

Negli ultimi mesi il fenomeno delle criptomonete è esploso. Come funzionano e come sono gestite queste monete virtuali? È davvero possibile creare moneta (scambiabile poi con euro o dollari) solo utilizzando un computer? La risposta è sì, e in queste pagine vi mostriamo cosa vi serve per “coniare”.

■ Di **Davide Piumetti**

CRIPTO MONETE

FUTURA REALTÀ O BOLLA SPECULATIVA?



Una criptovaluta (chiamata spesso anche criptomoneta) è un'idea nuova nel panorama economico mondiale e si basa sul concetto dell'anonimato e della prova di scambio, oltre che avere, di norma, uno schema di emissione preconcordato. Detto così sembra estremamente complicato, ma con il giusto percorso logico le monete virtuali sono alla portata di tutti. Iniziamo con il dire che le monete di questo tipo hanno poco o nulla in comune con quelle emesse dalle banche nazionali e hanno da una parte molte garanzie di equità e parità, ma dall'altra una serie di rischi potenziali non indifferenti.



Tutte utilizzano un sistema di crittografia digitale per convalidare le transazioni tra gli utenti, in modo da rendere sicuro e a prova d'errore lo scambio di denaro, delegando agli utenti stessi la generazione e la condivisione della prova della transazione.

La prima criptovaluta sviluppata, e quella decisamente più conosciuta e famosa, è il Bitcoin. Tutte quelle alternative, di cui parleremo in dettaglio più avanti, derivano come concetto da questa, con implementazioni più o meno diverse in modo tale da giustificare l'esistenza. La maggior parte dei concetti espressi nel seguito riguardano dunque i Bitcoin, ma sono altrettanto validi anche per le altre criptovalute.

Un po' di storia

Le criptomonete nascono idealmente alla fine del 2008 da Satoshi Nakamoto che pubblicò sul sito metzdowd.com un documento chiamato *Bitcoin: A Peer-to-Peer Electronic Cash System*, sancendo la nascita dell'idea alla base dei Bitcoin e di tutte le altre criptovalute. In precedenza altri avevano proposto dei sistemi di moneta elettronica simili, ma

nessuna ha avuto il successo che invece è stato riscontrato da questa pubblicazione, arrivata probabilmente sia nel momento sia nel posto giusto.

Nakamoto in realtà è uno pseudonimo dietro al quale resta ancora aperto un mistero. A oggi non si sa ancora se si tratti di una singola persona, maschile o femminile, o di un collettivo di sviluppatori e ciò ha contribuito almeno inizialmente a ipotizzare un'imparzialità della moneta e un'estraneità voluta a tutti i poteri economici forti presenti nel mondo.

Nel tempo si è ipotizzato che dietro a Nakamoto ci fosse il Trinity College di Dublino, svariati famosi programmatori sparsi per mezzo mondo o un gruppo di persone che ha collaborato alle prime stesure dei protocolli e-cash. Una pista nel tempo molto battuta (e che per le vicende dell'ultimo periodo ha ripreso vigore) porta al fondatore di MtGox, Jed McCaleb, un americano appassionato del Giappone e lì residente da anni, tra l'altro scomparso dalla scena poche settimane fa in maniera plateale, chiudendo i battenti e portandosi via svariati milioni di dollari.

Gli ultimi contatti reali con Nakamoto

risalgono al 2011 quando lasciò la rete passando formalmente la guida (in termini di programmazione) di Bitcoin a Gavin Andersen.

Il primo Bitcoin emesso dalla rete (direttamente da Nakamoto) è datato gennaio 2009 e diede il via all'escalation di emissioni secondo uno schema concordato (come vedremo nel dettaglio in seguito) che continua tutt'oggi. Inizialmente i Bitcoin rimasero confinati ad appassionati e sviluppatori che utilizzarono la rete per scambiarsi moneta e testarne le funzionalità crittografiche. Il controvalore con valute circolanti era nullo, non essendoci ancora un mercato o un cambio prestabilito (non essendoci neppure una logica di domanda e offerta).

Come funzionano

L'idea di base consiste in una rete di comunicazione peer-to-peer dedicata, tramite la quale una serie di nodi si scambiano informazioni relative alle transazioni e allo stato delle monete. Bitcoin, così come le altre criptovalute, non si basa infatti su un ente centralizzato, ma utilizza la rete distribuita così creata per tenere traccia di tutte

BITCOIN IN CINA

«Verso la fine del 2013 il cambio Bitcoin-Yuan rappresentava bel il 21% del totale delle transazioni di cambio con la valuta cinese.»



le transazioni sfruttando la completa crittografia delle informazioni per tracciare la generazione di nuova moneta e firmare la proprietà di ciascuna moneta presente nella rete.

In parole povere ogni moneta ha una sua firma univoca e il sistema globalmente sa in quale portafoglio virtuale è inserita. Lo scambio di moneta da un portafoglio all'altro avviene tramite una transazione che si propaga nella rete distribuita in modo che, dopo un tempo prestabilito, tutti i nodi sappiano della transazione e ne legittimino così il nuovo proprietario.

I portafogli digitali sono in questo modo completamente anonimi, chiunque può installarne uno sul proprio Pc (o dispositivo mobile) e avere in questo modo un indirizzo Bitcoin dal quale inviare o ricevere moneta. Il portafoglio è un concetto duplice e serve sia come reale contenitore di monete sia come surrogato di un ente di controllo centrale. In ogni portafoglio sono contenute le tracce delle transazioni Bitcoin effettuate, in modo che nessuno possa bloccare gli scambi di moneta, sequestrarla o svalutarla intenzionalmente creandone di nuova in maniera massiccia.

Le transazioni sono definite in maniera univoca come cambio di proprietà di una determinata quantità di moneta tra due peer, senza che un ente centrale ne sovrintenda il passaggio. Uno scambio avviene tramite l'invio a tutti i nodi della rete peer-to-peer connessi all'origine delle informazioni sul trasferimento di moneta indicando quali monete sono trasferite, mittente e destinatario. I primi nodi della rete, non appena recepiscono l'informazione, inseriranno il nuovo proprietario nella lista dei possessori di quella moneta e ritrasmetteranno l'informazione. Dopo un tempo finito tutta la rete sarà a conoscenza del nuovo proprietario della moneta, se nel frattempo è stato effettuato un nuovo trasferimento di proprietà tra le monete e questa informazione arriva ai nodi di destinazione prima della precedente non c'è nessun problema in quanto ogni moneta contiene le informazioni sul suo storico e di conseguenza "vale" la catena di transazioni più lunga.

