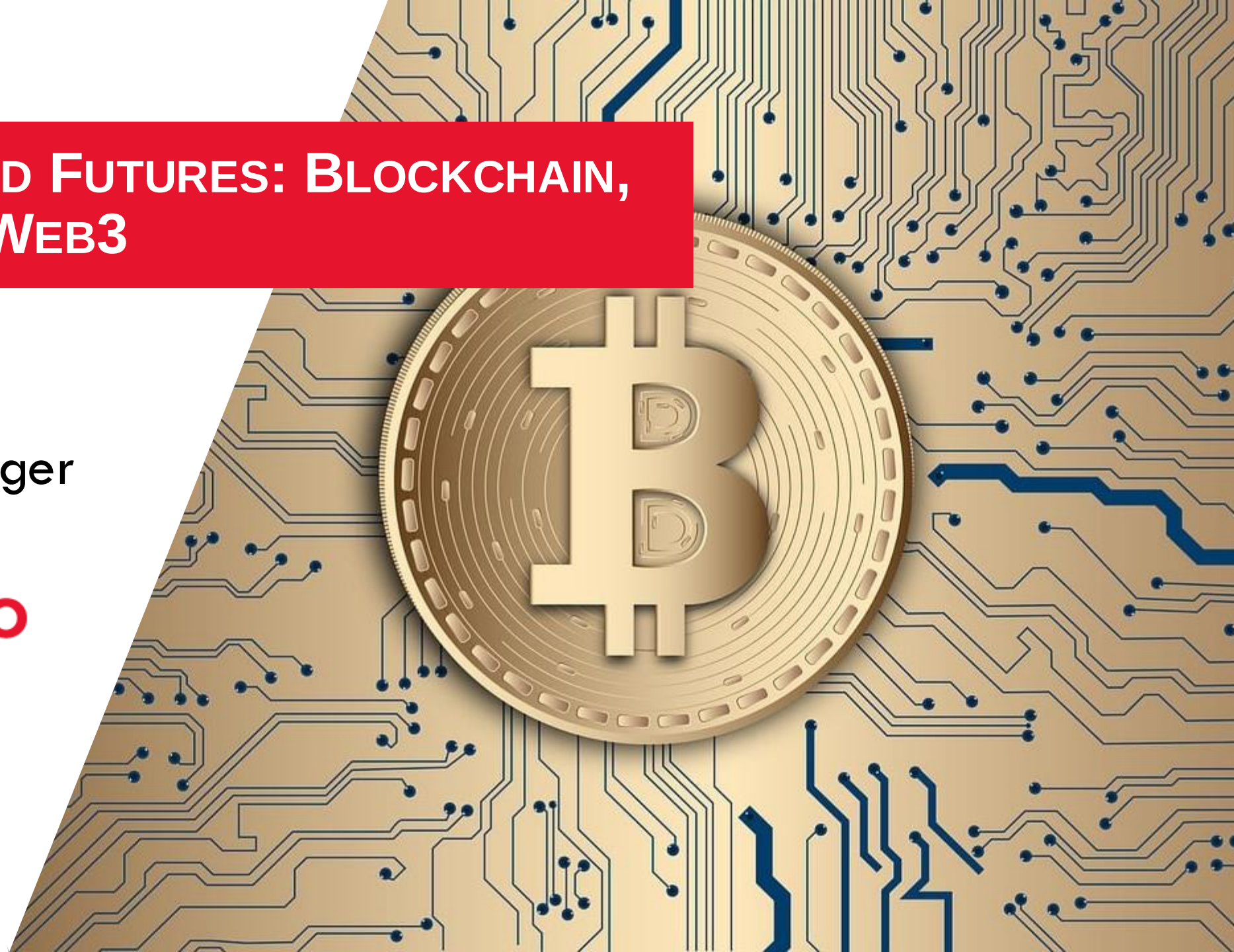
2024-2025

Decentralized Futures: Blockchain, Crypto, and Web3



Jacques-André
Fines Schlumberger

SciencesPo
ÉCOLE DU MANAGEMENT
ET DE L'INNOVATION

Objectives

- Have a clear understanding on how Blockchain technology works
  → Evolution from Traditional – Centralized – Decentralized Structures.

- Explore blockchain applications in various fields
  → Finance
  → Energy, Climate, Supply Chain, Identity…

- Imagine real DECENTRALIZED FUTURES

Plan

Session 1: Introduction to Blockchains
Session 2: Bitcoin, Ethereum & beyond
Session 3: Decentralized Finance (DeFi)
Session 4: Energy, Climate and Supply Chains
Session 5: Blockchain and Democracy
Session 6: Final Examination

Notation

- Individual or collective work on a blockchain technology or project (30%)
- Active in-class participation, and MCQ (20%)
- Final exam (50%)
  - use case or
  - essay

Let's get to know each other

1/ Quick survey

2/ Create a wordpress account here:
www.blockchain-x.eu

Session 1

Session 1: Introduction to Blockchains

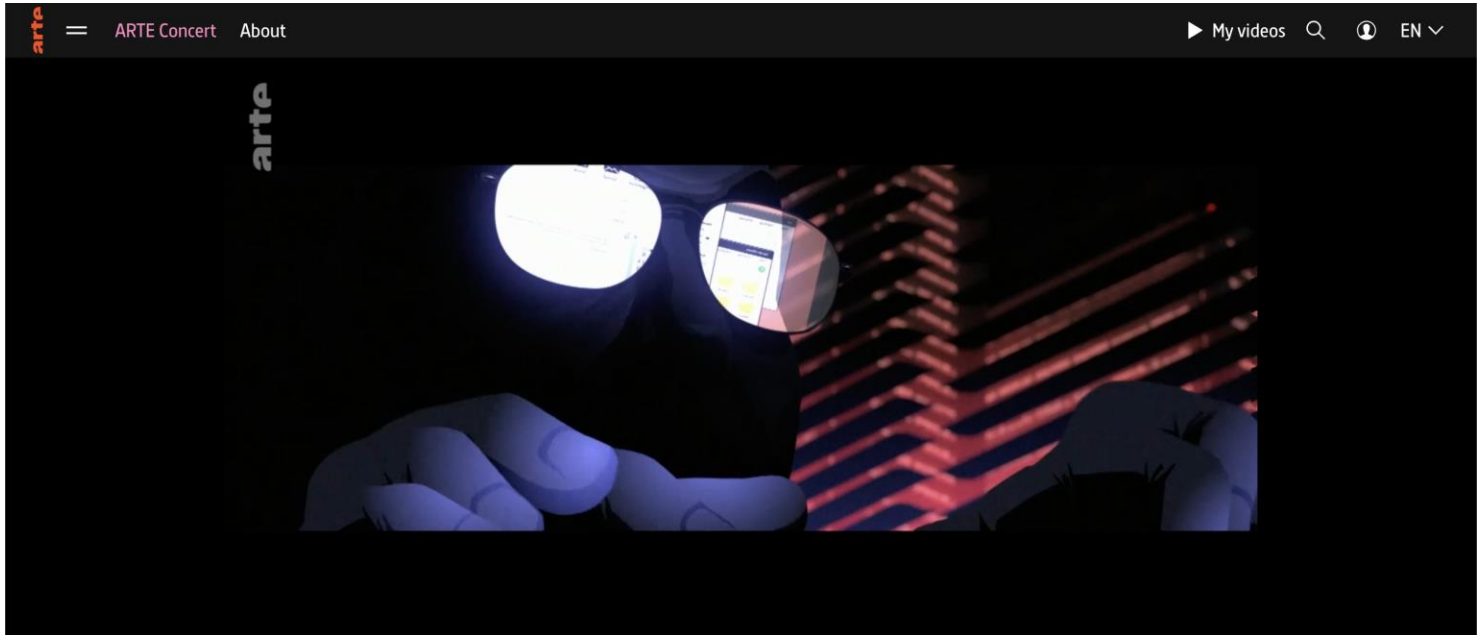
1. Required Viewing and Reading
2. History of digital cash
3. How does Blockchain work?
4. Public or private, permissioned or permissionless?
5. What type of token?
6. Custodial and non custodial wallet?

What is Bitcoin & bitcoins?

Bitcoin is a peer-to-peer currency
Peer-to-peer means that no central authority issues new money or tracks transactions. These tasks are managed collectively by the network.

The Satoshi Mystery - The Story of Bitcoin

Required viewing



https://www.arte.tv/en/videos/097372-001-A/the-satoshi-mystery-the-story-of-bitcoin/

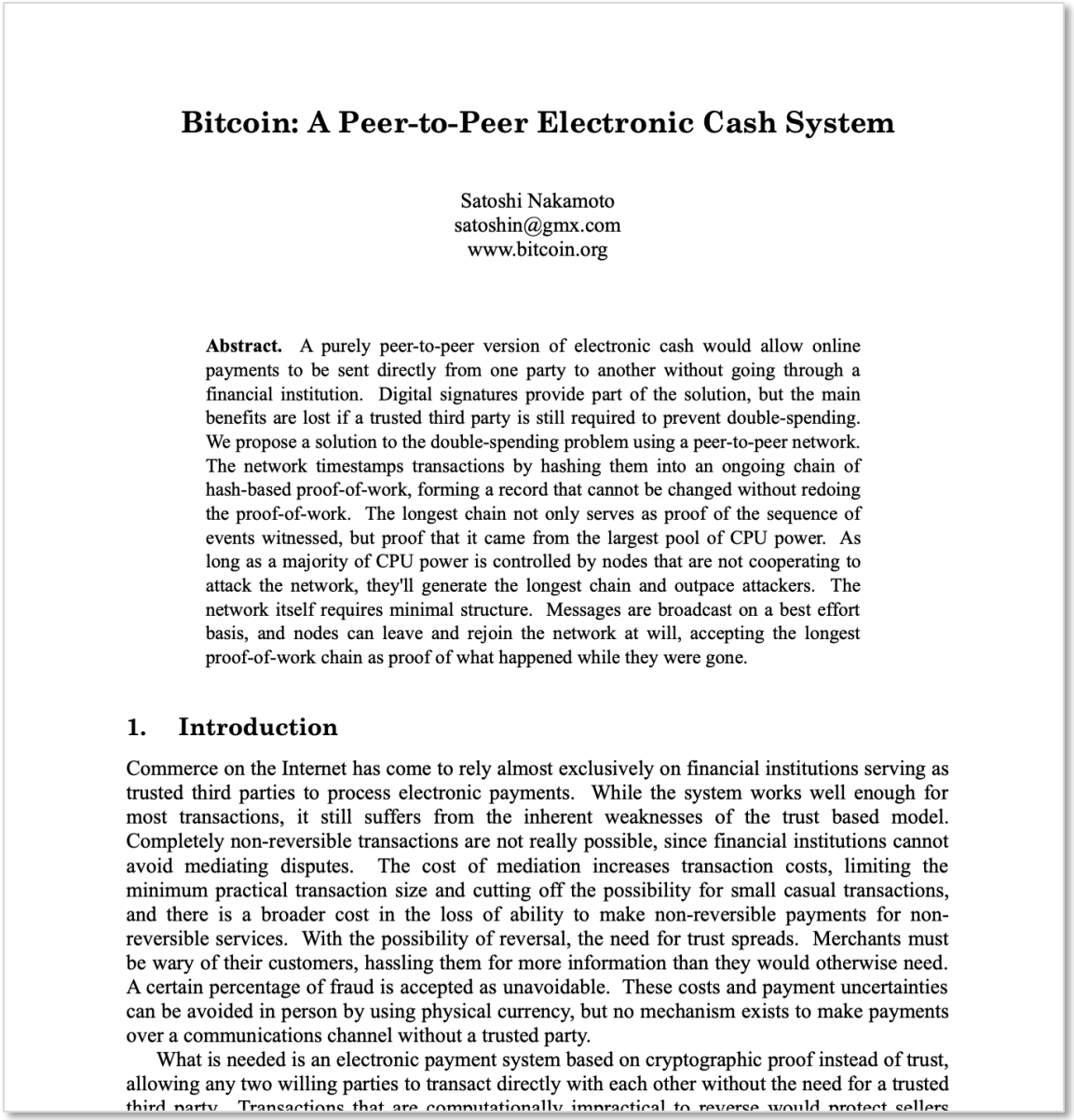
In the age of the Internet, "cypherpunks" tried to create an anonymous, autonomous, free and direct digital currency that worked without intermediaries. Many failed - but not Satoshi Nakamoto. In the middle of the subprime mortgage crisis, he was the first to publish the code for Bitcoin.

The genesis White Paper

Bitcoin: A Peer-to-Peer Electronic Cash System,
https://bitcoin.org/bitcoin.pdf, 2008

What did you read ?
What did you understand ?

Required reading



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

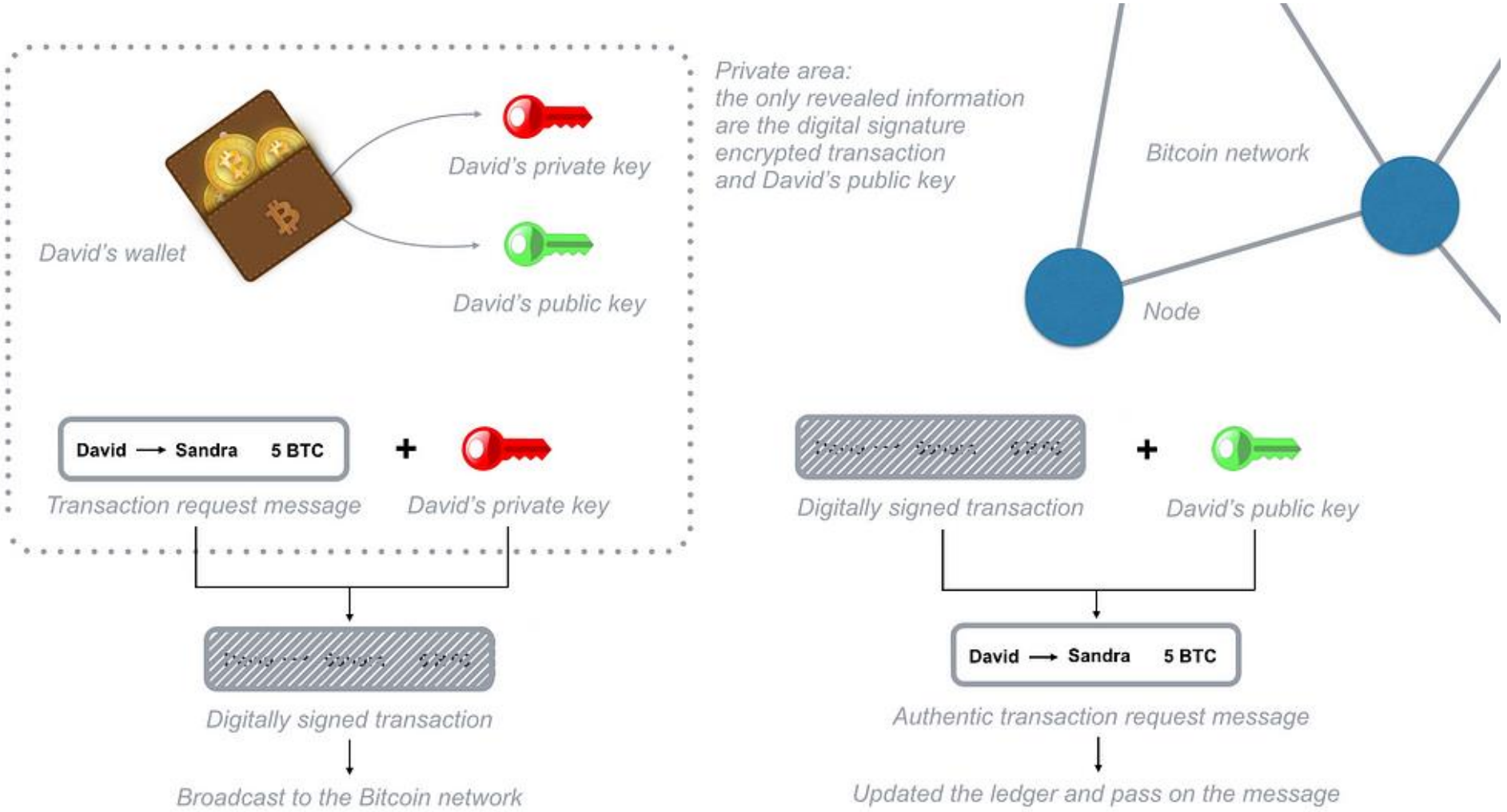
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

