I Cryptoasset e il loro mondo

Oggetti, tecnologie, pratiche

PISA - 3 marzo 2023

Cosa vedremo

Sommario

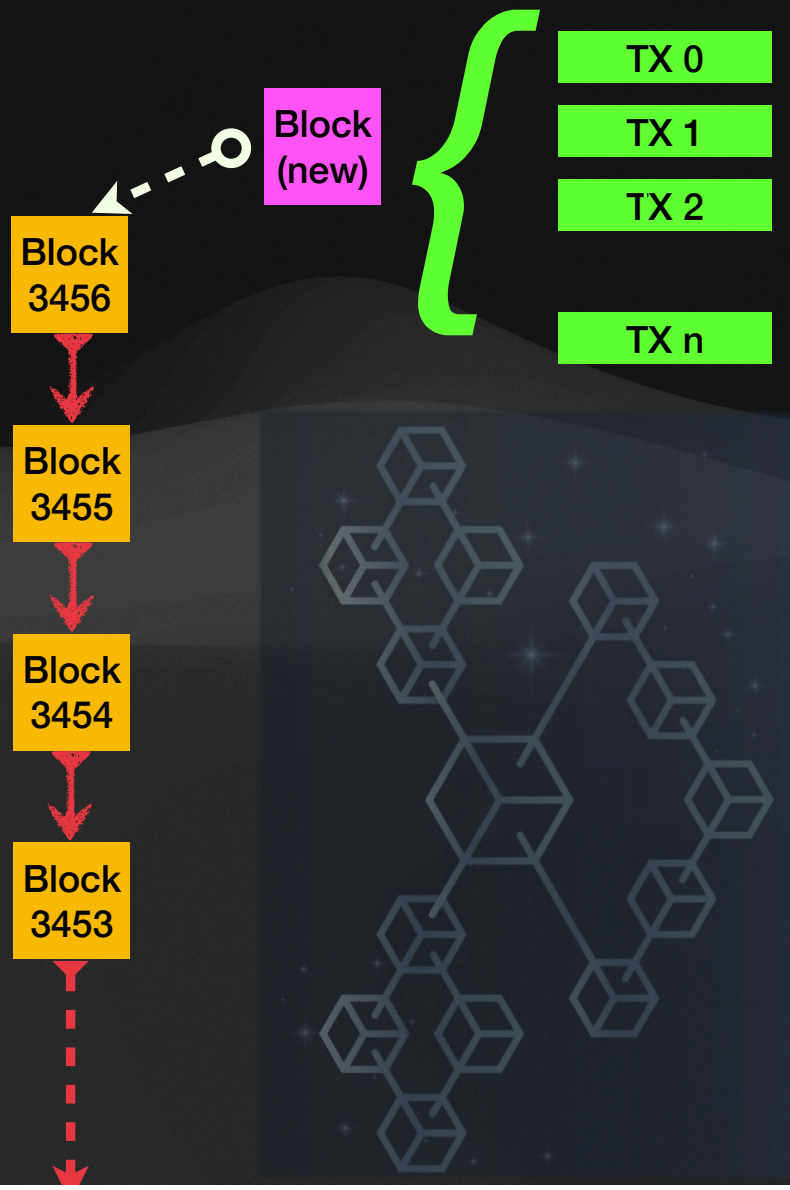
- Caratteristiche dei cryptoasset
- Cosa è una blockchain, PoW e PoS
- Wallet e custodia
- Coin, Token: tipologie e caratteristiche
- Cenni di operatività in CeFi e DeFi

Le “Crypto”