Un'altra caratteristica importante è che i Bitcoin hanno un metodo decentralizzato di creazione della valuta, in modo che nessun ente centrale ne possa controllare l'inflazione o la redistribuzione. Come la maggior parte delle criptovalute i Bitcoin hanno un numero prefissato

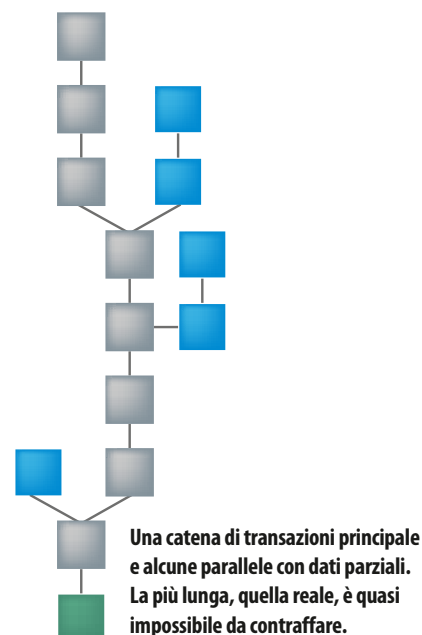
di monete che verranno emesse, il loro numero, che tende in maniera asintotica a 21 milioni, è previsto e prefissato. La rete è infatti programmata per emettere a intervalli previsti nuove monete, in modo che, grazie a una serie geometrica di durata 4 anni il loro numero cresca costantemente. A fine 2012 è stata generata la metà esatta delle monete, mentre nel 2016 arriveremo ai tre quarti (75%), di conseguenza nel 2020 i Bitcoin in circolazione saranno l'87,5% dei 21 milioni previsti. L'unità minima utilizzabile non è però l'intero Bitcoin (che risulterebbe davvero riduttivo), ma la sua ottava cifra decimale. L'unità minima trasferibile è dunque 0,00000001 Bitcoin.

Tecnica e pratica

Bitcoin utilizza il trasferimento tra conti pubblici utilizzando una crittografia a chiave anch'essa pubblica. Tutte le transazioni, come già accennato, sono di dominio pubblico e possono essere visualizzate su un database distribuito. Ogni portafoglio connesso alla rete contiene una coppia di chiavi crittografiche, una pubblica che rappresenta anche l'indirizzo Bitcoin del portafoglio e una privata che serve a autorizzare il pagamento solo al possessore della specifica moneta.

Ogni Bitcoin (o meglio la sua frazione minima) contiene la chiave pubblica del loro proprietario, sul database distribuito è quindi sufficiente interrogare ogni singola moneta per sapere a chi appartiene o interrogando un preciso indirizzo Bitcoin, sapere quante monete vi sono depositate. Nessun dato personale è richiesto o presente e tutto si svolge nel completo anonimato.

Una transazione avviene in maniera



molto semplice: l'utente proprietario rinuncia alla proprietà della moneta inserendo in coda l'indirizzo pubblico del destinatario firmandolo con la propria chiave privata. Successivamente trasmette un apposito messaggio di transazione ai nodi della rete a lui connessi, che validano firme e importi e la accettano nella catena principale, inoltrandola poi ai nodi a loro adiacenti.

I Bitcoin utilizzano sistemi di sicurezza per impedire ai proprietari di utilizzare due (o più) volte le stesse monete, prima che magari la rete sia venuta a conoscenza del passaggio virtuale di esse. Il concetto utilizzato è quello del *proof-of-work*, ovvero delle conferme delle transazioni su base temporale. In pratica ogni transazione viene inviata inizialmente in un particolare stato, ovvero quello di "non confermata" e si dirama nella rete in questo modo. Alcuni nodi della rete detti generatori, su base oraria (dipendentemente dal tipo di moneta), collezionano le transazioni non ancora confermate in un "blocco", ovvero un file contenente tutte le informazioni necessarie e, molto importante, un hash crittografico del precedente blocco valido noto al nodo.

Ogni nodo generatore, tramite un algoritmo, prova a costruire un hash valido del nuovo blocco così creato, con uno sforzo computazionale anche notevole (ma può essere aiutato, come vedremo più avanti). Quando viene trovata una soluzione, dopo un tempo che risulta casuale in base anche alla "fortuna" di trovare una soluzione dopo un numero ridotto di tentativi, il nodo comunica quando avvenuto alla rete e i restanti



Bitcoin: la moneta circolante equivale oggi a circa 8 miliardi di dollari.

Il percorso dei Bitcoin

Una transazione tra due portafogli Bitcoin è intrinsecamente sicura grazie a una serie di calcoli crittografici che permettono di identificare univocamente la transazione.

La sicurezza è resa attraverso una potenza di calcolo crittografico messa a disposizione dalla rete in cambio, ogni 10 minuti, di un premio in Bitcoin.

PORTAFOGLIO E INDIRIZZI



Bob e Alice hanno un "portafoglio" Bitcoin (un software) sul proprio Pc.



In un portafoglio può essere associato uno o più indirizzi Bitcoin.



Un indirizzo Bitcoin è una stringa di lettere e numeri. Inizia sempre con 1 e ha una lunghezza media di 31 caratteri.

CREARE UN NUOVO INDIRIZZO

Bob crea un nuovo indirizzo (tramite il portafoglio) sul quale riceve un pagamento.

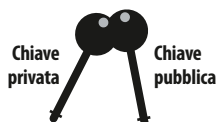


Ogni indirizzo rappresenta un singolo conto e ha il proprio ammontare in Bitcoin.

EFFETTUARE UN PAGAMENTO



Alice indica al proprio portafoglio di trasferire dei Bitcoin sull'indirizzo di Bob.



Crittografia a chiave pubblica

Quando Bob crea un nuovo indirizzo, in realtà crea una nuova coppia di chiavi crittografiche, coppia composta da una chiave pubblica e una privata. Quando Bob firma un messaggio con la sua chiave privata (che solo lui conosce) è possibile verificare se la firma è autentica utilizzando la sua chiave pubblica (che tutti conoscono). L'indirizzo Bitcoin rappresenta una chiave e la chiave privata è inserita nel portafoglio. La chiave pubblica permette dunque a tutti di verificare la firma della chiave privata di Bob.

Indirizzi L'indirizzo Bitcoin può sembrare a prima vista un indirizzo bancario, ma in realtà lavora in maniera molto diversa. Gli utenti Bitcoin possono creare quanti indirizzi vogliono e addirittura creane uno nuovo a ogni transazione effettuata. Più a lungo l'indirizzo di un utente resta sconosciuto e più la sua privacy è assicurata.

Entrano in scena i Bitcoin "miner".



VERIFICA DELLA TRANSAZIONE

I loro computer, grazie a software installabili da chiunque, raccolgono tutte le transazioni dell'ultimo blocco temporale (10 minuti per Bitcoin).

I sistemi cercano di calcolare l'hash crittografico del blocco secondo uno schema particolare.

