Lezione 19
BlockChain per la gestione delle criptovalute
30/11/2023

Prof. Gian Paolo Stella
Economia degli Intermediari Finanziari

A.A. 2023-2024

Agenda

- Blockchain
- Bitcoin
- Da Bitcoin a Ethereum
- Bitcoin Vs Ethereum
- Quotazione Storica Bitcoin
- Quotazione Storica Ethereum
- Confronto a 5 Anni
- Confronto a 1 Anno
- Il Nuovo Futuro
- Il Caso di El Salvador
- Le criptovalute e la sostenibilità ambientale

Blockchain 1/6

- La Blockchain è una Internet delle Transazioni, cioè un insieme di tecnologie in cui il registro delle transazioni è strutturato come una catena di blocchi, la cui validazione è affidata a un meccanismo di consenso, distribuito su tutti i nodi della rete autorizzati a partecipare a tale processo di registrazione.

- I nodi sono i partecipanti alla Blockchain, costituti fisicamente dai server di ciascun partecipante.
- La tecnologia blockchain si basa su dei registri distribuiti (*Distributed Ledger Technologies, DLT)* che permettono la lettura e scrittura di uno più o soggetti presenti nella rete.

- A seconda della DLT saranno diverse le modalità di controllo e di verifica delle azioni di scrittura, modifica del registro, il tipo di consenso fondamentale per il processo di validazione delle azioni di scrittura e la struttura dello stesso registro distribuito.

Blockchain 2/6

- Rispetto alla versione iniziale pubblicata nel "*White Paper*" di Bitcoin nel 2008 da Satoshi Nakamoto, la tecnologia Blockchain ha avuto un notevole sviluppo negli ultimi 15 anni, diventando non solo una tecnologia conosciuta, ma anche un termine comune e condiviso fra le aziende, università e governi.
- L'obiettivo del fondatore (o fondatori) di Bitcoin, Satoshi Nakamoto, fu quello di inventare un sistema di denaro elettronico *peer-to-peer* che non avesse bisogno di una rete di intermediari (es. banche) per poter funzionare.
- Le caratteristiche essenziali legate allo sviluppo di una tecnologia blockchain sono:
    a) Registro Immutabile;
    b) Transazione Tracciate;
    c) Tecniche Crittografiche volte a garantire la sicurezza delle transazioni.

Blockchain 3/6

- Secondo la descrizione dello stesso Nakamoto nel "*White Paper*" di Bitcoin, i blocchi che compongono la tecnologia Blockchain sono composti da gruppi di transazioni avvenute in un certo lasso di tempo.

•La validazione delle transazioni avviene attraverso il meccanismo informatico del *Timestamp,* che permette di associare data e ora certe e legalmente valide ad un documento informatico.

•Nel caso di uno scambio di criptovalute, la transazione è rappresentata dallo scambio tra due soggetti della criptovaluta stessa.

•Il blocco, quindi, non sarà altro che l'insieme di un certo numero di transazioni avvenute in un certo intervallo di tempo nel quale sono presenti i dettagli delle transazioni.

Blockchain 4/6

- Quando il blocco raggiunge un certo numero di transazioni deve essere chiuso, affinché se ne possa aprire un altro. L'unione di nuovi blocchi alla blockchain avviene attraverso un processo chiamato "*mining*" o "estrazione".

•I nodi della rete eseguono il processo di mining per creare nuovi blocchi e aggiungerli alla catena. Il processo di *mining* inizia con la raccolta delle transazioni non ancora confermate in un nuovo blocco.

•Il nodo che riesce a risolvere un complesso problema matematico crittografico, noto come "*proof of work*", è in grado di aggiungere il nuovo blocco alla catena e ricevere una ricompensa in criptovaluta.

•Una volta che il nuovo blocco è stato aggiunto alla catena, le transazioni incluse in esso sono considerate confermate e diventano parte della storia immutabile della blockchain.

Blockchain 5/6

- I nuovi blocchi vengono collegati alla catena tramite una funzione di *hash*, che utilizza l'hash del blocco precedente per creare un collegamento sicuro tra i blocchi.

•Un elemento chiave per la comprensione del meccanismo della blockchain è dato dall'importanza del concetto della tracciabilità. In particolare, coerentemente con quanto riportato dal *white paper* di Satoshi Nakamoto, la tracciabilità è fondamentale per avere memoria di tutti gli scambi avvenuti, specialmente per gli scambi di valute virtuali, al fine di evitare quindi che in una qualsiasi infrastruttura blockchain possa verificarsi il fenomeno del *Double Spending*.