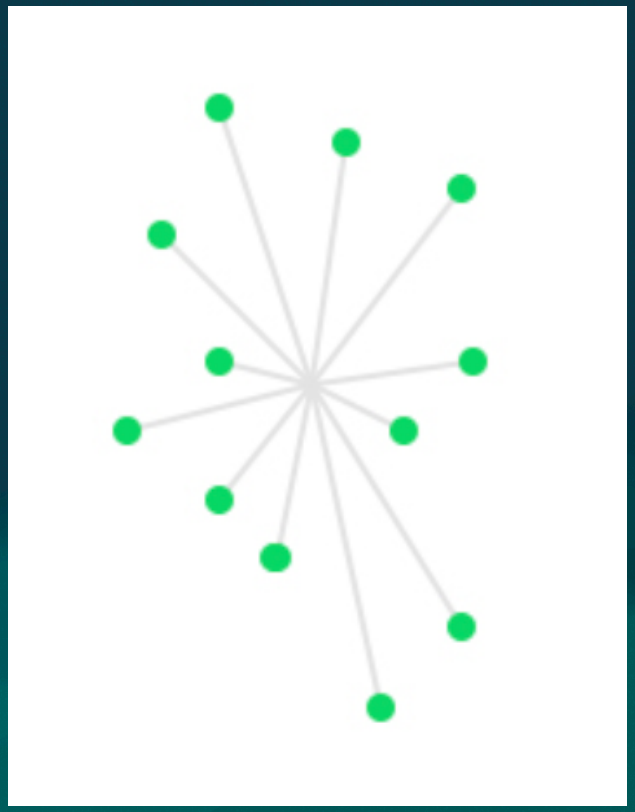
- Rappresentazioni nativamente digitali
- “Emesse” su una blockchain
- Passaggio di proprietà tramite transazioni firmate digitalmente
- Largo utlizzo di crittografia
- Programmabili

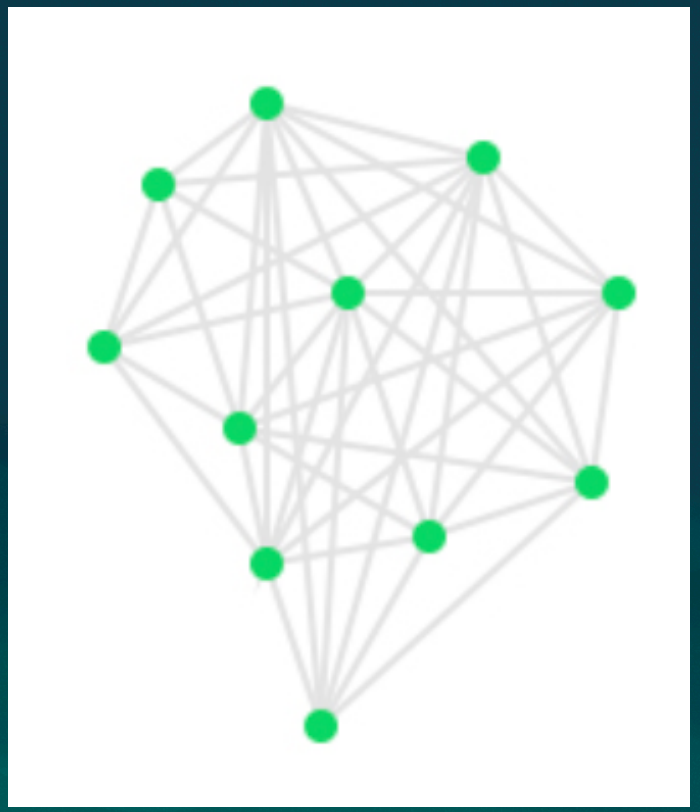
La Blockchain

- È un DLT (Distribuited Ledger Technology)
- Le informazioni (TX) sono validate e inserite in blocchi
- ogni blocco contiene una “marca temporale” ed è concatenato a quello precedente (blocco padre) tramite HASH criptografico
- L’intera blockchain è memorizzata interamente su molti nodi (full node) connessi tra loro (P2P)
- La validazione delle singole transazioni e dell’intero blocco avviene tramite un algoritmo di consenso distribuito
- Può essere privata o pubblica (permissionless)



Centralizzato vs Decentralizzato





Un nodo

Diversi tipi

- Mining
- Validazione
- Full Node
- LightNode
- altri…

Consenso

PoW - Mining

- Basato sulla potenza di calcolo
- Alti consumi energetici
- Massima sicurezza
- Accesso virtualmente possibile a tutti

