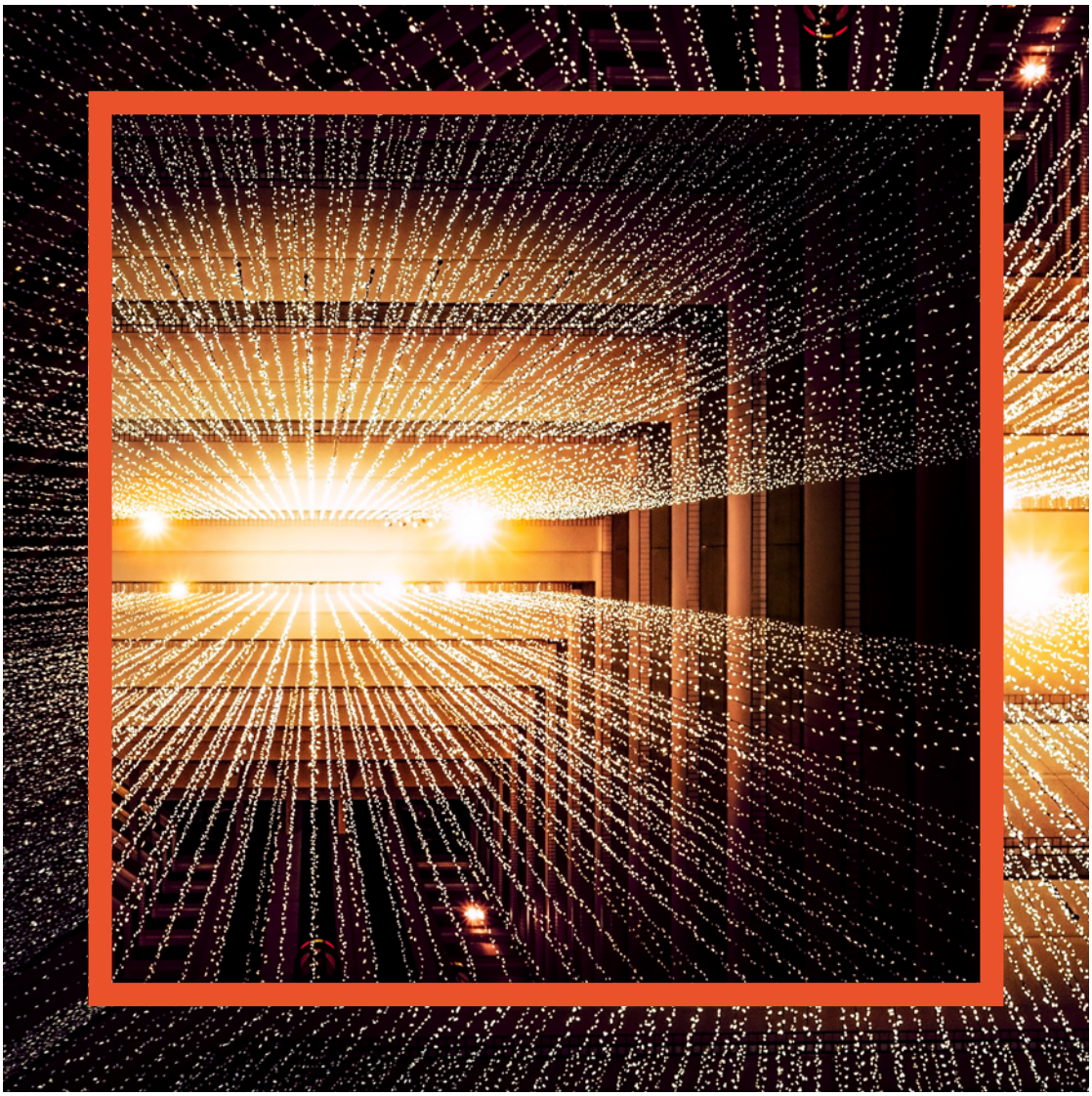
CRIPTOVALUTE:
da Bitcoin a Ether



Swissquote

Indice

BITCOIN (XBT)

La prima criptovaluta

Il Bitcoin è la prima valuta digitale in assoluto, creata nel 2009, un mese dopo il collasso di Lehman Brothers, dallo sviluppatore giapponese Satoshi Nakamoto. Può essere rappresentata da due simboli: XBT e BTC.

L'obiettivo principale era creare un sistema di pagamento elettronico anonimo, trasparente, decentralizzato e semplice da definire.