Blockchain 6/6

- La crittografia è anche necessaria sia per garantire la sicurezza delle transazioni sia per tutelare le informazioni personali dei soggetti coinvolti nella transazione.

- La tutela è garantita nella blockchain dalla presenza di due chiavi, una pubblica e l'altra privata.

•La chiave pubblica è un codice alfanumerico che può essere condiviso pubblicamente e utilizzato per cifrare i dati in modo che solo il possessore della chiave privata possa decifrarli.

- La chiave privata è un codice alfanumerico che deve essere tenuto segreto e utilizzato per decifrare i dati cifrati con la chiave pubblica.

•Nella blockchain, la chiave pubblica viene utilizzata per generare indirizzi connessi a dei *wallet* e per creare firme digitali che verifichino l'autenticità delle transazioni, mentre la chiave privata viene utilizzata per firmare le transazioni e per accedere al proprio *wallet,* contenente le proprie *cryptocurrencies*.

Criptoassets

- ***Le stablecoin***, che intendono mantenere un valore stabile in relazione ad uno o più asset: le più comuni sono "indicizzate" ad una valuta ufficiale; possono essere convertite al valore facciale o al valore di mercato delle riserve, poiché hanno come garanzia, totale o parziale, una serie di attività (cash, depositi, Treasury Bill, Commercial Paper, ma anche altre cripto asset) e sono utilizzate quasi esclusivamente come forme di pagamento.
- ***Cripto attività non stablecoin***, come il Bitcoin o Ether, le prime due criptovalute per capitalizzazione di mercato. Hanno una denominazione propria, non sono garantite da altri asset, non possono essere rimborsate dall'emittente.

Bitcoin 1/3

- Bitcoin probabilmente è una delle parole più sentite in questi ultimi anni, ma in pochi sanno dare una definizione esaustiva.
- Secondo Comandini “quando troviamo la parola bitcoin scritta con la lettera iniziale minuscola, ci si sta riferendo alla criptovaluta; se invece troviamo la parola Bitcoin con la lettera iniziale maiuscola stiamo invece parlando del protocollo open source diffuso da Satoshi Nakamoto sviluppato per l’utilizzo di questa criptovaluta. Bitcoin ha una serie di caratteristiche che lo rendono innovativo rispetto alle tradizionali valute.” (da zero alla luna, p. 43).
- Quindi il protocollo bitcoin è il modo in cui viene creato lo stesso, la criptovaluta invece è la rappresentazione digitale di valore.
- Dopo aver fatto questa breve distinzione tra il protocollo e la criptovaluta, è importante capire chi l’ha creata e in particolare in quale periodo storico è nata.
- L’ideatore è Satoshi Nakamoto, tuttavia, tale nome in realtà è uno pseudonimo utilizzato da una persona o un gruppo di persone per pubblicare il White Paper di Bitcoin il 31 ottobre 2008.

Bitcoin 2/3

- Da 10 anni in molti hanno provato a scoprire chi si cela dietro questo nome e nel 2015 è stato associato un anziano signore giapponese di nome Satoshi Nakamoto al creatore del protocollo. Tuttavia, la notizia fu smentita subito dopo, poiché non si trattava del programmatore che era riuscito a creare il nuovo mezzo di pagamento.
- Negli anni diversi nomi di famosi programmatori sono stati associati al fondatore Nakamoto e alcuni di questi avevano addirittura le chiavi dei blocchi iniziali della blockchain di bitcoin, ma non possedevano le chiavi del primo blocco, chiamato blocco genesi, che è stato creato da Nakamoto stesso.
- Analizzando il primo blocco della blockchain, Satoshi Nakamoto sarebbe in possesso ancora oggi di un milione di Bitcoin, che non ha mai spostato, il che lo rende in questo esatto momento uno dei 40 uomini più ricchi al mondo.
- La più importante proprietà su cui si basa bitcoin è la decentralizzazione, ossia la mancanza di un’autorità centrale che gestisce bitcoin. Data l’assenza di un’autorità, non vi è la necessità di pagamento delle commissioni per le transazioni a degli intermediari.

