Chiavi e Indirizzi

Davide3011

January 2025

1 Introduzione

Bitcoin è una criptovaluta decentralizzata progettata per consentire transazioni sicure, anonime e senza intermediari. La sicurezza di Bitcoin si basa su un sistema crittografico asimmetrico che utilizza coppie di chiavi: una chiave privata e una chiave pubblica. Questo sistema garantisce che solo il proprietario legittimo di una chiave privata possa autorizzare le transazioni associate.

Le chiavi private e pubbliche sono alla base della creazione degli indirizzi Bitcoin e della firma digitale delle transazioni. Questi meccanismi svolgono un ruolo essenziale per:

- Garantire la proprietà e il controllo esclusivo dei fondi.
- Verificare l'autenticità delle transazioni senza rivelare informazioni sensibili.
- Proteggere la rete da accessi non autorizzati e da tentativi di contraffazione.

La crittografia asimmetrica utilizzata da Bitcoin si basa sull'algoritmo della curva ellittica `secp256k1`, che offre un'elevata sicurezza combinata con un'efficienza computazionale. Attraverso un processo di derivazione matematica, la chiave privata genera la chiave pubblica, la quale può essere condivisa pubblicamente senza compromettere la sicurezza del sistema.

Grazie a questo approccio, Bitcoin non solo consente trasferimenti di valore in un ambiente decentralizzato, ma garantisce anche un elevato grado di anonimato e resilienza contro attacchi esterni.

2 Chiavi Private e Pubbliche

Le chiavi private e pubbliche costituiscono i pilastri fondamentali del sistema Bitcoin, garantendo sicurezza, autenticità e anonimato nelle transazioni. Ogni chiave è parte di una coppia crittografica generata utilizzando un algoritmo di curva ellittica (`secp256k1`). Qui di seguito vengono esplorate le caratteristiche di ciascuna chiave.

2.1 Chiave Privata

Una chiave privata è un numero casuale di 256 bit generato crittograficamente. Rappresenta il fulcro della sicurezza del sistema Bitcoin, poiché permette di firmare le transazioni, dimostrando la proprietà dei fondi associati. È fondamentale che la chiave privata venga mantenuta segreta, poiché chiunque la possieda può accedere ai fondi.

- **Formato:** La chiave privata può essere rappresentata in diversi modi:
  - In formato esadecimale, costituito da 64 caratteri (32 byte).
  - Nel formato **WIF** (Wallet Import Format), che utilizza una codifica Base58Check per rendere la chiave più leggibile e rilevare errori di battitura.
- **Generazione:** Le chiavi private devono essere create utilizzando generatori casuali sicuri per evitare collisioni o prevedibilità.

- **Esempio:**
  - Esadecimale: `e9873d79c6d87dc0fb6a5778633389...`
  - WIF (mainnet): `L5o8rUMg4P8V5j....`
- **Sicurezza:** Bitcoin utilizza uno spazio chiavi enorme (2^{256} combinazioni possibili), rendendo estremamente improbabile trovare o calcolare una chiave privata già in uso.

2.2 Chiave Pubblica

La chiave pubblica viene derivata matematicamente dalla chiave privata utilizzando la curva ellittica `secp256k1`. Questo processo è unidirezionale: mentre è semplice ottenere la chiave pubblica dalla chiave privata, l'operazione inversa è computazionalmente impraticabile.

- **Tipi di chiavi pubbliche:**
  - **Non compressa:** 65 byte (1 byte di prefisso, 32 byte per ciascuna coordinata x e y).
  - **Compressa:** 33 byte (1 byte di prefisso e 32 byte per la coordinata x).
- **Funzione:** La chiave pubblica serve per:
  - Generare gli indirizzi Bitcoin (P2PK, P2PKH, ecc.).
  - Verificare le firme digitali associate alle transazioni, garantendo che siano state effettuate dal titolare della chiave privata corrispondente.
- **Derivazione:** L'algoritmo di derivazione è basato sull'operazione di moltiplicazione di un punto sulla curva (`G`, punto generatore) per il valore della chiave privata.
- **Esempio:**
  - Non compressa: `04bfcab1cd4c...`
  - Compressa: `02bfcab1cd4c...`

2.3 Relazione tra Chiave Privata e Pubblica

La chiave pubblica può essere condivisa liberamente senza compromettere la sicurezza, mentre la chiave privata deve essere mantenuta segreta. La sicurezza del sistema si basa su:

- L'impossibilità pratica di calcolare la chiave privata partendo dalla chiave pubblica (problema del logaritmo discreto sulla curva ellittica).
- L'unicità e l'indipendenza delle chiavi generate casualmente.

