Università degli studi di Messina

Dipartimento di Scienze matematiche e informatiche,
scienze fisiche e scienze della terra

Corso di Laurea Triennale in INFORMATICA

Progetto di

CRITTOGRAFIA

"Crittografia presente nella tecnologia blockchain"

Realizzato da

DE PIETRO BERNARDO

Anno Accademico

2020/2021

Sommario

Lista delle figure

Capitolo 1: Introduzione

Con l'ascesa della criptovaluta Bitcoin, inizia l'ascesa anche di un'altra tecnologia che è direttamente correlata ad essa, cioè la Blockchain[1]. Satoshi Nakamoto definisce al momento della pubblicazione del protocollo bitcoin l'utilizzo di una tecnologia chiamata Blockchain. Per Satoshi questa tecnologia è molto utile per registrare tutte le transazioni di bitcoin avvenute e per ordinare quest'ultime cronologicamente.

Obiettivo del testo

Il testo si pone l'obiettivo di fornire una panoramica generale della tecnologia blockchain e della sua caratteristica più importante, cioè la crittografia.

[1] Si indica Blockchain con la "b" maiuscola quando ci si riferisce alla Blockchain di bitcoin. Mentre con la "b" minuscola ci si riferisce alla generica tecnologia della blockchain.

Capitolo 2: Blockchain

In questo capitolo vedremo una panoramica del mondo blockchain. Vedremo la nascita di questa tecnologia, successivamente vedremo un primo approccio con il suo funzionamento e infine vedremo che non esiste solo la blockchain di bitcoin ma bensì esistono diversi tipi di blockchain e diversi tipi di campi di applicazione.

Storia della blockchain

Per spiegare al meglio la nascita della blockchain dobbiamo fare un chiaro riferimento al Bitcoin[2]. Infatti nel 2008, veniva pubblicato il documento *"Bitcoin: A Peer-To-Peer Electronic Cash System"*, dove in questo documento l'autore descriveva l'utilizza della tecnologia peer-to-peer per lo scambio di valute digitali, appunto per lo scambio di bitcoin. Quindi Satoshi Nakamoto introduceva la possibilità di effettuare delle transazioni[3] di valute digitali direttamente tra due utenti andando eliminando il canale centralizzato e quindi evitando di avere una figura terza[4] durante l'operazione. A questo proposito Satoshi Nakamoto attraverso le parole chiave *"block"* e *"chain"* introduceva questa tecnologia con l'obiettivo di fungere da "libro mastro" di tutte le transazioni.

Definizione di blockchain

Una blockchain è essenzialmente un database distribuito di record o, per meglio dire, il database è formato dai registri pubblici[5] di tutte le transazioni che sono state eseguite e condivise dai partecipanti. Ogni transazione che avviene nei registri pubblici deve essere verificata dal consenso della maggioranza dei partecipanti al sistema.

Come funziona la blockchain?

Per spiegare al meglio il funzionamento della blockchain è utile prendere come esempio uno scambio di Bitcoin perché è intrinsecamente collegato alla tecnologia blockchain.
Bitcoin usa la prova crittografica al posto dell'attuale meccanismo del *trust-in-the-third-party* [6]per effettuare delle transazioni online. Ogni transazione è protetta attraverso la *firma*

[2] Bitcoin è una criptovaluta diventata famosa nell'ultimo decennio principalmente per via della sua crescita di valore.

[3] Le transazioni indicano uno scambio di risorse tra due utenti.

[4] Con figura terza si indicano tutti gli enti governativi o finanziari.

[5] I registri pubblici sono il luogo dove vengono immagazzinate tutte le transazioni avvenute.

[6] Il meccanismo trust-in-the-third-party indica che ogni transazione viene supervisionata di una terza figura di cui ci si fida.

digitale[7], è viene inviata alla "chiave pubblica" del destinatario, e digitalmente viene la transazione viene firmata con la "chiave privata" del mittente. Attraverso la firma con la chiave privata, il proprietario della criptovaluta autentica che la transazione è stata effettuata da lui. Il destinatario della criptovaluta per accedere al contenuto della transazione dovrà utilizzare la propria chiave privata.

Ogni transazione è visibile a tutti i nodi della rete e viene registrata in un registro pubblico dopo che viene verificata. Ogni singola transazione ha bisogno di essere verificata per la validazione prima di essere registrata all'interno del registro pubblico. La verifica dei nodi ha bisogno di garantire due cose prima di registrare qualsiasi transazione:

1. Il mittente possiede la criptovaluta.
2. Il mittente deve avere una sufficiente quantità di criptovaluta nel suo account, e questo viene verificato attraverso il controllo di tutte le transazioni effettuate dall'account del mittente. Questo garantisce che c'è effettivamente una quantità sufficiente di criptovaluta nel suo account prima di finalizzare la transazione.

Per capire meglio il funzionamento delle transazioni in blockchain, nella figura 1 vediamo il processo semplificato di una transazione.

