Il presente modulo riporta i concetti teorici di utilizzo di una moneta elettronica e sulla gestione delle transazioni. Per semplicità di esposizione si è trattato come riferimento la moneta elettronica Bitcoin ma i principi e la metodologia sono analoghi per qualsiasi altra valuta elettronica.

Bitcoin

Prof. Michele Tarantino

Introduzione

Il Bitcoin è una moneta elettronica di tipo virtuale e come tale viene scambiata elettronicamente tramite Internet in modo *peer-to-peer*. È stata creata nel 2009 da un anonimo conosciuto con lo pseudonimo di Satoshi Nakamoto. Tramite meccanismi appositi, gli utenti possono conservare il proprio denaro virtuale e scambiarselo da terminale a terminale, utilizzandolo come portatore di valore dove la moneta è accettata. Il nome Bitcoin si riferisce anche al software open source progettato per implementare il protocollo di comunicazione e la rete *peer-to-peer* che ne risulta. Convenzionalmente, il termine *BITCOIN* maiuscolo si riferisce alla tecnologia ed alla rete mentre il minuscolo *Bitcoin* si riferisce alla valuta in sé.

A differenza della maggior parte delle valute tradizionali, Bitcoin non fa uso di un ente centrale che lo genera (ad esempio una Banca Centrale): esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni, e sfrutta la crittografia a chiave privata per gestire gli aspetti funzionali come la generazione di nuova moneta e l'attribuzione di proprietà dei Bitcoin.

La rete BITCOIN consente il possesso ed il trasferimento anonimo delle monete; i dati necessari ad utilizzare i propri Bitcoin possono essere salvati su uno o più calcolatori sotto forma di "portafoglio" digitale (*Wallet*), o mantenuti presso terze parti che svolgono funzioni simili ad una banca. In ogni caso, i Bitcoin possono essere trasferiti attraverso Internet verso chiunque disponga di un "indirizzo Bitcoin". La struttura peer-to-peer della rete BITCOIN e la mancanza di un ente centrale rende impossibile per qualunque autorità, governativa o meno, di bloccare la rete, sequestrare Bitcoin ai legittimi possessori o di svalutarla creando nuova moneta.

Bitcoin è una delle prime implementazioni di un concetto definito *criptovaluta*, descritto per la prima volta nel 1998 da Wei Dai. Come ogni valuta, anche il Bitcoin ha il suo simbolo: ฿ oppure abbreviato BTC.

Rappresentazione dei Bitcoin

Le monete elettroniche possono essere viste come stringhe codificate, mediante algoritmi di crittografia, che vengono caricate in smart card oppure memorizzate in un dispositivo elettronico. Queste possono essere utilizzate da un utente per effettuare un pagamento senza la necessità di un ente esterno fidato (una banca o altro istituto finanziario).

Per la loro natura intrinseca i "gettoni elettronici" sono dati, e quindi come tali facilmente copiabili. Di conseguenza è necessario fornire un meccanismo di protezione contro le varie modalità di frode che possono essere messe in atto tramite l'utilizzo della moneta elettronica. Problemi tipici che si devono affrontare nell'utilizzo del Bitcoin sono quelli relativi alle transazioni elettroniche, a cui si vanno ad aggiungere:

- il problema del *double-spending*: spendere lo stesso gettone elettronico più volte;
- la possibilità di impersonare un utente spendendo i suoi gettoni virtuali invece che i propri.

Altre proprietà delle transazioni con i Bitcoin sono:

- accettabilità: il numero di utenti che accettano la moneta elettronica; adottare una moneta largamente accettata implica dare la possibilità a molti utenti di utilizzare tale moneta per acquistare i beni o servizi venduti e aumentare il segmento di vendita;
- comodità: il numero di azioni fisiche ed il tempo necessario da queste per effettuare un acquisto;
- costi: i costi dovrebbero essere gli stessi di una normale transazione elettronica;
- durabilità: rappresenta la capacità della moneta digitale di resistere alla possibilità di "perdita" di gettoni, come ad esempio in caso di crash di un sistema.

