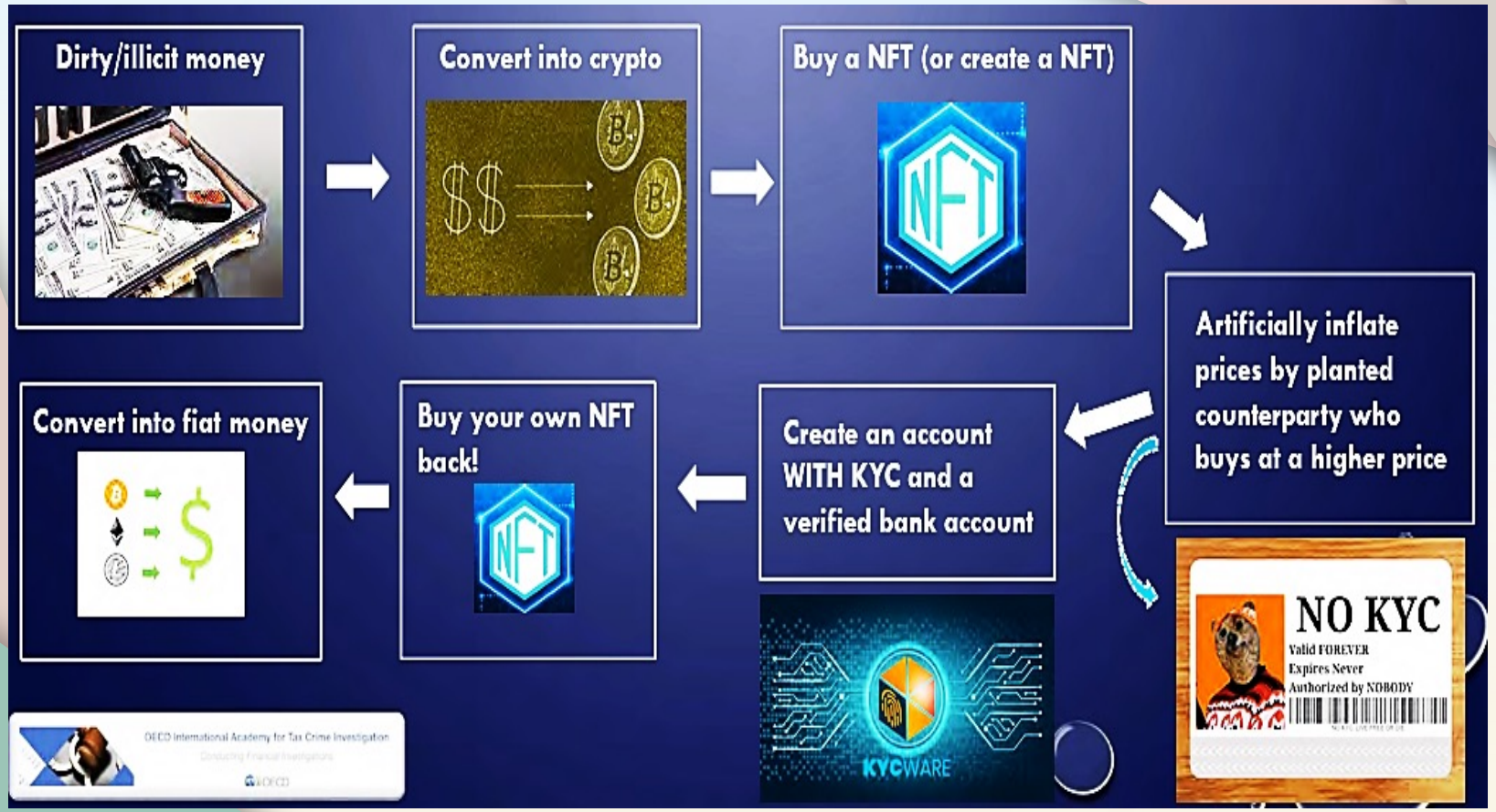
Non-Fungible Token Ecosystem



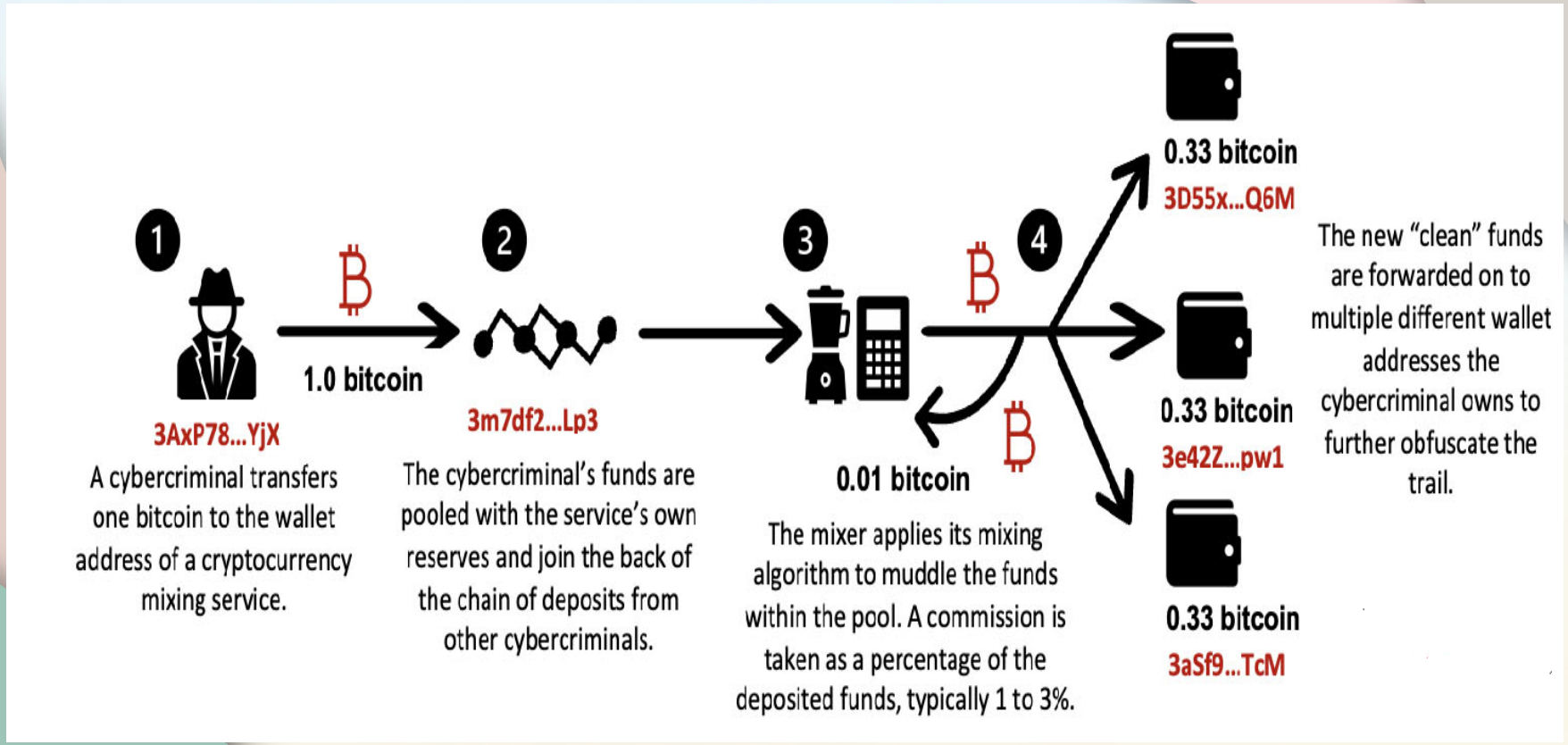
Regulatory Challenges in N F T- Regime

- Many NFT platforms do not perform KYC/AML checks!
- Shifting large amounts of money in a borderless, partly anonymous market!
- Criminal Abuse of NFTS
- Wash Trading
- NFTs mostly sold by bidding.- Ability to add/create value to something trivial!
- Arm's length principle?
- Fraud-prone?
- A transfer of physical property/ownership? Full or partial ownership ? Valuation matters.