Bitcoin 3/3

- La seconda caratteristica è l'anonimato: al contrario delle transazioni effettuate presso gli intermediari finanziari di cui si conoscono tutti i movimenti, le transazioni di bitcoin avvengono in maniera diversa, infatti, gli indirizzi dei portafogli non possono essere assolutamente collegati a determinati soggetti.
- L'anonimato del bitcoin però non è assoluto, infatti, dato che ogni singola transazione viene registrata e mantenuta all'interno della blockchain, per ipotesi, sarebbe possibile risalire alla quantità di bitcoin che possiede ogni portafoglio. Riuscire a capire quanti bitcoin possiede ogni soggetto, però, è un'impresa utopica, poiché un utente può utilizzare diversi portafogli e destinare una determinata quantità di bitcoin a tutti i portafogli in suo possesso.
- La terza proprietà è la velocità: al contrario del mondo bancario dove gli assegni possono impegnare anche qualche giorno per essere incassati e i bonifici per essere accreditati, le transazioni di bitcoin, dal momento in cui vengono inviate, vengono accettate quasi immediatamente.
- L'ultima proprietà è la sicurezza: la possibilità di essere truffati all'interno della blockchain di bitcoin è praticamente nulla. Una volta che i bitcoin vengono inviati, non è più possibile annullare la transazione e riottenerli indietro. Questo processo garantisce la ricezione dei bitcoin e quindi la riuscita del pagamento.

Da Bitcoin ad Ethereum

- Ehereum venne ideata e sviluppata nel 2013 dallo sviluppatore russo Vitalik Butarin. Egli aveva preso spunto dalla *blockchain* Bitcoin per creare qualcosa che potesse andare oltre, sfruttando l'innovazione apportata dalla *blockchain* e usando le sue caratteristiche per poterla estendere ad un'ampia gamma di applicazioni.
- Sebbene anche tale piattaforma avesse la finalità di consentire di trasferire denaro digitale, il suo obiettivo specifico era quello di consentire, per mezzo della piattaforma open source, a chiunque partecipi alla rete di sviluppare il proprio codice e cosi di potere sviluppare una serie di applicazioni decentralizzate da condividere con tutti.
- Per poter finanziare lo sviluppo e il lancio di tale tecnologia, i fondatori decisero di dare il via ad una campagna di *crowdfunding* tramite la pre-vendita dei *token,* con la quale riuscirono a raccogliere oltre18 milioni di dollari.
- Successivamente, nel 2015 avvenne il lancio ufficiale della piattaforma.