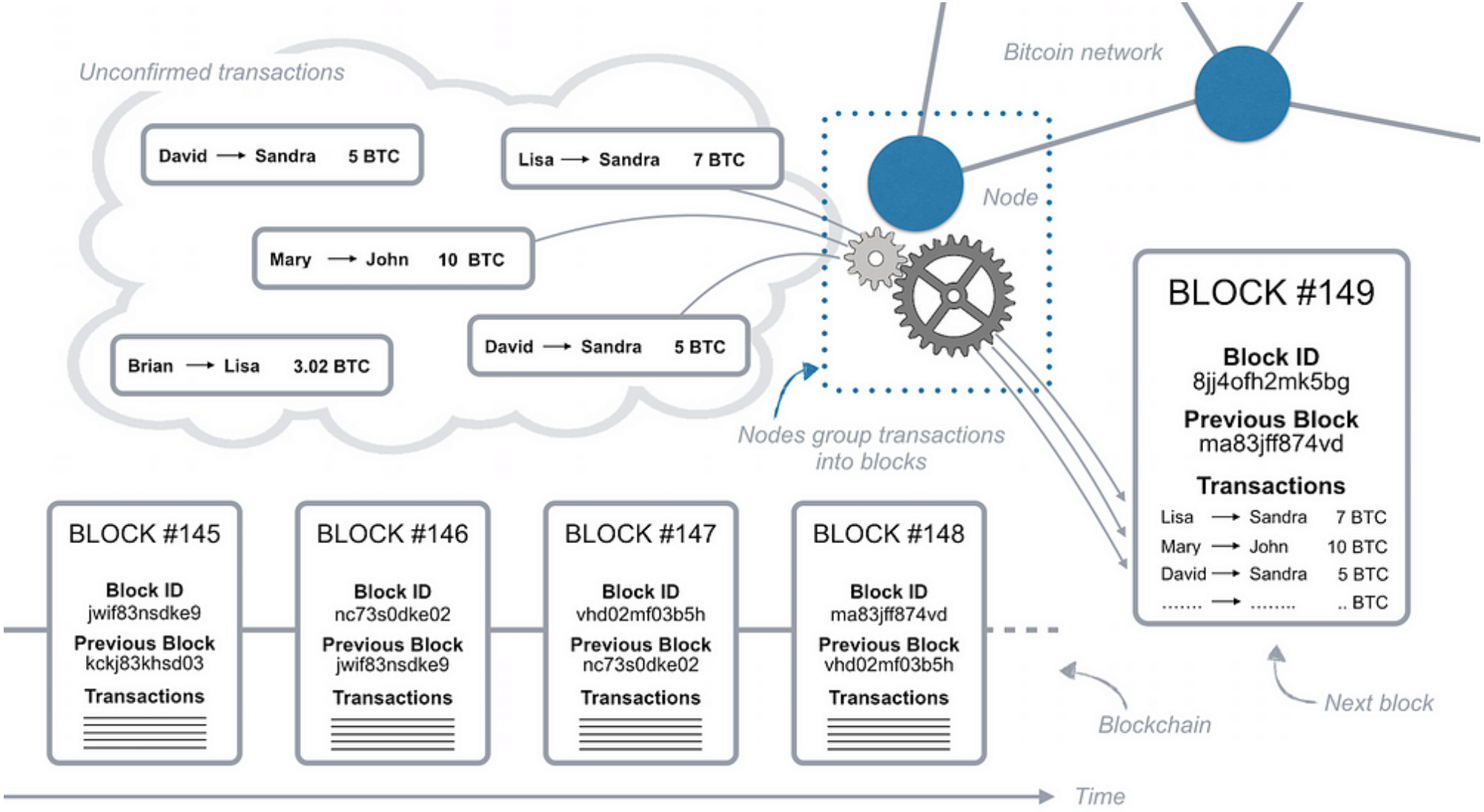
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers

1. How does Blockchain work?

1. Someone Wants to Send Bitcoin



The transaction is not yet confirmed



2. The Transaction is Broadcast to the Network

BITCOIN TRANSACTION REQUEST MESSAGE

"David sends 5 BTC to Sandra"

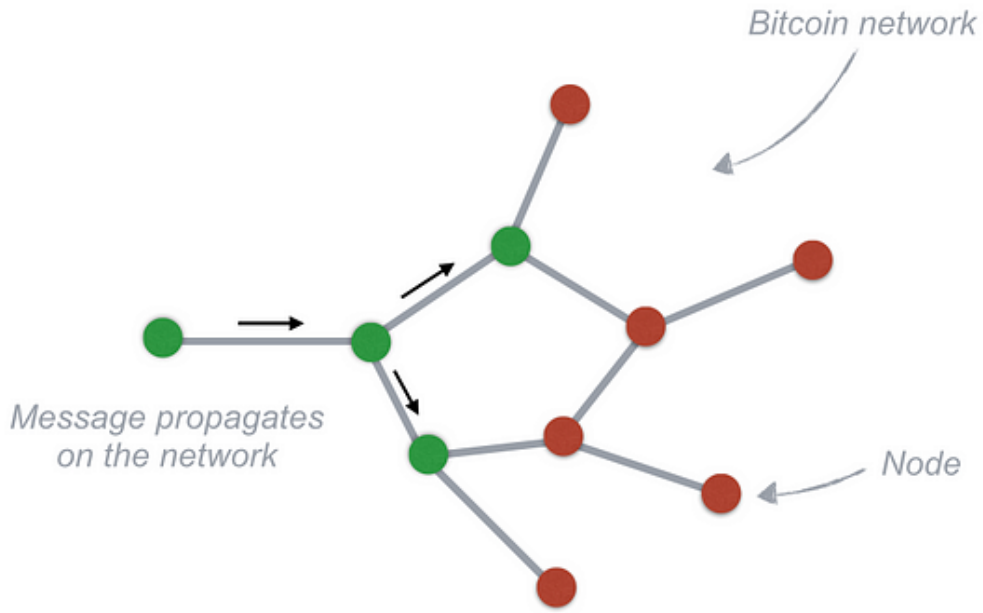
David → Sandra 5 BTC

LEDGER

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23

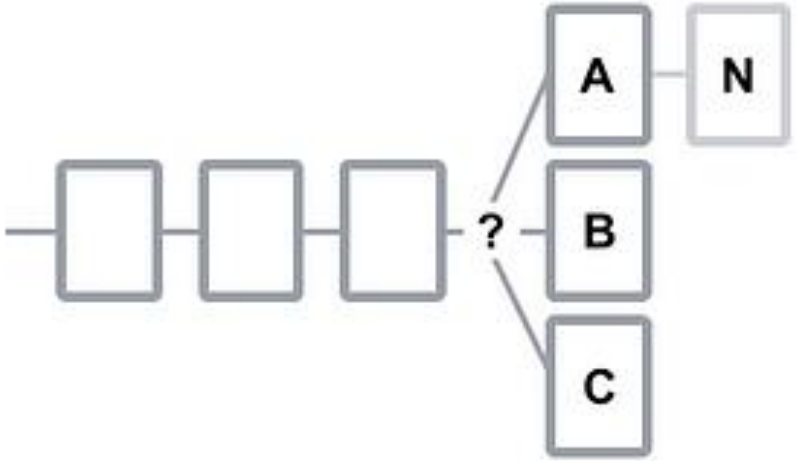
LEDGER

Account owner	Value
Mary	4
John	56
Sandra	88
Lisa	16
David	182
Brian	23

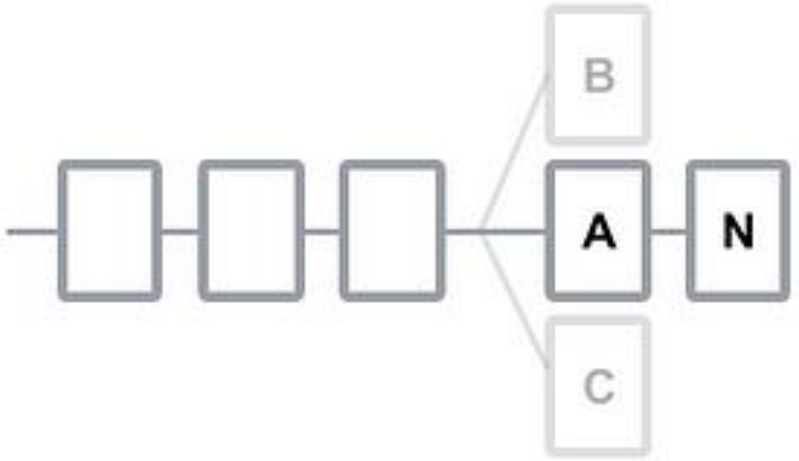


Each *node* receives the transaction request message, updates its own copy of the *ledger* and passes on the message to the nearby *nodes.*

3. Miners Get to Work (Mining Process)

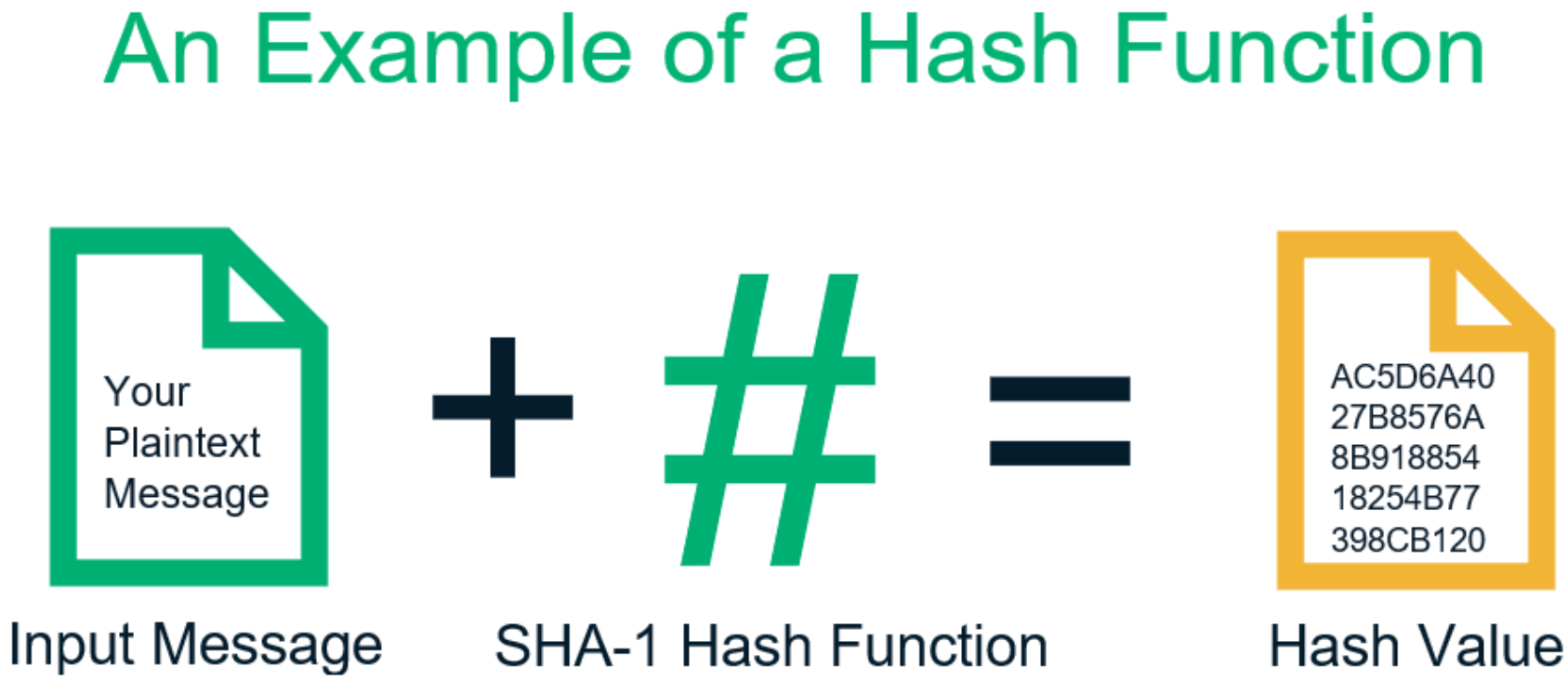


Each node than tries to add the new block (N) to the block they received first from the other nodes

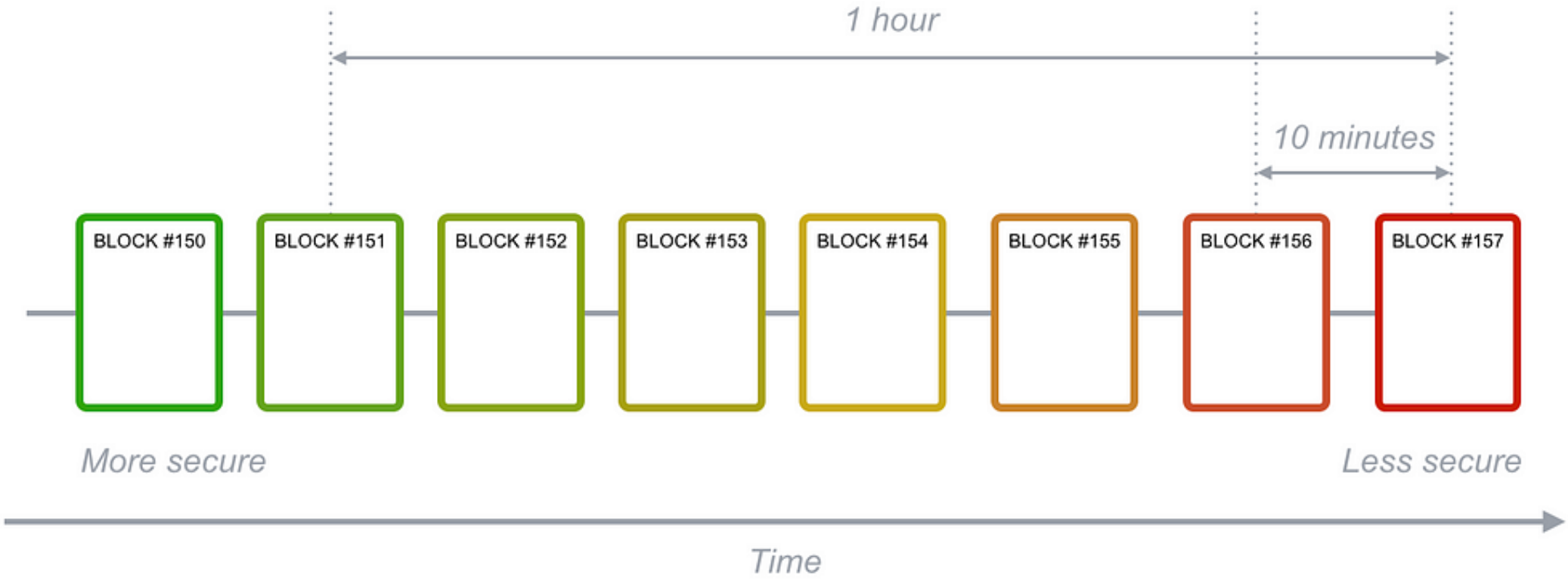


As soon as the new block (N) is added all the network adopt the longest chain possible (A+N) stabilising the whole network