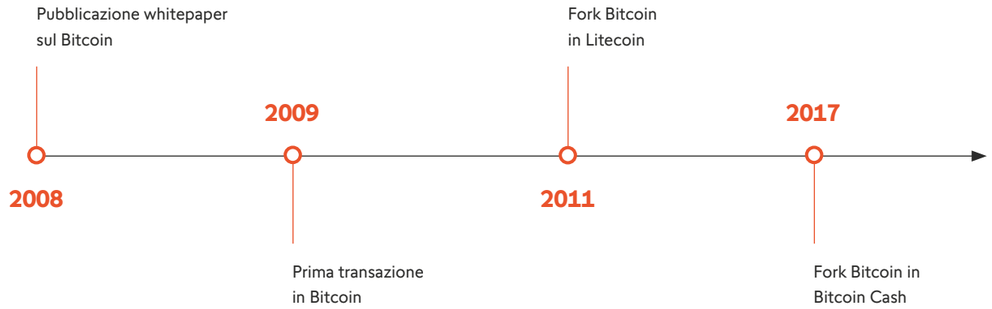
DATI PRINCIPALI (AL 25 MARZO 2020)

Crypto	Classifica	Capitalizzazione di mercato	Prezzo corrente
XBT	#1	EUR 113 miliardi	EUR 6'148

Grafico del prezzo

Fonte: CoinMarketCap

Aspetti generali



CRIPTOVALUTA: il Bitcoin è una moneta originale che fa riferimento a una rappresentazione digitale di un valore finanziario che può essere trasferito. Si basa su un calcolo e una criptazione matematica efficaci per garantire informazioni e transazioni.

DECENTRALIZZAZIONE: essendo decentralizzato, il Bitcoin non richiede un amministratore centrale né un intermediario. Le unità o le frazioni di Bitcoin possono essere inviate da un utente all'altro tramite la rete della blockchain del Bitcoin.

TECNOLOGIA: la blockchain è una catena di blocchi collegati tra loro e distribuiti tra gli utenti che fungono da ledger di dati invariabile.

OFFERTA LIMITATA: analogamente ad altre criptovalute, il Bitcoin è caratterizzato da un'offerta limitata. Significa che quando si raggiunge l'offerta massima di 21 milioni di unità, non vengono generati altri Bitcoin.

OPEN SOURCE: il protocollo del Bitcoin è open source e chiunque può accedere al codice, esaminarlo e contribuire al suo sviluppo.

Altre applicazioni della blockchain

BENEFICENZA
Ottimizzazione della trasparenza sull'uso dei fondi ricevuti.

SALUTE
Miglioramento della sicurezza dei record della sanità digitale e del monitoraggio della fornitura di farmaci.

Blockchain

Cos'è la blockchain?

La blockchain è la tecnologia sottostante che supporta il Bitcoin e tante altre criptovalute.

Si tratta di un database che funge da ledger digitale decentralizzato. I record dei dati sono organizzati in blocchi, associati tra loro a livello crittografico.

I principali vantaggi risiedono nella disponibilità permanente dovuta all'assenza di un singolo punto di errore e nella stabilità: i dati, infatti, non possono essere modificati in seguito alla registrazione sulla blockchain. La tecnologia blockchain elimina anche la dipendenza da intermediari e la necessità di affidarsi a un'unica organizzazione.

Perché la blockchain è sicura?

Nel caso del Bitcoin e tante altre valute virtuali, la tecnologia della blockchain garantisce che nessun Bitcoin venga distrutto o duplicato. Tutto questo è possibile grazie a due principali proprietà della blockchain:

Invariabilità

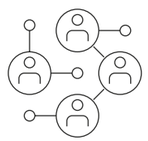
- Quando si conferma la validità di una transazione o della registrazione di qualsiasi tipo di dati, **non sono possibili altre modifiche e se ne garantisce così l'integrità.**

Consenso

- **Capacità di assicurare un unico ed effettivo stato della rete della blockchain** e, quindi, la validità di ogni transazione che vi si registra.

Altre applicazioni della blockchain

INTERNET OF THINGS
La blockchain consente di proteggere le funzionalità di raccolta dati offerte dall'IoT.



CATENA DI APPROVVIGIONAMENTO
Miglioramento della gestione della distribuzione dei prodotti e della trasparenza dei pagamenti.

Come funziona la blockchain del Bitcoin?

Come già indicato in precedenza, quando la transazione del Bitcoin è stata convalidata, non può essere modificata o eliminata dalla blockchain. Infatti, i dati vengono aggiunti per blocchi incatenati tra loro.

La catena di blocchi e le transazioni sono verificabili, dal momento che sono visibili a tutti. La blockchain può essere descritta come directory laddove ogni nuovo inserimento è collegato all'ultimo. Ad esempio, osservando il blocco classificato come 452°, è possibile verificare che è venuto dopo il blocco 451°. Inoltre, anche l'ultimo blocco inserito risulterebbe diverso se il primo blocco mai creato («il blocco genesis») fosse stato differente.

In che modo i blocchi della blockchain si collegano tra loro?

È semplice: la criptazione matematica alla base della blockchain del Bitcoin consente la generazione di un output univoco per ogni blocco, dai dati contenuti nell'ultimo. Tale output viene quindi trasferito al blocco successivo e fornisce un collegamento permanente tra i due, impedendo così per sua stessa natura qualsiasi tentativo di modifica successiva delle transazioni precedenti.

COS'È L'HASHING?

Per «hashing» si intende l'operazione in cui varie immissioni di diverse dimensioni generano vari output di dimensioni costanti. Inoltre, gli algoritmi di hashing genereranno sempre lo stesso output per una stessa immissione.

ANALOGIA DELLA BLOCKCHAIN

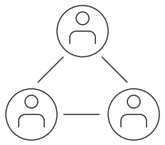
Classificazione blocco	Blocco		Analogia hash
1	hsgAO	→	EM
2	IzoEM	→	OF
3	pmzOF	→	LN

Come vengono creati i blocchi della blockchain?

