Alma Mater Studiorum - Università di Bologna

Campus di Cesena
Scuola di Ingegneria e Architettura
Corso di Laurea in Ingegneria Elettronica, Informatica e Telecomunicazioni

BITCOIN: LIMITI E SOLUZIONI TECNICHE DELLA SCALABILITÀ

Elaborato in Sistemi Distribuiti

Relatore: Prof.
ANDREA OMICINI
Correlatore: Ing.
NAZZARENO POMPEI

Autore della tesi:
OKSANA KOMARNYTSKA

Anno Accademico 2016/2017
I Sessione

PAROLE CHIAVE

Criptovaluta

Blockchain

Bitcoin

Scalabilità

Block Size

Hard Fork

Soft Fork

Alla mia famiglia.

Indice

Introduzione

Attualmente il sistema delle criptovalute è in crescita esponenziale. Una moneta che si distingue dalle altre nell'essere fra le più utilizzate e più conosciute monete digitali al mondo è Bitcoin. Infatti, nell'ultimo anno la sua crescita è stata talmente rapida da porre seri problemi al sistema distribuito di gestione delle transazioni. Sembra incredibile ma Bitcoin si sta rivelando la vittima del suo stesso successo. Pertanto oggigiorno la scalabilità rappresenta uno dei maggiori rischi al futuro di Bitcoin.

Bitcoin è una moneta virtuale creata nel 2009 da uno sviluppatore noto con lo pseudonimo di Satoshi Nakamoto. Essa si basa sul principio del *peer-to-peer* (p2p) ed è un protocollo *open source*. Ciò che la distingue dalle valute di tipo tradizionale è il fatto che essa è una moneta che utilizza un database distribuito tra i nodi della Rete i quali tengono traccia delle transazioni e con l'aiuto della crittografia gestisce gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione di proprietà. Pertanto bitcoin può essere scambiato tra gli utenti senza rincorrere ad intermediari, divenendo così la prima tipologia di pagamento trustless.

Attualmente esiste un limite tecnologico nella dimensione dei blocchi di Bitcoin che corrisponde a 1 MB, che permette di raggiungere un limite al massimo di sette transazioni per secondo, impostato per evitare che la rete venga ingolfata da tante transazioni di scarso valore. Con la crescita di Bitcoin il numero di transazioni effettuate ha raggiunto il limite di capacità del blocco e la barriera di 1 MB si sta traducendo in un collo di bottiglia. L'aumento delle commissioni e troppi ritardi rischiano di spostare il mercato di Bitcoin verso le altre crittovalute.

Sono state effettuate diverse analisi nel corso del tempo per poter aumentare la dimensione del blocco. Dal punto di vista tecnico è una banalità da eseguire. Tale modifica renderebbe la rete più fluida per far sì che gli utenti possono ricevere le proprie transazioni convalidate più facilmente. Nonostante tutti i vantaggi l'aumento del limite massimo avrebbe ripercussioni sulla sicurezza della rete.

Questa tesi si prefigge l'obiettivo di studiare la scalabilità del sistema Bitcoin, nonché le possibili soluzioni per risolvere questo problema.
L'elaborato seguirà dunque la seguente struttura:

- Il primo capitolo è finalizzato a descrivere il funzionamento del sistema Bitcoin.

- Il secondo capitolo è dedicato allo studio della scalabilità del sistema Bitcoin. Vengono messi in evidenza diverse proposte di miglioramento del protocollo riguardanti il problema della scalabilità nel corso degli anni. Inoltre, vengono illustrati i vantaggi e i limiti di un eventuale aumento del limite massimo della dimensione del blocco (Block Size).
- Il terzo capitolo è finalizzato ad analizzare quanto incide l'aumento di Block Size sul consumo di risorse e sul tempo di propagazione dei blocchi, nonché esaminare il sistema Bitcoin in un insieme di livelli di astrazione ai fini di esplorare tutte le problematiche della scalabilità in diversi settori del protocollo Bitcoin.
- Il quarto capitolo è finalizzato allo studio degli sviluppi recenti del settore che rappresenta la scalabilità del sistema Bitcoin, nonché nell'analisi dei progetti "Segregated Witness" e "Bitcoin Unlimited".

1 Bitcoin

Background

Bitcoin (abbreviata in genere con l'acronimo B ed i codici BTC o XBT) è una moneta virtuale creata nel 2009 da uno sviluppatore noto con lo pseudonimo di Satoshi Nakamoto. Essa si basa sul principio del *peer-to-peer* (p2p) ed è un protocollo *open source*. Ciò che la distingue dalle valute di tipo tradizionale è che essa è una moneta che utilizza un database distribuito tra i nodi della Rete che tengono traccia delle transazioni e fa ricorso alla crittografia per la gestione degli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione di proprietà della medesima. Ne consegue che essa non risente di tutti quei condizionamenti che sono propri delle monete stesse, a cominciare dal fatto di dover dipendere dalla fiducia loro concessa da autorità di garanzia esterne, come banche centrali o istituzioni finanziarie. Da questo punto di vista, Bitcoin nasce principalmente con l'obiettivo di permettere i trasferimenti in denaro che non si basino sulla fiducia in una terza parte.

Di norma, con il termine "Bitcoin" (con l'iniziale maiuscola) si fa riferimento alla tecnologia e alla rete, mentre, se l'iniziale è minuscola, il riferimento è alla valuta in sé.

La rete Bitcoin consente il possesso e il trasferimento anonimo delle monete, e i dati necessari all'impiego dei propri bitcoin possono essere salvati su uno o più pc, sotto forma di portafoglio digitale, oppure mantenuti in deposito presso terzi, che in tal modo assolvono a funzioni analoghe a quelle di una banca.

I bitcoin possono essere trasferiti in rete verso chiunque possieda un indirizzo *ad hoc* (noto come "indirizzo bitcoin"). L'aspetto cruciale, tuttavia, consiste nel fatto che la struttura *peer-to-peer* della rete Bitcoin e la mancanza di un ente centrale di controllo e regolazione rendono impossibile a qualsiasi autorità – governativa o meno – il blocco dei trasferimenti, il sequestro di bitcoin nel caso non si abbia il possesso delle relative chiavi o fenomeni come la svalutazione, imputabile all'immissione di nuova moneta.

Un'ulteriore peculiarità di Bitcoin è che l'emissione della valuta omonima è limitata e cresce fino a raggiungere il limite prestabilito di 21 milioni di unità. Ciò fa sì che il valore non può essere manipolato grazie all'inflazione, come può accadere invece con le valute tradizionali.

Scopo di questo capitolo è la descrizione del funzionamento del sistema di Bitcoin.

1.1. Cenni storici

Il termine *alternative currency* ("valuta alternativa") si riferisce a una qualunque forma di moneta o di titolo di credito utilizzati per lo scambio di beni e servizi tra i membri di una comunità, e collocati al di fuori dei circuiti monetari ufficiali.

La valuta alternativa, a sua volta, si divide in tangibile e digitale. La seconda (*digital currency*) è uno strumento di scambio basato su Internet, diverso dalla valuta fisica di tipo tradizionale, che permette transazioni istantanee e trasferimenti di proprietà senza alcun genere di limitazione.

Dal canto loro, le valute digitali si dividono in centralizzate e distribuite e/o decentralizzate, che si distinguono per la presenza o meno di un'entità centrale in grado di dirigere l'intero sistema. All'interno delle valute digitali decentralizzate esiste poi un sottoinsieme, denominato criptovaluta (*cryptocurrency*), al cui interno si inserisce Bitcoin, che fa ricorso alla crittografia per convalidare le transazioni e creare nuova moneta.

Come la maggior parte dei sistemi di nuova creazione, Bitcoin non è nata dal niente, ma è frutto della progressiva evoluzione di vari progetti precedenti, relativi a come risolvere il problema di creare un'alternativa digitale al denaro contante. Se ne erano occupati, ad esempio, David Chaum, nel suo paper "*Blind Signature for Untraceable Payments*"[1], e lo stesso Chaum, insieme a Stefan Brands, nel paper "*Minting Electronic Cash*"[2].

Nel novembre 2008 venne pubblicato un articolo, a firma di tale Satoshi Nakamoto, intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[3], nel quale veniva descritta una struttura concepita per trasferire il denaro digitale senza dover ricorrere al

[1] Cit. David CHAUM, "Blind signatures for untraceable payments", in *Advances in cryptology*, Springer, 1983, pp. 199-203.
[2] Cit. David Chaum e Stefan Brands, "Minting electronic cash", in *Spectrum, IEEE* 34.2. (1997), pp. 30-34.
[3] Cit. Satoshi NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, in https://bitcoin.org/bitcoin.pdf

coinvolgimento di servizi centralizzati o istituzioni finanziarie, risolvendo per la prima volta il problema del *double spending* (vale a dire del tentativo fraudolento di inviare a più destinatati la medesima quantità di denaro). Nonostante i notevoli sforzi fatti per individuare la reale identità di Satoshi, a tutt'oggi non si è scoperto molto di più su di lui e neppure si è appurato se si tratti di un singolo individuo o di un gruppo di persone che si celano dietro tale identità di comodo.

Il denaro digitale creato da Satoshi è gestibile utilizzando un software *open source* che può essere scaricato da ogni singolo utente ed appare del tutto evidente come la finalità principale di questa invenzione fosse quella di garantire che la verifica del denaro fosse gestibile da chiunque ne possedesse le chiavi.

La prima versione venne rilasciata all'inizio del 2009, come messa in pratica di un concetto già esistente, quello di "criptovaluta", che era stato descritto per la prima volta poco più di un decennio prima, nel 1998, da Wei Dai[4]. Non a caso, la nascita di questa peculiare tipologia di moneta ha avuto luogo proprio nel periodo forse più difficile della grande crisi economico-finanziaria apertasi nel 2008 negli Stati Uniti con la crisi dei mutui *subprime*, dunque in un momento in cui la fiducia nelle banche e negli organi centrali di controllo finanziario era ai minimi termini in tutto il mondo.

Nell'agosto 2010, una grave falla per la sicurezza venne trovata nel protocollo, a seguito della quale le transazioni non venivano correttamente verificate prima di essere immesse nella *blockchain*, il che avrebbe potuto consentire ad un eventuale aggressore di generare una quantità arbitraria di BTC. Tale falla venne sfruttata nel giro di pochi giorni, prima che venisse predisposta una patch correttiva, ma poi il "buco" venne chiuso e la situazione stabilizzata grazie a specifici interventi.

Negli anni successivi, il valore dei BTC è cresciuto sensibilmente, passando da semplici frazioni di dollaro agli attuali (luglio 2017) oltre 2.600. A partire dal 2011, del resto, varie associazioni hanno iniziato ad accettare BTC per le donazioni loro indirizzate; oppure – come nel caso della celebre Wikileaks – hanno utilizzato i BTC come strumento per ovviare al blocco delle donazioni tramite carte di credito e PayPal, attuato a loro danno dalle istituzioni creditizie su pressioni del governo USA. Nei due anni successivi, poi, si è dilatato notevolmente l'impiego di BTC in ambito commerciale, soprattutto grazie a

[4] Cit. http://weidai.com/bmoney.txt

payment processor come Bitpay e Coinbase, che consentono a qualsiasi sito Internet od esercente commerciale di accettare in pagamento BTC e convertirli con cambio fisso in valuta locale[5].

1.2. Crittografia

Al fine di poter comprendere correttamente molti meccanismi che stanno alla base di Bitcoin, è necessario introdurre alcuni concetti di crittografia, vale a dire della scienza che studia come preservare la riservatezza delle informazioni. Nel caso di Bitcoin, quello che realmente interessa non è tanto la riservatezza dei dati in sé, quanto la loro autenticazione (cioè la sicurezza in merito all'identità del mittente), integrità (cioè che non abbia subito manipolazioni) e non ripudiabilità (cioè che chi invia un messaggio non possa successivamente negare di averlo inviato).

Le proprietà che abbiamo appena citato possono essere ottenute grazie a un algoritmo di firma digitale, mentre un altro strumento essenziale alla comprensione di Bitcoin è la funzione di *hash*.

1.2.1. Hash

Una funzione crittografica di *hash* è un algoritmo matematico che trasforma dei dati di lunghezza arbitraria (messaggio) in una stringa binaria di dimensione fissa. Esso accetta in entrata un valore di lunghezza variabile e restituisce un valore di lunghezza fissa, di solito inferiore, denominato "valore di *hash*" oppure *message digest*. Quest'ultimo non dipende in maniera esplicita dall'ingresso, ma deve sembrare un valore casuale. A tal fine vengono impiegati algoritmi diversi, come MD5 e SHA.

Per fare un esempio, è possibile calcolare il valore di *hash* di una stringa utilizzando l'algoritmo SHA-1[6]. Se due file corrispondono esattamente, bit a bit, si avrà il medesimo

[5] Cit. Pier Francesco COSTA, *Bitcoin: aspetti tecnici, economici e politici di una crittovaluta*, Elaborato in Sistemi Distribuiti, Università di Bologna, Anno Accademico 2013/2014, p. 3 sg.

