LA RIVOLUZIONE Blockchain

CONSULCESI TECH

UNA TECNOLOGIA DESTINATA A CAMBIARE LE NOSTRE VITE

CHE COS'È UNA BLOCKCHAIN

La Blockchain è un registro. Ogni unità del registro è un "blocco", e i blocchi sono collegati tra loro nell'ordine in cui sono stati creati. Le Blockchain servono per due cose: registrare degli eventi, e assicurarsi che quella registrazione non venga mai cancellata. Uno dei motivi per cui è così difficile modificare i blocchi è che una blockchain vive attraverso una rete diffusa di computer, che devono approvare tutti i cambiamenti che avvengono.

Siccome non c'è un server centrale da manomettere o attaccare, gli hacker non possono semplicemente prendere il controllo di un singolo computer ed effettuare delle modifiche. Di conseguenza, i partecipanti possono fidarsi dei dati contenuti in una Blockchain senza doversi conoscere o fidarsi l'un l'altro e senza dover fare affidamento su un'autorità centrale.

.

L'IMPATTO SUL SISTEMA FINANZIARIO

Anche se c'è già chi ipotizza che le criptovalute in futuro possano addirittura sostituire il denaro contante, ad oggi, però, la vera rivoluzione è rappresentata dalla Blockchain, destinata ad avere sul sistema finanziario (e non solo) un impatto paragonabile a quello dei social network sulle relazioni interpersonali. La Banca d'Italia, che segue il fenomeno da almeno un paio d'anni con un tavolo dedicato, spiega che «l'insieme delle regole informatiche (protocollo) genera la reciproca fiducia dei partecipanti nei dati conservati ed è potenzialmente in grado di sostituire quella assicurata da 'pubblici registri' gestiti in maniera accentrata da un'autorità riconosciuta dal quadro regolamentare».

LE APPLICAZIONI ALLA NOSTRA QUOTIDIANITÀ

L'innovazione tecnologica su base Blockchain avrà enormi ripercussioni positive sui più disparati aspetti del nostro vivere quotidiano: attraverso l'uso degli Smart Contracts (brevi programmi auto-eseguibili su richiesta) sarà possibile eliminare tutte quelle intermediazioni e/o intermediari che ancora oggi sono imprescindibili per molte questioni amministrativo-economiche. Per fare un esempio concreto, non sarà più necessario che un atto sia certificato da una figura terza preposta allo scopo: ogni contratto verrà semplicemente validato attraverso una struttura matematica che ne certificherà l'origine e la validità in maniera certa, efficiente e soprattutto incorruttibile. Il tutto con enormi risparmi in termini economici, temporali e di controversie giudiziarie.
Ad oggi, i settori che possono godere di significativi benefici grazie all'applicazione della tecnologia Blockchain sono i più disparati, solo per citarne qualcuno:

- Le assicurazioni, che potranno ottimizzare i processi di negoziazione e la quotazione dei rischi corporate;
- La logistica e i trasporti, con aumento della trasparenza ed efficienza tra vettori, broker, consumatori, venditori e altre parti della supply chain;
- La filiera alimentare, che disporrà di nuovi strumenti in grado di garantire la migliore tracciabilità alimentare nella prospettiva di assicurare nuovi livelli di sicurezza alimentare e food safety.

UNA SEMPLIFICAZIONE ESTENSIBILE ALLA SANITÀ

Nel settore sanitario, la Blockchain potrebbe rivelarsi incredibilmente utile nella gestione e archiviazione dei più disparati documenti di carattere medico. Cartelle cliniche, fatture, risultati di ricerca e test hanno, infatti, saturato i professionisti del settore e i sistemi da loro usati. Per questo motivo molti professionisti stanno seriamente valutando la possibilità di applicare tali principi, soprattutto nell'ambito della tracciabilità dei farmaci, trial clinici, ricerca genomica e molto altro. Uno dei suoi possibili utilizzi potrebbe essere anche quello di verificare l'identità digitale del paziente, tenere traccia della cronologia delle prescrizioni mediche, delle somministrazioni di farmaci e della relativa assunzione delle terapie. Un ulteriore uso potrebbe riguardare, inoltre, la corretta applicazione dei protocolli terapeutici e dei dispositivi medici (tramite appositi device certificati).