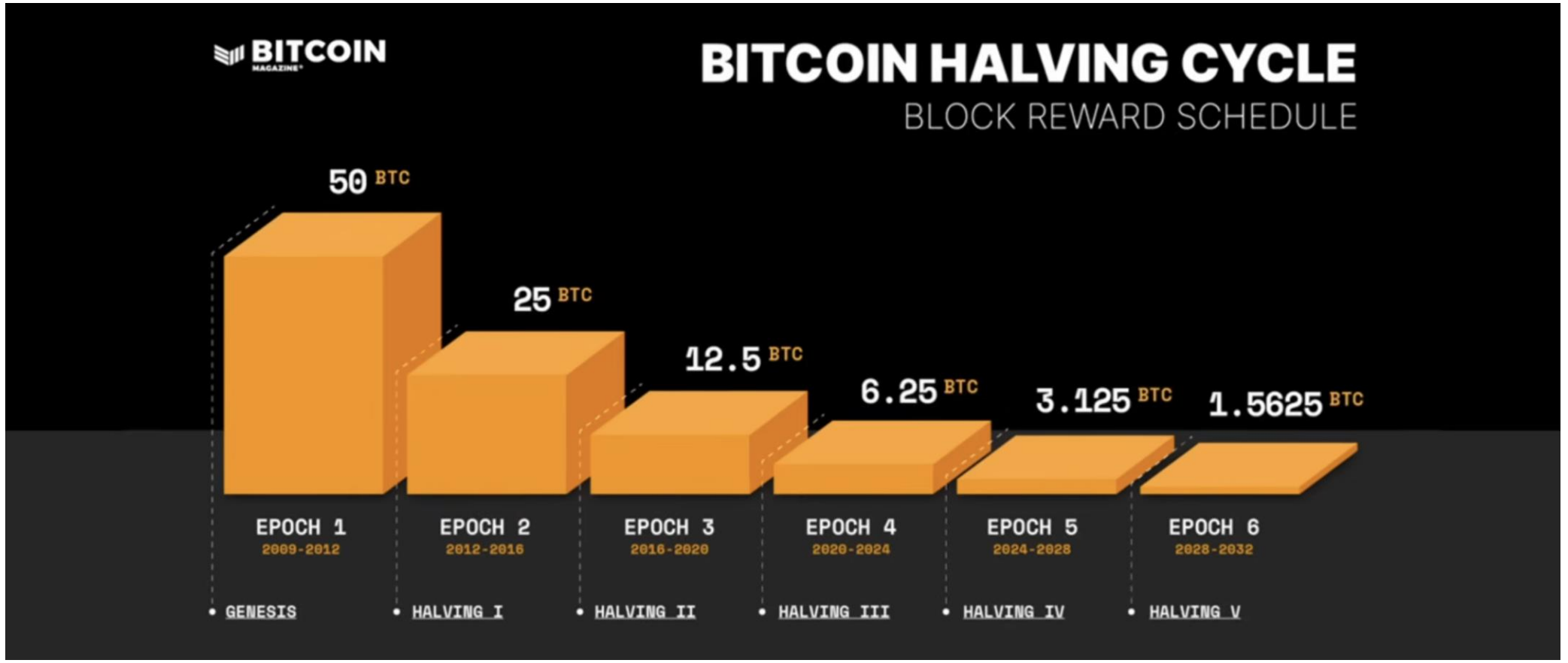
4. The Hash Function: The Secret Behind Mining



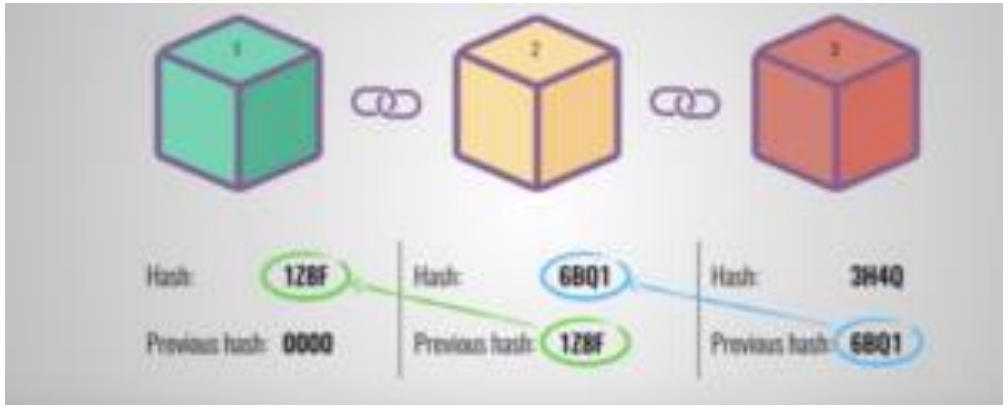
5. Adding a Block to the Blockchain

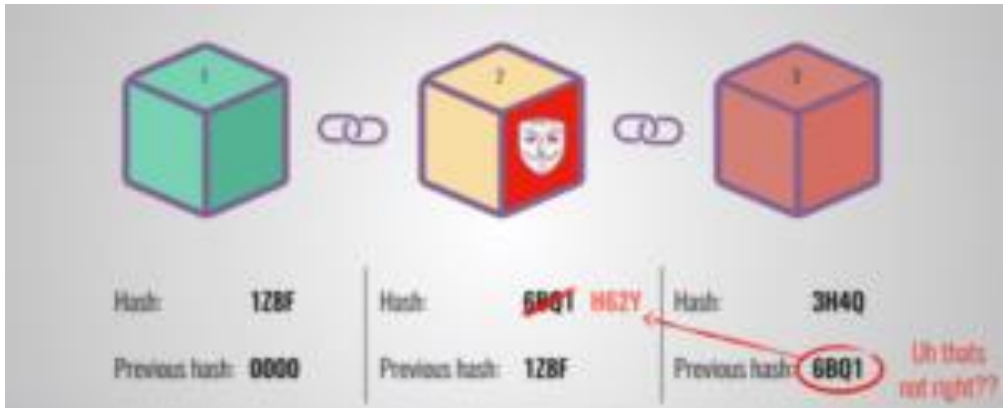


6. Miners Get Rewards



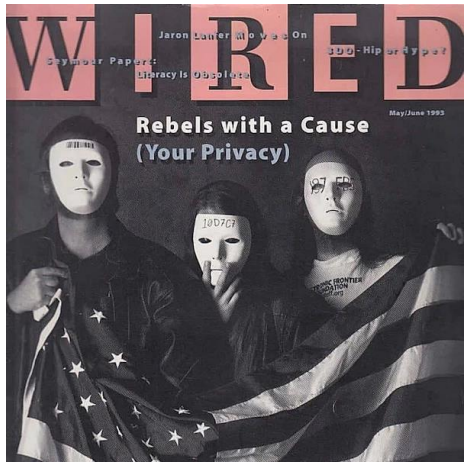
7. The Blockchain Keeps Growing





History

1990
Cypherpunk



A cypherpunk is one who advocates the widespread use of strong cryptography and privacy-enhancing technologies as a means of effecting social and political change.

1993
A Cypherpunk's Manifesto

David Chaum and DigiCash (1990s)

Adam Back and Hashcash (1997)

Wei Dai and B-Money (1998)

Nick Szabo and Bit Gold (1998-2005)

Hal Finney and Reusable POW (2004)

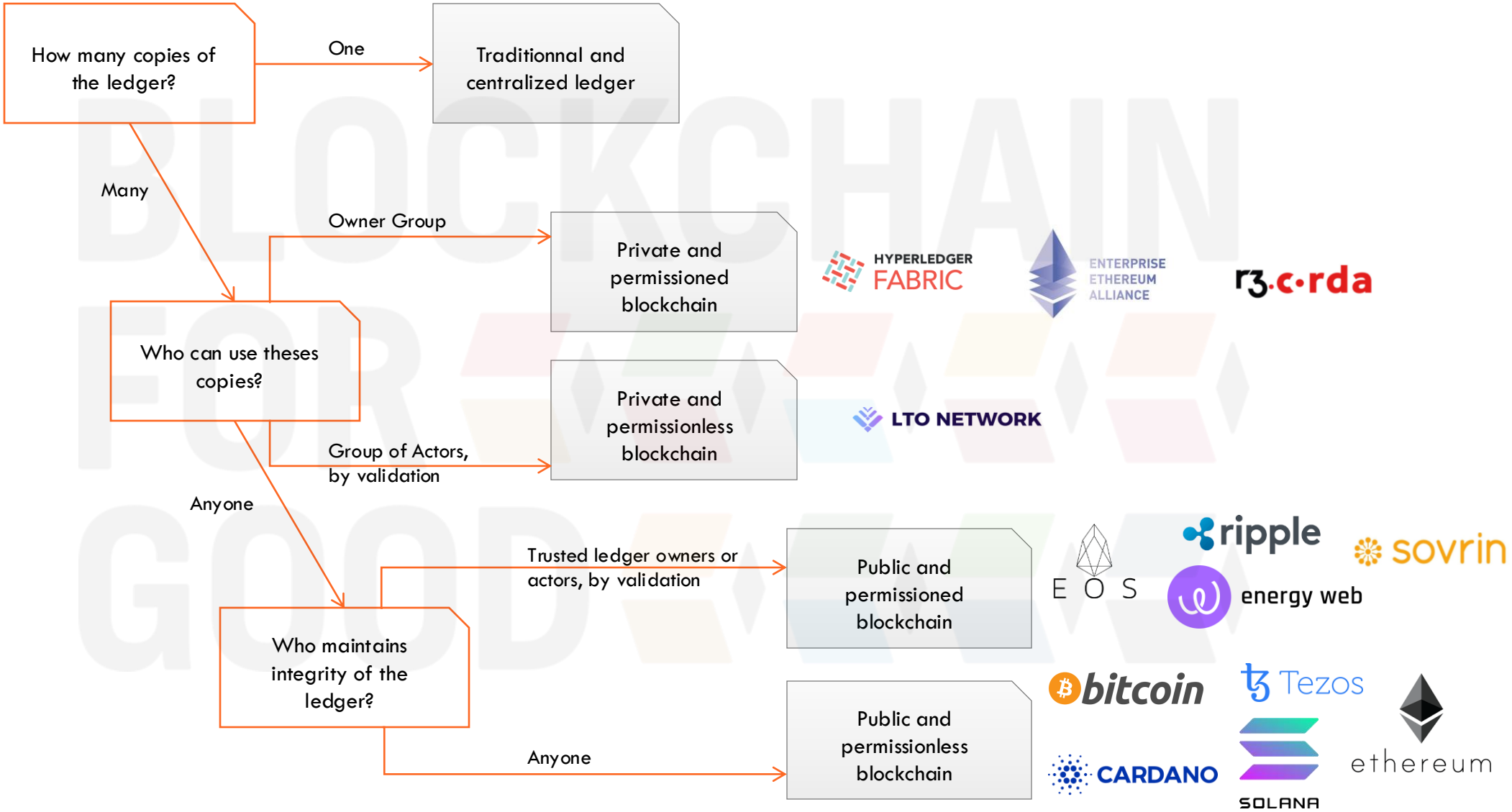
History

2009

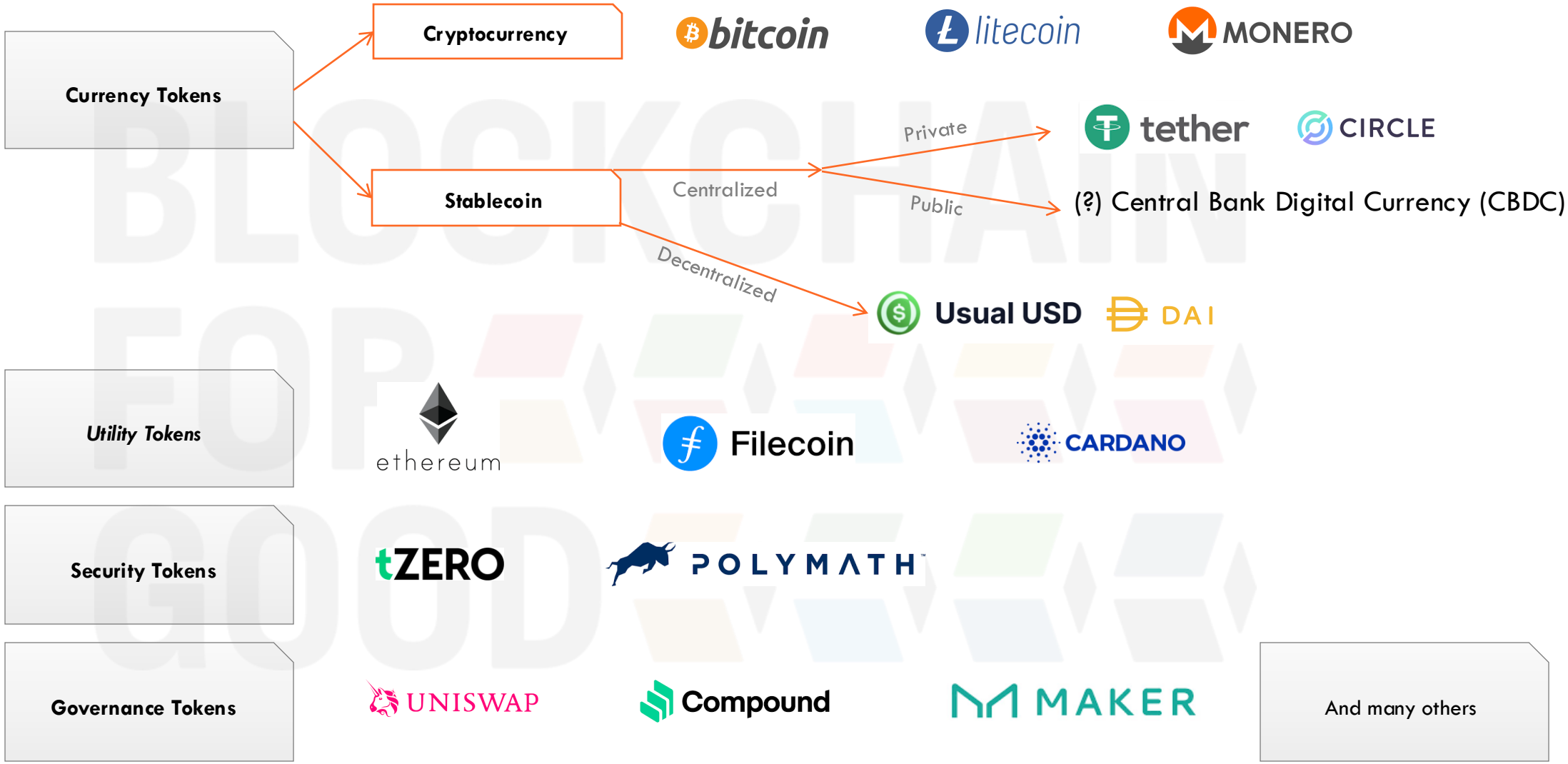
2015

2017

Public or private, permissioned or permissionless?



What type of token?