[6] SHA-1 ("Cantami o diva del pelide Achille l'ira funesta") = 1f8a690b7366a2323e2d5b045120da7e93896f47. Anche solo modificando un qualsiasi carattere della stringa in ingresso, si noterà che il valore di *hash* calcolato è completamente diverso:
SHA-1 ("Contami o diva del pelide Achille l'ira funesta") = e5f08d98bf118385e2f26b904cad23c734d530ffb

valore di *hash*, ma esiste pure la possibilità che due file diversi abbiano tale medesimo valore. Un evento del genere viene chiamato "collisione" e la probabilità del suo verificarsi dipende di norma dall'algoritmo di *hash* utilizzato e dalla lunghezza in bit del risultato: quanto maggiore sarà la lunghezza, tanto minore sarà la probabilità di collisione.

Il valore di *hash* viene utilizzato per verificare se un documento è stato alterato durante il transito. Il controllo dell'integrità ha luogo confrontando l'*hash* del messaggio prima e dopo la trasmissione.

1.2.2. Crittografia simmetrica

La crittografia simmetrica, nota anche come crittografia a chiave privata, è stata la prima forma di crittografia sviluppata dall'uomo. Essa prevede che, al fine di nascondere un messaggio per fare sì che questo sia leggibile solo dal destinatario, il mittente debba prima preoccuparsi di sottoporlo a cifratura. I cifrari, sotto questo profilo, sono algoritmi di cifratura e naturalmente ne esistono molti. Essi operano con una modalità per cui, se viene dato in ingresso all'algoritmo un messaggio in chiaro e un'informazione segreta (denominata "chiave"), l'algoritmo restituisce il messaggio cifrato e la chiave diventa l'unica informazione essenziale per decifrare il documento. La simmetria, a questo proposito, consiste appunto nel fatto che mittente e destinatario possiedano la medesima chiave, la quale risulta indispensabile sia per cifrare sia per decifrare[7], ciò che pone un problema non indifferente nel campo della comunicazione a distanza, in quanto mittente e destinatario devono avere la certezza di poter comunicarsi la chiave senza correre il rischio di essere intercettati.

1.2.3. Crittografia a chiave pubblica

Questo tipo di crittografia, nota anche come crittografia asimmetrica, consente di risolvere il problema appena citato: si provvede infatti a creare una coppia di chiavi (*keypair*), di cui una è nota come chiave privata e l'altra come chiave pubblica. La prima chiave viene generata casualmente e da essa si ricava – mediante una funzione

[7] Cfr. Pier Francesco COSTA, *Bitcoin: aspetti tecnici, economici e politici di una crittovaluta*, Elaborato in Sistemi Distribuiti, Università di Bologna, Anno Accademico 2013/2014, *op. cit.*, p. 7.

unidirezionale, che non consente di far derivare la prima dalla seconda – la chiave pubblica.

Gli algoritmi di crittografia a chiave pubblica operano in forma specifica, dato che richiedono una delle due chiavi per cifrare il messaggio e l'altra per decifrarlo. Così, se si intende inviare un messaggio cifrato, sarà sufficiente conoscere la chiave pubblica del destinatario e solo quest'ultimo avrà la possibilità di decifrare il messaggio utilizzando la propria chiave privata.

La crittografia a chiave pubblica viene impiegata, oltre che per lo scambio di messaggio cifrati, anche per l'attivazione di algoritmi di firma digitale: si provvede infatti a calcolare il valore di *hash* di un documento ed a cifrarlo con la propria chiave privata. A quel punto, si renderà necessario allegare tale nuovo valore – chiamato "firma" – al documento. Al fine di verificare la validità della firma sarà sufficiente decifrarla con la chiave pubblica e confrontarla con l'*hash* del documento. In caso di piena corrispondenza, la firma del documento sarà da ritenersi valida.

1.3. Come funziona bitcoin

1.3.1. Indirizzi

Esistono varie modalità per entrare in possesso di bitcoin:

- In primo luogo nei punti di scambio (*exchange*, il primo dei quali è divenuto operativo nel 2010), vale a dire i cambiavalute in cui è possibile acquistare e vendere BTC con euro, dollari e altre valute;
- In secondo luogo, ottenerli da qualcuno che ne è già in possesso mediante l'erogazione di beni o servizi;
- Per il tramite dell'attività di *mining*, che sarà analizzata nei paragrafi successivi.

I bitcoin vengono inviati e ricevuti utilizzando applicazioni mobili, software su computer oppure provider che forniscono un portafoglio digitale (*bitcoin wallet*). Essi sono poi mantenuti nel portafoglio digitale dell'utente registrato, al quale sono associate due chiavi, una pubblica e una privata. La chiave pubblica, in genere definita "indirizzo Bitcoin", è una specie di conto bancario ed è costituita da una sequenza alfanumerica di caratteri (di norma 34), che inizia sempre con i numeri 1 o 3. Ad esso l'utente può inviare oppure ricevere pagamenti. Dal momento che generare queste chiavi comporta costi e

tempi di calcolo ridotti, è utile specificare che ogni utente può ottenere un numero indeterminato di indirizzi.

Il problema dell'autenticazione, non essendovi un server centrale, viene quindi risolto mediante il ricorso a questa coppia di chiavi. Il messaggio che viene inviato al momento del pagamento conterrà la quantità di denaro da trasferire e la chiave pubblica del destinatario. Esso verrà "firmato" in forma digitale con la chiave privata del mittente, prima di essere inviato; ciò permetterà di fare sì che la chiave privata venga utilizzata per consentire che il pagamento sia autorizzato unicamente dall'effettivo proprietario della moneta[8]. A sua volta, il destinatario, nel momento in cui provvederà alla verifica della firma, avrà la prova crittografica del mittente, del destinatario e della quantità di denaro trasferita. Ne consegue che la chiave privata viene impiegata per fare in modo che il pagamento venga autorizzato solo dall'effettivo proprietario della moneta.

Bitcoin utilizza il sistema di firma digitale ECDSA[9] e, poiché le chiavi utilizzate da questo algoritmo sono assai lunghe e poco pratiche da gestire, si è preferito utilizzare come identificatore del destinatario, al posto della chiave pubblica, un *hash* lungo 160 bit della stessa, codificato in Base58Check, chiamato indirizzo. Tale codifica consente di verificare la correttezza formale dell'indirizzo al momento del suo inserimento.

1.3.2. Transazioni

Le transazioni di questa moneta digitale possono avere luogo via Internet tramite trasferimenti in denaro che non si basano sulla fiducia nei riguardi di terze parti (dunque questa è la prima forma di pagamento *trustless*). I terminali dei computer sono connessi gli uni con gli altri e, in base al protocollo p2p, si possono inviare direttamente bitcoin da persona a persona, senza ricorrere ad alcun tipo di mediatori, il che implica che le commissioni siano molto inferiori alla media.

---

[8] Cfr. Dario D'ANDREA, *Architetture di calcolo eterogenee per l'accelerazione del Bitcoin Mining*, Elaborato finale in Calcolatori Elettronici I, Università degli Studi di Napoli Federico II, Scuola Politecnica e delle Scienze di Base, Corso di Laurea in Ingegneria Informatica, Anno Accademico 2015/2016, Napoli 2016, p. 9 sg.

[9] Cfr. 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

Le tre garanzie principali da fornire sono, come già accennato: integrità (il destinatario deve essere sicuro che il messaggio non è stato alterato in alcun modo o addirittura sostituito); autenticazione (il destinatario deve essere sicuro dell'identità del mittente); non ripudiabilità (il mittente, dopo aver inviato il messaggio, non può negare di averlo inviato). Le transazioni vengono verificate, prima di essere immesse nella *blockchain*, da nodi speciali, detti "minatori".

In Bitcoin una moneta digitale è rappresentata da una catena di transazioni, che si incrementa progressivamente nel passaggio da un proprietario all'altro. Ogni proprietario trasferisce la moneta firmando digitalmente l'*hash* della transazione precedente e della chiave pubblica della catena.

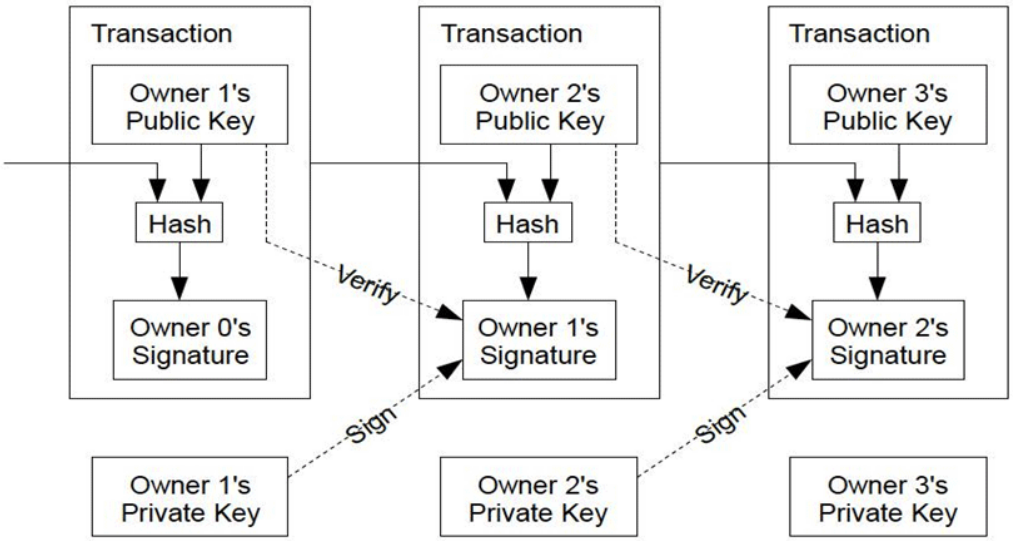

Fig. 1.1 Catena di transazioni Bitcoin

Chi riceve il pagamento ha la possibilità di controllare i vari passaggi di proprietà della moneta, verificando le firme presenti in ogni transazione, dal momento che la modifica di una sola transazione invaliderebbe tutte le precedenti, in quanto gli *hash* non corrisponderebbero più. In questo modo, tuttavia, chi riceve la moneta non può avere la certezza che uno dei precedenti proprietari non abbia inviato la stessa moneta a più persone, poiché questo sistema (detto del *double spending*) rappresenta indubbiamente uno dei problemi più gravi di un sistema di pagamento decentralizzato. Onde evitare

l'istituzione di organismi di controllo, che ricreerebbe quella centralizzazione che è quanto si desidera maggiormente evitare, l'unica possibilità al momento disponibile è che ogni utente possa essere a conoscenza di tutte le transazioni che hanno luogo all'interno del sistema, in modo da poter rifiutare transazioni che eventualmente abbiano già avuto luogo[10].

1.3.3. Timestamp

Bitcoin ha risolto il problema di datare le transazioni ricorrendo a un server di *timestamp* distribuito. Un server di questo tipo calcola il valore *hash* dell'oggetto che intende datare e lo pubblica ad esempio su un giornale. Il *timestamp* costituisce la prova che l'oggetto esisteva già prima che ne venisse calcolato l'*hash*, per cui è possibile stabilire una datazione anteriore a quella dell'uscita del giornale in edicola. Ogni *timestamp* include, oltre all'oggetto che deve datare, anche il valore *hash* del *timestamp* immediatamente precedente, creando in tal modo una catena. L'ordine dei *timestamp* – e dunque quello di creazione degli oggetti – non può a questo punto essere modificato, a meno di non ricreare da principio l'intera catena.

Onde realizzare una struttura distribuita di *timestamp*, composta da tanti nodi in configurazione *peer-to-peer*, Bitcon fa uso di un sistema *proof-of-work* simile ad Hashcash, che rende superflua la pubblicazione su un giornale, in quanto è facile da verificare. All'insieme di oggetti da datare viene aggiunto un numero, denominato *nonce*, di cui si calcola l'*hash* mediante l'algoritmo SHA-256[11]. Tale operazione viene ripetuta cambiando *nonce* finché non si ottiene un valore *hash* che inizi con un determinato numero di zeri (inferiore al *target value*). Occorre sottolineare che l'output della funzione di *hash* è totalmente imprevedibile, per cui l'unico modo per poter trovare un particolare valore di output consiste nel fare tentativi più o meno casuali, così come ci si comporterebbe nel caso si volesse indovinare la combinazione di una cassaforte.

Com'è ovvio, se si aumenta il numero degli zeri richiesti, aumenta esponenzialmente lo sforzo richiesto per trovare un *hash* valido. Se qualcuno volesse modificare la datazione di un oggetto, rimuovendolo da un *timestamp* ed inserendolo in un altro, dovrebbe rifare

[10] Cfr. Pier Francesco COSTA, *Bitcoin: aspetti tecnici, economici e politici di una crittovaluta*, Elaborato in Sistemi Distribuiti, Università di Bologna, Anno Accademico 2013/2014, p. 12 sg.
[11] L'acronimo SHA sta per *Secure Hash Algorithm.*

tutto il lavoro necessario a generare un *timestamp* valido senza il tale oggetto e tutti quelli successivi nella catena. L'unico modo per riuscirvi consiste nel poter disporre di una potenza di calcolo maggiore della rete nel suo complesso[12].

1.3.4. Blockchain

La catena di *timestamp* utilizzata in Bitcoin viene chiamata *blockchain*. Ogni *timestamp* viene definito "blocco" e contiene un numero variabile di transazioni. La *blockchain* non viene aggiornata in tempo reale, ma viene aggiunto un gruppo di transazioni, chiamato blocco, ogni dieci minuti. Ogni volta che viene aggiunto un blocco, si procede all'emissione di una quantità prestabilita di bitcoin, destinata al minatore che per primo sia riuscito a verificarne la validità.