Le maggiori peculiarità nell'utilizzo di questa moneta virtuale sono l'anonimato e la non tracciabilità delle movimentazioni di denaro, in netto contrasto con i principi delle transazioni bancarie. La transazione lascia in ogni caso una traccia permanente (informazione) del pagamento ma non viene memorizzata l'identità dei soggetti.

È possibile acquistare beni e servizi in rete, in tutto il mondo nei siti dove i Bitcoin vengono accettati. Oltre a mantenerli memorizzati nel proprio dispositivo elettronico, possono essere conservati in "banche virtuali" come possibilità di investimento ad alto rischio.

Architettura e Transazioni

Come scritto precedentemente Bitcoin è basata su una rete peer-to-peer di nodi (dispositivi) che cooperano al fine di mantenere corretto il funzionamento dell'intero sistema ed evitare attività non permesse. La transazione dei Bitcoin è definita come una catena di firme digitali che appartengono ai vari utenti che sono entrati in possesso e successivamente hanno speso quel

gettone. Prima di illustrare il funzionamento dell'architettura Bitcoin, sarà presentata la funzione di hash necessaria per crittografare le transazioni.

Ad ogni transazione viene inviato un codice *hash* generato da una funzione che prende in ingresso una stringa di lunghezza arbitraria producendo in uscita una nuova stringa di lunghezza predefinita che rappresenta una sorta di "impronta digitale" dei dati contenuti nella stringa di ingresso. La funzione di *Hash* è a senso unico: conoscendo l'*hash* deve essere difficile trovare il messaggio originale mentre possedendo il messaggio originale è possibile stabilire il suo hash univoco. Una funzione crittografica di hash deve approssimare una funzione "random" restando deterministica ed efficiente dal punto di vista computazionale. Deve quindi assicurare che ciascun output abbia la stessa probabilità di essere associato ad un input e restituire sempre lo stesso output a fronte dello stesso input.

Una funzione crittografica di hash è considerata insicura se è computazionalmente fattibile almeno una delle seguenti opzioni:

- calcolare un messaggio che produca un hash dato;
- trovare una "collisione" ovvero due messaggi diversi che producono il medesimo hash.

Un attaccante che fosse in grado di eseguire una delle due operazioni citate, potrebbe ad esempio sostituire un messaggio autorizzato con un altro senza che si possa provare la contraffazione.

Una funzione crittografica di hash di qualità dovrebbe rendere difficile calcolare anche solo due messaggi con hash sostanzialmente simili oltre che garantire un'ottima non-correlazione tra hash e messaggio: nessuna informazione del messaggio dovrebbe essere ottenuta dal suo hash. Ad un eventuale attaccante resta solo l'informazione relativa all'associazione tra messaggio ed hash: esso può riconoscere che il messaggio è stato di nuovo usato vedendo una seconda volta lo stesso hash.

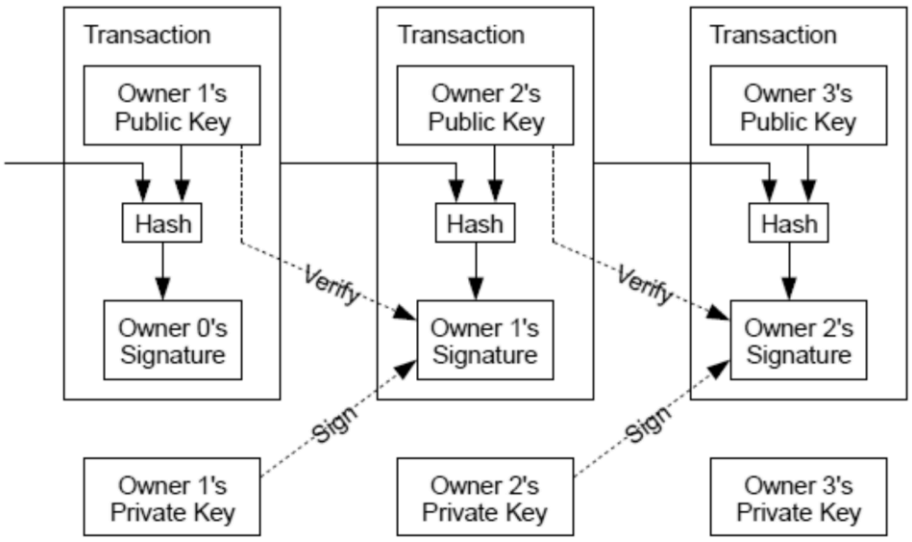
La funzione crittografica di hash ideale deve avere tre proprietà fondamentali:

