

Lecture 5

—

ERC20 - Fungible Tokens

Fungibility

What are Fungible Tokens?

Fungible

Exists an exact identical unit

1 Euro coin is not unique, many other 1 Euro coins

We care about **how much**.

Non-Fungible

No other unit is the same

A house is different from its neighbour

We care about **what feature**.

Notable Token ERCs

ERC20

Standard fungible token
Extremely widespread
Simple functionality

ERC777

ERC20 improvement
Backwards compatible
Some efficiency improvement in transactions
Supply control and authorization functionalities

ERC721

Standard non-fungible token
(NFT)
Extremely widespread
Most gaming, music, art
solutions built with this standard

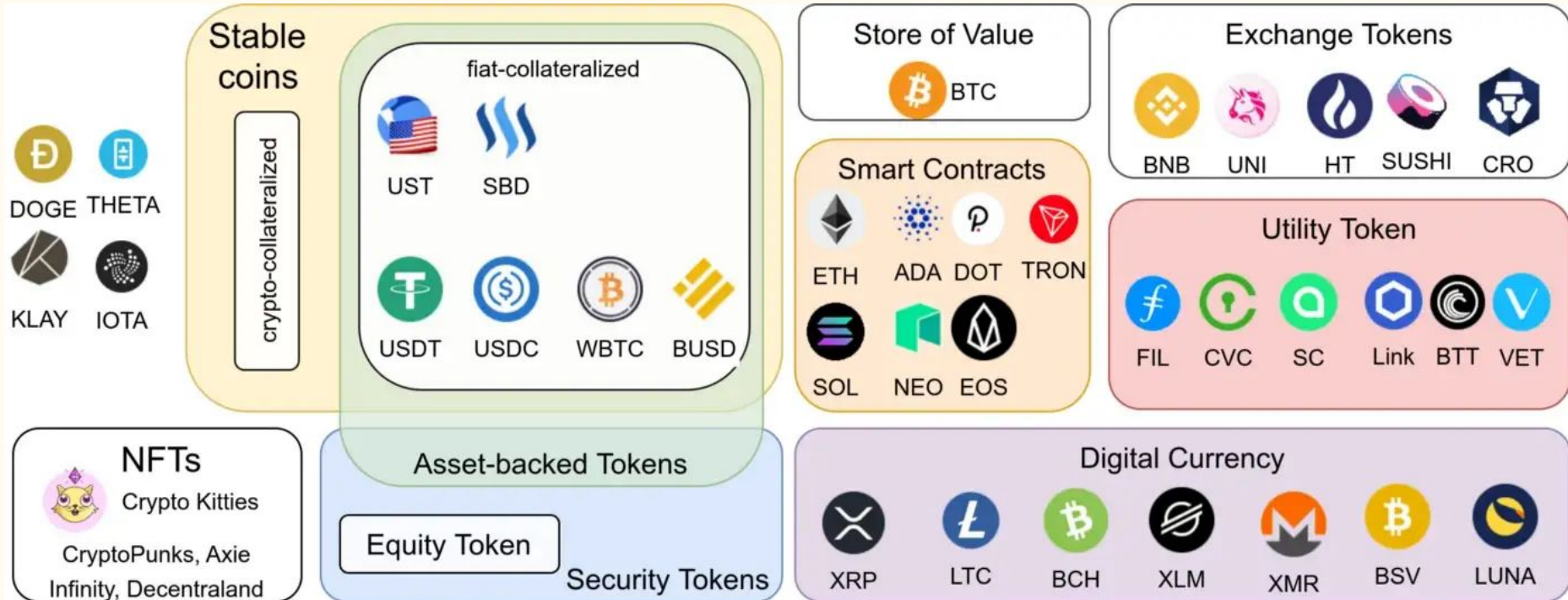
ERC1155

Mult Token Standard
Non fungible, semi-fungible,
fungible
Gas and storage efficiency
More exchange capabilities

Tokenomics

Supply, Demand, Valuation

Tokens - A representation of Value



Token Supply - Definitions

Max Supply - The total number of coins that can ever exist

- Bitcoin has a Max supply of 21 Million.
- Solana, Dogecoin has unlimited supply!

Issuance Rate / Supply schedule - rate at which coins are minted

- 90% of bitcoin has been mined. Last coin in 120 years
- Affects inflation / deflation of coin

Circulating Supply - Amount currently on the market

- Affected by issuance and burning

Total Supply - circulating supply plus locked/staked/reserved tokens

- Gap too big - possible market shock if there is supply flood

Token Supply - Control Mechanics

Reserve / Lockup - Company holds coins to prevent it circulation. Worrisome for users if too large, suspect of market manipulation.

