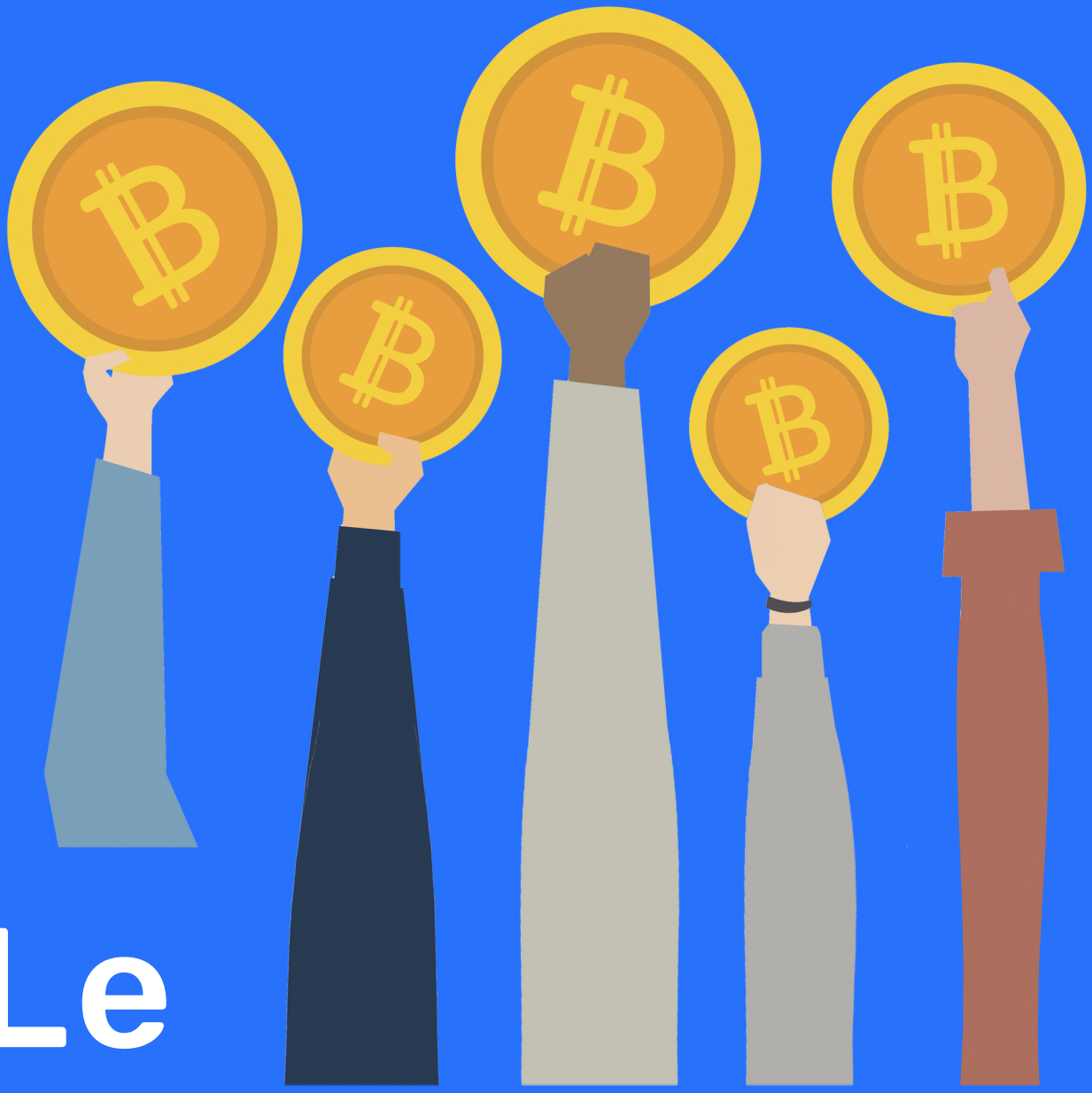
INVESTO.help



Le Criptovalute

Un’introduzione a cura di Investo.help

I - Le Basi

Le Cryptovalute

Una breve introduzione da parte di INVESTO.help

Le CryptoValute Cosa Sono?