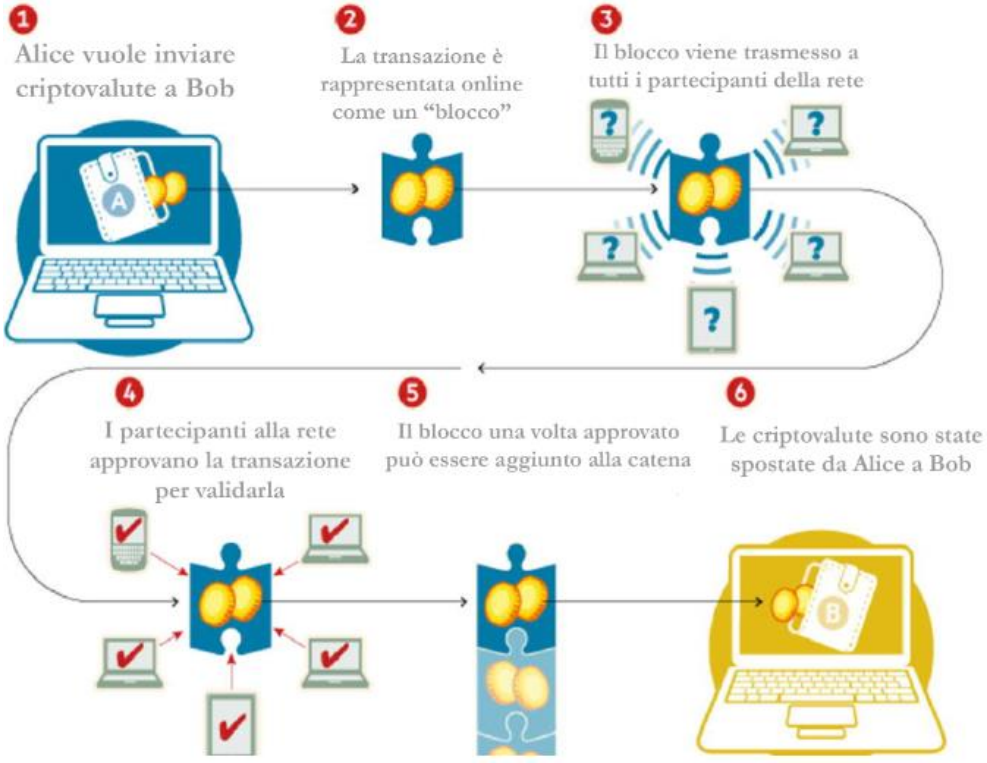


Figure 1: Fasi transazioni semplificate

[7] La firma digitale viene approfondita nel capitolo della crittografia.

Tipi di blockchain

Nel precedente paragrafo abbiamo preso in considerazione la blockchain utilizzata per la criptovaluta Bitcoin ma esistono diversi tipi di blockchain.
Andiamo a descrivere brevemente due principali alternative alla blockchain di Bitcoin.

Figure 2: Logo Ethereum

Ethereum

Secondo il sito ufficiale "Ethereum è una piattaforma decentralizzata che gestisce *contratti intelligenti* o *Smart Contract*[8]". Ethereum viene espresso sotto il concetto di database distribuito però la differenza principale con Bitcoin è che Ethereum è definita come "moneta altamente programmabile", cioè è possibile attraverso la creazione di codice, generare la criptovaluta (o *ether*[9]) molto più semplicemente e velocemente di Bitcoin.

Ripple

Ripple è una blockchain di tipo "ibrido" utilizzata per inviare denaro in tutto il mondo sfruttando le capacità di un'architettura basata sul modello Shared Decentralized Ledger[10]. Le istituzioni finanziare, entrando a far parte di questa rete globale, possono elaborare i pagamenti dei propri clienti in qualsiasi parte del mondo in modo istantaneo, affidabile ed economico.

Figure 3: Logo Ripple

Futuro della blockchain

Finora abbiamo visto la blockchain come un mezzo per immagazzinare transazioni di criptovalute, però la blockchain non si limita ad essere utilizzata solamente nel campo della finanza ma bensì la blockchain in futuro (ma già applicata in piccola parte) potrà essere utilizzata anche in altri campi.

[8] Gli smart contract sono descritti nell'appendice.

[9] L'ether è il nome della moneta digitale scambiabile nella blockchain di Ethereum.

[10] Le architetture dei ledger sono descritte nell'appendice.

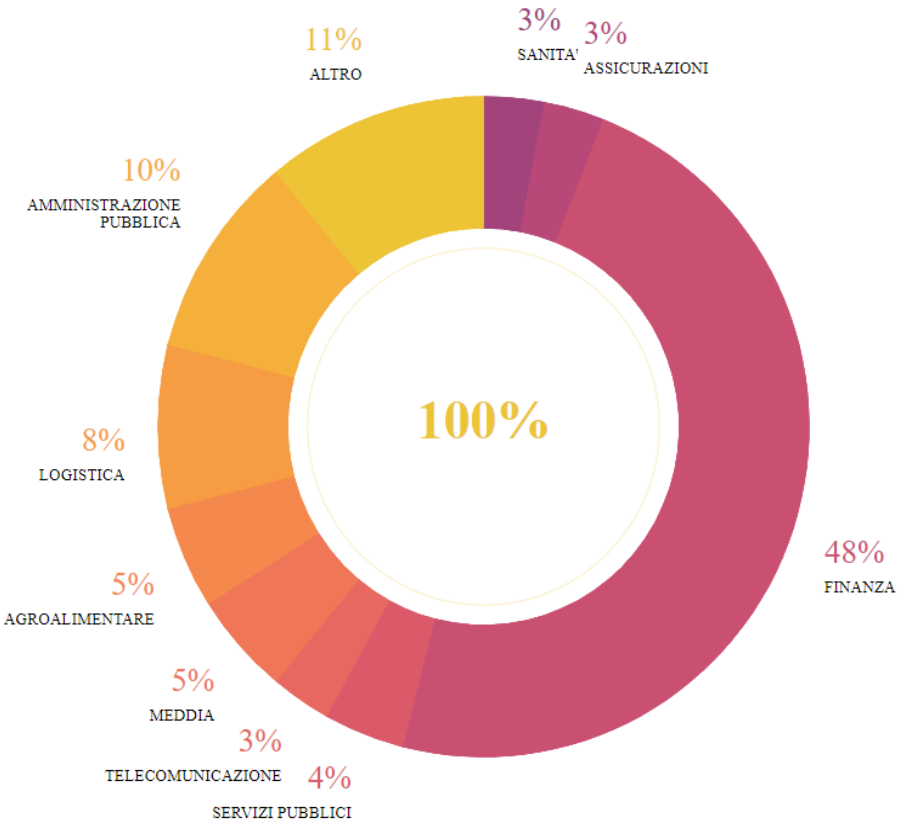


Figure 4: Campi di utilizzo blockchain

Capitolo 3: Crittografia

In questo capitolo andremo ad affrontare la crittografia principale che viene utilizzata nella tecnologia blockchain però qui andremo a vedere i singoli casi di crittografia fuori dal contesto blockchain. Nel capitolo 4 andremo ad unire quello che vedremo in questo capitolo con degli esempi di transazioni sulla blockchain.