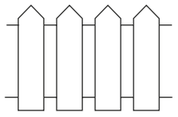
La produzione di nuovi blocchi è il risultato diretto di un processo noto come «mining». Come indicato in precedenza, i blocchi sono collegati insieme grazie alla crittografia. Per la produzione di nuovi blocchi è necessario l'impegno dei partecipanti in rete, che mettono a disposizione la loro capacità di calcolo per consentire la criptazione matematica dei dati delle transazioni.

I miner sono quindi responsabili della verifica di tutte le transazioni. Inoltre, la loro attività di mining è ricompensata sotto forma di Bitcoin appena creati che vengono immessi in rete.

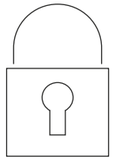
Cosa offre la blockchain del Bitcoin?



ELIMINA LE CONTROPARTI
Tutti i pagamenti in Bitcoin avvengono senza la necessità di una controparte, il che permette una riduzione delle commissioni di transazione e dei rischi generalmente associati alla partecipazione di intermediari.



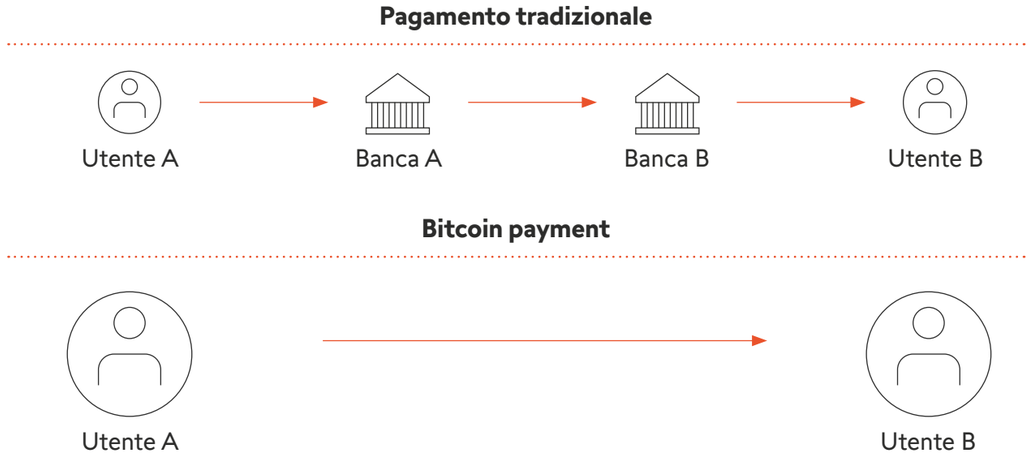
BASSE BARRIERE DI INGRESSO
La blockchain non ha limitazioni, ossia non è richiesta alcuna autorizzazione per partecipare e contribuire alla sua rete. Pertanto, un utente ha solo bisogno di una connessione a Internet per effettuare in maniera efficace transazioni con Bitcoin.



MIGLIORAMENTO DELLA SICUREZZA
In quanto decentralizzata, la blockchain non offre un singolo server centrale che potrebbe essere oggetto di azioni dannose. La blockchain funziona grazie a una rete di nodi sparsi e un hacker dovrebbe mirare contemporaneamente a un numero molto elevato di nodi per compromettere la rete.

Pagamenti in Bitcoin

Confronto con metodi di pagamento tradizionali



Quali sono le opzioni di storage non-custodial del Bitcoin?

Considerata l'assenza di terze parti, spesso sorgono domande sulle diverse possibilità disponibili relative allo storage non-custodial dei Bitcoin. Sono disponibili due opzioni principali: hot wallet e cold wallet.

Gli hot wallet sono software online che consentono agli utenti di memorizzare e inviare/ricevere Bitcoin in modo molto semplice. I conti dei proprietari di criptovalute possono essere considerati come un tipo di hot wallet.

Viceversa, i cold wallet vengono memorizzati offline (generalmente su un supporto fisico) e offrono un livello maggiore di sicurezza. Ledger è senza dubbio il fornitore più rinomato di cold wallet. Altre opzioni includono Trezor, KeepKey e CoolWallet S.

Nodi di Bitcoin

Cosa sono i nodi di Bitcoin?

I nodi di Bitcoin possono essere definiti come determinati tipi di programmi che interagiscono con la blockchain del Bitcoin. Essendo in costante comunicazione tra loro, questi nodi sono il motore che permette al Bitcoin di operare come criptovaluta completamente decentralizzata, garantendo il rispetto di tutte le regole definite.

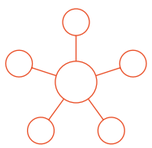
Nodi completi, nodi leggeri e nodi di mining sono le tre principali tipologie nella rete del Bitcoin.

NODI COMPLETI

Questi nodi rappresentano il fulcro della natura decentralizzata del Bitcoin. Si occupano di caricare e verificare le transazioni e i relativi blocchi.

NODI LEGGERI

I nodi leggeri hanno capacità ridotte rispetto ai nodi completi, ma richiedono meno risorse. Consentono agli utenti di individuare la loro transazione in uno specifico blocco.