A token can serve multiple functions and, for example, be simultaneously a utility, security, and governance token

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is **$2.65T**, a ▼ 0.29% decrease over the last day. Read More

Trending Coins

1	NEI	$0.008262	▲ 14.85%
2	TRUMP	$10.45	▲ 1.39%
3	PEPE	0.0_5$6707	▲ 1.53%
4	SNAI	$0.024	▲ 1.21%
5	BNB	$581.6	▲ 4.44%

Trending on DexScan

1	MERY/WCRO	$0.00002122	▼ 11.23%
2	STAR10/WBNB	$0.01469	▲ 31.85%
3	MATEZ/USDT	$17.78	▲ 7.47%
4	oGPU/WETH	$0.4149	▼ 1.76%
5	WEPE/WETH	$0.00005477	▲ 8.19%

Market Cap

$2.65T

▼ 0.29%

CMC100

$159.79

▼ 0.80%

Fear & Greed

21

Fear

Altcoin Season

15/100

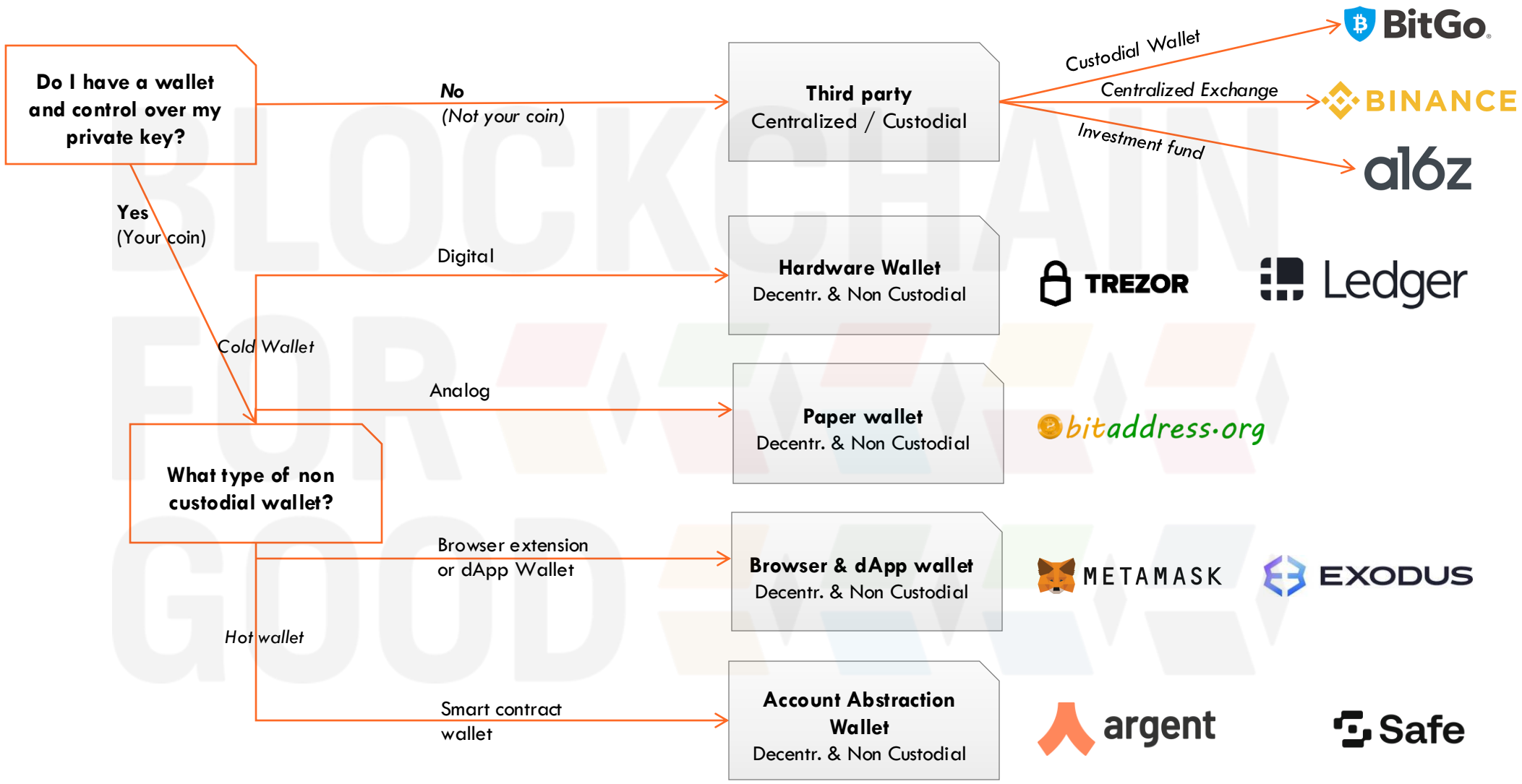
Bitcoin Altcoin

All Crypto | NFTs | Categories | Token unlocks | Rehypo | Memes | SOL | DOT | BNB | USA | AI | RWA | Gaming | DePIN | DeFAI | AI Agents

Coins | DexScan | Top | Trending | New | Gainers | Most Visited | Filters | Columns

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$80,956.61	▼0.51%	▼1.34%	▼10.41%	$1,605,885,839,084	$30,185,828,851 372.65K BTC	19.83M BTC	

Custodial or non-custodial wallet?



What is a non-custodial wallet?

To share

Adresse Bitcoin:
13feMFheEzwPcBJpqcpKaoBWJc9pqR6wb3

Clé Privée:
KxHjQp4jXDGSujcfvP9xH5dgVkk68nyyE1ME92NZf6pbReUucH4B

To keep secret

bitaddress.org

Session 2

Session 2: Bitcoin, Ethereum & beyond

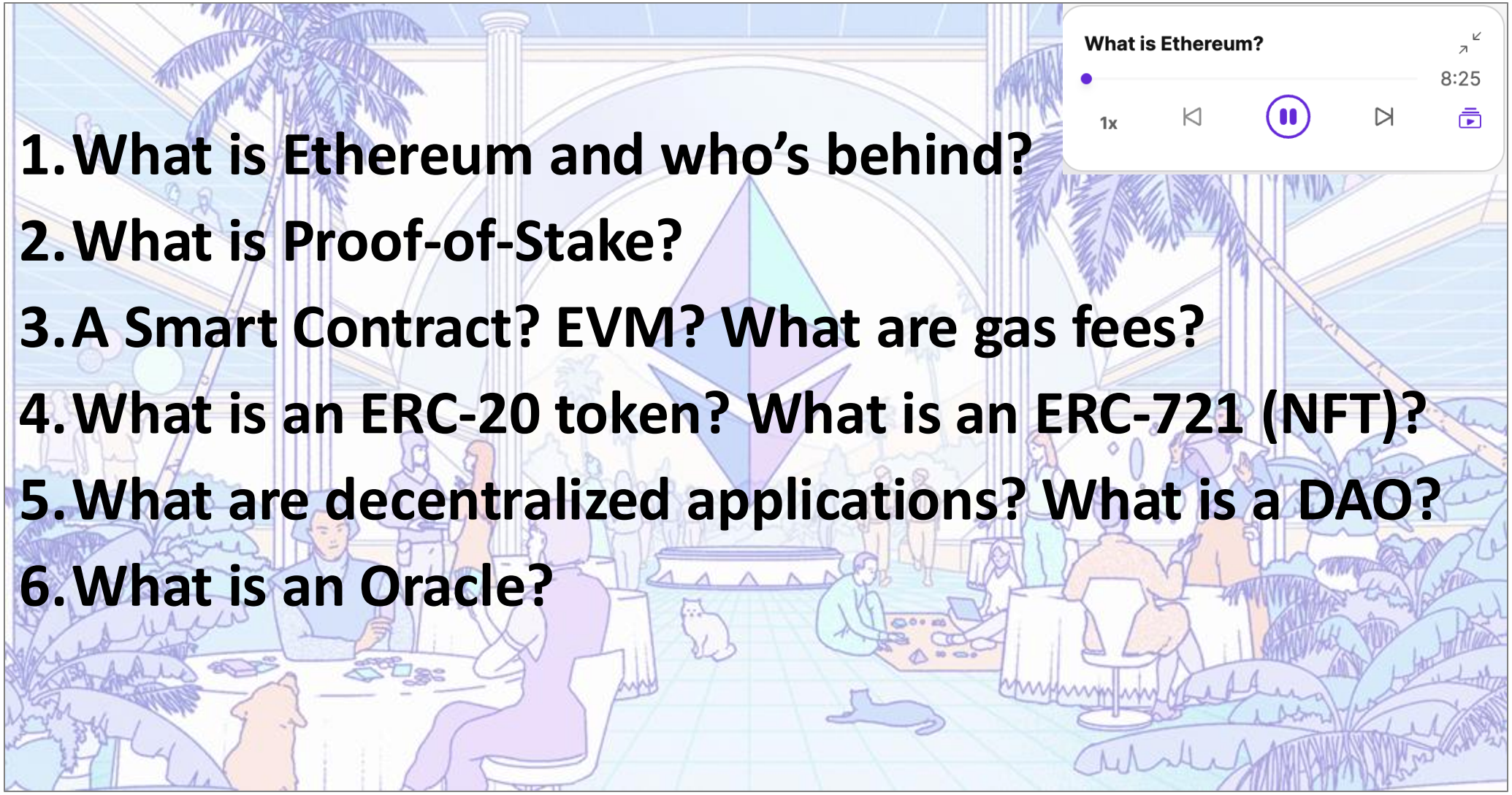
Previous session: ARTE, White paper, What type of token?

1. **Bitcoin: What are the Environmental Concerns of Bitcoin?**
   Collective discussion
2. **What is Ethereum and who's behind?** What is **Proof-of-Stake?** A **Smart Contract? EVM**? What are **gas fees**? What is an **ERC-20 token**? What is a **NFT**? What are **decentralized applications**? What is a **DAO**? What is an **Oracle?**
3. **What is the blockchain trilemma?**
4. **What is a layer 1, a layer 2? A native and non-native token?**
5. **Individual work: Analyze the 23 first tokens of…**

What are the Environmental Concerns of Bitcoin?

Source : https://ccaf.io/cbnsi/cbeci

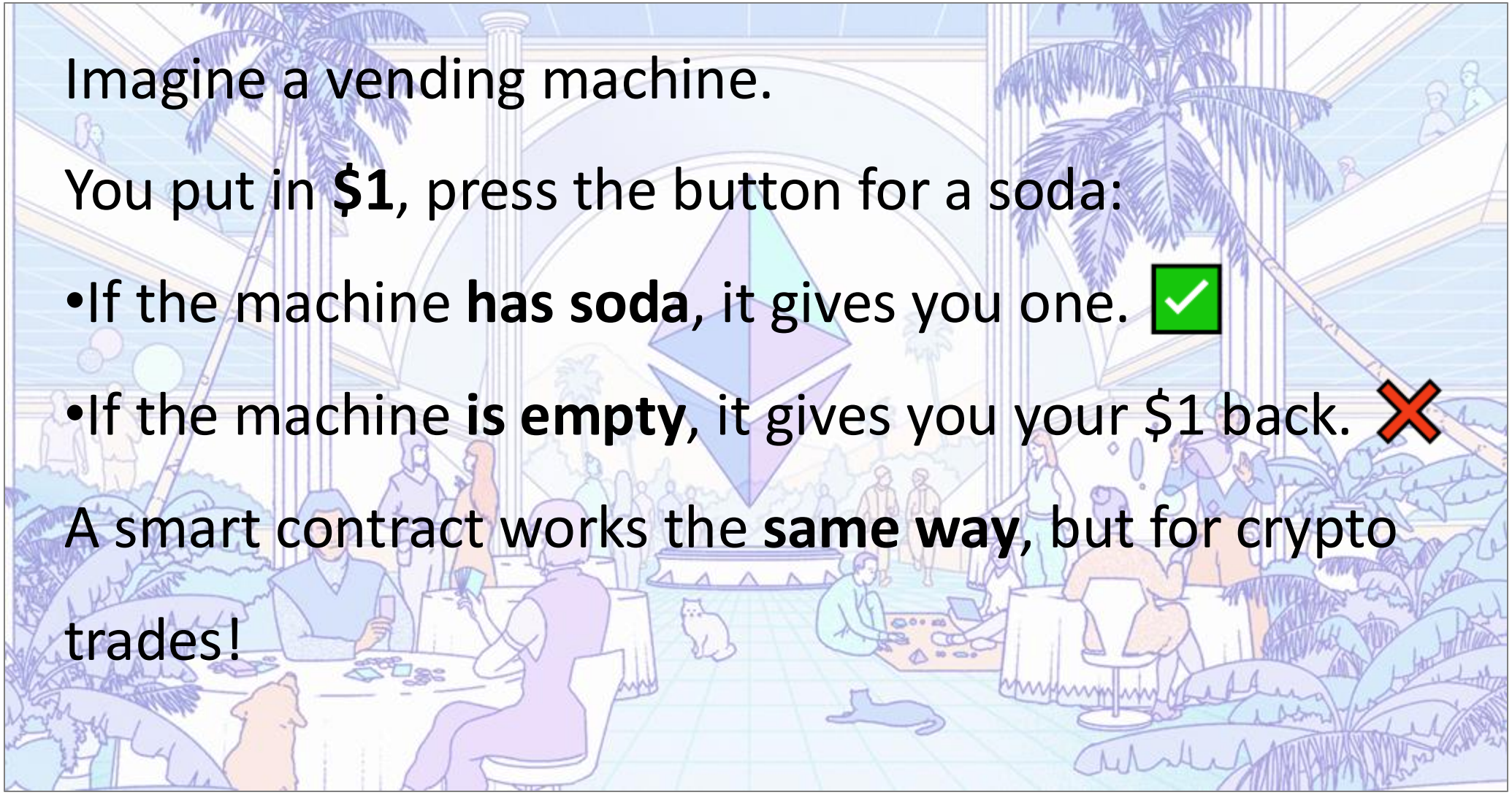
What is Ethereum?



1. What is Ethereum and who's behind?
2. What is Proof-of-Stake?
3. A Smart Contract? EVM? What are gas fees?
4. What is an ERC-20 token? What is an ERC-721 (NFT)?
5. What are decentralized applications? What is a DAO?
6. What is an Oracle?

Source : https://ethereum.org

What is a smart contract?



Imagine a vending machine.

You put in **$1**, press the button for a soda:

- If the machine **has soda**, it gives you one. ✅
- If the machine **is empty**, it gives you your $1 back. ❌

A smart contract works the **same way**, but for crypto trades!

What can Ethereum do?

Banking for everyone

Not everyone has access to financial services. An internet connection is all you need to access Ethereum and the lending, borrowing and savings products built on it.

An open internet

Anyone can interact with Ethereum network or build applications on it. This allows you to control your own assets and identity, instead of them being controlled by a few mega-corporations.

A peer-to-peer network

Ethereum allows you to coordinate, make agreements or transfer digital assets directly with other people. You don't need to rely on intermediaries.

Censorship-resistant

No government or company has control over Ethereum. Decentralization makes it nearly impossible for anyone to stop you from receiving payments or using services on Ethereum.

