

Bitcoin: P2P Digital Currency

Marco Mantilacci
Cristiano Santoni

1. Introduzione

Con il termine moneta elettronica (Digital Currency) si indica una tipologia di moneta che viene scambiata elettronicamente tramite Internet (più in generale tramite una qualsiasi rete) o appositi apparecchi come smart card e card reader. Alcune città (Hong Kong) e paesi (Belgio, Paesi Bassi) posseggono un sistema di moneta elettronica largamente utilizzato che sta pian piano soppiantando la moneta "tradizionale", soprattutto nelle spese quotidiane. Le monete elettroniche possono essere viste come stringhe codificate, mediante algoritmi di crittazione, che vengono caricate in delle smart card, oppure memorizzate in un PC. 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). Un'altra caratteristica della moneta elettronica (per lo meno nell'accezione classica di moneta) consiste nell'assenza di informazioni riguardo il proprietario di una moneta in particolare, ovvero a meno che non vi siano informazioni riguardanti il proprietario intrinseche nella rappresentazione digitale di una moneta, il suo possessore, attuale o passato, rimane anonimo. Da notare che la moneta elettronica potrebbe anche non essere legata al valore di una moneta reale. Un altro aspetto della moneta elettronica è che pagamenti con tale moneta possono essere effettuati anche tra persone non del tutto "fidate" (come avviene per i pagamenti in contante), a differenza di quanto avviene con le carte di credito in cui c'è sempre una banca che fa da intermediario fidato.

1.1 Requisiti di una moneta elettronica

I principali interessati alle caratteristiche di una moneta elettronica altri non sono che gli utenti di tale moneta, questi possono fondamentalmente essere divisi in due categorie: commercianti e acquirenti. Accanto a queste due categorie ce ne può essere un'altra, ovvero quella degli enti finanziari (qualora la moneta sia stata emessa da uno di essi). Acquirenti e commercianti possono essere accomunati su molti fronti in quanto spesso presentano gli stessi interessi, vediamo ora alcune caratteristiche che interessano queste due categorie di utenti.

La **sicurezza** è senz'altro un aspetto che interessa molto le due controparti di una compravendita. Per loro stessa natura i gettoni elettronici altro non sono che dati, quindi 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 di moneta elettronica. Alcuni esempi sono il problema del double-spending (spendere lo stesso gettone elettronico più volte), oppure la possibilità di impersonare un utente spendendo i suoi gettoni virtuali invece che i propri.

Un'altra caratteristica è l'**accettabilità**, ovvero quanto e da quanti una particolare moneta elettronica viene utilizzata. Ovviamente dal lato del commerciante adottare una moneta largamente accettata implica dare la possibilità a molti clienti di utilizzare tale moneta per acquistare i beni/servizi venduti, mentre l'utente ha possibilità di accedere a negozi (soprattutto online) dai quali prima non gli era possibile fare acquisti.

La **comodità** può essere vista come il numero di azioni fisiche ed il tempo da queste richiesto per effettuare un acquisto. Tale numero di azioni dovrebbe essere preferibilmente diverso in base alla cifra che si va a spendere, ovvero dovrebbe essere possibile fare piccole

spese in poco tempo e con poco sforzo, mentre per cifre maggiori sarebbe consono aumentare il numero di passi richiesti per effettuare la spesa.

Per quanto riguarda i **costi**, sarebbe preferibile non avere costi addizionali, in modo tale da non creare un limite minimo al valore delle transazioni. In questa categoria rientrano i costi sostenuti da cliente, commerciante e qualsiasi altro intermediario, nonché il tempo necessario per la gestione della transazione da parte di tutte le parti.

È importante per un servizio di moneta elettronica mantenere la **privacy** dei due attori della transazione, quindi, come per la moneta tradizionale, non dovrebbe essere possibile, da parte di una banca o di qualsiasi altro istituto finanziario, determinare se due transazioni sono state fatte dallo stesso utente.

La **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.

