UTXO: struttura, privacy e dinamiche delle transazioni Bitcoin

Cos’è un UTXO

Un **UTXO** (*Unspent Transaction Output*) è un **output di transazione Bitcoin non ancora speso**.
Ogni UTXO rappresenta una **porzione precisa di Bitcoin** controllata da una **chiave privata**.

Quando viene speso:

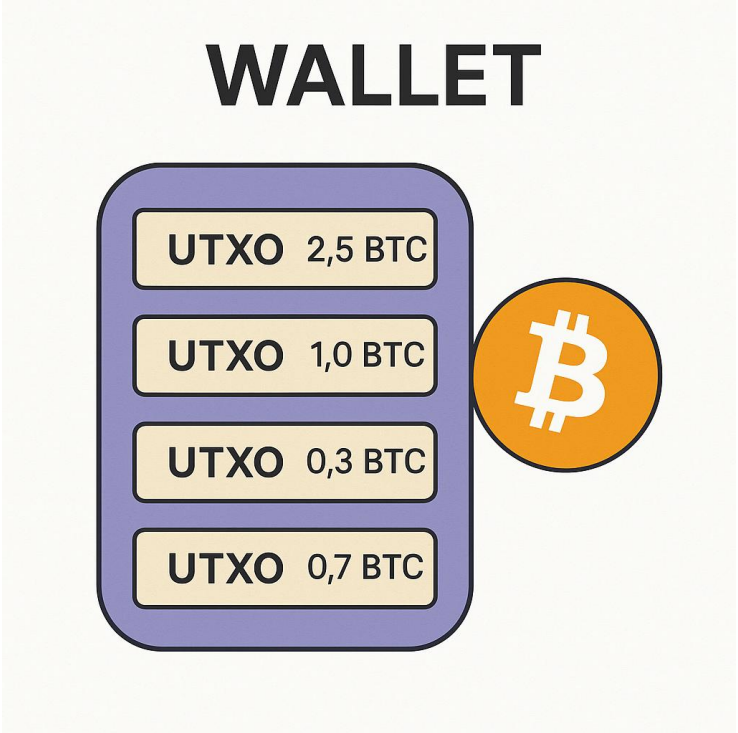
• L’UTXO **viene distrutto** come input.
• La transazione **crea nuovi UTXO**, che diventano disponibili per future spese.

In pratica, il modello UTXO funziona come un insieme di “banconote digitali”:
ogni spesa consuma alcune e ne genera di nuove.

Wallet e UTXO

- Il **wallet non contiene Bitcoin**, ma **UTXO**.
- Ogni **UTXO** è come una **banconota digitale** controllata da una chiave privata.
- Il **saldo** del wallet = somma di tutti gli **UTXO non spesi**.
- Il wallet decide **quali UTXO usare** per ogni transazione (*coin selection*).
- Se l'importo è minore dell'UTXO usato → crea un **UTXO di resto**.

Il wallet è il gestore intelligente delle tue "banconote digitali" Bitcoin.



Modello UTXO vs. Account Based

Account-based → un libro contabile con saldi aggiornati

UTXO → un portafoglio con banconote digitali separate.

Account-based vs UTXO Model

Account-based

.

- Ogni indirizzo ha **uno stato con saldo aggiornato**.
- Le transazioni **modificano direttamente i saldi** degli account.
- Stato globale condiviso e lineare.

Pro:
- Semplicità concettuale.
- Aggiornamenti rapidi.

Contro:
- **Privacy ridotta** (tutto è tracciabile per account).
- **Minor parallelismo** (dipendenze tra transazioni).

UTXO (Bitcoin)