UNA TECNOLOGIA DESTINATA A CAMBIARE LE NOSTRE VITE

LE NEW COIN

ALL'ORIGINE DEL CAMBIAMENTO

I Bitcoin nascono nel 2007 con l'avvio del progetto Open Source Bitcoin ad opera dell'ancora anonimo Satoshi Nakamoto. L'idea era quella di creare una valuta indipendente che non fosse controllata da nessuna autorità statale, che fosse trasferibile elettronicamente in tutto il mondo in modo istantaneo e con commissioni sulle transazioni estremamente basse.

IL PRIMATO DEI BITCOIN

Ad oggi sono in circolazione oltre mille monete digitali e tra queste i Bitcoin sono la più popolare per numero di transazioni, valore raggiunto e anche per un fattore storico. Per uscire dalla confusione che circonda il Bitcoin, abbiamo bisogno di separare il concetto di Bitcoin in due componenti. Da un lato, si colloca il Bitcoin inteso come token, un frammento di codice che rappresenta la proprietà di un valore digitale utilizzabile come "moneta di scambio" in transazioni tra soggetti diversi. Dall'altra parte, si colloca il Bitcoin inteso come Protocollo, una rete distribuita che mantiene un registro dei saldi di Bitcoin-the-token. Entrambi sono indicati come "Bitcoin". A differenza delle valute tradizionali, il sistema consente di inviare i pagamenti tra utenti senza passare attraverso un'autorità centrale, ad esempio una banca o un gateway di pagamento. Inoltre i Bitcoin, a differenza di dollari o euro, non sono stampati, ma sono prodotti attraverso un processo matematico da computer in tutto il mondo. Questo permette di avere un sistema di valuta che si basa su una certezza scientifica e che non subisce decisioni "centralizzate" né costi di intermediazione.

LE MONETE DIGITALI OGGI IN CIRCOLAZIONE

Litecoin, Ripple, Bitcoin Cash, Monero concettualmente hanno la stessa applicazione dei Bitcoin e vanno dunque intesi essenzialmente come strumenti di pagamento o come riserva di valore. Le cosiddette nuove "altcoins" (cioè alternative al Bitcoin) nell'ultimo triennio stanno letteralmente spopolando, soprattutto dopo l'avvento della seconda criptovaluta per capitalizzazione mondiale e cioè Ether (coin dell'asset Ethereum). Ethereum ha una connotazione più tecnologica e non a caso è la preferita dagli sviluppatori di tutto il mondo. C'è anche una differenza da non sottovalutare per la quantità disponibile: la riserva di Ethereum è illimitata mentre per Bitcoin il limite è di 21 milioni, 17 dei quali sono stati già "minati".

LA SICUREZZA DI UN PORTAFOGLIO ELETTRONICO

Mentre in tutto il mondo proliferano veri e propri bancomat dove acquistare i Bitcoin (ovviamente in cambio dei contanti si ottiene un accredito su un portafoglio elettronico), in Italia il sistema più utilizzato è quello della registrazione su portali web denominati Exchange (tra i più noti Bitstamp, Kraken, The Rock Trading, Coinbase) che permettono di acquistare Bitcoin o altre cryptocurrency attraverso carte di credito o associando un conto corrente. Il consiglio, una volta acquistati, è di trasferirli su un apposito "portafoglio" che può essere un'App per smartphone, un paper wallet o, meglio ancora, un device ad hoc come il Ledger Wallet.

UN ALTRO APPROCCIO ALLE TRANSAZIONI

Numerosi negozi (ora anche in Italia), siti di e-commerce e prestatori di servizi accettano pagamenti in Bitcoin e/o altre criptovalute. Tra le iniziative lanciate si va dallo skypass a St. Moritz alla possibilità, concessa da Consulcesi ai suoi clienti, di pagare in e-coin le azioni collettive. Inoltre, è possibile anche convertire la moneta virtuale nelle valute tradizionali.

UN INVESTIMENTO SUL NOSTRO FUTURO

UN BENE PIÙ PREZIOSO DELL'ORO

Come nel caso dell'oro si tratta di un bene rifugio e limitato. L'elemento tecnologico, in particolare il rigore matematico della certezza del proprio valore e l'impossibilità di contraffazione, pone i Bitcoin in una posizione privilegiata per chi cerca di proteggere i propri risparmi/capitali dalla fisiologica erosione dovuta a inflazione, crisi economica globale e perdita di appeal da parte dell'attuale valuta di riferimento mondiale, il dollaro americano. Quindi, seppure il Bitcoin non possa essere paragonato all'oro dal punto di vista fisico, in brevissimo tempo (circa 8 anni) è comunque diventato oggetto di enorme interesse da parte del mercato finanziario e, grazie alla sua assoluta garanzia matematica, probabilmente raggiungerà la medesima se non superiore maturità dell'oro in termini di adozione e fiducia da parte della popolazione mondiale.

