Obiettivi del corso

1. **Comprensione dei principi di base della blockchain**
2. **Approfondimento degli aspetti di sicurezza**
3. **Wallet e identità digitale**
4. **Algoritmi di consenso e protocolli avanzati**
5. **Attacchi e strategie di difesa**
6. **Normative e linee guida (NIST2)**
7. **Applicazioni pratiche e laboratori**

Che cos’ la Blockchain?

Un registro distribuito che memorizza transazioni in maniera:

- sicura
- verificabile
- permanente.

Il registro non è controllato da un'unica entità, ma è condiviso tra più nodi della rete.

Tuttavia, la blockchain non è qualcosa di ‘magico’ capace di risolvere qualsiasi problema di sicurezza o di inefficienza.

Che cos’ la Blockchain?

Esistono:

- questioni aperte
- criticità
- sfide tecnologiche

che richiedono:

- conoscenza
- esperienza
- studio critico.

Richiamo sui Fondamenti della Blockchain: Storia, Evoluzione, Architettura di Base

Storia ed Evoluzione

Breve excursus storico:

1991: Viene proposto un sistema per marcare documenti digitali con timestamp tramite l'uso di hash crittografici, al fine di garantire l'immutabilità nel tempo.
Anni 2000: Alcuni ricercatori iniziano a sperimentare idee di valuta digitale, come B-Money e Bit Gold.
2008: "Bitcoin: A Peer-to-Peer Electronic Cash System". Introduce per la prima volta il termine **blockchain** in un contesto economico e finanziario.
2009: Lancio della rete Bitcoin, considerato l'evento fondativo per la blockchain su larga scala. Viene estratto il primo blocco (il "genesis block").
2013-2015: Nasce Ethereum, che estende il concetto di blockchain introducendo gli smart contract – programmi eseguibili sulla rete decentralizzata. Questo passo permette di abilitare una vasta gamma di applicazioni (dApp, DeFi, NFT, ecc.).
2015-2017: Iniziano i primi progetti permissioned, come Hyperledger Fabric, promosso dalla Linux Foundation.
2017-2021: Crescita esponenziale di progetti DeFi (Finanza Decentralizzata), NFT (Non-Fungible Tokens), e iniziative di standardizzazione in campo internazionale.

Oggi la blockchain non è più soltanto "Bitcoin", ma comprende una costellazione di reti e protocolli differenti, ognuno con le proprie peculiarità in termini di sicurezza, scalabilità e governance.

Architettura di Base

- La bc descritta come una **catena di blocchi** in cui ogni blocco fa riferimento al blocco precedente.
- L'alterazione di un blocco comporterebbe la modifica di tutti i blocchi successivi, rendendo evidente e tracciabile ogni tentativo di manomissione.

Componenti chiave:

1. **Nodi della rete**
2. **Transazioni**
3. **Blocchi**
4. **Algoritmo di consenso**

Nodi, Transazioni, Blocchi: Analisi Tecnica

Nodi

Un **nodo** è qualunque entità che partecipa alla rete blockchain eseguendo il software specifico.

- **Full Node**: Contiene l'intera blockchain e partecipa al processo di validazione delle transazioni e dei blocchi. Può verificare in autonomia la validità delle transazioni senza affidarsi a terze parti.

- **Light Client (o Light Node)**: Scarica solo le intestazioni dei blocchi e un set ridotto di informazioni. Non può validare tutte le transazioni in maniera completa, ma si affida a full node per la conferma dei dati.

Transazioni

La **transazione** è un insieme di dati firmati digitalmente che indicano un cambiamento di stato nel registro.

Ad esempio:

1. Specifica l'**input**.
2. Specifica l'**output**.
3. È firmata con la **chiave privata** del mittente, a garanzia dell'autenticità.

È trasmessa alla rete per essere validata dai nodi.

Blocchi

Un **blocco** è un contenitore di transazioni convalidate e comprende diversi campi nella sua **intestazione** (block header):

- **Hash del blocco precedente**
- **Merkle Root**
- **Timestamp**
- **Nonce**
- **Difficoltà**

Il blocco è quindi una struttura dati che collega la storia passata (hash del blocco precedente) con le transazioni correnti. Questo legame crittografico crea la proprietà di **immutabilità**: cambiare il contenuto di un blocco (per esempio alterare una transazione) modifica il suo hash, rendendo incongruente il riferimento nel blocco successivo. Di conseguenza, per "riscrivere la storia" occorrerebbe rigenerare tutti i blocchi successivi, cosa che risulta praticamente impossibile.