Definizione di crittografia

La crittografia contiene una serie di metodi per occultare un messaggio, in modo da non essere comprensibile a persone non autorizzate a leggerlo. La crittografia consta di alcuni principi, tra questi troviamo:

- **Sistema crittografico**: è il sistema che realizza la funzionalità di natura crittografica, quindi è un algoritmo o protocollo;
- **Testo in chiaro**: è il contenuto originale del messaggio comprensibile a chiunque;
- **Testo cifrato**: è l'alterazione volontaria e reversibile del messaggio originale, cioè del testo in chiaro;
- **Chiave**: i metodi di cifratura utilizzano una chiave per cifrare il testo in chiaro. La chiave è nota solo al mittente ed al destinatario.

Crittografia asimmetrica

Esistono due principali sistemi crittografici, e sono:

- **Sistema simmetrico**: in questo tipo di sistema si utilizzano solamente delle chiavi segrete per cifrari i messaggi.
- **Sistema asimmetrico**: nel sistema asimmetrico ogni attore ha una chiave pubblica, visibile a tutti, e una chiave privata.

Ci concentriamo sulla crittografia asimmetrica poiché è una componente molto importante della blockchain.

Principalmente quando si utilizza la crittografia asimmetrica si possono realizzare due tipi di funzioni: nella prima funzione si utilizza la chiave pubblica per autenticare il messaggio inviato dal titolare con la chiave privata abbinata, mentre nella seconda funzione il messaggio viene cifrato con la chiave pubblica del destinatario per garantire che solo il titolare della chiave privata possa decifrarlo.

In pratica in un sistema che utilizza la crittografia asimmetrica chiunque può utilizzare la chiave pubblica di un utente per cifrare un messaggio, ma il messaggio può essere decifrato solamente da chi possiede la chiave privata del destinatario.

La sicurezza di questo tipo di crittografia dipende unicamente dal mantenere la chiave privata segreta mentre la chiave pubblica non può compromettere in alcun modo la sicurezza.

Segretezza

Vediamo un esempio per mantenere la segretezza quando si utilizza la crittografia asimmetrica:

1. Alice cifra un messaggio X con la chiave pubblica di Bob e genera il testo cifrato Y.
2. Bob utilizza la sua chiave privata per decifrare Y e ottenere X. Nessuno eccetto Bob può decifrare il messaggio X, neanche Alice che lo ha cifrato.

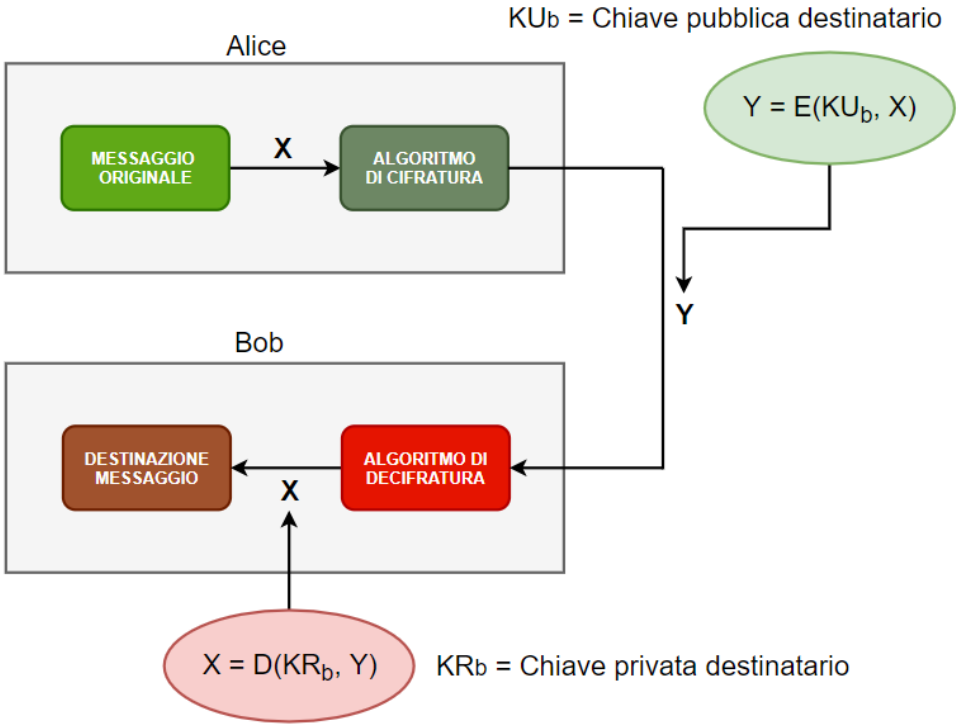


Figure 5: Segretezza messaggio

Autenticazione

L'autenticazione serve per certificare l'autore che ha inviato il messaggio. Le operazioni rimangono simili come nella segretezza con l'unica modifica che, Alice cifra il messaggio X con la sua chiave privata generando il messaggio cifrato Y, successivamente lo invia a n persone. Chiunque delle n persone che decifra il messaggio Y con la chiave pubblica di Alice otterrà il messaggio originale X e avrà la certezza che il messaggio è stato scritto da Alice poiché solo lei conosce la sua chiave privata.

