Alma Mater Studiorum · Università di Bologna

Campus di Cesena
Scuola di Ingegneria e Architettura

Corso di Laurea in Ingegneria Elettronica, Informatica e Telecomunicazioni

Bitcoin: aspetti tecnici, economici e politici di una crittovaluta

Elaborato in Sistemi Distribuiti

Relatore: Prof.
ANDREA OMICINI

Presentato da:
PIER FRANCESCO COSTA

Correlatore: Ing.
STEFANO MARIANI

I Sessione
Anno Accademico 2013/2014

"We choose to do these things,
not because they are easy,
but because they are hard."
- John F. Kennedy

Sommario

Bitcoin è una moneta digitale decentralizzata e parzialmente anonima. Viene scambiata tramite un software open source che utilizza la crittografia per garantire l'integrità e l'autenticità delle transazioni. Permette di inviare denaro digitale in maniera rapida, sicura ed economica attraverso Internet. La tesi si propone di analizzarne il fenomeno, partendo dalla sua storia fino alle possibili evoluzioni future. Vengono introdotte le basi di crittografia per comprenderne i concetti ed i meccanismi di funzionamento. In seguito viene analizzata l'implementazione del software e vengono discussi i principali vantaggi e criticità. La tesi esplora le possibili conseguenze di una sua adozione dal punto di vista economico e politico, e le innovazioni che potrebbe portare al sistema finanziario. Vengono infine mostrati alcuni esempi di software ispirati a Bitcoin che ne estendono ed ampliano le funzionalità nell'ambito dei sistemi distribuiti.

Indice

Introduzione

Ogni volta che affidiamo i nostri soldi ad una banca per inviare un bonifico, pagare online con carta di credito, ritirare contanti con il bancomat o semplicemente conservarli al sicuro, le stiamo dando fiducia. Fiducia che non fallisca, che i nostri soldi siano sempre disponibili su richiesta, che non vengano confiscati in maniera arbitraria. La fiducia che accordiamo riguarda anche i nostri dati personali, che non devono essere divulgati senza il nostro consenso. Se decidessimo di non concedere questa fiducia, potremmo comunque gestire il denaro in autonomia, tramite contante, ma avremmo molti svantaggi. Ad esempio non potremmo effettuare transazioni a distanza a costi bassi e in tempi brevi. Tutti i protocolli attuali hanno infatti la necessità di un ente terzo che garantisca la disponibilità delle parti coinvolte e verifichi la transazione.

Bitcoin nasce con l'obiettivo di permettere trasferimenti di denaro che non si basino sulla fiducia in una terza parte, ed è al tempo stesso un software distribuito, un protocollo ed una valuta. Si propone come una sorta di "contante digitale" che può essere scambiato tra gli utenti senza ricorrere ad intermediari, divenendo la prima forma di pagamento trustless.

L'obiettivo viene conseguito distribuendo una copia del database delle transazioni su ogni nodo della rete. Il database, che prende il nome di blockchain, tiene traccia di tutte le transazioni avvenute nella rete dal 1 gennaio 2009. I nodi sono connessi tra loro in modalità peer-to-peer, senza la presenza di server centrali. Questo tipo di architettura permette una notevole resilienza, flessibilità e rapidità di adattamento.

L'autenticità delle transazioni viene garantita da un meccanismo a firma digitale tramite chiave pubblica, garantendo che soltanto i reali possessori di una somma possano spenderla. Le transazioni vengono verificate, prima di essere immesse nella blockchain, da nodi speciali, denominati minatori.

I minatori svolgono il duplice ruolo di verifica della transazioni e di "emissione" dei bitcoin, anche se il termine, come vedremo più avanti, potrebbe essere fuorviante. La blockchain non viene aggiornata in tempo reale, ma viene aggiunto un gruppo di transazioni, chiamato blocco, ogni 10 minuti.

Ogni volta che viene aggiunto un blocco, viene emessa una quantità prestabilita di bitcoin , destinata al minatore che per primo è riuscito a verificarne la validità. Queste operazioni richiedono una notevole capacità di calcolo, perciò i minatori sono molti meno dei nodi totali della rete, ma il loro numero é comunque sufficiente a garantire la decentralizzazione della stessa.

Un'ulteriore caratteristica di Bitcoin è che l'emissione dell'omonima valuta, denominata di seguito BTC, è limitata, e cresce nel tempo asintoticamente fino a raggiungere il limite prestabilito di 21 milioni di unità. In questo modo il valore non può essere manipolato tramite l'inflazione, come invece può accadere con le valute tradizionali.

La trattazione fin qui fatta è volutamente generica, dato che i dettagli tecnici verranno analizzati seguito, ma serve per introdurre alcuni termini fondamentali per capirne la storia.

Capitolo 1

Crittovaluta: background

1.1 Storia

Bitcoin, come la maggior parte delle invenzioni, non nasce nel vuoto pneumatico, ma prende ispirazione da numerosi progetti precedenti.

Il problema di creare un'alternativa digitale al contante era già stato affrontato in vari paper di ricerca, tra cui *"Blind Signature for Untraceable Payments"* [1] di David Chaum e *"Minting Electronic Cash"* [2] di David Chaum e Stefan Brands, che si focalizzano su di un sistema ad emissione centralizzata, gestita ad esempio da una banca. Nel 1997 Adam Back inventò *"Hashcash"* [3], un software basato su proof-of-work[1] per prevenire lo spam via mail. Lo stesso anno, B-money [4] di Wei Dai e Bit-gold [5] di Nick Szabo cercarono di realizzare un sistema monetario basato sulla scarsità dei dati, la cui autenticità è garantita da una catena di proof-of-work.

Bitcoin venne presentato tramite un whitepaper pubblicato su Internet nel novembre del 2008 da un anonimo sotto il nome di Satoshi Nakamoto. *"Bitcoin: A Peer-to-Peer Electronic Cash System"* [6] descrive un sistema per trasferire denaro digitale senza l'utilizzo di istituzioni finanziare o servizi centralizzati, risolvendo per la prima volta il problema del double-spending[2] in maniera distribuita. In questo modo si può garantire l'indipendenza del sistema di pagamento da terze parti e aumentare il livello di riservatezza delle transazioni.

Il primo gennaio 2009 venne rilasciata la prima versione del client open-source. Iniziò anche la generazione dei primi blocchi. Il blocco 0, chiamato genesis block, contiene, tra le altre cose, la stringa: "*The Times 03/Ja-*

[1] Meccanismo per cui chi vuole usufruire di un certo servizio deve dimostrare di avere svolto una determinata quantità di lavoro.

[2] Tentativo fraudolento di inviare a più destinatari la stessa quantità di denaro.

n/2009 Chancellor on brink of second bailout for banks". Questa frase è il titolo della prima pagina del giornale inglese "*The Times*" che permette di postdatare la creazione del primo blocco, e alcuni vi vedono una velata critica alle istituzioni bancarie tradizionali.

Nei anni di sviluppo del progetto la difficoltà per generare BTC (sigla comunemente usata per indicare unità della valuta Bitcoin) era molto bassa, ed era quindi piuttosto facile ottenerne grandi quantità. Il loro valore non era però ancora rilevante, e non esistevano nemmeno siti, di seguito chiamati exchange, che permettessero il cambio con valuta tradizionale. Le prime compravendite avvenivano sul forum del progetto, `bitcointalk.org`. Una di queste diventerà in seguito famosa come la "pizza da 10.000 BTC" [7].

Il primo exchange divenne operativo nel luglio 2010 da Jed McCaleb (eDonkey2000, Overnet, Ripple) sul dominio mtgox.com.[3]

Ad agosto 2010 un grave falla [8] per la sicurezza venne trovata nel protocollo. Le transazioni non venivano correttamente verificate prima di essere incluse nella blockchain, e ciò avrebbe permesso ad un attaccante di generare una quantità arbitraria di BTC. La falla venne sfruttata pochi giorni dopo, prima dell'arrivo di una patch correttiva, e vennero generati dal nulla tramite un unico blocco 184 milioni di BTC. Nel giro di poche ore la falla venne chiusa e le transazioni annullate dagli sviluppatori.

Negli anni successivi il valore dei BTC aumentò sensibilmente passando da frazioni di dollaro a oltre $1200, e al momento (marzo 2014) è stabile attorno ai $600, dimostrando un'estrema volatilità. Nel 2011 varie associazioni hanno iniziato a ad accettare BTC per le donazioni. Ad esempio Wikileaks [9] li utilizzò per ovviare al blocco delle donazioni tramite carte di credito e PayPal, attuato da Visa e Mastercard su pressione del governo degli Stati Uniti.

Nel corso del 2012 e 2013 Bitcoin ha raggiunto sempre maggiore popolarità tra i commercianti, grazie sopratutto a payment processor come Bitpay e Coinbase, che permettono a qualsiasi sito o esercente di accettare BTC e convertirli con un cambio fisso in valuta locale.

Nel marzo 2013 un altro incidente coinvolge il protocollo Bitcoin. A causa di un bug non documentato presente nel database utilizzato in una vecchia versione dal client, avvenne un fork nella blockchain che durò diverse ore. Il problema venne risolto facendo migrare i minatori alla versione precedente del client, ma tutte le transazioni avvenute nel ramo "orfano" della blockchain vennero annullate.

[3] Doveva essere l'acronimo di "Magic The Gathering Online eXchange", ma il servizio di scambio carte collezionabili non uscì mai dalla beta, e il fondatore decise di riutilizzarlo come exchange per BTC.

Nell'ottobre 2013 venne chiuso Silk Road [10], sito per la compravendita su rete Tor di sostanze stupefacenti, materiale pericoloso e in generale di oggetti illegali in molte giurisdizioni. Il sito fungeva da luogo di incontro anonimo per venditori e acquirenti. Le comunicazioni avvenivano in maniera cifrata e i BTC erano utilizzati come strumento di pagamento, garantendo l'anonimato e la non tracciabilità. I prodotti venivano spediti utilizzando il sistema postale tradizionale. [11]

A febbraio 2014 Mtgox si dimostrò insolvente e dichiarò fallimento, con la perdita di oltre 800.000 BTC di proprietà degli utenti [12]. Durante l'anno precedente varie vicissitudini avevano incrinato la fiducia e la popolarità del servizio, ma in passato era stato uno degli exchange leader nel settore, raggiungendo il 70% del mercato.

1.2 Caratteristiche

Veloce ed economico In un'ora è possibile trasferire qualsiasi quantità di BTC a chiunque nel mondo a prezzi nell'ordine del centesimo di euro.

Pseudo-anonimo Chiunque può scaricare il software ed effettuare transazioni, senza registrarsi, senza comunicare dati personali e senza svelare la propria identità. Lo definiamo pseudo-anonimo in quanto se non si prendono determinati accorgimenti è possibile che le transazioni vengano comunque ricondotte all'identità dell'utente.

Nessuna autorità centrale Non dipende da nessuna organizzazione privata o ente governativo, e il valore dei BTC è liberamente contrattato sul mercato.

Irreversibile e non falsificabile Una volta che una transazione è stata effettuata ed è inclusa nella blockchain, non può più essere annullata, neanche dal mittente.

Impossibile da confiscare Soltanto l'utente ha la possibilità di muovere i propri BTC, nessuna autorità esterna può bloccarli o confiscarli senza il suo permesso.

Pensato per Internet I sistemi di pagamento tradizionali sono nati prima di Internet, e soffrono di difetti e problemi di sicurezza difficilmente risolvibili mantenendo la retrocompatibilità. Bitcoin nasce invece per essere utilizzato su Internet.

Inflazione determinata a priori L'emissione di nuovi BTC è determinata dall'algoritmo stesso del programma, e non può essere modificata.

1.3 Crittografia

Per capire molti meccanismi alla base di Bitcoin, è necessario introdurre alcuni concetti di crittografia. La crittografia è la scienza che studia come occultare informazioni. Si tratta di un argomento complesso, e per comprenderlo appieno è consigliabile consultare testi specifici [13]. Qui ci limiteremo ad accennare ad alcuni strumenti senza entrare troppo nel dettaglio.

La crittografia è usata principalmente per preservare la riservatezza delle informazioni ma non è la sua unica funzione. Nel contesto di Bitcoin non ci interessa tanto la segretezza dei dati, quanto l'autenticazione, l'integrità e la non ripudiabilità.

Autenticazione Chi riceve il messaggio è sicuro dell'identità del mittente

Integrità Chi riceve il messaggio è sicuro che questo non sia stato alterato.

Non ripudiabilità Chi invia il messaggio non può in seguito negare di averlo inviato.

Un algoritmo di firma digitale permette di ottenere le proprietà sopra descritte. Un altro strumento essenziale alla comprensione di Bitcoin è la funzione di hash.

1.3.1 Hash

Una funzione di hash accetta in ingresso un valore di lunghezza variabile e restituisce un valore di lunghezza fissa, di solito minore, chiamato valore di hash. Il valore di hash non dipende in maniera esplicita dall'ingresso, ma deve apparire come se fosse un valore casuale.

A questo scopo vengono utilizzati vari algoritmi, come MD5 e SHA. Ad esempio possiamo calcolare il valore di hash di una stringa utilizzando l'algoritmo SHA-1:

```
SHA1("Cantami o diva del pelide Achille l'ira funesta")
 = 1f8a690b7366a2323e2d5b045120da7e93896f47
```

anche solo cambiando un carattere qualsiasi della stringa in ingresso, il valore di hash calcolato è completamente diverso:

```
SHA1("Contami o diva del pelide Achille l'ira funesta")
 = e5f08d98bf18385e2f26b904cad23c734d530ffb
```

Se due file corrispondono bit a bit, avremo lo stesso valore di hash. Esiste la possibilità che due file diversi abbiano il medesimo valore di hash.

Questo evento si chiama collisione. La probabilità di collisione dipende solitamente dall'algoritmo di hash utlizzato e dalla lunghezza in bit del risultato. Maggiore la lunghezza, minore sarà la probabilità di collisione.