Questa breve guida introduttiva spiega le basi per approcciarsi al mondo delle Cryptovalute. Ci teniamo a precisare che questa breve introduzione è, appunto, un'introduzione e che non è e non sarà mai un manuale per investire in cryptovalute, quanto piuttosto una spiegazione a grandi linee con parole comprensibili riguardante il mondo della blockchain e la grande rivoluzione che sta portando e per poter far nascere nel lettore la voglia necessaria di continuare ad informarsi per conto proprio.
In questo mondo lo studio è fondamentale: se non avete la possibilità per mancanza di voglia, tempo libero, energie e quant'altro, potete affidarvi a società che offrono servizi di assistenza.
Queste società sostanzialmente raggruppano per voi le informazioni che vengono estratte in ore e ore di studio e le forniscono in pillole, facendo risparmiare una gran quantità di tempo a poco prezzo.

"Guardare le cryptovalute e non interessarsi alla blockchain è come guardare Google e ignorare internet"

Durante i primi 10 anni dalla nascita di internet soltanto in pochi hanno avuto l'ardore di comprare un computer in modo tale da estrarne il potenziale e basta vedere i creatori delle 10 società più quotate al mondo. Troverete i nomi di Bill Gates, Elon Musk, Mark Zuckenberg, Jeff Bezos (fondatori di grandi società).
Tutti loro, prima di altri, avevano intuito le potenzialità di internet e seppur con molto anticipo hanno investito tutto nei loro progetti ed Il mondo funziona da sempre così. Al nascere di una rivoluzione, pochi se ne accorgono, e quei pochi sono quelli che introdurranno la rivoluzione al resto del mondo.
La blockchain esiste, pochi ad oggi la stanno studiando ma costituisce una rivoluzione come quella della nascita di Internet.

Cos'è Il WEB e a cosa serve

Il Web

Il World Wide Web nasce nel 1991 da Tim Berners-Lee. Nella breve vita del web, possiamo già distinguere almeno 3 epoche:

Il Web 1.0

Uno strumento di difficile accesso a molti, dove le interfacce erano utilizzabili da soggetti che potevano maneggiare codici di programmazione e che era caratterizzato da un'architettura statica o in gergo "read-only". Aprendo il pc, ci si trovava di fronte ad un'interfaccia con possibilità limitate che nella maggior parte dei casi portavano ad aprire quello che viene chiamato un terminale di comando. Verso la fine della prima epoca appaiono i browser ossia

un flusso di utilizzo si potrebbe rappresentare come segue ossia;
Ricerca--> Consultazione--> Soluzione/Risposta.

Il Web 2.0.

In questo caso ci troviamo di fronte ad uno strumento dinamico, che non solo vuole essere letto, ma vuole che tu, poi, esprima la tua opinione a riguardo.
In questa epoca le interconnessioni e le raccolte di dati sono la matrice del cambiamento caratterizzata dalla nascita di molte aziende come Facebook, Instagram, Snapchat, Twitter ecc che non solo chiedono agli utenti di utilizzare il proprio prodotto, ma danno ampi spazi per esprimere dei pareri e avviare dei dibattiti.
In questo senso il paradigma non è più “read only” ma potremmo definirlo “read and write” trasformando il flusso di utilizzo nel seguente modo;

Ricerca--> Consultazione--> Informazione--> Dibattito/Opinione Personale.

Il Web 3.0

Con il Web3.0 nascono nuovi sistemi di crittografia uniti a sistemi di archiviazione che permettono di costruire sistemi distribuiti che per definizione vengono identificati come sicuri e inviolabili. Questi sistemi prendono il nome di “Blockchain”, dall’inglese, Catena di Blocchi. Ed è proprio qui che il flusso cambia totalmente e non rappresenta piu un qualcosa di specifico ma attraverso il Web3.0 e la Blockchain si apre una nuova era che è quella della DECENTRALIZZAZIONE.