PoS - Staking

- Basato sul possesso di capitali
- Bassi consumi energetici
- Sicurezza minore perchè dipende dalla decentralizzazione dei “fondi”
- Accesso possibile a chi detiene la coin della blockchain

PoW


Bitcoin mining infrastructure developed as of April

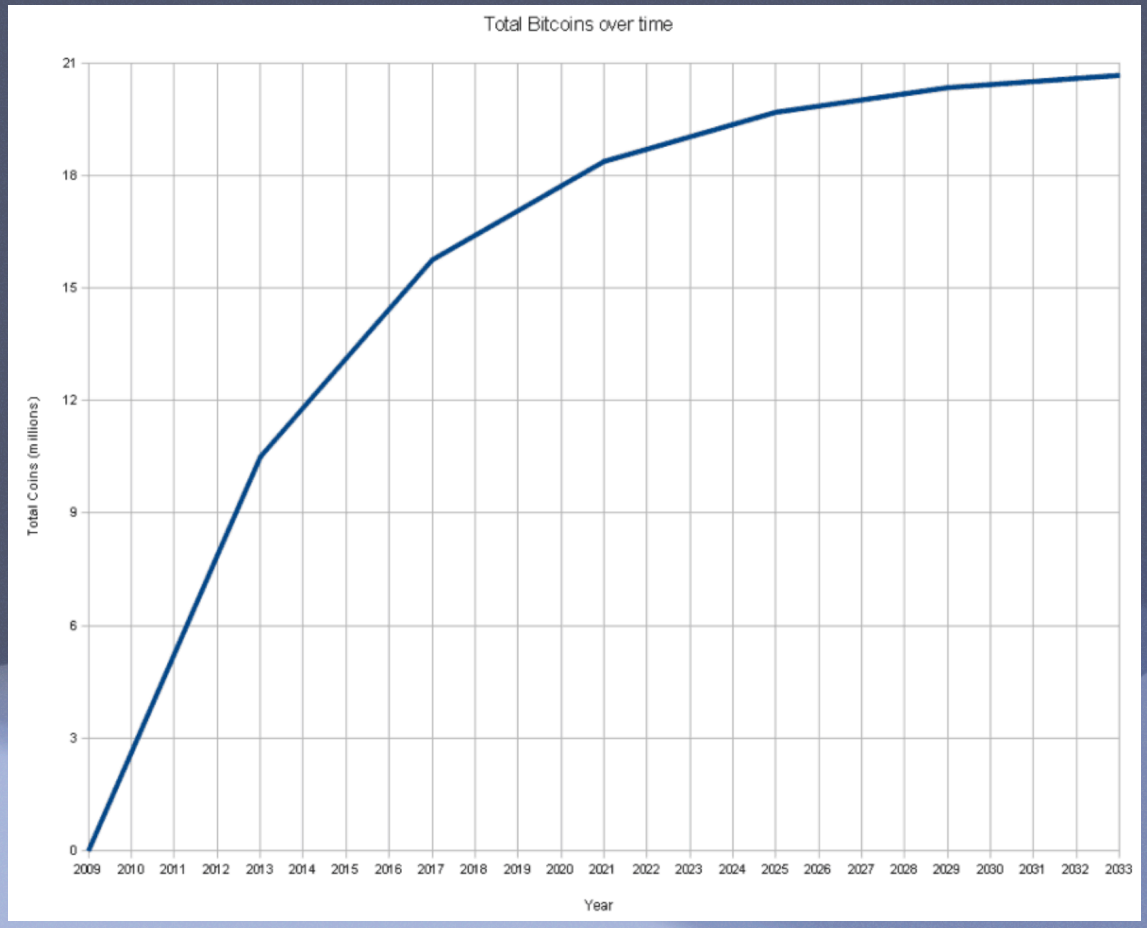

Company
Riot Blockchain, Inc.
Data Center Location
Rockdale, Texas
Energy Source
Mixed-grid generational resources
from Texas' ERCOT grid