FONDI REGOLAMENTATI E TRANSAZIONI PIÙ SICURE

Capitolo determinante l'opportunità di acquistare criptovalute anche attraverso la sottoscrizione di fondi (ne stanno nascendo di regolati in Europa). A differenza degli exchange, i fondi regolamentati sono maggiormente adatti alla tutela del sottoscrittore, essendo autorizzati e quindi sorvegliati da diverse autorità nazionali come MFSA, CSSF, Consob ecc. Questa loro caratteristica permette di aumentare il livello di professionalità, sicurezza e trasparenza attualmente lacunosi nel mercato delle criptovalute. Ne è esempio la frequenza con la quale i mezzi di informazione riportano notizie di exchange finiti sotto inchiesta. Un fondo d'investimento, oltretutto, è in grado di abbattere i costi di transazione per un singolo investitore (attualmente il costo dei vari exchange è altissimo), ma soprattutto gli permette di ridurre i rischi di hackeraggio.

Infatti, i fondi d'investimento per poter essere regolati devono garantire a se stessi ed ai propri sottoscrittori protocolli di sicurezza molto avanzati, come ad esempio protocolli di cold storage mediante controparti anch'esse regolate. I fondi regolamentati rappresentano la pietra angolare anche per ridurre gli adempimenti fiscali a carico degli investitori (il recente caso italiano sui dubbi relativi alla dichiarazione dei redditi ne è uno dei tanti esempi), consentendo agli Stati di tassare il settore in modo corretto e automatico, secondo norme riconosciute a livello internazionale, e di operare un controllo mirato ed efficace. Senza dimenticare anche che operare attraverso strumenti regolati è una garanzia di rispetto delle normative antiriciclaggio.

UN INVESTIMENTO A LUNGO TERMINE

Dalla loro nascita, i Bitcoin hanno continuato a crescere di interesse, attraversando fisiologici momenti di deprezzamento più o meno marcati, ma aumentando incessantemente di controvalore con la valuta tradizionale e di capitalizzazione totale. Considerato che la loro capitalizzazione ad oggi risulta ancora veramente modesta e pari circa alla metà rispetto a quella di Apple (la società più capitalizzata al mondo attualmente), è plausibile un ulteriore innalzamento verticale del valore nel medio/lungo termine.

LA DIFFERENZIAZIONE DEL PORTAFOGLIO

La crescita esponenziale di Bitcoin si è portata dietro anche quella di molte altre criptovalute e soprattutto di Ripple, che oggi vale complessivamente 126 miliardi di dollari. Meno di Bitcoin, che ne vale più del doppio, ma più di Ethereum, a lungo citata come principale alternativa.

Facendo una rapida stima, solo nel 2017 Ripple XRP (la valuta del sistema Ripple) è cresciuta del 30.000%. Ripple nasce da una società di San Francisco, che ha raccolto diverse decine di milioni di investimenti anche dalle banche come il Santander, e ciò gli ha già fatto guadagnare il titolo di "Bitcoin che piace alle banche". È quindi importante seguire l'andamento delle cosiddette nuove "altcoins" (cioè alternative al Bitcoin) al fine di diversificare i propri investimenti. In particolare, grazie allo sviluppo di Ethereum, sono venute alla luce migliaia di Initial Coin Offering (ICO) e cioè aste di prefinanziamento in criptomoneta per permettere a team di sviluppo di portare a termine propri progetti di innovazione tecnologica su base Blockchain in merito alle più disparate utilità del vivere comune.

DAL RISCHIO BOLLA ALLA PRESA D'ATTO DEL CAMBIAMENTO

A fine 2017 i Bitcoin hanno fatto registrare un calo del 40% in pochi giorni dopo un guadagno del 180% nelle settimane precedenti e di oltre il 1.500% nel corso dello stesso anno. Episodi simili si erano già registrati nel 2011 e nel 2014 e puntualmente il Bitcoin ha ripreso la sua ascesa: come è risaputo le bolle una volta esplose non ritornano più. Molto più logico pensare che il calo sia dovuto alla capitalizzazione degli investitori che hanno recuperato liquidità sui guadagni. La legittimazione delle criptovalute è inoltre dettata dai lori possessori: ad aprile 2017 erano tra i 6 e i 10 milioni, oggi fra i 20 e i 40 milioni. Bisogna comprendere la portata rivoluzionaria che riguarda soprattutto gli aspetti tecnologici più che quelli economici, sebbene a beneficiarne sarà anche il mercato finanziario globale, eliminando tutte le tossicità. Persino l'avvento della televisione e di internet era stato osteggiato e visto con diffidenza: va preso atto di un cambiamento.

