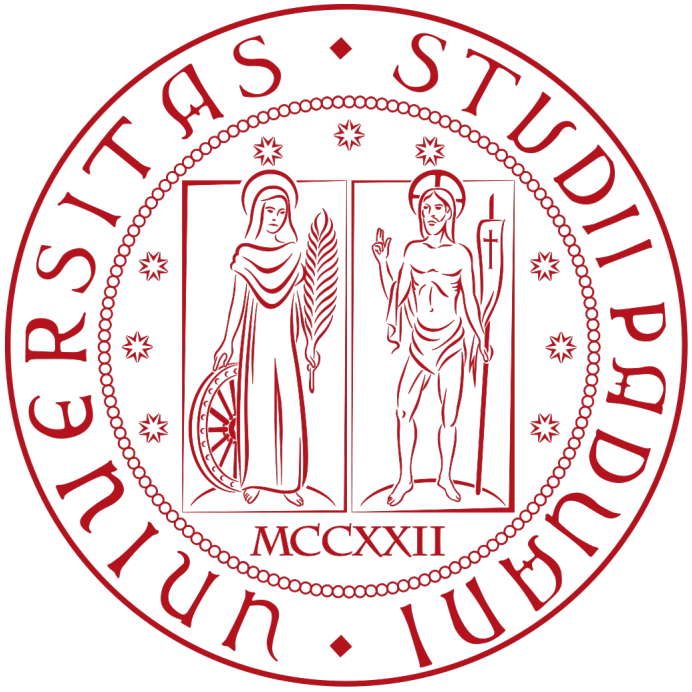
Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"

Scuola Di Scienze
Corso Di Laurea In Informatica



Servizi di supporto alle transazioni su Blockchain Ethereum

Informazioni sul documento

Titolo	Servizi di supporto alle transazioni su Blockchain Ethereum
Creazione	10 Novembre 2018
Redazione	Aaron Cesaro
Email di riferimento	aaron.cesaro@studenti.unipd.it

Sommario

Questo documento si presenta come Tesi di Laurea triennale per il corso di laurea in informatica dello studente Aaron Cesaro. In esso è contenuta una relazione dettagliata dell'attività di stage svolta presso l'azienda Sgame SA, situata a Lugano (Svizzera). Durante il tirocinio, della durata complessiva di 300 ore, ogni abiettivo prefissato è stato raggiunto con successo, permettendo allo studente di acquisire dettagliate conoscenze sulle tecnologie e le metodologie di sviluppo utilizzate dalla società. Particolare enfasi è stata data alla comprensione ed all'utilizzo della blockchain *Ethereum* e di tutti i sevizi di supporto necessari alla corretta integrazione dello stesso all'interno della piattaforma *Sgame Pro*.

Indice

1 Introduzione

1.1 Cos'è una Blockchain

1.1.1 Definizione

Blockchain è una tecnologia che permette la creazione ed amministrazione di un grande database distribuito tramite la gestione di transazioni condivisibili tra più nodi di una rete peer-to-peer. Si tratta quindi di un database strutturato in blocchi (*block*) che sono tra loro collegati (*chain*) in modo che ogni transazione avviata sulla rete debba essere validata dalla rete stessa. In estrema sintesi la *blockchain* è rappresentata da una catena di blocchi che contengono e gestiscono più transazioni facendo uso della crittografia per rendere sicuro l'immagazzinamento di dati ed il trasferimento di strumenti di valuta.

Pur essendo quest'ultima la definizione "formale" di *blockchain*, ritengo che essa non evidenzi con chiarezza e semplicità cosa effettivamente una *blockchain* sia.
Proverò quindi a scomporre ed analizzare la prima parte della definizione per rendere più fruibile il concetto.

1.1.2 Server based e P2P

La rete che normalmente viene utilizzata tutti i giorni per navigare in internet è quasi sempre *server based* [**Figura 1a**].
La peculiarità di questo sistema è che tutte le informazioni sono contenute in un solo posto, il *Server* (da qui il nome *server based*), il quale spesso gestisce un database che esercita il ruolo di archivio per l'immagazzinamento di dati ed effettua su di essi ricerche qualora vengano richiesti.