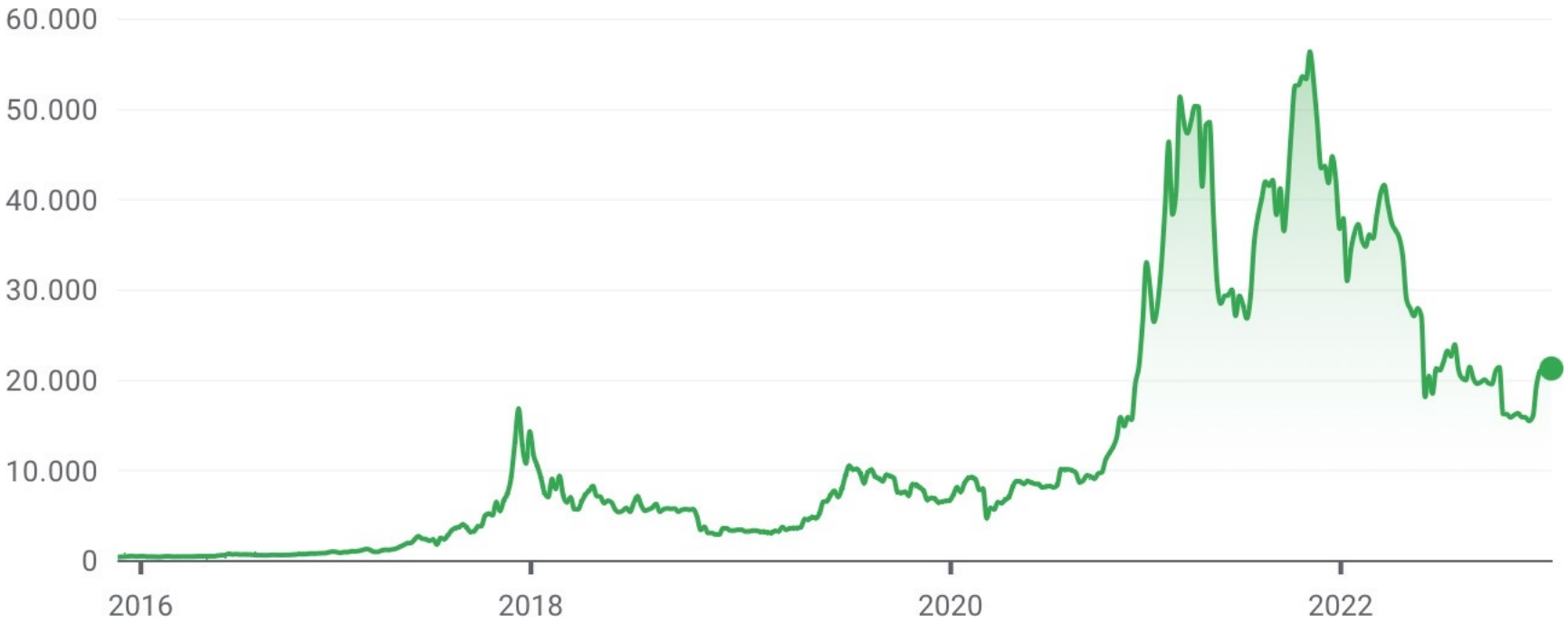
Bitcoin Vs Ethereum 1/2

- Come visto, Bitcoin e Ethereum rappresentano le *blockchain* più diffuse e con le rispettive criptovalute con maggiore capitalizzazione di mercato.
- Nonostante il pensiero alla base è il medesimo, queste due tecnologie presentano alcune differenze sostanziali tra loro.
- La *blockchain* Bitcoin è la prima in assoluto ed essere stata sviluppata ed applicata.
- In quanto l'obiettivo principale della *blockchain* era quello di giungere ad un sistema totalmente decentralizzato, il Bitcoin rappresenta tutt'ora la cripto valuta più decentralizzata, possedendo in assoluto la rete con il maggior numero di nodi e di *miners,* quella che richiede la maggior potenza di calcolo e che inoltre detiene la maggior quantità di quelle che vengono definite "*Hard fork*".

