Glossario bitcoin e blockchain (raccolta di vocaboli meno comuni in quanto limitati a un ambiente o propri di una determinata disciplina, accompagnati ognuno dalla spiegazione del significato o da altre osservazioni).

INDICE:

Altcoin: è il termine generico per indicare le valute digitali, di cui esiste un mercato e che sono possibili scambiare nei siti di Exchange.

ASIC (e Miner ASIC): è l'acronimo di Application Specific Integrated Circuit, che è un circuito di silicio che esegue soltanto una funzione. Nel mondo delle valute digitali, questi circuiti eseguono l'algoritmo SHA-256 al fine di minare Bitcoin e validare le transazioni. Un Miner ASIC è l'hardware che alloggia circuiti ASIC. Essi si avvalgono della tua connessione Internet via modem o wireless mode, indipendentemente dai Bitcoin del tuo computer desktop.

Bit: il bit è un'unità comune utilizzata per indicare una sotto-unità del bitcoin – 1,000,000 di bit equivalgono a 1 bitcoin (BTC o ฿). Questa unità è solitamente più appropriata per dare un valore o un prezzo a beni e servizi.

Bitcoin: letteralmente "moneta di bit". Definita "anche "valuta digitale", moneta elettronica", "criptovaluta". La definizione più completa è, a nostro avviso, "moneta digitale peer to peer". Bitcoin, con la B maiuscola, è usata quando si descrive il concetto di Bitcoin, o l'intero network stesso, per esempio "dobbiamo approfondire lo studio del protocollo di Bitcoin", mentre bitcoin con la b minuscola è usata per descrivere i bitcoin come un'unità di conto, per esempio "vorrei pagare in pizzeria con i miei bitcoin, chissà se li accettano". Spesso è abbreviato in BTC o XBT.

Block (blocco): un blocco è una registrazione di alcune o di tutte le più recenti transazioni che non sono ancora state registrate in alcuno dei blocchi precedenti, una parte della blockchain che contiene le informazioni relative alle transazioni avvenute successivamente al blocco precedente. Ogni blocco, in pratica, contiene tutte le transazioni da confermare e il numero di blocco che lo precede. La lunghezza della catena dei blocchi è un'informazione pubblica. Il tempo medio di creazione di ciascun blocco è di circa 10 minuti ed ogni nuovo blocco include delle transazioni, venendo poi aggiunto alla blockchain attraverso il processo di mining.

Blockchain: (catena di blocchi) è un registro pubblico e condiviso di tutte le transazioni bitcoin in ordine cronologico. L'ordine cronologico e la non modificabilità dei blocchi della blockchain rendono impraticabile il double spending, la doppia spesa, essendo la blockchain condivisa tra tutti gli utenti Bitcoin e utilizzata per verificare la permanenza delle transazioni. Nel mondo delle valute digitali è anche intesa come un termine che si riferisce alla totalità dei blocchi per cui i miner hanno trovato l'hash, a partire dalla nascita della valuta digitale in questione.

Block reward: Il termine si riferisce al reward, compenso, che i Miner ricevono quando trovano l'hash per un blocco di transazioni.

BTC: (o XBT) è l'abbreviazione esatta usata in ambito finanziario per bitcoin, in maniera simile a cui EUR lo è per Euro. Il simbolo ฿ è il suo corrispettivo, come lo sono € per Euro e $ per Dollaro ed e unità comune della moneta.

Chiave privata: una chiave privata (privat key) è una parte di dati segreti che provano che sei tu ad utilizzare bitcoin da un determinato portafoglio attraverso una firma crittografata. La tua chiave privata (o chiavi private) è conservata nel tuo computer se utilizzi un portafoglio software; è invece conservata in un server remoto se utilizzi un portafoglio web. La chiave privata non deve essere rivelata ad altri in

quanto permette di utilizzare i fondi dal portafoglio bitcoin con chiave pubblica corrispondente.