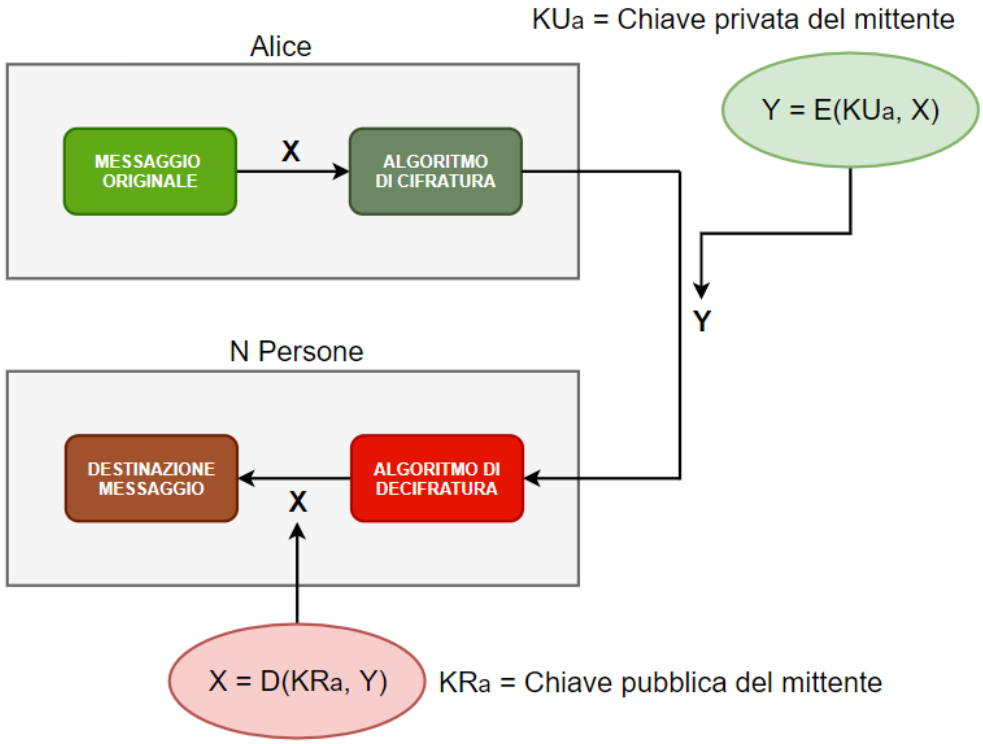


Figure 6: Autenticazione messaggio

Autenticazione e segretezza

Possiamo ottenere l'autenticità e la segretezza del messaggio utilizzando entrambi i metodi precedentemente visti. Quindi, facciamo un esempio per capire meglio come fare per mantenere la segretezza e assicurare l'autenticazione:

1. Alice cifra un messaggio X con la propria chiave privata e genera Y (certezza sull'identità del mittente);
2. Alice cifra il messaggio cifrato Y con la chiave pubblica di Bob (privatezza del messaggio), generando un messaggio Z e lo recapita a destinazione;
3. Bob decifra il messaggio Z con la propria chiave privata e ottiene Y;
4. Bob decifra Y con la chiave pubblica di Alice ottenendo il messaggio originale X.

Utilizzando questo metodo solo Bob può leggere il messaggio e allo stesso tempo ha la certezza che il messaggio è stato inviato da Alice.

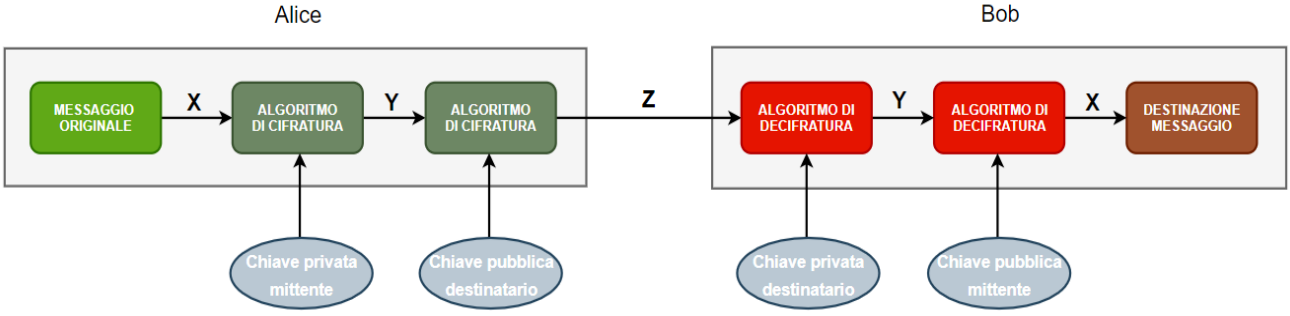


Figure 7: Segretezza e autenticità messaggio

Funzioni hash

La funzione hash è un algoritmo matematico che mappa i dati di lunghezza arbitraria, quindi un messaggio, in una stringa binaria di dimensione fissa chiamata **valore di hash** o **message digest**.
La resistenza alle collisioni delle funzioni hash si divide in due proprietà:

- Resistenza alle collisioni debole
- Resistenza alle collisioni forte

Queste due proprietà corrispondo a due diversi tipi di attacchi:

- **Attacco a forza bruta**: in pratica questo tipo di attacco è basato sulla creazione di due messaggi M e M', questi due messaggi devono produrre lo stesso valore hash cosicché il mittente del messaggio firmi il messaggio M ma allo stesso tempo l'attaccante ottiene la firma del messaggio M'.
- **Attacco del compleanno**: questo attacco è basato sul paradosso del compleanno[11]. Il mittente si prepara a "firmare" un messaggio aggiungendo il codice hash di m bit appropriato e crittografando tale codice hash con la propria chiave privata. Successivamente, l'attaccante genera $2^{m/2}$ varianti del messaggio, ognuna delle quali ha fondamentalmente lo stesso significato, e allo stesso tempo genera un ugual numero di messaggi che sono varianti del messaggio fraudolento da sostituire al messaggio originale. I due insiemi di messaggi generati vengono confrontati fin quando non si trovano due messaggi che producano lo stesso codice hash. Trovata la coppia, l'attaccante offre la variante al mittente che accettando la modifica e firmando il messaggio starà firmando anche il messaggio fraudolento perché i messaggi con lo stesso codice hash producono la stessa firma.

Caratteristiche di una funzione hash sicura

Le caratteristiche fondamentali che rende sicura una funzione hash sono:

1. Può essere applicata a messaggi M di qualsiasi lunghezza e produce un'uscita di lunghezza fissa h;
2. È facile calcolare h = H(M) per qualsiasi messaggio M;
3. Deve essere deterministico, cioè da input uguali si ottengono sempre output uguali (**coerenza**);
4. Dato h è computazionalmente impossibile determinare un M tale che H(M) = h (one-way, cioè **non invertibile**).

[11] Il paradosso del compleanno afferma che la probabilità che almeno due persone in un gruppo compiano gli anni lo stesso giorno è largamente superiore di quello che ci si potrebbe aspettare.