Bitcoin - bitcoin

- Satoshi Nakamoto
- Idee di fondo
  - Moneta slegata dal controllo centralizzato (governi)
  - Non intermediata (no banche)
  - Universalmente operabile
- Miti da sfatare
  - Controllo della rete non chiaro
  - Consumi Energetici
  - Illegalità non è il default
  - anonimato in parte, si privacy

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Bitcoin - bitcoin



Emissione totale prevista:
21.000.000

Attualmente è stata generata più del 90% della supply (19.3 Mil)

Halving (circa ogni 4 anni)

Complessità (circa ogni 2 settimane)

Blocco (circa ogni 10 minuti)

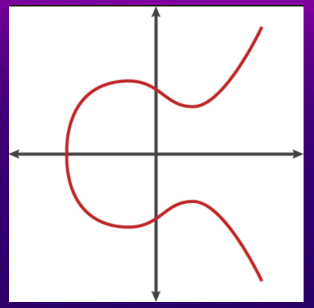
Wallet

- **NON CONTIENE I FONDI**
- **Garantisce l'accesso ai fondi**
- Genera e conserva la chiave privata (con vari livelli di sicurezza)
- Mostra il saldo dei fondi recuperandolo dai nodi
- Genera gli Address di ricezione
- Prepara e firma le transazioni e provvede ad inviarle ai nodi
- "Nasconde" la complessità di ECDSA

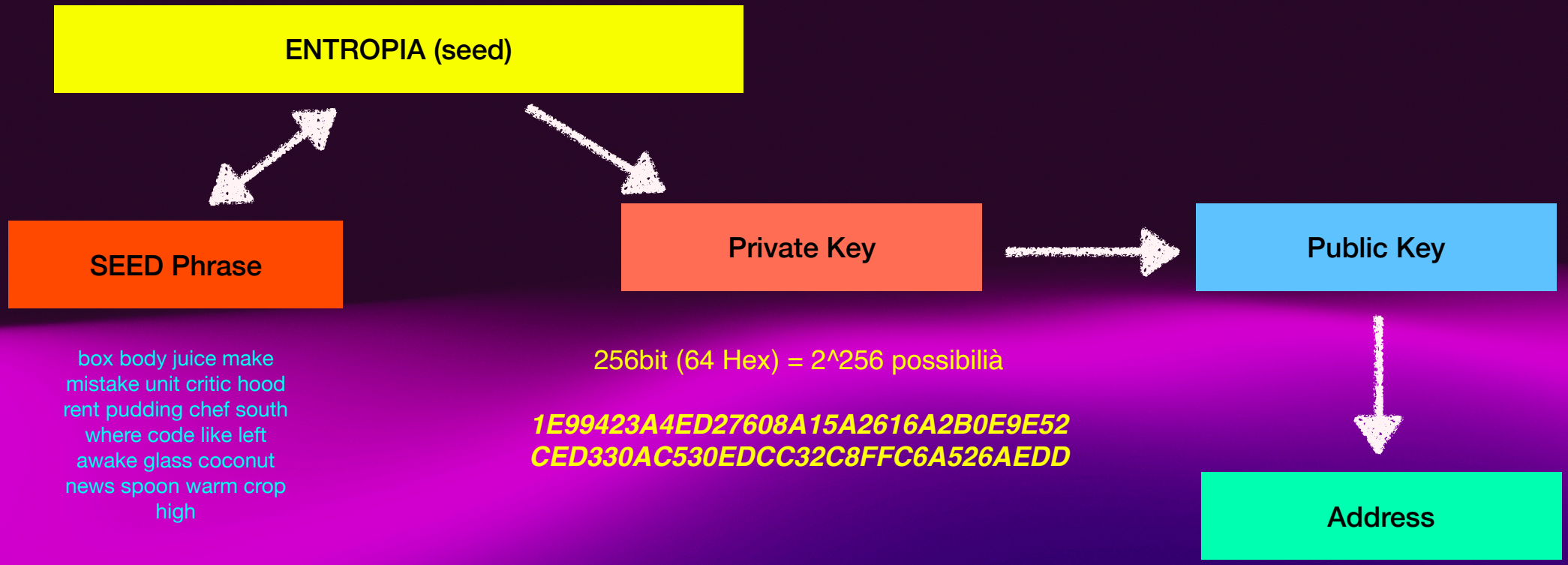
DEVE ESSERE PROTETTA !!!