1.3.2 Crittografia simmetrica

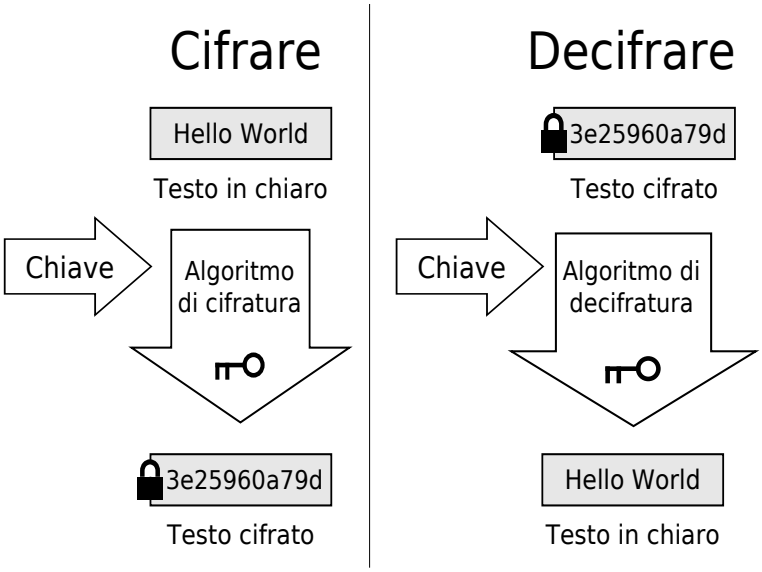

Figura 1.1: Crittografia simmetrica

La crittografia simmetrica, anche detta a chiave privata, è stata la prima forma di crittografia sviluppata dall'uomo. Per occultare un messaggio, in modo che sia leggibile solo dal destinatario, il mittente deve prima cifrarlo. Esistono vari algoritmi di cifratura, chiamati cifrari. Dato in ingresso all'algoritmo il messaggio in chiaro ed un'informazione segreta (di seguito chiamata chiave), l'algoritmo restituisce il messaggio cifrato. La chiave è l'unica informazione essenziale per decifrare il documento.

Per sviluppare un algoritmo sicuro, bisogna assumere che prima o poi diventi di pubblico dominio, e progettarlo in maniera tale che anche conoscendolo, i messaggi cifrati con tale algoritmo non siano decifrabili senza conoscere la chiave.[4] Il destinatario, anch'esso a conoscenza della chiave utilizzata, è quindi l'unico che può decifrarlo. Questo meccanismo prende il nome di crittografia a chiave simmetrica perché prevede che mittente e destinatario posseggano la medesima chiave, necessaria sia per cifrare che per decifrare. Esempi di algoritmi sono DES e AES.

[4]Principio di Kerckhoffs. [14]

E' facile accorgersi che la crittografia simmetrica comporta un problema non di poco conto nel campo della comunicazione a distanza: come fa il mittente a comunicare la chiave al destinatario, senza essere intercettato dall'attaccante? L'unico modo è quello di utilizzare un canale sicuro, a prova di intercettazione. Ma se questo canale non esistesse? Tralasciando gli algoritmi di negoziazione della chiave, esiste un genere di crittografia ideato appositamente per risolvere questo problema.

1.3.3 Crittografia a chiave pubblica

La crittografia a chiave pubblica, anche chiamata crittografia asimmetrica, permette di pensare in modo completamente diverso il problema. Viene creata una coppia di chiavi (keypair), una delle quali viene definita chiave privata, e l'altra chiave pubblica. La chiave privata viene generata casualmente, e da questa si ricava la chiave pubblica tramite una funzione unidirezionale, in modo che non sia possibile derivare la chiave privata da quella pubblica.

Gli algoritmi di crittografia a chiave pubblica funzionano in maniera particolare: richiedono una delle due chiavi per cifrare il messaggio, e l'altra per decifrarlo. In questo modo, se vogliamo inviare un messaggio cifrato, basta conoscere la chiave pubblica del destinatario. Solo questi potrà decifrare quindi il messaggio con la sua chiave privata. La crittografia a chiave pubblica viene usata, oltre che per scambi di messaggi cifrati, anche per implementare algoritmi di firma digitale. Un metodo è quello di calcolare il valore hash del documento e cifrarlo con la propria chiave privata. A questo punto è necessario allegare questo nuovo valore, che chiameremo firma, al documento. Per verificare la validità della firma è sufficiente decifrarla con la chiave pubblica e confrontarla con l'hash del documento. Se corrispondono la firma è valida.

Tra i vari algoritmi di firma a chiave pubblica, il più diffuso è RSA. Un altro metodo è denominato ECC (Elliptic Curve Cryptography) ed è basato sulle proprietà delle curve ellittiche. La firma digitale ci garantisce le tre proprietà fondamentali di autenticazione, integrità e non ripudiabilità.

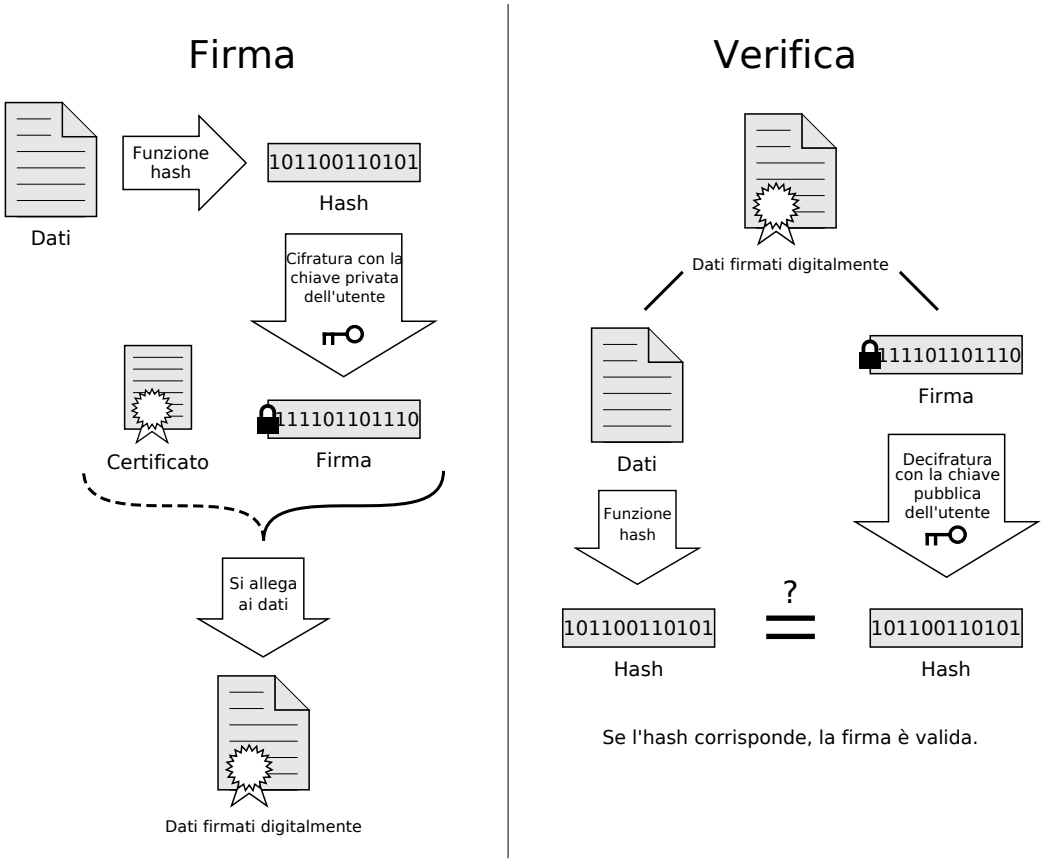

Figura 1.2: Firma a chiave pubblica

Capitolo 2

Bitcoin

2.1 Come funziona

Il problema principale che Bitcoin risolve è quello di garantire l'affidabilità di transazioni monetarie senza affidarsi ad un server centrale. Tradizionalmente si trasferisce denaro in maniera digitale tramite un server unico che gestisce il database con il bilancio e i dati degli utenti. L'utente che vuole inviare denaro si autentica in qualche modo sul server, e richiede di trasferire i propri fondi ad un altro utente. Il sistema quindi diminuisce dell'importo necessario il bilancio del mittente e aumenta dello stesso valore il bilancio dell'utente destinatario, garantendo che durante il trasferimento non venga mai generato o distrutto denaro. Varianti di questo metodo vengono utilizzate in ogni contesto finanziario, dalla banche tradizionali alle carte di credito, dai servizi online come PayPal ad agenzie per l'invio di denaro come Western Union.

Il primo problema da risolvere per poter fare a meno di un server centrale è quello dell'autenticazione. Dato un utente che che possiede un determinato bilancio, come si fa a garantire che solo quell'utente sia in grado di gestirlo e trasferirlo? Un possibilità è quella di utilizzare la firma digitale.

L'utente genera una coppia di chiavi pubblica e privata. Scrive un messaggio che contiene la quantità di denaro che vuole trasferire e la chiave pubblica del destinatario. A questo punto firma con la propria chiave privata il messaggio e lo invia. Il destinatario verificando la firma avrà quindi la prova crittografica del mittente, del destinatario e della quantità di denaro trasferita.

2.1.1 Indirizzi

Bitcoin utilizza il sistema di firma digitale ECDSA [15]. Le chiavi utilizzate da questo algoritmo sono piuttosto lunghe poco pratiche per l'utente finale.

Esempio di chiave pubblica:
041b43d5d4e9bab10f8b48dcb18677280cfa314f4c6c7dd4d8eb6f3
65e90077a6ac47085d5fb062f43468db66fb2ca40fb21e7e39fbd64
d39ba2c76c88a7c2dd75

Si è preferito utilizzare come identificatore del destinatario, al posto della chiave pubblica, un hash lungo 160 bit della stessa codificato in Base58Check [16], chiamato indirizzo. La codifica permette di verificare la correttezza formale dell'indirizzo al momento del suo inserimento.

Esempio di indirizzo:
31uEbMgunupShBVTewXjtqbBv5MndwfXhb

2.1.2 Transazioni

In Bitcoin una "moneta" digitale è rappresentata da una catena di transazioni. Ogni proprietario trasferisce la moneta firmando digitalmente l'hash della transazione precedente e della chiave pubblica del destinatario, attaccando il tutto alla fine della catena (vedi figura 2.1). Chi riceve il pagamento può controllare i vari passaggi di proprietà della moneta verificando le firme presenti in ogni transazione. La modifica di un'unica transazione invaliderebbe tutte le precedenti, in quanto gli hash non corrisponderebbero più.

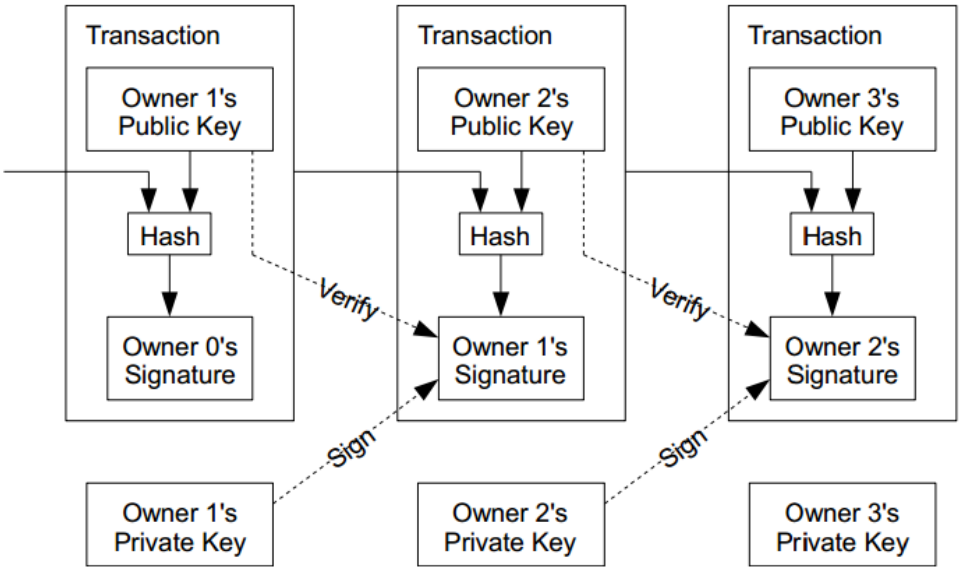

Figura 2.1: Catena di transazioni

In questo modo però chi riceve la moneta non può avere la certezza che uno dei precedenti proprietari non abbia inviato la stessa moneta a più persone, facendo in un certo senso biforcare la catena di transazioni. Il caso in cui una moneta venga spesa dallo stesso utente due o più volte in maniera fraudolenta è detto double-spending, è rappresenta uno dei più grossi problemi di un sistema di pagamento decentralizzato.

Un soluzione potrebbe essere quella di introdurre un'autorità centrale che controlli ogni transazione per prevenire tentativi di double-spending. Ogni moneta viene emessa direttamente da questa sorta di banca, e, quando un utente vuole trasferirla, viene inviata nuovamente alla banca, che la distrugge e consegna una nuova moneta al destinatario. Solo le monete emesse direttamente dalla banca sono ritenute affidabili, poiché al sicuro dal rischio di double-spending. Questo sistema reintroduce però la centralizzazione che si sta cercando di evitare.

L'utente che riceve una transazione deve quindi poter controllare che la moneta non sia stata già inviata a qualcun altro. L'unico modo, senza passare per un'autorità centrale affidabile, è che ogni utente sia a conoscenza di tutte le transazioni che avvengono nel sistema. Infatti se si accorge che una moneta è già stata inviata a qualcun altro prima che a lui, non la accetterà. Bisogna quindi che le transazioni siano pubbliche, ovvero che ci sia un unico storico delle transazioni condiviso tra tutti gli utenti, su cui questi siano d'accordo. L'utente che riceve la moneta deve insomma avere una prova crittografica che la maggioranza degli utenti era d'accordo sulla validità della transazione al momento dell'inclusione nella catena.

2.1.3 Timestamp

Bitcoin risolve il problema di datare le transazioni utilizzando un server di timestamp distribuito. Un server di timestamp calcola il valore hash dell'oggetto che vuole datare e lo pubblica su di un media affidabile, ad esempio su di un giornale. Il timestamp è la prova che l'oggetto esisteva prima che ne venisse calcolato l'hash. E' così possibile stabilire una datazione anteriore a quella di uscita del giornale in edicola. Ogni timestamp include, oltre all'oggetto che deve datare, anche il valore hash del timestamp immediatamente precedente, creando così una catena. L'ordine dei timestamp, e quindi quello della creazione degli oggetti, non può a questo punto essere modificato, a meno di non ricreare dall'inizio tutta la catena.

Per realizzare un sistema distribuito di timestamp, formato da tanti nodi in configurazione peer-to-peer, Bitcoin utilizza un sistema proof-of-work simile a Hashcash [3], che rende superflua la pubblicazione sul giornale. All'insieme di oggetti da datare viene aggiunto un numero, chiamato nonce, e se

ne calcola l'hash tramite l'algoritmo SHA-256 [17]. Questa operazione viene ripetuta cambiando nonce finché non si ottiene un valore hash che inizia con un determinato numero di zeri. Aumentando il numero degli zeri richiesti si aumenta esponenzialmente il lavoro medio richiesto per trovare un hash valido.