1. deve essere estremamente semplice calcolare un hash da qualunque tipo di dato;
2. deve essere estremamente difficile o quasi impossibile risalire al testo che ha portato ad un dato hash;

3. deve essere estremamente improbabile che due messaggi differenti, anche se simili, abbiano lo stesso hash.

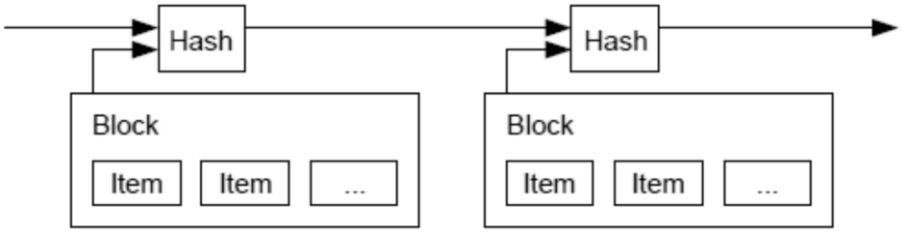
Oltre a queste tre proprietà fondamentali c'è da aggiungere il cosiddetto "effetto valanga", ossia la minima modifica del messaggio deve portare ad un'alterazione radicale dell'impronta del messaggio.

La catena di firme digitali che rappresenta un Bitcoin può essere divisa in transazioni atomiche: ogni proprietario trasferisce un Bitcoin firmando tramite firma digitale l'hash della precedente transazione e la chiave pubblica del destinatario; tali informazioni vengono poi aggiunte in coda al Bitcoin in fase di trasferimento. Il beneficiario può verificare la transazione utilizzando la chiave pubblica del cliente per decriptare l'ultima transazione e verificare che oltre all'hash della transazione precedente vi sia anche la propria chiave pubblica. Tramite questo meccanismo è possibile verificare che una transazione sia stata eseguita ma non che quel particolare Bitcoin sia già stato speso. Una semplice soluzione sarebbe quella di introdurre un'autorità centrale, detta zecca, che provvede a verificare ed autorizzare ogni transazione. Il problema di questa soluzione è che l'intero sistema di moneta elettronica dipende esclusivamente dal sistema zecca. Nell'architettura di Bitcoin si desidera evitare una soluzione centralizzata come questa, ma resta comunque la necessità di evitare il *double-spending*, ovvero si ha la necessità di controllare le ultime transazioni.



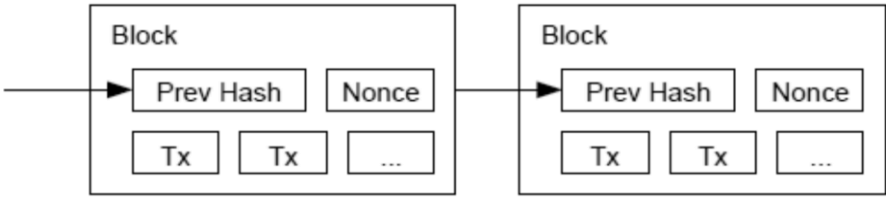
Per effettuare questo controllo senza la necessità di terze parti, le transazioni devono necessariamente essere annunciate pubblicamente: in questo modo il beneficiario di una transazione può verificare che la maggior parte dei nodi della rete hanno accettato la transazione che lo riguarda.