Chiave privata

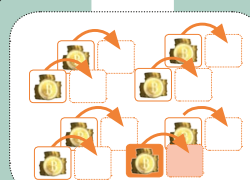


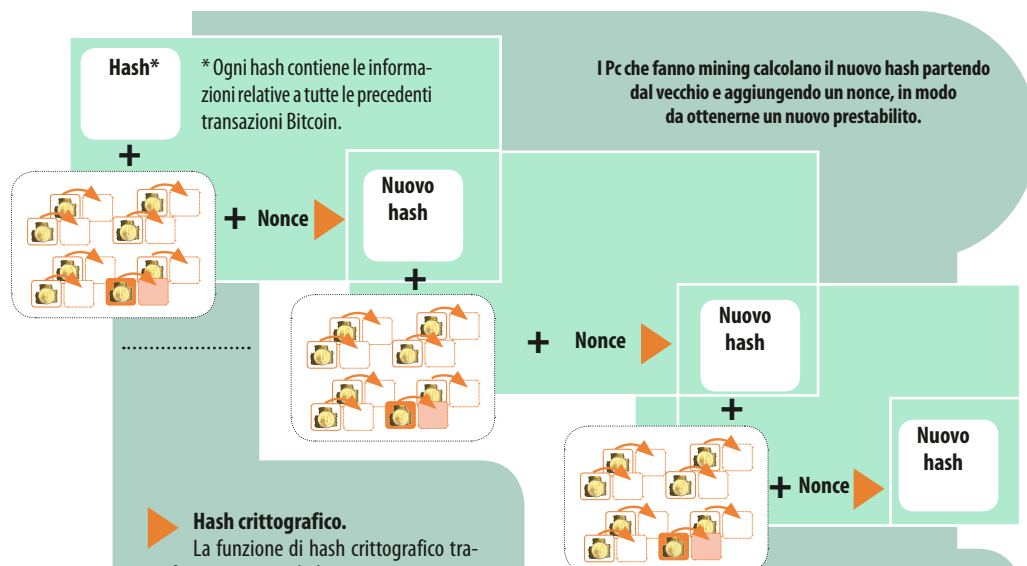
Il portafoglio di Alice contiene una chiave privata per ogni indirizzo presente. Il software firma la transazione (che indica ammontare e indirizzo di destinazione) con la chiave privata relativa all'indirizzo mittente.

Chiave pubblica



Chiunque sulla rete può verificare, usando la chiave pubblica di Alice per decifrare la transazione, che questa sia stata richiesta dal legittimo proprietario. (La chiave pubblica decifra i soli messaggi cifrati con quella privata e nessun altro).





Hash crittografico.

La funzione di hash crittografico trasforma una serie di dati in una stringa con una lunghezza fissa, chiamata hash. Cambiare anche di poco il messaggio originale può modificare drasticamente il risultato finale.

Esempio di dati	6d890asgsd809sadf
Esempio di dati	a8ds0d9vcx7sd76v6
Esempio di dati	1200as0das93312h

Nonce

I blocchi di dati contengono una piccola parte, detta nonce, che i miner generano casualmente cercando di ottenere un hash predeterminato. L'algoritmo non è diretto, ma vengono fatti dei tentativi finché non si trova un nonce adatto a ottenere un hash specificato.

Esempio di ????

0000 0000
0000 ...

Trovare un hash in questo modo è difficile a livello di calcolo in quanto non c'è un algoritmo diretto. Non si può avvicinarsi pian piano in quanto modifiche lievi del nonce portano a grandi modifiche dell'hash.



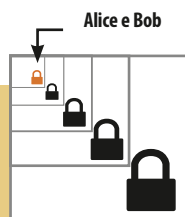
I nuovi hash richiesti da Bitcoin iniziano con un determinato numero di zeri. L'hash corretto si ha quando si trova un nonce che porta ad avere un hash minore di un valore predefinito. La difficoltà varia in base a quanto piccolo è il valore limite.

Ogni blocco contiene una transazione pre-emessa che viene firmata dal nodo che per primo trova l'hash. Questa è la ricompensa per lo specifico nodo e rappresenta lo stimolo per i miner di partecipare alla sicurezza delle transazioni.



TRANSAZIONE VERIFICATA

La transazione tra Alice e Bob inizia come non confermata e si annida nei blocchi per diverse volte. Dopo 6 conferme diviene definitiva. La difficoltà di revocare la transazione consiste nel convincere la rete della presenza di un'altra catena (con almeno 6 hash) che NON contiene la transazione. Per trovarla serve indicativamente il 51% della potenza della rete, rendendo di fatto una contraffazione di questo tipo impossibile.



nodi che ricevono il blocco lo validano prima di inserirlo a loro volta nella catena. Una transazione inserita in un nuovo blocco riceve dunque una conferma alla prima validazione e prosegue nella catena e, dopo che altri sei blocchi "figli" di quello in cui la transazione è entrata per la prima volta, ricevono conferme, la transazione passa dallo stato di "non confermata" a "confermata".

Il metodo di protezione si basa sull'idea che per poter annullare una transazione dopo la sua esecuzione l'unico modo è quello di generare una catena parallela identica ma senza la transazione in questione. Vista la potenza di calcolo necessaria alla generazione degli hash dei blocchi e la concorrenza dell'intera rete sul ramo "onesto" risulta praticamente impossibile per tutti i malintenzionati alterare la catena delle transazioni. Per creare una catena parallela tanto lunga e coerente servirebbe infatti il 51% della potenza di calcolo dell'intera rete, ragion per cui il tutto è nella pratica non realizzabile.

Una volta confermata, la catena risultante conterrà le informazioni su tutto lo storico dei pagamenti e di tutti i Bitcoin generati a partire dal creatore al proprietario ultimo. Il database risultante cresce costantemente nel tempo e, senza accorgimenti, diventerebbe in qualche tempo troppo grande e inutilizzabile. La rete ha però dei sistemi di gestione anche di questo problema, con una catena ridotta normalmente utilizzata e verificata, con la possibilità di richiamare quella completa solo quando necessario. Più avanti, nel capitolo sul mining, vedremo nel dettaglio alcuni aspetti legati a queste procedure che permettono a chiunque di generare moneta con il proprio personal computer.



Bitcoin e il successo

Il successo e la crescita di Bitcoin e criptomonete si deve probabilmente anche alla concomitanza con la crisi del debito sovrano europeo iniziata nel 2008 e non ancora del tutto conclusa.

Se il primo anno di vita è stato decisamente tranquillo (fino a fine 2009 gli scambi di valuta erano fatti a semplice scopo dimostrativo) il 2010 ha segnato l'inizio della storia Bitcoin sui mercati. La prima vera transazione è avvenuta a febbraio 2010, quando un utente acquistò due pizze per 10.000 Bitcoin (a oggi varrebbero oltre cinque milioni di euro...) e un altro utente mise all'asta altri 10.000 BTC per 50 dollari. Il mercato che venne a crearsi, con qualche piccolo investitore interessato portò il valore dei BTC a qualche millesimo di dollaro fino a giugno quando, in 5 soli giorni, il Bitcoin crebbe in valore del 1.000%. La parità con il dollaro si ebbe a marzo 2011, mentre a giugno dello stesso anno 1 BTC valeva 31 dollari, il picco della prima bolla speculativa.

Una lenta discesa e qualche piccolo movimento mantenne il Bitcoin a un valore tra 5 e 10 dollari fino alla fine dell'anno successivo.

Il 2012 si ricorda per una diffusione alle radici, con alcuni esercenti che

iniziarono a interessarsi della moneta e molti utenti che ne vennero a conoscenza pur senza entrare direttamente a far parte dei produttori o dei fruitori di essa. Qualcosa bolliva in pentola ed era pronto ad esplodere.

