Protocolli di Privacy e Advanced Cryptography nelle Blockchain

Introduzione

Nel corso degli ultimi decenni, la **ricerca crittografica** ha sviluppato strumenti sempre più sofisticati per combinare integrità, autenticazione e riservatezza. Molti di questi strumenti – come le **prove a conoscenza zero (Zero-Knowledge Proof, ZKP)**, le firme ad anello (ring signatures), la crittografia omomorfica e le soluzioni di **secure multiparty computation (MPC)** – sono oggi impiegati nelle blockchain per garantire scenari che, altrimenti, sarebbero preclusi.

- **ZK-SNARK** e affini hanno permesso la nascita di blockchain con transazioni completamente anonime (Zcash) o di protocolli di “privacy layer” (Aztec, Tornado Cash su Ethereum).

- **Ring signatures** e “Confidential Transactions” hanno caratterizzato progetti come Monero, Grin/MimbleWimble.

- **MPC** consente la condivisione di informazioni tra più parti senza che nessuna di esse debba rivelare i propri dati in chiaro.

Prove a Conoscenza Zero

Una **prova a conoscenza zero** è un protocollo che permette a un soggetto (Prover) di dimostrare a un altro soggetto (Verifier) di **conoscere** o possedere una certa informazione (ad esempio, la validità di una transazione, o la soluzione di un puzzle) **senza rivelare** l'informazione stessa. L'idea nasce negli anni '80, formalizzata come "zero-knowledge interactive proofs", in cui un Prover e un Verifier scambiano messaggi interattivi.

- **Completezza**: Se l'affermazione è vera e il Prover è onesto, il Verifier deve essere convinto con alta probabilità.
- **Solidità**: Se l'affermazione è falsa, il Prover non può ingannare il Verifier con alta probabilità.
- **Zero-Knowledge**: Il Verifier non apprende **alcuna informazione** aggiuntiva oltre alla veridicità dell'affermazione.

ZK-SNARK e ZK-STARK

La nascita delle **ZK-SNARK** (Succinct Non-interactive Argument of Knowledge) ha reso le prove zero-knowledge “non interattive” e di dimensione compatta (“succinct”). Esse consentono a un utente di generare una prova “corta” che chiunque può verificare off-line con un overhead minimo.

1. **ZK-SNARK**
    - Richiede spesso un “**trusted setup**” iniziale, in cui si generano parametri segreti (toxic waste) che, se trapelati, comprometterebbero il sistema.
    - Esempio d’uso: **Zcash** adotta ZK-SNARK per mascherare importi e indirizzi delle transazioni.
2. **ZK-STARK (Scalable Transparent ARguments of Knowledge)**
    - Elimina il bisogno di un trusted setup, a vantaggio di una trasparenza maggiore.
    - La dimensione delle prove è più grande rispetto a SNARK, ma la tendenza è a ridurre i costi computazionali.
    - Esempi: Progetti come StarkWare su Ethereum (StarkNet), aiming a soluzioni di rollup ZK.

Impieghi Pratici

- **Privacy finanziaria**: L’utente può dimostrare di avere abbastanza saldo senza rivelare l’importo effettivo. Oppure, in una “shielded transaction”, si nascondono mittente, destinatario e valore.

- **Verifica di integrità**: Un’azienda può dimostrare di aver rispettato certi parametri (es. emissioni di CO2) senza svelare i dati interni.

- **Layer 2**: Le ZK-SNARK consentono soluzioni di rollup (zkRollup) in cui centinaia di transazioni off-chain sono verificate on-chain con una singola prova. Ciò incrementa la scalabilità.

Limiti e Sfide

- **Trusted Setup**: Necessità di una cerimonia iniziale, con il rischio che se qualcuno conosce i parametri segreti possa falsificare prove. Alcuni progetti fanno cerimonie pubbliche con decine o centinaia di partecipanti.

- **Performance**: Generare prove ZK può essere costoso. Non è sempre applicabile a contratti molto complessi, se serve latenza bassa.

- **Verifica**: Pur essendo efficiente (verifica in tempo polinomiale “piccolo”), per l’uso di massa, è ancora un “collo di bottiglia” che richiede ottimizzazioni hardware (GPU) o miglioramenti di implementazione (ASIC).