1 toe	7 little	13 globe	19 cousin
2 miss	8 wink	14 thank	20 vibrant
3 arrive	9 any	15 clump	21 hockey
4 bonus	10 knee	16 connect	22 wave
5 gallery	11 exhaust	17 second	23 fragile
6 fan	12 below	18 bicycle	24 cricket

La SeedPhrase è TUTTO e SOLO il necessario per accedere ai fondi



ECDSA: Seed, PrivKey, PubKey, Address…



N.B.: Lo schema è esemplificativo
Le procedure sono più articolate per garantire molte funzionalità

Wallet

- Paper Wallet
- Software Wallet
- Hardware Wallet

Tipologie di ASSET

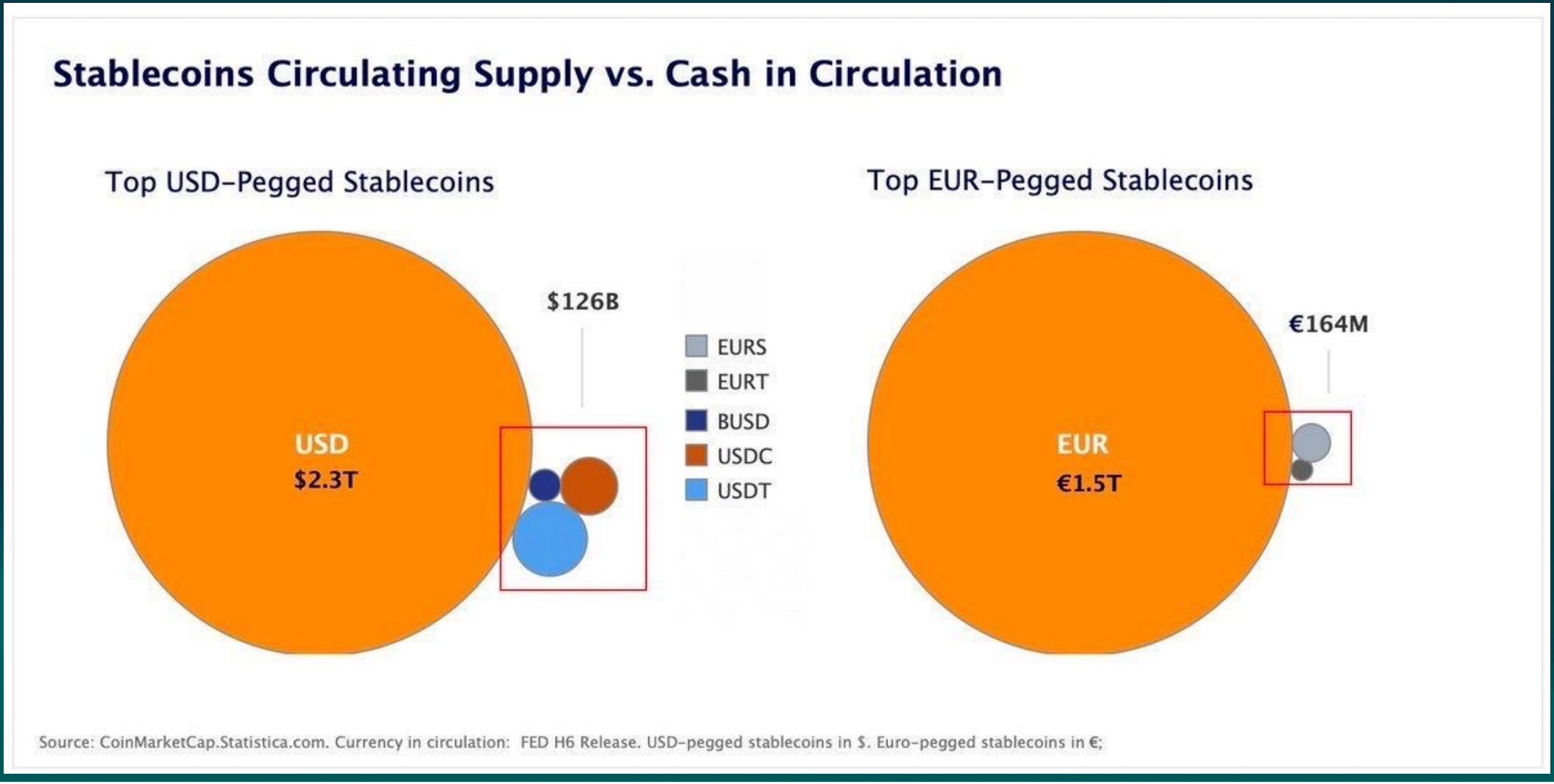
- **COIN** - sono la “valuta” nativa della blockchain, con essa si pagano le fee delle transazioni
  - Bitcoin
  - AltCoin
  - ShitCoin
- **TOKEN** - Asset “ospitati” in una blockchain non propria
  - Utility Token
  - Token di Governance
  - Fan Token
  - MemeCoin
  - …
- **NFT** - Asset identificati singolarmente, non frazionabili, rappresentativi di qualcosa che potrebbe provenire anche dal mondo fisico (Digital Twin)