Chiave pubblica (public key): è una sorta di "parola d'ordine" condivisibile con chiunque, sotto forma di sequenza di caratteri alfanumerici (lettere dell'alfabeto e numeri arabi). Per fare un'analogia bancaria potremmo definirla l'IBAN che accoppiata alla chiave privata (privat key o, sempre per usare un'analogia bancaria, il PIN segreto) viene usata per spendere i bitcoin. La creazione di un nuovo indirizzo genera un nuovo paio di chiavi, pubblica e privata, che vengono aggiunte al portafoglio (il nostro conto principale). Si possono possedere più coppie di chiavi, anche una per ogni transazione effettuata.

Conferma: indica che una transazione è stata processata e verificata dalla rete ed è praticamente impossibile che sia respinta. Normalmente basta una conferma ma perché la transazione passi allo stato definitivo di "confermata" sono necessarie 6 conferme (quando una transazione viene ammessa per la prima volta in un blocco, riceve una conferma. Ogni volta che quel blocco viene ammesso in blocchi successivi, riceve un'altra conferma. Dopo sei conferme, il client Bitcoin cambia stato ad una transazione portandola da "non confermata" a "confermata"). Il processo di conferma avviene attraverso il mining. Anche una singola conferma può essere considerata sicura per le transazioni di basso valore, sebbene per cifre maggiori come ad esempio 1.000 euro è consigliabile attendere le 6 conferme o più. Ogni conferma diminuisce esponenzialmente il rischio di una transazione respinta.

Crittografia: è la scienza che si occupa di proteggere delle informazioni rendendole incomprensibili a chi le dovesse intercettare, in modo che possano essere lette e capite solo dal destinatario, una branca della matematica che ci consente di creare prove matematiche per fornire elevati livelli di sicurezza. Il commercio e le operazioni bancarie online impiegano già la crittografia. Nel caso di Bitcoin la crittografia è impiegata per rendere impossibile a chiunque di spendere del denaro dal portafoglio di un altro utente o alterare la blockchain. Può essere anche utilizzata per criptare un portafoglio, in modo che non possa essere usato senza una password.

Cryptovaluta: altro termine generico usato per descrivere una valuta che è puramente basata sulla matematica come lo sono bitcoin, litecoin, zcash etc.

Difficulty: nel contesto Bitcoin, questa parola è usata per descrivere la difficoltà che un utente o una pool (gruppo di miners) deve fronteggiare quando vuole cercare l'hash di un nuovo blocco per la blockchain del Bitcoin.

Double Spend: se un utente malintenzionato prova a spendere i propri bitcoin verso due diversi indirizzi riceventi contemporaneamente, si tratta di doppia spesa. Il mining di Bitcoin e la blockchain esistono per creare un consenso sulla rete, per decidere quale delle due transazioni sia considerata valida ed abbattere il rischio di doppia spesa. Il double spending è comunque impedito dal processo messo in essere attraverso il mining e la blockchain: ogni transazione aggiunta alla blockchain assicura che la moneta non sia stata già spesa in precedenza.

ECDSA: abbreviazione per Elliptic Curve Digital Signature Algorithm, che è l'algoritmo leggero che il software Bitcoin utilizza per firmare le transazioni nel protocollo.

Exchange: un Exchange è un sito o un luogo dove i titolari di un account possono scambiare un valuta digitale per un'altra, o una valuta Fiat con una digitale e viceversa. TheRockTrading è un exchange italiano con base a Malta.

Fee o Transaction Fee: le transazioni che avvengono all'interno dei blocchi sono soggette ad un costo di transazione, chiamato transaction fee, generalmente davvero irrisorio, pagato ai miners che riescono a minare il blocco di cui farà parte la transazione stessa.

Firma: la crittografia asimmetrica consente l'uso della firma digitale in quanto il mittente di un messaggio può firmarlo attraverso la sua chiave privata e tutti sono in grado di verificare l'autenticità della firma grazie alla chiave pubblica. Nel caso di Bitcoin, un portafoglio Bitcoin e la sua/sue chiave privata/e sono collegati per mezzo di un vincolo matematico. Quando il tuo software Bitcoin firma una transazione con la chiave privata appropriata, l'intera rete può vedere che la firma combacia con i bitcoin spesi. E non c'è alcun modo per chiunque al mondo di indovinare la tua chiave privata per derubarti dei tuoi bitcoin.