Esempi di Struttura dei Dati e Formule di Hash

Funzioni Hash

Uno dei pilastri crittografici della blockchain è l'utilizzo delle **funzioni hash**, ovvero funzioni che prendono in input un messaggio di lunghezza arbitraria e producono in output un valore (digest) di lunghezza fissa. Proprietà fondamentali di una funzione hash crittografica H:

1. **Resistenza alla preimmagine:** Dato un valore $y = H(x)$, è computazionalmente infeasible trovare x.
2. **Resistenza alle collisioni**: È estremamente difficile trovare due valori diversi $x_1 \neq x_2$ tali che $H(x_1) = H(x_2)$.
3. **Efficienza**: Il calcolo di $H(x)$ deve essere veloce per ogni input x.

Funzioni Hash

Nella maggior parte delle blockchain moderne, si usano funzioni hash come SHA-256 (Bitcoin) o Keccak-256 (Ethereum). Ad esempio, **SHA-256** prende in input un messaggio m e produce un digest di 256 bit (32 byte):

$$\text{digest} = \text{SHA256}(m)$$

L'hash è al cuore del meccanismo di collegamento dei blocchi (ogni blocco contiene l'hash del blocco precedente) e di validazione delle transazioni (attraverso l'albero di Merkle).

Alberi di Merkle

Per raggruppare molte transazioni all'interno di un blocco in un modo efficiente e sicuro, si costruisce un **albero di Merkle** (Merkle Tree). L'idea è di calcolare gli hash di ogni transazione, poi di raggrupparli in coppie e calcolare gli hash delle concatenazioni, e così via, fino ad ottenere un unico hash in cima, detto **Merkle Root**.

Se abbiamo 4 transazioni T_1, T_2, T_3, T_4, si calcola:

$$H_1 = \mathrm{SHA256}(T_1), \quad H_2 = \mathrm{SHA256}(T_2), \quad H_3 = \mathrm{SHA256}(T_3), \quad H_4 = \mathrm{SHA256}(T_4)$$

Poi si calcolano gli hash dei blocchi concatenati a due a due:

$$H_{12} = \mathrm{SHA256}(H_1 \| H_2), \quad H_{34} = \mathrm{SHA256}(H_3 \| H_4)$$

Infine:

$$\mathrm{MerkleRoot} = \mathrm{SHA256}(H_{12} \| H_{34})$$

Questo processo costruisce una struttura ad albero che semplifica la verifica di singole transazioni senza dover scaricare l'intero blocco (verifica SPV).

Dimostrazione di Immutabilità dei Blocchi

Il concetto di "immutabilità" viene spesso spiegato in maniera intuitiva: "se cambi qualcosa, l'hash non corrisponde più e si rompe la catena". Formalmente, possiamo rappresentare un blocco B_i come un insieme di transazioni $\{T_1, T_2, \ldots, T_n\}$ e un header contenente:

$$H(B_i) = \mathrm{SHA256}(\mathrm{MerkleRoot}(\{T_j\}) \| \mathrm{nonce} \| \mathrm{timestamp} \| \mathrm{prevHash} \| \ldots)$$

Dove $\mathrm{prevHash} = H(B_{i-1})$. Se alteriamo T_k in B_i, allora cambia la Merkle Root, il che cambia $H(B_i)$. Di conseguenza, $H(B_{i+1})$ (che include $H(B_i)$ come campo) diventa invalido e si propaga in avanti, rendendo necessaria la ricalcolazione di tutti i blocchi successivi. Nel contesto di un sistema distribuito e con un meccanismo di consenso che premia i blocchi "onesti", riscrivere interamente la catena in modo coordinato è computazionalmente (e spesso economicamente) non conveniente se la rete è sufficientemente grande e distribuita.

Concetti di Decentralizzazione e Distribuzione

1. **Nessuna autorità centrale**: Ogni nodo può verificare da solo le transazioni e i blocchi, senza dover fidarsi di un intermediario.
2. **Rete peer-to-peer (P2P)**: I nodi si connettono tra di loro in maniera paritaria, scambiandosi informazioni sui nuovi blocchi e sulle nuove transazioni.
3. **Algoritmo di consenso**: Un protocollo matematico e computazionale per determinare in modo condiviso quale blocco sia il prossimo a essere aggiunto alla catena.

Tuttavia, la decentralizzazione è spesso un concetto **relativo**: alcune blockchain sono più distribuite di altre. Ad esempio, le cosiddette blockchain "permissioned" possono avere un numero ristretto di validatori, mentre quelle "permissionless" (come Bitcoin) permettono a chiunque di partecipare al processo di validazione.