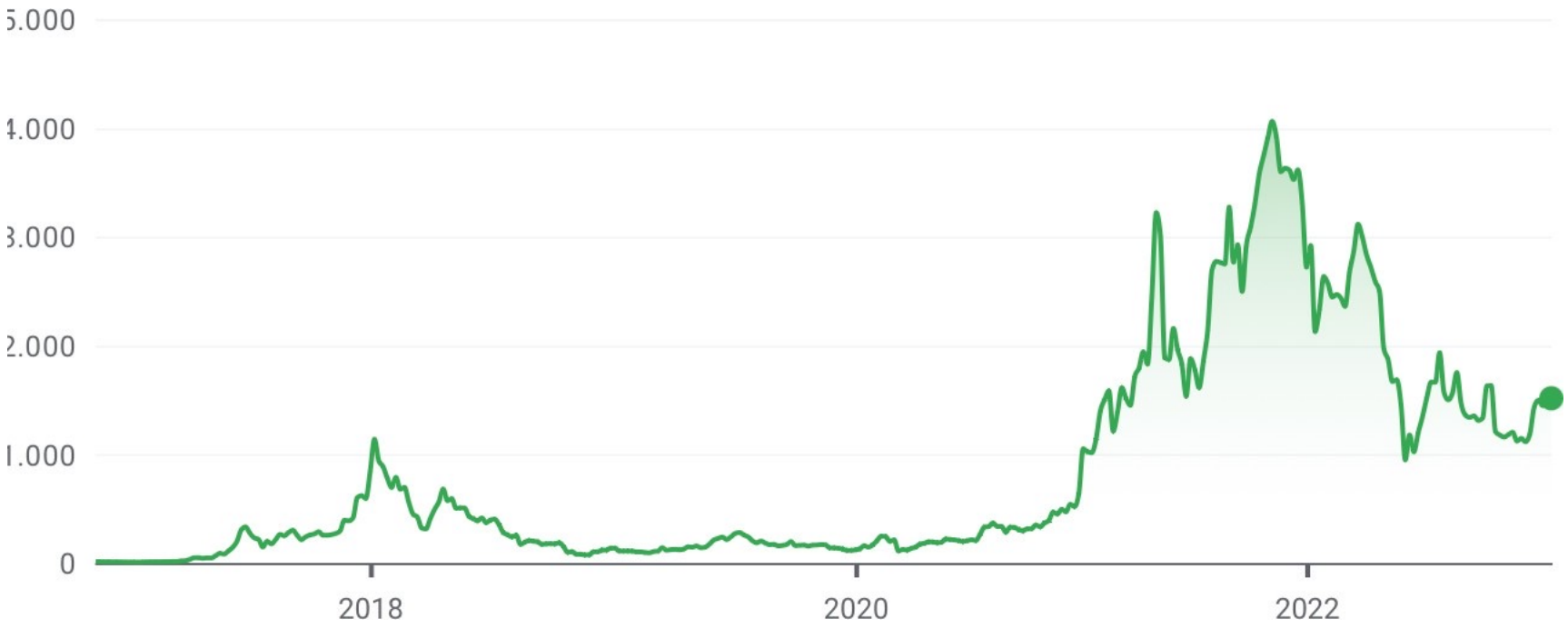
Bitcoin Vs Ethereum 2/2

- La *blockchain* Bitcoin nacque con l'obiettivo di fornire un sistema alternativo di pagamento decentralizzato, che potesse scardinare di fatto il ruolo dei tradizionali sistemi di pagamento e permettere l'esecuzione delle transazioni in via diretta senza presenza degli intermediari.
- La *blockchain* Ethereum è basata su queste caratteristiche ma ha voluto aggiungere molto altro, con l'aggiunta degli *smart contracts* e la possibilità di poter sviluppare le applicazioni decentralizzate (DApss e DAO); essa, pertanto, si è presentata come un progetto che potesse dare una spinta concreta all'intero campo della finanza decentralizzata.

