**Glossario**

**Altcoin:** una valuta digitale alternativa a Bitcoin. Molte altcoin nascono come fork di bitcoin con qualche cambiamento rispetto alla versione standard (ad esempio Litecoin).

**Asic:** acronimo di “Application Specific Integrated Circuit”, sono dei circuiti progettati per eseguire un unico compito (ad esempio, generare numeri casuali per un algoritmo di cifratura in particolare).

**Attacco 51%:** un attacco su blockchain in cui un agente controlla più del 50% del consenso della rete. Il consenso può tradursi in potenza di calcolo in caso di blockchain proof-of-work, valuta per la proof-of-stake, etc.

**Bitcoin:** la cryptovaluta più conosciuta, il gold standard delle crypto, creata nel 2009 da Satoshi Nakamoto. Utilizza una blockchain proof-of-work ed è la valuta con più miner.

**Blockchain:** una ledger distribuita, composta da pacchetti di transazioni immutabili detti blocchi. I blocchi rappresentano lo storico delle transazioni nella rete, e ognuno di essi è agganciato al blocco precedente tramite una firma digitale cifrata.

**Crypto/Cryptovaluta:** una forma di valuta digitale protetta, generata, e distribuita attraverso tecniche crittografiche varie.

**Decentralizzazione:** il trasferimento dell’autorità da un’organizzazione o ente centralizzato ad un network distribuito in cui l’autorità è divisa tra I vari nodi.

**Difficoltà:** un indice della potenza di calcolo necessaria, in hash, per vincere un blocco

**Fork:** una versione alternativa di una blockchain

**Gpu:** acronimo di “graphics processing unit”. Le gpu sono volgarmente delle schede video che, per ragioni di architettura, si prestano a minare alcune cryptovalute meglio di altri tipi di hardware.

**Hash:** una funzione che converte un input di numeri e lettere in un output criptato di lunghezza finita. Nel caso del mining, l’output di una funzione hash è l’elemento che serve per validare un blocco.

**Hashrate:** il numero di funzioni hash eseguite da un hardware, per un algoritmo specifico, in un determinato intervallo di tempo

**Ledger:** un registro in cui le informazioni possono essere solamente aggiunte, mentre I record precedenti restano immutati. Generalmente usato per immagazzinare transazione, può contenere anche informazioni di altro tipo.

**Market Cap:** il valore totale del mercato di una determinata cryptovaluta

**Miner:** l’entità singola che effettua il mining. Utilizzato sia per indicare il possessore delle macchine, sia la macchina stessa singolarmente

**Mining:** il processo attraverso il quale le transazioni vengono validate in una blockchain proof of work. Il mining prevede l’utilizzo di potenza di calcolo per risolvere problemi crittografici, validare blocchi, e attraverso la validazione generare nuova valuta.

**Proof of stake:** un sistema di consenso alternativo alla proof of work in cui la risorsa utilizzata per gestire il consenso è la valuta stessa.

**Proof of work:** un algoritmo di consenso in cui la risorsa utilizzata per gestire il consenso della rete è la potenza di calcolo impiegabile dai miner.

**SHA 256:** la funzione criptografica alla base della proof-of-work della blockchain bitcoin

**Whitepaper:** un documento in cuivengono definite le specifiche tecniche di una cryptovaluta.