Regolando la difficoltà in maniera proporzionale alla potenza dei nodi collegati alla rete, si può fare in modo che l'intervallo con cui vengono generati i timestamp da parte della rete sia grossomodo regolare. Se la potenza della rete aumenta o diminuisce è sufficiente aumentare o diminuire la difficoltà.

Se qualcuno volesse cambiare la datazione di un oggetto, rimuovendolo da un timestamp e inserendolo in un altro, dovrebbe rifare il lavoro necessario a generare un timestamp valido senza il tale oggetto e tutti quelli successivi nella catena. L'unico modo per riuscirci è avere una potenza di calcolo maggiore della rete nel suo complesso.

2.1.4 Blockchain

La catena di timestamp utilizzata in Bitcoin viene chiamata blockchain. Ogni timestamp viene chiamato blocco, e contiene un numero variabile di transazioni. Il tempo medio di generazione di un blocco tende a 10 minuti. Il lavoro svolto per generare blocchi validi viene svolto da nodi chiamati minatori.

La blockchain è un database distribuito che contiene tutta la cronologia delle transazioni avvenute sulla rete Bitcoin. E' formata da una catena principale, e da blocchi chiamati orfani. Può capitare infatti che due blocchi vengano generati quasi contemporaneamente a partire dallo stesso blocco genitore. In questo caso ogni minatore decide quale sia il blocco valido, e lo utilizza per costruire il blocco successivo. Nasce così una divisione nella catena, e i due rami si continuano ad allungarsi indipendentemente l'uno dall'altro. Il ramo su cui si concentra la maggior potenza di calcolo cresce più velocemente dell'altro, finché i minatori "di minoranza" non abbandonano il ramo orfano. Le transazioni incluse da quest'ultimo vengono ignorate e la costruzione dei blocchi continua sul ramo principale.

Le dimensioni della blockchain crescono linearmente con l'aumentare delle transazioni. Alla data odierna occupa circa 14 GB. Sono allo studio sistemi per comprimerne la dimensione, come il pruning [6, 18, 19].

2.1.5 Protocollo

Di seguito una sintesi del funzionamento della rete Bitcoin e del lavoro svolto dai nodi minatori:

1. Le nuove transazioni vengono inviate a tutti i nodi (broadcast).
2. Ogni minatore controlla che le transazioni siano valide e le raccoglie in un blocco insieme all'hash del blocco precedente.
3. Ogni minatore lavora per trovare un proof-of-work valido per il proprio blocco.
4. Quando un minatore trova un proof-of-work valido, lo invia insieme al blocco a tutti gli altri nodi.
5. I nodi accettano il nuovo blocco solo se contiene transazioni valide e non incluse in altri blocchi precedentemente.
6. I minatori dimostrano di accettare il nuovo blocco come valido utilizzandone l'hash nel calcolo del proof-of-work del blocco successivo della catena.

I nodi minatori considerano sempre la blockchain più lunga come quella valida, e lavorano per estenderla. Nel caso due nodi trovino due differenti versioni dello stesso blocco contemporaneamente, ognuno trasmetterà la propria versione al resto dei nodi. Ogni nodo lavora sul blocco che ha ricevuto per primo, ma conserva l'altro nel caso diventi parte del ramo più lungo.

2.1.6 Minatori e incentivi

Ovviamente non ci si può aspettare che i nodi che svolgono il ruolo di minatori lo facciano gratis. Ogni blocco presenta una transazione aggiuntiva verso un indirizzo stabilito arbitrariamente dal minatore, contenente un numero di BTC definito dal protocollo. In pratica ad ogni blocco trovato dal minatore corrisponde una ricompensa in BTC. In questo modo non solo si garantisce un incentivo ai minatori proporzionale al lavoro svolto, ma si trova anche un criterio per l'emissione di nuovi BTC. Vengono così premiati i nodi della rete che maggiormente contribuiscono alla sicurezza del protocollo.

Vista la competizione tra i nodi nel cercare di ottenere una maggior ricompensa possibile, è naturale un incremento nel tempo della capacità di calcolo della rete (hashrate[1]), con un parallelo aumento della difficoltà richiesta risolvere un proof-of-work.

La quantità di BTC emessa da un blocco è predeterminata e si riduce geometricamente col passare del tempo, dimezzandosi ogni 210,000 blocchi (circa ogni 4 anni). La prima riduzione è avvenuta il 28 novembre 2012,

[1]Si misura in hash/s. Indica numero di valori di hash calcolati in un secondo.

con la ricompensa passata da 50 BTC a 25 BTC per blocco. Il prossimo dimezzamento (12.5 BTC) avverrà approssimativamente ad ottobre 2016.

Un altro tipo di incentivo è rappresentato dalla fee, una sorta di tariffa che il mittente può decidere di pagare per velocizzare le transazioni. Le transazioni che contengono una fee vengono generalmente processate con maggiore priorità, dato che i minatori hanno interesse ad includerle nei blocchi. Il valore della fee viene infatti trasferito al minatore che trova per primo il proof-of-work del blocco.

Le tasse sulle transazioni svolgeranno un ruolo preponderante in futuro, quando la generazione di nuovi BTC sarà trascurabile, e queste rappresenteranno l'unica forma di incentivo.

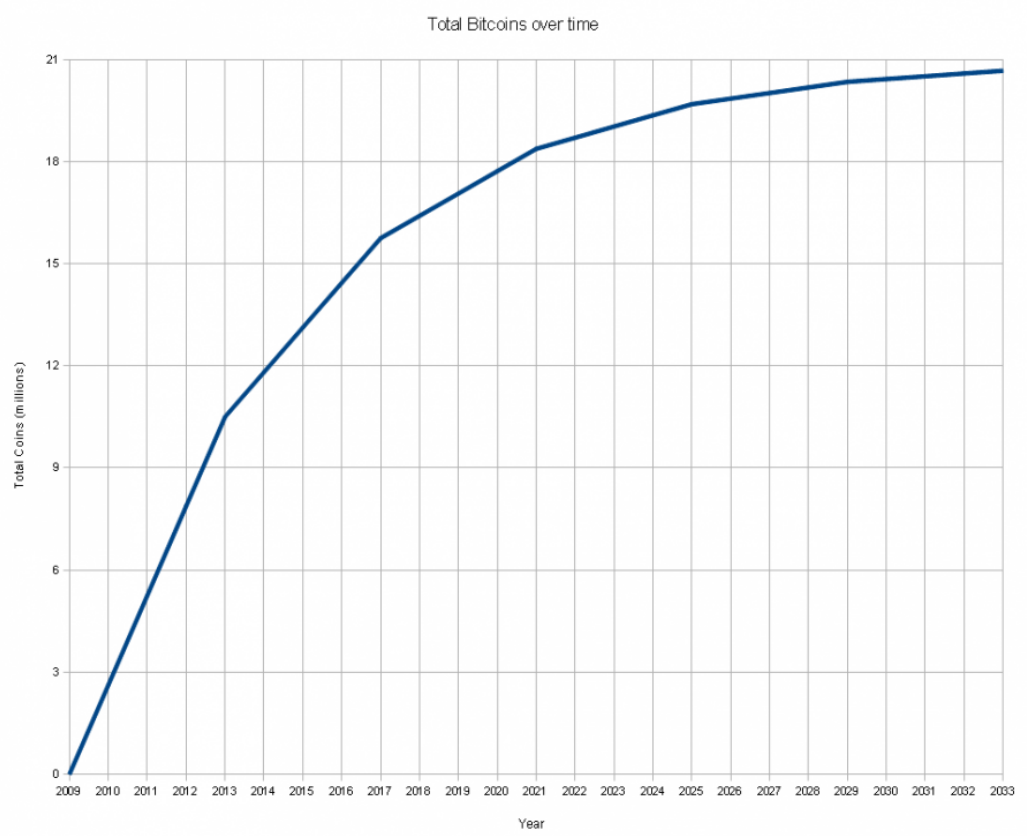

Figura 2.2: Quantità di BTC in circolazione

Se all'inizio, grazie ad una bassa difficoltà, bastavano un computer recente e una CPU veloce per minare svariati blocchi al giorno, nel corso degli anni è stato necessario passare all'utilizzo delle GPU, più veloci nei calcoli paralleli.

Successivamente si è passati all'utilizzo di FPGA[2] appositamente programmate per eseguire più velocemente il calcolo dello SHA-256. Nel 2013 sono stati rilasciati i primi dispositivi ASIC[3] appositamente realizzati per minare BTC, anch'essi in grado di sviluppare una potenza di calcolo svariate volte maggiore delle FPGA. Per fare un termine di paragone[4]:

Without specifying width for last column:

Dispositivo	Hashrate
CPU Intel Core i7 820	13,8 Mhash/s
GPU AMD Radeon 7870	460 Mhash/s
FPGA BitForce SHA256 Single	832 Mhash/s
ASIC CoinTerra TerraMiner IV	2.000.000 Mhash/s

Capacità di calcolo:

La corsa agli armamenti per realizzare dispositivi sempre più veloci ha portato la potenza globale del network a crescere esponenzialmente, fino a raggiungere, alla data attuale (30 marzo 2014), 39.573.889,99 Ghash/s. Espressi in altra unità di misura sarebbero 503.874,53 Petaflop/s.

Anche se non sarebbe corretto fare un confronto, visto che si tratta di una rete altamente specializzata in grado di eseguire solo hash, supera di gran lunga i più potenti supercomputer attualmente esistenti (i 500 supercomputer più potenti sviluppano una potenza totale di 250 Petaflop/s[5]) e la rete di calcolo distribuita più veloce (BOINC sviluppa 9,2 Petaflop/s[6]).

Lo sviluppo di ASIC sempre più efficienti ha aumentato enormemente la difficoltà, e il volume di denaro investito in apparecchiature per il mining ha raggiunto cifre record. C'è chi ha costruito delle vere e proprie mining farm in paesi con un basso costo della corrente elettrica (figura 2.3).

2.1.7 Quantità

Nel capitolo sulle transazioni abbiamo spiegato come venga trasferita la proprietà di una singola moneta alla volta. Siccome sarebbe poco pratico prevedere una transazione per ogni centesimo, in ciascuna transazione possono venire inclusi più input e output.

[2]Field Programmable Gate Array. Si tratta di schede integrate che possono essere programmate per svolgere determinati calcoli. Specializzate per eseguire un singolo algoritmo riescono a svolgere elaborazioni svariati ordini di grandezza più velocemente di CPU e GPU.

[3]Application Specific Integrated Circuit. Simili agli FPGA ma uno volta realizzati non possono essere riprogrammati.

[4]`https://en.bitcoin.it/wiki/Mining_hardware_comparison`

[5]`http://www.top500.org/lists/2013/11/`

[6]`http://boincstats.com/en/stats/-1/project/detail`

Figura 2.3: Mining farm negli Stati Uniti, stato di Washington [20]

Solitamente per trasferire BTC è necessario aggiungere in input diversi indirizzi, che sommati contengano una quantità maggiore o uguale alla quantità che vogliamo inviare. Vengono quindi aggiunti due output, uno con la quantità esatta verso l'indirizzo del destinatario, e l'altro che invia il "resto" della transazione ad uno degli indirizzi di proprietà del mittente.

In questo modo è possibile trasferire una qualsiasi quantità di BTC. Attualmente l'unità di misura più piccola è 0,00000001 BTC, denominata satoshi, ma modificando il protocollo è possibile aumentare indefinitamente la divisibilità dei BTC.

2.2 Come si usa

Dopo aver spiegato la logica di funzionamento, passiamo all'utilizzo pratico di Bitcoin. Esistono vari software sviluppati indipendentemente che permettono di collegarsi alla rete per inviare e ricevere BTC. Possiamo dividere i software in varie categorie: full clients, thin clients, signing only clients. Esistono anche alcuni servizi online che permettono di effettuare transazioni in BTC e mantenere un proprio saldo senza bisogno di scaricare alcun software sul proprio computer.

Le varie tipologie si differenziano per sicurezza, prestazioni, consumo di risorse e facilità di utilizzo.

2.2.1 Full clients

Si tratta di client Bitcoin tradizionali. Implementano interamente il protocollo Bitcoin: si collegano in modalità p2p agli altri nodi, scambiano blocchi e transazioni, salvano in locale una copia completa della blockchain, verificano tutte le transazioni ricevute e ne fanno il broadcast. Inoltre permettono all'utente di conservare sul PC le proprie chiavi private, la cronologia delle transazioni, il bilancio personale e una rubrica contenete gli indirizzi salvati. Sono tutti open source.

Solitamente offrono un'interfaccia grafica più o meno intuitiva, che permette di configurare il client e di effettuare e ricevere transazioni. Esistono varianti senza interfaccia grafica che si basano su linea di comando o API.

Uno dei principali svantaggi di un full client è la necessità di conservare sulla memoria locale l'intera blockchain, che attualmente (aprile 2014) ha raggiunto la dimensione di 16 GB[7]. Quest'operazione è necessaria per garantire il massimo livello di sicurezza, in quanto affidarsi a blockchain salvate in remoto su server di terze parti espone ad un certo livello di rischio, che seppure basso, è comunque presente.

I principali full client disponibili sono: Bitcoin Core [21], bitcoind (adesso integrato in Bitcoin Core) e GoCoin [22].

Bitcoin Core

Bitcoin Core (prima conosciuto come Bitcoin-qt o Satoshi Client) nasce per primo, sviluppato a partire dal codice di Satoshi Nakamoto, rilasciato sotto licenza MIT. Disponibile per Windows, Mac e Linux è il client più utilizzato, ma sta venendo soppiantato da altri software più agili e userfriendly.

L'interfaccia è spartana ed essenziale, e permette di gestire il proprio portafoglio di BTC. Le chiavi pubbliche e private vengono salvate automaticamente, una volta generate, nel file wallet.dat, assieme alla rubrica degli indirizzi. Il wallet può essere cifrato per aumentare il livello di sicurezza, ma rimane essenziale mantenere il PC su cui si trova installato al sicuro da minacce.

Il software tiene traccia delle transazioni effettuate sotto la scheda transactions. E' possibile visualizzare il numero delle conferme per ogni transazione. Questo rappresenta il numero di blocchi minati successivamente all'inclusione della transazione in un blocco.

Esiste una modalità di debug che permette di eseguire comandi attraverso un interprete a linea di comando integrato.