Accanto a queste caratteristiche ci sono quelle desiderabili da un eventuale istituto finanziario che emette la moneta elettronica (o un ente supervisore), ad esempio il **controllo immediato** su tutte le transazioni tramite l’accesso ad un sistema di gestione in modo tale da identificare ogni violazione della sicurezza prima possibile. Un’altra caratteristica desiderabile rappresenta la **tracciabilità** delle transazioni in modo tale da identificare il colpevole di un illecito, in particolare la tracciabilità è utile per verificare traffici internazionali di denaro ed evasione fiscale.

1.2 Compromessi

Tra le caratteristiche elencate prima ne abbiamo alcune che sono in ovvia contrapposizione, di conseguenza nella progettazione di un sistema di moneta elettronica si devono fare dei compromessi in base anche all’utilizzo che si prevede per la moneta stessa. Un’ovvia contrapposizione si ha tra tracciabilità e privacy: quando il sistema di moneta elettronica prevede un intermediario o un ente supervisore, questo cercherà di spingere per avere la possibilità di controllare i dati di ogni transazione eseguita, facendola passare come un servizio aggiuntivo dato all’utente per controllare le proprie transazioni.

Dal punto di vista dell’implementazione un esempio di scelta/compromesso da fare è la possibilità di avere un sistema online contro uno offline ovvero scegliere se verificare ogni transazione online, con i relativi tempi morti e problematiche in caso di assenza di connettività, oppure effettuare ogni transazione affidandosi solo alla sicurezza intrinseca del sistema di moneta virtuale. Nella versione offline si ha una maggiore somiglianza alla moneta tradizionale, inoltre si rende il sistema meno costoso non avendo necessità di un sistema intermediario che sia sempre in funzione, viene risparmiata banda altrimenti utilizzata per lo scambio di informazioni con l’intermediario (non avendo quindi problemi di bandwidth o assenza di connettività). D’altro canto la soluzione online è la migliore dal punto di vista degli istituti finanziari emittenti e/o supervisori, offrendo la tracciabilità ed il controllo desiderati sulle transazioni, come conseguenza di ciò la soluzione online rappresenta la più semplice soluzione al problema del double-spending.

Ancora sul lato implementativo si ha la possibilità di basare la moneta elettronica su strumenti hardware o su strumenti software. Una soluzione basata su un hardware dedicato potrebbe sembrare la soluzione migliore anche se fa sorgere alcuni problemi. L’utilizzo di una smart card (resistente alle manomissioni e che permetta l’utilizzo di funzionalità di sicurezza) aiuta nella risoluzione del problema del double-spending in un sistema offline (una volta che un gettone è stato speso questo viene cancellato dalla smart card), è molto flessibile ed ha un piccolo costo per transazione, tutte qualità desiderabili in un sistema pensato per le piccole e medie spese. L’utilizzo di tali dispositivi tuttavia non si adatta bene a spese di valore maggiore, infatti per transazioni elevate è necessaria una maggiore capacità di memorizzazione al fine di tenerne traccia per un periodo più lungo rispetto ad una spesa

di piccolo o medio taglio. Un secondo problema di questa soluzione è che questa richiede un hardware specifico (card reader) e l'adozione di tale hardware da parte dei consumatori, quindi un largo accordo tra i partecipanti. Inoltre queste smart card potrebbero essere caricate con dati (monete) non direttamente riconducibili all'effettivo proprietario ed utilizzabili senza l'impiego di una password, quindi la perdita o la distruzione della smart card implica la perdita dei soldi memorizzati in essa. Viene quindi a mancare la proprietà di durabilità e quindi l'adattabilità della soluzione a transazioni di grande valore. Inoltre il progresso tecnologico può rendere le smart card meno resistenti alla manomissione aprendo le porte a rischi per la sicurezza del sistema. Tra i vantaggi di un sistema software ci sono la reversibilità dei pagamenti in caso di frode e la possibilità di aggiornamento del sistema. Quest'ultima risulterà sicuramente più semplice in un sistema software rispetto a dover aggiornare gli apparecchi hardware di ogni utente che fa uso del servizio.