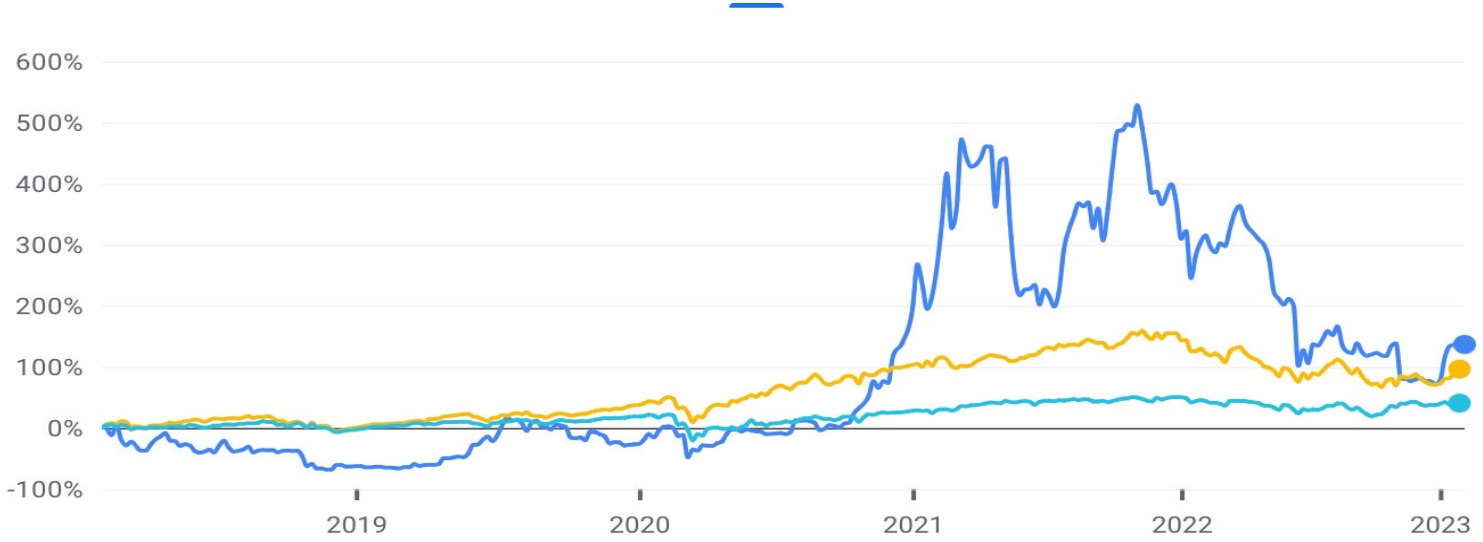
Quotazione Storica Bitcoin



Quotazione Storica Ethereum

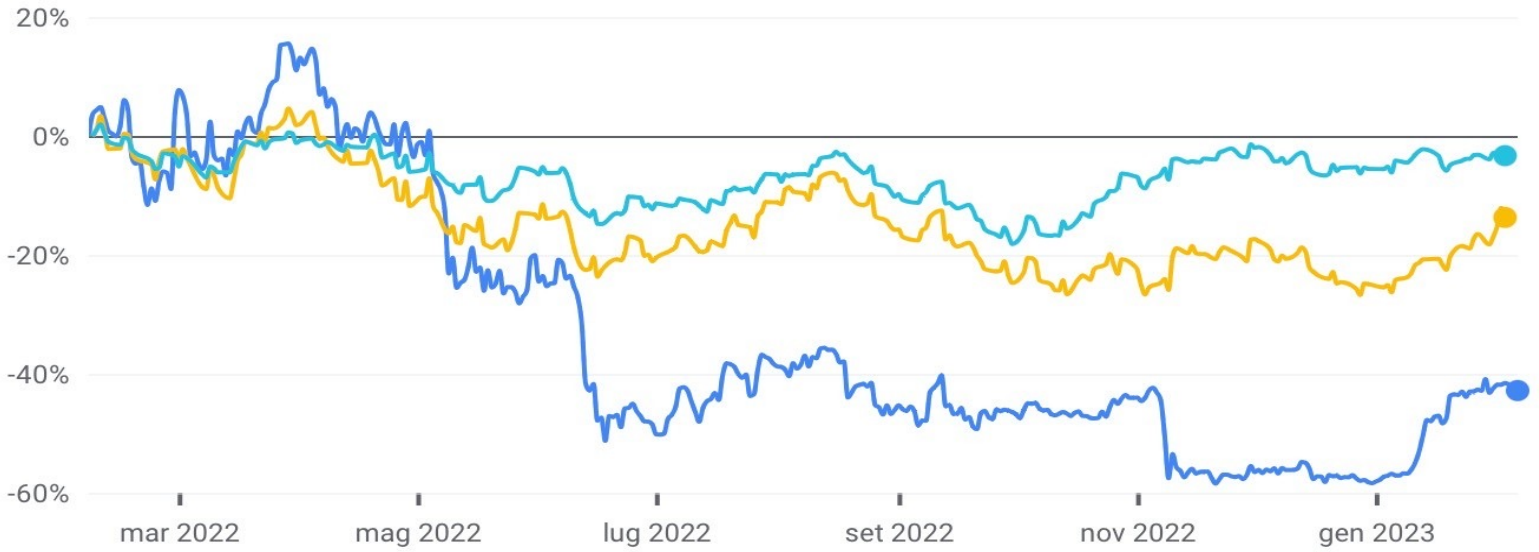


Confronto a 5 Anni



Bitcoin (BTC / EUR)	21.175,60	+12.213,12	↑136,27%
NASDAQ-100	12.573,36	+6.160,68	↑96,07%
Dow Jones	33.926,01	+9.735,11	↑40,24%

Confronto a 1 Anno



Bitcoin (BTC / EUR)	21.175,60	-15.858,72	↓42,82%
NASDAQ-100	12.573,36	-1.997,89	↓13,71%
Dow Jones	33.926,01	-1.165,12	↓3,32%

Il Nuovo Futuro? 1/2

- Da tempo si sta studiando l'ipotesi di creare altre forme di valute digitali, con caratteristiche ben distintive rispetto alle criptovalute: le *Central Bank Digital Currency* (Cbdc).
- La Cina ha avviato la sperimentazione dello yuan digitale nell'aprile 2020, attraverso le banche statali e le app di pagamento digitale utilizzate nel Paese; il lancio ufficiale è in calendario in queste settimane.
- Nel luglio scorso, la Bce ha avviato la fase di analisi del progetto di euro digitale, da utilizzare per i pagamenti al dettaglio, basato su un rapporto preparatorio dell'ottobre 2020; l'analisi dovrebbe durare 24 mesi.
- La Presidente della Bce ha dichiarato: "*Il nostro lavoro ha l'obiettivo di assicurare che nell'era digitale i cittadini e le imprese continuino ad avere accesso alla forma di moneta più la moneta della banca centrale*".