Genesis block: il blocco Genesis è il primo in assoluto ad entrare nella blockchain di qualunque valuta digitale.

Hash: è il termine matematico per un algoritmo che prende un insieme di dati di qualsiasi lunghezza e composizione e li converte in un tipo di dato di lunghezza e composizione fissa.

Hash Rate: per hash rate si intende l'unità di misura della potenza di elaborazione della rete Bitcoin. Per fini di sicurezza la rete Bitcoin deve eseguire delle operazioni matematiche intensive, quindi questo termine riferito al bitcoin definisce la quantità di hash che un particolare miner può svolgere in un dato periodo di tempo. La funzione crittografica di hash è di trasformare un insieme di dati (o un messaggio) in una stringa alfanumerica di dimensioni fissa chiamata valore di hash.

Indice Bitcoin: è un indice di media pesata che mostra i controvalori di un bitcoin rispetto alla singola unità di valuta per ciascuna delle maggiori nel mondo del mercato valutario: EUR (euro); USD (dollaro USA); JPY (yen giapponese); GBP (sterlina inglese); AUD (dollaro australiano).

Indirizzo Bitcoin: è equivalente ad un indirizzo fisico o ad un indirizzo e-mail, la sola informazione che devi fornire a qualcuno affinché possa inviarti dei bitcoin. Una differenza importante con l'email è che, comunque, con bitcoin ogni indirizzo dovrebbe essere utilizzato unicamente per una singola transazione, per mantenere protetto l'anonimato. Ciascun utente della rete Bitcoin possiede un portafoglio contenente coppie di chiavi crittografiche. Gli indirizzi sono una sequenza alfanumerica (lettere e numeri, come ad esempio 1Fuu8QXDuXBLoFmWUG3WzWavQCkH2EpEL3) e ciascun utente può generarne a sua discrezione (la creazione non richiede contatto con i nodi della rete), anche una per transazione.

Megahashes/sec: questo termine si riferisce alla quantità di tentativi di hashing possibili per una data unità di elaborazione, durante un periodo di tempo; normalmente un secondo.

Mining: per mining si intende il processo che fa eseguire all'hardware del computer calcoli matematici al fine di creare nuovi bitcoin e di confermare le transazioni per aumentare la sicurezza della rete bitcoin. I miners (minatori) in sostanza, anziché estrarre oro da una miniera, "estraggono" algoritmi utilizzando hardware dei loro computer ed elettricità. Come ricompensa per il loro servizio, i di bitcoin possono incassare delle commissioni sulle transazioni che confermano, insieme ai nuovi bitcoin appena creati.

Mining pool: è un insieme di miners che si uniscono in squadra per generare Bitcoin in modo collettivo. La maggior potenza di calcolo richiesta suggerisce di unire le potenze computazionali per essere più competitivi, anche a causa del maggior numero di minatori attivi e dalla ricompensa in bitcoin dimezzata, passata da 50 a 25, da 25 a 12,5 a blocco per soddisfare la regola dell'halving o dimezzamento della reward.

Output: quando una transazione ha luogo, l'output si riferisce all'indirizzo di destinazione usato nella transazione.

P2P: per peer to peer (abbreviato in P2P) si intendono i sistemi che funzionano come un collettivo organizzato permettendo ad ogni individuo di interagire direttamente con gli altri. Nel caso di Bitcoin, la rete è costruita in modo che ogni utente trasmetta le transazioni degli altri utenti. E, fatto di importanza cruciale, nessun entità terza come banche o Stati devono essere coinvolti nell'operazione.

Paper Wallet: letteralmente portafoglio cartaceo, è una forma di cold storage, per migliorare la sicurezza. Il termine si riferisce a semplici fogli di carta che contengono la stampa di un indirizzo pubblico di un portafoglio e le corrispondenti chiavi private in forma alfanumerica o di QRcode.