Ring Signatures: Monero e Oltre

Le **Ring Signatures** permettono di firmare un messaggio a nome di un gruppo di possibili firmatari (ring), senza rivelare quale membro effettivo abbia apposto la firma. In ambito blockchain, questo si traduce in transazioni con input “mischiati”:

1. **Monero**: Ogni input di una transazione è combinato con input “decoy” presi da transazioni precedenti, generando un ring. L’osservatore esterno non sa quale input stia effettivamente spendendo i fondi.

2. **Confidential Transaction e Range Proof**: Unito a una crittografia additiva (Bulletproof), Monero maschera anche l’importo.

Il meccanismo di ring signature offre **non ripudiabilità** (il gruppo viene “responsabilizzato”), ma **anonimato dell’individuo**. Il resto della rete vede una firma valida ma non sa chi nel ring ha firmato

Stealth Addresses

Progetti come Monero, Verge, e altre chain che puntano alla privacy, usano meccanismi di “stealth address” per evitare che un indirizzo statico identifichi l’utente. L’idea: per ogni transazione, si genera un nuovo indirizzo mascherato. Solo il destinatario può riconoscere i fondi tramite la propria chiave segreta.

MimbleWimble e Grin/Beam

MimbleWimble è un protocollo di privacy e scalabilità con “Confidential Transactions” e “CoinJoin” intrinseco. Le transazioni si fondono in un unico blocco, rendendo difficile capire quali input corrispondano a quali output. Progetti come **Grin** e **Beam** basano la sicurezza su “Pedersen Commitments” e prove a conoscenza zero (Bulletproofs) per dimostrare che la somma dei valori è zero senza svelare gli importi.

SECURE MULTI-PARTY COMPUTATION (MPC)

Definizione e Razionale

La **Secure Multi-Party Computation** è un insieme di protocolli che consentono a più parti di calcolare una funzione su input segreti, **senza** che nessuna parte debba rivelare i propri input. L'obiettivo è la collaborazione "senza fiducia":

- **Esempio**: Un gruppo di banche vuole calcolare un tasso medio su dati sensibili (portafogli, default rate) senza condividere i dati grezzi.

- **In blockchain**: L'MPC può gestire la generazione e la custodia di chiavi private (un "wallet collegiale" in cui la chiave è "spezzettata" tra più nodi)

Esempi d’Uso in Blockchain

1. **DAO con Voti Segreti**: I partecipanti inviano la propria preferenza cifrata, un protocollo MPC calcola il totale (o la maggioranza) senza divulgare il singolo voto.

2. **Wallet Multi-Sig**: Invece di usare lo script nativa multi-sig, si può generare una chiave ECDSA condivisa; per firmare una transazione, servono M partecipanti che eseguono un protocollo MPC.

3. **Randomness Decentralizzata**: La rete crea numeri casuali (es. VRF) in cui un subset di validatori calcola la random seed usando protocolli MPC, riducendo la manipolazione.

Limiti e Considerazioni

- **Overhead** in calcolo e comunicazione.

- **Complex code** → possibilità di bug.

- **Rischio di collusione**: Se troppi partecipanti si coalizzano, possono deviare i calcoli. Necessaria una soglia di onestà (es. se < 1/3 malevoli).

Crittografia Omomorfica

La **Fully Homomorphic Encryption (FHE)** consente di eseguire calcoli su dati cifrati e ottenere un risultato cifrato, il quale, una volta decifrato, coincide con quello che si otterrebbe calcolando in chiaro. In teoria, questo è un santo graal per la privacy on-chain, perché i nodi potrebbero validare transazioni o calcoli “cifrati” senza mai vedere i dati.

- **Limiti attuali**:
  - Prestazioni molto basse.
  - Chiavi e ciphertext di dimensioni ampie.

- **Ricerca**: Alcuni layer 2 e progetti accademici (TFHE, CKKS, BGV, ecc.) stanno migliorando i parametri. Potrebbe rivelarsi strategico in futuro, soprattutto per contratti enterprise con dati sensibili.

Differential Privacy e Private Data Aggregation

In alcuni contesti, si vuole elaborare statistiche su dati su blockchain, ma proteggendo la privacy individuale. La **Differential Privacy** (DP) prevede l’aggiunta di rumore matematico ai risultati aggregati, in modo che non si possano dedurre i singoli record. Non è un protocollo “nativo” da blockchain, ma può essere integrato in dApp di analisi, a condizione che gli smart contract gestiscano i meccanismi di aggiunta di rumore e i modelli di sicurezza (es. se un attaccante ottiene troppi query, potrebbe erodere la DP).