Il Nuovo Futuro? 2/2

- Ormai è inevitabile considerare le criptovalute parte integrante del sistema economico e quindi diventa indispensabile cercare di proporre un piano regolatorio sull'utilizzo delle stesse.
- A livello dell'UE, la Commissione europea ha deciso di fare un passo in avanti e regolamentare le valute digitali in un quadro normativo che possa essere uniforme e valido quindi in tutti i paesi membri.
- Proprio a riguardo, il 24 settembre 2020, la Commissione Europea ha deciso di adottare quello che viene chiamato "*Digital Finance Package* ", un pacchetto normativo sulla finanza digitale costituito al suo interno da vari documenti con l'obiettivo di poter sostenere la riprese economica in armonia con la transizione digitale, cercando cosi di poter dare una spinta per la modernizzazione dell'economia europea.

Il Caso Di El Salvador 1/4

- El Salvador è un piccolo paese nell'America centrale che confina ad est con l'Honduras e a nord col Guatemala.
- Nell'ultimo anno si è sentito molto parlare di questa piccola nazione, il motivo è molto semplice: è il primo paese al mondo che ha adottato bitcoin come valuta legale. Infatti, nel giugno 2021, il presidente di El Salvador, Nayib Bukele, ha annunciato che bitcoin sostituirà il dollaro americano.
- A settembre dello stesso anno il presidente Bukele annunciò che il governo aveva acquistato 400 bitcoin. Al momento dell'acquisto il prezzo di bitcoin si aggirava intorno ai 52.000 dollari, per un acquisto totale di circa 20 milioni di dollari.

Il Caso Di El Salvador 2/4

- L’adozione del bitcoin all’interno del sistema economico è un progetto azzardato per un paese che conta una popolazione di 6,5 milioni di abitanti e più della metà degli stessi non possiede un conto bancario. Inoltre il prodotto interno lordo è costituito da più del 20% in rimesse che provengono dagli Stati Uniti.
- L’obiettivo del presidente Bukele è proprio quello di sostenere e agevolare lo sviluppo economico in un paese in cui il pil pro capite medio tra il 2019 e il 2021 è di 4000 dollari.

Il Caso Di El Salvador 3/4

- Il secondo obiettivo dell'introduzione del bitcoin è proteggere i risparmi dei cittadini, poiché grazie all'utilizzo dello stesso, le commissioni per le rimesse dovrebbero essere più economicamente sostenibili.
- Per incentivare l'utilizzo di bitcoin all'interno del paese il presidente Bukele ha installato 200 sportelli automatici per convertire dollari in bitcoin o viceversa; in aggiunta è stato lanciato un wallet chiamato Chivo, che i cittadini potranno scaricare, e inserendo i loro dati, riceveranno 30 dollari in bitcoin.
- All'interno della piccola nazione vive un sentimento di scetticismo, la popolazione infatti non si trova d'accordo con la scelta del presidente.
- I cittadini, in realtà, non hanno l'obbligo di utilizzare bitcoin come valuta legale, dato che gli stipendi e le pensioni rimarranno in dollari i quali saranno liberamente convertibili in bitcoin.

Il Caso Di El Salvador 4/4

- I problemi di sicurezza non si sono fatti attendere, infatti, a pochi mesi dall'introduzione di bitcoin e dal lancio di Chivo, degli hacker hanno già preso di mira i portafogli dei cittadini salvadoregni, rubando più di 90.000 dollari.
- Oltre alla vulnerabilità dei portafogli dei cittadini, il paese deve affrontare un'ulteriore problema: la volatilità del prezzo di bitcoin.
- Pertanto il fondo monetario internazionale ha incentivato El Salvador di ritornare sui propri passi e rinunciare a bitcoin come valuta legale date le altissime probabilità di un aumento del debito pubblico del 96% entro il 2026.

Le criptovalute e la sostenibilità ambientale

- Un punto molto critico per le criptovalute è relativo al consumo di energia necessario ad assicurare l'attivita di mining.
- Gli interventi per limitare i danni per l'eccessivo utilizzo di energia sono da un lato, il ricorso il più possibile ad energie rinnovabili; dall'altro, la creazione di meccanismi che comportino un risparmio energetico come potrebbe essere la selezione casuale dei miner, in modo da non far lavorare contemporaneamente milioni di processori in competizione fra loro per creare un nuovo blocco.
- La necessità di ridurre i costi legati all'utilizzo dell'energia ha portato molti miner ad operare in Paesi freddi tipo Russia, Islanda, Groenlandia in cui l'energia ha un costo relativamente basso e il clima freddo permette l'utilizzo ottimale delle macchine.