Buyback / Burn - Company buys back tokens and destroys them to reduce supply, control inflation, boost prices.

Vesting and penalties - Amount locked for a certain amount of time, pay a penalty if liquidated early. Drives stability.

Staking - locking up funds for services. To receive rewards from nodes or earn yield from lending. Improves stability and ensures continued activity.

Token Demand Generation

Community / User base - How big is the community and how engaged they are.

- Attention Economy - Elon bought Dogecoin
- Artificial Users - trading bots

Technological Niche - project solves a technical need of the community.

- Data interactions from on and off chain.
- Consensus Mechanisms
- Trading Mechanisms

Conversion - blue ocean strategy, partnerships with existing large web2 companies.
Developing traditional use cases.

- Celo phone number to wallet mapping / DT SMS API

Valuation - Market Capitalization

$$\text{Market Cap} = \text{Circulating Supply} \times \text{Coin Price}$$

Market Capitalization - Example

There are currently 1000 Dauphine Coins in circulation. The current price is \$5 per coin.

Question 1: What is the current Market Capitalization?

Question 2: Dauphine decides to mint 1000 more coins and puts 500 in a reserve. After the mint, new coin price is \$3. What is the new Market Capitalization?

Question 3: A user locks 50 Dauphine Coins for rewards and Dauphine decides to burn 100 coins. Now, price goes up to \$4. What is the new Market Capitalization?

Valuation - Other Metrics

Total Addressable Market - What is the maximum amount of users that your protocol can capture?

Utility Token Model - How is the native platform token being used? What need does it address?

Core Team - Crypto is very new, what expertise does the core team have? Tech/Finance/Legal mix.

Community and Partnerships - Both users and enterprise service providers

Other Traditional Financial Metrics - Mostly used by VCs and applicable to exchanges and financial services. P/E ratio, Discounted Cash Flow, etc.

ERC20

The ERC20 Standard

<https://eips.ethereum.org/EIPS/eip-20>

function name() **public** view returns (string)

function symbol() **public** view returns (string)

function decimals() **public** view returns (uint8)

function totalSupply() **public** view returns (uint256)

function balanceOf(address _owner) **public** view returns (uint256 balance)

function transfer(address _to, uint256 _value) **public** returns (bool success)

function transferFrom(address _from, address _to, uint256 _value) **public** returns (bool success)

function approve(address _spender, uint256 _value) **public** returns (bool success)

function allowance(address _owner, address _spender) **public** view returns (uint256 remaining)

event Transfer(address indexed _from, address indexed _to, uint256 _value)

event Approval(address indexed _owner, address indexed _spender, uint256 _value)