Sistemi decentralizzati

Con il termine blockchain intendiamo una struttura ad architettura decentralizzata, in quanto la sua struttura è dislocata in una moltitudine di entità separate all’interno della quale cessano di esistere tutti gli intermediari che coinvolgono un flusso che viene attivato da due soggetti, un mittente e un ricevente.
Essenzialmente la struttura del web2.0 ha portato, in molti ambiti, ad un eccesso di centralizzazione di questi sistemi. Prendiamo come esempio il trattamento dei dati. Attualmente, la maggior parte di questi dati personali sono nelle mani di tre o quattro aziende (Google, Facebook, Amazon). Questa situazione si configura come un eccesso di centralizzazione e ciò si ripercuote in molti ambiti, dalle assicurazioni, alla finanza, alla pubblica amministrazione, alle identità digitali.
Il primo caso di sistemi decentralizzati potremmo identificarlo in quelli che vengono chiamati “database distribuiti”, ovvero dei database che non sono detenuti da un soggetto/ubicazione unico ma da una moltitudine di essi, e che, tramite il loro utilizzo, forniscono elementi utili allo scambio di una determinata quantità di informazioni.
Da un punto di vista di conservazione delle informazioni questi godono di una sicurezza in quanto, grazie alla loro dislocazione fisica in punti diversi, sono meno soggetti a fenomeni straordinari. Pensiamo ad esempio al caso di OVH, nota Data Center la quale, a causa di un incendio, ha subito la perdita di 2/3 dei database e conseguentemente dei dati conservati dai

propri clienti a causa appunto di un eccesso di centralizzazione. Questo grado di sicurezza cosi alto di cui godono i sistemi decentralizzati, non lo troviamo se si guarda a pericoli di altra natura, come gli attacchi informatici da parte di soggetti che non sempre hanno buone intenzioni. Ciò potrebbe dar vita ad una falsificazione o cancellazione delle informazioni stesse.
A questo punto, quindi, possiamo prendere i concetti dei sistemi decentralizzati e, unendoli a quelli della crittografia, possiamo cominciare a scrivere delle transazioni tra due soggetti all'interno di quello che viene definito "ledger" o registro delle transazioni, elaborate da un'architettura di calcolo distribuita (come detto sopra) ma con logica centralizzata, vale a dire che ciò che viene scritto deve essere validato da altri soggetti i quali, in maniera omogenea, verificano la correttezza delle operazioni al fine di garantire che il registro non venga riscritto o alterato in qualsiasi maniera. Ciò da origine ad una catena di informazioni continuamente in fase di scrittura, che nell'ambito della blockchain viene divisa in blocchi: da qui il suo nome "catena di blocchi".

Il Consenso Distribuito

Il consenso è un'azione tale per cui uno o più soggetti si mettono d'accordo per dare il loro parere riguardo una particolare questione.
Nell'ambito della blockchain si parla di Consenso Distribuito che spiegheremo tramite un esempio:

Immaginiamo che ci siano 6 persone ad un tavolo, e che stiano giocando ad un gioco nel quale ognuno di essi deve scegliere un numero, e il seguente ripetere tutti i numeri precedenti prima di aggiungere il suo e passare il foglio, gli altri possono annotarsi fino a quel punto dove erano arrivati.
(Si noti che i numeri in nero rappresentano il primo giro, e i numeri in rosso il secondo giro)
Avremo una situazione del genere al primo giro.
Il primo giocatore sceglie il numero 6. Il secondo sceglierà il 9, quindi scriverà 69, il terzo 694, il quarto 6943, il quinto 69437, il sesto 694379 scegliendo ogni volta il numero che vogliono preceduto da tutti quelli nominati prima.
A questo punto il primo, al secondo giro (in rosso) potrà reinserire un altro numero solo dopo aver riscritto la sequenza. Al contempo, tutti gli altri, controllano la corretta prosecuzione della catena. Ognuno di loro adesso quindi potrà, senza intermediari, scrivere il proprio numero senza alcuna possibilità di modificare la sequenza in quanto, qualora non corrisponda a quella che posseggono gli altri, non verrebbe validata dagli stessi.
In questo caso, siamo di fronte ad un consenso distribuito dal momento che tutti, simultaneamente sono in grado di verificare che la sequenza sia corretta. Se dovesse esserci una manomissione della sequenza tutti sarebbero nella condizione di potersi accorgere dell'errore. All'interno della blockchain con la parola consenso si fa spesso riferimento all'algoritmo alla base del funzionamento della blockchain stessa.

POW

Nel tempo si è assistito alla nascita di una moltitudine di algoritmi di consenso differenti, tra cui abbiamo uno dei primi che è POW o “proof of work”, dall’inglese, prova del lavoro. Esso richiede la soluzione di complicatissimi calcoli da parte dei miners affinché le transazioni vengano validate. Questo lavoro viene remunerato con la cryptovaluta di riferimento della blockchain. Si evince che ci sono dei soggetti che vengono remunerati per la risoluzione dei calcoli necessari ad elaborare le transazioni e quindi potremmo dire che la blockchain non è una cryptovaluta, ma le cryptovalute sono la blockchain e con questo potremmo dire per quanto le cryptovalute siano una minima applicazione delle potenzialità di questa tecnologia, esse sono necessarie ai fini della sua esistenza.
L’algoritmo POW viene utilizzato dalle principali blockchain come Bitcoin o Ethereum e viene riconosciuto per la sua sicurezza e, al contempo, criticato per le enormi quantità di energia che richiede.
Una maggior attenzione però ora richiede un nuovo algoritmo che sta progressivamente migliorando le sue prestazione e viene definito POS.

POS

Un secondo algoritmo di consenso che si è imposto nel panorama di questa tecnologia è chiamato proof of stake (POS). Esso prevede la validazione di un certo numero di operazioni da parte di quelli che vengono definiti validator, che equivalgono ai miner del POW, scelti casualmente sulla base della quantità di cryptovaluta che bloccano in qualità di “impegno” all’interno della blockchain. La quantità di moneta bloccata viene definita “stake”. La probabilità di essere scelti per l’esecuzione di un lavoro è direttamente proporzionale alla quota di moneta detenuta sul totale in staking.
A questo protocollo viene riconosciuto il pregio dell’efficienza in quanto non sono necessari i calcoli del pow e di conseguenza non prevede l’utilizzo di hardware e, quindi, il consumo di energia che causa e ad oggi esistono una moltitudine di algoritmi differenti tra i quali il proof of history, proof of coverage, proof of identity. Tutti, a loro modo, danno una visione del funzionamento di un ecosistema distribuito e decentralizzato, che mira ad essere il più sicuro possibile e, al contempo, scalabile senza uno spreco a livello energitico come viene attuato da altre crypto.

Scalabilità

Scalabilità si intende la capacità di una blockchain di elaborare un numero crescente di transazioni senza incorrere in malfunzionamenti o congestioni della rete. A questa caratteristica viene dato un valore che vuole appunto misurare la capacità di elaborare più transazioni simultaneamente, chiamato TPS, transazioni per secondo.
Questo valore misura la quantità di transazioni che una blockchain è in grado di effettuare in un secondo di tempo.

Il trilemma della blockchain.