Il 2013 rappresentò infatti l'anno di consacrazione sul mercato della moneta, con il cambio che iniziò a salire del 5% ogni giorno fino a superare i 250 dollari nel mese di aprile. I media più specializzati iniziarono a parlarne e alcuni problemi di sicurezza vennero alla luce e furono risolti. Con idee speculative e i governi che, in più fasi, hanno cercato di ostacolare l'ascesa della moneta, il resto dell'anno ha rappresentato un'escalation quasi incredibile. Fino a ottobre la moneta restò intorno ai 150 dollari come cambio, schizzando letteralmente alle stelle nel mese di novembre quando toccò il proprio massimo storico con oltre 1.200 dollari di controvalore. Al cambio le due pizze comprate 42 mesi prima si sono rivalutate in circa 12 milioni di dollari...

I mesi successivi hanno portato la moneta, vista anche alcune complicazioni di cui ci occupiamo in un capitolo a parte, a fluttuazioni speculative importanti, con controvalori variabili tra 650 e 800 dollari. Queste variazioni non sono però solo figlie di speculazioni esterne o di



L'INDIRIZZO BITCOIN

Un indirizzo Bitcoin è composto da una sequenza casuale di numeri e cifre, con lunghezza variabile e inizia sempre per 1. La lunghezza media è di poco superiore ai 30 caratteri. Un indirizzo potrebbe essere: 1465sadASDFS456dsa654sda231aGF.



Le alternative sono molte, alcune serie e altre, come la moneta basata sull'immagine di Flappy Bird, un po' meno...



problemi di sicurezza, ma derivano anche dall'arrivo di altre, agguerritissime, monete elettroniche alternative che, visto il successo di Bitcoin, si prefiggono di portare innovazione o alternanza in un mercato ancora quasi completamente vergine.

Le alternative

I Bitcoin sono la moneta più famosa e diffusa, ma non certo l'unica presente nel settore. Essendo il software originale di tipo open source sono moltissime le monete che negli ultimi mesi hanno fatto capolino nel panorama, alcune delle quali con un discreto successo.

Il funzionamento globale è identico per tutte, con solo qualche rara eccezione in cui tutte le monete sono emesse da subito e si lavora solo sullo scambio e non sulla produzione.

Ogni moneta ha di conseguenza il proprio client e wallet, e un tasso di cambio variabile con le altre. Le differenze rispetto ai Bitcoin restano (oltre che nel successo) nel numero di monete la cui emissione è prevista, nei tempi di calcolo di blocchi e hash (in dettaglio più avanti) e nelle varie ricompense ai contributori. Molte utilizzano l'algoritmo SHA-256 per la cifratura, proprio come Bitcoin, ma la maggior parte di quelle alternative prediligono l'algoritmo scrypt, più veloce ma sulla carta altrettanto sicuro. Tra le più importanti segnaliamo i Litecoin, rappresentati anche visivamente come "seconda" moneta elettronica (argento contro l'oro dei Bitcoin), il cui valore oscilla in questo periodo tra i 10 e i 20 dollari per 1 LTC (Litecoin). Altre monete (nello specchio vi proponiamo le prime per capitalizzazione, ovvero il loro controvalore in dollari sul mercato) sono gli Auroracoin, i Dogecoin,

o i Peercoin.

I primi rappresentano un'interessante soluzione, con un valore vicino ai 30 dollari e una capitalizzazione totale di oltre 300 milioni di dollari (i Bitcoin sono vicini agli 8 miliardi e i Litecoin a oltre 400 milioni), ma le altre due citate rappresentano dei casi particolari da considerare.

I Dogecoin sono una moneta nata quasi per scherzo, utilizzando il meme del cane Doge (che spopola sulla rete

da anni) e creandovi attorno una moneta virtuale. Complice il loro numero elevatissimo (100 miliardi di monete) e il rapido tempo di emissione questa moneta ha pian piano preso piede fino a diventare la quinta per capitalizzazione con oltre 50 milioni di dollari.

I Peercoin hanno invece caratteristiche diverse, avendo un blocco temporale di emissione fissato (come per i Bitcoin) in 10 minuti, ma nessun limite massimo al numero di monete circolanti.

Esistono ad oggi più di 100 criptomonete riconosciute e ogni giorno ne nascono di nuove. Per valutarle potete fare riferimento a uno dei tanti siti che le catalogano e ne tengono traccia dei movimenti: due su tutti: *coinwarz.com* e *coinmarketcap.com*.

Le criptomonete alternative sono interessanti sia per chi volesse interessarsi di scambi e investire qualche soldo nel loro commercio, sia per chi fosse interessato a produrle (come vedremo nel prossimo capitolo). La generazione domestica dei Bitcoin, la moneta più famosa, è infatti ad oggi quasi impossibile. La grande attenzione verso di essa fa in modo che le ricompense siano molto basse rispetto alla potenza computazionale richiesta, e quindi sconsigliabile. Produrre monete

alternative può rappresentare un duplice investimento, sia quello di generare moneta con un valore superiore a quello dell'energia consumata sia quello di generarne attendendo che il cambio, come per i Bitcoin, passi da pochi millesimi di dollaro a qualche decina o centinaio. Nel breve tempo intercorso tra la stesura e la verifica di questa parte, ad esempio, gli Auroracoin sono passati da un valore di circa 19 dollari ciascuno a 30 dollari. Un incremento del 50% in soli tre giorni.

Mining, ovvero produrre moneta

Qualche pagina fa abbiamo visto come alcuni particolari nodi della rete vengano utilizzati per il calcolo dell'hash dei blocchi e, quando uno di loro lo trova, si procede al passaggio successivo.

Tutte le reti di criptovalute premiano la scoperta di un hash corretto con una quantità predefinita di moneta, in modo da incentivare gli utilizzatori a supportare il calcolo della sicurezza delle transazioni tramite i propri Pc e la propria potenza computazionale.

Questo comporta che ad ogni slot di tempo prestabilito (nei Bitcoin di 10 minuti, nei Litecoin di 2,5 minuti e nei Dogecoin di 1 minuto) venga creata un determinata quantità di moneta, secondo un algoritmo tale da seguire la curva di emissione prestabilita durante la definizione della moneta.

I Bitcoin hanno ad esempio avuto una ricompensa di 50 BTC fino a fine 2012, quando è stata raggiunta l'emissione della metà della moneta predefinita, da quel momento il tempo di ogni blocco è rimasto a 10 minuti, ma la ricompensa è scesa a 25 BTC. Nel 2016 scenderà a 12,5 proprio per mantenere costante il rateo di emissione della moneta.