(a) Server based network (b) P2P based network

Figura 1: Tipologie di network

A differenza di una rete *server based*, in una rete *peer-to-peer* [**Figura 1b**] (anche detta *P2P*) non esiste la presenza di un server centrale che invia informazioni e tutti i

dati vengono scambiati direttamente tra i nodi collegati alla rete. Ogni utente è quindi un *client* ed un *server* contemporaneamente. Proprio per questa duplice funzione ogni dispositivo connesso viene detto *nodo* della rete.
La sostanziale differenza tra le due tipologie di rete risiede nel fatto che mentre nel primo caso il *server* contiene tutte le informazioni, nel secondo sono tutti e soli i *client* a contenere i dati.
Ciò significa che nel primo caso il proprietario del *server* può aggiungere, modificare o eliminare i dati che sono contenuti in esso, mentre nel secondo, anche se un nodo cancella o modifica i propri dati, gli altri nodi conterranno comunque tutte le informazioni originali. Da qui il termine distribuito.
È ora possible riprendere in mano la definizione originale: *blockchain* è una tecnologia che permette di creare e gestire un grande archivio di informazioni, non contenute in un unico posto, ma del quale esiste una copia in ogni nodo connesso alla rete.

1.2 Blockchain e Bitcoin

1.2.1 Ledger

In letteratura è ritenuto più intuitivo usare *Bitcoin* (BTC) per esporre, tramite esempi semplificati, il funzionamento di una *blockchain*.
Un *Bitcoin* è una singola unità di valuta digitale che, proprio come l'*Euro* non ha valore intrinseco, se non quello intenzionalmente attribuitogli grazie al consenso di scambio per l'acquisizione di beni o servizi.

Per tenere traccia della quantità di *Bitcoin* che ogni utente possiede si utilizza ciò che viene definito un *Ledger* (libro mastro), che altro non è che un file in cui viene tenuta traccia di tutte le transazioni. Il *ledger* non è contenuto in un server centrale come ad esempio quello di una banca, ma ne esiste una copia in ogni nodo partecipante alla rete. In [**Figura 2**] è riportato, anche se in modo estremamente semplificato, un esempio di *ledger*. Anche se nella realtà un ledger è molto diverso da quello in figura, nella pratica il disegno rappresenta fedelmente la funzione principale ricoperta da ogni copia del *ledger* posseduta dai singoli nodi. Nella colonna **Account** viene riportato il nome del proprietario dei *Bitcoin*, mentre nella colonna **Value** è indicata la quantità posseduta da ognuno dei partecipanti.

LEDGER

Account	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23
...	...

Figura 2: Ledger

Mettiamo caso che David voglia inviare cinque *Bitcoin* a Sandra. Per farlo è necessario che David mandi un messaggio sulla rete, il quale contiene la richiesta di transazione ed il numero di Bitcoin da lui posseduti. Come informazione aggiuntiva viene inoltre trasmessa la quantità di *Bitcoin* che possederà Sandra nel caso in cui la transazione avesse luogo. Il messaggio viene raggiunto dai nodi vicini a David i quali aggiornano i propri ledger con il risultato della possibile transazione (cioè David -5 BTC e Sandra +5 BTC) e rinviano il messaggio ai nodi a loro adiacenti. In questo modo il messaggio si espande per tutta la rete.