ERC20 Implementation

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/ERC20.sol>

The 5 minute challenge



Simple Token in 5 Minutes

<http://thetokenfactory.com/#/factory>



Products ▾

For Business

Resources ▾



How to Create Your Own ERC-20 Token in 10 Minutes

Create ERC-20 Token

Create Ethereum Token

Create Your Own ERC-20 Token

ERC-20 token

Stablecoins

Stability Mechanisms

Stablecoins

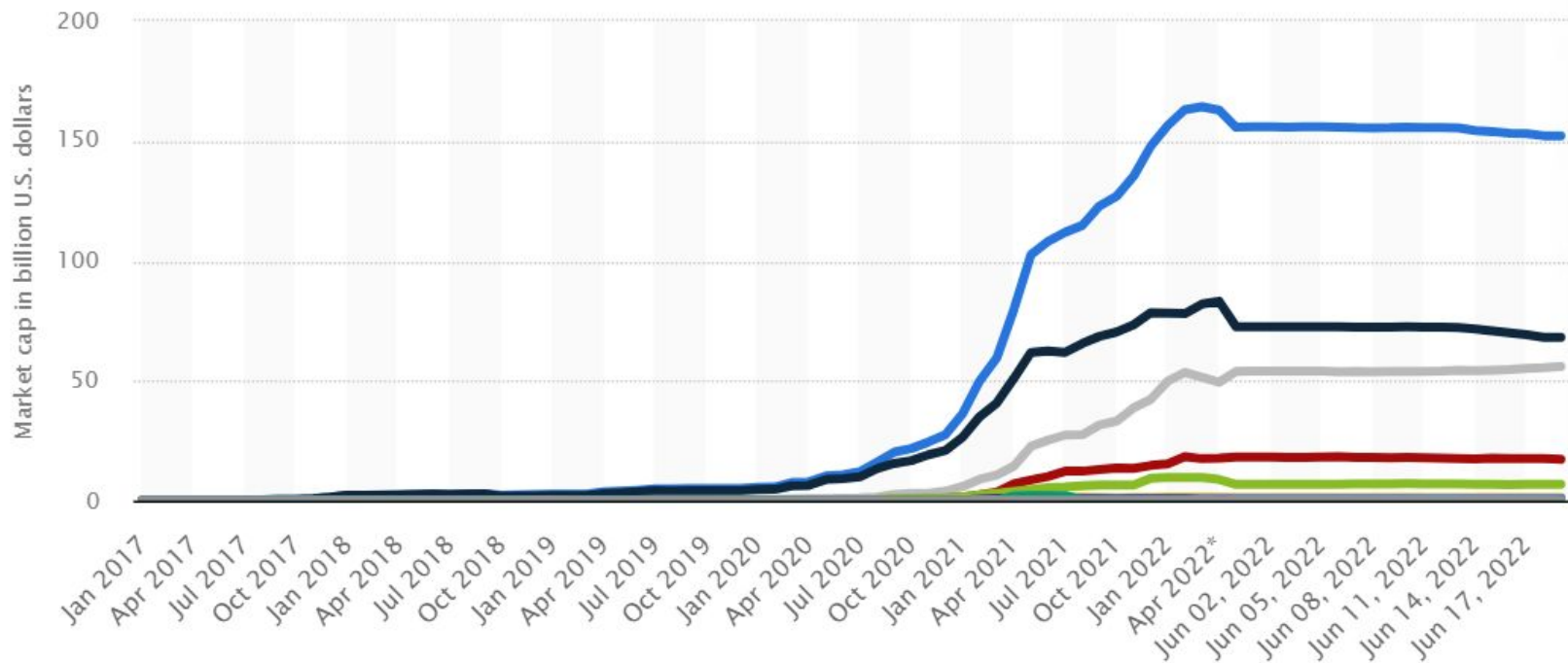
Have a relatively stable value because they are pegged to a target currency.

This target is usually the USD.

Volatility is good for short term strategies but stables balance out for long term investment strategies.

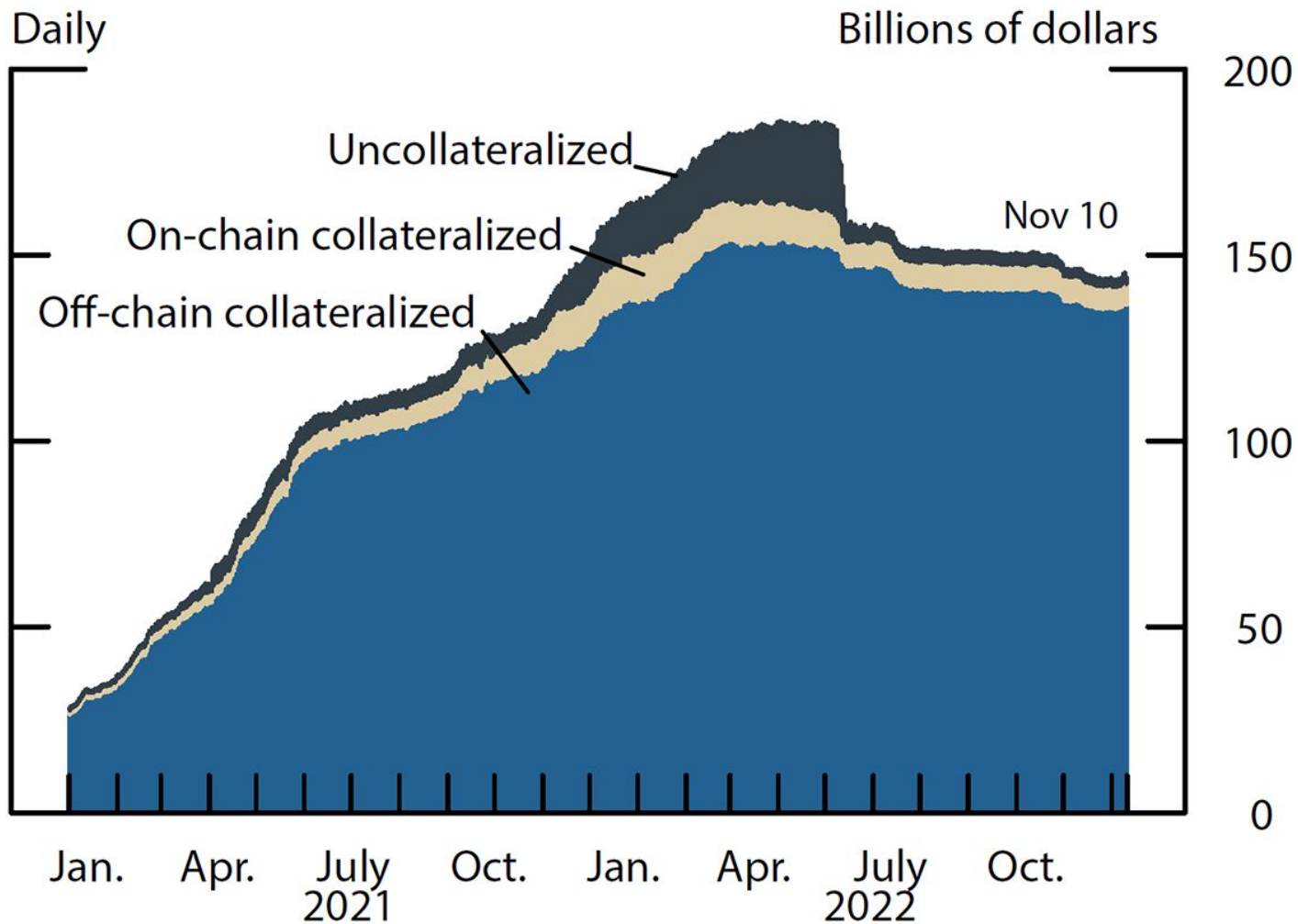
Managing liquidity.