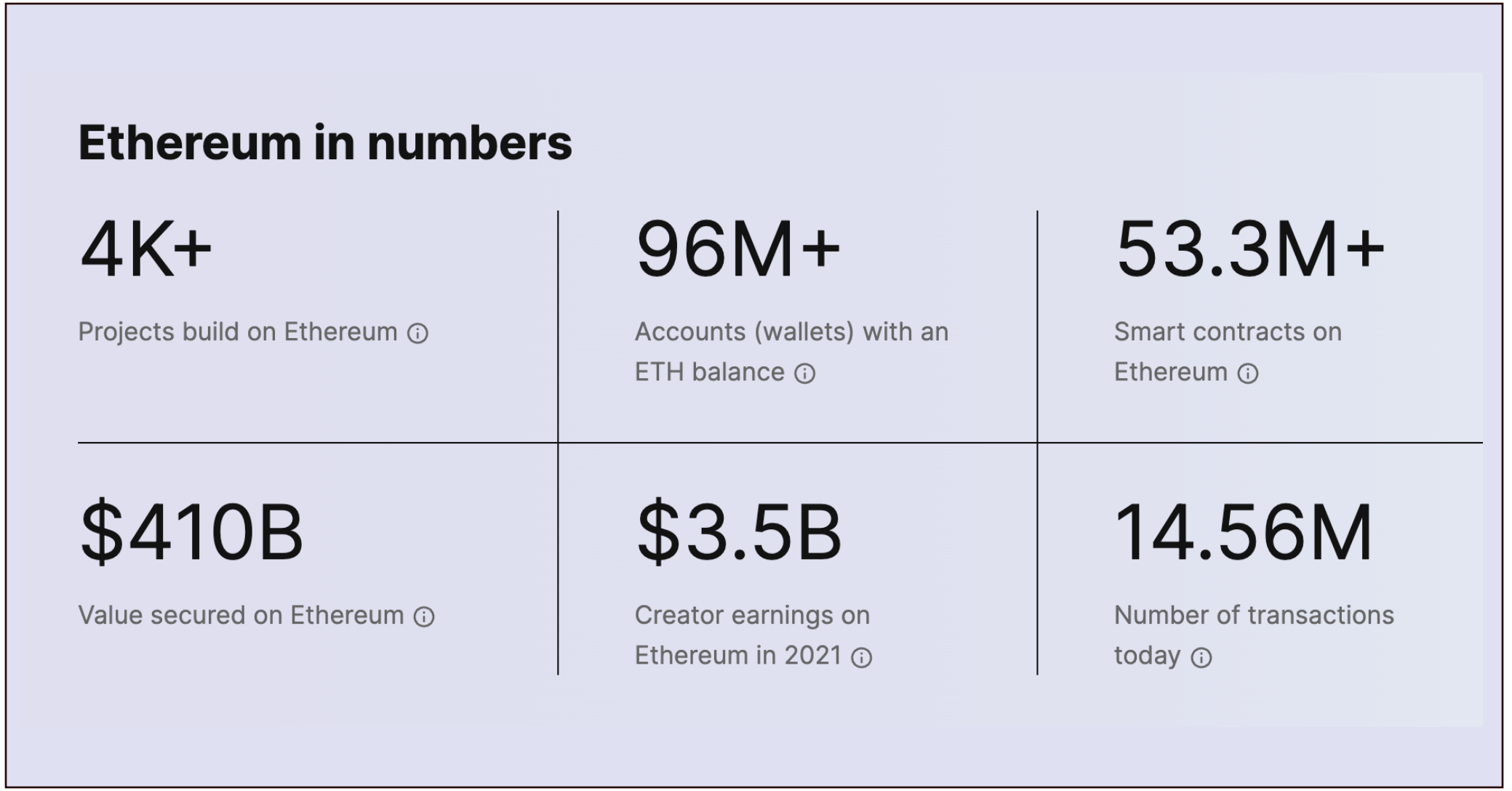
Commerce guarantees

Customers have a secure, built-in guarantee that funds will only change hands if you provide what was agreed. Likewise, developers can have certainty that the rules won't change on them.

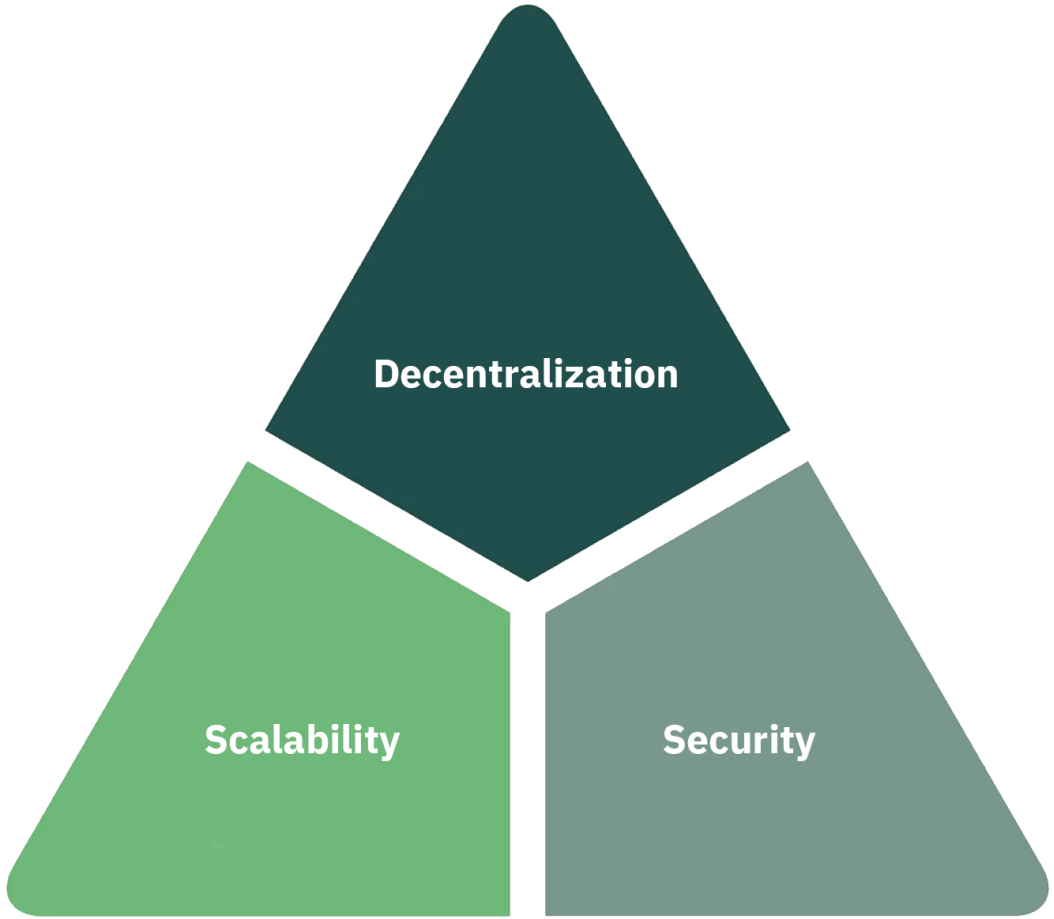
Composable products

All apps are built on the same blockchain with a shared global state, meaning they can build off each other (like Lego bricks). This allows for better products and experiences and assurances that no-one can remove any tools apps rely upon.

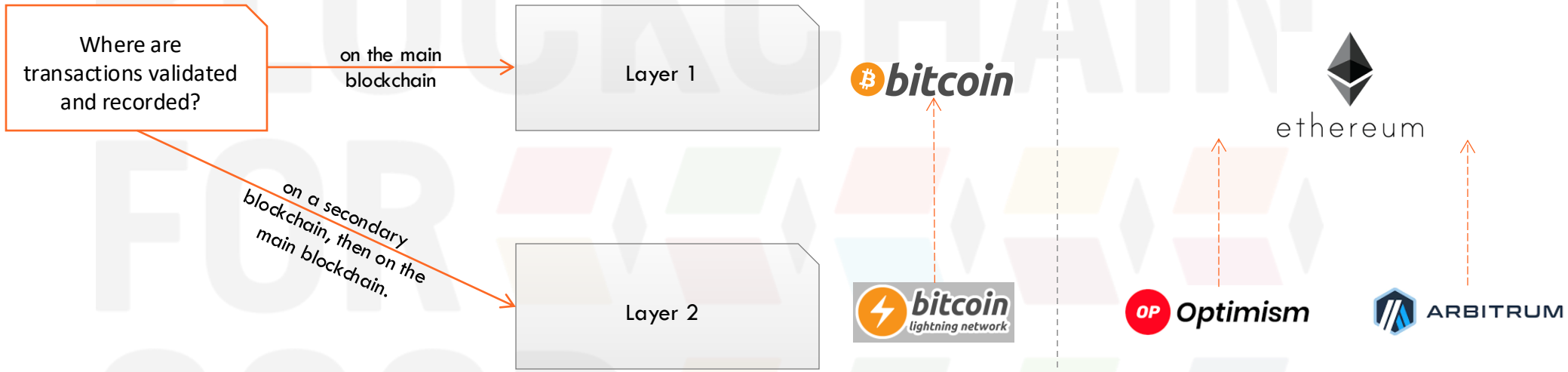
A few numbers



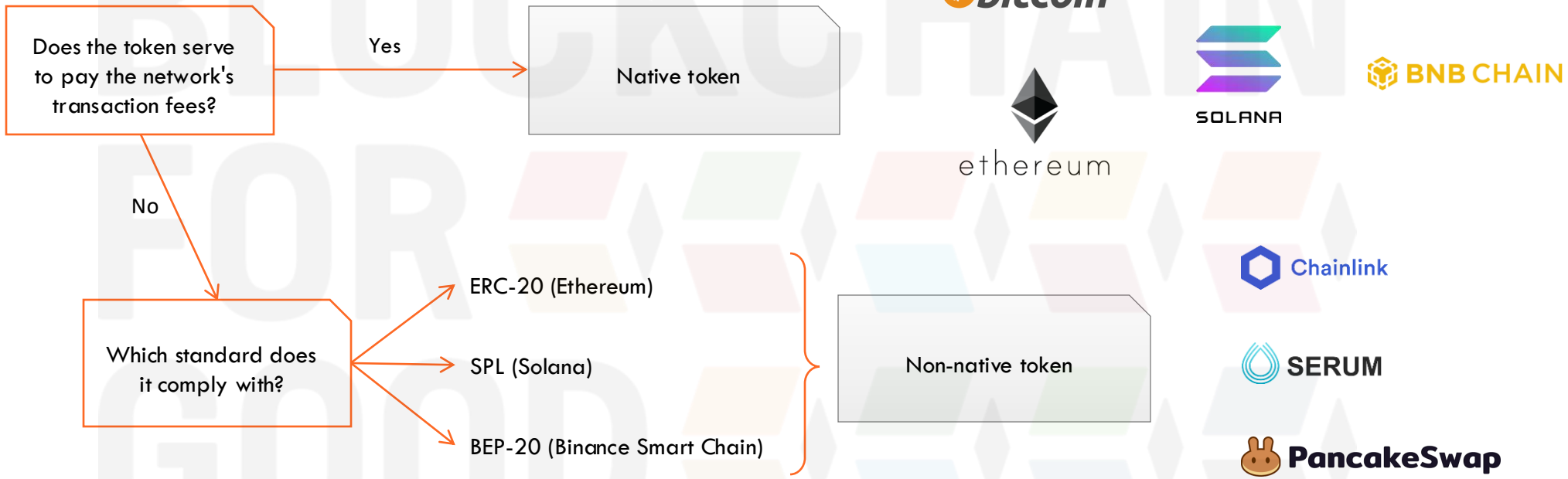
The Blockchain trilemma



Main blockchain - Layer 1 or secondary - Layer 2?



Native or not native token?

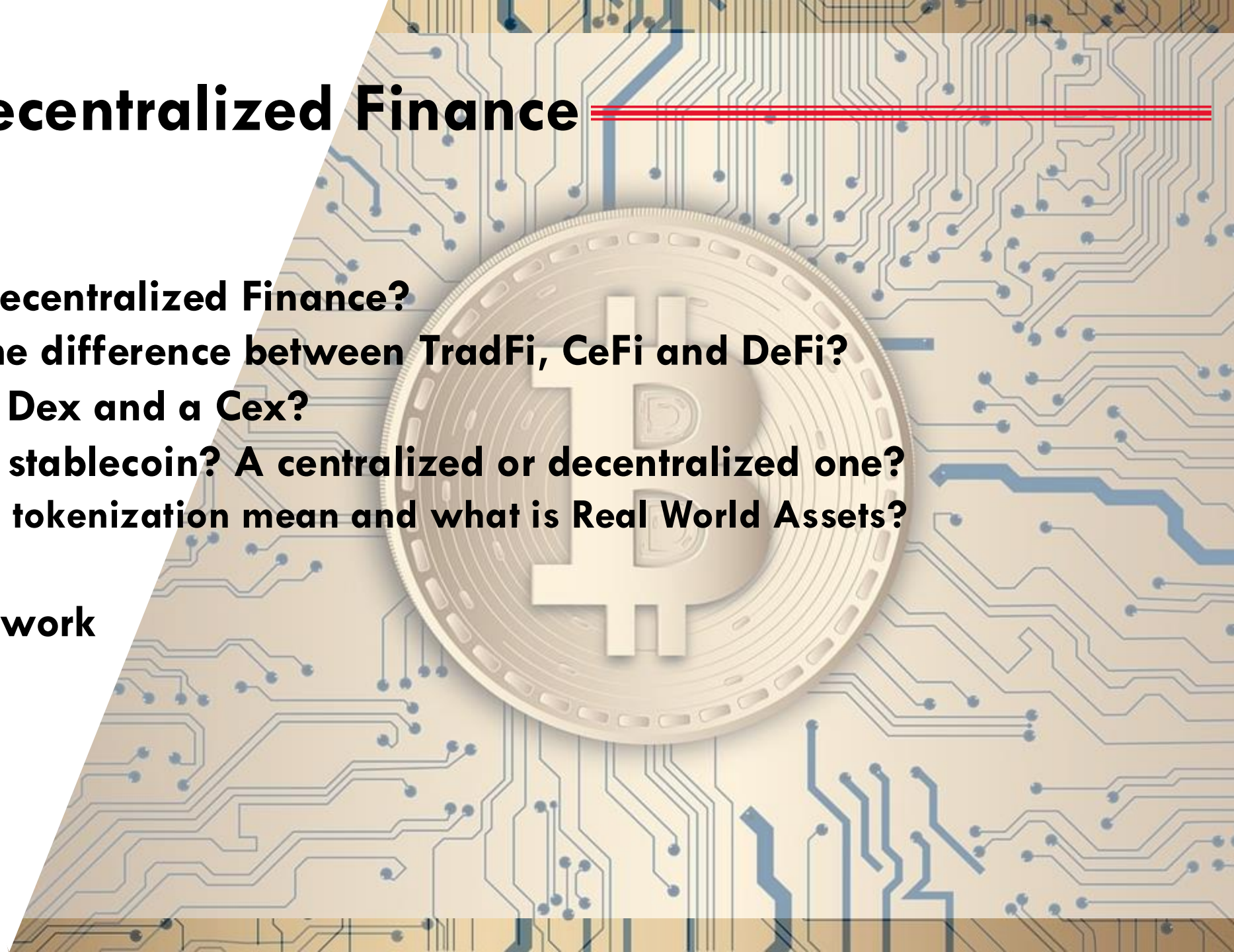


Individual work:
Analyze* the
23 first tokens of…

* Replace Bitcoin with Lightning Network and skip Ethereum

Session 3

Session 3: Decentralized Finance



1. What is Decentralized Finance?
2. What is the difference between TradFi, CeFi and DeFi?
3. What is a Dex and a Cex?
4. What is a stablecoin? A centralized or decentralized one?
5. What does tokenization mean and what is Real World Assets?