[7] `https://blockchain.info/charts/blocks-size`

Il primo avvio richiede la sincronizzazione della blockchain, che su di un computer di fascia media richiede più di una settimana, dato che ogni blocco scaricato dalla rete deve essere verificato. Questo rappresenta un notevole ostacolo per un nuovo utente, che potrebbe scoraggiarsi. Si preferisce quindi consigliare ai principianti software più agili, come i thin client.

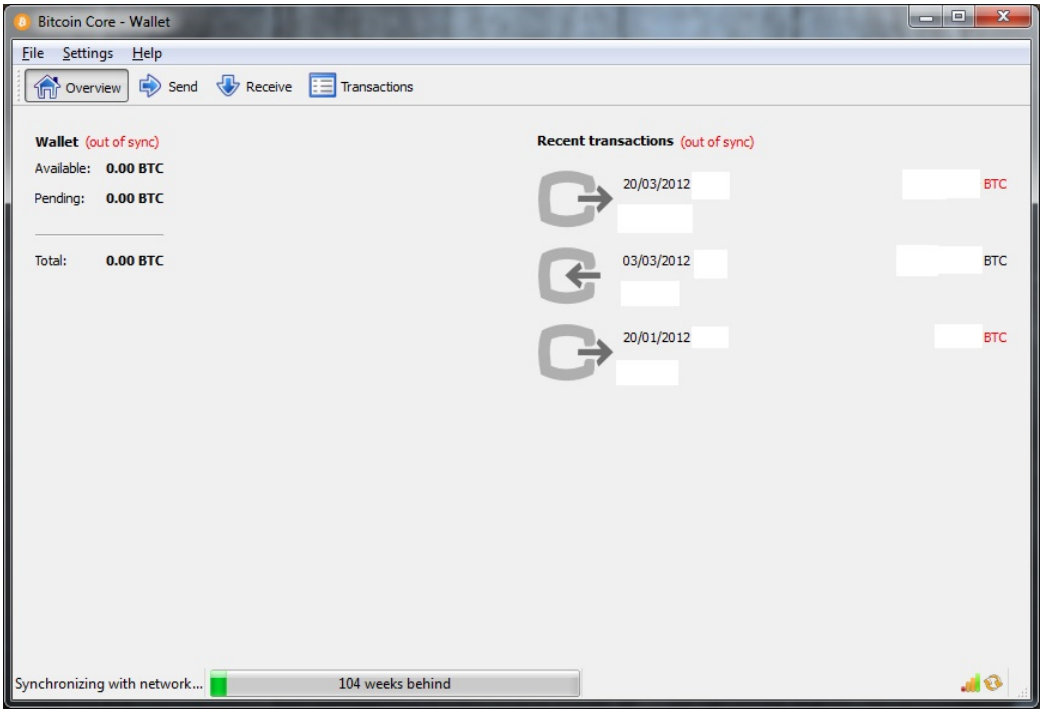

Figura 2.4: Interfaccia utente di Bitcoin Core 9.1

2.2.2 Thin clients

I thin client, al contrario, non scaricano né verificano l'intera blockchain, garantendo un consumo di risorse molto minore e la possibilità di utilizzare il software non appena installato. Permettono inoltre di accedere alla stragrande maggioranza delle funzionalità dei full client (inviare e ricevere BTC, visualizzare il bilancio, tenere una rubrica etc.).

Per verificare la validità delle transazioni senza scaricare l'intera blockchain esistono varie tecniche, tra cui la più sicura e utilizzata è la Simple Payment Verification (SPV), introdotta da Satoshi nel whitepaper originale [6, 23]. Il client si limita a collegarsi a diversi full client, che ritiene affidabili. Quindi controlla che la transazione si trovi sufficientemente in profondità nella blockchain, contando il numero di blocchi che la separano dall'ultimo. In

questo modo presume che la transazione sia valida, visto che è stata accettata da tutti gli altri nodi affidabili.

Questo schema di verifica è comunque vulnerabile nel caso un attaccante abbia il controllo della connessione ad Internet dell'utente. Il quale potrebbe indurre il client a collegarsi a nodi malevoli, che gli fornirebbero una porzione alterata della blockchain.

I principali thin client sono: Electrum [24], bitcoinj [25] e Multibit [26].

2.2.3 Signing only clients

Esiste un'altra categoria di client, che non svolge il ruolo di nodo nella rete Bitcoin, ma si occupa solo di conservare le chiavi dell'utente. Questi client vengono chiamati signing only, in quanto si occupano solo di firmare le transazioni con la chiave privata. Questo permette di avere prestazioni e efficienza molto superiori rispetto agli altri tipi di client.

La loro grande praticità è controbilanciata da un modello di sicurezza meno robusto, in quanto si affidano completamente ad un server gestito da una terza parte, che ospita un full client. Non avviene nessun tipo di verifica sulla validità delle transazioni. Il server è gestito dallo sviluppatore del client, che ha il controllo completo delle transazioni che l'utente riceve, e quindi può fargli credere di avere più o meno BTC rispetto al suo saldo reale, oppure può trasmettergli uno storico delle transazioni fittizio. Nel caso il client non sia compromesso, non è comunque in grado di rubargli BTC.

Grazie alle poche risorse richieste, è possibile realizzare client signing only per qualsiasi piattaforma. Alcuni esempi sono: Mycelium (applicazione mobile Android), Blockchain.info e Greenaddress.it.

Nel caso delle web application, le operazioni crittografiche di firma vengono eseguite in locale, all'interno del browser tramite JavaScript, in modo che le chiavi private non vengano mai mandate in chiaro al server. Nonostante tutte queste precauzioni, chi gestisce il server potrebbe comunque inviare al browser codice JavaScript malevolo per farsi inviare le chiavi private. L'utente potrebbe accorgersene solo controllando il codice sorgente ogni volta che accede al sito, ma si tratterebbe di una grande scomodità. In ogni caso, fino ad ora (aprile 2014), non si conoscono attacchi realizzati con questo metodo.

2.2.4 Web wallet

Un web wallet non è altro che un servizio web che si occupa di gestire i BTC al posto dell'utente. Permette a chiunque di aprire un'account su cui autenticarsi tramite username e password. E' possibile depositarvi BTC tramite un

indirizzo legato al proprio account e utilizzarne l'interfaccia grafica per decidere a chi mandarli. Il gestore del servizio in questo modo ha la disponibilità completa dei BTC degli utenti, come se fosse una banca tradizionale.

Un tempo piuttosto popolari, sono sempre meno usati, soprattutto a causa di problemi legati alla sicurezza e alla poca affidabilità dei gestori. Per esempio servizi con migliaia di utenti come Instawallet[8] e MyBitcoin[9] si sono rivelati inaffidabili o sono spariti con i soldi degli utenti.

La maggior parte dei web wallet è oggigiorno integrata nei servizi offerti dagli exchange, che per loro natura devono avere il controllo dei BTC scambiati dai propri utenti.

2.2.5 Exchange

Vari servizi, chiamati exchange, permettono di scambiare BTC con valuta tradizione, e viceversa. E' necessario trasferirvi danaro, tramite bonifico o altro metodo di pagamento non reversibile, oppure BTC, e quindi effettuare uno scambio tramite il motore di trading interno.

Soffrono spesso di problemi di sicurezza, principalmente a causa della scarsa professionalità degli operatori e per il fatto che rappresentano la preda più facile per criminali e malintenzionati. E' consigliabile utilizzarli solo per il tempo necessario ad effettuare conversioni, e non per conservare grandi somme di denaro.

La maggior parte degli exchange si sta dotando di procedure di identificazione dell'utente tramite documenti e prove di residenza, per soddisfare i vari regolamenti nazionali sul riciclaggio di denaro. Di conseguenza è difficile acquistare BTC in maniera anonima. I principali exchange che accettano dollari o euro sono: Bitstamp[10], Bitfinex[11] e BTC-E[12].

[8] `https://en.bitcoin.it/wiki/Instawallet`
[9] `https://en.bitcoin.it/wiki/MyBitcoin`
[10] `https://www.bitstamp.net/`
[11] `https://www.bitfinex.com/`
[12] `https://btc-e.com/`

Capitolo 3

Vantaggi e limiti

3.1 Costi

Trasferire denaro utilizzando BTC è più rapido ed economico rispetto ai più comuni sistemi di pagamento che utilizzano valute tradizionali, specialmente nel caso di pagamenti internazionali. E' possibile inviare BTC senza alcuna commissione, ma si consiglia comunque di pagare una fee, in modo da incentivare i minatori ad includere la transazione in un blocco il prima possibile. Ad aprile 2014 la fee consigliata era di 0,0001 BTC, al cambio 0,04 €.

Nella seguente tabella possiamo confrontare i costi e i tempi dei sistemi di pagamento internazionali più usati. I costi sono quelli più diffusi e potrebbero variare in base al paese in cui si usufruisce del servizio.

Strumenti di pagamento	**Costi mittente**	**Costi destinatario**	**Tempi**
Bitcoin	0,04 €	nessuno	pochi secondi - 60 minuti
Bonifico SEPA	0-5 €	nessuno	un giorno
Bonifico SWIFT	25-65 $	15 $	3-4 giorni
Carta di credito	nessuno	1,5-3%	pochi secondi
Paypal	nessuno	1,8-3,4%+0.35 €	pochi secondi
Western Union	5-10%	nessuno	pochi minuti
Vaglia postale	5%	nessuno	7/10 giorni

Nella tabella non sono state prese in considerazione le commissioni di cambio da valuta tradizionale a BTC e viceversa. La maggior parte degli exchange applica una maggiorazione vicina allo 0,5%.

Come si può vedere, Bitcoin è nettamente il sistema più economico, e uno tra i più rapidi. In velocità non riesce comunque a superare le carte

di credito, in quanto è necessario attendere almeno 10 minuti affinché una transazione sia inclusa in un blocco. Si può comunque decidere di accettare una transazione non confermata, se l'importo è di modesta entità.

I micropagamenti al di sotto di 1 € rappresentano un tallone d'Achille per Bitcoin, in quanto il costo fisso della transazione rappresenta una percentuale importante del valore.

3.2 Irreversibilità

Le transazioni effettuate tramite Bitcoin sono per loro natura irreversibili, ovvero, una volta incluse nella blockchain, non possono essere annullate dal mittente. L'unico modo per ritornare in possesso del proprio denaro è quello di farsi rimandare indietro i BTC dal destinatario. I soli sistemi di pagamento irreversibili e accessibili al grande pubblico sono Western Union, vaglia postale e bonifico internazionale. Non a caso, i primi due prevedono l'utilizzo del contante (anch'esso irreversibile) da parte del mittente. E' infatti molto rischioso offrire un un sistema di trasferimento di denaro irreversibile che accetta metodi di pagamento reversibili, come carte di credito. Pertanto Bitcoin è l'unico sistema di pagamento elettronico realmente irreversibile.

La mancanza di altri strumenti che abbiano una proprietà in apparenza così semplice da realizzare, non è casuale, ma è dovuta a motivi di natura sia legale che commerciale. Infatti nella maggior parte dei paesi al mondo, in primis in Europa e Stati Uniti, esistono leggi a tutela dei consumatori che prevedano, in caso di frode o di utilizzo non autorizzato del mezzo di pagamento (es. furto della carta di credito), che sia il gestore del sistema di pagamento a risarcire il consumatore.

Chi si accolla la perdita è l'esercente che aveva ricevuto il pagamento, che viene annullato (in gergo viene effettuato un chargeback). Ciò può avvenire, oltre che per una colpa del commerciante, come nel caso di merce difettosa o non spedita, anche se questi si comporta onestamente, ma la carta con cui viene pagato risulti rubata.

Per un commerciante Bitcoin rappresenta quindi un metodo di pagamento molto più sicuro ed affidabile, e lo mette al sicuro da tentativi di chargeback fraudolenti. E' d'altra parte più rischioso per l'acquirente, in quanto non fornisce alcun tipo di protezione dalle frodi, e non esiste una società a cui rivolgersi in caso di problemi.

E' possibile in ogni caso mitigare e bilanciare il rischio utilizzando sistemi di intermediazione e di risoluzione delle controversie (comunemente chiamati escrow [27]) a cui gli acquirenti e i venditori possono rivolgersi volontariamente.

3.3 Anonimato

Caratteristica molto pubblicizzata di Bitcoin è l'anonimato, anche se sarebbe meglio parlare di pseudoanonimato. Nonostante il database delle transazioni sia pubblico e accessibile a tutti, questo non fornisce alcun legame tra gli indirizzi delle transazioni e l'identità reale di chi li controlla. Il fatto che chiunque possa generare le proprie chiavi private e indirizzi, e iniziare ad utilizzare la rete Bitcoin senza fornire ad alcuna società i propri dati, garantisce un livello di privacy paragonabile a quello del denaro contante, che non viene offerto da nessun altra strumento di pagamento o istituzione finanziaria.

Se a questo anonimato iniziale uniamo però la tracciabilità garantita dalla blockchain, ci rendiamo conto che nella maggioranza dei casi è piuttosto facile identificare il proprietario di un indirizzo. Infatti il modo più semplice per un utente di procurarsi BTC è quello di acquistarli con valuta tradizionale presso un exchange. Molti di questi servizi sono obbligati per legge a verificare l'identità dei propri clienti (in quasi ogni stato esistono leggi antiriciclaggio). L'exchange è quindi in possesso dell'identità dell'utente e può associarla all'indirizzo su cui cui vengono depositati i BTC acquistati.

Con questi dati è molto facile facile seguire il flusso di denaro attraverso i vari indirizzi. Nel caso l'utente fornisca informazioni false all'exchange è comunque identificabile tramite i bonifici o altri mezzi di pagamento non anonimi che utilizza per depositare valuta tradizionale.

Esiste anche un framework, BitIodine [28], in grado di etichettare automaticamente gruppi indirizzi appartenenti alla stessa persona, metterli in relazione con liste di indirizzi pubblici e permette di seguire manualmente le singole transazioni in maniera intuitiva.

Ci sono tuttavia metodi per far perdere le proprie tracce e aumentare il livello di anonimato delle transazioni.

3.3.1 Mixer

Un mixer è un servizio che permette di rendere non tracciabili le transazioni Bitcoin. L'utente deposita BTC sul wallet che offre il servizio, e poi li trasferisce su di un altro indirizzo, pagando una commissione. I BTC ricevuti non sono in realtà gli stessi depositati, ma appartengono ad altri utenti del servizio. In questo modo è possibile ottenere BTC non associati alla propria identità reale su qualunque indirizzo.