La *blockchain* è un database distribuito che contiene tutta la cronologia delle transazioni avvenute sulla rete Bitcoin; è composta da una catena principale e da blocchi chiamati orfani. Questo perché può accadere che due blocchi vengano generati quasi contemporaneamente a partire dal medesimo blocco genitore. In tal caso, ogni minatore decide quale sia il blocco valido e lo utilizza per costruire il blocco successivo. Nasce così, all'interno della catena, una divisione e i due rami continuano ad allungarsi, indipendentemente l'uno dall'altro. Il ramo su cui si concentra la maggiore potenza di calcolo cresce più celermente dell'altro, finché i minatori non decidono di abbandonare il ramo orfano. Quando ciò accade, le transazioni incluse da quest'ultimo vengono ignorate e la costruzione dei blocchi continua sul ramo principale[13]. Ne consegue che il *blockchain* viene utilizzato per dare ordine alle transazioni, mentre la catena delle transazioni tiene conto dei cambiamenti di proprietà della moneta.

Le transazioni sono per loro natura irreversibili, per cui, una volta incluse nella *blockchain*, non possono essere annullate. L'unica modalità per ritornare in possesso della

[12] Cfr. Pier Francesco COSTA, *Bitcoin: aspetti tecnici, economici e politici di una crittovaluta*, Elaborato in Sistemi Distribuiti, Università di Bologna, Anno Accademico 2013/2014, *op. cit.*, p. 13 sg.
*[13] Cit. *Ivi*, p. 14.

propria moneta consiste nel farsi rimandare indietro i bitcoin dal destinatario[14]. In ogni caso, chiunque può controllare la *blockchain* e osservare le transazioni in tempo reale.

1.3.5. Protocollo

Questa è la sequenza di funzionamento di Bitcoin:

- Le nuove transazioni vengono mandate a tutti i nodi;
- Ogni minatore controlla che le transazioni siano valide e le raccoglie in un blocco insieme all'*hash* del blocco precedente;
- Ogni minatore opera per trovare un *proof-of-work* valido per il proprio blocco;
- Quando ciò accade, lo invia insieme al blocco a tutti gli altri nodi.
- I nodi accettano il nuovo blocco solo se contiene transazioni valide e non incluse in precedenza in altri blocchi;
- I minatori danno prova 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. Ogni nodo opera sul blocco che ha ricevuto per primo, ma conserva l'altro nel caso diventi parte del ramo più lungo[15].

1.3.6. Minatori e incentivi

L'attività di verificare transazioni e aggiungere blocchi al *blockchain* è chiamata *mining* (letteralmente "estrazione") e viene svolta da nodi speciali, chiamati *miners* ("minatori"). I minatori svolgono il duplice ruolo di verifica delle transazioni e di emissione dei bitcoin. Per il lavoro svolto, che implica consumo di risorse di calcolo e di energia elettrica, i *miners* vengono premiati mediante l'emissione di nuova moneta. Vengono in tal modo premiati i nodi della rete che più contribuiscono alla sicurezza del protocollo. Ciò non costituisce soltanto una forma di incentivo, ma anche un'altra modalità di emissione della valuta. La quantità di BTC emessa da un blocco è

[14] Cfr. Dario D'ANDREA, *Architetture di calcolo eterogenee per l'accelerazione del Bitcoin Mining*, Elaborato finale in Calcolatori Elettronici I, Università degli Studi di Napoli Federico II, Scuola Politecnica e delle Scienze di Base, Corso di Laurea in Ingegneria Informatica, Anno Accademico 2015/2016, Napoli 2016, *op. cit.*, p. 15.
[15]Cfr. Pier Francesco COSTA, *Bitcoin: aspetti tecnici, economici e politici di una crittovaluta*, Elaborato in Sistemi Distribuiti, Università di Bologna, *op. cit.*, p. 14 sg.

predeterminata e si riduce geometricamente con il passare del tempo, dimezzandosi ogni 210 mila blocchi.

Un altro tipo di incentivo è rappresentato dalla *fee* (commissione), vale a dire da quella specie di tariffa che il mittente può decidere di pagare al fine di velocizzare le transazioni. Le transazioni accompagnate da una *fee* vengono gestite in via prioritaria, dato che i minatori hanno interesse ad includerle nei blocchi. Quel che è certo è che la gestione delle transazioni si è fatta sempre più difficile e complessa, e oggi effettuare il *mining* richiede notevoli investimenti. Di conseguenza, la maggioranza dei minatori non lavora più da sola, ma si unisce per formare le *mining pools*, in quanto ciò consente loro di ottenere più facilmente i risultati sperati.

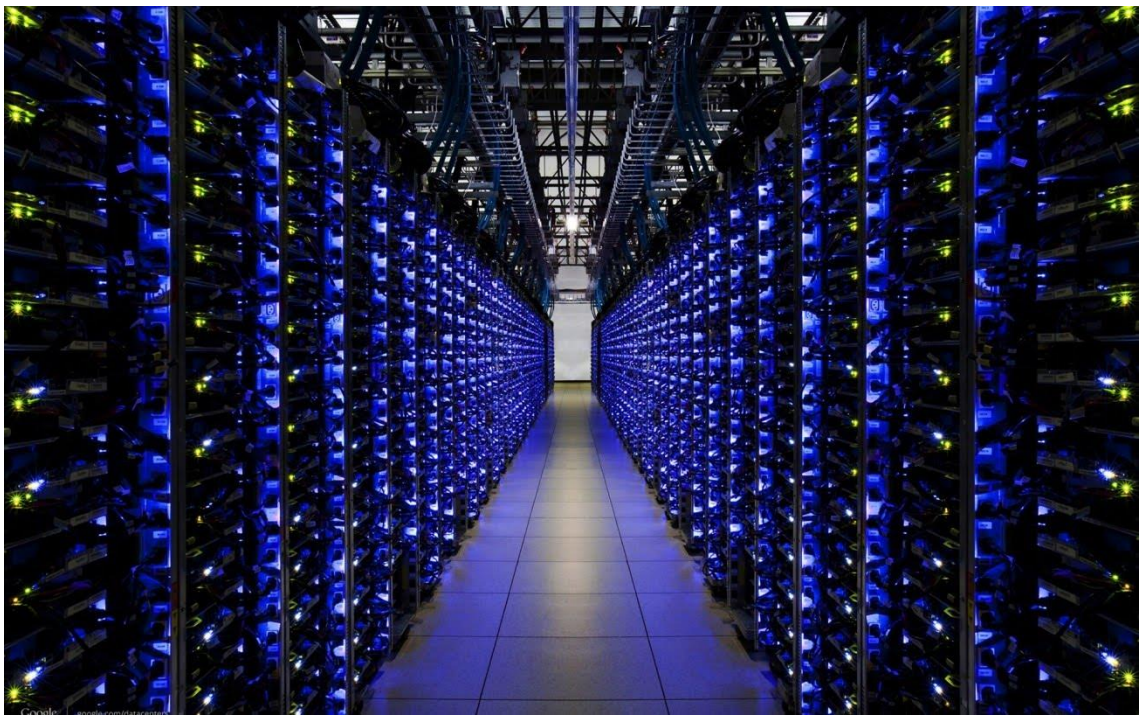

Fig. 1.2. Mining Farm Bitcoin

1.3.7. Quantità

Al momento attuale, l'unità di misura più piccola è di 0,00000001 BTC, denominata "satoshi"; tuttavia, modificando il protocollo, è possibile aumentare indefinitamente la divisibilità dei BTC.

2 Scalabilità

Background

Come ben si sa, nel momento in cui il valore di un oggetto sale troppo velocemente il problema maggiore diventa la sua sostenibilità di crescita esponenziale. Anche Bitcoin non è riuscito a evitare questa regola del mercato. Infatti, nell'ultimo anno la sua crescita è stata talmente fulminea da aver mandato in tilt il sistema distribuito di gestione delle transazioni. Sembra inverosimile, ma con l'aumento della popolarità di Bitcoin si profilano all'orizzonte i maggiori rischi riguardo al suo futuro.

Il sistema Bitcoin si regge su un grande database distribuito che tiene traccia di tutte le transazioni. Attualmente esiste un limite tecnologico nella dimensione dei blocchi di Bitcoin che corrisponde a 1 MB, che permette di raggiungere un limite al massimo di sette transazioni per secondo, impostato per evitare che la rete venga ingolfata da tante transazioni piccolissime.

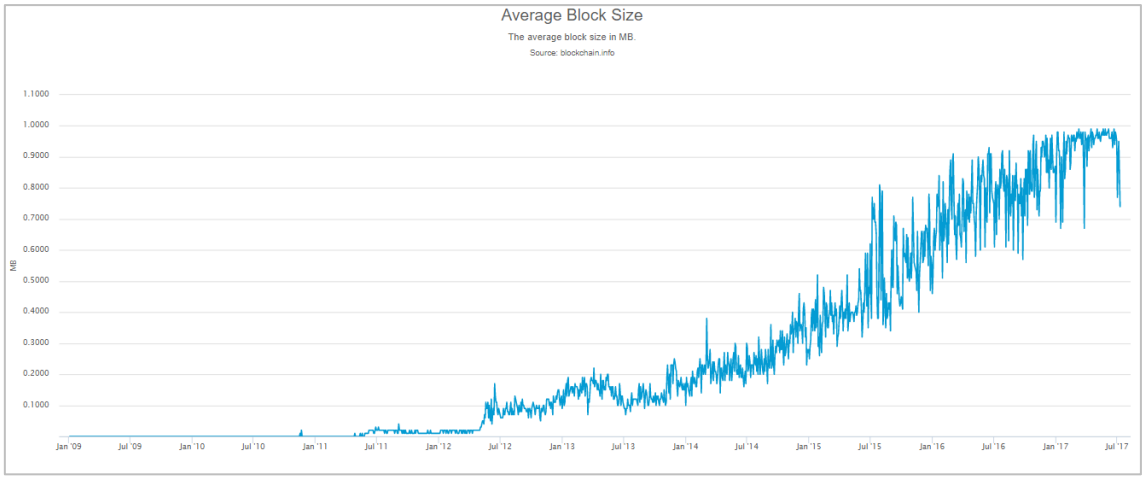

Figura 2.1. Dimensione media del blocco nella blockchain di Bitcoin nel tempo.

Con la crescita di Bitcoin il numero di transazioni effettuate ha raggiunto il limite di capacità del blocco e la barriera di 1 MB si sta traducendo in un collo di bottiglia. Gli utenti sono indotti ad aumentare le commissioni per avere le transazioni confermate. Troppi ritardi (anche più di 24 ore) e l'aumento delle commissioni delle transazioni rischiano di spostare il mercato verso le altre crittovalute.

La soluzione che si sta percorrendo consiste nello scindere il sistema in due piattaforme complementari: una con limite nella dimensione dei blocchi incrementato e un'altra uguale all'originale.

2.1. Cenni storici

Bitcoin Core inizialmente è stato rilasciato senza nessun limite di dimensione del blocco. Tuttavia il limite massimo dei messaggi di rete era limitato dal codice a 32 MiB, causando così un margine superiore alla dimensione del blocco [7].

```
static const unsigned int MAX_SIZE = 0x02000000; /*32MiB*/
```

Il 15 luglio 2010 Satoshi Nakamoto modifica il codice di Bitcoin Core in modo che non crei i blocchi più grandi di 990.000 byte [8].
Due mesi dopo, nel settembre 2010, Satoshi Nakamoto modifica il codice mettendo un limite a 1.000.000 byte (1 MB) [9].

main.h
(https://github.com/bitcoin/bitcoin/blob/master/src/consensus/consensus.h)

```
static const unsigned int MAX_BLOCK_BASE_SIZE = 1000000;
```

In entrambe le date non ha dato delucidazioni in merito al limite della dimensione del blocco ma, nelle sue dichiarazioni successive, in un post su BitcoinTalk[16,17] [10][11] si è dichiarato a favore dell'aumento di Block Size, ma senza specificare date future su un possibile fork.

Poi, alcuni suoi post successivi [12] suggeriscono che il blocco a 1 MB non era stato pensato per limitare il consumo di banda o facilitare il mantenimento di un nodo completo su un computer domestico. Ma che il limite dal principio era destinato a essere sollevato per favorire maggiormente la diffusione.

La prima proposta riguardante l'aumento del limite massimo della dimensione del blocco risale al 31 gennaio 2013 e fu pubblicata anche nel forum di BitcoinTalk come discussione dal titolo "The Max Block Size Fork" [13].

Il dibattito è sotteso da discussioni sui benefici e sulle potenziali debolezze di diversa natura. Da una parte l'aumento del limite massimo della dimensione del blocco è indispensabile in caso di rapido incremento del numero di transazioni. Mentre, dall'altra parte, le opinioni che non sono a favore indicano che ciò cambierà completamente il protocollo del Bitcoin. Infatti, probabilmente, cambierà anche la quantità di offerta di

[16] 3 ottobre 2010: alla proposta su BitcoinTalk di incrementare il limite massimo di blocco Nakamoto rispose:

> "Possiamo procedere ad inserire gradualmente un cambiamento più avanti, se ci dovessimo avvicinare maggiormente ad una situazione che lo richiede".