Evoluzione dei Paradigmi di Utilizzo: Oltre la Valuta

Sebbene Bitcoin abbia introdotto la blockchain come un sistema di pagamento e di riserva di valore, le potenzialità si sono poi estese a:

- **Smart Contract**: Contratti programmabili che vengono eseguiti automaticamente al verificarsi di determinate condizioni (p.e. su Ethereum).
- **Tokenizzazione**: Rappresentazione di asset fisici e digitali come token su una blockchain.
- **Finanza Decentralizzata (DeFi)**: Prestiti, scambi di token, assicurazioni e altri servizi finanziari gestiti interamente da smart contract.
- **Supply Chain**: Tracciamento di prodotti lungo la filiera, garantendone l'origine e l'autenticità.
- **Identità Digitale**: Creazione di identità verificabili e non falsificabili, con il controllo delle proprie credenziali da parte dell'utente.
- **Notarizzazione**: Registrazione di documenti (o hash di documenti) su una blockchain per garantire la data certa e l'inalterabilità.

Vantaggi e Limiti della Blockchain

Vantaggi

1. **Immutabilità**: Le transazioni registrate non possono essere modificate senza che ciò risulti evidente.
2. **Trasparenza**: In molte blockchain pubbliche, chiunque può verificare l'intera storia delle transazioni.
3. **Sicurezza crittografica**: La struttura a blocchi, il chaining tramite hash e l'utilizzo di chiavi private/pubbliche forniscono un alto livello di sicurezza.
4. **Non intermediazione**: Riduce o elimina la necessità di intermediari (banche, autorità centrali, ecc.).
5. **Affidabilità e resilienza**: L'assenza di un singolo punto di controllo riduce il rischio di collasso del sistema.

Limiti

1. **Scalabilità**: Molte blockchain pubbliche faticano a gestire grandi volumi di transazioni in tempi rapidi.
2. **Consumo energetico (PoW)**: Meccanismi come il Proof of Work richiedono notevoli risorse computazionali e energetiche.
3. **Costi di transazione**: Soprattutto nei momenti di congestione di rete, le fee possono aumentare considerevolmente.
4. **Privacy**: La trasparenza, se da un lato è un vantaggio, dall'altro può esporre le transazioni e le identità a potenziali analisi di terze parti (chain analysis).
5. **Regolamentazione incerta**: In molti Paesi, le norme su criptovalute e blockchain sono ancora in fase di evoluzione.

Sintesi e Connessioni con le Prossime Lezioni

- **Capito come si è evoluta la blockchain storicamente**, dai primi studi sulla crittografia e sui timestamping di documenti, fino a Bitcoin, Ethereum e altre piattaforme.
- **Compreso l'architettura di base** e il funzionamento di blocchi, transazioni e nodi, evidenziando il ruolo fondamentale delle funzioni hash (SHA-256, Keccak, ecc.) e della struttura a catena crittograficamente vincolata.
- **Visto i principali vantaggi** (immutabilità, sicurezza, decentralizzazione) e i **limiti intrinseci** (scalabilità, costi, consumi energetici, privacy parziale).

Nelle lezioni successive, ci concentreremo su aspetti più specifici, come:

- **Teoria della blockchain e aspetti critici**: Vedremo i meccanismi di crittografia in modo più dettagliato, comprese firme digitali, key management e differenze tra blockchain pubbliche e permissioned.
- **Sicurezza dell'identità digitale e dei wallet**: Analizzeremo i sistemi di gestione delle chiavi (Public Key Infrastructure), come vengono generate e conservate le chiavi private, e quali sono le vulnerabilità tipiche dei portafogli digitali.
- **Protocolli di sicurezza nella blockchain**: Approfondiremo i principali protocolli di sicurezza adottati dalle blockchain moderne, individuandone i punti di forza e di debolezza.
- **Algoritmi di consenso (Proof-of-Work, Proof-of-Stake, Algorand, ecc.)**: Approfondiremo il funzionamento di tali algoritmi e confronteremo le rispettive proprietà.
- **Attacchi sulla blockchain**: Esamineremo attacchi famosi (51% attack, Sybil, eclipse, ecc.) e vedremo come difendersi a livello di rete e di protocollo.
- **Hyperledger Fabric e NIST**: Tratteremo un esempio di blockchain permissioned come Hyperledger Fabric, analizzandone l'architettura, i modelli di consenso e la sicurezza. Successivamente, vedremo come le linee guida NIST possono essere applicate a livello di recovery dei wallet e dei dati.