NODI DI MINING

I nodi di mining possono essere descritti come nodi completi con la capacità aggiunta di mining e, quindi, di produzione dei blocchi. Tali nodi convalidano le transazioni prima di ritrasmetterle ad altri nodi.

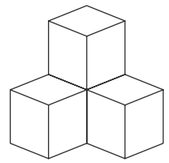
Halving del Bitcoin

Cos'è l'halving del Bitcoin?

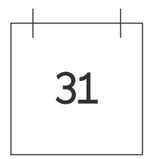
Per «halving del Bitcoin» si intende il caso in cui il normale premio dei miner per la verifica delle transazioni viene dimezzato. Questo evento si verifica ogni volta che 210'000 Bitcoin sono stati sottoposti a mining, generalmente ogni quattro anni.

		Premio per blocco per i miner a seguito dell'halving
Gennaio 2009	Lancio Bitcoin	50 BTC
Novembre 2012	1° halving Bitcoin	25 BTC
Luglio 2016	2° halving Bitcoin	12.5 BTC
Maggio 2020	3° halving Bitcoin	6.25 BTC
2024	4° halving Bitcoin	3.125 BTC
2028	5° halving Bitcoin	1.5625 BTC

Si verifica circa ogni 4 anni



Evento maggiore che regola l'offerta di Bitcoin



Il prossimo halving avverrà intorno al 18 maggio 2020

Perché si verifica?

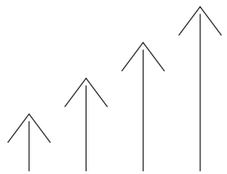
L'halving del Bitcoin è integrato nel software della blockchain e coinvolge direttamente i miner. I miner giocano un ruolo chiave perché la loro attività consente la verifica di ogni transazione con Bitcoin.

Le transazioni sono verificate per blocchi. Dopo aver verificato un blocco di transazioni, un miner riceve un premio che consiste in un numero di nuovi Bitcoin. Il giorno stesso e fino all'halving successivo, un miner riceve 12.5 BTC per blocco verificato. Dopo il successivo halving, questo premio sarà dimezzato.

Gli halving proseguiranno fino a raggiungere l'offerta massima di 21 milioni di Bitcoin, prevista attorno al 2'140. In seguito, i miner riceveranno ugualmente le commissioni di transazione per continuare a essere incentivati a verificare le transazioni con Bitcoin.

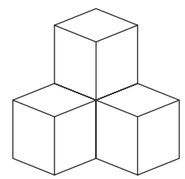
Halving ed evoluzione del prezzo del Bitcoin

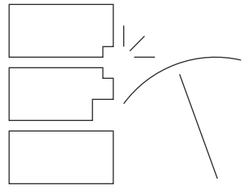
Quali sono le conseguenze dell'halving del Bitcoin?



Storicamente, i prezzi del Bitcoin aumentano un mese prima dell'halving e durante il periodo successivo a esso. Finora, i prezzi del Bitcoin non sono mai scesi al di sotto del valore precedente l'ultimo halving. I fattori sono molteplici: un aumento dell'attenzione sui Bitcoin e la riduzione automatica dell'offerta di nuove emissioni.

Finora, i prezzi del Bitcoin non sono mai scesi al di sotto del valore precedente l'ultimo halving. I fattori sono molteplici: un aumento dell'attenzione sui Bitcoin e la riduzione automatica dell'offerta di nuove emissioni. In questo modo viene controllata l'inflazione del Bitcoin.





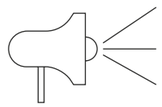
È prevedibile che un determinato numero di miner possa interrompere la sua attività in seguito alla riduzione del 50% del premio per blocco, che non potrà coprire i costi energetici e di calcolo a loro carico. Tuttavia, ciò non dovrebbe avere alcun effetto sulla velocità con cui le transazioni vengono verificate, perché la difficoltà nella verifica viene compensata rapidamente dal software.

Transazioni con Bitcoin

Come funziona effettivamente una transazione con Bitcoin?

Esempio: Vanessa desidera inviare 10 BTC a Chad

1

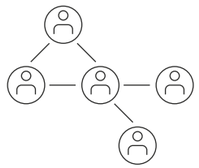


Vanessa informa la rete di miner che desidera inviare 10 BTC a Chad. Quindi, invia loro l'indirizzo di Bob, la sua firma personale e la chiave pubblica per consentire ai miner di confermare la sua identità.

2

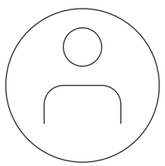
I miner controllano che la verifica della transazione si riveli redditizia per loro. Quindi, si assicurano che i 10 BTC appartengano a Vanessa e che la transazione sia valida prima di inserirla in un blocco.

3



Il miner trasmette le informazioni all'intera rete di miner, affinché questi possano verificarne la validità e tutti le aggiungano alla copia della propria blockchain.

4



Chad riceve realmente i 10 BTC che Vanessa gli ha inviato.

Verifica automatica dell'identità

Nessuna dipendenza da una controparte centrale

Tracciabilità migliorata e permanente

Forks

Cosa sono i fork Bitcoin?