Per garantire tale transazione viene introdotto il *timestamp server* il quale è utilizzato per annunciare pubblicamente l'accettazione di un blocco di transazioni. Questo server calcola l'hash di un blocco di oggetti annunciando successivamente il risultato calcolato. Tale sistema viene utilizzato per verificare che in un determinato istante una certa transazione era già avvenuta (in quanto faceva parte del blocco del quale è stato calcolato l'hash). Quindi, viene utilizzato come "timestamp" (marcatore temporale) l'hash calcolato sul blocco assieme al timestamp del blocco precedente, formando quindi una catena in cui ogni nuovo timestamp rinforza i precedenti.



Il calcolo dell'hash viene fatto in maniera distribuita (si parla quindi di server distribuito) tra tutti i nodi della rete proprio per sfruttare al massimo le capacità della rete P2P.

Al fine di implementare un timestamp server distribuito in una rete peer-to-peer è utilizzato un sistema di *proof-of-work* (POW). Per sistema di proof-of-work si intende l'utilizzo del risultato di un operazione computazionalmente difficile (ma di semplice verifica) come "firma" su un blocco di dati che si desidera proteggere al fine di evitare che questi vengano corrotti o replicati. Nel caso di Bitcoin l'operazione da svolgere consiste nella ricerca di un valore che, aggiunto al blocco di informazioni, faccia in modo che il risultato del calcolo dell'hash tramite l'algoritmo di controllo SHA-256 abbia un certo numero di zeri all'inizio. Tale operazione ha costo medio esponenziale nel numero di zeri richiesti. Una volta trovata la soluzione per un determinato blocco, questo non può più essere cambiato senza dover rifare la firma. Maggiore è il numero di blocchi che verranno accettati (ovvero per i quali verrà trovata una soluzione), maggiore sarà il lavoro da rifare per effettuare una modifica al blocco in questione (dovendo ricalcolare anche le soluzioni per i blocchi successivi). Il sistema di POW permette anche di risolvere il problema della rappresentanza nel processo decisionale a maggioranza: se la maggioranza si fosse basata sul numero di IP (one-IPAddress-oneVote) questa potrebbe essere sovvertita da chiunque sia in grado di istanziare più indirizzi IP. Il sistema POW è basato invece sulla regola one-CPU-one-vote. La decisione della maggioranza viene presa in base alla catena più lunga la quale rappresenta il maggior sforzo computazionale fatto finora.



Al fine di mantenere costante il numero di blocchi generati per unità di tempo la difficoltà dell'algoritmo (ovvero il numero di zeri iniziali richiesti) viene aggiustato costantemente: se la generazione dei blocchi avviene troppo velocemente la complessità verrà aumentata, nel caso in cui avvenga troppo lentamente, essa verrà diminuita.

Funzionamento della rete

La rete BITCOIN funziona seguendo i seguenti passi:

1) le nuove transazione sono inviate in broadcast a tutti i nodi;
2) ogni nodo colleziona le transazioni ricevute all'interno di un blocco;
3) ogni nodo cerca una soluzione alla POW per il proprio blocco;
4) quando un nodo trova la soluzione invia il blocco in broadcast a tutti i nodi;
5) i nodi accettano il blocco solo se tutte le transazioni in esso sono valide e non già spese;
6) i nodi accettano il blocco mettendosi a lavorare sul blocco successivo utilizzando l'hash appena ricevuto.

La rete considera da un punto di vista euristico corretta la catena più lunga. Nel caso in cui due nodi inviassero "nello stesso istante" due diverse versioni di un blocco, entrambe con soluzione corretta della POW, i vari nodi inizieranno a lavorare al blocco successivo prendendo per buono il primo blocco ricevuto tra i due, salvando comunque anche il secondo. Una volta che verrà trovata la soluzione alla POW per il blocco successivo, questo verrà inviato in broadcast a tutti i nodi; in questo modo tutti i nodi si uniformeranno a lavorare sulla catena di blocchi attualmente diventata la più lunga. Il broadcast delle nuove transazioni non deve necessariamente essere verso tutti i nodi: una volta che una transazione è inviata ad un numero sufficientemente grande di nodi, sarà presto inclusa in un blocco. Il broadcast dei blocchi rende il sistema tollerante ala perdita di messaggi: infatti se un nodo non riceve un blocco, una volta che esso riceverà il blocco successivo si accorgerà di non aver ricevuto il blocco precedente e ne farà richiesta.