Serve as a medium of exchange between volatile currencies.



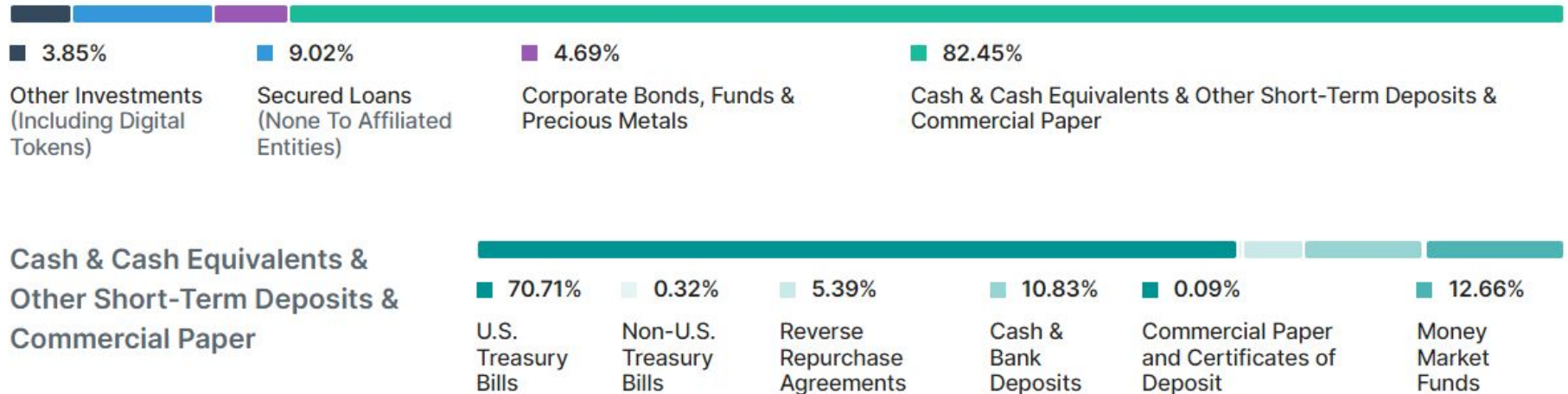
Stability Mechanisms

On chain	Off chain
Backed by other cryptocurrencies. Beware the circular dependencies.	Backed by traditional financial assets. Fiat currencies, bonds, stocks, fixed assets, etc.
Algorithmic	Mix
Also known as Uncollateralized. Using economic algorithms to controlling circulation and reserve.	Usually a mix of assets and strategies.