Questo approccio mostra tuttavia alcuni limiti. Il servizio può tenere traccia delle operazioni e degli indirizzi degli utenti, permettendo a chi entra in possesso dei log di ricostruire i legami tra i vari indirizzi. Un altro serio problema è che il gestore del servizio potrebbe rubare i BTC che gli vengo-

no affidati dagli utenti. Anche nel caso si tratti di una persona onesta, il servizio sarebbe comunque un bersaglio molto appetibile per cybercriminali malintenzionati. La quantità di BTC presenti sul wallet deve infatti essere abbastanza grande per garantirne il funzionamento. Per questo motivo vengono comunemente utilizzati come mixer anche i wallet offerti dai grossi exchange che non richiedono identificazione per le sole transazioni in BTC.

I limiti dei mixer tradizionali stanno venendo superati da nuovi protocolli di mixing p2p[1], come Coinjoin [29], SharedCoin [30] e CoinSwap [31]. Questi sistemi permettono di rendere anonime le transazioni senza utilizzare mixer di terze parti, eliminando il rischio di essere derubati dal gestore del server.

3.4 Scalabilità

Uno dei dubbi maggiori riguardo al futuro di Bitcoin è il problema della scalabilità. Sono state fatte varie analisi nel corso del tempo, alcune anche molto critiche [32]. Ci si chiede infatti se con un aumento esponenziale degli utenti e delle transazioni, sarà possibile installare, sincronizzare e mantenere attivo un nodo completo su di un normale computer di fascia media. Questo requisito è da alcuni ritenuto essenziale affinché il protocollo si possa considerare realmente distribuito e decentralizzato.

Un'analisi quantitativa è stata realizzata sulla wiki ufficiale [33]. E' stato preso come metro di paragone il circuito per carte di credito internazionale Visa, che processa in media circa 2000 transazioni al secondo(tps). Il picco massimo delle transazioni su rete Bitcoin è stato raggiunto a dicembre 2013 con 100.000 transazioni in un giorno [34], ovvero 0,86 tps. Attualmente esiste un limite nella dimensione dei blocchi di 1 MB, che permette di raggiungere al massimo 7 tps, per evitare che la rete venga inondata di moltissime transazioni di scarso valore. Eventualmente questo limite potrà essere alzato. Nel caso Bitcoin raggiungesse il volume di 2000tps sono stati calcolati i vari requisiti per eseguire un nodo completo.

Capacità di calcolo E' il parametro meno critico, in quanto anche una CPU Intel Core i7 da 2,2Ghz può facilmente elaborare la mole di lavoro richiesta.

Connessione ad Internet Anche questo requisito non desta preoccupazioni, in quanto il flusso di dati diretto verso il nodo dovrebbe essere di circa 8 megabit al secondo, gestibile con le attuali connessioni ADSL residenziali.

[1] `http://www.coindesk.com/taxonomy-bitcoin-mixing-services-policymakers/`

Capacità di storage E' il collo di bottiglia. Attualmente lo spazio necessario per la blockchain è di 14 GB, ed è destinato a crescere linearmente con il numero di transazioni. A 2000tps richiederebbe 72 GB al giorno per un totale di oltre 2 Terabyte al mese. Esistono progetti per ridurre le dimensioni della blockchain e ridurre i dati richiesti per la semplice verifica delle transazioni, ma al momento non sono ancora stati implementati.

In caso di rapida crescita del numero delle transazioni, i requisiti di memoria rappresenterebbero quindi un'ostacolo per la scalabilità. Se l'aumento avvenisse più rapidamente dell'evoluzione tecnologica predetta dalla legge di Moore [35], sarebbe difficile per il singolo utente mantenere un nodo completo attivo su di un PC domestico. I costi sarebbero quindi elevati e supererebbero i vantaggi (maggiore sicurezza), facendo probabilmente migrare la maggior parte degli utenti non professionali verso thin client e soluzioni web-based, con tutte le conseguenza sulla decentralizzazione e diversificazione della rete che ne conseguono.

Le aziende che adottano Bitcoin come metodo di pagamento e quelle che lavorano nell'ecosistema potrebbero comunque permettersi di mantenere attivi dei full client, per avere maggiore indipendenza, personalizzazione e sicurezza.

Alcuni vedono il passaggio della responsabilità della rete dall'utente all'azienda come una progressiva centralizzazione, che porterebbe la rete Bitcoin a diventare sempre più simile al sistema bancario attuale. Bisogna però evidenziare che si tratterebbe in ogni caso di un modello molto più aperto alla concorrenza e democratico dell'attuale settore bancario. Facendo di Bitcoin un servizio di denaro elettronico con un grado di decentralizzazione molto maggiore rispetto alle alternative.

3.5 Vulnerabilità

Come in ogni software, così anche Bitcoin soffre di falle e vulnerabilità. E' utile suddividerle in due categorie. Vulnerabilità insite nel protocollo e falle nell'implementazione.

3.5.1 Protocollo

Le prime sono le più conosciute ma anche le più difficili da risolvere, in quanto modificare il protocollo significa cambiare le regole per l'intero sistema. Se tutti gli utenti e miner non accettano le nuove regole all'unanimità aggiornando il software alla versione corretta, si può creare un fork della blockchain,

con un ramo che segue le nuove regole e un altro che segue le vecchie, di fatto minando alla base l'unità della piattaforma Bitcoin. Gli sviluppatori cercano quindi di limitare al minimo le modifiche al protocollo.

Nel corso degli anni sono stati proposti vari miglioramenti al protocollo, denominati BIP(Bitcoin Improvement Proposals) [36].

Esistono d'altra parte vulnerabilità insiti nel paradigma stesso del progetto Bitcoin, e non possono essere modificati, a meno di non volerne stravolgere la natura.

Una di queste debolezze è la vulnerabilità ad un attacco 51%.

Attacco 51%

Un attaccante che gestisca più del 50% della potenza di calcolo potrebbe battere il resto della rete nella costruzione di una blockchain più lunga, provocando così un fork. Questo gli permetterebbe di modificare l'ordine delle transazioni o escluderle arbitrariamente. Potrebbe quindi annullare transazioni che ha fatto in passato e spendere più volte, fraudolentemente, gli stessi BTC.

Si ritiene che sia più redditizio, per chi ha una potenza di calcolo così elevata, utilizzarla per minare nuovi blocchi ottenendo la ricompensa, piuttosto che effettuare una attacco di questo tipo. Un attaccante non interessato ad arricchirsi potrebbe comunque fare grossi danni.

L'eventualità che un solo soggetto controlli più del 50% dell'hashrate della rete, seppur inedita, non è così remota. La maggioranza dei minatori infatti non lavora più in solitario, ma si unisce ad altri minatori per formare una mining pool. La funzione di una mining pool è quella di unire gli sforzi di tanti minatori, suddividendo in seguito l'eventuale ricompensa tra tutti i partecipanti in funzione del lavoro svolto. In quanto tutti i minatori afferenti ad una mining pool cedono di fatto la loro capacità di calcolo al gestore della stessa, dal punto di vista della rete viene vista come un inico nodo. E' possibile che raggiunga un hashrate molto elevato, ed è già successo che un singola pool superasse, anche se per poco tempo, il 50%.

Esistono altri difetti del protocollo, ma il loro studio porterebbe via molto spazio, per cui ci limitiamo a citare la wiki ufficiale [37].

3.5.2 Implementazione

Le falle presenti nell'implementazione, anche se di solito facilmente correggibili, sono più difficili da trovare e per questo molto insidiose.

Ogni nuovo aggiornamento dei client, in particolare Bitcoin Core, viene testato per sicurezza su una rete denominata Testnet, che ricalca in tutto e

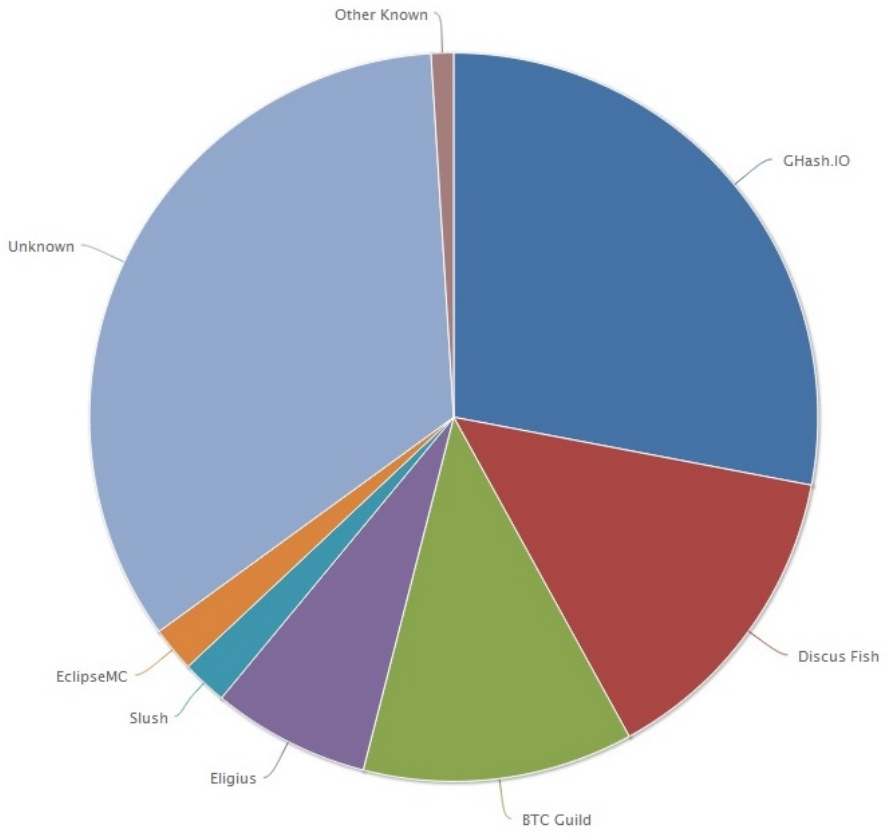

Figura 3.1: Distribuzione dell'hashrate tra le varie pool.

per tutto la rete Bitcoin, pur avendo una blockchain incompatibile [38]. Tutti i client sono open source, e il codice è liberamente disponibile per controllare la presenza di bug, ma nonostante questo a volte emergono problemi seri.

Output Overflow

Si tratta del primo e più grave bug scoperto nel client ufficiale [39]. Durante l'agosto 2010 un falla (overflow) nel processo di verifica della validità delle transazione inclusa nel blocco 74.638 permise ad un attaccante di generare 184 milioni di nuovi BTC e di mandarli a due indirizzi diversi. La transazione fraudolenta venne velocemente individuata nel blocco, il bug isolato e la versione corretta della blockchain ripristinata nel giro di 5 ore.

Blockchain Fork

L'11 marzo 2013 una transazione particolarmente grande provocò un fork nella blockchain[2]. La causa è da ricercarsi nel database del client ufficiale. Con l'uscita della versione 0.8 venne infatti cambiato il tipo database utilizzato per la memorizzazione delle transazioni, passando da BerkeleyDB al più efficiente LevelDB. Per ragioni tecniche i due database erano stati erroneamente configurati per gestire transazioni di dimensione massima differente.

Nonostante il comportamento delle due versioni dovesse essere identico, la versione 0.7, usata dalla stragrande maggioranza dei minatori, non accettava come valide le transazioni più grandi di 256 KB, mentre la versione 0.8 le accettava. Perciò, quando il blocco numero 225.430, più grande di 256 KB, venne minato, una parte della rete lo vide come valido e un'altra parte lo ignorò, continuando a lavorare per trovare un blocco alternativo. Questo diede origine ad un fork e a due rami di blockchain incompatibili tra loro.

Il problema venne individuato nelle ore successive e gli sviluppatori decisero per il minore dei mali: venne chiesto alle mining pool che utilizzavano la versione 0.8 di effettuare un downgrade alla versione 0.7, in modo da permetter ad una delle due blockchain di prevalere sull'altra. Cosa che avvenne nel giro di 6 ore. In seguito venne predisposto un piano di migrazione alla versione 0.8 limitando temporaneamente la dimensione massima dei blocchi a 256 KB anche su questa versione.

[2] `http://www.reddit.com/r/Bitcoin/comments/1a51xx/now_that_its_over_the_blockchain_fork_explained/`

Capitolo 4

Aspetti economici

Non si può parlare di Bitcoin senza analizzare, almeno in parte, il modello economico a cui si ispira. In realtà, per fare maggior chiarezza, è necessario evidenziare che non è il sistema p2p Bitcoin ad ispirarsi ad un determinato modello economico, ma la valuta BTC. Sarebbe infatti possibile adattare l'architettura del sistema a varie politiche monetari, e quella attuale è solo una delle possibili.

4.1 Caratteristiche di una moneta

Tradizionalmente si definisce qualcosa come moneta se svolge tre funzioni: unità di conto, mezzo di scambio e riserva di valore. C'è un dibattito molto acceso riguardo alla natura dei BTC [40]. Possono essere considerati una moneta?

Unità di conto

L'alta volatilità del prezzo di cambio dei BTC li rende una unità di conto poco pratica. Non a caso, i servizi che permettono l'acquisto di beni e servizi in cambio di BTC, solitamente stabiliscono un prezzo fisso in Euro o Dollari, che viene convertito in BTC al momento del pagamento. Questo espediente, assieme a servizi come Bitpay e Coinbase, permette ai negozianti di non assumersi il rischio di cambio.

Per svolgere la funzione di unità di conto, Bitcoin dovrebbe essere stabile nel prezzo e largamente utilizzato, permettendo al negoziante di pagare i propri fornitori e dipendenti in BTC, senza la necessità di convertirli in valuta tradizionale. Assumerebbero così un valore non in rapporto alle altre valute, ma in rapporto alla quantità di beni acquistabili con essi.

Mezzo di scambio

E' il ruolo che Bitcoin svolge meglio, in quanto il trasferimento è rapido, i costi sono bassi, non ha limiti geografici, non è sequestrabile né reversibile. Un difetto, rispetto al contante, è che ovviemente richiede dispositivi che siano connessi a Internet per funzionare.

La sostenibilità economica del sistema è un'ulteriore incognita. I minatori infatti sostengono notevoli costi per l'hardware e l'energia elettrica, che vengono in larga parte compensati dai nuovi BTC generati. Un'altra fonte di introito sono le fee presenti nelle transazioni. Queste attualmente sono una parte trascurabile rispetto ai BTC minati. In futuro, quando i nuovi BTC generati tenderanno a zero, le fee da sole dovranno fornire un incentivo sufficiente. Il panorama più ottimistico è quello che prevede un numero di transazioni molto elevato e un alto valore dei BTC. In tal caso le fee basterebbero.

Se ciò non dovesse avvenire, il numero dei minatori e la potenza totale del network calerebbero, fino a trovare un nuovo equilibrio economicamente sostenibile.

