

QUANT-01



**MATTEO
MAGGIONI**

- Laureato in Economia delle istituzioni e dei mercati finanziari presso l'Università Cattolica di Milano. Membro dell'International Federation of Technical Analysts (IFTA) e socio della Società Italiana Analisi Tecnica (SIAT).
- Attualmente sono trader istituzionale sui mercati delle commodities.
- Specializzazione in strumenti derivati su indici azionari ed obbligazionari in ottica di breve periodo. Prediligo il trading algoritmico, basato sia su metodi tradizionali che innovativi, tra i quali il machine learning.
- Docente per FinecoBank SpA, per la Società Italiana Analisi Tecnica (SIAT) e per l'Ordine degli Ingegneri della provincia di Roma.
- Faccio parte del comitato scientifico della SIAT.
- Ho tenuto numerose conferenze sul trading in Italia e all'estero, tra cui Expo di Borsa Italiana, ITF di Rimini e Rotary Club.
- Sono autore e coautore di vari libri dedicati al trading e alle strategie di investimento.
- Dal 2012 mi occupo anche di valute digitali e blockchain e sono coautore dei libri "Bitcoin Revolution" e "Tutto su Bitcoin", editi da Hoepli.

QUANT01.AI@GMAIL.COM

ALTCOIN

Lezione 3 - 19/05/2021

1

STATISTICHE

2

CAMPI DI SVILUPPO

3

ETHEREUM

4

ALTRE CRIPTOVALUTE



1 Statistiche

Total market capitalization



Dominance Index



Cryptos

9411

Exchanges

367

Market Cap

2 T

24h Volume

212 B

Dominance index

BTC 50%
ETH 13%

Fonte: coinmarketcap.com - Dati aggiornati al 21 Aprile 2021



Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is \$1.96T, a ▲ 7.43% increase over the last day. [Read more](#)



Fiat Rankings

Compare to the largest fiat currencies in the world 🏆




\$FIO Earn Campaign

Learn and Earn with our latest campaign!

[☆ Watchlist](#)[Portfolio](#)[Cryptocurrencies](#)[Categories](#)[DeFi](#)[NFT](#)[Polkadot Eco](#)[BSC Eco](#)[Solana Eco](#)[Yield Farming](#)[Show rows](#)

100 ▾

[Filters](#)

# ▲	Name	Price	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ	Last 7 Days
1	<div> Bitcoin BTC</div> <div>Buy</div>	\$52,833.99	▲ 6.55%	▼ 7.82%	\$987,555,734,182	\$58,544,960,641 1,108,093 BTC	<div> ⓘ 18,691,675 BTC</div> <div></div>	
2	<div> Ethereum ETH</div> <div>Buy</div>	\$2,448.07	▲ 11.88%	▲ 8.27%	\$283,057,961,825	\$38,083,080,713 15,556,345 ETH	115,624,763 ETH	



2 Campi di sviluppo

Marco setttori

**VALUTE
DIGITALI**

**SMART
CHAIN**

DeFi

NFT

STORAGE

Esempi di applicazione

**SISTEMI DI
PAGAMENTO**

DIRITTI DI AUTORE

**SISTEMI DI
AUTENTICAZIONE**

HEALTHCARE

NOTAIO E LAGELE



3

Ethereum

Nascita di Ethereum

- Inizio 2013: la piattaforma Ethereum fu menzionata da Vitalik Buterin nel Bitcoin Magazine, di cui lo stesso era fondatore.
- Inizio 2014: il White Paper, scritto da Vitalik Buterin, viene formalizzata da Gavin Wood nel cosiddetto Yellow Paper.
- 30 Luglio 2015: rilascio della prima versione live della piattaforma (versione Frontier).



La rivoluzione di Ethereum



Ethereum è una piattaforma decentralizzata del Web 3.0 per la creazione e pubblicazione peer-to-peer di contratti intelligenti (smart contracts) creati in un linguaggio di programmazione Turing-completo.

