BLOCKCHAIN REVOLUTION ITALIAN SUMMIT

www.blockchainrevolution.it

Blue Chain

www.bluechain.it

Glossario - blockchain and new tech

BLOCKCHAIN
Significa letteralmente “catena di blocchi”. È una rete informatica di nodi che gestisce in modo univoco, immutabile e sicuro, un registro contenente dati e informazioni (per esempio transazioni) in maniera aperta, condivisa e distribuita senza la necessità di un’entità centrale di controllo e verifica. La tecnologia Blockchain, alla base di Bitcoin, Ethereum e altre piattaforme, permette la validazione dei dati concatenati e quindi la trasmissione di valore afferente a qualsiasi filiera.

BLOCCO
Tipo di struttura dati utilizzato nei registri blockchain per raggruppare le transazioni. I blocchi sono tra di loro concatenati, tramite l'inclusione dell'hash del blocco precedente.

CONSENSO
Accordo della maggioranza dei partecipanti a una rete sulla validità di una sequenza storica di transazioni.

NODO VALIDATORE
Nodo di una rete facente parte del gruppo di validatori che sono responsabili della creazione di blocchi e della trasmissione di questi blocchi alla rete. Per creare un nuovo blocco i validatori devono seguire le regole specificate dall’algoritmo di consenso.

CHIAVE PRIVATA
Informazione, utilizzata nei sistemi di crittografia asimmetrica, che consente, tra l'altro, di "firmare" un documento in modo verificabile e non ripudiabile. Nelle criptovalute è utilizzata tipicamente per disporre trasferimenti da un conto ad un altro. La custodia della chiave privata è uno degli elementi più delicati nell'utilizzo delle criptovalute.

PROOF OF WORK
Algoritmo di consenso che richiede all’utente di risolvere un problema matematico complesso per verificare una transazione. Chi risolve il problema, e dimostra in questo modo di aver compiuto un lavoro, tipicamente riceve una ricompensa.

FORK
Possibile creazione di una versione alternativa del registro, in conseguenza di una modifica del protocollo base della rete. Le due catene possono poi progredire entrambe viluppando registri divergenti.

DISTRIBUTED LEDGER
Tecnologie in cui tutti i nodi di una rete possiedono la medesima copia di un database che può essere letto e modificato in modo indipendente dai singoli nodi. Le modifiche al registro vengono regolate tramite algoritmi di consenso che permettono di raggiungere il consenso tra le varie versioni del registro, nonostante esse vengano aggiornate in maniera indipendente dai partecipanti della rete.

CRITTOGRAFIA
Branca della matematica che definisce metodi e algoritmi per nascondere le informazioni e renderle accessibili solo in presenza di certe condizioni (per esempio, conoscenza di una certa chiave). La crittografia è ampiamente utilizzata all'interno delle piattaforme blockchain.

PEER-TO-PEER
è un’architettura di calcolo distribuito, ovvero una struttura informatica nella quale più computer singoli interagiscono fra loro. I nodi (ovvero ciascun dispositivo che riesca a comunicare con gli altri facenti parte di una stessa rete) si dicono “equivalenti”, perché sono contemporaneamente sia server e che client, hanno pari livello gerarchico e si coordinano senza necessità di entità centrali.

MINING
Processo mediante il quale le transazioni di bitcoin vengono verificate, raggruppate in blocchi, validate e aggiunte alla Blockchain. Questo avviene attraverso la risoluzione di problemi di crittografia che richiedono una spesa di tempo ed energia, ricompensata tramite fee ed emissione di nuovo valore.

HASHING - HASH
Risultato di una funzione che trasforma i dati in una stringa Hash, di lunghezza fissa unidirezionale, dal quale è impossibile risalire ai dati di input. Può essere visto come la versione elettronica di un'impronta digitale, per qualsiasi tipo di dati.

PROOF OF STAKE
Algoritmo di consenso in cui le evoluzioni del registro non sono validate con sforzo computazionale, ma in cui gli utenti garantiscono la validità delle transazioni mettendo at stake, ossia impegnando, una quota delle proprie criptovalute. Così i validatori sono incentivati a comportarsi onestamente per non perdere quanto impegnato.

INTERNET OF VALUE
Rete digitale di nodi che si trasferiscono valore attraverso un sistema di algoritmi e regole crittografiche. Tale rete permette di aggiungere il consenso, anche in assenza di fiducia, sulle modifiche da apportare a un registro distribuito che tiene traccia dei trasferimenti di asset digitali univoci.