Ma potrebbe anche accadere che, a causa della forte domanda di transazioni da parte degli utilizzatori, il valore medio delle fee cresca ben oltre i valori attuali, rendendo Bitcoin meno conveniente, soprattutto per il settore dei micropagamenti, limitandone l'utilità.

Riserva di valore

Ha le potenzialità di diventare una buona riserva di valore, vista la quantità limitata di BTC in circolazione e le spese nulle per conservarli. Attualmente però non è adatto a causa dell'elevata volatilità e del conseguente rischio di cambio. In caso di una futura stabilizzazione dei prezzi, potrebbe fungere da bene rifugio come l'oro o gli immobili.

Una critica fatta da diversi economisti è che i BTC, a differenza dell'oro, non hanno un valore intrinseco, indispensabile per poter essere considerati una moneta, secondo alcune teorie monetarie[1].

Inoltre se un grave bug fosse scoperto nel protocollo, i loro valore potrebbe rapidamente crollare a zero. Data la giovinezza del progetto e il fatto che non è possibile escludere che questo bug esista, si tratto di uno scenario non così improbabile.

Se nonostante ciò in futuro Bitcoin prendesse piede come riserva di valore, i volumi delle transazioni potrebbero progressivamente diminuire e i BTC

[1]Teorema della regressione di Von Mises. `wiki.mises.org/wiki/Regression_theorem`

venire unicamente conservati in previsione del loro valore futuro, piuttosto che utilizzati per effettuare acquisti. Questo porterebbe ad un impoverimento dell'economia che ruota attorno ai BTC e una riduzione progressiva delle persone pronte ad accettarli, rendendoli di fatto inutili come moneta.

4.2 Indipendenza dalle banche

Bitcoin rappresenta una rivoluzione dal punto di vista economico, tra le altre cose, perché elimina la necessità di fidarsi di una terza parte in una transazione finanziaria a distanza. Questa frase sancisce una delle conquiste più dirompenti e potenzialmente "disruptive" del protocollo: ogni utente può essere la propria banca, con tutti i vantaggi e i rischi che ne conseguono.

Già nel genesis block è inserito un indizio sull'ostilità di Satoshi Nakamoto, lo pseudonimo dietro lo sviluppo di Bitcoin, all'attuale sistema finanziario, ritenuto corrotto, instabile e troppo influenzabile dalla politica. Ne è una prova la recente crisi finanziaria, nata dalla bolla dei mutui sub-prime statunitensi del 2008, e in breve diventata la più grave dopo quella del '29.

Bitcoin viene concepito come sistema che permetta al singolo utente di essere la banca di se stesso. Questo non vieta che possano esistere entità che svolgono sulla rete BTC un ruolo simile a quello svolto attualmente dalla banche (conti correnti remunerati, piattaforme di investimento, prestiti e mutui etc.), ma significa che non è strettamente necessario utilizzarle per trasferire e gestire in sicurezza il proprio denaro.

Questo approccio ha ovviamente anche dei lati negativi. Chi sceglie di gestire per conto proprio denaro sotto forma di BTC rinuncia ad ogni tipo di protezione e assicurazione bancaria in caso di furto. E, date le caratteristiche di anonimato dei BTC, è molto difficile recuperarli. Inoltre nell'ecosistema BTC la maggior parte dei servizi non sono assicurati in caso di insolvenza, al contrario delle banche tradizionali, i cui correntisti vengono risarciti dallo stato, fino ad una certa quota[2], in caso di fallimento.

E' evidente che un'adozione massiccia di Bitcoin o di crittovalute simili da parte delle persone comuni minaccerebbe e rivoluzionerebbe il mercato bancario attuale, ed infatti molte banche iniziano a guardare con interesse misto a timore il settore delle monete digitali.

[2]In italia esiste il Fondo Interbancario di Tutela dei Depositi, che garantisce fino a 100.000 euro per correntista. `https://www.fitd.it`

4.3 Modello monetario e deflazione

Le valute tradizionali dei vari stati sono solitamente emesse e controllate da una banca centrale. Queste operano in maniera formalmente indipendente dallo stato, stabiliscono la politica monetaria e in caso di necessità possono agire da prestatori di ultima istanza. Chiunque utilizzi una determinata moneta, subisce in un modo o nell'altro le conseguenze delle scelte della banca centrale che emette quella valuta.

Le banche centrali della maggior parte dei paesi occidentali perseguono una politica monetaria che mira a mantenere un'inflazione bassa ma costante, in modo da stimolare l'economia e mantenere un basso livello di disoccupazione. Questo approccio, che trova i sui fondamenti nella Teoria Monetaria Moderna[3], è criticato da chi ritiene che l'immissione di nuova moneta, decisa arbitrariamente dalle banche centrali, provochi una progressiva riduzione di valore del denaro già circolante, penalizzando di fatto le persone con uno stipendio fisso, che vedono il loro potere d'acquisto scendere nel tempo.

Un'altra scuola di pensiero, denominata Austriaca[4], sostiene che una moneta, per svolgere adeguatamente il proprio compito, debba essere legata al valore di un qualche bene specifico, come l'oro. Inoltre ritiene che possano coesistere più monete in concorrenza tra loro, anche emesse da banche private, in modo che il cittadino possa scegliere liberamente quale usare.

Possiamo vedere nei BTC l'implementazione di alcuni di questi concetti. Innanzitutto il modello di emissione prevede che vengano emessi al massimo 21.000.000 di BTC come descritto nel sottocapitolo 2.1.6. In questo modo Bitcoin ricalca, anche nei nomi (minatori) una risorsa materiale finita, come l'oro, che può essere estratto ma non generato a piacere. Inoltre l'operazione di estrazione richiede uno sforzo economico variabile che permette di mantenere un tasso di inflazione predeterminato.

L'inflazione, da subito programmata per decrescere nel tempo, si trasforma presto in deflazione, quando la domanda di BTC supera l'offerta. Il loro valore è così portato a crescere nel tempo, al contrario delle valute tradizionali. Il tutto è programmato in anticipo mediante algoritmi e l'utente non deve temere nessun cambiamento nella politica monetaria.

Bitcoin rappresenta quindi un tipo di moneta deflattiva, ritenuta generalmente dannosa per un'economia basata sui consumi, in quanto non li incentiva. Conservare una moneta che aumenta di valore è infatti più conveniente che spenderla. Nonostante questo esistono settori del mercato che si com-

[3] `http://en.wikipedia.org/wiki/Modern_Monetary_Theory`
[4] `http://en.wikipedia.org/wiki/Austrian_School`

portano in maniera deflattiva, ma che sono lo stesso molto dinamici, come quello dell'hi tech.

I maggiori economisti ritengono dannoso un modello monetario deflazionistico [41]. L'analisi di quale sia il miglior modello monetario applicabile esula dallo scopo della tesi e dalle nostre competenze.

Figura 4.1: Capitalizzazione in USD

Capitolo 5

Aspetti politici

Bitcoin suscita reazioni contrastanti nel mondo della politica. Le maggiori critiche sono sull'anonimato, che faciliterebbe fenomeni quali l'evasione fiscale, il riciclaggio di denaro e il trasferimento di capitali all'estero. Questo ha portato convinto alcuni governi a proibirne l'uso, come Islanda e Vietnam, ed altri a limitarlo tramite licenze obbligatorie per svolgere il ruolo di exchange, come Cina, Russia e India [42]. Inoltre c'è il timore che si possa rivelare uno strumento rischioso per per gli investitori ed i risparmiatori, in quanto non regolamentato e soggetto a forti rischi speculativi. La maggior parte delle nazioni non si è però espressa in maniera chiara sulla legalità di Bitcoin.

Essendo un progetto ancora giovane, per i tempi della politica, se ne discute ancora poco, ma la consapevolezza di questo strumento da parte delle istituzioni sta lentamente aumentando. La Banca Centrale ha di recente pubblicato un rapporto sul denaro elettronico, includendo anche Bitcoin [43].

5.1 Liberismo

Le forze politiche di matrice liberista ritengono che lo stato debba regolare il meno possibile la sfera pubblica, e di conseguenza ogni strumento che permetta l'indipendenza dai governi è ben vista. Bitcoin rappresenta, una possibile soluzione, in quanto si tratterebbe di una forma di moneta al di fuori del controllo dello stato e delle banche centrali. Data la popolarità dei movimenti antigovernativi e liberisti negli Stati Uniti, non stupisce che alcuni candidati politici abbiano deciso di sostenere Bitcoin, scegliendolo anche come metodo per accettare donazioni [44].

5.2 Anarco-liberismo

Nata nel XX secolo, questa teoria politica propone l'instaurazione di una società priva di tassazione dove ogni servizio venga offerto dai privati tramite spesa volontaria e nella quale sia eliminato ogni ricorso alla coercizione dello Stato, ritenuto intrinsecamente autoritario.

Bitcoin può risultare utile agli anarcoliberisti, in quanto permette di eliminare lo stato anche nel settore dell'emissione della moneta, senza dover ricorrere a società private che emettono moneta, o meglio affiancandosi ad esse. Un aspetto che analizzeremo in seguito è quello degli smart contract, ispirato anch'essi ad una visione dei rapporti tra le persone come contratti volontari.

5.3 Cypherpunk

Un movimento di attivisti che ritengono che l'unico modo di garantirsi la privacy sia quello di utilizzare strumenti di crittografia per celare le proprie comunicazioni a governi e multinazionali. Bitcoin è ispirato a questi ideali, e le sue caratteristiche di anonimato vanno a braccetto con gli ideali di questo movimento politico.

5.4 Anonimato

L'anonimato rappresenta per i governi nazionali un elemento di forte diffidenza nei confronti di Bitcoin. Il fatto che tramite strumenti come i mixer, alla portata di tutti, sia possibile muovere ingenti somme di denaro in maniera non tracciabile, apre tutta una serie di problematiche per il controllo dei capitali. Renderebbe estremamente semplici molte attività illegali che al momento sono ostacolate dal controllo delle istituzioni finanziarie e dei maggiori sistemi di pagamento.

Allo stesso tempo, in un'epoca in cui la privacy dell'individuo è sempre più minacciata, Bitcoin permette al cittadino comune di proteggersi dalla raccolta indiscriminata di dati sui suoi acquisti e relativa profilazione pubblicitaria. In particolar modo nel caso governi non democratici che cercano di ridurre i diritti civili tramite il controllo dei capitali.

Iniziative come quelle che, col fine di trasformare gli stati occidentali in cashless society, cercano di imporre sempre maggiori limiti alla circolazione del denaro contante, potrebbero spingere verso l'adozione di crittovalute e monete digitali. Bitcoin rappresenta infatti un'alternativa all'oligopolio

dei circuiti di carte di credito internazionali (Visa, Mastercard, American Express etc.), naturali beneficiari della transizione al denaro elettronico.

Il primo tentativo in Italia di regolamentare Bitcoin, è stato tramite un emendamento al decreto legge *"Destinazione Italia"*, presentato in data 8 gennaio 2014 [45]. La proposta prevede che per transazioni al di sopra di 1000 € il titolare di ogni transazione in BTC debba essere identificato. Non viene però spiegato come e in che modo calcolare il tasso di cambio ufficiale, né come vada identificato. Attualmente l'emendamento non risulta ancora approvato.

5.4.1 Il caso Wikileaks

Wikileaks rappresenta un esempio interessante dell'uso di Bitcoin come strumento per scavalcare i limiti dei sistemi di pagamento tradizionali. Come noto, si tratta di un'organizzazione internazionale fondata nel 2006 da Julian Assange. Raccoglie documenti ottenuti tramite spifferate anonime (leaks). Il materiale riguarda spesso prove di attività illegali segrete svolte da governi, agenzie di intelligence, multinazionali private. Wikileaks garantisce alle proprie fonti l'anonimato e pubblica i documenti una volta verificati.

In seguito alla pubblicazione della corrispondenza segreta di varie ambasciate statuinitensi nel novembre 2010, le donazioni al progetto tramite Bank of America, Visa, Mastercard, Paypal e Western Union vennero bloccate. La motivazione ufficiale del blocco fu la violazione dei termini di servizio, senza nessun intervento della magistratura, ma probabilmente avvenne a causa delle forti pressioni politiche da parte del governo degli Stati Uniti.

I gestori del progetto hanno quindi deciso di accettare Bitcoin come metodo alternativo per le donazioni nel giugno 2011. Nel corso del tempo si è dimostrato un ottimo strumento per superare il blocco. Inoltre l'anonimato ha permesso a molte persone di donare senza rischiare di essere accusate di finanziamento di attività illegale. Ad oggi Wikileaks dichiara che le donazioni tramite crittovaluta sono la sua fonte di sostentamento principale [46].

5.5 Tassazione

Per i governi i Bitcoin rappresentano un'incognita dal punto di vista della tassazione. In primo luogo è difficile stabilire cosa sono, ovvero se vadano considerati come un bene o una valuta. La scelta più naturale sarebbe la seconda, ma i BTC non sono emessi da nessuno stato, requisito per essere riconosciuti come moneta a corso legale. Viceversa se fossero considerati alla stregua di un bene, nel caso di scambio con valute tradizionali, sarebbero

soggetti all'imposta sul valore aggiunto (IVA). La distinzione è importante perché beni e valute vengono tassati in maniera differente nel caso di reddito da capitale.

L'Italia non ha ancora una posizione ufficiale in merito. Negli Stati Uniti l'IRS[1] ha stabilito che sono da considerarsi una proprietà, alla stregua di azioni, e quindi vanno dichiarati e tassati di conseguenza [47].

In secondo luogo, a causa delle sue caratteristiche di anonimato, è molto difficile individuare evasori fiscali che fanno uso di Bitcoin. Questo aspetto rappresenta un grosso svantaggio per le agenzie delle entrate.

L'affermazione di Bitcoin come strumento di pagamento legittimo e riconosciuto dallo stato richiederà il superamento di queste criticità.

5.6 Criminalità

Da quanto visto non deve stupire che il mondo della criminalità sia interessato a Bitcoin. Garantendo un anonimato inferiore solo al contante, ed una maggiore praticità, rappresenterebbe un buon metodo per spostare denaro frutto di attività illecite. Attualmente la sua utilità in questo settore è però ridotta, visto che sarebbe necessario utilizzare exchange che, come abbiamo visto, richiedono un'identificazione nella maggior parte dei casi.

I BTC si prestano anche a truffe o raggiri, visto la loro irreversibilità, che permette al truffatore che si fa inviare denaro in cambio di beni o servizi di scappare con il bottino senza onorare i patti.