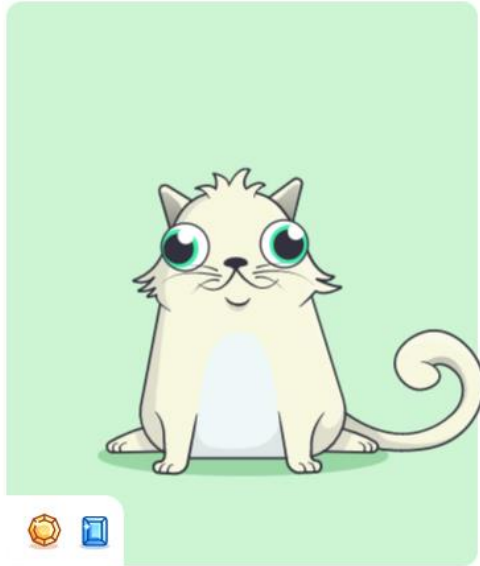


SMART CONTRACT

Cos'è l'Ether?



- Ether non è altro che una cryptovaluta, lanciata nel 2015, supportata dalla tecnologia Ethereum.
- Analogamente al Bitcoin, Ether è un sistema basato su Blockchain.
- Per finanziare il lavoro di sviluppo, Ethereum ha lanciato un'offerta pubblica di pre-vendita di Ether. È durata 42 giorni ed ha totalizzato la raccolta di 31591 Bitcoin, pari (al tasso di cambio del 2 settembre 2014) a circa \$ 18,4 milioni.
- La quotazione sul mercato risale ad inizio Agosto 2015, con un prezzo di circa 0,3 \$ per un Ether.



457507



⌘ Gen 0 ⌚ Fast (1m)



3 # Ethereum

Opensea.io



OpenSea



Search items, collections, and accounts

[Browse](#)

[Activity](#)

[Rankings](#)

[Blog](#)

[Community](#)

[Create](#)



[New](#)

[Art](#)

[Domain Names](#)

[Virtual Worlds](#)

[Trading Cards](#)

[Collectibles](#)

[Sports](#)

[Utility](#)

The largest NFT marketplace

Buy, sell, and discover rare digital items

[Explore](#)

[Create](#)

SOFT FORK

Sono degli aggiornamenti di un protocollo che provocano una temporanea divergenza nella blockchain.

- La divergenza persiste fino a quando i vecchi nodi non riconoscono i nuovi blocchi.
- Durante questa fase di attesa l'aggiornamento è reversibile.
- Possono apportare delle modifiche limitate al protocollo.

HARD FORK

Sono un cambiamento radicale di un protocollo che provocano una permanente divergenza nella blockchain.

- I vecchi nodi non riconosceranno mai più i nuovi blocchi generati dai nodi aggiornati.
- I nuovi blocchi vanno a far parte di una nuova Blockchain nativa.
- L'aggiornamento è irreversibile.

Ethereum Classic



**ETHEREUM
CLASSIC**

Codice: ETC



- Uno dei primi progetti creati per sfruttare gli smart contracts di Ethereum è stato lanciato nel 2016 con il nome di DAO (Decentralized Autonomous Organization).
- Il successo è stato immediato ed in meno di un mese sono stati raccolti fondi pari a circa il 14% della capitalizzazione di Ether.
- Poche settimane dopo sono stati rubati mediante un attacco hacker circa un terzo degli Ether raccolti.
- Questo evento ha decretato non solo la morte del progetto DAO ma anche lo scisma di Ethereum.

A seguito dei tentativi falliti per recuperare i token rubati e di un acceso dibattito su come intervenire, la comunità Ethereum è stata chiamata a votare sulla proposta di modifica del codice del protocollo in modo da poter restituire i fondi illecitamente sottratti.

L'esito positivo della votazione ha portato quindi ad una biforcazione della catena al blocco numero 1.920.000, il 20 Luglio 2016.

Tuttavia una minoranza di sviluppatori e miners non ha condiviso questa decisione ed ha continuando a supportare la versione originale di Ethereum, mossa dalla volontà di non modificare il codice e garantire l'immutabilità della blockchain.



4 Altre criptovalute

Bitcoin Cash



BITCOIN CASH

Codice: BCH



- Il primo hard fork della catena bitcoin si è verificato il 1° agosto 2017 con la formazione del blocco numero 478.558 e la nascita del bitcoin cash.
- Questa nuova valuta è stata creata a seguito di un acceso dibattito nella community bitcoin relativo alla scalabilità.
- Il bitcoin è in grado di gestire un numero relativamente basso di transazioni e per questo motivo non si pone al momento come una vera alternativa alla moneta ma è piuttosto da assimilare ad una riserva di valore o ad uno strumento di investimento.