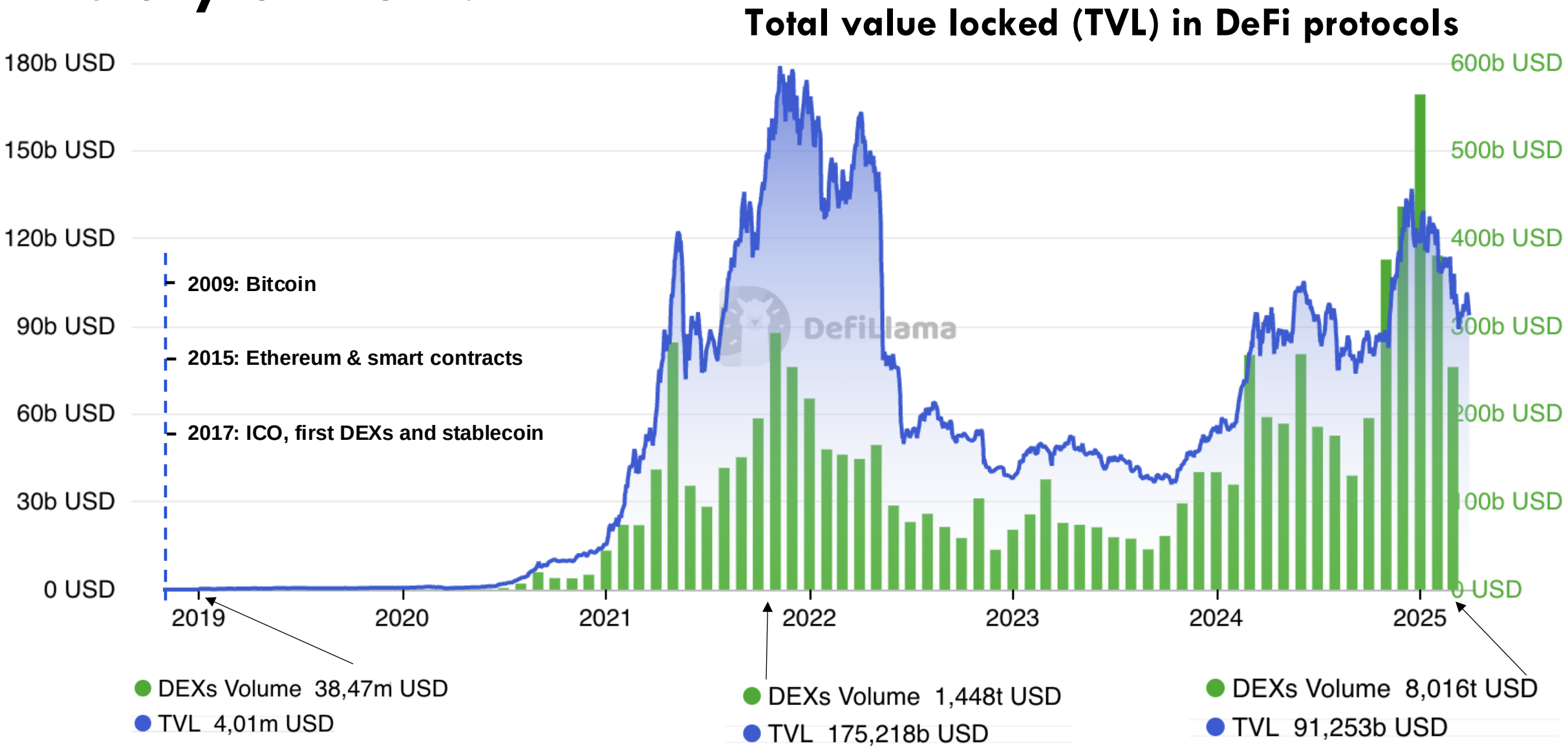
6. Individual work

What is DeFi?

Decentralized finance refers to the blockchain-based ecosystem of permissionless and transparent financial services.

2017

History of DeFi?



Why is DeFi so revolutionary?

Financial Inclusion

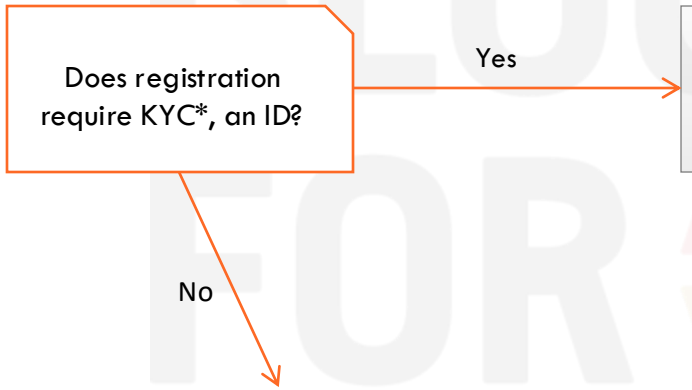
Censorship Resistance

Transparency and Security

Lower Costs

Innovation and Flexibility

Centralized or decentralized Exchange?



BINANCE

kraken

- The platform is centralized
- It holds clients' funds
- Transactions are validated through an order book system
- High liquidity
- Potential targets for attacks

UNISWAP

Curve

- Users keep their funds in their wallets
- Exchanges are made directly between users via smart contracts
- Smart contracts may contain vulnerabilities

*Know your customer, or KYC, is the process of verifying the identity of a company's clients

How a DEX Trade Uses Smart Contracts?

Let's say you have 1 Ethereum (ETH),
and you want to swap it for USDC

Step-by-Step Explanation

p. 24 - a wallet
p. 29 - Smart contract

So, DeFi works with

Smart Contracts

On a public and permissionless Blockchain

With Tokens (often non native)

Governed in a decentralized way

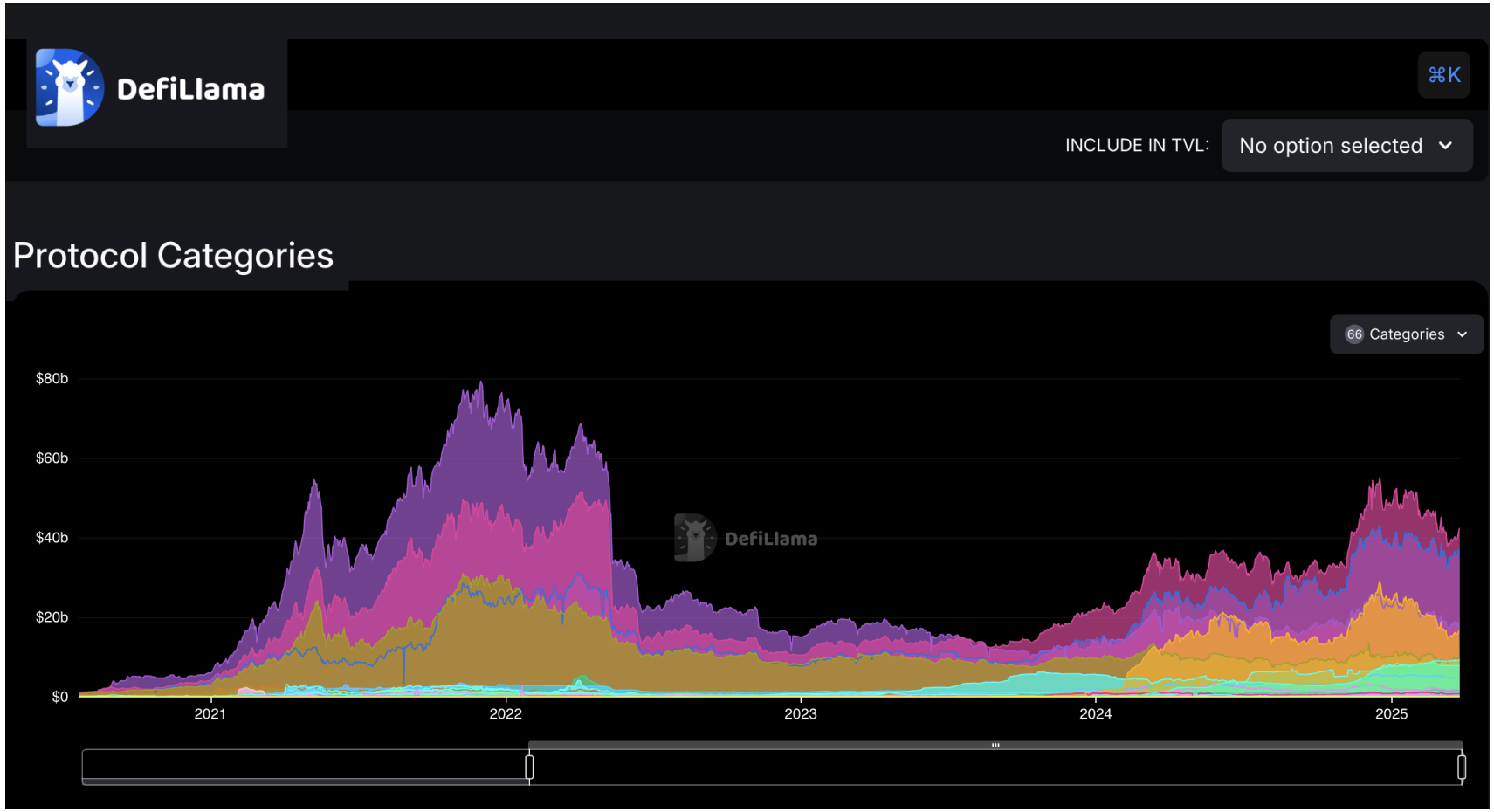
And with Oracles

TradFi – CeFi – DeFi?

TradFi – CeFi – DeFi?

	Cryptocurrencies and blockchains		Traditional Finance (TradFi)
Services	**Decentralized Finance (DeFi)**	**Centralized Finance (CeFi)**	
Exchange (Trading)	Decentralized Stablecoins *Ex : DAI, Usual* Decentralized Exchange (DEX) *Ex : Uniswap*	Centralized Stablecoins *Ex : USDC* Centralized Exchange (CEX) *Ex : Binance*	Fiat Money *Ex : Euro, dollar* Exchanges and brokers *Ex : Paris stock exchange*
Loans and borrowings	Decentralized Exchange *Ex : Compound*	Crypto bank Ex : BlockFi	Commercial Bank Professional lenders Ex : Crédit Agricole
Investments	Decentralized Funds, DAO Ex : MolochDAO	Crypto Investment Funds Ex : A16Z	Investment Funds, ETP (Exchange Traded Product) Ex : BlackRock

What type of decentralized financial services?

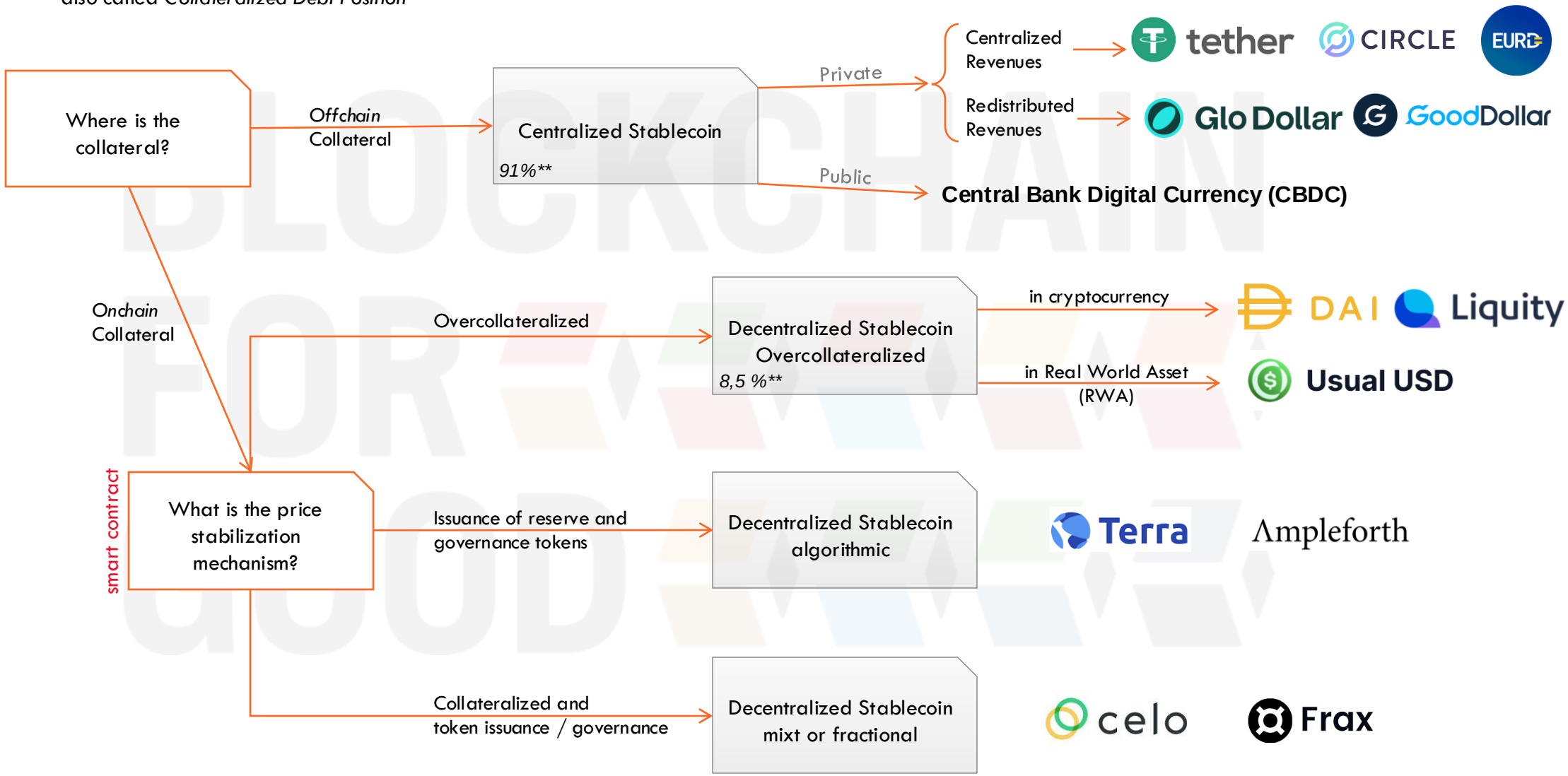


Mar 25, 2025

- Lending $41,737b
- Dexs $19,678b
- Restaking $16,414b
- CDP $9,886b
- Derivatives $4,848b
- Bridge $3,215b
- Cross Chain Bridge $1,775b
- Farm $1,729b
- Indexes $511,37m
- Payments $508,73m
- Others $2,9b

Centralized or decentralized stablecoin*?

*also called *Collateralized Debt Position*



**...of the total Stablecoin Supply, 225 billion $ in March 2025. Dune & Artemis Stablecoin_Report, March 2025.

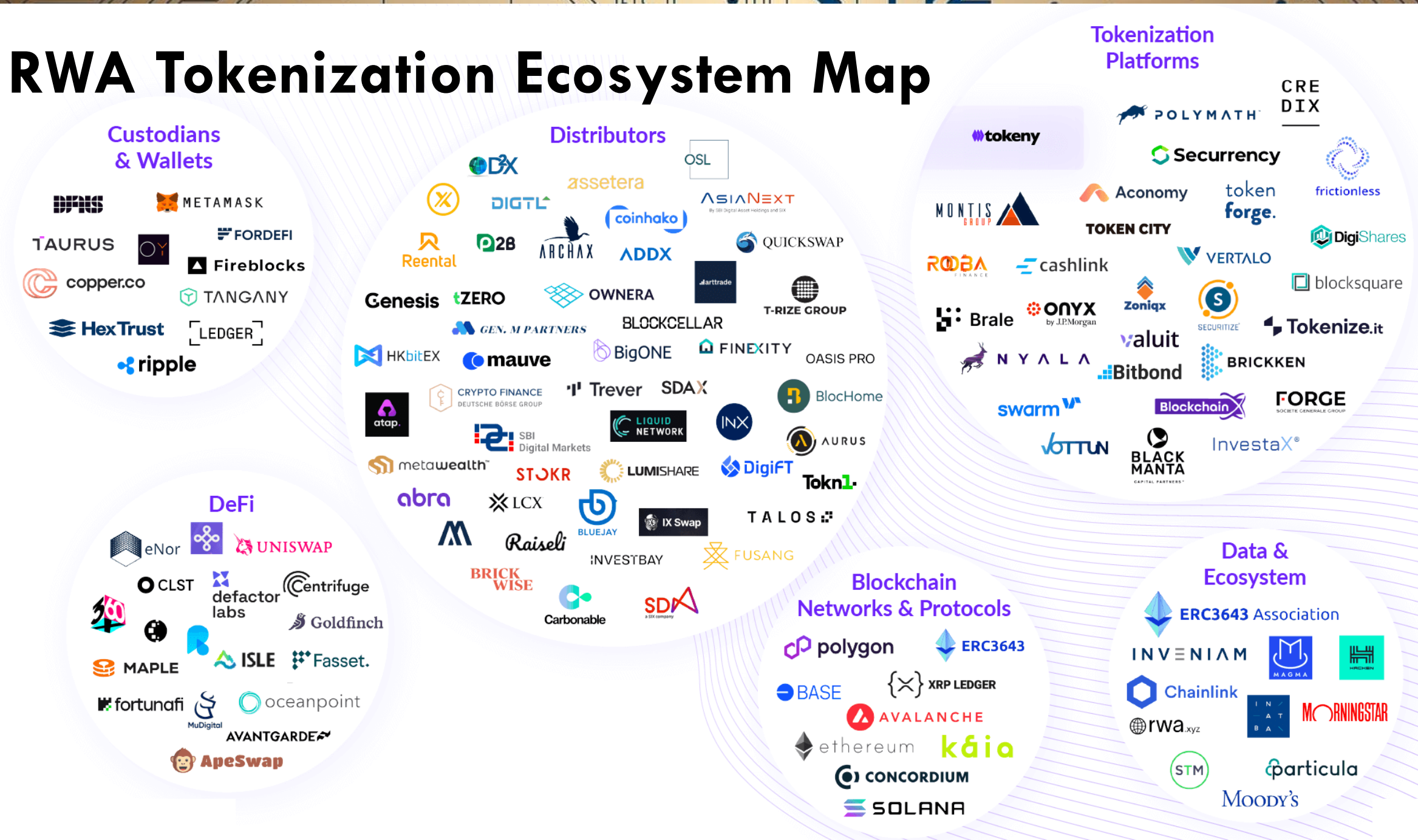
What does tokenization mean?