Generazione dei Bitcoin

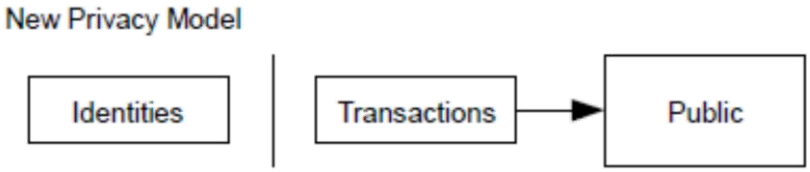
I Bitcoin sono mantenuti in un “portafoglio elettronico” chiamato Wallet. Per Wallet si intende il programma che permette di entrare nella rete BITCOIN. Il portafoglio virtuale contiene indirizzi e chiavi per effettuare le transazioni economiche, ad esempio spedire del denaro. Questo fa del wallet una banca personale per Bitcoin e può essere di diverso tipo: può essere installato sullo smartphone per piccoli pagamenti con *QR Code*, può essere un servizio web oppure può essere un software che offre pieno controllo del Wallet anche in modalità offline, ma in questo caso backup e sicurezza del denaro sono a piena responsabilità del possessore. È possibile in oltre guadagnare nuovi Bitcoin collegando il Wallet ad un *Miner*. Per *Miner* si intende un calcolatore messo a disposizione del P2P di BITCOIN per l’operazione di verifica della correttezza di un’operazione. Agli albori del Bitcoin, bastava un modesto computer per poter svolgere questo ruolo, ma le potenze di calcolo necessarie sono sempre più alte (si parla di 5 quintilioni di operazioni al secondo nel mondo) e si sono creati gruppi di professionisti che sono in grado di gestire e guadagnare con questa nuova moneta. È ancora possibile essere un Miner singolo con un computer dotato di scheda e processore ASIC appositamente creati per il mining (estrazione), ma i guadagni spesso non riescono neppure a coprire i costi del consumo elettrico per tenerli sempre accesi. Questo quindi permette di sfruttare la potenza del processore e della scheda video di un dispositivo per la creazione di nuovi Bitcoin; più la potenza di elaborazione di quest’ultimi sarà alta più Bitcoin si potrà essere in grado di generare. Non potranno più essere coniati più di 21 milioni di Bitcoin. Sono disponibili in quantità limitata, ubbidiendo a un preciso modello matematico che si arresterà nel 2140.

Privacy

Nel modello di banca tradizionale la privacy è garantita non consentendo l'accesso alle informazioni che riguardano la singola transazione, in particolare, alle identità delle parti coinvolte e all'identità della terza parte di fiducia.

Questo modello chiaramente non può essere applicato al Bitcoin proprio perché quest'ultimo, per funzionare, ha bisogno che tutte le transazioni siano rese pubbliche. La privacy può essere