Il Bitcoin Cash presenta tre principali differenze tecniche rispetto al Bitcoin:

- Aumento a 8 MB delle dimensioni dei blocchi, con un conseguente aumento del numero delle transazioni contenute in ogni blocco.
- Nuova tipologia di firma digitale per le transazioni che aumenta la sicurezza dei portafogli hardware ed elimina il problema dell'inefficienza di firma, noto come "quadratic hashing".
- Un nuovo algoritmo per il calcolo della difficoltà per cercare di mantenere il più possibile costante a 10 minuti il tempo di formazione dei blocchi.

Litecoin



LITECOIN

Codice: LTC



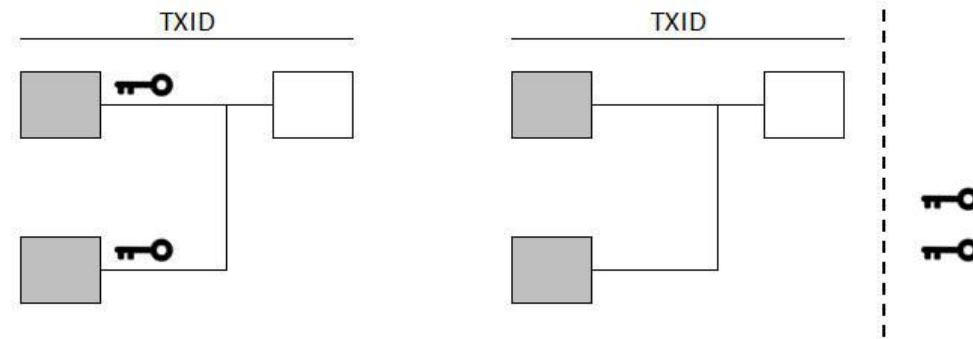
- Fondata nel 2011 da Charlie Lee, un ex dipendente di Google, è la valuta digitale più longeva dopo il bitcoin.
- I blocchi vengono generati mediamente ogni 2 minuti e mezzo con un tempo quattro volte inferiori a quello dei bitcoin.
- Si basa su un algoritmo di hash di tipo Scrypt, più semplice da eseguire e meno dispendioso dal punto di vista energetico rispetto all'algoritmo SHA-256.
- L'offerta di moneta è quadrupla rispetto a quella del bitcoin, ovvero 84 milioni di coin, e viene distribuita come forma di remunerazione per l'attività svolta dai minatori.

Il vero elemento distintivo si è concretizzato nel corso del 2017 con l'integrazione di SegWit (Segregated Witness). Questo aggiornamento ha prodotto due effetti:

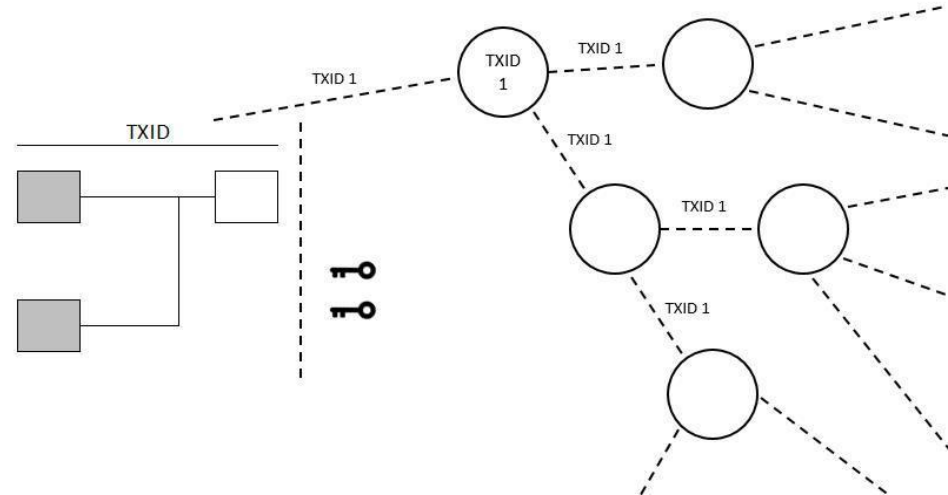
1. Aumenta il numero di transazioni contenute in un blocco.
2. Migliora la malleabilità delle transazioni.

.

Le firme digitali vengono invece separate dai dati delle transazioni e spostate in una sorta di blocco esterno, consentendo alle transazioni di essere più piccole. In questo modo il codice identificativo viene creato considerando tutti i dati della transazione, ad eccezione delle firme digitali. Quindi, in sostanza, SegWit separa la parte "validante" dalla parte "effettiva" di una transazione.