DECENTRALIZZAZIONE
Trasferimento di autorità e responsabilità da un'organizzazione centralizzata a una rete distribuita.

ALGORITMO DI CONSENSO
Protocollo con cui viene raggiunto l'accordo tra i nodi di una rete su una singola versione di un registro distribuito. Questi algoritmi permettono ai partecipanti della rete di concordare sul contenuto del registro, anche in presenza di un certo numero di attori malintenzionati o di un guasto alla rete.

NODO
Computer sulla rete che gestisce una copia del registro blockchain.

CHIAVE PUBBLICA
Può essere utilizzata da chiunque per crittografare una transazione, che potrà essere decifrata solo tramite la conoscenza della chiave privata corrispondente. Nelle criptovalute-la chiave pubblica viene tipicamente utilizzata per identificare un conto, a cui sono associati degli asset, controllabili tramite la conoscenza della corrispondente chiave privata.

QUALI ELEMENTI COMPONGONO UN BLOCCO:
- Index, il numero assoluto del blocco, ovvero la sua posizione all’interno della catena
- Timestamp, l’orario in cui il blocco viene generato
- Previous HASH, cioè l’HASH del blocco precedente
- Tutte le informazioni legate al valore trasportato dal blocco
- HASH del blocco stesso, cioè il suo codice identificativo, che dipende da tutti i dati precedentemente descritti
- NONCE è il numero che, aggiunto agli altri dati, genera un hash con un determinato numero di zeri che serve per chiudere e validare il blocco. Il lavoro dei Miners è la ricerca del Nonce.

SMART CONTRACT
Insieme di istruzioni espresse in linguaggio informatico e visibili a tutti, che vengono eseguite automaticamente da una rete Blockchain al verificarsi di predeterminati eventi. Una volta attivato lo smart contract, la sua esecuzione è garantita e non arrestabile. In alcune piattaforme uno smart contract è anche in grado di ricevere e inviare transazioni.

IoT
Con Internet of Things (IoT) ci si riferisce al processo di connessione a Internet di oggetti fisici di utilizzo quotidiano, dagli oggetti più familiari usati in casa, come le lampadine, alle risorse in ambito sanitario, come i dispositivi medici, ai dispositivi indossabili, a quelli smart e, per finire, alle smart city.

AI
L'intelligenza artificiale è un insieme di tecnologie differenti che interagiscono per consentire alle macchine di percepire, comprendere, agire e apprendere con livelli di intelligenza simili a quelli umani.

TOKEN
Particolare tipologia di asset digitale che può essere scambiata su una blockchain. I token sono spesso utilizzati come rappresentazioni di altri beni digitali o fisici o di un diritto, come la proprietà di un asset o l'accesso a un servizio.

METAVERSO
è un'espansione virtuale del mondo reale dove viviamo e interagiamo attraverso un avatar, anche tramite alcuni dispositivi tecnologici indossabili. Il Metaverso, nel prossimo decennio, rivoluzionerà quasi tutti gli aspetti della vita e del business, abilitando la collaborazione in spazi virtuali, luoghi fisici aumentati e una combinazione di entrambi. Inoltre, creerà nuove linee di business e trasformerà le interazioni tra clienti e aziende.

CYBER SECURITY
è la prassi di proteggere i sistemi, le reti e i programmi dagli attacchi digitali.
La sicurezza informatica, nota anche come sicurezza digitale, è la pratica volta a proteggere le informazioni digitali, i dispositivi e le risorse personali. Compresi le informazioni personali, gli account, i file, le fotografie, e persino il denaro.

CLOUD
Letteralmente "nuvola informatica", termine con cui ci si riferisce alla tecnologia che permette di elaborare e archiviare dati in rete. In altre parole, attraverso internet il cloud consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla workstation locale.

BIG DATA
Pensiamo un attimo al nostro quotidiano, interazioni sui social network, un click su un sito web, i nostri smartphone interconnessi, tutto ciò genera un flusso di dati incredibilmente elevato. Enormi volumi di vari dati analizzabili in tempo reale: tutto questo sono i Big Data. Una raccolta di dati informativi così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza.

ROBOTICA
La robotica è la disciplina dell'ingegneria che studia e sviluppa metodi che permettano a un robot di eseguire dei compiti specifici riproducendo in modo automatico il lavoro e il comportamento umano.