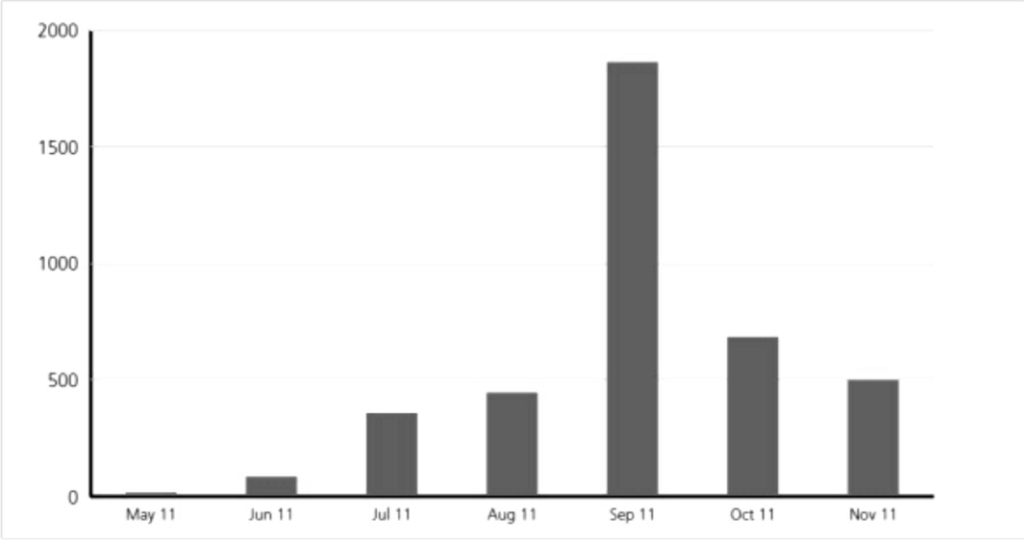
raggiunta interrompendo il flusso di informazioni da un'altra parte, ossia mantenendo le chiavi pubbliche in anonimato. Nel modello del Bitcoin tutti possono vedere che qualcuno sta inviando un pagamento a qualcun altro ma senza nessun tipo di informazione che collega la chiave pubblica o l'indirizzo bitcoin con l'identità di un determinato soggetto.



Inoltre, come misura aggiuntiva di privacy, per ogni transazione il sistema prevede anche la possibilità di utilizzare chiavi differenti. Questo chiaramente permette di aumentare il livello di privacy anche nel caso l'identità del proprietario di una chiave fosse rivelata. Infatti, cambiando spesso coppia di chiavi, sarà impossibile risalire ad altre transazioni realizzate dallo stesso soggetto del quale, in qualche modo, ne è stata scoperta l'identità.

Possibili minacce

La natura delle monete digitali rendono i Bitcoin un bersaglio molto appetibile da parte dei criminali informatici. Il seguente grafico indica il numero di furti di monete bitcoin avvenuti da maggio a novembre 2011, fornendo un'idea di quanto la sicurezza informatica è una questione di primaria importanza all'interno di tecnologie di *digital - currency*.



Dobbiamo dire che in generale bitcoin è molto robusto e ha difese contro molti tipi di attacchi. Tuttavia, come abbiamo visto, non è totalmente immune.

Vediamone alcune:

1. *Furto del Portamonete:*

Il portamonete di default non è criptato e perciò diventa un target primario per un eventuale furto di bitcoin. Nel 2011 fu creato uno Spam che pubblicizzava un falso software per effettuare mining. Questo tool conteneva un malware disegnato per inviare i file riguardanti il portafoglio delle vittime ad una postazione remota. L'ultima versione del client Bitcoin, la 0.6, prevede la possibilità che l'utente possa criptare tutti i dati inerenti al suo portamonete.

2. *Denial of Service (DoS):*

Il Denial of Service è un particolare tipo di attacco che ha come scopo quello di fermare l'operatività dell'obiettivo e non quello di rubare dei dati. Normalmente i pacchetti con le richieste hanno un indirizzo sorgente falso, in questo modo l'intruso non può essere identificato facilmente.
Supponiamo ad esempio che un attaccante abbia l'obiettivo di sovraccaricare la rete BITCOIN. La prima cosa che può fare è inviare milioni di piccole transazioni tra alcuni dei propri account. Per esempio può mandare Bitcoin tra vari indirizzi in rapida sequenza: A→B→C→A→B→C. Bitcoin prevede delle protezioni contro attacchi di questo tipo: il sistema è in grado di rilevare dei dati inviati in rapida sequenza da una singola sorgente e automaticamente disconnettere il relativo nodo dalla rete. Dobbiamo aggiungere, in conclusione, che non si possono escludere attacchi di Denial of Service più elaborati che siano in grado di causare il blocco della rete, ad esempio utilizzando molti diversi indirizzi Bitcoin (*DDoS – Distribuited Denial of Service*). E' previsto comunque, come funzionalità di sicurezza "indiretta", un pagamento di commissioni per transazioni con un basso valore di bitcoin in modo tale da rendere l'attacco non conveniente da un punto di vista strettamente economico.