La malleabilità è un tipo di attacco che può essere intrapreso da un nodo della rete per modificare il codice identificativo di una transazione, prima che la stessa venga confermata e diffusa sulla blockchain. Con la separazione introdotta da SegWit diventa quasi impossibile che si possa verificare la malleabilità delle transazioni.



Ripple



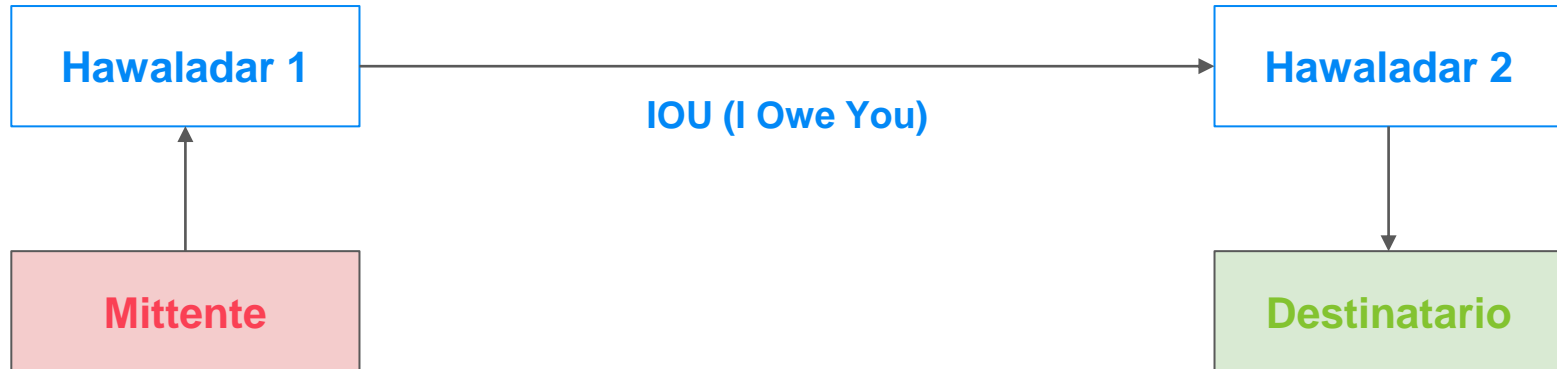
RIPPLE

Codice: XRP



- Le origini di Ripple risalgono al lontano 2004, quando Ryan Fugger avviò il progetto Ripplepay con l'obiettivo di creare un sistema monetario privo di intermediari.
- Le idee di Fugger furono poi riprese nel 2011 da Jed McCaleb, che insieme ad Arthur Britto e David Schwartz, iniziò a lavorare su un sistema di valuta digitale in cui il consenso era garantito dai membri del network piuttosto che dall'attività di mining.
- La squadra si allargò con l'arrivo dell'investitore Chris Larsene e poco dopo nacque il protocollo di pagamento, denominato Ripple Transaction Protocol (RTXP).

La logica sottostante a Ripple è molto simile ad un sistema di pagamento antico, sviluppato in Medio Oriente durante il medioevo, noto come “hawala”. In arabo, hawala significa trasferimento e consiste in un sistema di pagamento informale, in cui dei privati si accordano con altri privati per eseguire una transazione di denaro



Generalizzando si può affermare che Ripple è un sistema di pagamento che digitalizza il metodo hawala. Si basa infatti sul medesimo flusso operativo e sul rapporto di fiducia tra le persone.

Con Ripple il ruolo svolto dai mediatori hawala è sostituito da siti internet o attività commerciali, denominati gateway, che comunicano tra di loro in modo esclusivamente digitale.

Stellar Lumens



STELLAR LUMENS

Codice: XLM



- È un progetto open source nato nel 2014 in seguito all'uscita di Jed McCaleb da Ripple
- L'obiettivo è quello di creare un'infrastruttura per trasferire il denaro in modo sicuro, veloce e decentralizzato.
- L'architettura di Stellar si fonda sulla presenza di ancore ovvero di operatori terzi che fungono da ponte tra le valute fiat e la rete Stellar, in modo simile a quanto svolto dai gateway di Ripple.
- Le ancore conservano i depositi in valuta fiat emettendo dei crediti in Lumens ovvero la valuta digitale che viene utilizzata nella rete Stellar.