Il calcolo dell'hash consiste, nella pratica, nel trovare una soluzione a un problema noto: trovare un numero tale che l'hash (SHA-256 o Scrypt) del blocco in

CARATTERISTICHE DELLE PRIME 7 CRIPTOVALUTE (PER CAPITALIZZAZIONE)

Nome	Tag	Hash	Capitalizzazione (USD)	Tempo blocco	Ricompensa	Cambio difficoltà	Difficoltà al 10/03/2014	Monete totali da emettere	Monete emesse al 10/03/2014	Valore al 10/03/2014 (USD)
Bitcoin	BTC	SHA-256	7.990.666.044	10 minuti	25 BTC	2.016 blocchi	3.815.723.798	21.000.000	14.496.350	639,44
Litecoin	LTC	Scrypt	430.639.814	2,5 minuti	50 LTC	2.016 blocchi	3.921	82.000.000	26.427.804	16,29
Auroracoin	AUR	Scrypt	314.775.620	10 minuti	25 AUR	8 blocchi	3.061	21.000.000	10.613.201	29,66
Peercoin	PPC	SHA-256	70.260.223	10 minuti	102,88 PPC	1 blocco	89.241.344	Nessun limite	21.213.631	3,31
Dogecoin	DOGE	Scrypt	50.644.523	1 minuto	0-500.000 DOGE	240 blocchi	1.216	100.000.000.000	58.525.169.337	0,001
Namecoin	NMC	SHA-256	28.288.171	10 minuti	50 NMC	2.016 blocchi	3.070.377.120	21.000.000	8.206.242	3,44
Feathercoin	FTC	Scrypt	7.254.199	2,5 minuti	200 FTC	504 blocchi	198	336.000.000	35.890.800	0,2

questione risulti inferiore (o superiore) a una data soglia. Per fare questo i software utilizzati devono procedere per tentativi.

Il tempo medio di calcolo di un hash dipende dunque dalla potenza computazionale utilizzata. Più la rete si ingrandisce e più nodi concorrono al calcolo e più ridotto sarà il tempo di calcolo dell'hash corretto e, potenzialmente, i 10 minuti fissati potrebbero anche ridursi di moltissimo.

Per questo motivo, dopo un intervallo di blocchi prefissato per ciascuna

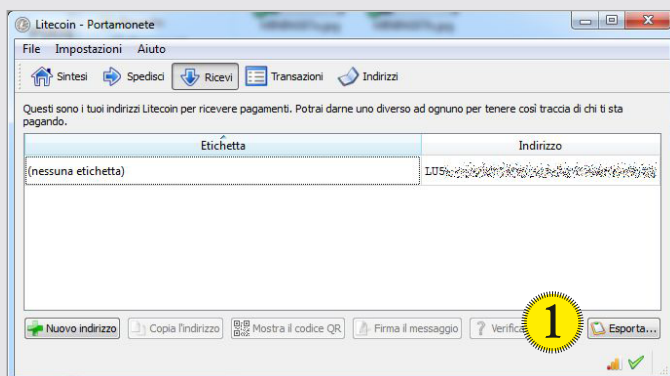
moneta (nei Bitcoin ogni 2.016 blocchi, nei Litecoin ogni 2.016 blocchi e nei Dogecoin ogni 204 blocchi) il sistema adegua automaticamente la difficoltà di calcolo (aumentandola o riducendola) per riportare la media a quella prevista. Questo succede per tutte le monete, ma è davvero evidente nell'ultimo anno con Bitcoin in cui la difficoltà è cresciuta in maniera esponenziale tanto quanto il valore della moneta o la potenza immessa nella rete. Il successo di una moneta porta infatti a un sempre più intenso calcolo da parte di utenti che

cercano un ricavo dopo la scoperta di un blocco, con un crescere della difficoltà necessaria a mantenere costante il tempo di emissione della moneta. Nel caso di Bitcoin l'escalation è evidente: la difficoltà a inizio 2012 era di circa 1 milione, mentre a fine giugno dello stesso anno è arrivata a 2 milioni, raggiungendo i 3 a inizio ottobre. A quel punto la rete aveva una potenza di calcolo di circa 20 GH/s (Giga Hash al secondo, il numero di hash provati ogni secondo per cercare quello corretto). Dopo un periodo di calo si è arrivati a

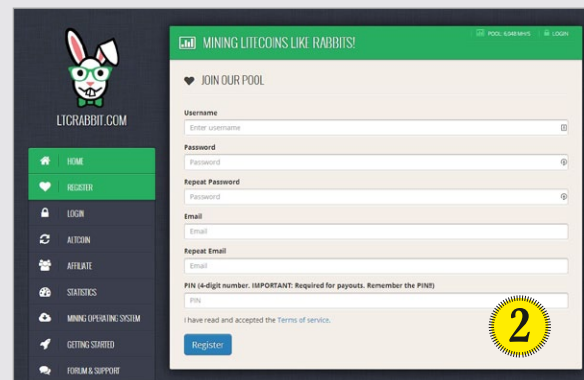
SETUP DI UN MINER

Creare una stazione domestica dedicata al mining (o adibire parte della potenza del proprio Pc per questo lavoro) è nel complesso molto semplice e in questa mini-guida vi spiegheremo come fare. Iniziamo con un piccolo

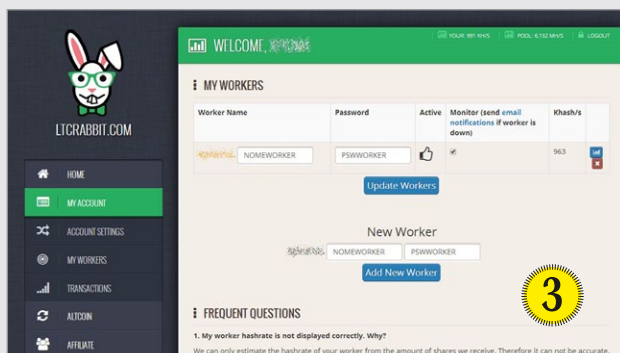
distinguo: le schede grafiche dedicate sono utili per questo, mentre i processori, anche molto potenti, ottengono risultati piuttosto scarsi. La grande parallelizzazione delle unità interne delle Gpu permettono infatti di calcolare



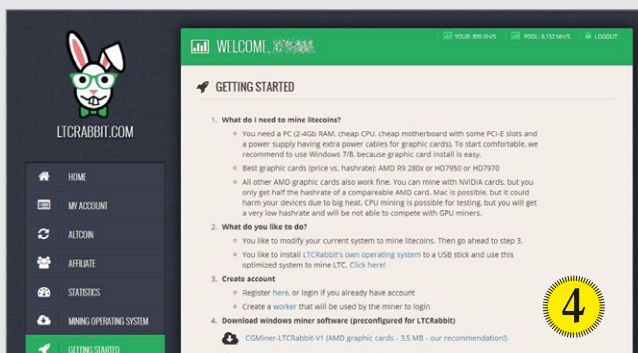
La prima cosa utile, ma non indispensabile, è un wallet della moneta scelta. In questo caso utilizziamo i Litecoin e quindi scarichiamo e installiamo il client dal sito ufficiale. La prima sincronizzazione con la rete può richiedere parecchio tempo. Nell'immagine la sezione *Ricevi*, in cui trovate l'indirizzo del vostro wallet.