Off Chain Collateralized Stable - Tether

Reserves Breakdown



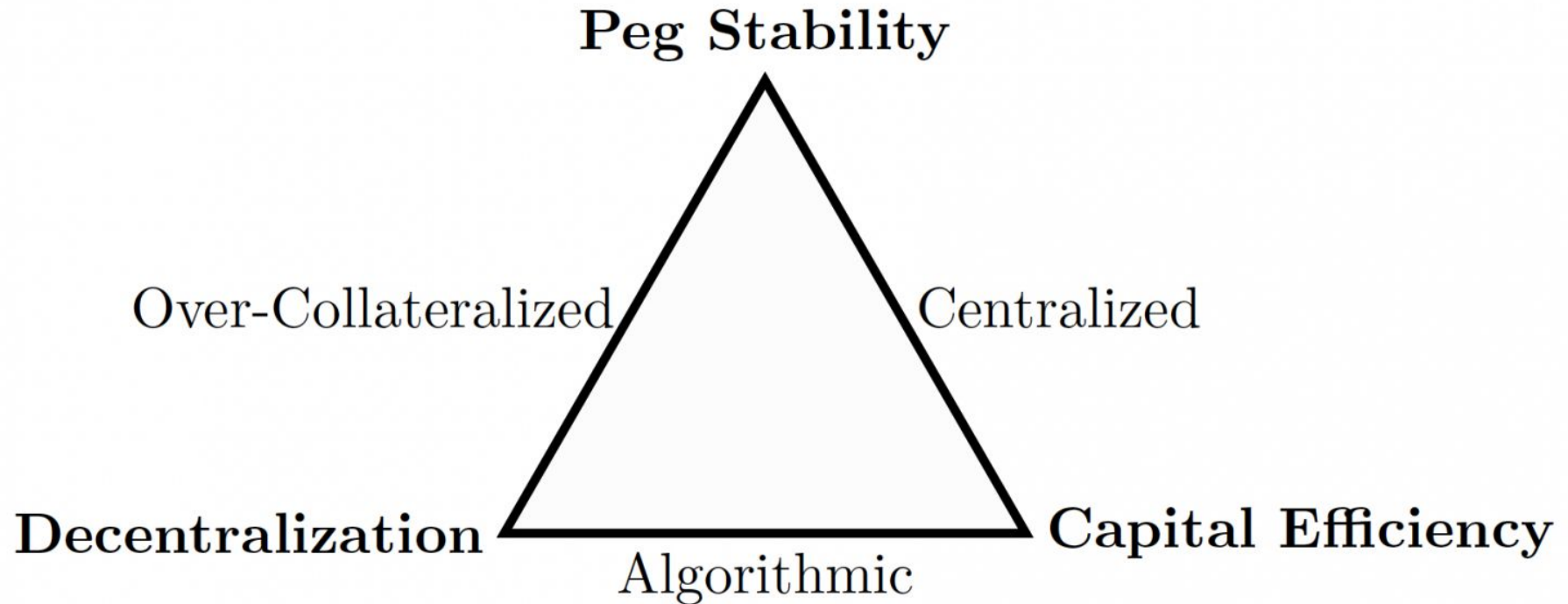
Source: <https://tether.to/en/transparency/#reports>