2. Bitcoin

Bitcoin è una moneta elettronica nata nel 2009 dal progetto di Satoshi Nakamoto. Questo progetto prevedeva la realizzazione di un sistema di moneta elettronica peer-to-peer, quindi con architettura distribuita, senza la necessità di un ente centrale. Per tenere traccia delle transazioni Bitcoin utilizza un database distribuito tra i nodi della rete mentre utilizza la crittografia per implementare misure di sicurezza per evitare l'impersonificazione ed il double-spending. I gettoni elettronici spendibili (identificati sempre con il nome di bitcoin o BTC) vengono memorizzati in un computer sotto forma di portamonete oppure salvati in server che offrono tale servizio di memorizzazione. Il trasferimento di bitcoin avviene tra due indirizzi Bitcoin ovvero tra due qualsiasi persone che abbiano a disposizione il software per l'utilizzo di questo protocollo. L'assenza di un ente centrale rende impossibile per qualunque autorità la manipolazione del valore dei bitcoin. Inoltre, dato che il massimo numero di monete disponibili in circolazione è stato fissato, il bitcoin non dovrebbe essere soggetto all'inflazione.

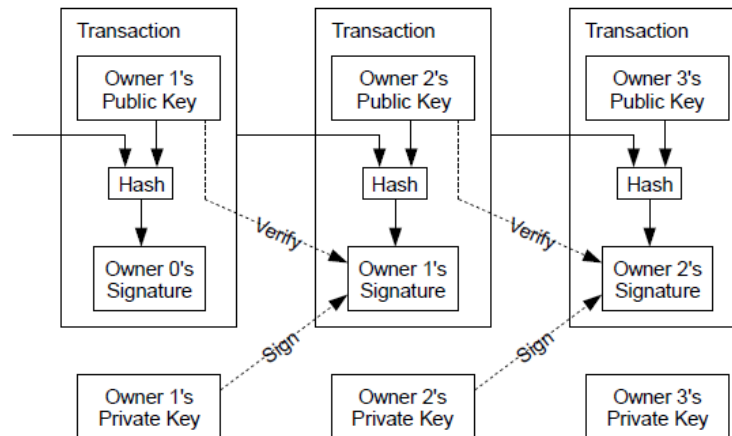
2.1 Architettura

Come detto precedentemente Bitcoin è basata su una rete peer-to-peer di nodi che cooperano al fine di mantenere corretto il funzionamento dell'intero sistema ed evitare attività non permesse. I bitcoin sono definiti come una catena di firme digitali, tali firme appartengono ai vari utenti che sono entrati in possesso e successivamente hanno speso quel gettone. Prima di illustrare il funzionamento dell'architettura Bitcoin, verranno descritti alcuni componenti alla base di essa.

2.1.2 Transazioni

La catena di firme digitali che rappresenta un bitcoin può essere divisa in transazioni: 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 decrittare 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 o meno 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

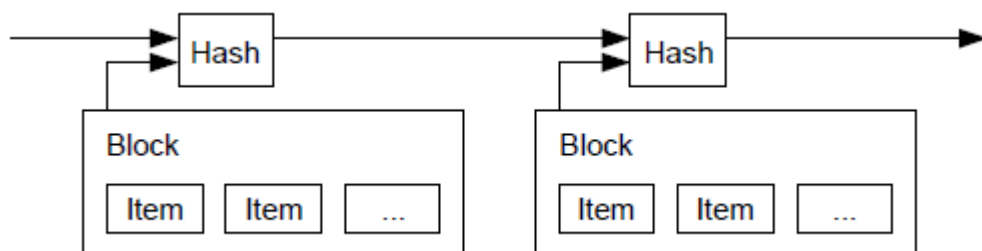
esclusivamente dal sistema zecca. Nell'architettura di Bitcoin si desidera evitare una soluzione centralizzata come questa, ma resta comunque la necessità di evitare il double-spending, ovvero si ha la necessità di controllare le ultime transazioni (le più problematiche per il double-spending).



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.