Le similitudini con Ripple sono evidenti, ma in realtà le differenze tra i due progetti sono più sostanziali di quello che si possa pensare. In particolare:

- Stellar è gestita da una fondazione senza scopo di lucro, la Stellar Development Foundation (SDF).
- Il codice sorgente dei due progetti è completamente diverso. Stellar è inoltre molto più aperto ai contributi di sviluppatori esterni e con la Stellar Build Challenge assegna premi monetari ai contributi migliori.
- Stellar utilizza un algoritmo di consenso noto come Stellar Consensus Protocol (SCP), i cui punti di forza sono da ritrovare nella decentralizzazione, flessibilità, sicurezza e bassa latenza. Mentre Ripple utilizza un algoritmo basato sul voto probabilistico.
- Stellar si rivolge soprattutto ad una clientela privata, mentre Ripple è più concentrata sull'offerta di servizi per operatori istituzionali.

EOS

Codice: EOS



- È un progetto lanciato nel 2017 dalla società block.one, di cui fa parte Daniel Larimer, uno degli sviluppatori più attivi e lungimiranti nel settore blockchain.
- Permette lo sviluppo di applicazioni decentralizzate (DApps), con una scalabilità sia orizzontale che orizzontale e con una latenza minima.
- I token EOS sono utilizzabili dagli utenti all'interno della piattaforma, garantendo anche il diritto di voto mediante l'algoritmo di DPoS (Delegated Proof of Stake).

Tether



TETHER

Codice: USDT




- È una stablecoin ovvero una criptovaluta il cui valore rimane costante nel tempo.
- Ha un legame uno-a-uno con il dollaro americano e l'euro e garantisce che per ogni token sul mercato ci sia una corrispettiva riserva in valuta fiat.
- Il numero complessivo di Tether è variabile: per ogni dollaro convertito in Tether nasce un nuovo token e per ogni dollaro richiesto indietro un token muore.
- È quindi da utilizzare non tanto in ottica speculativa ma piuttosto come valuta alternativa al dollaro per passare da una valuta all'altra o trasferire fondi tra piattaforme diverse.

AAVE

Codice: AAVE



- È un protocollo che permette di prestare e di ricevere in prestito criptovaluta.
- L'obiettivo è di creare una fonte di liquidità da fornire ai progetti blockchain.
- Funziona attraverso dei collateralizzati in criptovaluta o stable coin.
- Il tasso di interesse si aggiusta automaticamente in base ad un classico incrocio domanda ed offerta.

Assets ▼	Market size ▼	Totale preso in prestito ▼	Deposito APY ▼	Variable Prestito APR ▼	Fisso Prestito APR ▼		
 USD Coin (USDC)	466,72M	417,85M	6,12 %	3,98 %	10,99 %	<button>Deposita</button>	<button>Prendere in prestito</button>
 USDT Coin (USDT)	213,54M	196,32M	10,40 %	15,71 %	23,71 %	<button>Deposita</button>	<button>Prendere in prestito</button>
 DAI	178,68M	142,08M	5,55 %	3,98 %	11,99 %	<button>Deposita</button>	<button>Prendere in prestito</button>
 Decentraland (MANA)	35,76M	180,4K	0,00 %	0,08 %	3,11 %	<button>Deposita</button>	<button>Prendere in prestito</button>
 Binance USD (BUSD)	26,46M	21,01M	2,84 %	3,97 %	—	<button>Deposita</button>	<button>Prendere in prestito</button>
 REN	17,01M	1,08M	0,05 %	0,99 %	1,41 %	<button>Deposita</button>	<button>Prendere in prestito</button>
 ChainLink (LINK)	16,29M	74,35K	0,00 %	0,07 %	3,10 %	<button>Deposita</button>	<button>Prendere in prestito</button>

Cardano



CARDANO

Codice: ADA



- È stato sviluppato dalla società IOHK, fondata da Charles Hoskinson e Jeremy Wood, con l'obiettivo di creare una piattaforma blockchain di terza generazione.
- La blockchain ha una struttura multistrato che permette una maggiore flessibilità in fase di sviluppo ed aggiornamento, ma anche un elevato grado di sicurezza.
- Cardano utilizza un nuovo algoritmo di tipo Proof of Stake, noto come Ouroboros, che si caratterizza per garantire la casualità nella scelta del nodo validatore.