[17] Successivamente Nakamoto si dichiara a favore di un possibile fork:

> "Il limite della dimensione massima del blocco può essere inserito in modo graduale, come ad esempio:
>
> ```
> if (blocknumber > 115000)
>     maxblocksize = largerlimit
> ```
>
> Le modifiche potranno essere intraprese prima che il limite si riveli critico, in modo che, nel momento in cui il sistema raggiunge quel numero di blocco e la nuova versione entra in vigore, le versioni più vecchie che non lo hanno risultino già obsolete.
>
> Quando saremo vicini al numero di blocco limite, posso inserire un avvertimento alle versioni vecchie per garantire che sappiano che è necessario l'aggiornamento".

Bitcoin precedentemente fissata a soli 21 milioni. Inoltre l'aumento del limite massimo di dimensione del blocco avrebbe delle conseguenze sulla decentralizzazione e sulla diversificazione della rete.

Da questa discussione nasce la proposta di Jeff Garzik che si basa sulla possibilità di concedere ai minatori la scelta delle dimensioni massime dei blocchi, che è l'idea principale sulla quale si fonda Bitcoin Unlimited. Tale proposta ha suscitato diverse critiche all'interno della comunità, si suppone infatti che i minatori più grandi con potenza di hash maggiore avranno sotto controllo la rete Bitcoin e ciò avrebbe conseguenze sulla decentralizzazione della rete.

In seguito sono stati proposti diversi miglioramenti al protocollo riguardanti il problema della scalabilità, denominati BIP (Bitcoin Improvement Proposals):

BIP 101 [20]

22 giugno 2015 Gavin Andrsen presenta il progetto di miglioramento al protocollo denominato BIP 101 [14]. Secondo questa proposta, il limite della dimensione del blocco dovrebbe aumentare fino a 8 MB nel 2016 e poi raddoppiare ogni due anni fino a raggiungere 8.192 MB nel 2036, dopo il 2036 il limite dovrebbe rimanere costante. La ragione che sta alla base di questa proposta è che la potenza della CPU e la capacità di storage crescono esponenzialmente con la legge di Moore [15] quindi dovrebbero essere in grado di sostenere l'aumento biennale del limite massimo della dimensione blocco. Il progetto ha avuto tante critiche in quanto si basa sul adottamento di hard fork che nel caso di non accordo fra tutti i principali membri del sistema Bitcoin provocherebbe una scissione permanente nella blockchain con tutte le conseguenze negative riguardanti il prezzo e la fiducia degli utenti. Inoltre, mentre il limite di dimensione del blocco in BIP 101 cresce ad una velocità prevedibile, è difficile valutare se tale velocità corrisponderebbe alla crescita della rete Bitcoin in futuro.

Bitcoin XT Fork [16]

Non avendo ottenuto il supporto dalla comunità di Bitcoin, Gavin Andresen e Mike Hearn decidono di proseguire per la loro strada implementando il progetto BIP 101 in un hard fork Bitcoin XT separato da Bitcoin Core. Inizialmente Bitcoin XT è stato presentato con l'aumento di memoria dinamico, cioè si estende solo quando serve, per fare in modo

che la Bitcoin Core e bitcoin XT siano perfettamente compatibili**.** Gli sviluppatori di Bitcoin si sono dati una tempistica secondo la quale entro gennaio del 2016 Bitcoin XT doveva essere utilizzato da almeno il 75% degli utenti Bitcoin e solo in questa condizione il limite massimo del blocco doveva iniziare ad aumentarsi biennalmente. Nel 2016 la proposta non ha ottenuto il consenso necessario per entrare in vigore sulla rete Bitcoin quindi il suo uso è stato in costante perdita dal marzo 2016 in poi [17].

BIP 100

Si tratta di propsta di Jeff Garzik che si basa sull'idea di concedere ai minatori di votare per l'aumento o la diminuzione della dimensione massima dei blocchi all'interno di una gamma da 1MB a 32 MB.

BIP 109 e Bitcoin Classic Fork

*S*i tratta di una proposta si Gavin Andrsen secondo la quale il limite della dimensione del blocco dovrebbe aumentare a 2MB. Tale proposta è stata implementata a febbraio 2016 in un hard-fork Bitcoin Classic separato da Bitcoin Core che presente tuttora ma costituisce una frazione davvero ridotta.

2.2. Numero massimo di transazioni per secondo

Attualmente il limite della dimensione del blocco corrisponde a 1 MB [18], anche se una piccola quantità di questo spazio (ad esempio l'intestazione del blocco) non è disponibile per memorizzare le transazioni [19].

La dimensione di ogni transazione dipende da diversi fattori, ad esempio dalla quantità di ingressi e uscite della transazione oppure a seconda se si tratta di ingressi di firma singola o ingressi di firma multipla.

Il metodo più immediato per calcolare il numero di transazioni al secondo (Tps) è dividere per la dimensione media di una transazione la dimensione massima di un blocco della blockchain (1 Mb) divisa per il numero medio di secondi tra i blocchi.

Ad esempio:

1 MB: dimensione massima di un blocco della blockchain;

240 byte: dimensione media di una transazione;

600: il numero medio di secondi tra i blocchi, in media ogni 10 min. (600 sec.) viene minato un blocco.

$$1.000.000/240/600 = \sim 7 \text{ Tps}$$

2.3. Hard fork e soft fork

In base a quanto accennato precedentemente, la maggior parte delle proposte principali riguardanti il problema della scalabilità di Bitcoin richiede l'adottamento delle manovre di hard fork o di soft fork. Vediamo ora le differenze e gli effetti di queste due operazioni [20].

Il *soft fork* è un aggiornamento del protocollo Bitcoin. Generalmente si tratta del passaggio da una regola più permissiva a una meno permissiva. Questo cambiamento solitamente è ben gradito da tutti i nodi, *miners*, client e altri software che cooperano con Bitcoin. La caratteristica principale dell'adottamento di soft fork è la *reversibilità*. L'idea principale del soft fork è quella di nascondere le modifiche ai vecchi client (pre-soft-fork), in modo che siano in grado di leggere i nuovi dati senza accorgersi delle modifiche.

L'*hard fork* è una sostituzione del protocollo Bitcoin che provoca una scissione permanente nella blockchain. Generalmente questa manovra permette di avere una situazione che prima non era valida (ad esempio aumento del blocco a 2 MB). Con un hard fork non è possibile mantenere il vecchio client senza conseguenze (ad esempio, nel caso di aumento del blocco a 2 MB, dopo il primo blocco minato più grande di 1 MB, si creerebbe una suddivisione della blockchain, in quanto i nuovi e i vecchi client lavorerebbero con regole incompatibili). Caratteristica principale nell'adottamento di hard fork è la *irreversibilità.*

Nel passato il Bitcoin ha subito diversi soft fork e alcuni hard fork. Bitcoin XT (luglio, 2015) e Bitcoin Classic (10/02/2016) sono tra i più popolari hard fork.

Ambedue sono ancora presenti ma costituiscono una frazione davvero ridotta: non superano il 2,5% del totale in termini di tutti i nodi messi insieme [21].

2.4. Confronto con Visa

Wiki ufficiale ha realizzato un'analisi quantitativa riguardante la scalabilità di Bitcoin [22]. Come metro di paragone è stato preso il circuito per carte di credito Visa, che può supportare in media 2000 transazioni al secondo (tanto da toccare punte giornaliere di 4000 Tps), mentre la rete Bitcoin permette di raggiungere un limite massimo di 7 Tps.

Nel caso Bitcoin raggiungesse il volume di 2000 Tps sono stati calcolati diversi requisiti:

Connessione a Internet. È il parametro meno critico, in quanto il flusso di dati verso il nodo dovrebbe essere di circa 8 megabit al secondo[18], gestibile con le attuali connessioni Adsl residenziali.

Capacità di calcolo. Questo requisito non causa problemi, in quanto anche una Cpu Intel Core i7 da 2,2 Ghz può facilmente elaborare la mole di lavoro richiesta.

Capacità di storage. È il collo di bottiglia. Attualmente la dimensione della blockchain è di circa 120 Gb e tende a crescere linearmente all'aumentare delle transazioni. Nel caso in cui Bitcoin raggiungesse il volume di 2000 Tps, la capienza dovrebbe aumentare, ciò richiede un aumento significativo nel consumo delle risorse, questo limiterebbe la possibilità di un singolo utente di mantenere un nodo completo attivo su un PC domestico. Esistono diversi progetti per limitare le dimensioni della blockchain e ridurre i dati richiesti per la verifica delle transazioni, ma al momento non sono ancora stati implementati.

[18] Siccome la dimensione della transazione varia da 0,2 kilobyte a più di 1 kilobyte, supponiamo che la dimensione media di una transazione sia 512 byte:
(2000tps * 512 byte) / 1024 / 1024 = 0.97 MB al secondo * 8 = 7,8 MB / secondo.

2.5. Espressioni di scalabilità

La notazione matematica O-Grande [23] è utilizzata per descrivere il comportamento asintotico delle funzioni ed è considerata come una scorciatoia utilizzata dagli scienziati informatici per descrivere il livello della scalabilità del sistema.

Segue una lista di classi di funzioni comunemente incontrate nell'analisi di scalabilità. Tutte queste espressioni vanno considerate per *n* che tende all'infinito. Le funzioni sono elencate per magnitudine crescente (ogni classe di funzioni elencata è un sovrainsieme delle precedenti).

- *O(1) (costante)* significa che un sistema ha più o meno le stesse proprietà indipendentemente da quanto grande diventa.
- *O(n) (lineare)* significa che un sistema scala linearmente: raddoppiando il numero di cose (utenti, transazioni, ecc.) raddoppia la quantità di lavoro.
- *O(n2) (quadratica)* significa che un sistema scala quadraticamente: raddoppiando (2x) il numero di cose quadruplica (4x) la quantità di lavoro.

2.5.1. Propagazione dei blocchi O(1)

Bitcoin Core trasmette le transazioni non confermate e dopo trasmette blocchi contenenti molte delle stesse transazioni. Questa ridondanza dei blocchi può essere eliminata per consentire ai minatori di propagare grandi blocchi più rapidamente ai nodi di rete attivi e potrebbe anche significativamente ridurre l'esigenza di picchi di banda del minatore.

2.5.2. Fabbisogno totale di risorse di convalida della rete O(n2)

Mentre lo sforzo di convalida necessario per ciascun nodo completo cresce semplicemente in O(n), lo sforzo di convalida combinato di tutti i nodi cresce di O(n2) mantenendo costante il decentramento. Per un singolo nodo, ci vuole il doppio delle risorse al fine di elaborare le transazioni del doppio degli utenti, mentre per tutti i nodi ci vuole un combinato pari al quadruplo delle risorse per poter elaborare le transazioni del doppio degli utenti, ipotizzando che il numero di nodi pieni aumenti in proporzione al numero di utenti.

Ogni transazione Bitcoin on-chain deve essere elaborata da ogni nodo completo. Supponendo che una determinata percentuale di utenti esegua dei nodi completi (n) e che ciascun utente crei in media un determinato numero di transazioni (di nuovo n), in tal caso il fabbisogno totale di risorse della rete sarà pari a n2 = n * n.

Ad esempio:

• Immaginiamo che una rete inizi con 100 utenti e 2 nodi totali (una proporzione del 2%).

• La rete raddoppia in termini di utenti, che diventano 200. Il numero di nodi raddoppia anch'esso, arrivando a 4 (mantenendo un rapporto del 2% di sicurezza decentralizzata a basso livello di fiducia).

Tuttavia, raddoppiare il numero di utenti equivale a raddoppiare il numero di transazioni, e ogni nodo deve elaborare ciascuna transazione. Dunque, ogni nodo si trova a effettuare il doppio del lavoro con la sua larghezza di banda e la sua Cpu. Con il raddoppio del numero di nodi e il raddoppio della quantità di lavoro per nodo, il lavoro totale aumenta di 4 volte.

In breve, ciò significa che il costo complessivo per il mantenimento di tutte le transazioni on-chain quadruplica ogni volta che raddoppia il numero di utenti.

Lo sforzo di risorse di convalida fatto da ogni singolo nodo completo aumenta linearmente O(n), e i critici della comunità affermano che questo costituisce l'unico fatto rilevante in termini di dimensionamento della scalabilità. Alcuni critici, inoltre, sottolineano come la rivendicazione del fabbisogno totale di risorse di convalida della rete O(n2) parta dal presupposto che la decentralizzazione debba essere mantenuta costante come le scale di rete, e che questo non sia un principio fondante di Bitcoin.

2.6. Block Size Soft limits

Nel corso degli anni Bitcoin Core ha preconfigurato un limite per bloccare i blocchi superiori a 1 MB. Tali "limiti" sono le opzioni di configurazione che aiutano i minatori a produrre i blocchi di dimensioni ragionevoli. Siccome un blocco può essere composto anche da una singola transazione, un minatore può sempre restringere le sue dimensioni con:

```
blockmaxsize = <dimensioni>
```

Si discute sulla possibilità di concedere ai minatori di votare per l'aumento o la diminuzione della dimensione massima dei blocchi.