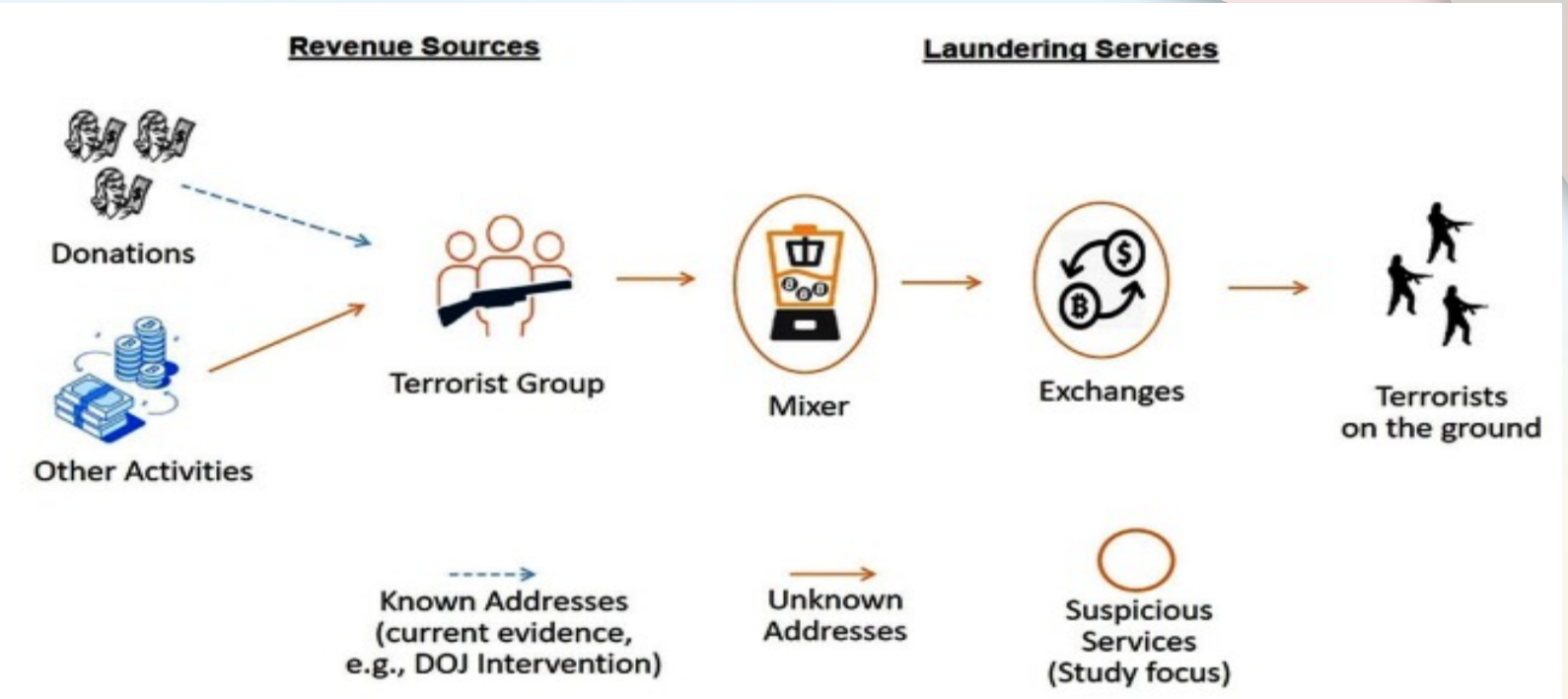
Money Laundering through N F T



Challenges posed by Crypto



Challenges posed by Crypto



Importance of NFT Platforms

NFT marketplaces/platforms Important source of information

- 269 platforms, 2.460.000 wallets, 10.275.000.000 $, 231.000.000.000 $
- Even in colder prevailing market conditions, still high trading volume?!
- Where to go to? (USA, HK, ?, …) Data Protection Laws -GDPR?
- Legal powers of tax administrations/law enforcement?

Observe NFTs & follow the money:-

- Payment methods (debit/credit card, Paypal, Crypto's)
- Payment via cryptocards, the investigators nightmare?! (eg advcash.gi)
- Responsibility/accountability of the platforms/marketplaces!?

What is DeFi

DeFi is in short for decentralized finance.

DeFi is an umbrella term for peer-to-peer financial services on public blockchains, primarily Ethereum.