3 Evoluzione degli Indirizzi Bitcoin

3.1 P2PK (Pay-to-PubKey)

Introdotti nel 2009, gli indirizzi Pay-to-PubKey (P2PK) rappresentano il formato più semplice e originale degli indirizzi Bitcoin. In questo schema, i fondi sono direttamente associati alla chiave pubblica e le transazioni richiedono una firma creata dalla corrispondente chiave privata per essere spese.

- **Funzionamento:**
  - La chiave pubblica viene inclusa nella blockchain come parte della transazione.
  - Per spendere i fondi, il proprietario deve fornire una firma valida generata dalla chiave privata corrispondente.

- **Caratteristiche:**
  - Molto semplice da implementare, in quanto non utilizza ulteriori livelli di hashing o script.
  - Gli indirizzi P2PK non hanno un formato visibile come gli indirizzi moderni (ad esempio, P2PKH o P2SH). La chiave pubblica è memorizzata direttamente nella transazione.
- **Limitazioni:**
  - La chiave pubblica viene esposta sulla blockchain una volta utilizzata, rendendola un potenziale bersaglio per attacchi crittografici.
  - Sebbene la crittografia ECC sia attualmente sicura, l'esposizione della chiave pubblica potrebbe diventare un problema in futuro, ad esempio con l'avvento del quantum computing.
  - La mancanza di anonimato, poiché la chiave pubblica è visibile e legata alla transazione.
- **Mainnet:**
  - In mainnet, le transazioni P2PK contenevano direttamente la chiave pubblica.
  - Questo approccio è stato utilizzato nelle prime transazioni, incluse quelle create dal blocco genesi (Blocco 0).
- **Testnet:**
  - Lo schema P2PK è stato replicato anche su testnet, seguendo la stessa logica di implementazione utilizzata in mainnet.
- **Esempi Storici:**
  - La transazione coinbase del blocco genesi (Blocco 0) utilizza un indirizzo P2PK. La chiave pubblica del destinatario è memorizzata direttamente nella transazione.
  - Alcune delle prime transazioni Bitcoin (2009-2010) hanno utilizzato questo schema prima che venissero introdotti i formati P2PKH.

Evoluzione: Con l'introduzione degli indirizzi Pay-to-PubKey-Hash (P2PKH), il formato P2PK è stato gradualmente abbandonato. Gli indirizzi P2PKH offrono un livello di sicurezza superiore, proteggendo la chiave pubblica attraverso un processo di hashing prima che venga registrata nella blockchain. Sebbene il formato P2PK non sia più utilizzato, rimane una parte importante della storia di Bitcoin.

3.2 P2PKH (Pay-to-PubKey-Hash)

Introdotti per migliorare la sicurezza e la privacy delle transazioni Bitcoin, gli indirizzi Pay-to-PubKey-Hash (P2PKH) rappresentano un'evoluzione rispetto agli indirizzi P2PK. In questo schema, invece di utilizzare direttamente la chiave pubblica, viene utilizzato il suo hash. Questo approccio offre una protezione aggiuntiva contro eventuali attacchi crittografici e migliora l'anonimato degli utenti.

- **Funzionamento:**
  - La chiave pubblica viene prima elaborata utilizzando l'algoritmo SHA-256 e successivamente l'algoritmo RIPEMD-160, generando un hash di 160 bit.
  - L'indirizzo Bitcoin è quindi formato combinando questo hash con un prefisso che identifica la rete (mainnet o testnet), e infine codificato in Base58Check.
  - Per spendere i fondi associati a un indirizzo P2PKH, è necessario fornire la chiave pubblica completa e una firma valida generata dalla corrispondente chiave privata.
- **Caratteristiche:**
  - Gli indirizzi P2PKH sono il formato più comunemente usato e supportato in Bitcoin.
  - Offrono un livello di sicurezza superiore rispetto agli indirizzi P2PK grazie alla protezione crittografica aggiuntiva fornita dall'hashing.

  - L'utilizzo dell'hashing garantisce che la chiave pubblica venga rivelata solo quando i fondi vengono spesi, riducendo il rischio di attacchi futuri.