POLKADOT

Codice: DOT



- È un network che permette l'interconnessione di diverse blockchain interne o esterne al progetto, con l'obiettivo di sviluppare infrastrutture informatiche per un web decentralizzato.
- Permette di creare delle “parachain” ovvero delle blockchain specializzate ma integrate nel progetto principale.
- Le interazioni sulle parachains sono elaborate in parallelo, consentendo sistemi altamente scalabili.
- Utilizza un originale algoritmo di consenso noto come (GHOST-based Recursive Ancestor Deriving Prefix Agreement).

UNISWAP

Codice: UNI



- È un protocollo di scambio decentralizzato (DEX) all'interno dell'ecosistema Ethereum, lasciando il controllo dei fondi nelle mani dell'utente
- Fornisce anche un protocollo di liquidità Market Maker Automatizzato (AMM).
- Utilizza inoltre un modello noto come Costante Product Market Maker (CPMM) che permette di creare pool di liquidità.

Monero



MONERO

Codice: XMR

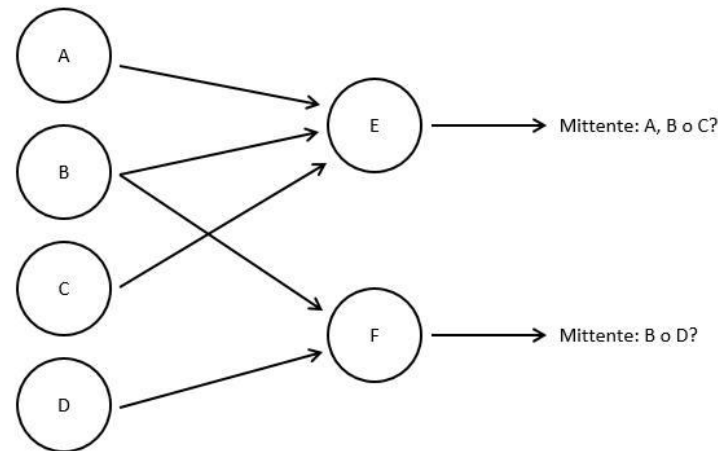


- È stata lanciata il 18 Aprile 2014, con il nome di Bitmonero ma subito rinominata in Monero che in lingua esperanto significa “moneta”.
- Garantisce un anonimato totale per le transazioni digitali mediante l’uso di Stealth Addresses, Ring Signatures, e RingCT.
- Utilizza un proprio algoritmo di tipo PoW, noto come RandomX che presenta le caratteristiche di essere ASIC-resistant e CPU-friendly.

Con la tecnologia “Ring Signature”, la quale la firma può essere eseguita da qualsiasi membro di un gruppo di utenti che dispongono delle chiavi.

La chiave pubblica del mittente e del destinatario vengono mescolata con le chiavi di altri utenti rendendo impossibile comprendere chi effettivamente ha svolto la transazione.

- Chi tra i mittenti A, B, C e D ha inviato una transazione ai destinatari E e F?
- Le possibilità sono varie e non esiste una risposta certa.