Stablecoin

Asset “peggate” a FIAT in vari modi:

- **Collateralizzate in FIAT (USDT, USDC, BUSD…)**
- **Collateralizzate in Crypto (DAI, …)**
- **Algoritmiche (USDD, il fu USTC…)**
- **Miste**

Stablecoin


Stablecoins Circulating Supply vs. Cash in Circulation
Top USD-Pegged Stablecoins
$126B
USD
$2.3T
EURS
EURT
BUSD
USDC
USDT
Top EUR-Pegged Stablecoins
€164M
EUR
€1.5T
Source: CoinMarketCap.Statistica.com. Currency in circulation: FED H6 Release. USD-pegged stablecoins in $. Euro-pegged stablecoins in €;

CeFi - DeFi

CeFi : Centralized Finance (intermediata)

DeFi : Decentralized Finance (non intermediata)

Vediamo degli esempi…

Riferimenti web utili 1/3

Portali informativi

- coinmarketcap.com (quotazioni ed info token, statistiche su exchange, etc…)
- coingecko.com (quotazioni ed info token, statistiche su exchange, etc…)
- defillama.com (statistiche ed informazioni su DeFi)

Software Wallet (Free)

- https://bluewallet.io/ (Bitcoin, mobile)
- https://metamask.io/ (Ethereum & EVM compatibili, browser extension)
- https://trustwallet.com/ (Multichain, browser extension & mobile)

Riferimenti web utili 2/3

Blockchain Explorer

- blockstream.info (Bitcoin)
- https://mempool.space/ (Bitcoin & Lightning Network, interrattivo)
- etherscan.io (Ethereum)
- bscscan.com (BNB chain)
- polygonscan.com (Polygon/Matic)
- snowtrace.io (Avalanche)
- explorer.solana.com (Solana)

Riferimenti web utili 3/3

CeFi (Finanza Centralizzata)

- binance.com (CEX e CeFi)
- kraken.com (CEX e CeFi)
- coinbase.com (CEX e CeFi)
- nexo.com (CeFi, prodotti avanzati)
- youngplatform.com (CEX Italiano)
- crypto.com (CEX, CeFi)

DeFi (Finanza Decentralizzata)

- curve.fi (DEX)
- aave.com (Money Market)
- uniswap.org (DEX)
- sushi.com (DEX)
- http://yearn.finance (Yield Aggr.)
- https://stargate.finance/ (Bridge)