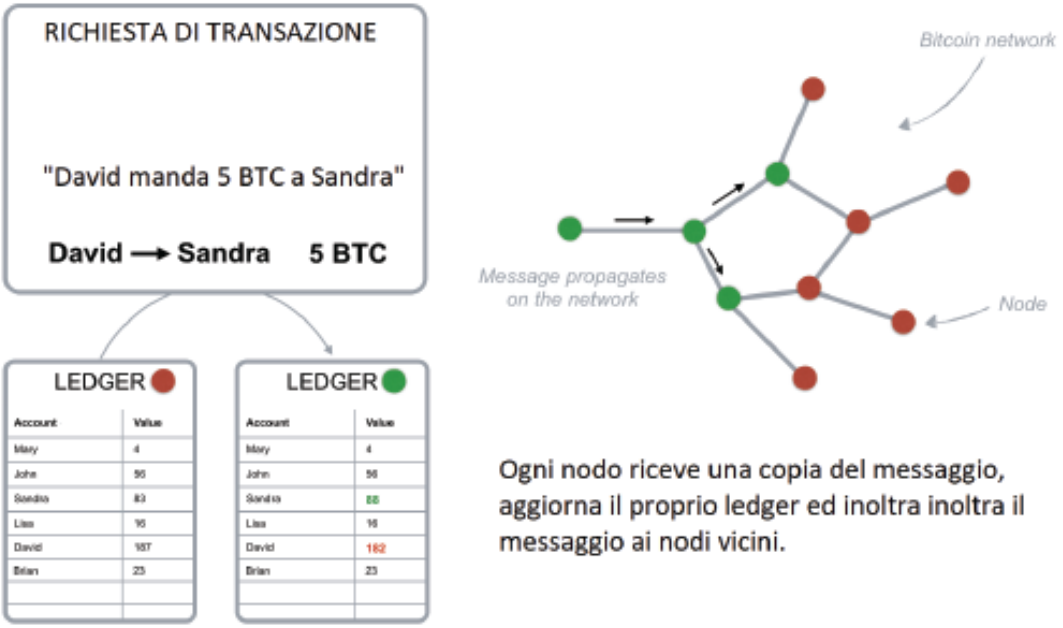


Figura 3: Richiesta di transazione tra due nodi

Il fatto che il ledger sia mantenuto da tutti i nodi implica tre cose fondamentali, che stanno alla base del concetto della blockchain:

- tutti sono a conoscenza di tutte le transazioni che avvengono sulla rete;
- se la transazione non và a buon fine nessuno se ne prende la responsabilità in quanto non esiste un'entità centrale che si prenda carico dell'esito delle transazioni;
- non esiste il bisogno di garanzie o fiducia in quanto la sicurezza è ottenuta tramite particolari funzioni matematiche estremamente sicure.

1.2.2 Transazioni

Perchè una transazione possa avere luogo è necessario ciò che viene definito un *Wallet* (portafogli), ossia un software che permetta di depositare e scambiare scriptovaluta, tra cui *Bitcoin*. Poichè deve essere possibile solo ed esclusivamente al proprietario di un determinato *Wallet* inviare i propri *Bitcoin*, ogni *Wallet* è protetto tramite una tecnica crittografica che usa una coppia di chiavi tra loro connesse. Esse prendono il nome di chiave privata (*private key*) e chiave pubblica (*public key*).