2.6.1. Vantaggi e limiti

Visto che un blocco può essere composto anche da una singola transazione, un minatore può sempre restringere le sue dimensioni, ma lasciargli decidere anche le dimensioni massime potrebbe creare dei *problemi* per diversi motivi:

- *I minatori ricavano il beneficio, gli altri ne pagano i costi*: i grandi blocchi procurano più commissioni ai minatori, ma i minatori non hanno bisogno di conservare questi blocchi per più di qualche giorno. Gli altri utenti che necessitano della piena sicurezza della validità o che provvedono a servizi volti ad alleggerire portfoli degli altri pagano i costi del downloading e dello stoccaggio di questi blocchi di grandi dimensioni.

- *I minatori più grandi possono permettersi la banda larga più potente*: ciascun minatore deve scaricare ogni transazione contenuta in un blocco, il che significa che deve sostenere il costo di una connessione ad alta velocità. Ciononostante un minatore che possiede un hash rate di 8,3% del totale può rientrare dai costi con i circa 300 Btc che riesce a produrre giornalmente, mentre un minatore che possiede un hash rate dello 0,7% deve riuscire a rientrare dalle spese con i soli 25 Btc giornalieri.

- *Produzione dell'hardware centralizzato*: solo poche compagnie al mondo producono equipaggiamento efficace per il *mining* e molte di esse hanno deciso di cessare la vendita al pubblico. Questo proibisce agli utenti ordinari di Bitcoin di partecipare al processo anche se sarebbero disposti a sostenerne i costi.

- *Le votazioni a favore di minatori più grandi*: le votazioni basate sulle dimensioni dell'hash rate metterebbero i minatori attualmente maggiori in condizione di imporre i propri vincoli alla minoranza, il che porterebbe a una situazione simile a una lobby potente che può permettersi di far approvare regolamenti a danno dei piccoli utenti.

- *I minatori potrebbero ignorare gli effetti sugli altri utenti*: questo si dimostrò durante i fork del luglio 2015 [24] (quando, nonostante le grandi perdite di oltre $50.000 dovute a catene invalide, e nonostante i minatori fossero stati avvisati che perseverare con i fork avrebbe danneggiato gli altri utenti, essi continuarono imperterriti nel *mining*).

Tuttavia vi sono altri motivi a *favore* della possibilità di dare ai minatori la scelta della dimensione dei blocchi:

- *Partecipanti autenticati*: i minatori sono parte attiva in Bitcoin e lo possono provare aggiungendo dati ai blocchi che essi stessi creano, mentre è molto più difficile autenticare gli utenti di Reddit e BitcoinTalk.

- *Blocchi grandi aumentano i costi dei minatori*: i piccoli minatori dotati di connessioni non efficienti sarebbero svantaggiati dalla produzione dei blocchi molto grandi. Ne soffrirebbero però anche i grandi minatori perché potrebbero vedersi ridurre le percentuali dei loro profitti a causa dei costi da sostenere per la banda larga e altre spese connesse.

2.7. Effetti dell'aumento del Block Size

In base a quanto affermato precedentemente, oggi lo spazio disponibile dentro ogni blocco è limitato a 1 MB, che permette di raggiungere un limite al massimo di 7 transazioni per secondo. Sono state effettuate diverse analisi nel corso del tempo per poter aumentare la dimensione del blocco. Dal punto di vista tecnico, qualunque persona sarebbe capace di fare una modifica al protocollo Bitcoin e proporla al resto della rete. Tale modifica renderebbe la rete più fluida per far sì che gli utenti possano ricevere le proprie transazioni convalidate più facilmente. Ciò farebbe diminuire la competizione fra gli utenti, che aumentano le commissioni per i *miners* per ricevere una conferma delle transazioni, pertanto il costo delle transazioni sarebbe più conveniente. Ma nonostante tutti i vantaggi, l'aumento del limite massimo avrebbe ripercussioni sulla sicurezza della rete.

2.7.1. Sicurezza degli utenti

Un eventuale aumento delle dimensioni dei blocchi potrebbe avere degli effetti sulla sicurezza degli utenti. La sicurezza di Bitcoin è fortemente dipendente dal numero di utenti attivi che proteggono i loro bitcoin con un nodo pieno come Bitcoin Core. Più sono gli utenti attivi che utilizzano i nodi pieni più è difficile per i minatori ingannarli, facendogli accettare bitcoin falsi o attuando altri tipi di frodi.

I nodi completi devono scaricare e verificare ogni blocco, inoltre la maggior parte di nodi archivia i blocchi e in più re-invia transazioni ad altri utenti della rete. Maggiori diventano le dimensioni dei blocchi, maggiori diventano le difficoltà per fare tutto ciò. Per questo motivo si ritiene che l'aumento delle dimensioni dei blocchi comporti una riduzione degli utilizzatori di nodi pieni e nello stesso tempo limiterebbe anche il numero di chi avrebbe intenzione di utilizzare i nodi pieni in un secondo momento. Inoltre i blocchi pieni possono favorire la centralizzazione del *mining*, in un momento in cui il *mining* è già fortemente centralizzato. In questo modo si rendono più semplici le transazioni essendo queste già state confermate più volte.

2.7.2. Sicurezza della Proof-of-work (Pow)

La sicurezza del Pow dipende da quanto spendono i minatori in hardware di calcolo. Tuttavia, per produrre efficacemente, i minatori hanno anche bisogno di investire nella banda larga, in modo da poter ricevere nuove operazioni e blocchi creati da altri *miners* e per poter caricare nuovi blocchi; inoltre devono investire denaro anche in Cpu utili a convalidare le transazioni. Tali costi aggiuntivi non contribuiscono direttamente alla sicurezza Pow.

All'aumento delle dimensioni dei blocchi corrisponde un aumento della necessità della larghezza di banda. Se le dimensioni dei blocchi aumentano più velocemente dei costi della larghezza di banda e del deprezzamento dell'hardware, i minatori avranno meno soldi per la sicurezza Pow in rapporto al reddito netto di guadagno. Inoltre, i blocchi più grandi hanno un rischio maggiore di diventare obsoleti (orfani), il che è correlato direttamente a una minore sicurezza del Pow. Ad esempio, se il tasso medio di blocchi obsoleti in rete è del 10% vuol dire che il 10% di Pow eseguita non protegge le operazioni sui blockchain.

Al contrario, i blocchi più grandi che hanno una rendita per la transazione più bassa possono far aumentare la domanda di transazioni a catena. In questo modo il guadagno finale dei minatori sarà maggiore nonostante una rendita media per transazione più bassa. Ciò incrementa la sicurezza di rete, aumentando il reddito che sostiene la generazione della Proof-of-work.

2.7.3. Transazioni in sospeso

Uno dei problemi maggiori riguardo al limite nella dimensione dei blocchi è il problema delle transazioni in sospeso. Se i blocchi non sono abbastanza grandi da includere tutte le transazioni in sospeso, i minatori mettono le transazioni in coda. Le operazioni che comprendono blocchi a maggiore rendita saranno elaborate prima dei blocchi di transazioni meno redditizi. Partendo dal presupposto che i blocchi più grandi non causerebbero una diminuzione della domanda di elaborazione delle transazioni on-chain dovuti a una percezione di mancata resistenza al decentramento da parte del network, i blocchi che invece sono troppo piccoli per includere tutte le transazioni in sospeso si tradurranno in una diminuzione della domanda di elaborazione a catena. Perciò le transazioni saranno meno di quante sarebbero se i blocchi fossero grandi abbastanza da includere tutte le transazioni in sospeso.

3 Analisi della scalabilità

Background

Scalabilità rappresenta uno dei maggiori rischi riguardo al futuro di Bitcoin. Il numero di transazioni realizzate ogni secondo ha raggiunto il limite di capacità del blocco. La barriera di 1 MB non è più sufficiente e gli utenti sono costretti ad aumentare le commissioni per avere le transazioni confermate, perciò ora Bitcoin non è più conveniente per fare le transazioni di basso importo, ad esempio un caffè retribuito con Bitcoin costerebbe il doppio. Pertanto le transazioni di Bitcoin hanno raggiunto il record storico dei ritardi (anche più di 24 ore) che cresce in tempo reale. Dunque, è necessario aumentare la dimensione del blocco per aumentare la velocità massima di elaborazione delle transazioni di Bitcoin e ridurre i ritardi di conferma. Come emerge dalla tabella 3[19] [25], anche un aumento di block size pari a 2 MB sarebbe sufficiente per risolvere momentaneamente i problemi con i ritardi di conferma, pertanto la *usability* della crittovaluta ne trarrebbe un grande vantaggio. D'altra parte è difficile prevedere come l'aumento di block size influenzerà la capacità di storage e il traffico Internet con tutte le conseguenze sulla sicurezza e la decentralizzazione della rete.

Througpt, tps	Block Size, MB	Network load, %	Median processing time, min	Processing of 90% tx, min
3.5	*1*	*100.0*	*129.1*	*380.0*
	2	*50.0*	*8.5*	*29.0*
	3	*33.3*	*7.3*	*24.7*
	4	*25*	*7.0*	*23.5*
	8	*12.5*	*7.0*	*23.0*
	20	*5.0*	*7.0*	*23.0*

Tab. 3.1. Tempo di elaborazione delle transazioni in base alla dimensione del blocco e al carico di rete.

[19] Cfr. BitFury Group "Block Size Increase" in *Block Size Mathematics*, p. 2 http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

L'obiettivo di questo capitolo è analizzare quanto incide l'aumento di *block size* sul consumo di risorse e sul tempo di propagazione dei blocchi, nonché esaminare il sistema Bitcoin in un insieme di livelli di astrazione ai fini di esplorare tutte le problematiche della scalabilità in diversi settori del protocollo Bitcoin.

3.1. Analisi matematica

Come abbiamo visto nel capitolo precedente, le preoccupazioni maggiori riguardanti l'aumento del limite massimo della dimensione del blocco sono la capacità di storage e il traffico Internet in vari punti dei nodi della rete. Il 6 settembre 2015 BitFury Group ha realizzato un'analisi matematica sugli effetti dell'aumento di block size sui requisiti della memoria[20]. Dato che dal 2015 i parametri chiave delle principali caratteristiche della rete Bitcoin sono cambiati a causa della sua crescita, rianalizziamo l'analisi di BitFury Group con i valori attuali.

3.1.1. Parametri chiave

Qui di seguito vengono definite alcune caratteristiche fondamentali dei nodi pieni, ai fini di svolgere un'analisi quantitativa sul consumo delle risorse per diversi valori di *block size*.

Il *throughput massimo* è il numero massimo teorico di transazioni al secondo che il sistema Bitcoin è in grado di gestire, attualmente equivale a 7 tps.

Il *throughput* è il numero vero di transazioni al secondo che il sistema Bitcoin è in grado di gestire. Visto che i tempi di coda delle transazioni sono lunghi [26] il network Bitcoin riesce a raggiungere al massimo 3 o 4 transazioni al secondo. Quindi d'ora in avanti consideriamo il valore di *throughput* corrispondente a 3.5 tps.

Il *numero di transazioni in un blocco* [27] è il prodotto tra throughput e il numero medio di secondi fra i blocchi, per ogni Block Size di 1MB vale 2100 transazioni.

La capacità di storage è il prodotto tra dimensione del blocco e intervallo di tempo fra i blocchi.

$$\langle \text{Capacità di Storage / giorno} \rangle = 1 \cdot 144 = 144 \text{ MB};$$

[20] Cfr. BitFury Group "Block Size Increase" in *Block Size Mathematics*, p. 2 -7 http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

$$\langle \text{Capacità di Storage / anno} \rangle = 1 \cdot 144 \cdot 365 = 52560 \text{ MB};$$

Il *tempo di verifica del blocco* è il prodotto fra tempo di elaborazione delle transazioni, numero medio di transazioni in un blocco e il fattore 0,2 [28].

$$\langle \text{Tempo di verifica del blocco} \rangle = 0.2 \cdot 2100 \cdot 0.000333 = 0.13 \text{ sec}$$

Il tempo di elaborazione delle transazioni si basa sul presupposto che un nodo è in grado di elaborare 3000 transazioni al secondo [29].

L'utilizzo della RAM[21] è la variabile più difficile da stimare in quanto dipende da tanti fattori e differisce a seconda del nodo. Utilizziamo un valore empirico di 4 GB [30], che corrisponde a una dimensione del blocco pari a 1 MB.

3.1.2. Analisi

Per ogni parametro chiave elencato viene calcolato un valore stimato corrispondente ai valori di *block size* di Bitcoin pari a 2MB, 4MB, 8MB, 16MB e 32MB. Le stime dei parametri elencati vengono calcolati moltiplicando il valore base (corrispondente al *block size* di 1MB), per il fattore di scala N che rappresenta il moltiplicatore per la dimensione del blocco.

I fattori di scala per ogni parametro sono stati stabiliti secondo le seguenti ipotesi:

- Supponendo che la dimensione media delle transazioni sia sempre costante. In questo caso il throughput, il numero di transazioni in un blocco e la capacità di storage scalano linearmente O(N) con aumento di block size.
- Supponendo che il tempo di elaborazione delle transazioni sia costante O(1), trascurando il tempo che serve per la ricerca nel set di uscite non utilizzate [31] che scala logaritmicamente.