5. Per qualsiasi blocco x è computazionalmente impossibile trovare una y ≠ x tale che H(y) = H(x) - (**resistenza debole alle collisioni**);
6. È computazionalmente impossibile trovare una coppia (x, y) tale che H(x) = H(y) (**univocità, resistenza forte alle collisioni**);
7. Output uniformemente distribuito (**Casualità**).

Algoritmi di hash

La struttura utilizzata dalla maggior parte delle funzioni hash è quella ideata da Merkle, che consiste in una funzione hash iterata. La funzione hash prende un messaggio in input e lo divide in L blocchi di dimensioni fisse pari a *b* bit.

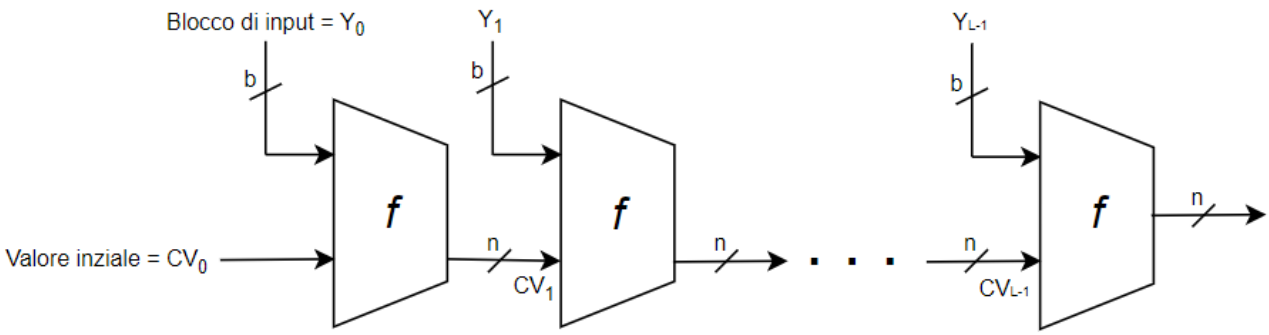


Figure 8: Algoritmo di hash

L'algoritmo di hash comporta la ripetizione di una funzione di compressione f, che accetta due input (la variabile di concatenamento CV e un blocco Y di *b* bit) e produce un output di *n* bit.
All'inizio del calcolo della funzione di hash, la variabile di concatenamento ha un valore prefissato dall'algoritmo (Valore inziale CV_0). Ad ogni iterazione CV_i sarà uguale a $f(CV_{i-1}, Y_{i-1})$.
Se la funzione di compressione è resistente alle collisioni precedentemente viste lo sarà anche la funzione iterata.

Firma digitale

Le firme digitali sono contraddistinte da alcune proprietà, e sono:

- Controllare l'autore, la data e il momento della firma;
- Autenticare i contenuti del messaggio;
- Verifiche da parte terzi per risolvere dispute.

Quindi dopo aver definito queste proprietà capiamo subito che la funzione di firma digitale include la funzione di autenticazione.
Uno schema di firma digitale deve soddisfare dei requisiti, tra questi troviamo:

- La firma deve essere una configurazione di bit che dipende dal messaggio firmato;
- La firma deve utilizzare informazioni specifiche del mittente in modo da impedirgli sia modifiche al messaggio che la possibilità di negare di aver inviato il messaggio;
- Deve essere relativamente facile produrre la firma digitale.
- Deve essere relativamente facile riconoscere e verificare la firma digitale.
- Deve essere computazionalmente impossibile falsificare una firma digitale costruendo un nuovo messaggio per una firma digitale esistente oppure costruendo una firma digitale fraudolenta a partire da un determinato messaggio.
- Deve essere possibile conservare una copia della firma digitale.

Principalmente le firme digitali si dividono in due categorie: **firme digitali dirette** e **firme digitali arbitrate**.

Firme digitali dirette

Le firme digitali dirette sono caratterizzate dal rapporto unico tra mittente e destinatario. Si presuppone che il destinatario possieda la chiave pubblica del mittente. La firma digitale viene fatta dal mittente firmando l'intero messaggio o solo l'hash con la chiave privata. È anche possibile criptare il tutto con la chiave pubblica del destinatario.
È molto importante che prima della cifratura del messaggio, esso vengo firmato.
La sicurezza dipende dalla chiave privata del mittente che può essere compromessa o può pretendere di averla perduta. Per ottenere la segretezza, come precedentemente visto, si potrebbe cifrare tutto con la chiave pubblica del destinatario.

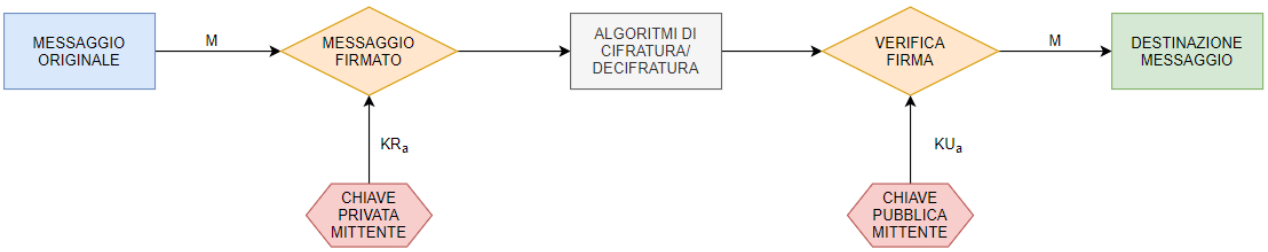


Figure 9: Semplificazione schema firma digitale diretta

Guardando attentamente la categoria delle firme digitali dirette notiamo che la credibilità dello schema è basata completamente sulla sicurezza della chiave privata del mittente. Infatti, se un mittente in seguito all'invio di un messaggio volesse negare di aver inviato un determinato messaggio, potrebbe sostenere che la chiave privata è stata persa, rubata o falsificata.
Per rendere meno probabile la presenza di questo problema si possono impiegare dei controlli amministrativi sulla chiave privata, ma purtroppo il problema non può essere eliminato definitivamente.

Firme digitali arbitrate

Le firme digitali arbitrate comportano la presenza di un arbitro.