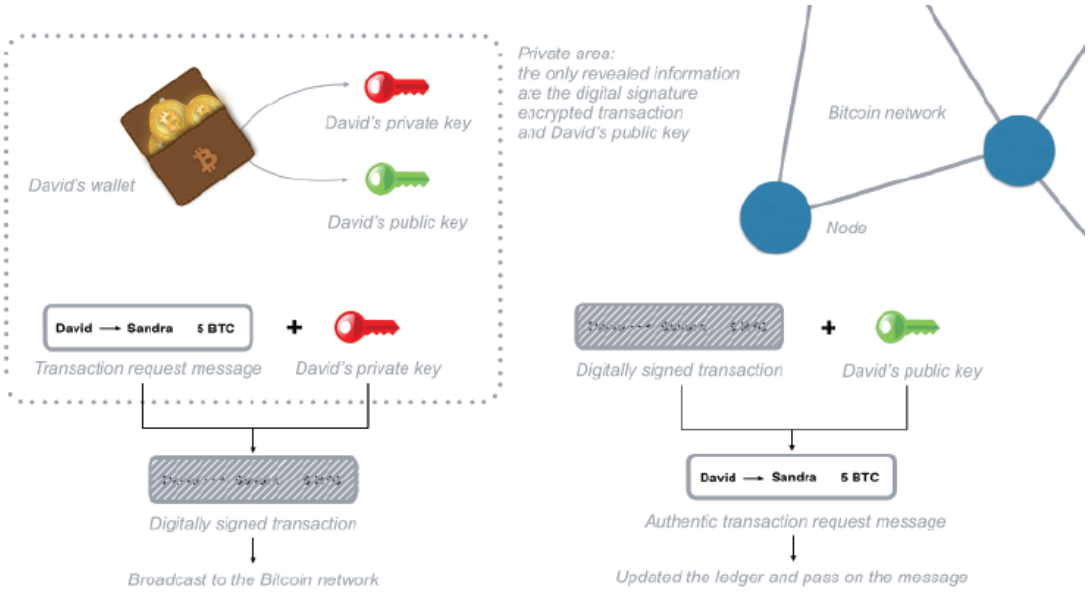


Figura 4: Verifica della transazione tramite chiavi

Ogni messaggio in uscita da un singolo indirizzo viene criptato con una chiave privata il quale, una volta derivata la corrispondente chiave pubblica con cui è possibile identificare univocamente l'indirizzo di partenza (*from*),deve poi essere validato dal nodo locale. La validazione è necessaria per accertarsi che la transazione sia stata realmente messa sulla rete dal proprietario dell'account. A questo punto solo i possessori della chiave pubblica associata potranno decifrare il messaggio.
Quando David vuole mandare 5 *Bitcoin* a Sandra, deve inviare sulla rete il messaggio criptato con la sua chiave privata in modo che venga identificato come il possessore di un certo numero di *Bitcoin* e sia di conseguenza l'unico a poter sbloccare il proprio *Wallet*. Tutti gli altri nodi validano la transazione, verificando tramite la chiave pubblica di David che la richiesta di inviare valuta sia effettivamente partita da lui. In questo modo si ottiene la validazione della transazione. In altre parole per poter inviare un *Bitcoin* è necessario provare alla rete di essere i possessori dell'indirizzo da cui partono i *Bitcoin*. Nella rete inoltre non viene tenuto conto del bilancio dei singoli utenti, ma vengono semplecemente registrate le transazioni che avvengono. La verifica di una transazione in

questo modo si riduce semplicemente al controllo di tutte le transazioni passate, effettuate dall'utente che vuole inviare una certa somma di *Bitcoin*.

1.2.3 Blocchi

Su una *blockchain* le transazioni vengono ordinate tramite accorpamento con altre transazioni avvenute in un lasso di tempo definito. In altre parole più transazioni vengono raggruppate insieme ed inserite dentro a quello che viene chiamato *Block* (Blocco). Ogni *block* contiene quindi un definito numero di transazioni ed un collegamento al nodo precedente. In questo modo si viene a creare una catena di blocchi molto simile ad una *linked list*. Da qui il nome *blockchain* (catena di blocchi).