In seguito vi consigliamo di associarvi a un pool proporzionale o PPS, in modo da facilitare la scoperta di blocchi e guadagnare in base a quante share produce il vostro Pc. Un buon pool per principianti è LTCRabbit (www.ltcrabbit.com).



Il secondo passaggio è quello di aggiungere un worker al vostro account. Un worker è l'identificativo del miner che installerete sul vostro Pc. È infatti possibile creare più worker, anche su Pc differenti, che si collegano e portano share sullo stesso account. Inserite qui il nome e la password e ricordate che ogni worker sarà identificato dalla coppia VOSTROUSERNAME.NOMEWORKER.



Il sito offre una piccola guida su come installare e avviare il worker sul proprio sistema. Per le schede AMD è consigliato il CGMiner. Il programma, .exe, viene lanciato tramite un file batch che contiene le informazioni essenziali.
`cgminer.exe --script-o stratum+tcp://eu.ltcrabbit.com:3333 -u USERNAME.WORKER -p PASSWORD -g 1 -w 256 --thread-concurrency 8192 --intensity 18`

4 milioni a fine febbraio, a 20 milioni a metà giugno e a 100 a inizio settembre fino al trampolino che ha portato a 500 a inizio novembre, al miliardo a dicembre e ai 4-5 miliardi oggi. La crescita è stimata in circa il 20% ogni 2 settimane, come potete vedere dalla tabella e lo schema in queste pagine. In questa "corsa all'oro" battezzata in inglese *mining* (che significa estrazione in termini minerari), tutti i nodi della rete concorrono per il calcolo della soluzione al problema crittografico dell'hash. Il primo a trovare una

soluzione valida la inoltra agli altri nodi della rete e, se validata, riceve come ricompensa la moneta corrispondente. Per il mining, che può portare a guadagni anche elevati, si può utilizzare sia il processore sia la scheda grafica, utilizzando software appositamente sviluppati che effettuano questi calcoli. Per i Bitcoin in particolare, visto il successo commerciale, sono anche stati sviluppati dei processori appositi (Asic ovvero *Application Specific Integrated Circuit*) in grado di effettuare solo quell'operazione ma in maniera rapidissima,

permettendo ai loro possessori di guadagnare moltissime monete.

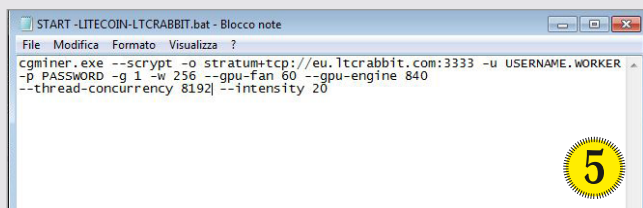
Mining personale

A questo punto vi chiederete come sia possibile partecipare al mining, in modo da incamerare qualche criptomoneta e guadagnare dei soldi.

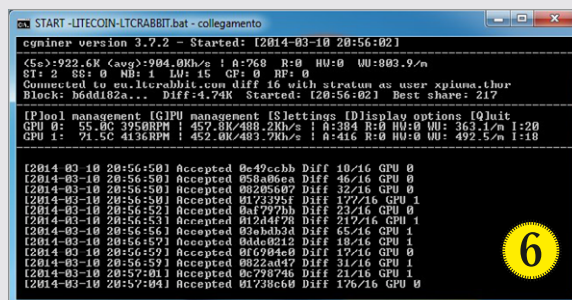
Innanzitutto facciamo una distinzione tra due distinte possibilità, il solo mining e il pool mining. La prima modalità permette agli utenti di partecipare in solitaria al calcolo dell'hash e di ricevere

hash molto più velocemente delle Cpu, con un divario anche di 100 volte. Tra le due grandi famiglie, Nvidia GeForce e AMD Radeon è quest'ultima che ottiene risultati migliori, con divari, a parità di prezzo, molto importanti. Nel seguito vi mostreremo come creare un miner per Litecoin su un sistema dotato di una scheda AMD Radeon HD6950, non certo un modello recente ma più che adatto allo scopo. Sui siti principali delle criptomonete (o sui Wikia ad essi collegati) si trovano spesso elenchi e comparazioni tra i maggiori modelli

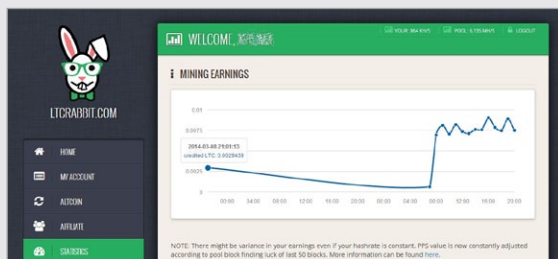
di schede grafiche, in modo da capire meglio (anche in virtù del consumo di corrente) come orientarsi. C'è infatti da tenere in considerazione che il proprio sistema consuma energia elettrica e che per far sì che "il gioco valga la candela" bisogna produrre di più rispetto alla spesa. Un buon modo per farsi un'idea (e confrontare la resa delle varie criptomonete) è usare il sito coinwarz.com che permette, una volta inserita la potenza e il consumo del proprio sistema, di capire costi e spese in un arco temporale definito.



Importante inserire il nome del server a cui connettersi (lo trovate nel sito del pool), il nome utente e il nome del worker e la password. I parametri successivi sono specifici per la scheda HD6950, trovate quelli migliori nelle varie liste accennate in precedenza. Gpu fan indica la percentuale rispetto alla velocità massima a cui impostare la ventola, mentre con Gpu engine si può settare la velocità di clock della scheda. L'intensità, il valore finale variabile da 8 a 20, indica quanta parte della Gpu riservare al calcolo. A 20 è tutta dedicata e il sistema risulta instabile e quasi inutilizzabile, provate il migliore per la vostra configurazione.



Il programma in funzione: in alto la quantità di hash calcolati negli ultimi 5 secondi e quelli medi totali. Le shares accettate (A) e quelle rifiutate (R). Questa configurazione ha 2 Gpu (identificate come 1 e 2) e per ciascuna di esse è possibile vedere temperature, velocità della ventola e ogni dettaglio. Premendo G è possibile accedere alla configurazione avanzata delle schede in termini di velocità di clock, di intensità di calcolo e altri parametri.



TRANSACTION HISTORY				
TX #	Date	TX Type	Payment Address	Amount
16617133	2014-03-10 20:01:13	Fee_PPS		0.00015009
16617132	2014-03-10 20:01:13	Credit_ALT		0.00000101
16617131	2014-03-10 20:01:13	Credit_PPS		0.00750429
16603811	2014-03-10 19:01:13	Fee_PPS		0.00017791
16603810	2014-03-10 19:01:13	Credit_ALT		0.00000120
16603809	2014-03-10 19:01:13	Credit_PPS		0.00889538
16590532	2014-03-10 18:01:13	Fee_PPS		0.00014948
16590531	2014-03-10 18:01:13	Credit_ALT		0.00000101
16590530	2014-03-10 18:01:13	Credit_PPS		0.00747444
16577340	2014-03-10 17:01:13	Fee_PPS		0.00015726

Una volta configurato il client comincia il mining e, in base alla politica del pool (LTCRabbit lo fa ogni ora) vi verranno riconosciuti dei Litecoin. Il pool trattiene una piccola percentuale sui Litecoin calcolati e con questi si mantiene. A volte, come si vede nell'immagine, sfrutta la capacità della rete per fare mining anche su altre monete offrendo una rendita extra ai contribuenti, sempre in Litecoin.