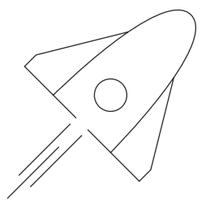
I fork sono per il protocollo del Bitcoin ciò che gli aggiornamenti rappresentano per i vari software informatici che utilizziamo tutti i giorni. Infatti, i fork Bitcoin permettono di risolvere i vari problemi del protocollo e migliorare ulteriormente le possibilità e le prestazioni.

Il protocollo del Bitcoin è ciò che definisce le norme che regolano il funzionamento del protocollo delle criptovalute, che tutti i nodi della rete devono seguire (ad es. le dimensioni di un blocco). Pertanto, ogni fork può avere importanti conseguenze sul funzionamento del Bitcoin.

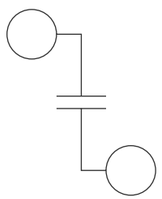
Cos'è un soft fork?

Sono disponibili due tipi di fork: soft e hard fork. Un soft fork Bitcoin è essenzialmente una modifica del protocollo del Bitcoin che resta compatibile con le versioni precedenti rispetto all'ultima.

Significa che i nodi più obsoleti (ossia i nodi che esistevano prima del fork e che non sono stati aggiornati) sono ugualmente in grado di elaborare transazioni, purché non violino le nuove regole definite dal fork. Inoltre, anche in caso di soft fork, i nodi più obsoleti scelgono generalmente di essere aggiornati, dato che ciò consente loro di risultare più efficienti nelle rispettive operazioni.



Più conveniente per gli utenti: nessuna necessità di aggiornamento



Minore probabilità di un chain split

Cos'è un hard fork?

Un hard fork è anch'esso una modifica del protocollo del Bitcoin, con l'eccezione che i nodi più obsoleti che non si aggiornano all'ultima versione del protocollo non potranno continuare con la loro attività.

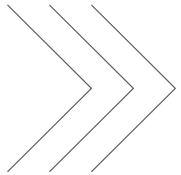
I due principali tipi di hard fork

I due principali tipi di hard fork

La maggior parte dei nodi si aggiorna volontariamente alla versione più recente e abbandona quindi la versione più obsoleta (ossia la vecchia catena) lasciandola con un piccolo numero di partecipanti.

Hard fork controversi

Generalmente, ciò avviene quando la community non concorda sull'aggiornamento e si traduce nella creazione di due blockchain separate (ossia un chain split) e quindi di due criptovalute indipendenti.



Gli hard fork offrono maggiore flessibilità perché la compatibilità con le regole delle versioni precedenti non ha bisogno di essere garantita

Il Bitcoin - Hard fork Bitcoin Cash

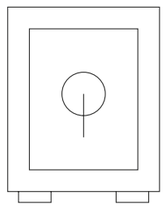
Questo hard fork si è verificato nell'agosto del 2017, quando la community si è divisa sul modo in cui sarebbero stati risolti i problemi relativi alla scalabilità del Bitcoin. Con un fork sempre basato sulla blockchain originale, tutti i proprietari di Bitcoin hanno ricevuto la stessa quantità di unità di Bitcoin Cash al momento del fork.

Algoritmi Proof-of-Work

Consenso della blockchain

Come indicato in precedenza, il consenso è una delle due principali caratteristiche della blockchain. La blockchain può generalmente ottenere consenso tramite 2 tipi di algoritmi: Proof-of-Stake (PoS) e Proof-of-Work (PoW). La blockchain del Bitcoin utilizza quest'ultimo.

L'obiettivo originale degli algoritmi PoW era la difesa dagli attacchi DoS («Denial of Service»). Gli attacchi DoS generalmente interrompono l'accesso degli individui alle reti, sovraccaricandole o mandandole in crash con altre operazioni pericolose.



Grazie all'uso degli algoritmi Proof-of-Work, un attacco riuscito alla blockchain del Bitcoin richiederebbe notevoli capacità di calcolo e si rivelerebbe piuttosto dispendioso in termini di tempo. Inoltre, l'elevato costo associato gioca un ruolo dissuasivo molto importante.

Come funzionano gli algoritmi Proof-of-Work?

Per aggiungere un blocco alla blockchain dei Bitcoin, i miner competono tra loro per risolvere complessi problemi matematici (ossia produrre un hash) grazie alla loro capacità di calcolo. Quindi, i miner trasmettono la loro soluzione ad altri nodi (miner) della rete affinché verifichino che la soluzione sia corretta.

Ognuno di questi blocchi dispone di un «hash» che rappresenta effettivamente il lavoro svolto dai miner, ossia la prova del lavoro (Proof-of-Work). Per hackerare la blockchain del Bitcoin, un soggetto esterno malintenzionato dovrebbe produrre un ledger più lungo di quello esistente (con tutti i blocchi a partire dalla creazione), il che richiederebbe una capacità di calcolo quasi irraggiungibile.

Riepilogo

La criptovaluta più famosa

Realizzato nel 2009, il Bitcoin è la criptovaluta attualmente più nota. L'obiettivo era creare «denaro elettronico peer-to-peer per Internet» che fosse «completamente decentralizzato, senza una banca centrale e terze parti cui affidarsi per operare».