Tokenization refers to the process of converting rights to an asset, a service, or a unit of value into a digital representation - a "token" - on a public blockchain.

Examples: dollar, electricity, carbon credit, energy certificate, gold, real estate, fine art…

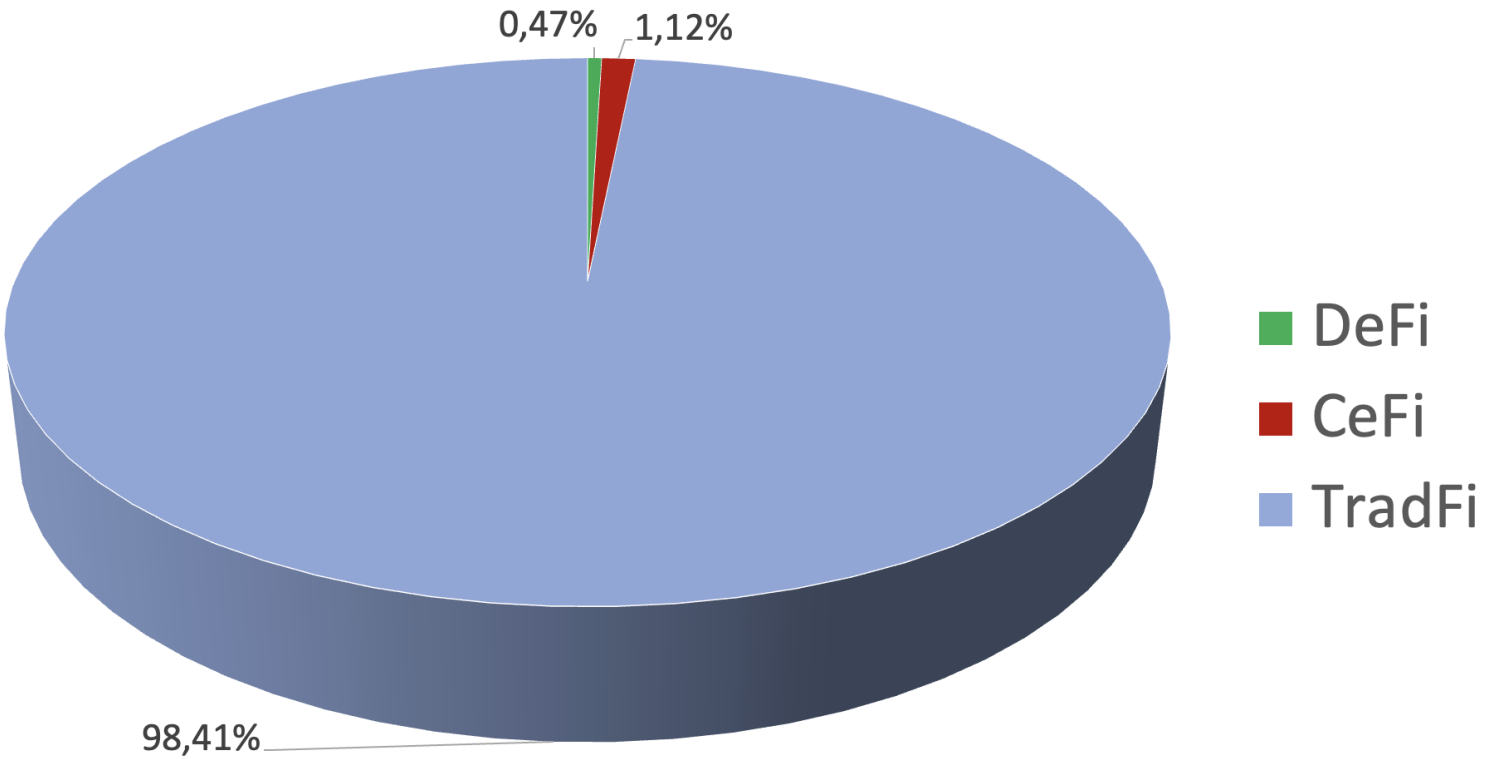
1. Fractional Ownership
2. Liquidity
3. Transparency and Trust
4. Automation of Processes

RWA Tokenization Ecosystem Map

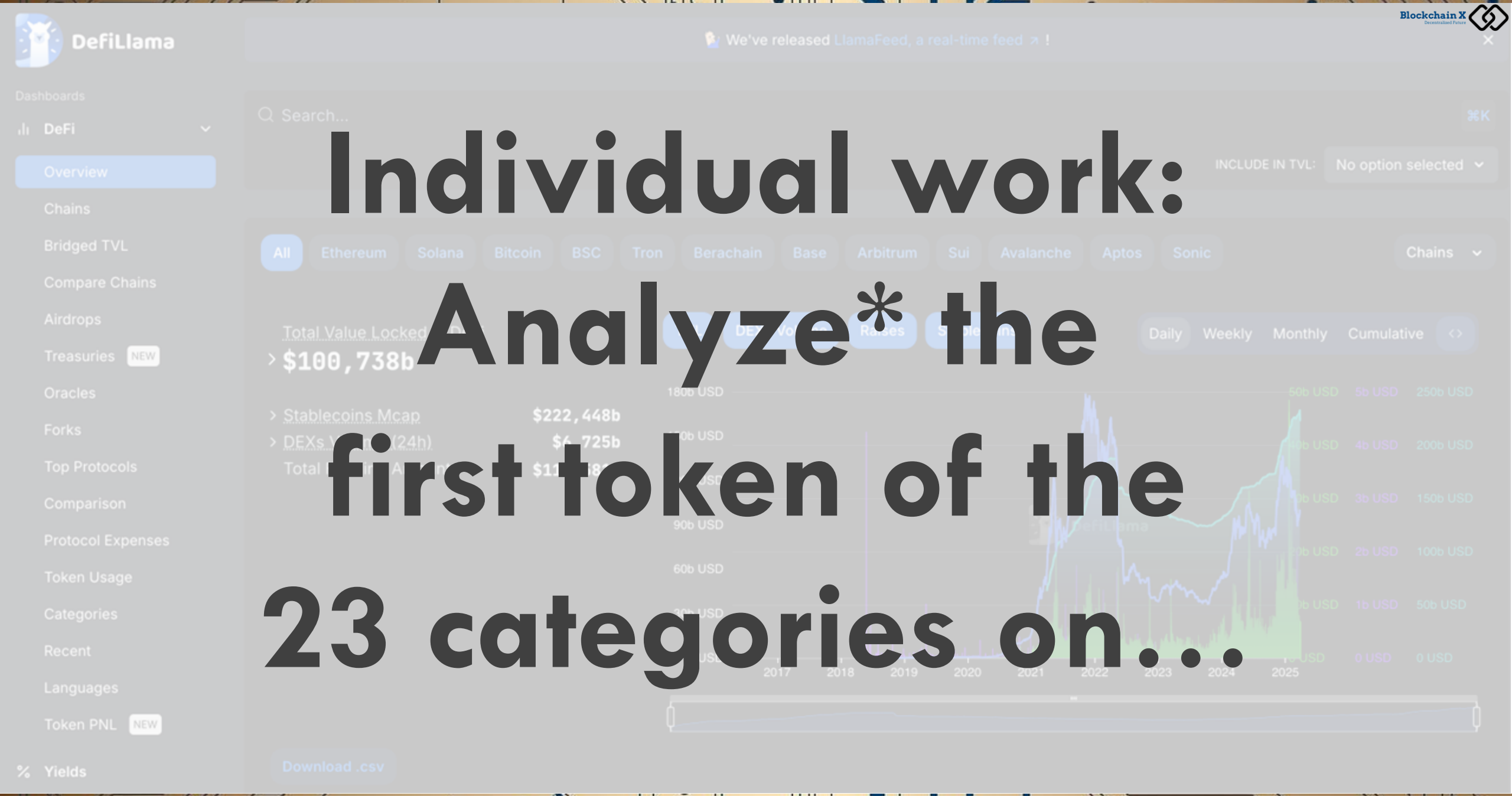


Source: https://tokeny.com/

Financial Capitalization of TradFi, CeFi & DeFi?



Individual work: Analyze* the first token of the 23 categories on...



Session 4

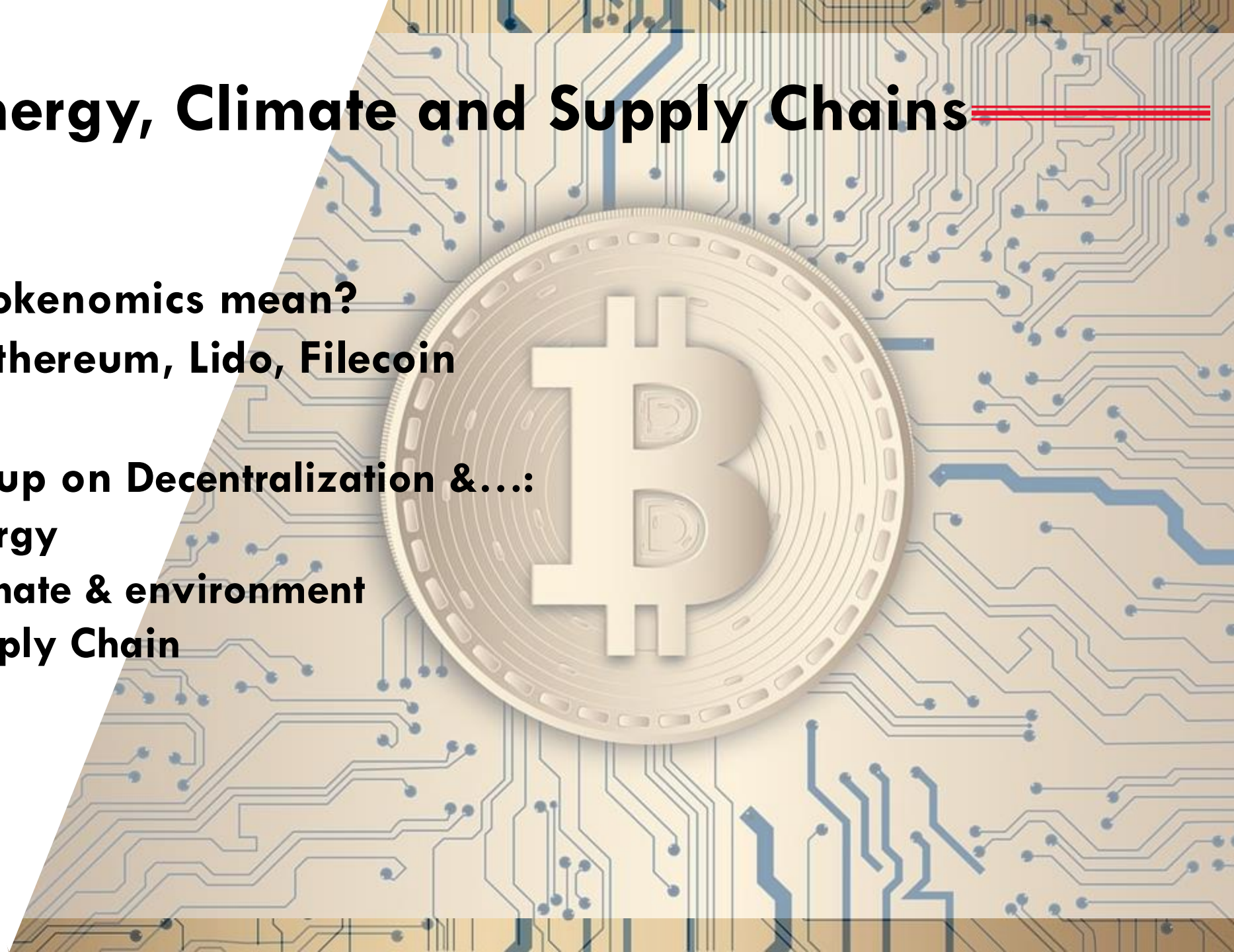
Session 4: Energy, Climate and Supply Chains

What does tokenomics mean?

→ Bitcoin, Ethereum, Lido, Filecoin

Working group on Decentralization &…:

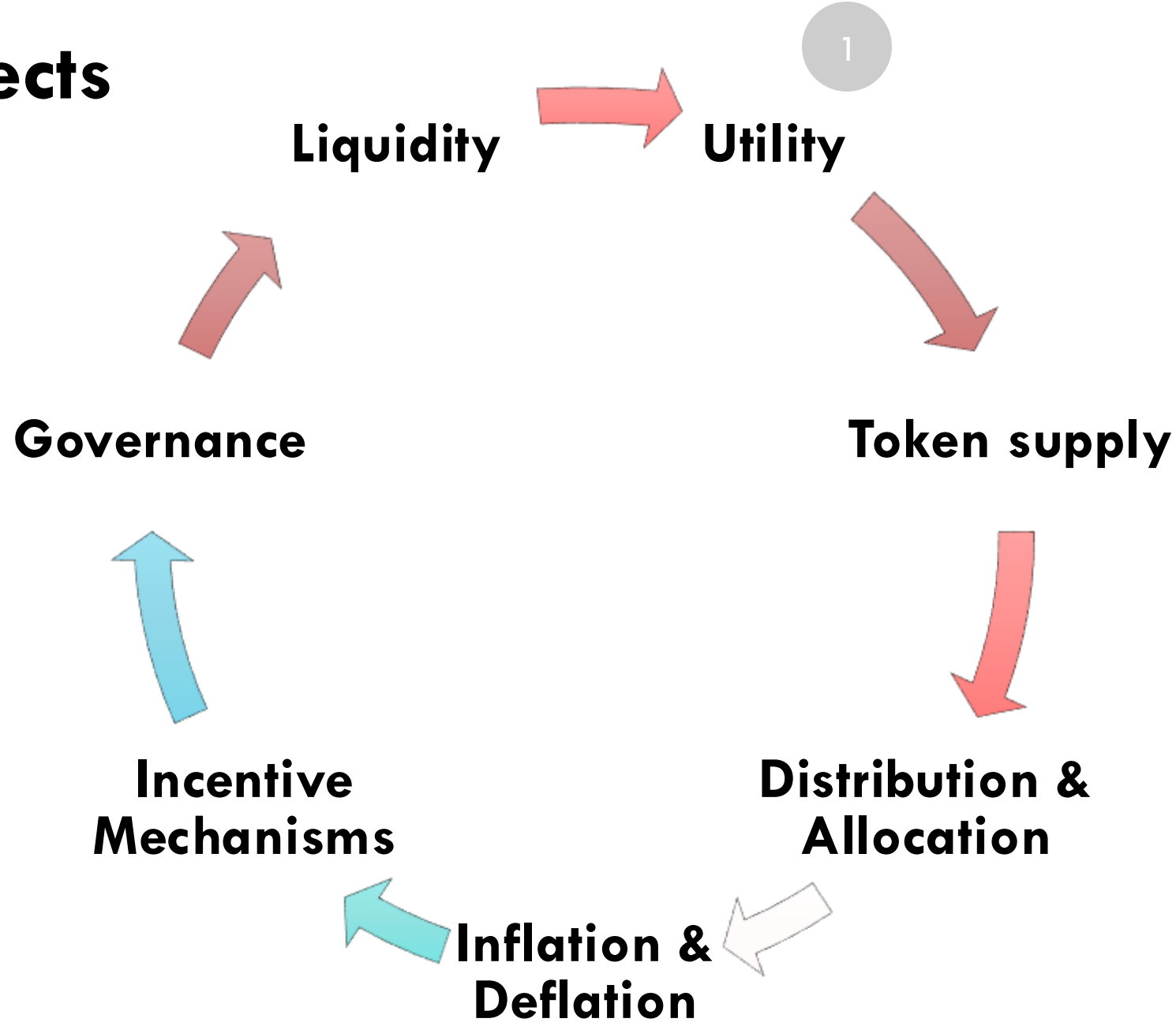
A. **…Energy**
B. **…Climate & environment**
C. **…Supply Chain**



Tokenomics?