Zcash



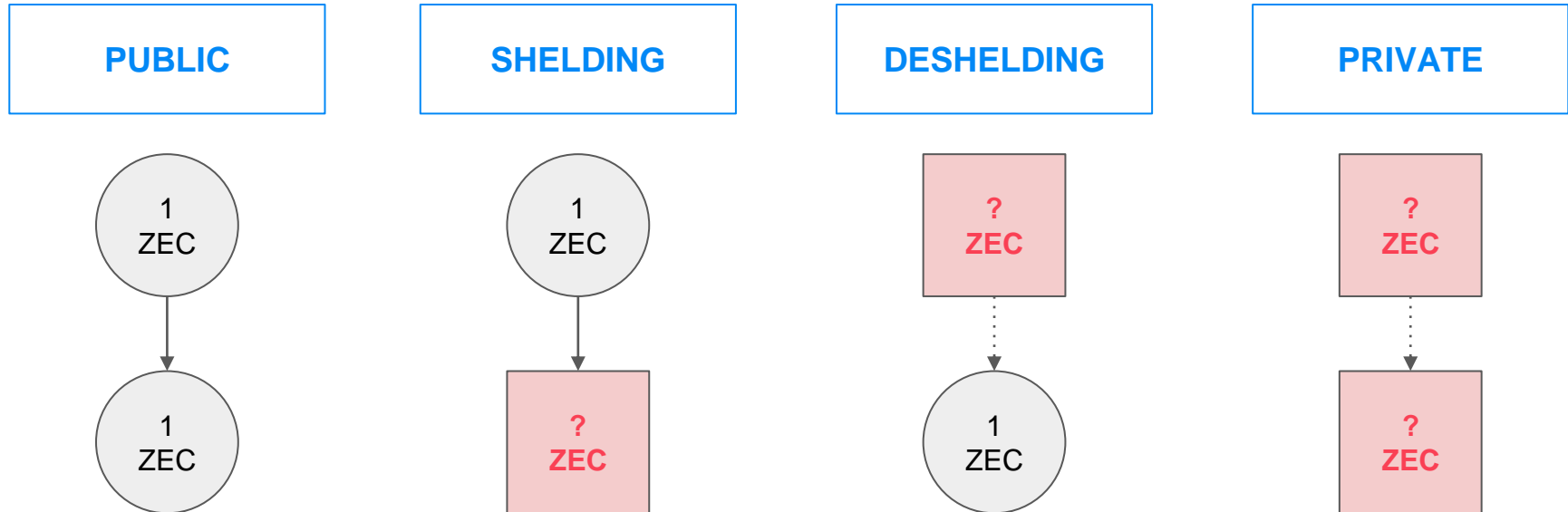
ZCASH

Codice: ZEC



- È stato lanciato a Gennaio 2016, su iniziativa di Zooko Wilcox-O'Hearn come biforcazione del bitcoin e con lo specifico obiettivo di garantire un anonimato totale nelle transazioni.
- Utilizza un metodo di crittografia zero-knowledge, noto come zk-SNARKs (zero-knowledge Succinct Non-interactive Argument of Knowledge).

Le transazioni anonime sono di tipo opzionale e possono riguardare anche solo uno dei due soggetti coinvolti. Le combinazioni possibili per svolgere una transazione sono quattro:



Le differenze tra queste tipologie di transazioni dipendono dalle caratteristiche degli indirizzi del mittente e del destinatario, che si distinguono in:

- **t-address (t-addr)**: è un indirizzo pubblico ed inizia sempre con la lettera “t”. Le transazioni in entrata e in uscita da questo indirizzo sono liberamente consultabili, così come avviene per ogni indirizzo bitcoin.
- **z-address (z-addr)**: è un indirizzo privato ed inizia sempre con la lettera “z”. Le transazioni in entrata ed in uscita da questo indirizzo non vengono mai rese pubbliche e sono consultabili solo dal possessore del wallet.

Dash



DASH

Codice: DASH



- È Il progetto Dash è stato lanciato ufficialmente il 18 gennaio 2014 inizialmente con il nome di XCoin.
- L'obiettivo era di creare una valuta digitale che cercasse di risolvere alcuni limiti del protocollo Bitcoin, in particolare l'anonimato e la velocità delle transazioni.

Due tipologie di funzioni applicabili alle transazioni:

1. **PrivateSend**: garantisce l'anonimato di una transazione, mediante un processo di mescolamento con altre transazioni che presentano questa funzione.
2. **InstantSend**: permette di confermare una transazione in meno di un secondo.

La novità del progetto Dash è stata quella di aver introdotto un'architettura a due livelli basata su:

- **Mining**: è basato su un meccanismo di consenso PoW, ma con la peculiarità di utilizzare l'algoritmo X11 che combina undici funzioni hashing diverse (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo).
- **Masternodes**: hanno diritto a ricevere una remunerazione per l'attività di Proof of Service (PoSe) che svolgono a sostegno del funzionamento del network Dash. Nello specifico, si occupano di PrivateSend, InstantSend e Decentralized Governance by Blockchain (DGBB).

QTUM

Codice: QTUM



- È una piattaforma blockchain ibrida, che combina la stabilità della blockchain bitcoin con la tecnologia degli smart contract di Ethereum.
- È compatibile con gli smart contract di Ethereum garantendo anche la retro compatibilità in caso di aggiornamento del codice.
- Permette di costruire applicazioni decentralizzate e adatte ai dispositivi mobili.
- Si base su un algoritmo Proof of Stake (PoS) che è molto più flessibile, scalabile ed economico del PoW.

Nem



NEM

Codice: NEM



- Così come per il bitcoin, anche per il NEM non è nota la vera identità del suo ideatore.
- Mira alla creazione di una nuova economia basata su principi di decentralizzazione, libertà finanziaria e pari opportunità.
- Presenta delle caratteristiche uniche, tra le quali: Proof of Importance (PoI), Vesting e Harvesting.