2.1.3 Timestamp Server

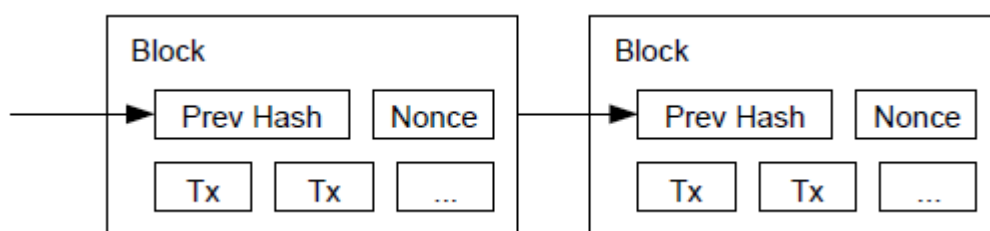
Il timestamp server viene utilizzato per annunciare pubblicamente l'accettazione di un blocco di transazioni. Questo server calcola l'hash di un blocco di oggetti annunciando successivamente il risultato calcolato. Tale sistema viene utilizzato per verificare che in un determinato istante una certa transazione era già avvenuta (in quanto faceva parte del blocco del quale è stato calcolato l'hash). Quindi viene utilizzato come "timestamp" l'hash calcolato sul blocco insieme 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, nella sezione successiva verrà spiegato il motivo di questo "spreco di risorse".

2.1.4 Proof-of-work

Al fine di implementare un timestamp server distribuito in una rete peer-to-peer verrà 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 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 il lavoro da capo. Successivamente maggiore è il numero di blocchi che verranno accettati (ovvero per i quali verrà trovata una soluzione) e 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-IP_address-one-vote) questa potrebbe essere sovvertita da chiunque sia in grado di istanziare più 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.

2.1.5 Funzionamento della rete

La rete Bitcoin funziona seguendo i seguenti passi:

- 1) Le nuove transazioni 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 come corretta la catena più lunga ed i nodi lavorano per estendere quest'ultima. 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, essa verrà presto inclusa in un blocco. Il broadcast dei blocchi rende il sistema tollerante alla 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.

2.2 Privacy

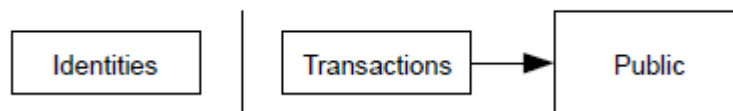
Nel modello di banca tradizionale la privacy è garantita non consentendo l'accesso alle informazioni che riguardano la singola transazione, in particolare, alle identità delle parti coinvolte e all'identità della terza parte di fiducia.

Traditional Privacy Model



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.

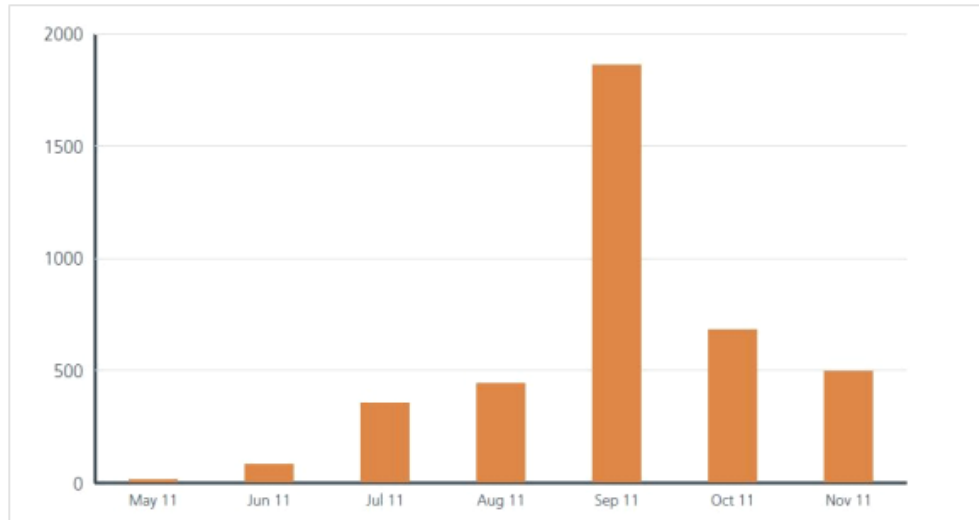
New Privacy Model



Inoltre, come misura aggiuntiva di privacy, per ogni transazione il sistema prevede anche la possibilità di utilizzare chiavi differenti. Questo chiaramente ci 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.