L'arbitro effettua la validazione di ogni messaggio firmato e provvede a datare il messaggio e a inviarlo al destinatario. L'arbitro non deve necessariamente vedere il contenuto del messaggio.

Questo tipo di approccio può essere applicato sia ai sistemi simmetrici che a quelli asimmetrici.

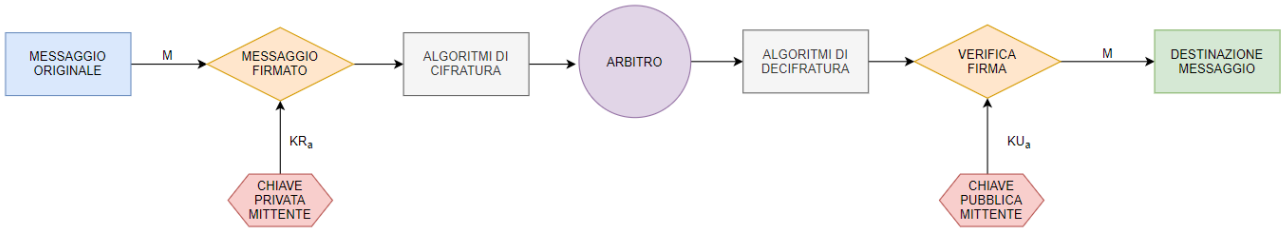


Figure 10: Semplificazione schema firma digitale arbitrata

Capitolo 4: Struttura della blockchain

Dopo aver dato una definizione generica della crittografia divisa dal concetto blockchain, in questo capitolo è presente la descrizione specifica di ogni componente della tecnologia blockchain con le relative componenti crittografiche.

Componenti blockchain

Blockchain è una tecnologia che a prima vista può essere complessa, tuttavia, può essere semplificata andando a esaminare ogni componente individualmente.

Funzioni hash

La funziona hash che viene spesso utilizzata nella maggior parte delle blockchain è la SHA-256. All'interno di una rete blockchain, le funzioni hash sono utilizzate per molte attività, come:

- Derivazione dell'indirizzo (lo vedremo in seguito).
- Creazione di identificatori univoci.
- Sicurezza del block data[12]: quando viene stabilito un nodo sarà fatto l'hash del block data, creando un digest che sarà immagazzinato all'interno del block header[13].
- Sicurezza del block header: quando viene stabilito un nodo sarà fatto l'hash del blocco header. Se ad esempio la rete blockchain utilizza il modello di consenso *proof-of-work*[14], verrà fatto l'hash del block header semplicemente utilizzando un differente valore di *nonce*[15]. Una volta creato l'hash digest del block header, l'intestazione del blocco corrente verrà inclusa all'interno del blocco successivo, dove saranno protetti i dati del block header corrente.

Transazioni

Una transazione rappresenta un'interazione tra utenti della rete. Ogni blocco della blockchain può contenere zero o più transazione.

I dati che compongono una transazione possono essere differenti per ogni blockchain, tuttavia il meccanismo delle transazioni è in gran parte lo stesso. Un utente della rete blockchain invia informazioni alla rete blockchain. L'informazione inviata dovrebbe include l'address del mittente, la sua chiave pubblica, una firma digitale, gli input e output della transazione.

[12] Il block data viene approfondita nel paragrafo dei blocchi.
[13] Anche il block viene approfondito nel paragrafo dei blocchi.
[14] Con il proof-of-work ogni utente che verifica una transazione deve fornire la prova che ha validato una transazione.
[15] Il nonce è un numero arbitrario che può essere combinato con i dati per produrre diversi digest dello stesso messaggio.

Una singola transazione di criptovaluta tipicamente richiede almeno le seguenti informazione, ma può contenerne di più:

- **Input** – Gli input sono generalmente una lista di asset digitali da trasferire. Una transazione farà riferimento alla fonte, cioè alla provenienza dell'asset digitale, o possiamo dire che la transazione contiene un riferimento agli eventi passati dell'asset. Poiché l'input alla transazione è un riferimento a eventi passati, gli asset non cambiano. Nel caso delle criptovalute questo significa che non è possibile aggiungere o rimuovere valore negli asset. Tuttavia, un singolo asset digitale può essere suddiviso in multipli nuovi asset oppure tanti nuovi assets possono essere uniti per formare una nuova risorsa più grande. La suddivisione e l'unione verrà specificata negli output della transazione.
  Il mittente deve fornire la prova che può avere accesso agli input di riferimento, generalmente avviene firmando digitalmente la transazione.
- **Output** – Gli output sono generalmente gli account che faranno da recipiente per gli asset digitali forniti o ricevuti. Ogni output specifica il numero di asset digitali trasferiti al nuovo proprietario, l'identificatore del nuovo proprietario, e un set di condizioni che i nuovi proprietari dovranno soddisfare per poter utilizzare quelle risorse.
  Nell'output esiste anche il meccanismo del "make change", questo meccanismo fa sì che, nel caso in cui l'asset digitale è maggiore di quello che si vuole inviare, esso suddivide la transazione in più output, dove il mittente invia la quantità esatta al destinatario e la rimanenza la invia a sé stesso.