[21] Valore approssimativo che permette di mantenere il tempo di elaborazione delle transazioni. I sistemi con meno RAM sono validi, ma elaborano transazioni con elevati ritardi. Consideriamo un utente medio, per i nodi specializzati i requisiti della RAM sono più alti in quanto devono memorizzare nella RAM l'intera uscita della parte di transazione non utilizzata (Unspent Transaction Output, UTXO [31]) per verificare le transazioni in ingresso e i blocchi non spesi. Ovviamente l'insieme di informazioni non deve risiedere completamente nella RAM, anche se altri metodi di memorizzazione portano a un elevato tempo di verifica delle transazioni.

- Suppponendo che il tempo di verifica del blocco scali logaritmicamente in base alla dimensione della cache, dalle indagini di BitFury Group [30] il suo fattore di scala corrisponde a:

$$N(1 + \log_2 N / \log_2 S);$$

dove la variabile S indica il numero di transazioni della cache [33] e t rappresenta il tempo di ricerca di ogni transazione.

- L'utilizzo della RAM scala linearmente in quanto i fattori che contribuiscono al suo consumo come UXTO [31] e la dimensione delle transazioni nella cache mostrano una crescita lineare.

Caratteristiche	Fattore di scala	Block Size, MB					
		1	2	4	8	16	32
Throughput, tps	*N*	3,5	7	14	28	56	112
Numero di transazioni in un blocco	*N*	2100	4200	8400	16800	33600	67200
Capacità di storage giornaliera, MB	*N*	144	288	576	1152	2304	4608
Capacità di storage annuale, GB	*N*	51	103	205	441	821	1643
Elaborazione delle transazioni, ms	*1*	0,33	0,33	0,33	0,33	0,33	0,33
Tempo di verifica del blocco, s	$N(1 + log_2 N / log_2 S)$	0,15	0,33	0,71	1,51	3,23	6,86
Traffico annuale, TB	*N*	4,4	8,8	17,7	35,4	70,7	141
Utilizzo della RAM, GB	*N*	4	8	16	32	64	128
Nodi esclusi, %	*n/a*	0	10	30	65	90	95

Tab. 4 Consumo delle risorse dei nodi pieni a seconda della dimensione del blocco.

Inoltre sono state calcolate le stime di quanti nodi non funzionerebbero più, dopo un eventuale aumento di *block size*, senza appropriati aggiornamenti hardware. Le caratteristiche dell'hardware del nodo sono basate su un'indagine eseguita da Steam [34] secondo la quale il computer tipico di oggi che supporta un nodo non dispone di meno di 8 GB di RAM. Dalla tabella vediamo che un *block size* pari a 4 MB richiede 16 GB di RAM, il che porta a escludere il 30% dei nodi.

Inoltre dall'indagine svolta vediamo che l'aumento di Block Size siriflette anche sul traffico Internet e sullo spazio sul disco. Ad esempio un Block Size pari a 8 MB richiede più di 34 GB di spazio sul disco per elaborare circa 3 TB di traffico al mese.

Si può notare anche che il tempo di verifica del blocco ha degli effetti negativi per i valori di Block Size maggiori di 4MB in quanto porta a elevati tempi di trasmissione e a un aumento dei blocchi orfani.

In breve, dall'analisi svolta si deduce che in caso di *block size* anche solo pari a 4 MB i requisiti di memoria rappresenterebbero un ostacolo per la scalabilità e per un singolo utente sarebbe molto difficile mantenere un nodo completo su di un PC domestico, facendo probabilmente migrare la maggior parte degli utenti non professionali verso thin client con tutte le conseguenze del caso sulla decentralizzazione della rete.

3.2. Analisi basata sulla riparametrizzazione

Un altro punto fondamentale riguardante l'analisi dell'aumento di *block size* è lo studio della propagazione dei blocchi della rete Bitcoin basato sulla riparametrizzazione[22] [34].

Il nocciolo dello studio è il parametro denominato *X% effective throughput* che rappresenta il rapporto fra la dimensione del blocco e la percentuale di ritardo, con *X* che indica la percentuale dei nodi che si propagano.

$$\text{X\% effective throughput} = \frac{\text{block size}}{\text{X\% ritardo della propagazione}}$$

L'obiettivo principale dello studio era determinare il valore massimo di block size e il valore minimo di latenza che sarebbero in grado di garantire la propagazione del 90% dei nodi (*90% effective throughput*).

Dall'analisi svolta per garantire il valore minimo di latenza e il valore massimo di block size accettabili deve essere soddisfatta la seguente condizione:

$$\frac{\text{block size}}{\text{X\% effective throughput}} < block\ interval$$

[22] Cfr. Kyle Croman, Christian Decker "On Scaling Decentralized Blockchains (A Position Paper)" in *Limits of Scalability by Reparametrization, 2016* http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf data ultima consultazione: 9 luglio 2017.

Pertanto, data l'attuale rete sovrapposta e l'intervallo di blocco medio (10 min.), per garantire la propagazione del 90% dei nodi, la dimensione del blocco non dovrebbe superare i 4 MB. Un blocco pari a un 4 MB corrisponde al 90% dell'*effective throughput* di al massimo 27 tps.

Dall'altro lato per garantire il 90% di *effective throughput* e utilizzare completamente la larghezza di banda della rete, l'intervallo del blocco medio non dovrebbe essere inferiore ai 12 sec.

3.3. Riprogettazione del protocollo Bitcoin

Diversi studi [34] [35] hanno discusso sulle tecniche di riprogettazione del protocollo Bitcoin che permetteranno alla blockchain di scalare oltre i parametri applicati al sistema Bitcoin odierno. Le tecniche di riprogettazione del protocollo Bitcoin[23] [34] si basano sulla scomposizione del sistema Bitcoin in un insieme di livelli di astrazione chiamati "*piani*", ordinati in una gerarchia di dipendenza dal basso verso l'alto: piano rete, piano consensus, piano storage, piano vista e piano laterale.

3.3.1 Piano rete

La funzione principale del piano rete è propagare i messaggi di transazione. Tuttavia a livello di rete i nodi propagano solo i messaggi che rappresentano le transazioni valide. Gli studi hanno dimostrato che il protocollo di rete di Bitcoin non utilizza completamente la larghezza di banda della rete sottostante, rendendo il piano rete di Bitcoin il collo di bottiglia nell'elaborazione delle transazioni. Si deduce logicamente che per migliorare la scalabilità di Bitcoin bisogna migliorare il progetto del suo piano rete.
Si distinguono due inefficienze fondamentali nel piano rete di Bitcoin:

- Per evitare il denial-of-service mediante la propagazione di transazioni non valide un nodo deve ricevere e convalidare completamente una transazione prima di propagarla ulteriormente. Questa convalida locale delle transazioni contribuisce significativamente al tempo complessivo di propagazione.

[23] Cfr. Kyle Croman, Christian Decker "On Scaling Decentralized Blockchains (A Position Paper)" in *Rethinking the Design of a Scalable Blockchain* , 2016 http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf data ultima consultazione: 9 luglio 2017.

- Il protocollo di livello di rete di Bitcoin propaga prima tutte le transazioni e poi propaga blocchi contenenti molte delle stesse transazioni. Ciò richiede che ciascuna transazione venga trasmessa due volte. Per risolvere questa ridondanza si potrebbe fare affidamento su un protocollo di riconciliazione impostato, in cui i nodi recuperano solo le transazioni che non possiedono in un blocco appena minato [36] [37]. Altrimenti si potrebbe utilizzare una rete dedicata, centralizzata e ad alta velocità per la comunicazione tra i miner; fra l'altro i miner utilizzano già questa opzione [38].

3.3.2. Piano consensus

Il fattore chiave del piano *consensus* è quella di rivelare un insieme di transazioni accettate a livello globale perché vengono elaborate. In quanto astrazione generale tale piano contiene i messaggi dal piano rete e le transazioni di output da inserire nel libro mastro del sistema.

Il protocollo blockchain di Bitcoin si basa su un compromesso tra la velocità del consenso, la larghezza di banda e la sicurezza. C'è infatti un trade-off fra i primi due e la sicurezza. Il trade-off può essere eliminato con un protocollo blockchain alternativo offrendo un tempo di consenso e una larghezza di banda limitati solo dal piano rete. Esistono diverse soluzioni per la riprogettazione del protocollo blockchain a livello del piano *consensus*:

- *Proof of stake*[24] [39]. Diverse proposte sono basate sul metodo *proof of stake* che permette di ottenere consenso eliminando la spesa computazionale del *proof-of-work*. Nel *proof of stake*, i possessori della valuta ottengono il diritto di creare i blocchi depositando i propri fondi. Queste tecniche tuttavia non hanno le garanzie formali di convergenza del sistema.

[24] La *Proof-of-stake* (PoS), traducibile in Italiano come, "la prova di avere una posta in gioco" è il nome attribuito a un metodo finalizzato alla messa in sicurezza di una rete di criptovaluta e per ottenere un consenso adeguato fra gli utenti. Esso si basa sul principio secondo cui a ciascun utente occorre richiedere di dimostrare il possesso di una determinata quantità di criptovaluta.

- *Consortium consensus blockchain* [40]. Si tratta di una tecnica che consiste nel limitare il controllo del processo di consenso a un numero predefinito di nodi, per poter ridurre i costi di prestazione dovuti al decentramento della rete Bitcoin. Questa tipologia di blockchain è definita "parzialmente decentralizzata". Nel sistema Bitcoin l'utilizzo del protocollo di consensus più efficace (come ad esempio BFT "*Byzantine Fault Tolerant*" [41]) con un ridotto numero di enti di fiducia consentirebbe di rimuovere molti degli ostacoli alla scalabilità di Bitcoin; in particolare potrebbe ottimizzare i valori della latenza e di throughput con minore consumo di memoria e larghezza di banda.
- *Frammentazione.* Una possibile tecnica per migliorare la scalabilità del piano Consensus è quella di scomporlo, cioè dividere il compito di consenso tra i gruppi di nodi che operano in modo concorrente, allo scopo di migliorare la capacità di trasmissione e ridurre i requisiti di memoria.
- *Delega di fiducia e gerarchia di sidechain* [42]. Un'altra tecnica per migliorare la scalabilità è quella di creare una gerarchia delle "istanze di consenso" a livello inferiore, comunemente denominate "sidechain". Le *sidechian* hanno un grado di decentralizzazione inferiore rispetto alle blockchain di alto livello e possono eseguire il protocollo non-proof-of-work, come BFT.

3.3.3 Piano storage

Il piano storage funziona come una memoria globale che conserva e fornisce la disponibilità per i dati autenticati prodotti dal piano consensus.

La funzione del piano storage può essere vista come un'astrazione con due interfacce:

- Contiene ed elabora le istruzioni della modifica della memoria – scrive e cancella operazioni dal piano consensus.
- Supporta le richieste di lettura da qualsiasi entità nel sistema.

Nel sistema Bitcoin il piano di storage può essere visto come un memorizzatore del suo libro mastro: memorizza i blocchi di nuova estrazione e non supporta le operazioni di cancellazione. L'unica operazione di lettura generalmente supportata dal piano storage è quando Bitcoin scarica i contenuti di tutto il libro mastro, un procedimento che richiede circa 4 giorni. Ciò presenta come risultato una notevole inefficienza del piano storage di Bitcoin. Inoltre Bitcoin memorizza l'intero libro mastro e di conseguenza il sistema memorizza molti duplicati dello stesso. La comunità che si occupa di Bitcoin ha proposto diverse idee interessanti che possono essenzialmente scomporre l'archiviazione di una struttura di dati [43] ma non è chiaro come queste idee possano essere implementate.

3.3.4. Piano vista

La funzione principale del piano vista consiste nella possibilità di accedere e autenticare una struttura dati derivata dal libro mastro completo il cui stato è ottenuto applicando tutte le transazioni. Una vista può essere memorizzata nel piano storage e distribuita in modo autenticato - Bitcoin non implementa questa ottimizzazione per le viste, pertanto i nuovi minatori hanno bisogno di circa 4 giorni per ricostruire un set di output di transazioni non spese UTXO (che può essere considerato come una vista).
Per i minatori di Bitcoin non è necessario operare sul libro mastro completo che memorizza l'intera storia delle transazioni, in quanto possono operare localmente in una visualizzazione del registro chiamato *output di transazioni non spese* (UTXO), che specifica il saldo corrente di tutte le entità del sistema. Nel caso di Bitcoin questa visualizzazione del registro è considerata come una vista. Analogamente in crittovaluta Ethereum [44], gli *smart contract* possono definire lo stato del libro mastro. Le parti di uno smart contract possono desiderare di accedere e autenticare tale stato senza leggere le altre parti del libro mastro.

3.3.5. Piano laterale (sidechain)

Sidechain ("pegged sidechains") rappresenta un'evoluzione che consente a diverse blockchain alternative legate alla blockchain Bitcoin e tra di loro di essere interoperabili con un legame bidirezionale che permette di spostare il valore di Bitcoin da una catena all'altra. In quanto astrazione generale piano sidechain è costruito dalle catene che stanno di fianco alla blockchain principale. L'idea di base sta nell'utilizzo di un legame

bidirezionale grazie al quale i bitcoin possono essere trasferiti tra ogni blockchain ad un tasso di scambio prefissato. Ciascuno di questi “catene laterali” rappresenta una quantità di riserve bitcoin messe a disposizione, in modo che le parti possono regolare ripetutamente le loro quote, scambiando bitcoin fuori banda affinché le risorse non vengono versate alla blockchain Bitcoin. Esistono diversi progetti riguardanti blockchain Bitcoin a livello del piano *laterale*:

- *Lightning Network* [45] sono le reti di pagamento bilaterali che usano la rete Bitcoin come camera di compensazione periodica.
- *Canali full duplex* [46] si tratta di un piano rete separato e un piano di consenso peer-to-peer indipendente sostenuto da Bitcoin.