On Chain Collateralized Stable - DAI

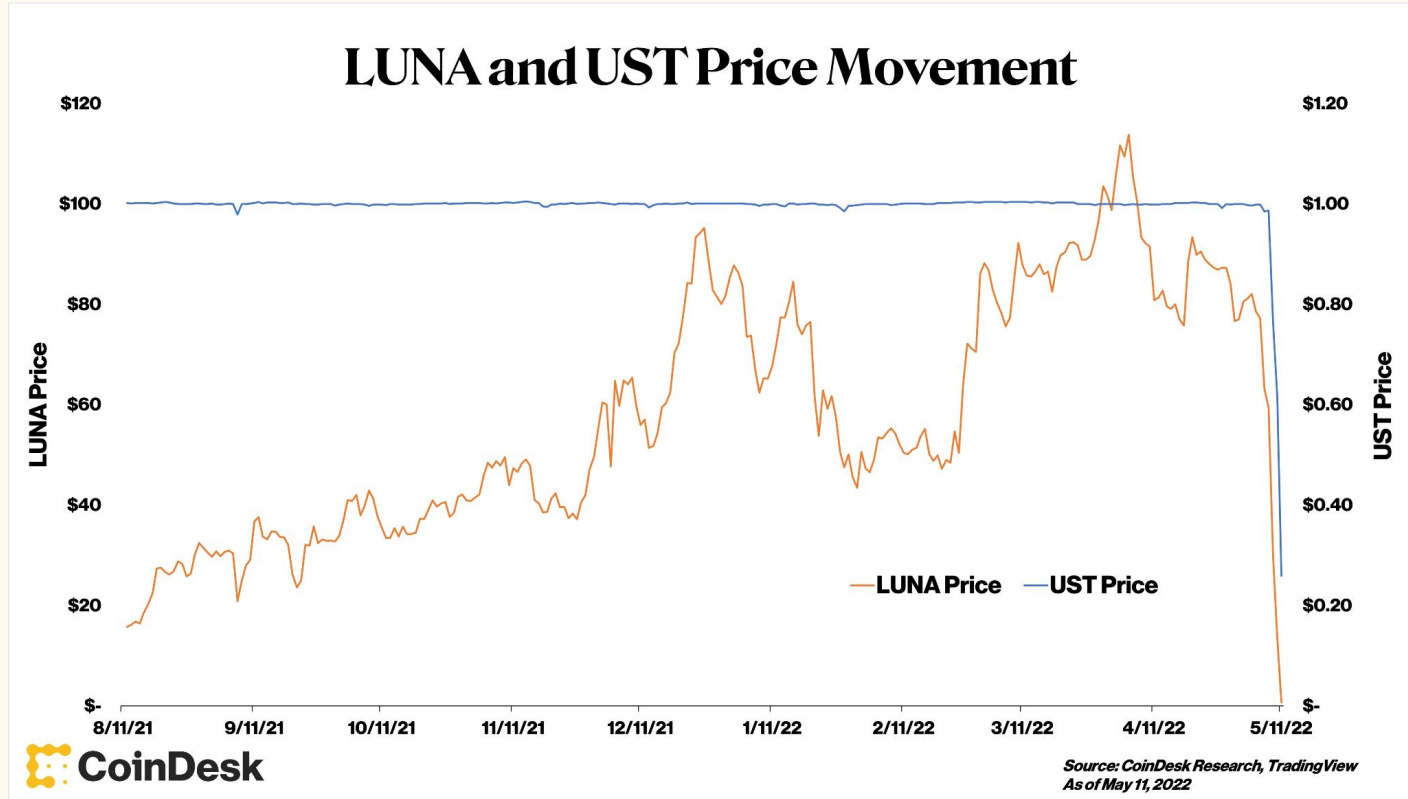
The infamous "borrow money into existence" strategy

1. User wants 100 DAI coins (Let's say DAI price is at \$1,05)
2. Minimum DAI collateralization ratio stands at **150%**
3. User needs to lock $\$1,05 \times 100 \times 1.5 = \$157,50$ of ETH
4. User locks the ETH and MakerDAO mints 100 DAI into existence
5. User returns 100 DAI at a later point, the locked value is return (or liquidated)
6. 100 DAI is burned out of existence

The Stablecoin Trilemma



Terra / Luna crash



Central Bank Digital Currencies

Landscape and Considerations

Central Bank Digital Currencies - Governments react

The concept of DeFi aims to solve a lot of limitations of traditional finance. For example, a huge portion of the world is unbanked. Cross border payments not keeping up with immigration trends.

Huge players like Facebook (Libra) and JP Morgan (JPMCoin) wanted to centralize and manage financial systems.

