Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

CrypTO

Crittografia e Teoria dei Numeri

APPLICAZIONI TECNOLOGICHE DELLA CRITTOGRAFIA: LA BLOCKCHAIN

Danilo Bazzanella (CrypTO - https://crypto.polito.it)

29 maggio 2025

Politecnico di Torino

DISMA

La tecnologia Blockchain

Gli strumenti matematici per costruire una Blockchain:

- **Sistema crittografico a chiave pubblica**
- **Firma digitale**
- **Funzione hash**

Sistemi a chiave pubblica (Sistemi asimmetrici)

Nei sistemi a chiave pubblica **ogni utente ha due chiavi, una pubblica e una privata**, e non c'è il problema dello scambio chiavi, perchè ogni utente se le può generare entrambe autonomamente.

La chiave pubblica di un utente serve a tutti gli altri per cifrare un documento a lui destinato e la chiave privata viene usata dall'utente per decifrare. **Essendo lui l'unico che conosce la chiava privata è l'unico che può decifrare.**

Firma digitale

Firma digitale

Protocollo che permette di attestare l'autenticità e la non ripudiabilità di un documento elettronico

L'idea di base delle firme digitali è di produrre un dato (**che dipende dal documento che si vuole firmare, oltre che dalla chiave pubblica del firmatario**) che chiunque può facilmente verificare essere soluzione di una istanza di un problema matematico molto difficile, che **solo chi conosce la chiave segreta può produrre in un tempo ragionevole**.

Funzione Hash

Funzione hash

Una funzione hash è una funzione che trasforma qualsiasi sequenza binaria di lunghezza arbitraria in una sequenza lunga n bit (n fissato), con le seguenti proprietà:

- calcolabile efficientemente
- impossibile da invertire in tempi ragionevoli
- effetto valanga
- estremamente difficile trovare collisioni

Bitcoin

Bitcoin ha un obiettivo piuttosto limitato, anche se molto ambizioso, gestire il trasferimento di valore in una rete, cioè funzionare da forma di **denaro**.

Bitcoin permette di trasferire la proprietà dei bitcoin (BTC) da una persona a un'altra, anzi più precisamente da un indirizzo Bitcoin a un altro indirizzo Bitcoin.

L'indirizzo Bitcoin è la chiave pubblica (primo strumento).

Mediante la **firma digitale** (secondo strumento), che può fare solo chi conosce la chiave segreta, si possono trasferire i BTC da un indirizzo ad un altro.

Una semplice transazione di Bitcoin consiste quindi di:

- **un indirizzo di input** da dove provengono i BTC
- **un indirizzo di output** dove finiscono i BTC
- **il tutto firmato digitalmente** con la chiave segreta corrispondente all'indirizzo di input

Per fare tutto ciò non abbiamo avuto bisogno della Blockchain: bastano un sistema a chiave pubblica e la relativa firma digitale.

Rimangono però due problemi:

- **l'indirizzo di input deve avere ricevuto bitcoin in passato**
- **non deve essere possibile spendere due volte gli stessi bitcoin** (**double spending**)

Blockchain: Le transazioni sulla rete Bitcoin vengono **raggruppate in blocchi** e ogni blocco viene collegato al precedente, inserendo in ogni blocco **la hash del blocco precedente** (terzo strumento).

Si costruisce quindi una **catena ordinata di blocchi**, condivisa da tutta la rete (peer-to-peer), in modo che **tutta la rete possa verificare la validità di tutte le transazioni, evitando i double spending.**

Sicurezza della Blockchain

L'immutabilità della Blockchain è data dal fatto che ogni nodo della rete peer-to-peer ne ha una copia (nessuno può attaccare migliaia di computer contemporaneamente) e che ogni blocco è legato al precedente mediante una funzione hash.

Il vero problema di sicurezza per una Blockchain è la sua dinamicità, data dalla necessità di inserire nuovi blocchi in continuazione.

Ogni Blockchain ha la necessità di avere un **protocollo di consenso**, cioè un modo condiviso per inserire i blocchi.

Protocollo di consenso di Bitcoin

Ci sono molti diversi protocolli di consenso, ma quello più utilizzato e che utilizza anche Bitcoin è la **proof-of-work** (PoW), che significa **"prova di lavoro"** .

Un **miner** per avere diritto a inserire un blocco deve inserire nel blocco un **numero casuale (nonce)** e calcolare la hash del blocco (nuovo utilizzo del terzo strumento), cambiando il nonce **fino a che tale hash non sia minore di un certo target fissato e noto a tutta la rete** (che viene regolarmente adattato per mantenere la velocità di creazione dei blocchi a circa un blocco ogni 10 minuti).

Compenso ai miner e creazione dei Bitcoin

- **Coinbase transaction** il miner ha diritto a inserire una prima transazione nel blocco, di importo stabilito. Tale transazione è senza indirizzo di input
- **Compenso** in questo modo si creano i bitcoin assegnandoli ai miner, come compenso al lavoro per il sistema
- **Conio dei bitcoin** questo è l'unico modo in cui vengono creati i bitcoin
- **Halving** ogni (circa) 4 anni il compenso ai miner viene dimezzato

Oltre Bitcoin

Come abbiamo visto la **Blockchain** può essere usata per decentralizzare la gestione del denaro, come in Bitcoin, senza quindi avere bisogno una autorità centrale (Banca, Banca Centrale, Stato...).

La cosa molto interessante è che i risultati ottenuti da Bitcoin con la propria Blockchain può essere utilizzata in qualsiasi altra situazione nella quale si volesse **gestire una comunità senza una autorità centrale, in modo decentralizzato, eliminando almeno in parte la necessità di una autorità centrale e della fiducia reciproca**.

Differenza tra Bitcoin e le altre criptomonete

Assenza totale di una autorità centrale e quindi vera decentralizzazione

Nonostante la difficoltà di cancellare completamente le autorità centrali, viviamo in un mondo talmente opaco e basato sulle autorità, che comunque la Blockchain può essere utile per fare qualche passo avanti, in moltissime attività economiche:

- **Criptomonete, token e NFT**
- **Finanza Decentralizzata (DeFi)**
- **Certificazione di qualità e di filiera**
- **Assicurazioni**
- **Notarizzazione**
- **Logistica e trasporti**
- **Reti energetiche e di telecomunicazioni...**

CrypTO

Crittografia e Teoria dei Numeri

Grazie per l'attenzione

Politecnico di Torino

1859

DISMA