Il Glossario dell'Osservatorio Blockchain & Distributed Ledger

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.

BITCOIN
Prima criptovaluta che utilizza la tecnologia Blockchain. Bitcoin, 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 Satoshi Nakamoto.

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.

BLOCKCHAIN
Tecnologia alla base di Bitcoin, Ethereum e altre piattaforme, in cui il registro distribuito è strutturato come una catena di blocchi contenenti transazioni.

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.

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.

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

CORDA
Piattaforma Distributed Ledger open source, creata nel 2016 dal consorzio bancario R3 per essere utilizzata dalle istituzioni finanziarie.

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.

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.

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

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

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.

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.

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.

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 sviluppando registri divergenti.

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.

HASH
Risultato di una funzione che trasforma i dati in un unico digest di lunghezza fissa 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.

HYPERLEDGER
Progetto avviato dalla Fondazione Linux per supportare la creazione di Blockchain permissioned e favorire lo sviluppo collaborativo di Distributed Ledger open source.

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.

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

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

LIGHTNING NETWORK E PLASMA
Protocolli cosiddetti di secondo livello utilizzati per rendere più veloci le transazioni e risolvere il problema della scalabilità. Funzionano tramite canali one-to-one tra i nodi, che vengono aggiornati al di fuori della Blockchain e sulla quale vengono registrati occasionalmente.

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.

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.

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

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.

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

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

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.

PEER-TO-PEER
Architettura di rete informatica in cui i nodi hanno pari livello gerarchico e si coordinano, sulla base di qualche protocollo, senza necessità di entità centrali.

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.

PREDICTION MARKET
Mercato creato con lo scopo di fornire previsioni su eventi futuri. Questi mercati si basano sulle previsioni degli utenti, che speculando su accadimenti futuri scommettono su un risultato di un determinato evento. In base alle quote delle scommesse è poi possibile identificare quale evento è più probabile secondo la totalità degli utenti.

PROOF OF CONCEPT
Realizzazione di una prova o un prototipo di un determinato progetto, allo scopo di verificarne la fattibilità.

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.

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.

PROTOCOLLO
Insieme di regole che determinano il modo in cui i dati vengono scambiati e trasmessi.

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".

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.

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.

STEALTH ADDRESS
Nella criptovaluta Monero, indirizzi che impediscono qualsiasi possibile associazione tra una transazione e il suo destinatario, nascondendone così l'identità.

TANGLE
Particolare tipologia di registro basato su grafici aciclici diretti (DAG). La principale innovazione del Tangle è che le transazioni vengono processate in parallelo, il che permette di raggiungere una maggiore scalabilità e di ridurre i costi e i tempi di validazione.

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.

TURING COMPLETEZZA
Caratteristica di un linguaggio di programmazione che ne indica il massimo grado di espressività possibile, ovvero la capacità di descrivere ogni logica accessibile con qualsiasi altro linguaggio di programmazione.

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.