Il Bitcoin è supportato dalla blockchain

La criptovaluta è supportata dalla blockchain, che la arricchisce con diverse caratteristiche, quali l'invariabilità o una sicurezza e una tracciabilità superiori.

Il Bitcoin è in costante miglioramento

Poiché il suo protocollo è open source, il Bitcoin ha un'importante community che contribuisce notevolmente al suo sviluppo.

Il futuro del Bitcoin

In ragione della sua fornitura limitata (21 milioni di unità di Bitcoin), il Bitcoin viene spesso indicato come l'«oro digitale». È stato finora sottoposto a mining circa il 90% dei Bitcoin. Tuttavia, in ragione degli halving, occorrerebbero altri 100 anni prima che tutti i Bitcoin siano sottoposti a mining. Pertanto, a causa della sua scarsità e difficoltà di produzione e all'elevata liquidità associata al Bitcoin, diversi osservatori indipendenti vedono la criptovaluta come un porto sicuro e un attivo il cui valore sarà apprezzato nel tempo.

ETHEREUM (ETH)

Trading corrente

Rilasciato nel 2015 e spesso indicato come l'«MS Windows» delle criptovalute, Ethereum viene utilizzato per sviluppare applicazioni decentralizzate. La criptovaluta ad esso associata, Ether, è la seconda maggiore del mercato.

L'inventore di Ethereum, Vitalik Buterin, ha sviluppato il concetto di «smart contract», ossia programmi eseguiti sulla blockchain.

DATI PRINCIPALI (AL 25 MARZO 2020)

Crypto	Classifica	Capitalizzazione di mercato	Prezzo corrente
ETH	#2	EUR 14 miliardi	EUR 123.16

Grafico del prezzo

Fonte: CoinMarketCap

Aspetti generali

Cos'è Ethereum?

Ether e Bitcoin sono criptovalute molto famose. La principale differenza tra le due sta nel fatto che Ethereum consente di utilizzare gli **smart contracts** e di creare **applicazioni decentralizzate (dapp).**

Applicazioni decentralizzate

Mentre il Bitcoin è principalmente un sistema di trasferimento di denaro basato sulla blockchain, lo scopo di Ethereum è diverso poiché l'obiettivo principale è **consentire agli sviluppatori di creare e pubblicare applicazioni decentralizzate (denominate dapp) sulla relativa blockchain.** Tante altre criptovalute disponibili su Swissquote quali Eos, Chainlink o Tezos, offrono anche la possibilità di sviluppare e utilizzare dapp.

Inoltre, si prevede che gli smart contract risolvano diverse complessità che gli interessati affrontano durante negoziazione, compensazione e liquidazione delle operazioni in titoli, gestione delle richieste di risarcimento o anche dei documenti della catena di approvvigionamento.

Ether, la criptovaluta

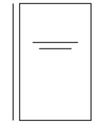
Ethereum può essere definita come una piattaforma software decentralizzata ed Ether come la criptovaluta associata a essa. **In quanto tale, Ether non è solo una criptovaluta negoziabile, ma è anche utilizzata dagli sviluppatori per pagare vari servizi forniti sulla rete Ethereum, quali esecuzione o monetizzazione di applicazioni.**

Ether può essere ottenuta tramite trading su un exchange cripto e mining. A differenza del Bitcoin, Ether non richiede capacità settoriali dato che incoraggia il mining decentralizzato da parte degli individui, con algoritmi proof-of-work (problemi di matematica complessi da risolvere per confermare la formazione di un blocco).

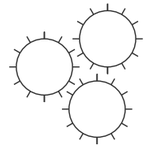
Smart contract

Cos'è uno smart contract?

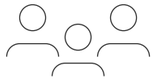
In sintesi, gli smart contract potrebbero essere descritti come contratti digitali a esecuzione automatica. Più specificamente, si tratta di codici informatici il cui obiettivo è facilitare il trasferimento di valore, contenuto o proprietà. **La principale caratteristica degli smart contract sta nel fatto che consentono questo trasferimento di proprietà o qualsiasi altra operazione che supportano solo se vengono soddisfatte determinate condizioni definite in precedenza.** Ciò consente di intraprendere operazioni sicure tra terze parti sconosciute e una velocità di esecuzione senza pari.



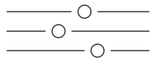
Pubblicamente disponibile sul ledger



Esecuzione automatica di operazioni e trasferimenti specifici



Non richiede l'intervento di un intermediario



Interamente personalizzabile

VANTAGGI

- Offre maggiore sicurezza per i contratti stipulati in modo tradizionale
- Riduce i costi delle transazioni
- Garantisce una sicurezza completa anche con terze parti sconosciute

Ethereum Virtual Machine (EVM)

L'EVM viene spesso indicata come la principale innovazione di Ethereum. Si tratta di un software che consente lo sviluppo e l'esecuzione di applicazioni basate su blockchain nella maniera più efficiente possibile, proteggendole da tutte le interferenze con altri programmi sulla blockchain stessa.