2.3 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, dandoci 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 ne è totalmente immune. Vediamone alcuni:

2.3.1 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 tool per effettuare mining¹. Questo tool conteneva un malware disegnato per far 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.

2.3.2 Denial of Service (DoS)

Un attaccante può pensare di portare il funzionamento della rete al limite delle prestazioni fino a renderla non più in grado di erogare il servizio.

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: $A \rightarrow B \rightarrow C \rightarrow A \rightarrow B \rightarrow C$. 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

¹ Con mining ci si riferisce all'azione di spendere potenza di calcolo al fine di trovare una soluzione per la POW al blocco attuale, nel caso si riesce a trovare la soluzione si percepisce un incentivo in BTC.

esempio utilizzando molti diversi indirizzi Bitcoin. 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.

2.3.3 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 quanto più la rete sarà grande, in quanto, richiederà che l'attaccante disponga di un numero di risorse più elevato.

2.3.4 Violazione degli algoritmi crittografici

Si tratta di una minaccia non immediata ma piuttosto a medio-lungo termine. Infatti, il protocollo di 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. Bisogna notare che tutta la sicurezza in internet (dalle banche alle comunicazioni segrete) dovranno essere riviste, perché basata sugli stessi algoritmi.

3. Conclusioni

La sfida sul futuro delle nuove tecnologie che utilizzano il web può essere riassunta come una lotta del controllo centralizzato contro una radicale decentralizzazione. Questa battaglia ha già mietuto vittime e rivoluzionato il mondo in una dozzina di diverse industrie, dagli editori ai dettaglianti, dal settore musicale alle aziende che sviluppano software.

Bitcoin è il primo esempio di critto moneta, realmente implementato, che con il suo sistema di tipo peer2peer ha aperto un nuovo fronte in questa battaglia, **decentralizzando la disponibilità di moneta** e togliendola dal controllo delle varie istituzioni finanziarie.

Durante il lavoro abbiamo visto come il bitcoin è una moneta che è basata su tecnologie informatiche che garantiscono un **robusto 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**, ovviamente, sono il fatto che Bitcoin potrebbe facilitare **operazioni illegali**, come ad esempio la vendita di materiale contraffatto o illegale. Di contro, però, abbiamo gli **aspetti positivi**: i cittadini onesti

che rispettano le leggi **possono portare avanti i loro affari senza nessuno che li possa controllare**. Volete donare denaro a WikiLeaks o a qualche altra organizzazione politicamente scomoda? Nessun problema. Vivete sotto un regime oppressivo e volete comprare un libro o un documentario censurati? Ecco come fare. Non c'è da meravigliarsi che la **Electronic Frontier Foundation**, l'organizzazione internazionale no profit di avvocati e legali rivolta alla tutela dei diritti digitali e della libertà di parola nel contesto dell'odierna era digitale, definisca Bitcoin come **“una moneta a prova di censura”**.

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", e questo punto non cambierà nel prossimo futuro. 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). Quindi pensare attualmente ad un punto vendita in bitcoin, che necessita di effettuare transazioni economiche rapide, risulta difficile.

Possiamo concludere dicendo 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 il bitcoin, come scritto nel suo sito ufficiale, non viola nessun accordo governativo e finanziario e perciò possiamo sostenere che la sua diffusione nei prossimi anni, allo stato attuale delle cose, sarà strettamente legata al numero di soggetti, aziende o enti che saranno disposti ad accettarla in cambio di cose e servizi utili.

Fonti

- Bitcoin: A Peer-to-Peer Electronic Cash System - <http://bitcoin.org/bitcoin.pdf>
- Bitcoin wiki - <https://en.bitcoin.it/wiki/Category:Technical>
- Wikipedia: Bitcoin - <http://en.wikipedia.org/wiki/Bitcoin>
- Wikipedia: Electronic Money - http://en.wikipedia.org/wiki/Electronic_money
- SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS - http://doc.utwente.nl/18925/1/survey_havinga.pdf