Sicurezza dell’Identità Digitale e dei Wallet

Concetti chiave contesto blockchain

Ogni interazione in una rete decentralizzata richiede la creazione e la gestione di **chiavi crittografiche**

Identità digitale → insieme di **credenziali crittografiche**

Wallet → archiviare (o generare) e proteggere la **chiave privata** dell'utente

La **Public Key Infrastructure**, con i suoi concetti di **certificati digitali**, **autorità di certificazione (CA)** e **gestione delle chiavi**, costituisce lo scheletro normativo e tecnologico con cui molte organizzazioni garantiscono l'autenticità e l'affidabilità delle chiavi pubbliche.

Concetti chiave contesto blockchain

In questa sezione approfondiremo:

1. **Public Key Infrastructure**: cos'è, come funziona e perché è cruciale nella gestione dell'identità digitale.
2. **Progettazione e sicurezza dei wallet**: tipologie di wallet, gestione delle chiavi private, meccanismi di difesa.
3. **Aspetti specifici di sicurezza dell'identità digitale**: best practice, minacce comuni, scenari di utilizzo e possibili attacchi

Public Key Infrastructure

Concetti di Base

La **Public Key Infrastructure (PKI)** fornisce e gestisce:

1. **Generazione di chiavi**: (pk,sk)
2. **Emissione di certificati**: associando una pk a un’identità tramite un **certificato digitale** firmato dalla CA.
3. **Distribuzione** e **revoca**
4. **Convalida**: come un'entità *A* verifica l’autenticità del certificato di un’entità *B*.

Autorità di Certificazione (CA)

Ente fidato che rilascia i certificati digitali.

- **Root CA**
- **Intermediate CA**

Se utente si connette a un sito con HTTPS, il browser verifica la firma del certificato del sito usando una catena di fiducia che risale fino a una CA radice preinstallata.

In Fabric, i peer verificano le firme dei certificati di altri peer o client controllando la catena di fiducia interna.

Certificati Digitali

Un **certificato digitale** collega una chiave pubblica a un'entità includendo informazioni quali:

- Nome dell'entità.
- Chiave pubblica associata.
- Periodo di validità.
- Firma digitale della CA che garantisce l'autenticità dei dati contenuti.

Il formato più diffuso è lo standard **X.509**.

Chiunque disponga della chiave pubblica della CA può verificare la validità del certificato controllandone la firma e le date di scadenza.

Gestione delle Chiavi (Key Management)

La PKI richiede procedure ben definite di:

1. **Generazione**
2. **Protezione**
3. **Rotazione**
4. **Revoca**

PKI e Blockchain Permissionless

- **Namecoin**: sistema DNS decentralizzato, registrando nomi di dominio e certificati su blockchain.
- **ENS (Ethereum Name Service)**: consente di registrare nomi ".eth" e associarli a indirizzi Ethereum, semplificando l'esperienza utente e riducendo i rischi di digitare a mano un address lungo.

PKI e Blockchain Permissioned

In **Fabric**, la PKI ha un ruolo cruciale:

- Ogni organizzazione ha una **CA** che rilascia certificati ai propri peer e client.
- Il ledger contiene la definizione degli **MSP (Membership Service Provider)**, ovvero regole su come validare i certificati e stabilire quali CA sono attendibili.
- Le politiche di endorsement possono richiedere firme di determinati peer (identificati dai loro certificati) per approvare una transazione.

Progettazione e Sicurezza dei Wallet

Tipologie di Wallet

1. **Hardware Wallet (cold wallet)**
2. **Software Wallet (hot wallet)**
3. **Paper Wallet**
4. **Custodial Wallet**

Meccanismi di Protezione

Il cuore della sicurezza di un wallet risiede nella protezione della chiave privata. Alcune tecniche:

- **Passphrase + Cifratura**
- **Seed mnemonic**
- **Multi-Factor Authentication**
- **Multisig**

Esempio generazione di un Wallet Ethereum

```
from eth_account import Account #key/addr per eth
import secrets

def generate_eth_account():
    priv_key = "0x" + secrets.token_hex(32)
    acct = Account.from_key(priv_key)
    return priv_key, acct.address

if __name__ == "__main__":
    generate_eth_account()
```

Esempio generazione di un Wallet Fabric

```
fabric-ca-server start -b admin:adminpw

fabric-ca-client register --id.name alice --id.secret alicepw
--id.type client --url http://localhost:7054 --tls.certfiles
ca-cert.pem --mspdir msp

fabric-ca-client enroll -u http://alice:alicepw@localhost:7054
--tls.certfiles ca-cert.pem --mspdir aliceMsp
```

Aspetti Specifici di Sicurezza dell’Identità Digitale

Phishing e Social Engineering

Gran parte degli attacchi rivolti ai wallet sfruttano la **debolezza umana**:

- Email di phishing o siti clonati che inducono l’utente a inserire la propria passphrase o il seed.
- Attacchi di ingegneria sociale (telefonate, chat, finti supporti tecnici) che spingono l’utente a rivelare informazioni riservate.