REGOLAMENTAZIONE E LEGISLAZIONE

I 50 PAESI CHE HANNO GIÀ RICONOSCIUTO LE CRIPTOVALUTE

Di fronte all'espansione del mercato delle criptovalute non tutti i Paesi stanno reagendo allo stesso modo a livello legislativo. Un gruppo di Stati, 50 in tutto, ha deciso di dotarsi di sistemi di controllo per seguire passo dopo passo il modo in cui le criptovalute andranno a convivere (o collidere) con i sistemi valutari tradizionali. In questi Paesi le valute digitali sono state ufficialmente riconosciute come un sistema valido per effettuare pagamenti o altri tipi di attività finanziarie. Il gruppo comprende Stati Uniti, Unione Europea, Australia, Messico, Canada, Argentina, Venezuela, Sudafrica, Arabia Saudita, India, Iran, Regno Unito, Islanda, Bielorussia, Hong Kong, Taiwan, Georgia, Israele, Kenya, Malesia, Nuova Zelanda, Norvegia, Senegal, Singapore, Tunisia, Turchia, Filippine, Svizzera, Corea del Sud e Giappone. Altri, invece, hanno vietato l'uso delle valute digitali e le operazioni finanziarie a esse collegate: è il caso di Bolivia, Ecuador, Vietnam, Kirghizistan, Libano, Marocco e Namibia.

VERSO UNA REGOLAMENTAZIONE COMUNE A LIVELLO INTERNAZIONALE

Sulla necessità di una regolamentazione comune, che tuteli chi vuole investire in criptovalute e nella tecnologia Blockchain, i pareri sono unanimi. A gennaio 2018, l'ex ministro dell'Economia Padoan ha dichiarato: «La Blockchain è una tecnologia e un conto è la tecnologia, un conto è l'uso che se ne fa. La tecnologia da sola non crea bolle. Tutto questo sistema dovrà essere regolato». Lo stesso mese, la Commissione europea, insieme all'Europarlamento, ha deciso di lanciare un Osservatorio e un Forum ad hoc con l'obiettivo di identificarne "rischi ed opportunità". «Voglio che l'Europa sia all'avanguardia nel suo sviluppo», ha dichiarato la commissaria al digitale Mariya Gabriel, puntando a creare «un mercato digitale unico per la Blockchain invece di un mosaico di iniziative». Anche il Fondo monetario internazionale sostiene che «la cooperazione tra regolatori sarebbe utile» in tema di criptovalute.

IL QUADRO DI RIFERIMENTO IN ITALIA

Ad oggi non esiste ancora una normativa fiscale specifica che regoli la detenzione e la compravendita di Bitcoin o di altre criptovalute. In attesa che il Governo, o le istituzioni Europee, decidano in merito, l'unico riferimento ufficiale per l'Italia rimane la Risoluzione numero 72/E dell'Agenzia delle Entrate del settembre 2016, secondo cui le operazioni in Bitcoin effettuate da persone fisiche sono assimilabili a operazioni di acquisti e vendite di valuta. Pertanto, come chiarito in una recente risposta ad un interpello, sono due i quadri a cui fare riferimento: quello RW e quello RT. Nel primo va indicato il valore delle somme in Bitcoin possedute al 31 dicembre 2017, nel secondo le plusvalenze sulle quali va pagata l'imposta. Per quanto attiene al quadro RW, l'importo posseduto alla fine del 2017 va indicato solo se il controvalore è superiore ai 15 mila euro, perché questa è la soglia prevista per le valute estere e solo se i Bitcoin sono tenuti su una piattaforma online all'estero. Per quanto riguarda le plusvalenze, queste sono imposte con una aliquota pari al 26%, soltanto nel caso in cui le criptovalute possedute abbiano superato il controvalore di 51.645,69 euro per almeno sette giorni lavorativi.