Un altro settore particolarmente attivo è quello dei malware. Ne esistono di vari tipi. Alcuni, una volta compromesso un sistema, si occupano di svuotare tutti gli indirizzi Bitcoin le cui chiavi private sono memorizzate sulla macchina. Altri utilizzano i processori e le schede grafiche dei computer vittima per effettuare operazioni di mining. Stanno però diventando meno diffusi, visto l'aumentare dei requisiti hardware necessari per minare.

E' stato inoltre individuato un ransomware[2], chiamato CryptoLocker, che prevedeva come opzione di pagamento anche Bitcoin, ad un costo più basso rispetto agli altri metodi.

[1] Internal Revenue Service. Svolge le funzioni dell'Agenzia delle Entrate negli Stati Uniti.

[2] Malware che cifra i dischi locali della macchina su cui si installa, impedendone l'accesso al legittimo proprietario. Permette di ottenere la chiave per decifrare i dati solo pagando un riscatto.

Esistono anche siti anonimi per la compravendita di materiale illegale. Vengono realizzati solitamente comme hidden services su rete Tor[3] e permettono di acquistare beni e servizi vietati dalla legge tramite BTC. L'esempio più famoso è Silk Road.

5.6.1 Il caso Silk Road

Nato nel 2011, Silk Road ha svolto il ruolo di mercato di compravendita di sostanze stupefacenti, materiale illegale e, per un certo periodo, armi da fuoco [10]. Il sito non era accessibile tramite la normale rete Internet, ma solo mediante rete Tor. L'accesso anonimo rendeva impossibile per chiunque individuare la posizione dei server che lo ospitavano e l'identità degli utenti che lo visitavano.

Il sito offriva uno spazio ai venditori dove mostrare le caratteristiche e il prezzo della merce. Inoltre per aumentare la sicurezza e ridurre il numero di truffe era stato aggiunto un sistema di escrow e di feedback, simile a quello di eBay.

La consegna della merce era effettuata tramite posta. Veniva consigliato di fornire indirizzi di luoghi abbandonati e nomi inventati. Il fatto che le comunicazioni tra acquirente e venditore non potessero venire tracciate dalle forze dell'ordine, permetteva al compratore di negare in seguito l'acquisto, nel caso il pacco contenente sostanze illegali fosse stato intercettato nei centri di smistamento postale. Esisteva comunque il rischio di essere trovati in possesso del materiale acquistato.

Durante il periodo in cui rimase attivo, Silk Road raggiunse un notevole volume di vendita, in una ricerca quantificato in 22 milioni di dollari all'anno [11, 48].

Il sito è stato sequestrato il 2 ottobre 2013 dall'FBI, dopo l'arresto del sospetto gestore Ross Ubricht, noto con lo pseudonimo di Dread Pirate Roberts, che attualmente si trova sotto processo.

[3]Tor (The Onion Router) è un sistema di comunicazione anonima. `https://www.torproject.org/`

Capitolo 6

Oltre Bitcoin

Bitcoin rappresenta solo la punta dell'iceberg di tutta una nuova categoria di tecnologie. I paradigmi su cui si basa (blockchain, proof-of-work, crittografia) possono seriamente cambiare il modo in cui i sistemi distribuiti vengono concepiti, progettati e sviluppati. Bitcoin rappresenta l'implementazione di una singola funzionalità, quella di moneta digitale, ma non è di certo l'unica realizzabile o la più interessante. Nel corso del tempo vari progetti ispirati a Bitcoin sono stati realizzati.

6.1 Monete alternative

Si tratta di progetti simili a Bitcoin, in quanto si tratta sempre di monete digitali, ma con differenti caratteristiche tecniche od economiche. Vista la facilità con cui possono essere create, prendendo il codice opensource di altre monete e modificandolo, ormai ne esistono diverse centinaia.[1] Di seguito alcuni esempi.

6.1.1 Litecoin

Una delle prime monete alternative, introdotta nel 2011 [49]. Il protocollo è in gran parte lo stesso di Bitcoin, con alcune modifiche.

Vengono generati nuovi blocchi ogni 2,5 minuti invece che ogni 10, rendendo più rapide le conferme. Il numero di LTC generati tende ad un massimo di 84 milioni. A differenza di Bitcoin, non utilizza un algoritmo di mining basato su SHA-256. Si affida invece a Scrypt come proof-of-work [50]. Questo é stato scelto dagli sviluppatori per l'uso massiccio di memoria che comporta,

[1] `http://mapofcoins.com/`

in modo da rendere inefficiente l'utilizzo di GPU, FPGA e ASIC, mantenendo il mining alla portata di PC con normali CPU.

Nonostante questo sono stati realizzati comunque dispositivi dedicati al mining di monete basate su Scrypt.[2]

Litecoin rappresenta un esempio di moneta clone di Bitcoin, che non aggiunge reali innovazioni e non pone le basi per nuovi casi d'uso.

6.1.2 Primecoin

Introdotta nel luglio 2013 basa il suo algoritmo di mining sulla ricerca di catene di numeri primi [51]. Gli sviluppatori sostengono che in questo modo lo schema di proof-of-work adottato, oltre a mantenere la sicurezza della moneta, è anche utile alla ricerca scientifica. L'algoritmo genera catene di Cunningam[3] e Bi-twin[4], molto studiate in ambito matematico.

In soli pochi mesi di attività ha già raggiunto numerosi record nella scoperta di numeri primi.[5]

6.2 Applicazioni distribuite

Oltre alle monete alternative sono state realizzate varie applicazioni distribuite ispirate al funzionamento di Bitcoin. Queste cercano di risolvere problemi diversi rispetto al semplice trasferimento di denaro. Alcune utilizzano una o più blockchain, altre adottano metodi diversi.

Quello che le accomuna è il cercare di risolvere il problema del consenso distribuito, ovvero permettere a nodi di pari livello (peers) di trovare un accordo e, una volta trovato, di non poterlo più modificare.

6.2.1 Namecoin

E' stato il primo fork di Bitcoin, ideato nel 2011 [52]. Si propone di realizzare un naming system salvando le coppie chiave valore sulla propria blockchain. E' usato principalmente come DNS alternativo, e permette la registrazione di domini .bit.

Namecoin è anche il nome della moneta digitale (NMC) necessaria per registrare un dominio sul sistema. Viene generata attraverso il mining, con lo

[2] `http://zeusminer.com/`

[3] `http://en.wikipedia.org/wiki/Cunningham_chain`

[4] `http://en.wikipedia.org/wiki/Bi-twin_chain`

[5] `https://github.com/primecoin/primecoin/wiki/World-records`

stesso algoritmo di Bitcoin. E' prevista la scadenza dei domini e la possibilità di rinnovarli.

Un DNS realizzato in maniera decentralizzata offre il vantaggio/svantaggio di non essere censurabile, in quanto non esiste un'autorità centrale che controlla l'assegnazione di domini. Non è quindi possibile decidere chi abbia diritto ad un dominio e chi no; da una parte limitando la censura, dall'altra impedendo il sequestro ad opera dell'autorità giudiziaria in caso di contenzioso legale. Per visualizzare i siti che si appoggiano a questo DNS è necessario installare il client Namecoin e un plug-in per il browser.

6.2.2 Bitmessage

Implementa un sistema di messaggistica tramite l'utilizzo di una blockchain. Ogni utente può generare un indirizzo dove ricevere messaggi di testo cifrati, che saranno visibili soltanto a lui. Il programma permette quindi di inviare informazioni in maniera anonima e sicura. Ogni nodo deve possedere la blockchain completa contenente tutti i messaggi. Per alleviare il problema dello storage gli sviluppatori hanno stabilito un tempo massimo entro cui i messagi vengono automaticamente cancellati. Esiste inoltre un sistema antispam di tipo proof-of-work per evitare che la piattaforma venga inondata di messaggi, peggiorandone le prestazioni.

6.2.3 Ripple

Ripple si propone come un protocollo per transazioni finanziarie (Ripple Transaction Protocol o RTXP) su Internet [53].

Permette a chiunque di trasferire denaro in valuta tradizionale o digitale. E' basato sulla fiducia e sul trasferimento di crediti e debiti. Ogni utente, oltre al proprio bilancio, ha la possibilità di aprire delle linee di credito verso gli altri utenti. Le linee di credito sono rappresentate dalla fiducia che un utente ripone in un altro utente. La fiducia viene espressa dalla quantità di denaro che l'utente è disposto a prestare. Non scenderemo troppo nel dettaglio riguardo alla logica di funzionamento, ma invitiamo a consultare la wiki ufficiale del progetto.[6]

La parte interessante è che Ripple agisce come una sorta di camera di compensazione automatica tra utenti, permettendo di trasferire denaro e di ritirarlo fisicamente presso altri utenti che hanno il ruolo di gateway, ovvero fungono da banche. Idealmente Ripple si propone come federation protocol[7]

[6] `https://ripple.com/wiki/Ripple_for_Users`

[7] `https://ripple.com/wiki/Federation_protocol`

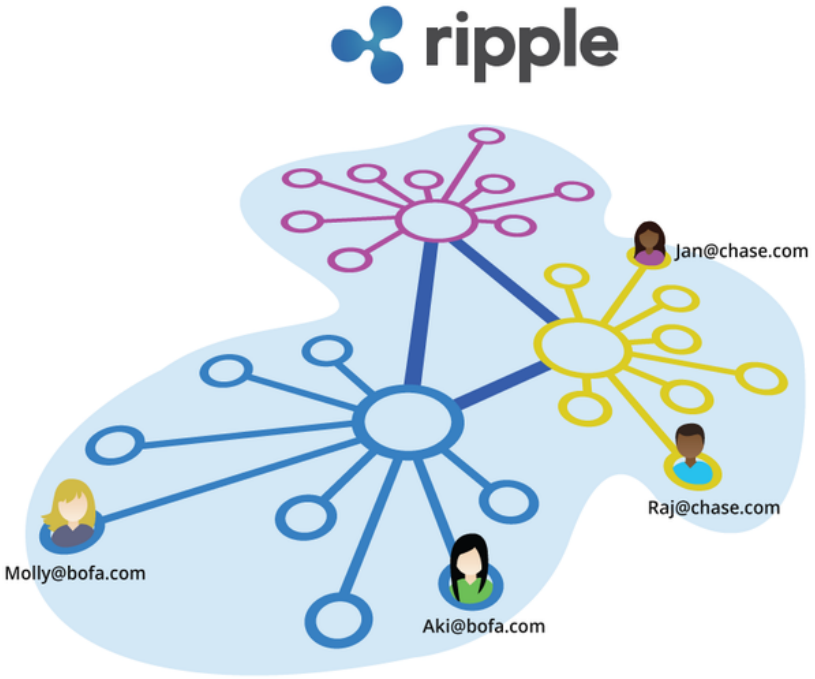

Figura 6.1: Federazione di reti indipendenti

in grado di standardizzare le transazioni tra istituzioni finanziarie tradizionali e utenti.

La flessibilità di Ripple permette di trattare qualsiasi valuta, anche inventata o immaginaria, semplicemente scegliendo un codice a tre lettere e creando una rete di fiducia tra persone che la accettano. E' possibile scambiare le monete tra loro grazie ad un mercato di valuta integrato nel software.

Ripple ha anche una propria moneta interna, denominata XRP, che a differenza delle altre non si basa sul concetto delle linee di fiducia, ma può essere inviata a chiunque. Gli XRP svolgono due ruoli essenziali: servono come sistema antispam e come meta-moneta.

Ogni volta che un utente vuole effettuare una transazione o aprire una linea di fiducia consuma una parte degli XRP, che devono essere acquistati dagli sviluppatori del protocollo. Sono inoltre essenziali per fare da ponte nello scambio di valute che non hanno un cambio diretto sul mercato.

I bilanci degli utenti e le linee di credito vengono gestite attraverso un database distribuito simile alla blockchain, chiamato ledger. Ogni nodo contiene una copia dell'ultimo ledger valido.

Il processo di formazione del consenso è molto diverso dal proof-of-work

di Bitcoin. Ogni client ha infatti una lista di di nodi affidabili, chiamata UNL (Unique Node List). Ogni nodo propone le proprie modifiche al ledger agli altri nodi. Quando un nodo riceve una proposta di modifica, la accetta solo se proviene da un nodo presente nella propria UNL. A questo punto, quando la maggior parte dei nodi ha accettato la modifica, questa viene inclusa nell'ultimo ledger valido, che diventa lo stesso per tutti i nodi.

Questo processo, escludendo ogni forma di mining, è molto più veloce e meno dispendioso in termini di risorse, permettendo così un aggiornamento ogni 5/10 secondi, contro gli oltre 10 minuti della blockchain di Bitcoin. E' quindi possibile installare un full node su dispositivi poco potenti, come PC e smartphone.

L'approccio al problema del consenso ha però degli inconvenienti. Non è chiaro infatti se possa garantire la sicurezza delle transazioni e l'indipendenza da terze parti. Tutto dipende da come vengono configurate le UNL dei vari nodi. Gli sviluppatori sostengono che sia sufficiente aggiungere server fidati che non abbiano incentivi a unire le forze per sovvertire il network. Ad esempio, scegliendo server gestiti da banche e istituzioni finanziare di paesi diversi, come Stati Uniti e Cina, sarebbe poco probabile una loro collaborazione per influenzare la rete Ripple.

In ogni caso il sistema è ancora molto giovane e dovrà prima essere testato a regime per trarre conclusioni sulla sua sicurezza.

6.2.4 Ethereum

Ethereum è un progetto ancora embrionale e, oltre ad un whitepaper[8], esistono solo alcune implementazioni di proof of concept, ma si tratta probabilmente di una delle applicazioni distribuite più ambiziose nate sulla scia di Bitcoin [54].

Si propone come piattaforma di sviluppo per applicazioni distribuite e decentralizzate. Essenzialmente cerca di adattare le tecnologie e gli accorgimenti introdotti da Bitcoin per creare una rete che non sia solo in grado di effettuare transazioni, ma di eseguire programmi e salvare dati. Una sorta di piattaforma cloud anonima e decentralizzata in cui ogni nodo partecipa all'esecuzione dei programmi.

Ethereum è anche il nome del linguaggio Turing completo ideato per programmare tramite tale piattaforma.

Gli sviluppatori si occupano di creare il programma, caricarlo sulla rete e inviare all'indirizzo del programma una certa quantità di crittovaluta, denominata Ether. A questo punto i nodi che sono interessati ad eseguire

[8] `https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper`

il codice possono farlo, e ricevono ad ogni ciclo una quantità prefissata di Ether. Quando il "carburante" si esaurisce, i nodi terminano l'esecuzione. Allo stesso modo è possibile conservare quantità di dati pagando in Ether, in maniera proporzionale alla quantità e alla durata dello storage.