NFT (Non-Fungible Token)
sono dei "certificati digitali" coniati in una unica tiratura o tiratura limitata, basati sulla tecnologia blockchain, volti a identificare in modo univoco, insostituibile e non replicabile la proprietà di un prodotto digitale.

ON CHAIN
Espressione che qualifica le transazioni blockchain tradizionali, validate dalla rete e registrate in un blocco sulla rete principale.

OFF CHAIN
Espressione che si riferisce alle transazioni che non vengono registrate sulla blockchain, ma vengono validate separatamente. In genere si utilizzano questi sistemi per aumentare la velocità o la privacy delle transazioni.

SIDE CHAIN
Nuova Blockchain che è legata ad un'altra, di riferimento, tramite un collegamento bidirezionale che consente l'interscambiabilità di asset tra le due reti. La blockchain originale viene solitamente chiamata "main chain".

MINERS
Durante la creazione di un blocco, il miner calcola un codice che identificherà il blocco all'interno della blockchain. Questo codice identificativo deve rispettare dei criteri di complessità ed è molto difficile da calcolare; questa sorta di puzzle è chiamat proof-of-work.

CRIPTOVALUTA
Moneta digitale decentralizzata che utilizza tecniche crittografiche e sistemi di allineamento degli incentivi per garantire la sicurezza degli scambi tra gli utenti. A differenza delle valute tradizionali, non esistono enti centrali che intermediano le transazioni e le regole con cui avvengono gli scambi sono scritte in un software open-source pubblicamente verificabile.

PORTAFOGLIO/WALLET
Sistema di custodia delle chiavi private a cui sono collegate criptovalute e che può comunicare con la rispettiva blockchain. Il portafoglio può essere online, offline o su un dispositivo fisico

STABLECOIN
Asset digitali che godono delle garanzie e delle proprietà tipiche delle criptovalute, ma il cui prezzo è stabilizzato rispetto ad un asset di riferimento che può essere una moneta fiat, come il dollaro o l'euro, un bene come l'oro, oppure un indice di prezzi.

BITCOIN
Prima criptovaluta che utilizza la tecnologia Blockchain, Bitepin, nato nel 2008, è stato implementato e lanciato nel 2009 da una persona o un gruppo di persone che si identificano sotto lo pseudonimo di SatoshiNakamoto.

ETHEREUM
Piattaforma, basata sulla tecnologia blockchain, che consente la scrittura di smart contract e la creazione di applicazioni distribuite non censurabili (DApp). Il token nativo di questa blockchain è chiamato ether e viene utilizzato sia per svolgere operazioni computazionali all'interno della rete sia per scambiare valore tramite transazioni.

ZERO KNOWLEDGE PROOF
Famiglia di tecniche che consentono di dimostrare la sussistenza di alcune condizioni (per esempio la disponibilità di fondi sufficienti a compiere una transazione) senza svelare nessun'altra informazione. Questo consente, per esempio, di garantire l'integrità e la correttezza delle transazioni economiche, senza rivelare informazioni come mittente, destinatario, e importo.

DOUBLE SPENDING
Situazione nella quale un utente cerca di spendere la stessa moneta digitale più volte, ad esempio inviando lo stesso pagamento a due destinatari differenti.

DAPP
Applicazione decentralizzata, simile alle app tradizionali, che si appoggia sulle piattaforme blockchain e sul loro network distribuito, per ottenere garanzie di non censurabilità.

GOVERNANCE
Insieme di regole e procedure che disciplinano la gestione di una piattaforma blockchain e le modalità con cui si possono proporre ed eventualmente apportare modifiche al suo funzionamento.

ICO
Acronimo di Initial Coin Offering, rappresentano l'azione di generare e vendere agli investitori interessati un nuovo token, con l'obiettivo di finanziare lo sviluppo di un particolare progetto.

ORACOLO
Soggetto il cui scopo è registrare, all'interno della blockchain, informazione proveniente dal mondo "reale" che sia di interesse per il funzionamento degli smart contract. Le informazioni possono anche essere fornite in associazione a una prova crittografica che ne garantisca la provenienza.

INDIRIZZO
Informazione, spesso rappresentata in forma di stringa alfanumerica e associata ad una chiave pubblica, utilizzata per identificare un'entita che può ricevere e trasmettere asset su un network blockchain.

OPEN SOURCE
Software, il cui codice è accessibile e modificabile dagli utenti.