Best practice:

- Mai fornire la chiave privata o la seed phrase a terzi.
- Verificare sempre l’URL del sito o dell’app.

Malware e Keylogger

Nel caso di un **hot wallet** un malware può:

- Rubare i file che contengono la chiave privata.
- Registrare la passphrase digitata dall'utente (keylogger).
- Sostituire l'indirizzo di destinazione durante la transazione (clipboard hijacking).

Difese:

- Usare un antivirus aggiornato.
- Mantenere aggiornati il sistema operativo e le app.
- Valutare un hardware wallet per transazioni di valore significativo.

Attacchi a Exchange e Custodial Wallet

La sicurezza dipende in gran parte dall'exchange stesso. Nel corso degli anni, molte piattaforme sono state hackerate (es. Mt.Gox), causando perdite enormi agli utenti. L'exchange custodisce le chiavi degli utenti in hot wallet e in cold wallet; se il suo sistema risulta compromesso, i fondi possono essere rubati.

Recupero e Backup

Un aspetto spesso trascurato è il **recovery** di un wallet. Se l'utente perde la chiave privata (ad esempio perché si rompe l'hard disk o si smarrisce il dispositivo), i fondi non sono più accessibili. Per mitigare tale rischio, occorre:

- Eseguire backup periodici del file keystore (per i software wallet).
- Stampare o annotare su carta il seed di ripristino.
- Conservare il backup/seed in un luogo sicuro, separato dal resto delle proprie apparecchiature.

Aspetti di Sicurezza dell’Identità Digitale: Oltre la Blockchain

La blockchain non risolve magicamente tutti i problemi di identità digitale. In molti casi, l'identità sul ledger è ridotta a un "possesso di una chiave privata". Se l'obiettivo è creare un sistema di **identità legale** (ad esempio, un passaporto o una patente su blockchain), occorre un processo di "onboarding" e di validazione iniziale che coinvolga enti governativi o soggetti certificatori. Solo così si può garantire che un determinato indirizzo corrisponda realmente a una persona fisica o giuridica, evitandone l'anonimato completo.

Vari progetti puntano a definire standard di **Self-Sovereign Identity (SSI)**, in cui l'utente detiene le proprie credenziali, e la blockchain funge da strato di verifica e revoca. Tuttavia, l'adozione su larga scala è ancora limitata e la normazione a livello globale incompleta.

Casi di Studio: Identity Management su Blockchain

3.11.1 KYC (Know Your Customer) Decentralizzato

Molte istituzioni finanziarie devono svolgere procedure di KYC. Invece di ripetere la verifica dei documenti per ogni nuovo servizio, si potrebbe creare un sistema su blockchain permissioned in cui:

- Un'entità certificante (ad es. una banca) validi l'identità di un utente e rilasci un attributo firmato digitalmente su un ledger.
- Altre banche leggano e riconoscano quell'attributo, riducendo i tempi e i costi di KYC.
- La privacy venga tutelata, mostrando solo la prova dell'avvenuta certificazione, senza rivelare documenti sensibili.

3.11.2 eIDAS e SPID

Nell'Unione Europea, i regolamenti eIDAS cercano di fornire un quadro normativo per l'identità digitale transfrontaliera. In Italia, SPID (Sistema Pubblico di Identità Digitale) è un esempio di identità digitale centralizzata. Alcune iniziative sperimentali valutano l'uso di blockchain per rendere più flessibili e "self-sovereign" le credenziali SPID, ma resta da vedere se la struttura permissionless si adatti alle normative. Più plausibile un modello permissioned, con organismi governativi come autorità.

Verso il Futuro: DID e SSI

La tendenza alla **Self-Sovereign Identity (SSI)** cerca di ridurre il ruolo di autorità centralizzate, consentendo all'utente di controllare le proprie credenziali in modo autonomo. I **Decentralized Identifier (DID)** sono uno standard del W3C che definisce:

- Come rappresentare un identificativo univoco in forma di URI (es. `did:example:1234...`).
- Come legare questo DID a un insieme di chiavi e attributi.
- Come le **Verifiable Credentials** possano essere rilasciate e verificate, senza che un singolo punto di controllo possa revocare o censurare l'identità.

Molti di questi progetti si appoggiano a blockchain (spesso permissionless) per la pubblicazione dei DID o dei record di revoca, creando un registro immutabile. Tuttavia, la parte di "verifica dei documenti reali" rimane ancorata al mondo offline e alle autorità governative. L'obiettivo a lungo termine è costruire un **ecosistema** dove l'utente possa muoversi tra servizi diversi presentando credenziali "verificabili crittograficamente", ma senza rivelare informazioni non necessarie (ad es. esibire solo la prova di essere maggiorenne, senza mostrare data di nascita completa).