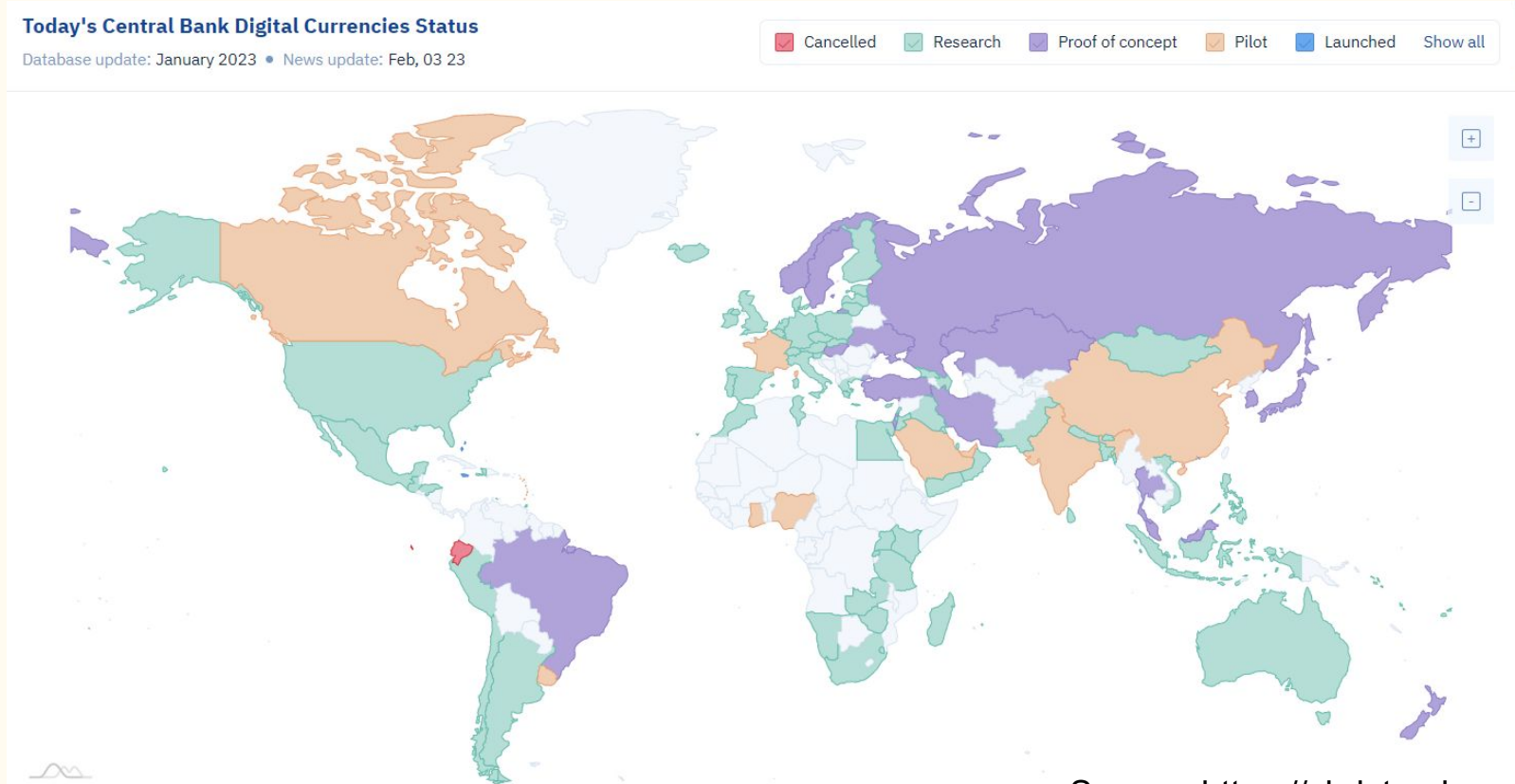
Central Bank wanted to maintain monetary (both local and foreign) policy.



Bruno Le Maire 
@BrunoLeMaire

In the current conditions, we should refuse the development of [#Libra](#) in Europe while working on improving the efficiency of our common payment system. We should also work on the creation of a digital public currency [#Eurofi2019](#)

CBDC - Current Landscape



Source: <https://cbdctracker.org/>

Two types of currencies

Wholesale

Only available to banks. Both commercial and intermediary. Used for reserves, remittances, Interbank settlements.

Retail

Available to businesses and consumers. Could be used as legal tender of a country or other forms of financial instruments like loans, bonds, stocks, etc.