LITECOIN (LTC)

Trading corrente

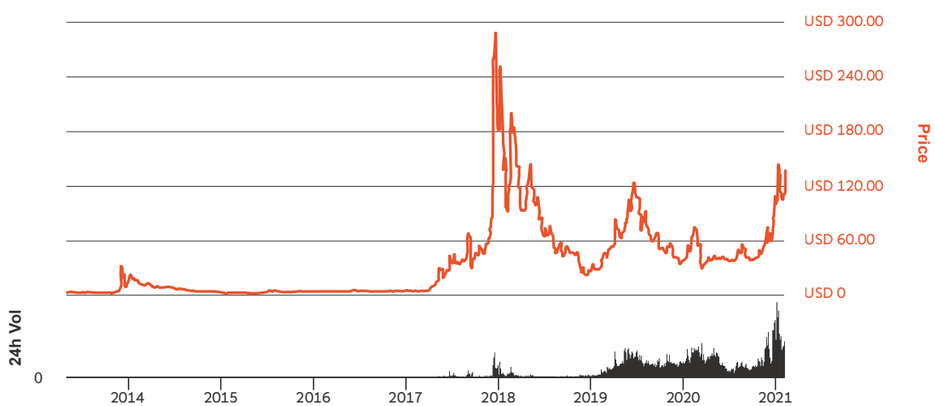
Fondata nel 2011 da Charlie Lee, ex ingegnere di Google, Litecoin è una delle prime criptovalute a essere stata lanciata. Il principale obiettivo di questa creazione era stabilire una valuta digitale che fosse più adatta all'utilizzo quotidiano rispetto al Bitcoin.

Anche Litecoin si basa sul medesimo codice open source del Bitcoin. Il suo principale vantaggio sta nel fatto che il codice consente la creazione di un blocco ogni 2.5 minuti, rispetto ai 10 minuti del Bitcoin.

DATI PRINCIPALI (AL 25 MARZO 2020)

Crypto	Classifica	Capitalizzazione di mercato	Prezzo corrente
LTC	#7	EUR 2.3 miliardi	EUR 35.78

Grafico del prezzo



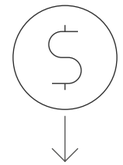
Fonte: CoinMarket Cap

Aspetti generali

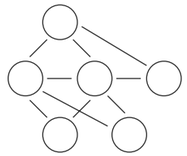
Quali sono le differenze tra Litecoin e Bitcoin?

Litecoin è una criptovaluta che deriva da un fork del client core del Bitcoin. In pratica, significa che Litecoin è fondata sulla base di codici open source iniziale dei Bitcoin, a cui gli sviluppatori hanno aggiunto nuove funzioni. In quanto tale, Litecoin si basa anche sulla tecnologia blockchain e si affida a un sistema completamente decentralizzato. Tuttavia, le nuove funzioni sono state realizzate a supporto dell'obiettivo di Litecoin di risolvere problemi che il Bitcoin non era destinato ad affrontare.

Velocità di transazione 4 volte più veloce



Transazioni meno costose



Different mining algorithm

Transazioni rapide e a costo quasi zero

Sebbene entrambe le criptovalute facciano affidamento sull'algoritmo proof-of-work, Litecoin utilizza Skrypt, che appare come un metodo di mining più libero, rispetto all'algoritmo SHA-256 del Bitcoin. Infatti, richiede meno risorse al processore rispetto a SHA-256, perché non complica le operazioni per il mining, evitando che diventi accessibile solo ai miner con elevate capacità di calcolo. **L'algoritmo Skrypt consente a Litecoin di ridurre notevolmente i costi delle transazioni.**

Affinità con il Bitcoin

Proprio come nel caso dei Bitcoin, l'offerta di Litecoin è limitata, il che comporta la protezione della criptovaluta dall'inflazione e contribuisce a preservarne il valore. Le transazioni con Litecoin vengono verificate come quelle con Bitcoin, grazie ai miner che vengono ricompensati per ogni blocco di transazione confermato. Come per il Bitcoin, il premio per i miner è dimezzato dopo ogni halving (il prossimo è previsto nel 2023).

RIPPLE (XRP)

Trading corrente

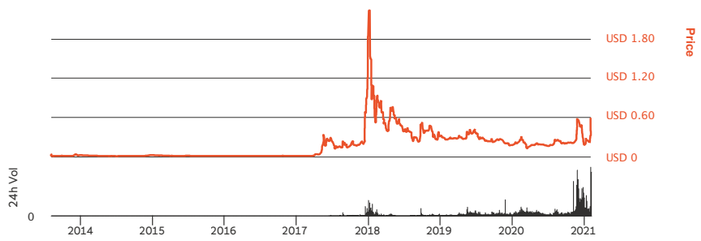
Ripple consente transazioni ultra-rapide (circa 4 secondi) e offre commissioni particolarmente basse, combinate con una rete scalabile. Il sistema centralizzato in tempo reale di Ripple è in grado di gestire circa 1'500 transazioni al secondo.

La principale caratteristica di XRP è la rete che lo supporta, che può essere considerata alla stregua di un exchange che facilita i pagamenti tra banche e altri istituti finanziari.