TIPI DI RICOMPENSE DEI MINING POOL

PROP	Proporzionale	Quando si trova un blocco la ricompensa è distribuita tra i worker in base alle share trovate da ciascuno.
PPLNS	Pay Per Last N Shares	Simile al proporzionale ma tiene conto solo di un numero finito di shares.
PPS	Pay Per Shares	Ogni share inviata frutta un predeterminato numero di monete.
RBPPS	Round Based Pay Per Share	Come il PPS ma i pagamenti sono ritardati fino alla conferma definitiva del blocco.
SMPPS	Shared Maximum Pay Per Share	Come PPS ma il pool non paga più di quanto ha guadagnato.

la ricompensa in maniera completa qualora il proprio sistema trovasse l'hash preciso del blocco. Inutile dire che partecipare a questa corsa da soli, pur con Pc potentissimi, è l'equivalente nelle criptovalute di Don Chisciotte contro i mulini a vento. Un sistema, anche di fascia alta, ha una potenza di calcolo di qualche centinaio di MH/s (per SHA-256) o KH/s (per Scrypt), mentre ad esempio la rete intera Bitcoin ha un rateo di oltre 30 miliardi di MH/s. In questo caso la possibilità, in circa 10 minuti di tempo, di trovare per primi il blocco sono davvero minime.

La seconda possibilità, vivamente caldeggiata, è quella di prendere parte a un pool, ovvero un gruppo di macchine che lavora al di sotto della stessa "bandiera" e mette in comune la potenza di calcolo per emergere nel panorama delle criptovalute. Esistono moltissimi pool differenti, sia per caratteristiche sia per politica interna. Il funzionamento è altrettanto differente, con alcuni stili che

hanno preso piede più di altri. Li trovate descritti nella tabella qui a fianco. Uno dei più utilizzati è il PPLNS, un sistema proporzionale su base temporale (tiene conto delle ultime n share inviate alla rete rispetto al totale del pool). Per gli utenti domestici forse il migliore resta però il semplice PPS, che permette di ricevere dal pool una somma proporzionale alle share inviate. Alcuni pool chiedono una percentuale (da 0 a 5%) sui guadagni effettuati o sui trasferimenti di moneta verso altri portafogli (o anche entrambe), mentre altri non lo fanno.

Per fare mining personale servono dunque tre cose: un Pc con una buona scheda grafica (le Gpu sono molto più veloci delle Cpu a calcolare gli hash), una connessione a Internet sempre attiva (per ricevere e inviare i dati) e un account su un pool (e una moneta) a vostra scelta. In un box dedicato in queste pagine vi mostriamo una guida passo passo su come selezionare un pool, attivare un account e iniziare il mining con il proprio Pc.

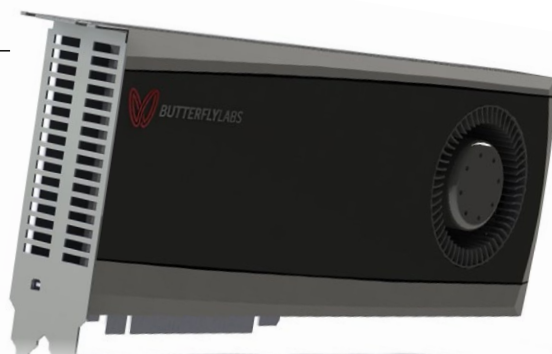
Dove e come scambiare

Così come esistono mercati di scambio per le monete tradizionali, luoghi fisici o virtuali in cui si possono scambiare euro per dollari, rubli per yuan e così via, anche per le criptomonete esistono degli ambienti simili. In molti siti

è possibile scambiare le criptomonete tra di loro, mentre pochi altri hanno la funzione di portale e permettono di scambiare criptomonete per valuta reale. Un ottimo per le sole criptomonete è *coinex.pw* (ha anche dei pool per il mining), mentre per scambi più articolati vi segnaliamo *cryptsy.com* o *virucurex.com*. Il loro funzionamento è semplice e ricalca quello dei mercati di scambio normale. Il possessore di una quantità di moneta fa un'offerta di vendita (o di acquisto) di monete fissando il cambio. A quel punto se il sistema rileva un altro utente che ha fatto l'offerta opposta e il prezzo coincide allora l'affare si conclude. Nell'esempio che vedete in questa pagina abbiamo messo in vendita 500 Lottocoin al prezzo di 0,0399 Dogecoin ciascuno, per un cambio di 19,95 Dogecoin. In basso nella pagina potete vedere gli ordini di acquisto e di vendita attivi e regolarvi di conseguenza. Certamente chi è interessato a vendere cerca il controvalore più alto possibile, mentre chi acquista cerca di spendere il meno possibile. Il tasso di cambio delle monete varia in questo modo, secondo la legge di domanda e offerta.

Bancomat, ATM e negozi e ultime news

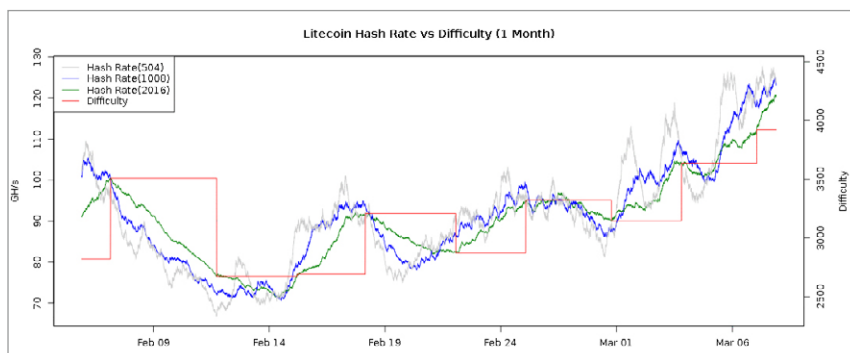
Negli ultimi mesi il mercato delle criptomonete ha attraversato alti e bassi.