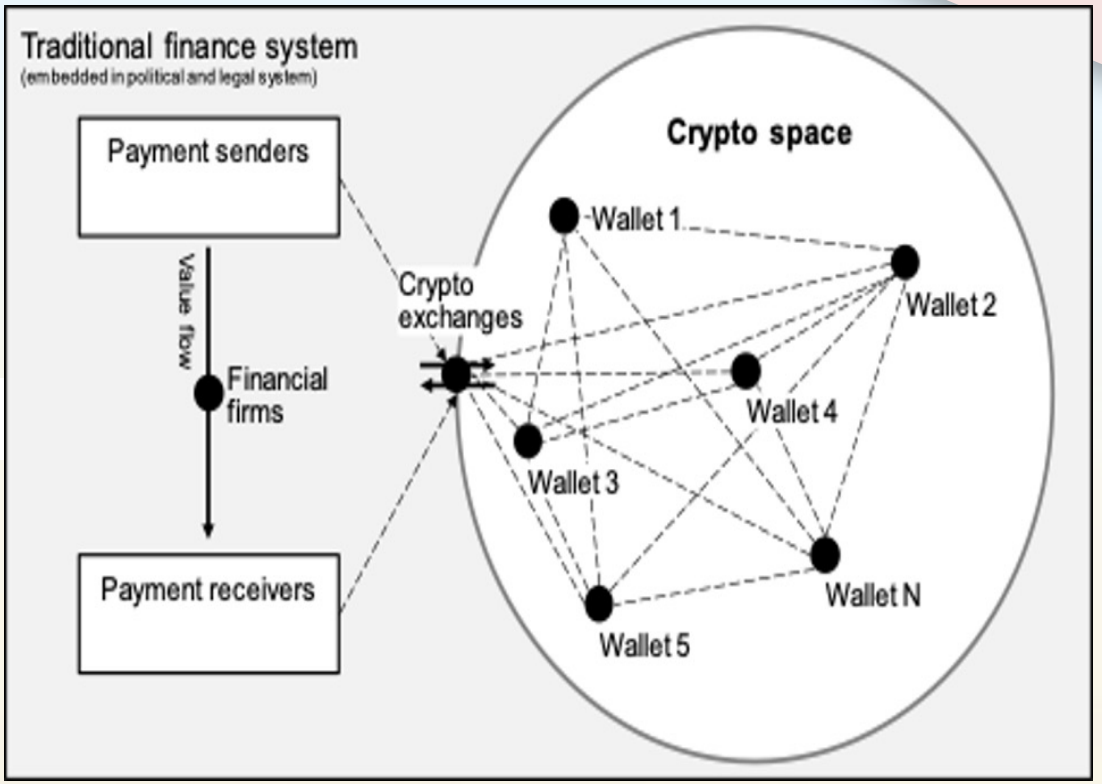
It provides an alternative to traditional financial systems without the need for intermediaries such as banks or other financial institutions.

It uses smart contracts.

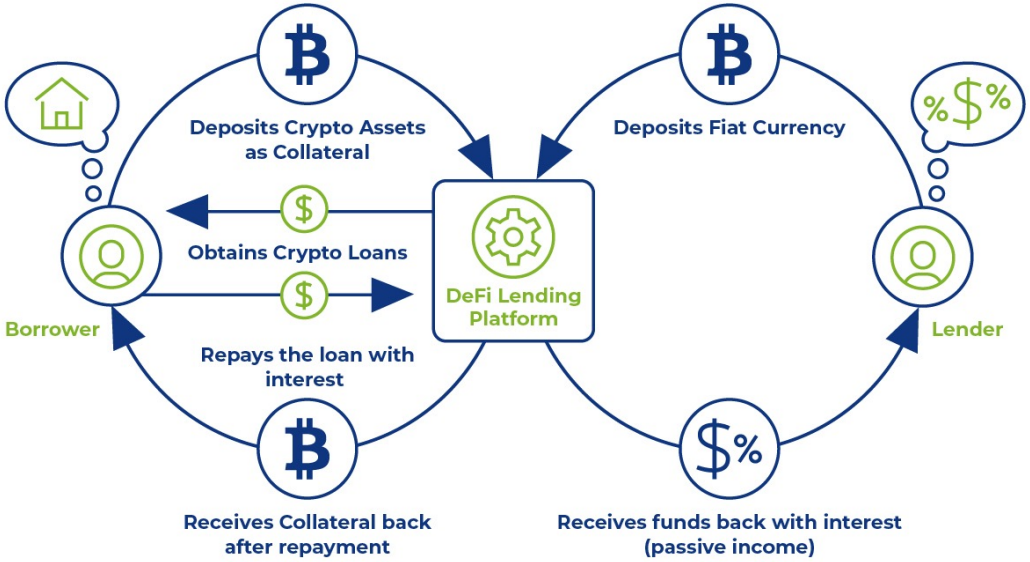
DeFi offers a range of financial services such as lending, borrowing, trading, and investing in cryptocurrencies .

It also provides access to decentralized exchanges, which allow users to trade cryptocurrencies without the need for a centralized exchange .