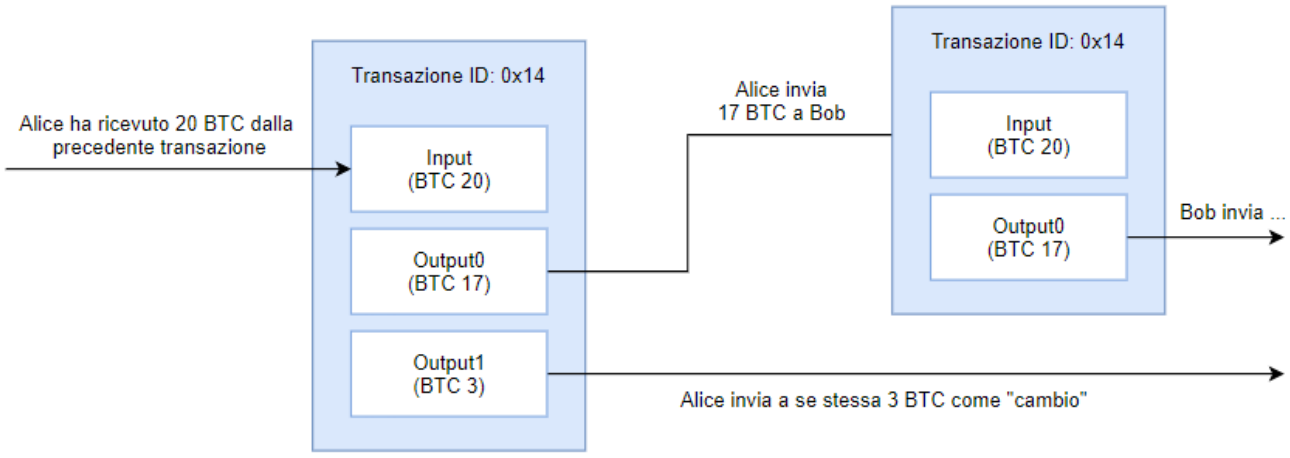


Figure 11: Esempio di transazione bitcoin

Una volta effettua una transazione è importante determinare la validità e l'autenticità di essa. La validità di una transazione indica che la transazione va incontro ai requisiti del

protocollo adottato dalla blockchain. L'autenticazione di una transazione è importante, poiché determina che il mittente dell'asset digitale ha veramente accesso agli asset inviati. Le transazioni sono tipicamente firmate digitalmente dal mittente associando la sua chiave privata e la transazione può essere verificata in qualsiasi momento utilizzando la sua chiave pubblica (questo processo è il sistema crittografico asimmetrico visto nel capitolo precedente).

Crittografia asimmetrica

Nel capitolo precedente abbiamo visto come funziona la crittografia asimmetrica. In questo paragrafo viene fornito un sommario dell'uso della crittografia asimmetrica nella maggior parte delle reti blockchain:

- Le chiavi private sono usate per firmare digitalmente le transazioni.
- Le chiavi pubbliche sono usate per derivare l'address degli utenti.
- Le chiavi pubbliche sono usate per verificare le firme digitali generate con le chiavi private.
- La crittografia asimmetrica fornisce l'abilità di verificare che l'utente che effettua il trasferimento all'altro utente è in possesso della chiave privata in grado di firmare la transazione.

Derivazione degli address

La maggior parte delle blockchain fanno uso di un *address*, che è una stringa di caratteri alfanumerici. Questa stringa viene derivata utilizzando le funzioni hash. Un metodo per generare un address è creare una chiave pubblica, su quest'ultima si applica un algoritmo hash, il risultato sarà l'address.

Figure 12: Derivazione address

Blocchi (Blocks)

Ogni volto che un nodo pubblica un blocco, ad esso vengono aggiunte le transazioni. Un *block* contiene un *block header* e un *block data*. Molte blockchain utilizzano diversi campi all'interno del block header e del block data. Questi campi sono i seguenti:

- Block Header
    - Il numero di blocco, noto anche come altezza del blocco in alcune blockchain.

- Il valore hash del precedente block header.
- Una rappresentazione hash del block data.
- Un timestamp[16].
- La misura del blocco.
- Il valore del nonce.

- Block Data
  - Una lista delle transazioni e dei registri inclusi nel blocco.
  - Altri dati aggiuntivi opzionali.

Concatenamento dei blocchi

I blocchi sono concatenati insieme dove ogni blocco contiene l'hash digest del precedente blocco header, insieme di questi blocchi forma la cosiddetta *blockchain*.

Nella figura 13 vediamo una generica catena di blocchi. È importante notare che i blocchi sono concatenati seguendo una linea temporale poiché questo sistema evita di creare nuovi blocchi prima aver raggiunto la misura massima dell'ultimo blocco.

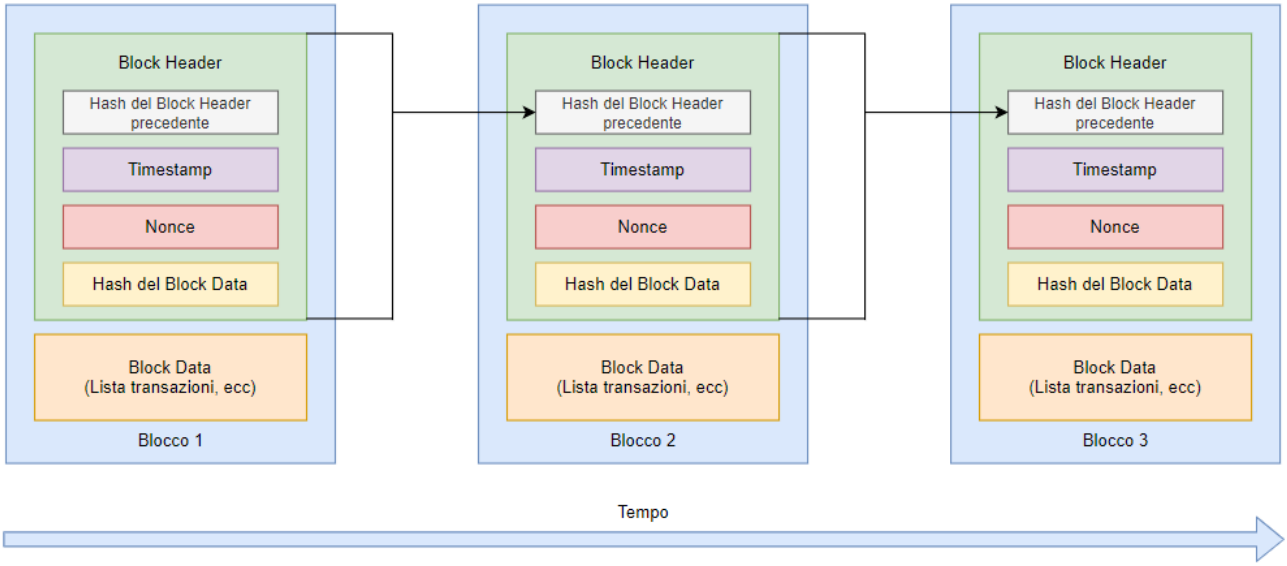


Figure 13: Generica Catena di Blocchi

Capitolo 5: Sicurezza

Come in ogni tecnologia attualmente presente, la tecnologia blockchain non è sicura al cento percento. In questa capitolo vedremo alcuni problemi legati alla sicurezza presenti nella tecnologia blockchain.