4 Sviluppi recenti

Background

All'interno della comunità di Bitcoin il dibattito sulla scalabilità è oggetto di interesse e accese discussioni. La tensione tra i gestori è talmente alta da aver comportato la nascita di due comunità concorrenti. Le proposte che hanno ottenuto maggiori consensi sono *Segregated Witness* e *Bitcoin Unlimited*. Inoltre negli ultimi mesi si parla sempre di più di *Segwit2x* e di *UASF BIP148.* Per fare chiarezza di seguito saranno trattati brevemente questi "movimenti".

Segregated Witness (spesso abbreviato in SegWit) è un *soft-fork* che permette al protocollo di Bitcoin di gestire più transazioni. L'idea di base consiste nel separare le firme dal resto dei dati della transazione e di raccoglierle e in un albero distinto. Le firme sono indispensabili solo al momento della convalida, ma rappresentano circa 60% della dimensione di ogni transazione. Pertanto, questa separazione permetterà di ridurre le dimensioni delle transazioni e di conseguenza più transazioni potranno stare all'interno di un blocco. Secondo alcune stime [47], l'adozione di SegWit comporterebbe un aumento della capacità del blocco analoga a quella che si avrebbe se il blocco venisse aumentato a 1.7 ~ 2 MB. Inoltre l'adozione di SegWit rende possibile l'utilizzo di tecnologie Lightning Network [48] che possono rendere le transazioni immediate, anonime e con commissioni più economiche. Per far sì che SegWit sia attiva (loked-in) è obbligatoria l'approvazione da parte del 95% della rete Bitcoin. Attualmente hanno segnalato il supporto a SegWit solo il 46% dei nodi [49].

Bitcoin Unlimited (spesso abbreviato in BU o BTU) è un nuovo protocollo Bitcoin, sviluppato da un team diverso da quello di Bitcoin Core, introdotto nel 04/09/2015. BU aggiunge la possibilità di modificare la massima dimensione di un blocco generato, ciò permetterebbe ai miners di originare i blocchi in base alla loro convenienza economica. Ma dal momento in cui un miner decidesse di generare un blocco più grande di 1 MB e fosse seguito da altri si darebbe via ad una *hard-fork* e alla suddivisione della blockchain in due monete diverse: Bitcoin Unlimited e Bitcoin. Dal momento della sua introduzione BU ha ottenendo molti consensi ed attualmente è supportato da 41% dei

nodi [50] (sebbene si ritiene che la maggior parte dei consensi sia dovuta a di Jihan e Roger, i finanziatori di BU [51]).

UASF[25] [53] *BIP148*[26] [52] è un sistema introdotto il 12 marzo 2017 con lo scopo di forzare l'accettazione di SegWit il prima possibile. Il sistema aprirà una finestra temporale tra l'1 agosto 2017 e 15 novembre 2017: in questo intervallo di tempo i *miners* e i nodi della rete Bitcoin dovranno attivare o non il segnale di supporto a SegWit. Dopo il 15 novembre BIP148 forzerà l'introduzione di SegWit nella rete Bitcoin.

SegWit2x (*SegWit2MB*) [54] è una proposta supportata da più di 50 aziende leader del settore crittovalute, che rappresentano circa 83% dell'hash rate della rete Bitcoin. Il 23 maggio 2017 durante il *Consensus* a New York chiamato "*Bitcoin Scaling Agreement at Consensus 2017*" 52 aziende hanno firmato un accordo che stabilisce l'attivazione di SegWit con il consenso del'80% della rete Bitcoin (in sostanza bastanti solo loro) e l'avvio di un *hard-fork* per portare Block Size a 2 MB entro 6 mesi. *SegWit2x* è stato attivato 19 giugno 2017 e attualmente ha superato la quota del 80%. [55]. Per far sì che *SegWit2x* e *BIP148* siano compatibili gli sviluppatori hanno aperto una porta dove i *miners* potranno entrare per mantenere compatibilità ed evitare scissioni.

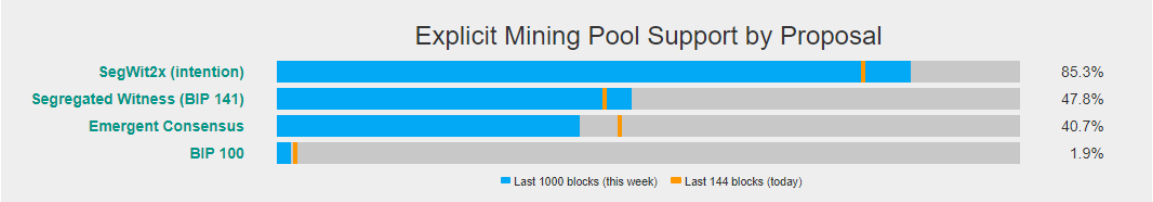

Fig. 4.1. Coin Dance, Bitcoin Block Details

L'1 giugno 2017 è stato attivato *Compatibility-oriented omnibus proposal'* [56], si tratta di un *BIP?* (senza numero) che ha lo scopo di evitare che ci siano scissioni tra Bitcoin Core e le proposte di *Bitcoin Scaling Agreement at Consensus 2017* (BIP148,

[25] USAF (*User Activated Soft Forks*) è un sistema di attivazione temporaneo di un soft-fork. Un soft-fork che ricorre ad USAF impone l'accettazione dello stesso con l'imposizione dei nodi, entro una data prestabilita.
http://www.uasf.co/

[26] BIP 148 *Bitcoin Improvement Protocol* che ha lo scopo di forzare l'ingresso di SegWit nella Network di Bitcoin costringendo i miners ad aderire. https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki

SegWit2x e altre). BIP? interromperà la sua funzione 15 novembre 2017, quando sarà presa una decisione definitiva sull'attivazione di SegWit.

L'obiettivo principale di questo capitolo consiste nell'analizzare i progetti Segregated Witness e Bitcoin Unlimited.

4.1. Segregated Witness

Segregated Witness (spesso abbreviato in *SegWit*) è stato ufficialmente rilasciato nell'ottobre del 2016 nella versione "v0.13.1" del codice del Bitcoin Core [50]. È stato proposto per la prima volta da Pieter Wuiller durante la II Conferenza riguardante la scalabilità di Bitcoin tenuta *a Hong Kong* il 6 dicembre 2015 [51]. Il progetto consiste nel rimuovere i dati relativi alle firme dal resto dei dati di una transazione che poi vengono registrati e trasferiti nei blocchi di Bitcoin. Questa separazione consente di ridurre le dimensioni delle transazioni e più transazioni potranno stare all'interno di un blocco.

Dal punto di vista tecnico ogni transazione è costituita da due componenti principali:

- Il primo ha la funzione di sbloccare i bitcoin bloccati in transazioni precedenti (UTXO) a tale scopo si utilizzano dei dati chiamati "input". Gli "input" contengono gli script (definiti "*scriptSig*") che rappresentano le istruzioni per sbloccare gli UTXO. Le istruzioni di sblocco operano sulla firma e sulla chiave pubblica corrispondenti all'indirizzo mittente.
- Il secondo componente è costituito da uno o più "output" detti *lucchetti* che hanno la funzione di bloccare la stessa quantità (o inferiore) di bitcoin all'indirizzo del destinatario. Gli output contengono gli script chiamati "*scriptPubKey*".

In sostanza i bitcoin si muovono dagli input agli output all'interno di una transazione, mentre vengono bloccati e sbloccati contemporaneamente.

```
scriptSig: <sig> <pubKey>
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

Segregated Witness realizza due cambiamenti all'interno della transazione:

1. Sposta la firma dal campo "*scriptSig*" ad un nuovo campo "*witness*". Il campo "*witness*" fa parte della transazione ma non sarà incluso nell'hash della transazione cioè non avrà nessun impatto su *txid*.
2. Trasforma il campo "*scriptPubKey*" in modo che abbia due significati diversi a seconda se si tratta del vecchio nodo (SegWit non aggiornato) o del nuovo nodo:
    - Per il vecchio client la condizione di blocco diventa un generico "*ANYONE CAN SPEND*" - un output all'apparenza non destinato a nessun indirizzo dato che il vecchio nodo non legge i nuovi script.
    - Per i nuovi client si tratta di leggere un nuovo script "pay-to-witness-public-key-hash" P2WPKH che manda bitcoin a un indirizzo preciso:

```
witness: <signature> <pubkey>
(campo nel quale vengono trasferiti la firma e la chiave pubblica del mittente)
scriptSig: (empty)
(campo svuotato della firma e della chiave pubblica del mittente)
scriptPubKey: 0 <20-byte-key-hash>
```

Nel momento in cui viene eseguito l'hash della transazione per ricavare il suo ID (*txid*), il campo "*witness"* non viene incluso. Tale campo, essendo svincolato da *txid* e dall'hash del blocco, diventa l'unica parte della blockchain separabile. Si procede quindi, con la costruzione di un *Merkle Tree* solo per i campi "*witness*" di tutte le transazioni del blocco. *Merkle Root* relativo ai campi "*witness"* viene immesso come input della coinbase del blocco.

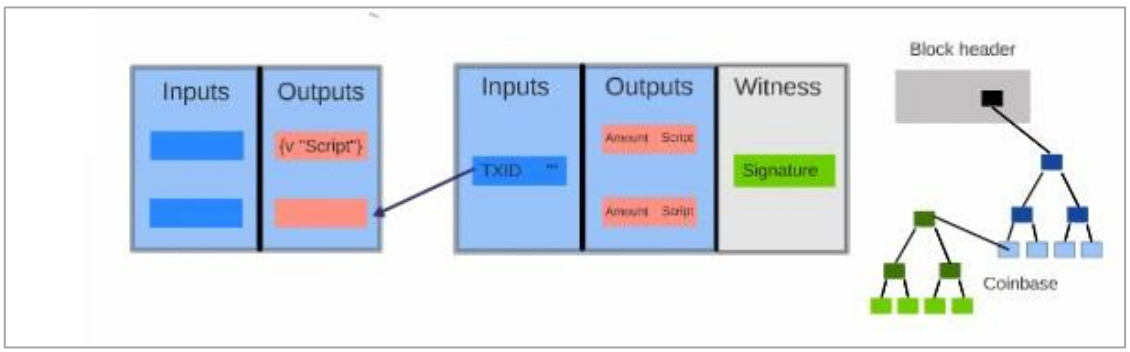

Fig. 4.2. La composizione di una transazione con Segregated Witness

Secondo le stime [60] [54], l'adozione di SegWit comporterebbe un aumento della capacità del blocco analoga a quella che si avrebbe se il blocco venisse aumentato a 1.7 ~ 2 MB.

Inoltre, Segregated Witness risolve il problema di "*transaction maleability*" [52] - un bug presente dalla nascita di Btcoin che permette ad un utente di cambiare ID di una transazione facendola figurare come non esistente mentre in realtà è andata a buon fine. È una vulnerabilità che espone i servizi al rischio di avere transazioni false. Con l'adozione di SegWit ogni transazione avrà un *txid* inalterabile fin dalla sua creazione. Risolvere il bug di "*transaction maleability*" significa alleggerire la rete Bitcoin, aumentando la sicurezza delle transazioni da 160 bits a 256 bits.

Dato che il sistema SegWit è un *soft-fork,* è possibile analizzare le conseguenze della sua attivazione per i client non aggiornati. I nodi non aggiornati (vecchi nodi) non riusciranno più a comprendere i nuovi comandi che vincolano i bitcoin nel campo *scriptPubKeys* e di conseguenza questi bitcoin si mostreranno a loro non vincolati a nessun indirizzo "*ANYONE CAN SPEND*". Quindi, nel caso in cui il nodo non aggiornato dovesse ricevere una transazione del nuovo tipo là etichetterà come 'non standard' (la transazione non infrange nessuna regola ma il client non la comprende), il suo client non la accetterà per la prima volta nello stato di transazione non confermata, ma là accetterà all'interno di un blocco minato. Pertanto un nodo dovrà aspettare che la transazione abbia almeno una conferma (sia inclusa nel blocco) per vederla apparire nel suo programma.

Tra l'altro il sistema "Segregated Witness" è stato già adottato per le atre crittoavalute minori come Litecon, Statis, Vertcoin. Ad esempio grazie a SegWit adesso il *Litecoin* ha una velocità di transazione superiore a ben 8 volte rispetto a quella del Bitcoin e i prezzi più che raddoppiati.

La seguente tabella riassume i principali limiti e i vantaggi del sistema SegWit:

Vantaggi	*Limiti*
• *Risolve il bug "transaction maleability";* • *Aumenta la capacità del blocco (raddoppia);* • *Si aggiorna facilmente;* • *Risolve il problema della scalabilità (momentaneamente*); • *Aumenta la sicurezza delle transazioni da 160 bits a 256 bits;* • *Riduce il costo delle commissioni;* • *Permette di attivare Lightning clients;* • *Aumenta l'affidabilità del protocollo.*	• *Gli effetti del soft-fork;* • *Non costituisce una soluzione a lungo termine per la scalabilità;* • *Gli effetti sulla centralizzazione dovuti ai blocchi più grandi.*

Tab.4.1. I principali limiti e i vantaggi del progetto Segregated Witness.

4.2. Bitcoin Unlimited

Bitcoin Unlimited (spesso abbreviato in BU o BTU) è un nuovo protocollo Bitcoin introdotto nel 04/09/2015, sviluppato da un nuovo team diverso da quello di Bitcoin Core. BU aggiunge la possibilità di modificare la massima dimensione di un blocco generato, il che permetterebbe ai minatori di originare i blocchi in base alla loro convenienza economica. Ma dal momento in cui un miner decidesse di generare un blocco più grande di 1 MB e fosse seguito da altri si darebbe via ad una *hard-fork* e alla suddivisione della blockchain in due monete diverse: Bitcoin Unlimited e Bitcoin. Gli utenti si troveranno con due diversi blockchain con una storia in comune e con tutti i rischi di un *hard-fork* e dell'aumento della dimensione del blocco che sono stati esplorati nei capitoli precedenti.

Qui in seguito saranno elencate le principali proposte del team di Bitcoin Unlimited [80]:

- Aggiunta dell'opzione per modificare la massima dimensione di un blocco generato. Questo permette ai minatori di BU di votare per l'aumento o diminuzione della dimensione massima del blocco. Il valore di default sarà 1MB compatibile con i nodi di Bitcoin Core.
- Aggiunta dell'opzione "BU" nel menu per accedere alle sue specifiche.
- Aggiunta dell'opzione per modificare la massima dimensione dei blocchi approvata.
- Aggiunta dell'opzione "Traffic Shaping". Visto il crescere della dimensione dei blocchi, gli utenti avranno la possibilità di impostare la banda da utilizzare per Bitcoin. Questa opzione permetterà ai client di lavorare con una rete domestica.
- Correzione del bug delle notifiche. Nel caso di ricezione di tante modifiche alcune non vengono mostrate.

La seguente tabella riassume i principali limiti e vantaggi del sistema Bitcoin Unlimited:

Vantaggi	*Limiti*
• *Aumento della capacità del blocco;* • *Risolve il problema della scalabilità in modo permanente;* • *Riduce il costo delle commissioni.*	• *Gli effetti del hard-fork;* • *Gli effetti sulla centralizzazione dovuti ai blocchi più grandi;* • *Cambiamento radicale non dimostrato e non rivisto;* • *Problemi di sicurezza relative alle commissioni;* • *Diversi settori di attacco incustoditi.*

Tab. 4.2. I principali limiti e i vantaggi del progetto Bitcoin Unlimited.

Conclusioni

In conclusione posso affermare che Bitcoin è una moneta elettronica con grosse potenzialità, ma allo stato dei fatti presenta ancora tanti ostacoli. La prima barriera da superare sarà sicuramente quella da risolvere il problema della scalabilità. La soluzione che si sta percorrendo è quella di adottare la tecnologia "Segregated Witness" – un progetto strutturalmente solido, che tra l'altro è stato già testato sulle altre criptovalute minori. Inoltre l'adozione di Segregated Witness rende possibile l'utilizzo di tecnologie Lightning Network che possono rendere le transazioni immediate e con commissioni più economiche. Sebbene la tecnologia Segregated Witness non costituisce una soluzione a lungo termine per la scalabilità, risulta comunque corredata da aspetti vantaggiosi. Infatti presenta una soluzione definitiva al bug "*transaction maleability*" e aumenta la sicurezza delle transazioni. Secondo la proposta *SegWit2x* dopo l'attivazione di Segregated Witness entro 6 mesi si prevede l'avvio di un hard-fork per portare Block Size a 2 MB. Tuttavia la durata temporale di questa soluzione risulta subordina dalla diffusione dei bitcoin. Di fatti qualora si dovesse verificare una crescita esponenziale del sistema Bitcoin la soluzione appena descritta sarebbe praticabile solo per un periodo limitato di tempo.

Dall'altra parte si propone l'attivazione di un *hard-fork* Bitcoin Unlimited che presenta delle soluzioni apparentemente definitive al problema della scalabilità del sistema Bitcoin. Tuttavia il progetto risulta comunque corredato da aspetti svantaggiosi come i problemi di sicurezza e tutte le conseguenze dell'attivazione del hard-fork.

Da parte mia, credo che l'attivazione del progetto Segregated Witness è un buon punto di partenza per risolvere nell'immediato futuro il problema della scalabilità del sistema Bitcoin. Credo inoltre che in un futuro più lontano un intero ecosistema di criptovalute risolverà applicazioni specifiche e che Bitcoin rimarrà più confinato all'aspetto del mantenimento del valore della moneta.

.

Bibliografia

[1]. Pedro Franco, "*Understanding Bitcoin: Cryptography, Engineering and Economics*", October 2014

[2]. David CHAUM, "*Blind signatures for untraceable payments*", in *Advances in cryptology*, Springer, 1983

[3]. Dario D'ANDREA, "*Architetture di calcolo eterogenee per l'accelerazione del Bitcoin Mining"*, Elaborato finale in Calcolatori Elettronici I, Università degli Studi di Napoli Federico II, Scuola Politecnica e delle Scienze di Base, Corso di Laurea in Ingegneria Informatica, Anno Accademico 2015/2016, Napoli 2016

[4]. Pier Francesco COSTA, "*Bitcoin: aspetti tecnici, economici e politici di una crittovaluta"*, Elaborato in Sistemi Distribuiti, Università di Bologna

[5]. David Chaum e Stefan Brands, *"Minting electronic cash*", in *Spectrum, IEEE* 34.2. (1997)

[6]. Satoshi NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, in https://bitcoin.org/bitcoin.pdf

[7]. Earliest known Bitcoin code, src/main.h:17

[8]. Bitcoin Core commit a30b56e, 15 Luglio 2010

[9]. Bitcoin Core commit 8c9479c, 7 Settembre 2010

[10]. https://bitcointalk.org/index.php?topic=1347.msg15145#msg15145

[11]. https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366

[13]. https://bitcointalk.org/index.php?topic=532.msg6306#msg6306

[14]. *Gavin Andresen (2015). Aumento del limite massimo della dimensione del blocco (BIP 101)*

https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

[15]. *Legge di Moore Wikipedia*

https://it.wikipedia.org/wiki/Legge_di_Moore, data ultima consultazione: 3 giugno 2017

[16]. 22 *Il sito ufficiale di Bitcoin XT*

https://bitcoinxt.software/ data ultima consultazione: 3 giugno 2017

[17]. 23 *Quantità media dei nodi nella Bitcoin XT nel tempo*

https://coin.dance/nodes/xt data ultima consultazione: 3 giugno 2017

[18].https://github.com/bitcoin/bitcoin/blob/41076aad0cbdfa4c4cf376e345114a5c29086f81/src/consensus/consensus.h#L10 data ultima consultazione: 3 giugno 2017

[19]. https://bitcoin.org/en/developer-reference#getheaders, data ultima consultazione: 3 giugno 2017

[20]. https://www.weusecoins.com/hard-fork-soft-fork-differences/, data ultima consultazione: 3 giugno 2017

[21]. https://coin.dance/nodes, data ultima consultazione: 8 giugno 2017

[23]. https://it.wikipedia.org/wiki/O-grande Comportamento asintotico delle funzioni, data ultima consultazione: 10 giugno 2017

[24]. https://en.bitcoin.it/wiki/July_2015_chain_forks, data ultima consultazione: 11 giugno 2017

[25]. BitFury Group "*Block Size Increase*" in Block Size Mathematics, p. 2-8 http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf, data ultima consultazione: 15 giugno 2017

[26] 7 *Transactions Per Second? Really?* http://hashingit.com/analysis/33-7-transactions-per-second , data ultima consultazione: 2 maggio 2017.

[27]. *Numero medio di transazioni in un blocco* https://blockchain.info/it/charts/n-transactions-per-block, data ultima consultazione: 7 luglio 2017.

[28]. *BitFury Group. "Block Size Increase"* https://bravenewcoin.com/assets/Whitepapers/block-size-1.1.1.pdf , data ultima consultazione: 3 giugno 2017

[29]. *Scalability, English Wikipedia* https://en.bitcoin.it/wiki/Scalability , data ultima consultazione: 7 luglio 2017.

[30]. *BitFury Group. "Block Size Increase"* https://bravenewcoin.com/assets/Whitepapers/block-size-1.1.1.pdf, data ultima consultazione: 3 giugno 2017

[31]. *Unspent transaction output set. Statoshi.info*

https://bitcoin.org/en/glossary/unspent-transaction-output , data ultima consultazione: 2 maggio 2017

[32]. *Transactions. Statoshi.info*
http://statoshi.info/dashboard/db/transactions data ultima consultazione: 3 luglio 2017.

[33]. *Sondaggio Hardware & software. Steam*
http://store.steampowered.com/hwsurvey/?platform=pc, data ultima consultazione: 11 giugno 2017.

[34]. *On Scaling Decentralized Blockchains*
http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf , data ultima consultazione: 12 giugno 2017.

[35]. Y. Minsky, A. Trachtenberg, and R. Zippel. *Set reconciliation with nearly optimal communication complexity*. In IEEE Trans. on Information Theory, 2003.

[36]. H. D. Johansen, R. V. Renesse, Y. Vigfusson, and D. Johansen. Fireflies: *A secure and scalable membership and gossip service*. ACM Trans. Comput. Syst., 2015.

[37]. Y. Minsky, A. Trachtenberg, and R. Zippel. *Set reconciliation with nearly optimal communication complexity*. In IEEE Trans. on Information Theory, 2003.

[38]. *J. Poon and T. Dryja. The bitcoin lightning network*
https://lightning. network/lightning-network-paper.pdf, data ultima consultazione: 7 luglio 2017

[39]. S. King and S. Nadal. PPCoin: "*Peer-to-Peer Crypto-Currency with Proof-of-Stake"*, agosto 2012.

[40]. Jeremy Clark, Sarah Meiklejohn "*Financial Cryptography and Data Security"* pp. 121-122.

[41]. L. Shin. "*Bitcoin blockchain technology in financial services: How the disruption will play out."* Forbes, 14 settembre 2015.

[42]. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Tim´on, and P. Wuille. *Enabling blockchain innovations with pegged sidechains*. https://www.blockstream.com/sidechains.pdf, data ultima consultazione: 7 luglio 2017.

[43]. G. Maxwell. https://bitcointalk.org/index.php?topic=314467#msg3371194 data ultima consultazione: 7 luglio 2017.

[44]. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Tim´on, and P. Wuille. *Enabling blockchain innovations with pegged sidechains*. https://www.blockstream.com/sidechains.pdf, data ultima consultazione: 7 luglio 2017

[45]. J. Poon and T. Dryja. *The bitcoin lightning network*. https://lightning. network/lightning-network-paper.pdf, data ultima consultazione: 5 luglio 2017

[46]. C. Decker and R. Wattenhofer. *A fast and scalable payment network with bitcoin duplex micropayment channels.* In Stabilization, Safety, and Security of Distributed Systems, pages 3–18.

[47] *Capacity increases for the Bitcoin system* https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011869.html, data ultima consultazione: 3 luglio 2017

[48]. *Lighting network, Scalable Instant Bitcoin/Blockchain Transactions* https://lightning.network/, data ultima consultazione: 3 luglio 2017

[49]. *Prcentage of blocks signalling SegWit Support* https://blockchain.info/it/charts/bip-9-segwit, data ultima consultazione: 4 luglio 2017

[50]. *Percentage of blocks signalling BU support* https://blockchain.info/it/charts/bitcoin-unlimited-share, data ultima consultazione: 4 luglio 2017

[51]. *Roger Ver confirms he'll sell his Bitcoin: 130K BTU trade a "Great Deal"* http://bitcoinist.com/roger-ver-sell-bitcoin-btu-trade/, data ultima consultazione: 4 luglio 2017

[52]. *bip-0148.mediawiki* https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki, data ultima consultazione: 7 luglio 2017

[53]. *USAF* http://www.uasf.co/, data ultima consultazione: 8 luglio 2017

[54]. *Bitcoin Scaling Proposal SegWit2x Moves Ahead with Initial Code Release* http://www.coindesk.com/first-look-bitcoin-scaling-proposal-segwit2x-gets-alpha-release/, data ultima consultazione: 8 luglio 2017

[55]. *Coin Dance, Bitcoin Block Details* https://coin.dance/blocks data ultima consultazione: 8 luglio 2017

[56]. *Compatibility-oriented omnibus proposal'*
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-May/014445.html**,** data ultima consultazione: 7 luglio 2017
[57]. *Github Bitcoin core v0.13.1*
https://github.com/bitcoin/bitcoin/releases, data ultima consultazione: 8 luglio 2017
[58]. *Scaling Bitcoin 2015 Phase II - December 6th-7th Hong Kong*
https://scalingbitcoin.org/event/hongkong2015#cfp, data ultima consultazione: 6 luglio 2017
[59]. *Transaction Malleability Bitcoinwiki*
https://en.bitcoin.it/wiki/Transaction_Malleability, data ultima consultazione: 6 luglio 2017
[60]. *What is Segregated Witness*
http://learnmeabitcoin.com/faq/segregated-witness, data ultima consultazione: 6 luglio 2017