- **Mainnet:**
  - Gli indirizzi P2PKH su mainnet iniziano con il prefisso `1`.
  - Esempio: `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`.

- **Testnet:**
  - Gli indirizzi P2PKH su testnet iniziano con i prefissi `m` o `n`.
  - Esempio: `mipcBbFg9gMiCh81Kj8tqqdgoZub1ZJRfn`.

- **Vantaggi:**
  - Miglioramento significativo della sicurezza, poiché l'hash è meno vulnerabile a tentativi di crittoanalisi rispetto alla chiave pubblica grezza.
  - Riduzione della dimensione dei dati registrati nella blockchain, migliorando l'efficienza del sistema.
  - Compatibilità con una vasta gamma di software wallet e applicazioni.

- **Limitazioni:**
  - Sebbene più sicuri dei P2PK, gli indirizzi P2PKH non supportano funzionalità avanzate come gli script complessi o i contratti multi-firma (questi sono stati successivamente introdotti con P2SH).
  - La rivelazione della chiave pubblica al momento della spesa può ancora rappresentare un rischio se la sicurezza crittografica dell'algoritmo ECC venisse compromessa in futuro.

- **Esempi Storici:**
  - Gli indirizzi P2PKH sono stati adottati poco dopo l'inizio del network Bitcoin per affrontare le limitazioni degli indirizzi P2PK.
  - Una delle prime transazioni pubbliche, inviata da Satoshi Nakamoto a Hal Finney, ha utilizzato un indirizzo P2PKH.

Evoluzione: Gli indirizzi P2PKH sono rimasti il formato standard per molti anni, grazie alla loro semplicità e sicurezza. Sebbene oggi siano stati in parte sostituiti da formati più avanzati come P2SH e SegWit, rimangono largamente utilizzati sia su mainnet che su testnet, dimostrando la loro robustezza e versatilità.

3.3 WIF (Wallet Import Format)

Le chiavi private possono essere rappresentate in WIF, un formato Base58Check:

- Prefisso: `0x80` per mainnet, `0xEF` per testnet.
- Esempio: `5JxW7Gg...` (mainnet), `93HjVaP...` (testnet).

3.4 P2SH (Pay-to-Script-Hash)

Gli indirizzi P2SH supportano script complessi come multi-firma.

- **Mainnet**: Iniziano con `3`, ad esempio `3J98t1Wp...`.
- **Testnet**: Iniziano con `2`, ad esempio `2NBFNJT...`.

3.5 BIP 32: Portafogli HD (Hierarchical Deterministic)

Permettono di derivare una gerarchia di chiavi figlie da una chiave master.

- **Backup**: Basta salvare la chiave master o la seedphrase associata.
- Compatibile sia con mainnet che testnet.

3.6 BIP 39: Seedphrase

Standardizza l'uso delle seedphrase, sequenze di 12 o 24 parole generate da un'entropia iniziale.

- Migliora il backup e la portabilità dei wallet.
- Supportato sia su mainnet che testnet.

3.7 SegWit e Bech32

Segregated Witness separa le firme dalle transazioni, riducendone le dimensioni.

- **Mainnet**: Indirizzi `bc1q...` per P2WPKH.
- **Testnet**: Indirizzi `tb1q...` per P2WPKH.

3.8 Taproot e Schnorr (BIP 341)

Introducono privacy e contratti intelligenti avanzati.

- **Mainnet**: Indirizzi `bc1p...`.
- **Testnet**: Indirizzi `tb1p...`.

3.9 Lightning Network

Il Lightning Network utilizza indirizzi BOLT 11 per transazioni off-chain veloci e a basso costo.

4 Tabella Riassuntiva

Tipo	**Formato Mainnet**	**Formato Testnet**	**Note**
P2PK	Chiave pubblica	Chiave pubblica	Esposizione della chiave pubblica
P2PKH	`1...`	`m` o `n...`	Hash della chiave pubblica
WIF	`5...`	`9...`	Chiave privata codificata
P2SH	`3...`	`2...`	Supporto a script complessi
BIP 32	Gerarchico	Gerarchico	Backup semplificato
BIP 39	Seedphrase	Seedphrase	12-24 parole
SegWit	`bc1q...`	`tb1q...`	Miglioramento della scalabilità
Taproot	`bc1p...`	`tb1p...`	Privacy avanzata
Lightning	BOLT 11	BOLT 11	Pagamenti off-chain