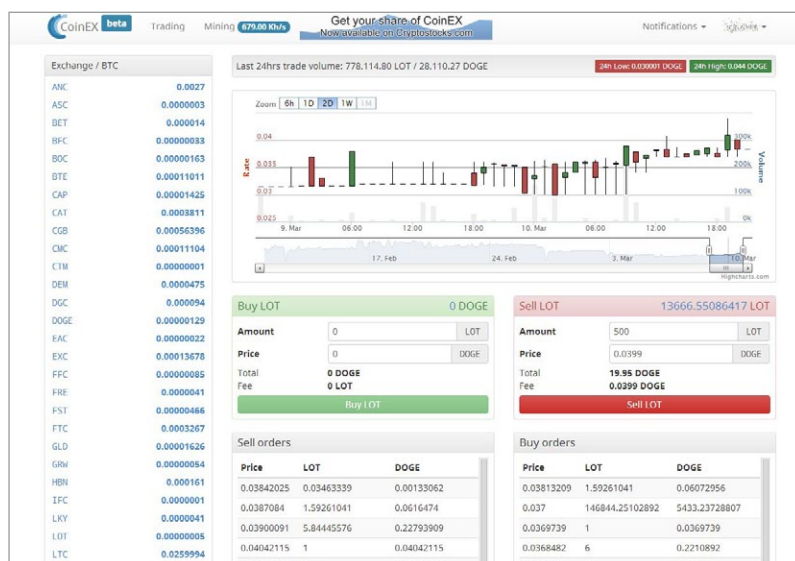
Una scheda dedicata al calcolo dell'hash per i Bitcoin. Questa "Monarch" genera 600 GH/s, mentre una scheda Radeon R290X arriva a malapena a 1 GH/s e un Core i7 solo 0,05 GH/s.

BITCOIN: DIFFICOLTÀ E HASH RATE

Data	Difficoltà	Hash Rate
13 Marzo 2014	4.298.421.497	31.569.413 GH/s
28 Febbraio 2014	3.815.723.799	27.314.015 GH/s
05 Febbraio 2014	2.621.404.453	18.764.744 GH/s
24 Gennaio 2014	2.193.847.870	15.704.175 GH/s
02 Gennaio 2014	1.418.481.395	10.153.885 GH/s
21 Dicembre 2013	1.180.923.195	8.453.378 GH/s
29 Novembre 2013	707.408.283	5.063.826 GH/s
05 Novembre 2013	510.929.738	3.657.378 GH/s
06 Ottobre 2013	189.281.249	1.354.928 GH/s
04 Settembre 2013	86.933.018	622.291 GH/s
03 Agosto 2013	37.392.766	267.668 GH/s
11 Luglio 2013	26.162.876	187.281 GH/s
05 Giugno 2013	15.605.633	111.709 GH/s
12 Maggio 2013	11.187.257	80.082 GH/s
05 Aprile 2013	7.673.000	54.925 GH/s
01 Marzo 2013	4.367.876	31.266 GH/s
05 Febbraio 2013	3.275.465	23.447 GH/s
08 Gennaio 2013	3.249.550	23.261 GH/s
10 Dicembre 2012	3.370.182	24.125 GH/s
12 Novembre 2012	3.368.767	24.115 GH/s
03 Ottobre 2012	3.054.628	21.866 GH/s
06 Settembre 2012	2.694.048	19.285 GH/s
12 Agosto 2012	2.190.866	15.683 GH/s
30 Luglio 2012	2.036.671	14.579 GH/s



Nei Litecoin l'andamento della difficoltà si modifica ogni 2.016 blocchi per mantenere il tempo di generazione costante e controllare di conseguenza l'emissione di moneta ogni 2,5 minuti.



Uno scambio di criptomonete. Nell'immagine una proposta di vendita di 500 Lottocoin in cambio di 19,95 Dogecoin. In alto il grafico con la quotazione tra le due monete negli ultimi due giorni.

Gli alti sono rappresentati dal lancio sul mercato di alcuni sistemi ATM (il nostro bancomat) in grado di accettare Bitcoin in cambio di moneta contante o fornire quest'ultima in cambio di una transazione in Bitcoin. Questo ha aumentato la credibilità di queste monete, così come l'impossibilità dei governi attuali di limitarne l'utilizzo. Alcuni hanno addirittura dichiarato fuorilegge le monete di questo tipo, bandendole dal proprio territorio con la paura di un coinvolgimento nel cambio della moneta nazionale e una sua contestuale svalutazione. Le criptomonete non hanno però modificato la propria rotta, risultando spesso insensibili alle volontà dei governi centrali.

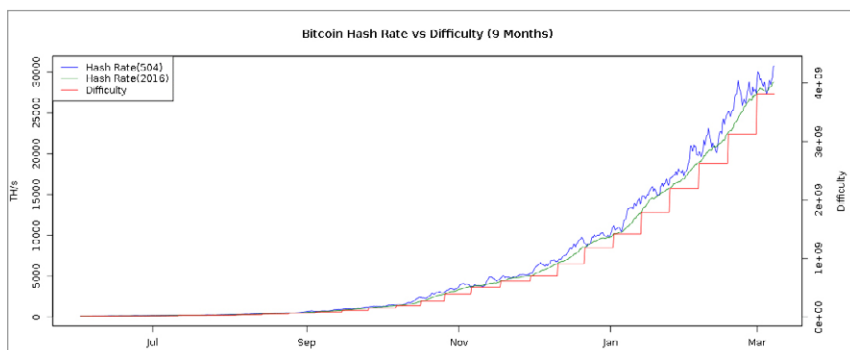
A oggi alcuni negozi (anche in Italia) accettano pagamenti in Bitcoin. La legge non regola le transazioni di questo tipo e, almeno per il momento,

sono completamente libere e legali. In altri paesi anche le alternative hanno iniziato a prendere piede, tant'è che in alcuni stati si trovano negozi che accettano anche Litecoin. Soldi, tanti e scaturiti dal nulla, sono però un richiamo davvero forte anche per speculatori e criminalità. Dopo il picco di novembre dei Bitcoin, il cui valore ha superato i 1.250 dollari per un breve periodo temporale, alcuni problemi di varia natura ne hanno fatto crollare il valore e modificato l'opinione pubblica sull'argomento.

Mt-Gox, uno dei maggiori siti di scambio tra criptovaluta e valuta corrente, ha di punto in bianco chiuso i battenti e cancellato le proprie tracce. Il proprietario si sarebbe infatti dileguato con svariati milioni di dollari senza che gli utenti appoggiati a esso fossero avvertiti o rimborsati. Questo ha

causato delle ripercussioni notevoli in ogni parte del mondo, con alcuni fatti di cronaca davvero spiacevoli tra cui dobbiamo segnalare una serie di suicidi avvenuta nel sud-est asiatico a causa di sopravvenute bancarotte.

Le criptovalute sono un nuovo, interessante, esperimento sociale che potrebbe anche cambiare la vita di tutti noi. Con questo articolo abbiamo voluto darvi una base di conoscenza tale da poter riflettere autonomamente sul loro utilizzo e sul loro futuro. Fare mining o trading con queste monete può essere un investimento favoloso, capace di rendere ricchissimi con pochi spiccioli. Il rovescio della medaglia è ovviamente quello che tutto questo può anche rivelarsi una bolla gigantesca (e ciò è forse più probabile che il contrario). Se intendete investire qualcosa in questo particolare mondo prestate dunque molta attenzione in quanto la possibilità di perdere l'investimento è sostanzialmente molto elevata. •



Il successo dei Bitcoin ha portato a un sempre maggior interesse e una crescita esponenziale nella potenza di calcolo della rete. La difficoltà, per avere emissione costante, è salita alle stelle.