Designing CBDCs - 3 pillars

Methodology



Infrastructure



Governance

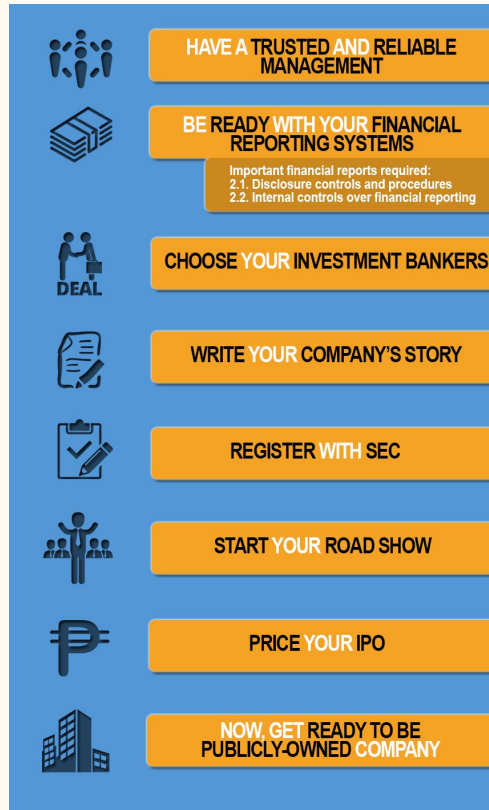


Blockchain Fundraising

ICO, STO, IEO, IDO

Fundraising - Traditional

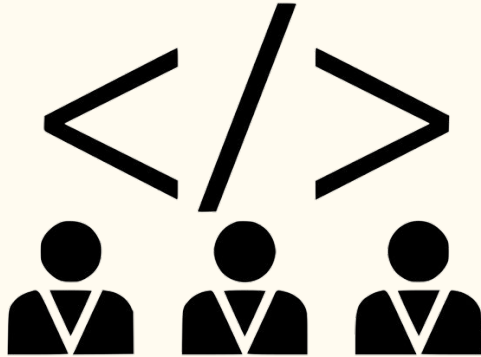
IPO



Crowdfunding



ICO - Initial Coin Offering



1. Offering discounted tokens, utility tokens or STOs
2. Raise capital without VCs. Fast and flexible.
3. High decentralization, low regulation
 - Site not functioning correctly and transactions fail
 - Marketing done by development team
 - Plagued by scams - development team vanishes
4. Users
 - Healthy competition
 - Believers and community
 - Liquidity and developers



xxx.wordpress.com

Utility Tokens

A token which provides access to specific product or service on a blockchain

- Receives special/limited edition NFTs
- Payment for specific services
 - Filecoin - storage
 - Chainlink - data
- Ecosystem Perks
 - BNB holders enjoy 25% reduced fees
 - Web2 equivalent - Vente Privee

LINK - Utility token deep dive

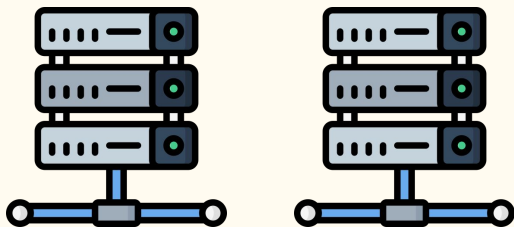


Smart Contract pay Oracles LINK for this information retrieval and verification.

A Service Level Agreement is created:

1. Oracle reputation
2. Order Matching - Nodes must bid to fulfill this data request.
LINK used
3. Aggregating contract - collects all bids and computes final results from all oracles

Penalties can be charged in LINK for fake / low quality data



Nodes are integration point with blockchain and traditional data sources

Use LINK tokens to vote which nodes can supply information to the Oracle - data reliability and verification.

Receive LINK as a reward for data delivered to an Oracle

STO - Security Token Offering

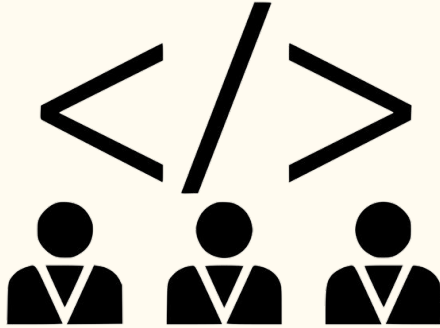
US Securities Act:

A contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party.

STO - Some Examples

- Bitcoin
 - No, Bitcoin has no registered entity that is for profit
- NFT that records ownership of a car
 - No, this is ownership, not profit generation
- DauphineSwap token which promises returns through trading by the university
 - Semi. Dauphine promises returns and the profits were made by the the university. Legally a security token from TradFi POV.
 - Token has no promise of ownership/equity - more like a utility token. Different legal understandings of STOs here (equity / debt).

IEO - Initial Exchange Offering



1. Similar token offering to ICO
2. Must partner with an exchange! (Binance, FTX)
3. Exchange does the due diligence checks
 - User trust - Exchange reputation
 - Marketing done by exchange
 - Less scams (2% acceptance Binance launchpad)
4. Users
 - Tap into exchange user base
 - Liquidity secure - market making mechanisms

IDO - Initial DEX Offering

CEX	DEX
  	   
Listing fees Other fees: trade volume, Market Making	No listing fees Other fees: lower but unstable
Opaque vetting process	Community voted
Large or global user base	Small or local user base

Type of Token Sale	Initial Coin Offering (ICO)	Initial Exchange Offering (IEO)	Initial DEX Offering (IDO)
Where Sale Takes Place	Token Issuer's Website	Exchange Platform	DEX (Decentralized Exchange) Launchpad
Centralized vs Decentralized	Centralized	Centralized	Decentralized
KYC Required	Yes	Usually	Sometimes
Due Diligence	By Participant	By Exchange & Participant	By DEX LaunchPad & Participant
Popularity	Highest in 2017	Highest in 2018-19	Highest in 2020-21