LO SVILUPPO DELLA CYBERSECURITY

UN GRANDE LIBRO CONTABILE

Il funzionamento è quello di un grande libro contabile, chiamato Blockchain: qui tutte le transazioni confermate sono comprese sotto forma di blocchi. Una volta a sistema, la transazione entra in un network di computer peer-to-peer degli utenti per ricevere la conferma. Tutti gli utenti prendono dunque consapevolezza di ogni operazione e ciò impedisce furti e di spendere più volte la moneta.

LA TRACCIABILITÀ CONTRO GLI SCOPI ILLECITI

Sostenere che i Bitcoin e le criptovalute siano il regno dell'illegalità e che i criminali li utilizzino per scopi illeciti è assolutamente falso poiché la stragrande maggioranza delle attività illegali vengono svolte attraverso l'utilizzo delle monete attualmente circolanti (dollaro, euro, yen, ecc.). In realtà il Bitcoin e le altre criptovalute, ad eccezione di alcuni rarissimi casi, sono quanto di più tracciabile e certificato possa esistere poiché ogni transazione viene impressa in maniera indelebile sulla Blockchain, ovvero sul registro mastro che è pubblicamente consultabile da chiunque. Di fatto, è lo strumento più trasparente che esista oggi a livello di transazioni mondiali.

UN SISTEMA TRANSAZIONALE DI MASSIMA SICUREZZA

Già diverse startup, anche in Italia, sono attive nello sviluppo di sistemi di security basati proprio sulla Blockchain, crittografando e certificando le informazioni, migliorando la gestione dell'identità digitale e garantendo così agli utenti un livello di sicurezza altissimo. In questo scenario, il settore finanziario è protagonista assoluto, come dimostra la moltiplicazione delle alleanze e dei consorzi internazionali che mettono insieme gli sviluppatori tecnologici e i player del settore. Ad attrarre è soprattutto la garanzia di maggiore efficienza, rapidità e trasparenza della Blockchain.

LE ICO A SUPPORTO DI SFIDE IMPORTANTI

LE ICO COME INITIAL COIN OFFERING

Nel mondo della finanza si parla di IPO, l'Offerta Pubblica Iniziale (dall'inglese: Initial Public Offering) con cui un'azienda vende azioni proprie per raccogliere capitali. Nel mondo delle criptovalute esiste invece uno strumento non dissimile, chiamato ICO (Initial Coin Offering), con cui un'azienda offre al mercato degli asset (token), con il medesimo scopo di reperire capitali. L'ICO è saldamente legato alle aziende attive nel mondo delle criptovalute che, solo nei primi 200 giorni del 2017, hanno raccolto 1,27 miliardi di dollari.

TRA TRADING, STARTUP, FUNDRAISING E CHARITY

Le ICO riguardano strettamente solo il trading di criptovalute? Assolutamente no: ormai anche startup e colossi della tecnologia sono interessati alle Initial Coin Offering. Per quanto riguarda le startup e i potenziali investitori, l'ICO semplifica la partecipazione al fundraising, permette anche a piccoli investitori di contribuire e soprattutto fornisce un asset liquido che consente in qualsiasi momento di liquidare o meno la propria partecipazione. Non solo nuove realtà, ma anche i big player dell'hi-tech puntano sulle ICO: per citare i casi più eclatanti, Telegram, l'app di messaggistica, ha raccolto dai fondi d'investimento richieste per 3,8 miliardi di dollari nel quadro della sua ICO e Kodak, dopo essere quasi fallita con l'avvento digitale, ha creato KodakCoin pensata per essere utilizzata da fotografi e agenzie marketing come mezzo di pagamento sicuro e immediato per vendere i propri scatti, facendo registrare un vero e proprio boom in Borsa. Anche la beneficenza si fa tramite ICO: CharityStars, la piattaforma che permette di raccogliere online denaro per iniziative benefiche mettendo all'asta appuntamenti con personaggi famosi o beni di loro proprietà, ha lanciato AidCoin, detta anche "la criptovaluta della beneficenza", raggiungendo in meno di due ore l'obiettivo di 6.000 Ethereum, oltre 6,5 milioni di euro, che si era prefissato con la sua ICO avviata e chiusa a tempo di record con l'adesione di oltre 1.500 sostenitori.