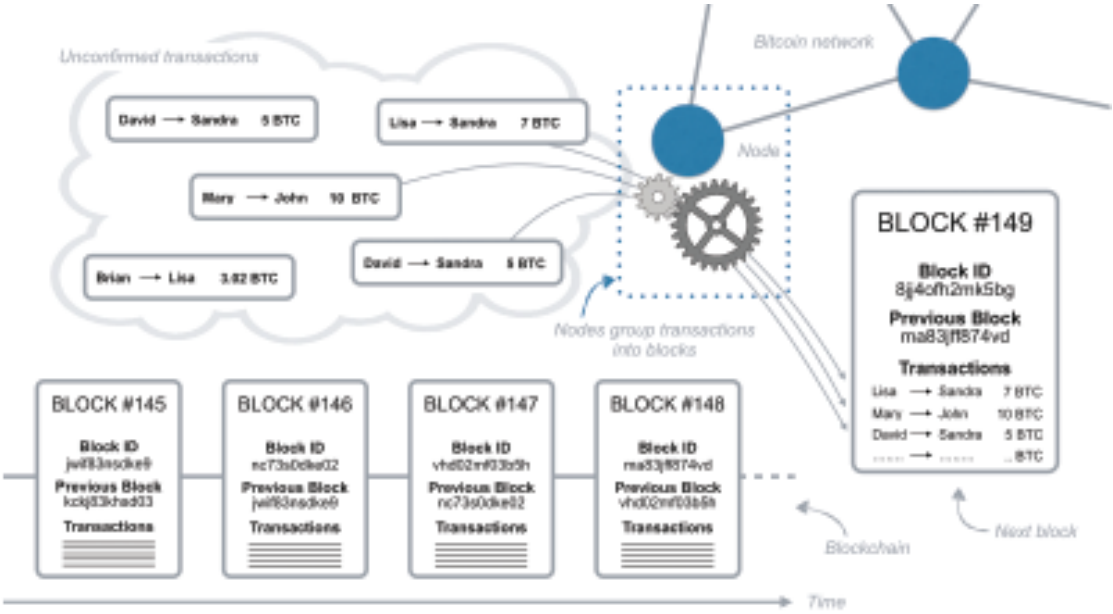


Figura 5: Rappresentazione di una blockchain

Le transazioni contenute nello stesso blocco sono considerate come avvenute nello stesso lasso temporale, mentre le transazioni che ancora non sono state raggruppate in un blocco sono considerate *Unconfirmed*, cioè non ancora validate.
Ogni nodo della rete può raggruppare più transazioni e creare un blocco, suggerendo alla rete di inserirlo come prossimo blocco della catena.
Per essere effettivamente inserito nella rete un blocco deve contenere la soluzione ad un complesso problema matematico che, per essere risolto richiede una grossa potenza di calcolo, ed un pò di fortuna. La risposta altro non è che un numero e l'unico modo per sapere quale sia il numero corretto da inserire consiste nel provarli tutti. Il nodo che per primo risolve il problema acquisisce il diritto di inserire il prossimo blocco sulla catena e lo invia a tutti i nodi adiacenti.

1.2.4 Mining

A questo punto sorge spontaneo una domanda, ossia: "Se i Bitcoin posseduti da un account sono il risultato della somma di tutte le transazioni inviate e ricevute da quell'account, come è possibile ottenere altri *Bitcoin*?"
La risposta a questa domanda é: "tramite il *mining*".
Il *mining* è l'attività svolta dai nodi definiti *miners*, i quali, tramite la risoluzione di un complesso problema matematico, validano i blocchi, permettendo così a tutti i partecipanti alla rete di inviare e ricevere transazioni.
La validazione di un blocco nella pratica è una attività molto dispendiosa, sia in termini di energia elettrica che di consumo di banda.
Perchè la catena possa proseguire (cioè perchè possano essere effettuate nuove transazioni) è necessario che i blocchi siano inseriti nella catena e per farlo è necessario risolvere questo problema matematico.
Il modo escogitato per ripagare chi indovina il numero che valida il blocco (cioè svolge il lavoro di *miner*) è una ricompensa in *Bitcoin* da parte della rete. Questa ricompensa è ciò che incentiva le persone a provvedere al necessario lavoro computazionale per far continuare la catena e mantenere la rete utilizzabile. Senza i *miners* i blocchi non potrebbero essere validati, la catena si fermerebbe e le transazioni non potrebbero più avere luogo.

1.3 Ethereum

1.3.1 Cos'é Ethereum

Come *Bitcoin*, *Ethereum* è una *public blockchain*.
Sebbene ci siano alcune significative differenze tecniche tra le due, la distinzione più importante da notare è che *Bitcoin* ed *Ethereum* differiscono sostanzialmente per scopo e capacità.
Il *Bitcoin* è stato lanciato come valuta alternativa, o moneta digitale, ed offre una particolare applicazione della tecnologia *blockchain*, ossia un sistema di pagamento elettronico.
Ethereum invece viene principalmnte utilizzato per applicazioni decentralizzate tramite l'utilizzo degli *Smart Contract*.
A differenza di *Bitcoin*, *Ethereum* utilizza due concetti di *token*: il primo prende il nome di *Ether* e corrisponde alla "moneta" effettivamente scambiata tra gli utenti della rete, il secondo viene invece utilizzato per pagare i *miners*, i quali includono le transazioni nei blocchi, e prende il nome di *gas*.

1.3.2 Smart Contract

Uno *Smart Contract* è un programma che contiene un insieme di regole a cui le parti interessate accettano di aderire.
Nel caso in cui le regole definite all'interno di uno smart contract siano soddisfatte l'accordo tra le parti viene automaticamente applicato.
Il codice di uno *Smart Contract* facilita, verifica e impone la negoziazione o l'esecuzione di un accordo o di una transazione e corrisponde alla forma più semplice di automazione decentralizzata.
Il successo di *Ethereum* (e la più grande differenza con *Bitcoin*) dipende proprio dal concetto di *Smart Contract*. grazie a cui è possible programmare una serie definita di azioni che vengono attuate se e solo se le condizioni in esso contenute vengono soddisfatte.