“Token” + “Economics” = Tokenomics

7 key aspects



Comparison of 4 Tokens

1. Utility

- What is the token used for? (e.g., payments, governance, staking, access to services)
- Does the token provide any special rights or benefits?
- Is the token essential for the ecosystem, or is it optional?

Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
What is the token used for?	Digital store of value, payments	Smart contracts, gas fees, staking	Governance for Lido protocol	Paying for decentralized storage
Special rights/benefits?	Highly secure, widely accepted	Enables dApps, DeFi, NFTs	Voting on protocol decisions	Provides access to decentralized storage
Essential for the ecosystem?	Yes, Bitcoin network runs on BTC	Yes, ETH is needed for transactions & staking	Optional, only needed for governance	Yes, FIL is required for storage transactions

2. Token Supply

- What is the total supply of the token?
- How many tokens are currently in circulation?
- Is there a burn mechanism? If so, how does it work?

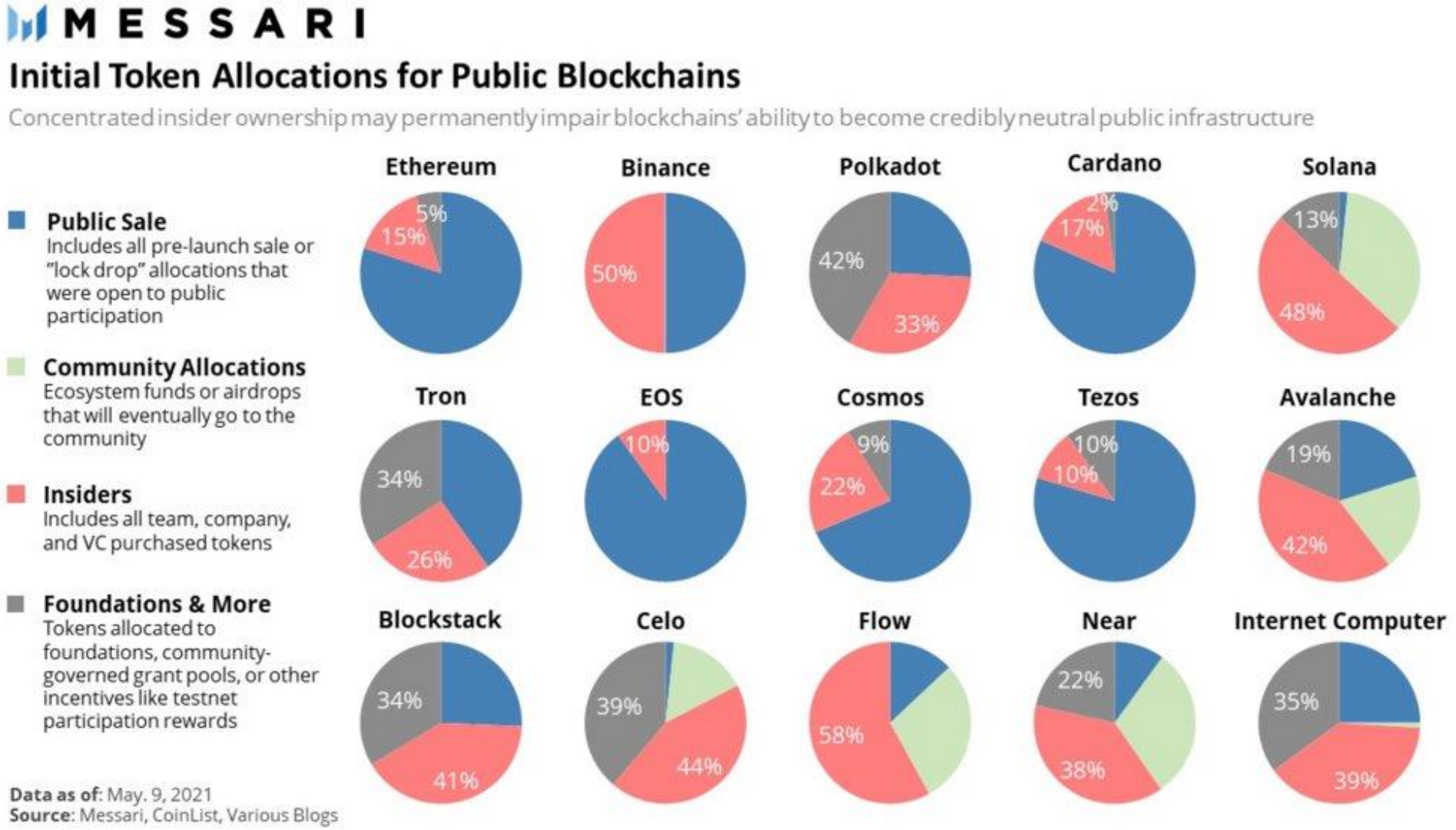
Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
Total Supply	21 million BTC (fixed)	No fixed cap (inflationary)	1 billion LDO	2 billion FIL (max supply)
Circulating Supply	~19.7 million BTC	~120 million ETH	~890 million LDO	~600 million FIL
Burn Mechanisms	No burning mechanism	**EIP-1559** burns ETH in transactions	No burn mechanism	No burn mechanism

3. Distribution & Allocation

- How were the tokens initially distributed? (e.g., ICO, fair launch, pre-mined)
- What percentage of tokens is allocated to the team, investors, and the community?
- Are there any lock-up periods or vesting schedules?

Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
Initial Distribution?	Mined from genesis block	Pre-mined + ICO (2014)	Initial allocation to team, investors, community	ICO in 2017
Team, investors, community allocations?	No pre-mine, fully mined	Initial pre-mine to founders	36.3% to early investors, 6.5% to validators	~30% to investors & foundation
Lock-up/Vesting?	No lock-ups	Some ETH held in staking contracts	No vesting for most tokens	6-year vesting for some early investors

Initial Token Allocation. What's wrong?



4. Inflation & Deflation

- Does the token have a fixed supply, or are new tokens issued over time?
- How is inflation or deflation controlled? (e.g., staking rewards, token burns)
- What impact does the supply mechanism have on price stability?

Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
Fixed or new tokens issued?	Fixed, decreasing emissions (halving every 4 years)	New ETH issued for staking but offset by burns	No new issuance	Mining-based emission with declining rewards
Inflation/deflation control?	Halving reduces supply growth	EIP-1559 burns ETH, reducing inflation	No deflation mechanisms	Gradual reduction in new FIL issuance
Impact on price stability?	Supply shock every halving	Inflationary but burn reduces pressure	Price fluctuates based on governance demand	Supply inflation may affect price

5. Incentive Mechanisms

- How does the project encourage users to hold or use the token?
- Are there rewards for staking or participating in governance?
- Are there mechanisms to prevent hoarding or manipulation?

Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
How does it encourage holding?	Scarcity & long-term store of value	Staking rewards for validators	Governance participation	Rewards for storage providers
Staking or participation rewards?	No staking	Staking ETH for rewards	LDO stakers influence protocol governance	FIL miners earn storage rewards
Anti-manipulation mechanisms?	Mining difficulty adjusts to secure network	Slashing penalties for bad validators	Governance voting prevents centralization	Storage providers must provide collateral

6. Governance

- Can token holders vote on decisions related to the project?
- What type of governance model does the project use? (e.g., DAO, centralized)
- How decentralized is the decision-making process?

Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
Can token holders vote?	No governance token	No direct token governance	Yes, LDO holders vote on proposals	No direct governance, but community influences upgrades
Governance model?	Developer & miner-driven	Ethereum Improvement Proposals (EIPs)	DAO-based	Community-driven proposals
Decentralization?	Highly decentralized	Moderately decentralized, core developers lead	DAO structure but some concerns about centralization	Network is decentralized but Filecoin Foundation has influence

7. Liquidity & Market Dynamics

- On which exchanges can the token be traded?
- How liquid is the token? (Are there enough buyers and sellers?)
- Do lock-up periods or vesting schedules affect market availability?

Question	Bitcoin (BTC)	Ethereum (ETH)	Lido (LDO)	Filecoin (FIL)
Where can it be traded?	All major exchanges	All major exchanges	Most major exchanges	Many major exchanges but lower volume than BTC/ETH
How liquid is it?	Most liquid crypto asset	Highly liquid	Less liquid than ETH, BTC	Moderate liquidity
Market impact of lock-ups?	No lock-ups	Staked ETH is locked but gradually unlocked	No major lock-ups	Vesting schedules impact FIL's market availability

Prompt for an IA tool

Make the tokenomics of « chainlink » with this framework:

1. Utility

- What is the token used for?
- Does the token provide any special rights or benefits?
- Is the token essential for the ecosystem, or is it optional?

2. Token Supply

- What is the total supply of the token?
- How many tokens are currently in circulation?
- Is there a burn mechanism? If so, how does it work?

3. Distribution & Allocation

- How were the tokens initially distributed?
- What percentage of tokens is allocated to the team, investors, and the community?
- Are there any lock-up periods or vesting schedules?

4. Inflation & Deflation

- Does the token have a fixed supply, or are new tokens issued over time?
- How is inflation or deflation controlled?
- What impact does the supply mechanism have on price stability?

5. Incentive Mechanisms

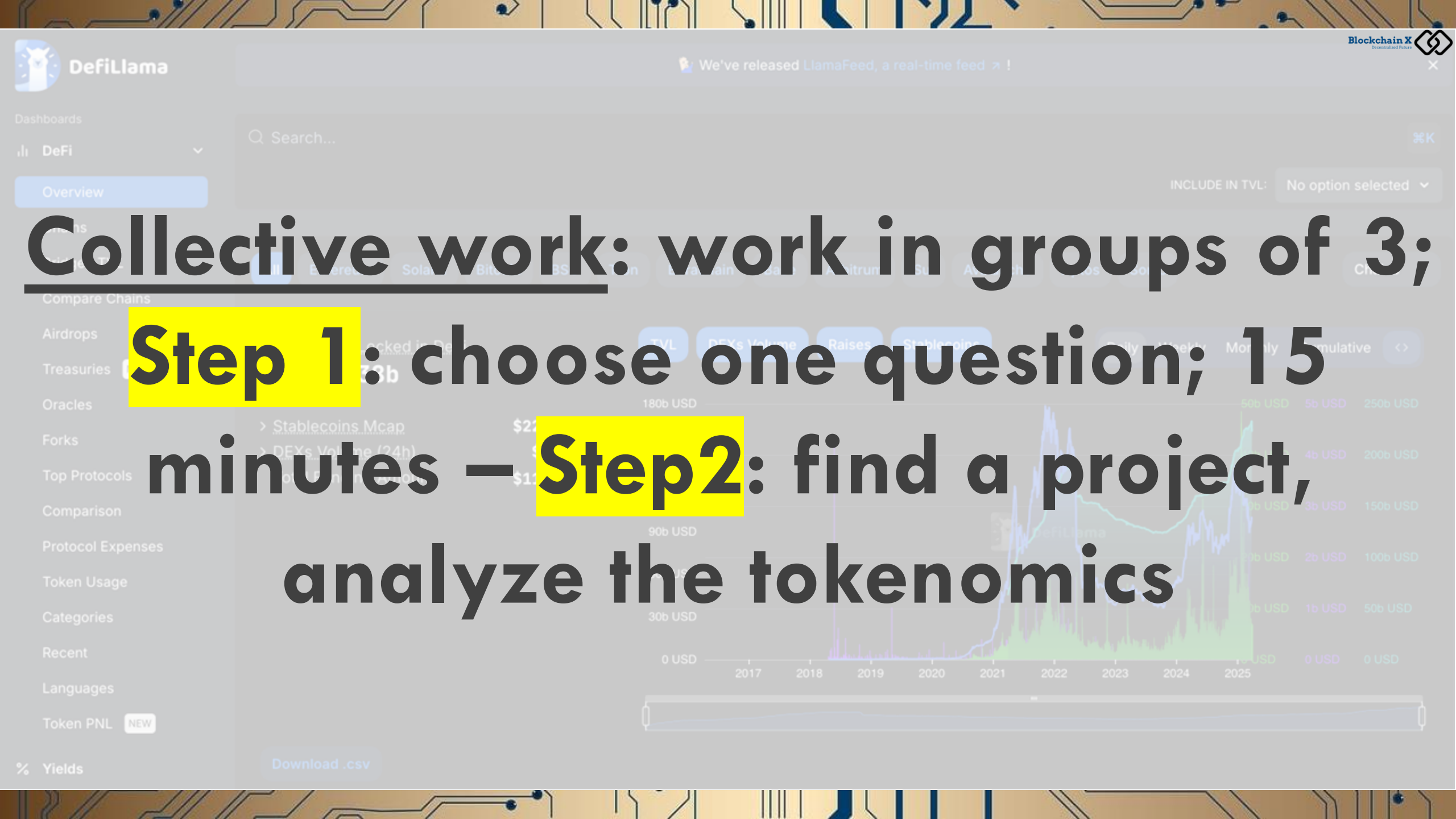
- How does the project encourage users to hold or use the token?
- Are there rewards for staking or participating in governance?
- Are there mechanisms to prevent hoarding or manipulation?

6. Governance

- Can token holders vote on decisions related to the project?
- What type of governance model does the project use?
- How decentralized is the decision-making process?

7. Liquidity & Market Dynamics

- On which exchanges can the token be traded?
- How liquid is the token?
- Do lock-up periods or vesting schedules affect market availability?



Collective work: work in groups of 3; Step 1: choose one question; 15 minutes — Step2: find a project, analyze the tokenomics

Collective work in group of 3 – STEP 1

1. **Energy**
    1. How can blockchain ensure the traceability and certification of green energy?
    2. What is a peer-to-peer (P2P) energy market and how does it work on a blockchain?
    3. How can blockchain optimize the operation of smart grids?
    4. How can tokenization and decentralized finance support the energy transition?

2. **Climate & Environment**
    1. What are tokenized carbon credits and how do they work?
    2. How can tokenization and decentralized finance support the energy transition?

3. **Supply Chain**
    1. Can blockchain be used to tokenize and track an entire supply chain?
    2. How can blockchain-based reward systems incentivize plastic waste collection?

Collective work in group of 3 – STEP 2

1. **Energy**
   1. Certification of green energy
   2. P2P energy market
   3. Optimizing smart grids
   4. DeFi for the energy transition

Powerledger

energy web

DOW

SUNCONTRACT

2. **Climate & Environment**
   1. Tokenized carbon credits
   2. DeFi for Climate

Toucan

Glow

OPEN FOREST PROTOCOL

Carbonable

3. **Supply Chain**
   1. Tokenization of supply chain
   2. A blockchain-based reward systems for waste collection

.arianee

Ambrosus

Plastiks