Gli Ether vengono generati dagli stessi nodi che partecipano alla computazione, secondo un modello di proof-of-work. In questo caso la prova del lavoro svolto è l'esecuzione stessa del programma, risolvendo una delle critiche fatte a Bitcoin: lo spreco di risorse. Inoltre non sarebbe neppure possibile realizzare dispositivi dedicati al mining di Ether, in quanto si tratterebbe di CPU general purpose, dovendo eseguire algoritmi di programmi sempre diversi.

Il codice prima di essere caricato può venire offuscato per mantenerlo segreto. Infatti, affinché il sistema funzioni è evidenti che tutti i programmi debbano essere pubblici, in quanto eseguiti su diversi nodi della rete.

I programmi sviluppati tramite Ethereum possono comunicare tra loro e con l'esterno della rete tramite i cosiddetti feed, che avvisano il programma quando una particolare condizione viene soddisfatta.

Ad esempio è possibile realizzare un sistema di scommesse automatiche per partite di calcio. Il programma presenta vari indirizzi a cui è possibile inviare Ether, Bitcoin, o qualsiasi altra crittovaluta, in base al risultato atteso. Aggiungendo un feed che punta verso un sito con il resoconto ufficiale della partita(ad esempio Fifa.com), il programma distribuisce autonomamente le vincite in base al risultato. Il funzionamento dell'algoritmo può essere reso completamente trasparente, impedendo vari tipi di truffa, che possono invece avvenire attraverso i circuiti di scommesse tradizionali.

E' chiaro che con questo tipo di piattaforma è possibile realizzare applicazioni per gli scopi più disparati: voto online, trading finanziario, crowfunding, assicurazioni, contratti di qualsiasi tipo e perfino smart property, con il giusto supporto hardware.

6.3 Smart contracts

Uno degli sviluppi più interessanti di piattaforme come Bitcoin, Ripple o Ethereum sono gli smart contract [55], protocolli per la verifica e l'applicazione di regole in un accordo tra più parti. Gli smart contract si propongono di sostituire i contratti tradizionali in modo da renderne più facile e veloce l'interperetazione e l'applicazione, sostituendo al linguaggio naturale un linguaggio formale elaborabile da un computer. Consentono risparmi notevoli di tempo e di costi, in quanto funzionano automaticamente senza l'intervento

umano. Un esempio ampiamente utilizzato è il Digital Rights Management (DRM).

Il limite di questi contratti è che possono essere utilizzati per lo più in ambito digitale, anche se tentativi di applicarli al mondo reale sono sempre più frequenti. Un esempio primitivo può essere un distributore automatico. Quando inseriamo la moneta il software interno autorizza automaticamente l'erogazione di un prodotto, consentendo così un passaggio di proprietà senza l'intervento umano.

Con il termine smart property si indica un bene il cui utilizzo, accesso o cambio di proprietà sia regolato da uno smart contract. Esempi molto rudimentali di smart property possono essere le auto dotate di immobilizer, oppure gli smartphone cifrati tramite pin. In entrambi i casi si tratta di oggetti impossibili da utilizzare senza possederne la chiave, ovvero violandone il contratto.

Utilizzando le crittovalute come chiave, questi sistemi possono essere implementati in maniera più efficacie. Per esempio si possono realizzare auto collegate a Internet che si accendono solamente se il proprietario ha pagato le rate del leasing tramite transazioni tracciabili in Bitcoin. Oppure aziende che distribuiscono azioni con la possibilità di esercitare il diritto di voto tramite blockchain. In generale produrre oggetti che non devono necessariamente essere acquistati per poter essere utilizzati, ma semplicemente sbloccati. Si potrebbe anche pensare di introdurre tipi di prestito garantiti da smartproperty, che in caso di insolvenza vengono bloccate e trasferite al creditore

Tutte queste possibilità, in caso di domanda da parte del mercato, aspettano solo di essere esplorate. Si tratta in ogni caso di questioni molto delicate dal punto di vista etico e politico.

Conclusione

Bitcoin rappresenta il capostipite di una nuova generazione di tecnologie p2p che rivoluzioneranno molti ambiti. Permette di inviare valore tramite Internet a chiunque in maniera sicura ed economica. In un mondo in cui oltre la metà della popolazione non ha accesso a conti correnti o a servizi finanziari[9], questa possibilità rappresenta una grande innovazione.

Nonostante si tratti di software ancora in fase sperimentale, nel corso del tempo ha più volte dimostrato notevole resistenza agli attacchi, flessibilità e scalabilità. Lo sviluppo non è naturalmente concluso, e vari aspetti attendono di essere migliorati, come le prestazioni e il problema della centralizzazione del mining. A parte questo Bitcoin si rivela un sistema sorprendentemente affidabile.

La possibilità di bypassare le istituzioni finanziarie e l'indipendenza dal controllo delle banche centrali sono viste con una certa diffidenza dalla politica, anche se alcuni partiti, specialmente di stampo liberista, stanno iniziando ad apprezzare queste caratteristiche. Bitcoin è percepito da molti come un fenomeno ancora di nicchia, e i tentativi di regolamentazione procedono lentamente e in maniera poco organica. Un quesito che rimane aperto è se Bitcoin possa essere effettivamente regolamentato, dato che esperienze simili nel campo dei sistemi p2p per la condivisione di materiale protetto da copyright hanno avuto esito negativo.

Porta inoltre una ventata di innovazione in un settore, quello bancario, da sempre avverso al rischio. Le prime reazioni non si sono fatte attendere: alcune sono state positive, altre addirittura hanno portato al divieto di aprire exchange in determinati paesi. Le maggiori incognite emergono dal punto di vista legale, dato che non esiste ancora una regolamentazione omogenea a livello globale, senza la quale molti attori del settore bancario e IT attendono alla porta.

Indipendentemente dal successo o meno di Bitcoin come moneta di Internet, è stato introdotto un nuovo paradigma nello sviluppo di sistemi distributi, profondamente basato sulla crittografia e sulla decentralizzazione.

[9] `http://mckinseyonsociety.com/half-the-world-is-unbanked/`

Molti software stanno venendo sviluppati con lo scopo di ampliarne e differenziarne le funzioni. Bitcoin rappresenta solo la prima ondata, quella delle crittovalute, e presto arriveranno interi sistemi di elaborazione basati sugli stessi principi. Le possibilità sono innumerevoli e molte attendono ancora di essere esplorate.

Bibliografia

[1] David Chaum. "Blind signatures for untraceable payments". In: *Advances in cryptology*. Springer. 1983, pp. 199–203. URL: http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF (visitato il 24/03/2014).

[2] David Chaum e Stefan Brands. "Minting'electronic cash". In: *Spectrum, IEEE* 34.2 (1997), pp. 30–34. URL: http://homepage.cs.uiowa.edu/~cremer/courses/cs2/ecasharticle.pdf (visitato il 24/03/2014).

[3] Adam Back et al. *Hashcash - A Denial of Service Counter-Measure*. 2002. URL: ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf (visitato il 24/03/2014).

[4] Wei Dai. *B-money*. 1998. URL: http://www.weidai.com/bmoney.txt (visitato il 24/03/2014).

[5] Nick Szabo. *Bit-gold*. 2005. URL: http://unenumerated.blogspot.it/2005/12/bit-gold.html (visitato il 23/03/2014).

[6] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf/ (visitato il 23/03/2014).

[7] *Pizza for bitcoins?* 18 Mag. 2010. URL: https://bitcointalk.org/index.php?topic=137.0 (visitato il 23/03/2014).

[8] *overflow bug SERIOUS*. 15 Ago. 2010. URL: https://bitcointalk.org/index.php?topic=823.0 (visitato il 23/03/2014).

[9] Andy Greenberg. *WikiLeaks Asks For Anonymous Bitcoin Donations*. 14 Giu. 2011. URL: http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/ (visitato il 23/03/2014).

[10] Emily Flitter. *FBI shuts alleged online drug marketplace, Silk Road*. 2 Ott. 2013. URL: http://news.yahoo.com/fbi-raids-alleged-online-drug-market-silk-road-153729457.html (visitato il 23/03/2014).

[11] Nicolas Christin. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace". In: *Proceedings of the 22nd international conference on World Wide Web*. International World Wide Web Conferences Steering Committee. 2013, pp. 213–224.

[12] Rachel Abrams Matthew Goldstein e Hiroko Tabuchi. *Erosion of Faith Was Death Knell for Mt. Gox*. 28 Feb. 2014. URL: http://dealbook.nytimes.com/2014/02/28/mt-gox-files-for-bankruptcy/ (visitato il 23/03/2014).

[13] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, 1996.

[14] Auguste Kerckhoffs. *Journal des sciences militaires*. 1883. URL: http://petitcolas.net/fabien/kerckhoffs/ (visitato il 23/03/2014).

[15] Don Johnson, Alfred Menezes e Scott Vanstone. "The elliptic curve digital signature algorithm (ECDSA)". In: *International Journal of Information Security* 1.1 (2001), pp. 36–63.

[16] *Base58Check encoding*. URL: en.bitcoin.it/wiki/Base58Check_encoding (visitato il 27/03/2014).

[17] FIPS PUB. *Secure Hash Standard (SHS)*. 2012.

[18] *Ultimate blockchain compression w/ trust-free lite nodes*. 17 Giu. 2012. URL: https://bitcointalk.org/index.php?topic=88208.0 (visitato il 27/03/2014).

[19] JD Bruce. "Purely P2P Crypto-Currency With Finite Mini-Blockchain". In: (mag. 2012). URL: http://bitfreak.info/files/pp2p-ccmbc-rev1.pdf (visitato il 27/03/2014).

[20] Dylan Love. *What It's Like Inside The World's Largest Bitcoin Mining Operation*. 10 Mar. 2014. URL: http://www.businessinsider.com/worlds-largest-bitcoin-mining-operation-2014-3 (visitato il 01/04/2014).

[21] *Bitcoin Core client*. URL: https://github.com/bitcoin/bitcoin (visitato il 08/04/2014).

[22] *GoCoin client*. URL: http://www.assets-otc.com/gocoin (visitato il 08/04/2014).

[23] *Thin Client Security*. URL: https://en.bitcoin.it/wiki/Thin_Client_Security#Header-Only_Clients (visitato il 08/04/2014).

[24] *Electrum*. URL: http://www.assets-otc.com/gocoin (visitato il 08/04/2014).

[25] *Bitcoinj client*. URL: https://code.google.com/p/bitcoinj/ (visitato il 08/04/2014).

[26] *MultiBit client*. URL: https://multibit.org/ (visitato il 08/04/2014).

[27] Bitcoin Reporter. *The Need For Bitcoin Integrated Escrow*. URL: http://bitcoinreporter.com/articles/the-need-for-bitcoin-escrow (visitato il 08/04/2014).

[28] Michele Spagnuolo. "BitIodine: Extracting Intelligence from the Bitcoin Network". Tesi di laurea mag. Politecnico di Milano, 2013.

[29] Gregory Maxwell. *CoinJoin*. URL: https://bitcointalk.org/index.php?topic=279249.0 (visitato il 08/04/2014).

[30] *SharedCoin*. URL: https://github.com/blockchain/Sharedcoin (visitato il 08/04/2014).

[31] Gregory Maxwell. *CoinSwap*. URL: https://bitcointalk.org/index.php?topic=321228.0 (visitato il 08/04/2014).

[32] Dan Kaminsky. *Some Thoughts On Bitcoin*. URL: http://www.slideshare.net/dakami/bitcoin-8776098 (visitato il 08/04/2014).

[33] *Scalability*. URL: https://en.bitcoin.it/wiki/Scalability (visitato il 08/04/2014).

[34] *Dati sul numero delle transazioni*. URL: https://blockchain.info/charts/n-transactions (visitato il 08/04/2014).

[35] Gordon E Moore et al. *Cramming more components onto integrated circuits*. 1965.

[36] *Bitcoin Improvement Proposal*. URL: https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals (visitato il 08/04/2014).

[37] *Vulnerbilità*. URL: https://en.bitcoin.it/wiki/Weaknesses (visitato il 08/04/2014).

[38] *Testnet*. URL: https://en.bitcoin.it/wiki/Testnet (visitato il 08/04/2014).

[39] *Output overflow bug*. URL: http://www.monetarism.co.uk/the-beginners-guide-to-bitcoin-everything-you-need-to-know/ (visitato il 08/04/2014).

[40] Paul Krugman. *Bitcoin Is Evil*. URL: http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/ (visitato il 08/04/2014).

[41] Paul Krugman. *Why is deflation bad?* URL: http://krugman.blogs.nytimes.com/2010/08/02/why-is-deflation-bad/ (visitato il 08/04/2014).

[42] *Bitlegal*. URL: http://www.bitlegal.io/ (visitato il 08/04/2014).

[43] European Central Bank. *Virtual Currency Schemes*. 2012. URL: www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (visitato il 11/07/2014).

[44] *Bitcoin Takes Stage In Texas Senate Campaign*. URL: http://www.npr.org/blogs/itsallpolitics/2014/01/10/260572933/bitcoin-takes-stage-in-texas-campaign (visitato il 08/04/2014).

[45] *Anche l'Italia si accorge di Bitcoin*. URL: http://punto-informatico.it/3977384/PI/News/anche-italia-si-accorge-bitcoin.aspx (visitato il 08/04/2014).

[46] *Bitcoin and Litecoin Top Sources of WikiLeaks Donations*. URL: http://www.coindesk.com/bitcoin-litecoin-source-wikileaks-donations/ (visitato il 08/04/2014).

[47] *Bitcoin is legally property, says US IRS. Does that kill it as a currency?* URL: http://www.theguardian.com/technology/2014/mar/31/bitcoin-legally-property-irs-currency (visitato il 08/04/2014).

[48] *Black Market Drug Site 'Silk Road' Booming: $22 Million In Annual Sales*. URL: http://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales/ (visitato il 08/04/2014).

[49] *Litecoin*.

[50] Colin Percival. *Stronger key derivation via sequential memory-hard functions*. 2009. URL: http://www.tarsnap.com/scrypt/scrypt.pdf (visitato il 04/07/2014).

[51] *Primecoin*.

[52] *Namecoin*. URL: http://namecoin.info/ (visitato il 06/07/2014).

[53] *Ripple*. URL: https://ripple.com/ (visitato il 06/07/2014).

[54] *Ethereum*. URL: https://ethereum.org/ (visitato il 06/07/2014).

[55] *Smart contracts*. URL: http://szabo.best.vwh.net/idea.html (visitato il 06/07/2014).