GLOSSARIO

Altcoin • Valute digitali il cui mercato non ha una gran capitalizzazione o non sono riconosciute al pari delle incombenti criptovalute quali Bitcoin, Litecoin, Dashcoin e Dogecoin.
ASIC • Acronimo di Application Specific Integrated Circuit, ovvero 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.
Bit • Unità comune utilizzata per designare un singolo sottosistema di un Bitcoin. 1.000.000 bit è equivalente a 1 Bitcoin.
BitPay • Software che implementa un sistema di pagamento con il quale si permette ad un commerciante come eBay, Amazon di accettare Bitcoin come pagamento per i suoi beni e servizi.
Blocco • Record permanente dei dati memorizzati nella Blockchain, agendo come una pagina o un registro. Ogni blocco contiene e conferma le transazioni in sospeso. Circa ogni 10 minuti, in media, un nuovo blocco (insieme alle transazioni che contiene) viene creato.
Block Genesis • Vedi Genesis Block.
Block reward • Il termine si riferisce al reward, compenso, che i Miner ricevono quando trovano l'hash per un blocco di transazioni.
Blockchain • Catena di blocchi intesa nel mondo delle valute digitali, è 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.
BTC (o XBT) • Questa è l'abbreviazione esatta usata in ambito finanziario per Bitcoin, in maniera simile a cui EUR lo è per Euro.
Criptovaluta • Questo è il termine generico usato per descrivere una valuta che è puramente basata sulla matematica come lo sono Bitcoin, Litecoin ecc.
Crittografia • Un ramo della matematica utilizzato da cryptocurrencies che utilizza prove matematiche per consentire elevati livelli di sicurezza. Nel caso di Bitcoin, la crittografia garantisce che altri non sono in grado di spendere fondi dal portafoglio di un altro utente o di corrompere la Blockchain.
Cryptocurrency • Una forma di valuta non tangibile che viene prodotta dalla soluzione matematica di problemi basata sulla crittologia.
Difficulty • Nel contesto Bitcoin, questa parola è usata per descrivere la difficoltà che un utente o un pool deve fronteggiare quando vuole cercare l'hash di un nuovo blocco per la Blockchain del Bitcoin.
ECDSA • Questa è l'abbreviazione per Elliptic Curve Digital Signature Algorithm, che è l'algoritmo leggero che il software Bitcoin utilizza per firmare le transazioni nel protocollo.
Exchange • Una piattaforma centrale per lo scambio di forme diverse di valute e beni. Tipicamente, gli scambi Bitcoin vengono utilizzati per scambiare la crittografia con le unità monetarie tradizionali.
Faucet • Quando uno sviluppatore o una squadra sviluppano, stabiliscono che una valuta digitale possa essere minata (pre-mined) in una certa quantità prima del rilascio e poi regalare queste monete pre-minate.
FIAT • Si riferisce alle valute tradizionali basate sulla stampa su carta e che è regolata da un'organizzazione come la banca centrale. Esempi comprendono l'Euro, il Dollaro Americano ed il Dollaro Australiano.
Firma • Una sequenza matematica prodotta dalla combinazione di chiavi private e pubbliche insieme, dimostrando che una transazione Bitcoin proveniva da un particolare indirizzo.
Flip • Rappresenta lo scambio di cryptocurrencies.
Fork • Modifica del protocollo di crittografia che non è compatibile all'indietro. Un fork della Blockchain si verifica quando i nodi che eseguono la nuova versione del protocollo creano una Blockchain separata incompatibile con il software più vecchio.
Genesis block • Il blocco Genesis è il primo in assoluto ad entrare nella Blockchain di qualunque valuta digitale.
Hash • Algoritmo che prende una quantità variabile di dati e la converte in una lunghezza più breve e fissa di dati.

Indice Bitcoin • 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; USD; JPY; GBP e AUD.

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.

Miner ASIC • L'hardware che alloggia circuiti ASIC. Essi si avvalgono della connessione Internet via modem o wireless mode, indipendentemente dai Bitcoin del computer desktop.

Mining • Il processo di generazione di nuovi Bitcoin attraverso il processo matematico di risolvere problemi crittografici utilizzando hardware di calcolo.

Multisig • Termine contratto per indirizzi multi-firma che consentono a più utenti di partecipare parzialmente ad un indirizzo con una chiave pubblica. La possibilità di accedere a fondi da un indirizzo di questo tipo richiede che i seguaci multipli accedano all'account. Di conseguenza, gli indirizzi multisig sono molto più resistenti al furto.