La regola di default attuale per la tariffa è la seguente:

- 0,01 BTC per transazioni con valore minore di 0,01 BTC (per generare 1000000 di transazioni l'attaccante dovrebbe “investire” 10000 bitcoin);
- per transazioni con valore superiore a 0,01 BTC si applica di volta in volta una tariffa proporzionale al valore.

3. *Cancer Nodes:*

Un attaccante potrebbe riempire la rete con un numero grande di client controllati da lui stesso. Avendo a disposizione un numero di nodi molto alto potrebbe influenzare i comportamenti della rete stessa eseguendo, da questo punto in poi, altri tipi di attacco:

- può negare in modo arbitrario l’accettazione di transazioni;
- può effettuare un *double - spending* dei propri Bitcoin;
- può controllare la catena dei blocchi.

Questo tipo di attacco risulterà più difficile con reti di grandi dimensioni, in quanto richiederà che l’attaccante disponga di un numero di risorse più elevato.

4. *Violazione degli algoritmi crittografici:*

Si tratta di una minaccia non immediata ma piuttosto a medio - lungo termine. Infatti, il protocollo di gestione della rete Bitcoin potrà subire delle modifiche nel futuro, quando gli attuali algoritmi di firma e hash saranno a rischio a causa di un aumento della potenza di calcolo dei computer. Oggi sono usati ECDSA (*Elliptic Curve Digital Signature Algorithm*) per la firma digitale e SHA-256 per il calcolo dell'hash.

Conclusioni

Bitcoin è il primo esempio di *critto moneta*, realmente implementato, che con il suo sistema peer-to-peer ha decentralizzando la disponibilità di moneta togliendola dal controllo delle varie istituzioni finanziarie. Il Bitcoin è una moneta che è basata su tecnologie informatiche che

garantiscono un elevato livello di sicurezza mettendola al riparo da eventuali tentativi di frode. La sua natura la rende anche una moneta che offre un livello di privacy assoluto. Questa caratteristica può aprire degli scenari più o meno positivi. Quelli meno positivi riguardano la transazione di operazioni illegali, come ad esempio la vendita di materiale contraffatto o illegale. Dall'altra parte i cittadini onesti che rispettano le leggi possono effettuare transazioni economiche via Internet senza terze parti. Le transazioni effettuate con Bitcoin, non avendo intermediari, prevedono dei costi minimi di utilizzo che sono del tutto insignificanti se paragonati a quelli delle attuali transazioni commerciali che utilizziamo quotidianamente. La comodità, intesa come il numero di azioni fisiche ed il tempo da queste richiesto per effettuare un acquisto, è forse l'unico punto debole della valuta. Le transazioni possono impiegare effettivamente decine di minuti per essere "confermate". Anche con un aumento di qualche ordine di grandezza della potenza di calcolo complessiva della rete, la difficoltà di generare un blocco si auto-regolerà per garantire un obiettivo di 6 blocchi all'ora (1 blocco ogni 10 minuti).

Si può concludere che il Bitcoin ha tutte le caratteristiche per diventare nel prossimo futuro una moneta digitale riconosciuta in tutto il mondo, a patto che eventuali interessi di corporazioni non soffocheranno l'innovazione finanziaria rendendola di fatto fuori legge. Al momento Bitcoin, come scritto nel sito ufficiale, non viola nessun accordo governativo e finanziario e il suo utilizzo sarà strettamente legato al numero di soggetti, aziende o enti che saranno disposti ad accettarla in cambio di beni e servizi.

Resta connesso e informato sui prossimi eventi, corsi e seminari:

Web
www.profmicheletarantino.com

Email
profmicheletarantino@gmail.com

Telefono
349 83 54 521

Facebook
@micheletarantinodocente

Instagram
@profmicheletarantino

Hai bisogno di un modulo personalizzato? Non esitare a contattarmi!