Il trilemma afferma che le tre caratteristiche della blockchain risiedono in: decentralizzazione, scalabilità, sicurezza.
Ogni protocollo, che sia POW o POS, mira ad ottenere il miglior risultato ma, secondo il trilemma, non riesce ancora a garantire lo stesso grado di performance in tutti questi tre aspetti. Infatti sostiene che una blockchain non può coprire tutti e tre questi punti e che nel suo funzionamento deve sacrificare in parte uno dei tre aspetti a favore degli altri due.
Una forte decentralizzazione aumenta la sicurezza della blockchain ma, a causa della moltitudine di soggetti che devono validare le operazioni, rinuncia a una parte (non necessariamente rilevante) di scalabilità. Al momento in cui questa guida viene scritta, ci sono alcuni progetti - come Algorand o Kadena - che affermano di aver superato il trilemma potendo garantire il massimo dei tre aspetti. A questo rimandiamo per uno studio più approfondito.

Bitcoin

Acronimo (BTC)

Nel 2008, un informatico dal nome Satoshi Nakamoto, pubblica uno studio: Bitcoin, A peer to peer electronic cash system.

All'interno di questo elaborato viene descritto un network che combina un numero molto grande di macchine, ognuna delle quali segue una serie di semplici regole matematiche. Questo studio sarà poi alla base della nascita della prima blockchain chiamata Bitcoin.
Chi sia Satoshi Nakamoto, ad oggi non è dato saperlo. Si sentono parecchie teorie. Gli antagonisti della blockchain sostengono sia uno pseudonimo utilizzato dalle banche per arricchirsi. Altri sostengono che lo studio sia stato finanziato dalle organizzazioni criminali per poter riciclare del denaro visto il trend che vede sempre di più il contante in disuso. I "romantici", per cosi dire, della blockchain sostengono sia stata creata da un gruppo di hacker all'indomani della crisi dei mutui subprime del 2007 che, scoppiando in America, ha invaso oltre mezzo mondo. A difesa di questa teoria c'è ciò che viene definito "Easter Egg". Gli Easter Egg potremmo definirli come degli indizi nascosti appositamente da autori, sceneggiatori, scrittori, che nel caso di bitcoin, si cela nella prima transazione mai avvenuta di Bitcoin, definita blocco genesi. Il blocco è stato minato il 3 gennaio 2009 e recita: "il cancelliere sull'orlo del secondo salvataggio delle banche". Su queste frasi ci sono ampi dibattiti sulla sua natura critica del sistema bancario mondiale, come se costituisse la goccia che fa traboccare il vaso della pazienza delle persone nei confronti delle decisioni spesso spregiudicate delle banche nei confronti dell'economia, e dei risparmi delle persone fino a toccare l'intera vita delle persone stesse.
Quindi, Satoshi Nakamoto, crea bitcoin con l'intento di creare un network peer-to-peer che permetta lo scambio di valore senza alcun istituto finanziario coinvolto.

“Una versione puramente peer-to-peer di denaro elettronico consentirebbe di inviare i pagamenti online direttamente da una entità all’altra senza passare attraverso un istituto finanziario”
-Satoshi Nakamoto-

Siamo ancora all’alba dello sviluppo e dell’utilizzo della tecnologia blockchain.
Questa può essere applicata efficacemente nella finanza, social media, tracciamento della filiera alimentare, banche, governi, vendita al dettaglio. Sono veramente infiniti i possibili utilizzi di questa tecnologia che aumenterebbe la sicurezza e la trasparenza di ogni servizio.
Quello che possiamo consigliarti, è di interfacciarti il più possibile con persone del settore, e cogliere le opportunità di apprendimento che possono sorgere da una chiamata al telefono, o un caffè al bar, o una fiera di settore. Lo scambio di informazioni, e il brainstorming sono fondamentali in un modo ancora cosi poco denso di bibliografia e di fonti ufficiali. La blockchain farà, senza alcun dubbio, parte del nostro futuro, non ti resta che smettere di dargli le spalle e cominciare a guardare nella stessa direzione.

Scansiona il codice qr
ed entra nel network di notizie
per investitori consapevoli

notizie.investo.help

il portale ufficiale di notizie e informazione
di investo.help

INVESTO.help