Payment Processor: aziende che offrono un software che implementa un sistema di pagamento con il quale si permette ad un commerciante, on line e off line come un ristorante o un qualsiasi negozio o azienda, di accettare bitcoin come pagamento per i suoi beni e servizi. Società italiane sono Tinkl.it e Inbitcoin, dite che vi mandiamo noi del BitcoinVenetoTeam;-)

Portafoglio o wallett: l'equivalente di un portafoglio materiale ma sul network di Bitcoin che contiene le chiavi private e pubbliche legate ad un preciso indirizzo. Per la precisione il tuo portafoglio contiene le chiavi private che ti permettono di usare i bitcoin allocati nella blockchain. Ogni portafoglio Bitcoin può mostrarti il bilancio totale di tutti i bitcoin che controlla e ti permette di inviare bitcoin o frazioni di bitcoin ad un altro indirizzo bitcoin. Questo processo non richiede il pagamento di commissioni ad enti come banche o gestori della carta di credito, ma solo di una piccola fee ai miner.

Proof of work o PoW: per Proof of Work, prova di lavoro, si intende ogni output o quantità di dati, prodotta da ogni tentativo per trovare un hash minando bitcoin. Nella blockchain l'hashing di un blocco richiede tempo e lavoro e questi sforzi si traducono in dati difficili da produrre ma facili per gli altri da verificare. Le prove di lavoro sono

generalmente utilizzate all'interno delle pool per ridistribuire equamente il reward dei blocchi minati.

Regole del bitcoin: La criptovaluta non viene emessa da una banca centrale. Per crearla, c'è bisogno di una operazione detta mining, "estrazione". Come i minatori in cerca d'oro, i miners scavano tra i blocchi alla ricerca di nuove monete. Non si usano picconi e setacci ma computer e capacità di calcolo. La pepita è un codice capace di sigillare un blocco e allungare la catena (Blockchain) che in sé racchiude il database di tutte le operazioni in bitcoin concluse fino a quel momento. Per ricompensare chi, per primo, ha rintracciato il codice-pepita e consentito di allungare la catena, il sistema assegna una ricompensa, mettendo così in circolazione nuova moneta. Quando, nel 2008, Satoshi Nakamoto definì le regole della criptovaluta introdusse alcuni limiti.

I. i bitcoin non potranno essere più di 21 milioni.
II. il sistema si adatta in modo tale da generare, in media, un blocco ogni 10 minuti.
III. Nakamoto (chiunque sia) ha previsto un dimezzamento della ricompensa (detto halving) ogni 4 anni.

In sostanza, la generazione dei Bitcoin rallenta in modo geometrico. Ecco perché, se dal 2008 al 2016 è stato prodotto il 75% dei bitcoin, bisognerà aspettare il 2040 per toccare, praticamente, il 100%. Il protocollo prevede il dimezzamento per evitare che l'inflazione rosicchi il valore della criptovaluta dato che, se stampo moneta all'infinito, il rischio è che diventi carta straccia.

Satoshi: è l'unità più piccola di bitcoin (8 decimali, 1 centomilionesimo di bitcoin)

SHA-256: ogni moneta digitale deve avere implementata una forma di crittografia che indichi la funzione utilizzata per creare un hash. Nel Bitcoin la funzione utilizzata come base per la creazione degli hash è SHA-256, come accade ad esempio nelle prove di lavoro PoW.

Transazione: consiste nel trasferimento di valuta tra due indirizzi bitcoin usando la crittografia a chiave pubblica. Tutte le transazioni sono pubbliche, memorizzate e una volta confermate sono irreversibili.

Valute FIAT: la denominazione si riferisce alle valute tradizionali basate sulla stampa su carta o su scrittura in database informatici, regolate da un'organizzazione come una Banca Centrale. Esempi ne sono l'Euro, il dollaro USA etc.

Ora che hai imparato le parole base del mondo bitcoin, **Contattaci** per sapere dove terremo il prossimo corso!

Bitcoin Veneto Center Team

Mobile: +39 340 5035130 - E-mail: center@bitcoinveneto.it

Telegram: @BTCVeneto - Skype: bitcoinveneto