Nodo • Si riferisce a un computer completo di client che esegue una Blockchain. Serve a condividere blocchi e transazioni in tutta la rete utilizzando l'infrastruttura client-to-client.

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

P2P • Peer-to-peer si riferisce a interazioni dirette e decentralizzate di crittografia tra due parti o più. Nessuna banca o altra istituzione finanziaria è richiesta come terzo.

Paper Wallet • Alcune persone preferiscono archiviare i loro Bitcoin in un paper wallet, 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.

Private Key • Una firma crittografica che consente all'utente di accedere e spostare i Bitcoin da un portafoglio specifico.

Proof of work • Prova di lavoro, si intende ogni output, quantità di dati, prodotta da ogni tentativo per trovare un hash minando Bitcoin. Nella Blockchain l'hashing di un blocco richede 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 dei pool per redistribuire equamente il reward dei blocchi minati.

PSP • Fornitore di servizi di pagamento. I PSP fungono da agenti Bitcoin per i commercianti che accettano pagamenti online.

Public key • Chiave pubblica, è una sequenza di caratteri alfanumerici (lettere dell'alfabeto e numeri arabi) che indica l'indirizzo di un portafoglio Bitcoin. Ad ogni chiave pubblica corrisponde una chiave privata che serve per firmare digitalmente le transazioni online.

Satoshi • Il più piccolo sottosistema di un Bitcoin attualmente disponibile (0.00000001 BTC).

Satoshi Nakamoto • Lo pseudonimo utilizzato dall'inventore originale del protocollo Bitcoin.

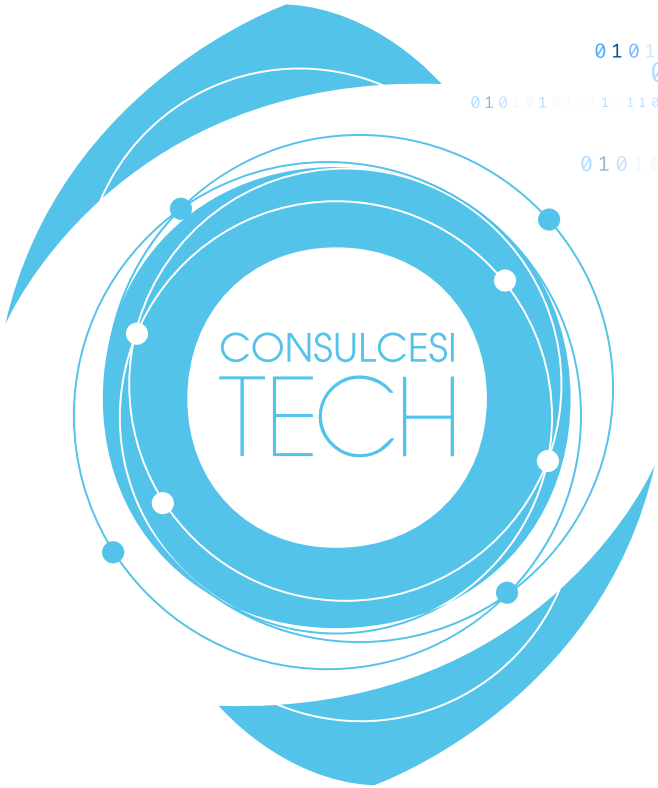
SHA-256 • Ogni moneta digitale deve avere implementata una forma di crittografia che indichi la funzione utilizzata per creare un hash. Nel Bitcoin la funzione utilizzata come base per la creazione degli hash è SHA-256, come accade ad esempio nelle prove di lavoro.

Transaction Fee • Alcune transazioni che avvengono all'interno dei blocchi sono soggette a un costo; questo costo è chiamato transaction fee. Questi costi di transazione, generalmente davvero irrisori, sono pagati ai Miner che riescono a minare il blocco di cui fanno parte.

Volatilità • La volatilità del mercato riflette la misurazione del movimento dei prezzi per un periodo di tempo per un'attività finanziaria negoziata, compreso il Bitcoin.

Wallet • Per conservare i Bitcoin e le altre monete digitali si utilizzano dei cosiddetti wallet, portafogli, che contengono le chiavi private e pubbliche legate ad un preciso indirizzo.

Wallet Paper • Vedi Paper Wallet.



Via Giuseppe Motta, 6
6828 Balerna – Svizzera

info@consulcesi.tech
www.consulcesi.tech

Consulcesi GROUP | we are different!