DATI PRINCIPALI (AL 25 MARZO 2020)

Crypto	Classifica	Capitalizzazione di mercato	Prezzo corrente
XRP	#3	EUR 7.0 miliardi	EUR 0.16

Grafico del prezzo



Fonte: CoinMarketCap

Breve storia

2004 — Primo prototipo di Ripple come sistema monetario digitale decentralizzato (RipplePay)

2012 — Creazione di OpenCoin, azienda tecnologica incentrata sulle soluzioni di pagamento per istituti finanziari

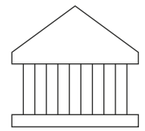
2015 — Rebranding ufficiale di Ripple Labs (ex OpenCoin) in Ripple

Aspetti generali

Le principali funzioni di Ripple

Convertibile in tutte le valute

Transazioni eseguite in meno di 4 secondi



Realizzato per istituti finanziari

Il ledger XRP

The XRP ledger (XRPL)

- **Sistema distribuito open source che consente transazioni finanziarie istantanee,** storage dei dettagli contabili e servizi di cambio valuta.
- **Il consenso viene raggiunto tramite l'algoritmo proprietario di Ripple,** applicato grazie a una rete di convalida di nodi indipendenti.
- **I clienti di Ripple hanno accesso a un elenco di nodi affidabili (UNL) cui tutti devono attenersi allo stato attuale del ledger.** Pertanto, la verifica delle transazioni di Ripple non si basa sul mining.

Una criptovaluta per istituti finanziari

Ripple è la prima criptovaluta dedicata alle banche e agli istituti finanziari. **Il suo obiettivo è risolvere i problemi che questi ultimi devono affrontare, in termini di limiti di liquidità correlati a possibili fluttuazioni dei tassi di cambio, velocità di liquidazione (4 secondi rispetto a 2-3 giorni per i sistemi di pagamento tradizionali), offrendo al contempo il livello di sicurezza associato all'uso della blockchain.**

BITCOIN CASH (BCH)

Trading corrente

Il Bitcoin Cash è stato creato tramite il fork Bitcoin dell'agosto del 2017. A differenza del Bitcoin, si tratta di «una moneta elettronica peer-to-peer per Internet. È completamente decentralizzata, senza banca centrale e terze parti cui affidarsi per operare».

L'idea alla base della sua creazione era offrire transazioni pressoché immediate riducendone l'elevato costo normalmente associato al Bitcoin. Ciò permette al Bitcoin Cash di essere utilizzato nelle piccole transazioni di tutti i giorni, al contrario del Bitcoin.

DATI PRINCIPALI (AL 25 MARZO 2020)

Crypto	Classifica	Capitalizzazione di mercato	Prezzo corrente
BCH	#5	EUR 3.8 miliardi	EUR 204.55

Grafico del prezzo

Source: CoinMarketCap

Le origini del Bitcoin Cash

Il Bitcoin Cash è stato creato tramite un hard fork con Bitcoin nel 2017. La blockchain del Bitcoin Cash è stata modificata per aumentare le dimensioni di un blocco di transazioni da 1 MB del Bitcoin a 8-32 MB.

Aspetti generali

Maggiore scalabilità e spese inferiori

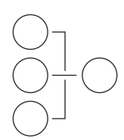
Capacità di elaborazione delle transazioni

L'obiettivo della nuova versione della blockchain del Bitcoin Cash è quello di risolvere i problemi associati alle commissioni di transazioni superiori che alcuni utenti Bitcoin sostenevano aumentando sostanzialmente le dimensioni di un blocco.

La blockchain del Bitcoin Cash riduce il tempo richiesto dalle transazioni per poter essere inserite in un blocco, senza incentivare i miner a definire un costo superiore. Pertanto, il Bitcoin Cash risulta più pratico per i micropagamenti e consente alla rete di evitare la congestione anche in periodi di attività superiori.

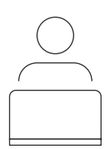
Grazie alle maggiori dimensioni del blocco, il Bitcoin Cash può offrire ai miner anche premi superiori per il mining di un blocco, in quanto quest'ultimo sarà composto da più transazioni.

Funzioni condivise con il Bitcoin

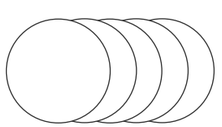


Basato su blockchain

Codice open source



Algoritmo proof-of-work



Fornitura limitata (21 milioni di unità)

PROSSIMI PASSI – INIZIARE A FARE TRADING CON SWISSQUOTE

1

Vai a **swissquote.com/trading**

2

Apri un conto demo.

3

Puoi esercitarti a fare trading con denaro virtuale (CHF 10'000). Nessun rischio e nessun obbligo.

Prova subito una demo!

Perché operare con Swissquote?

- 20 anni di esperienza nel trading on line
- Accedi a 3 milioni di prodotti sulle principali borse valori internazionali
- La piattaforma di trading più completa sul mercato
- Assistenza clienti in più lingue
- Formazione e istruzione con webinar online
- Applicazioni mobili ad alte prestazioni
- Gruppo internazionale quotato sulla SIX Swiss Exchange (SIX:SQN)

Swissquote viene regolarmente citata e consultata dai media finanziari globali.

Bloomberg

CNBC

FINANZ und WIRTSCHAFT

LE TEMPS

Investing.com

Neue Zürcher Zeitung

swissquote.com/crypto-assets/education