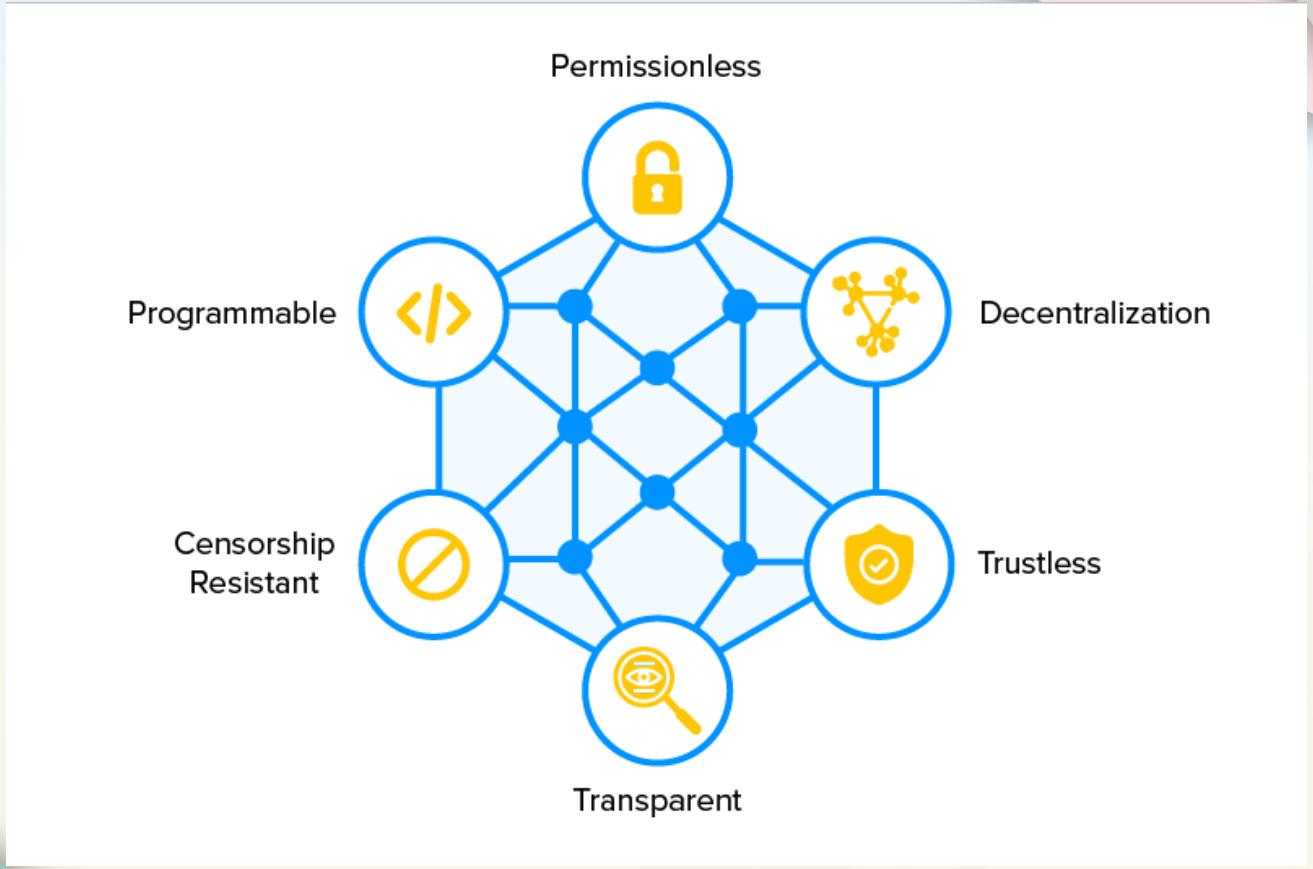
Traditional Vs Crypto Loans



What are Crypto Loans?



Benefits of DeFI Transactions



Why do people invest in Crypto currency:

Profit Potential: The rapid price appreciation of crypto currencies **like Bitcoin and Ethereum** in the past has created a perception of high returns.

Diversification: diversify investment portfolios. -uncorrelated with traditional investments like stocks and bonds- spreads risk.

Decentralization: Financial sovereignty and distrust centralized financial systems.

Innovation: Blockchain technology to disrupt various industries, such as finance, supply chain, and healthcare.

Speculation: High volatility- profit from short-term price fluctuations.

Hedging Against Inflation: Hedge against inflation. -protect against the devaluation of fiat currencies.

Financial Inclusion: They provide financial services to people who are unbanked or underbanked.

Technological Enthusiasm: Passionate about the underlying technology and believe in its potential to transform industries.

Accessibility: Markets are open 24/7 ; trading is accessible to anyone with an internet connection.

Early Adoption: Early adopters of cryptocurrencies have seen substantial gains.


Thank
You