Con il PoI, ad ogni utente che possiede almeno 10.000 XEM viene assegnato un punteggio di importanza (importance score), non solo in base al numero di monete possedute, come di solito avviene con il PoS, ma anche al numero di transazioni ricevute ed effettuate. In questo modo si cerca di scoraggiare l'accumulo di monete e di rendere più uniforme la distribuzione della ricchezza.

Di conseguenza, un utente che mira esclusivamente ad accumulare XEM avrà un punteggio di importanza inferiore rispetto ad un utente attivo che contribuisce alla circolazione della moneta. L'utilizzo di questo algoritmo di consenso rende il NEM una valuta più rispettosa dell'ambiente, più equa e più sicura.

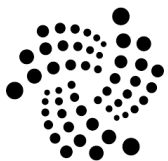
Il saldo di un account si divide in due parti:

- Vested: si compone delle valute che sono “maturate”.
- Unvested: si compone delle valute che non sono ancora “maturate”.

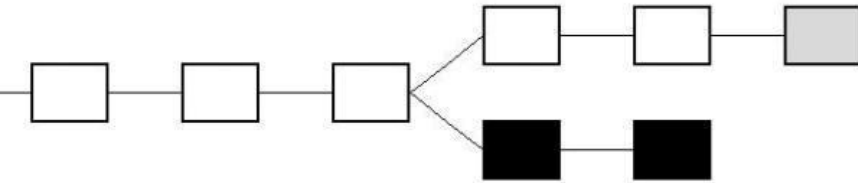
La maturazione (vesting) è un processo ideato per aumentare e garantire la fiducia all'interno del sistema NEM. In particolare ogni volta che un account riceve nuovi XEM, questi vengono aggiunti al saldo unvested per essere poi gradualmente spostati al saldo vested. Il trasferimento si attiva ogni 1440 blocchi, ovvero una volta al giorno, e riguarda solo 1/10 delle valute contenute nell'account unvested.

IOTA

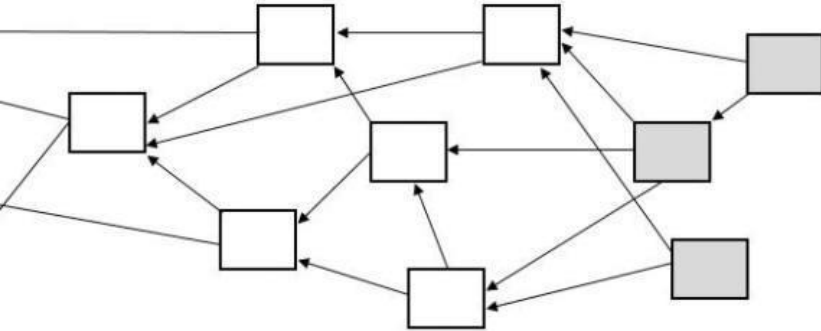
Codice: MIOTA



- È l'acronimo di Internet of Things Application ed è uno dei progetti più innovativi nel campo della crittografia dedicata a semplificare la comunicazione tra dispositivi intelligenti.
- La classica struttura blockchain è poco flessibile se applicata al settore dell'Internet of Things, che si caratterizza per un numero elevato di micro pagamenti.
- È quindi indispensabile passare ad un'architettura diversa che possa garantire costi bassi, velocità di esecuzione e soprattutto scalabilità: il DAG (Directed Acyclic Graph), che prende il nome di “tangle” (groviglio).



Con la blockchain le informazioni sono contenute nei blocchi ordinati cronologicamente.



Con il DAG le informazioni non sono raggruppate, ma semplicemente collegate con altre informazioni.

Le l'utilizzo della tangle garantisce a IOTA le seguenti caratteristiche:

- **Scalabilità**: le transazioni che possono essere approvate non presentano limiti numerici e temporali.
- **Decentralizzazione**: il consenso è ottenuto da ogni utente che svolge una transazione. Non è quindi necessaria un'attività di mining.
- **Priva di costi da transazione**: non essendoci minatori con IOTA non sono presenti incentivi e costi di transazione.
- **Immunità**: la funzione hash utilizzata nel protocollo IOTA, nota come Curl, si caratterizza per essere estremamente veloce e sicura, garantendo una sorta di immunità dall'arrivo dei computer quantici.



Disponibili su Amazon, Hoepli e nelle principali librerie



QUANT-OI

Grazie... e buon trading

QUANT01.AI@GMAIL.COM