[16] Il timestamp indica l'ora e la data in cui è stato creato un blocco.

Sicurezza informatica

L'utilizzo della tecnologia blockchain non rimuove i rischi inerenti alla sicurezza informatica che richiedono una gestione del rischio ponderata e proattiva. Molti di questi rischi sono spesso ricollegati all'elemento umano. Pertanto un solido programma di sicurezza informatica rimane vitale per proteggere la rete e le organizzazioni partecipanti dalle minacce informatiche, in particolare poiché gli hacker sviluppano una maggiore conoscenza delle reti blockchain e delle loro vulnerabilità.

Fatta la precedente premessa, gli standard e linee guida esistenti per la sicurezza informatica rimangono altamente affidabili per garantire la sicurezza dei sistemi che si interfacciano o che si basano su reti blockchain. Quindi in generale, gli standard e linee guida esistenti permettono di avere una base solida per proteggere le reti blockchain dagli attacchi informatici.

Attacchi informatici basati sulla rete

Le tecnologie blockchain sono altamente pubblicizzate come estremamente sicure grazie alla progettazione a prova di antimanomissione e resistente alle manomissioni: una volta che una transazione è immagazzinata in un blocco pubblico, generalmente non può più essere modificata. Tuttavia, questo è vero solo per le transazioni che sono state immagazzinate nel blocco pubblico. Le transazioni che non sono state incluse all'interno di un blocco sono vulnerabili a diversi tipi di attacchi. Per le reti blockchain che, ad esempio, utilizzano i timestamp transazionali questo potrebbe avere dei risvolti positivi ma anche soprattutto negativi su una transazione. Gli attacchi Denial of Service possono essere condotti sulla piattaforma blockchain o sugli smart contract implementati sulla piattaforma.

Le reti blockchain e le loro applicazioni non sono immuni da malintenzionati che possono condurre scansioni della rete per scoprire e sfruttare le vulnerabilità.

Utenti malintenzionati

Il problema più grande per gli utenti malintenzionati è quella di ottenere una potenza sufficiente per causare danni alla rete. Però se questa potenza viene raggiunta, l'utente potrebbe causare danni molto ampi alla rete, le azioni di mining[17] dannose possono includere:

- Oscurare le transazioni di utenti, nodi o persino di interi paesi specifici.

[17] Con mining si intende l'azione di verificare una transazione per riscuotere il premio per la validazione di una transazione.

- L'utente maleintenzionato può creare una catena alternativa in segreto. Una volta che la catena alternativa è più lunga della catena reale, i nodi onesti passeranno alla catena che ha maggiore lavoro svolto (questo tipo di atteggiamento da parte della rete è descritta nel protocollo blockchain). Questo tipo di attacco compromette il principio per cui una rete blockchain è a prova di manomissione e resistente alle manomissioni.

Appendice

Ledger

Un *ledger* è una collezione di transazioni. Attualmente i ledger sono stati archiviati digitalmente, spesso in grandi database di proprietà e gestiti da una terza parte centralizzata di fiducia.

Smart Contract (Contratti intelligenti)

Uno *smart contract* è una collezione di codice e dati che viene distribuita utilizzando transazioni firmate crittograficamente sulla rete blockchain. Gli smart contract sono eseguiti dai nodi della rete blockchain. Tutti i nodi che eseguono gli smart contract devono derivare gli stessi risultati dall'esecuzione e, questi risultati vengono registrati all'interno della blockchain.

Modello di consenso Proof of Work

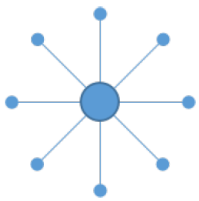
In un modello di consenso proof of work (PoW), un utente pubblica il blocco successivo essendo il primo a risolvere l'enigma ad alta intensità di calcolo. La soluzione di questo enigma è la "prova" o "proof" che gli utenti hanno eseguito il lavoro. L'enigma è progettato per essere difficile da risolvere ma la verifica che la soluzione sia valida è facile. Questo tipi di modello di consenso viene utilizzato dal protocollo Bitcoin.

Criptovaluta

La criptovaluta è un asset/moneta/unità digitale di un sistema, il quale è crittograficamente inviata da un utente all'altro della rete blockchain.

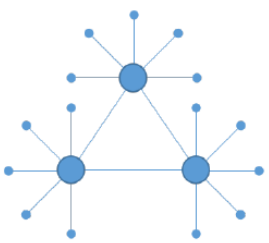
Network centralizzato

Il network centralizzato è una rete dove i partecipanti dovrebbero comunicare con un'autorità centrale per comunicare con un altro utente. Poiché tutti i partecipanti devono passare attraverso unnica fonte centralizzata, la perdita di quella fonte impedirebbe a tutti i partecipanti di comunicare.



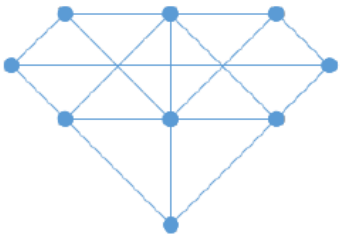
Network decentralizzato

Il network decentralizzato è una rete dove ci sono multiple autorità dove ognuna di queste forma un network centralizzato per un sezioni di partecipanti. Poiché alcuni partecipanti si trovano divisi in sezioni di network centralizzati, la perdita di una sezione impedisce solamente



ai partecipanti di quella sezione di comunicare con altri partecipanti mentre la restante rete potrà continuare a comunicare normalmente.

Network distribuito



Un network distribuito è una rete dove ogni partecipante può comunicare con un altro partecipante senza passare attraverso una autorità centralizzata. Poiché esistono diverse vie di comunicazione, la perdita di qualsiasi partecipante non blocca le comunicazioni. Questo tipo di network è anche conosciuto come *network peer-to-peer*.