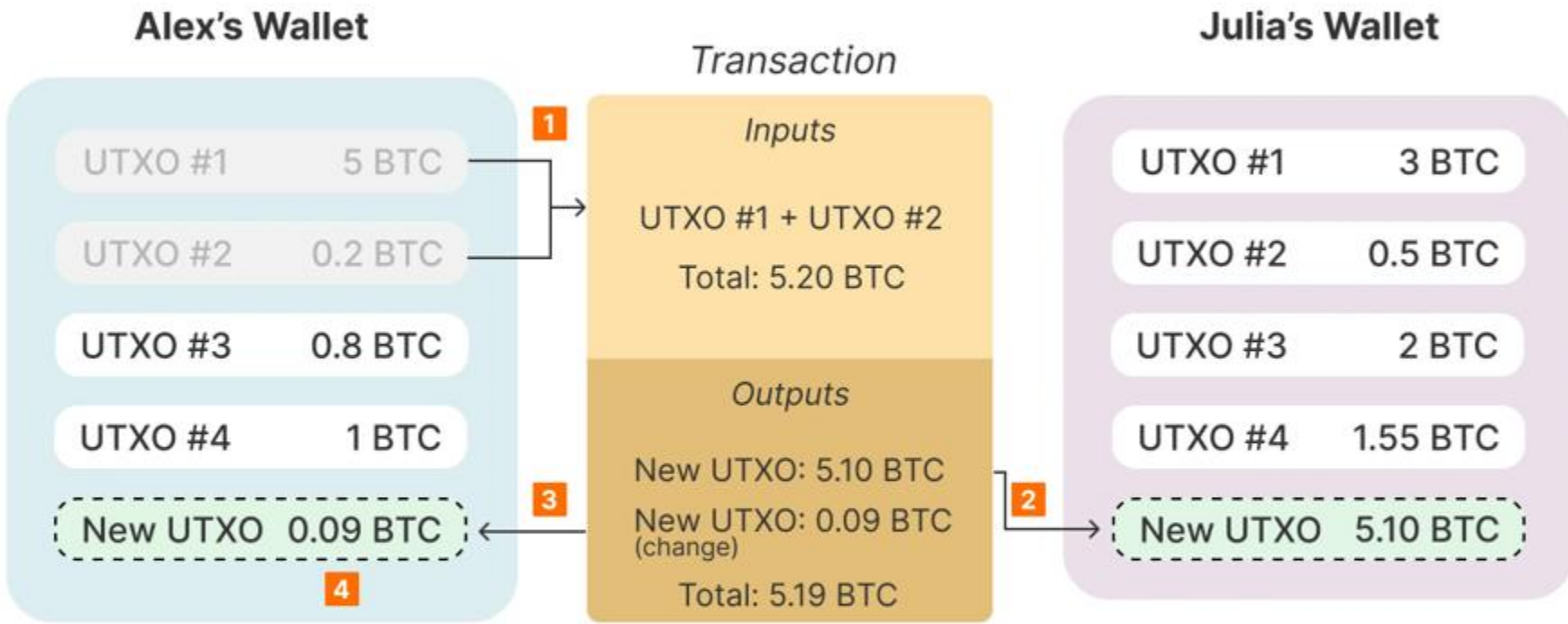
- Ogni transazione **consuma UTXO** e **crea nuovi output non spesi**.
- Nessun saldo unico: il "saldo" è la **somma degli UTXO controllati**.
- Ogni UTXO è **indipendente e verificabile**.

Pro:
- **Maggiore privacy potenziale** (molti indirizzi, output separati).
- **Scalabilità e parallelismo** nelle verifiche.
- Fondamento di **Lightning Network** e **CoinJoin**.

Contro:
- Gestione più complessa del portafoglio.

Bitcoin UTXO Model

Alex wants to send 5.10 BTC to Julia



1. Alex's wallet selects the best UTXOs to get to the transaction amount or greater. Since UTXOs are indivisible, the wallet will select two UTXOs.
2. The wallet creates a new UTXO for Julia in the amount of the transaction.
3. The wallet creates a new UTXO for Alex, which is the "change."
4. The transaction fee is not paid to the miner as an output of the transaction. It is inferred by the difference between the value of the inputs and the value of the outputs.

Fee, dimensioni, consolidamento e dust limit

Fee (commissioni)

- Le fee si calcolano in **satoshi per byte**, non in percentuale sul valore inviato.
- Dipendono dalla **dimensione della transazione**, non dall'importo in BTC.
- Le transazioni SegWit e Taproot sono più **efficienti** (meno byte = meno fee).

Dimensione della transazione

- Ogni **input** e **output** aggiunge peso in byte.
- Più UTXO vengono spesi → **transazione più grande e costosa**.
- Il wallet sceglie automaticamente gli input ottimali (*coin selection*).

Consolidamento

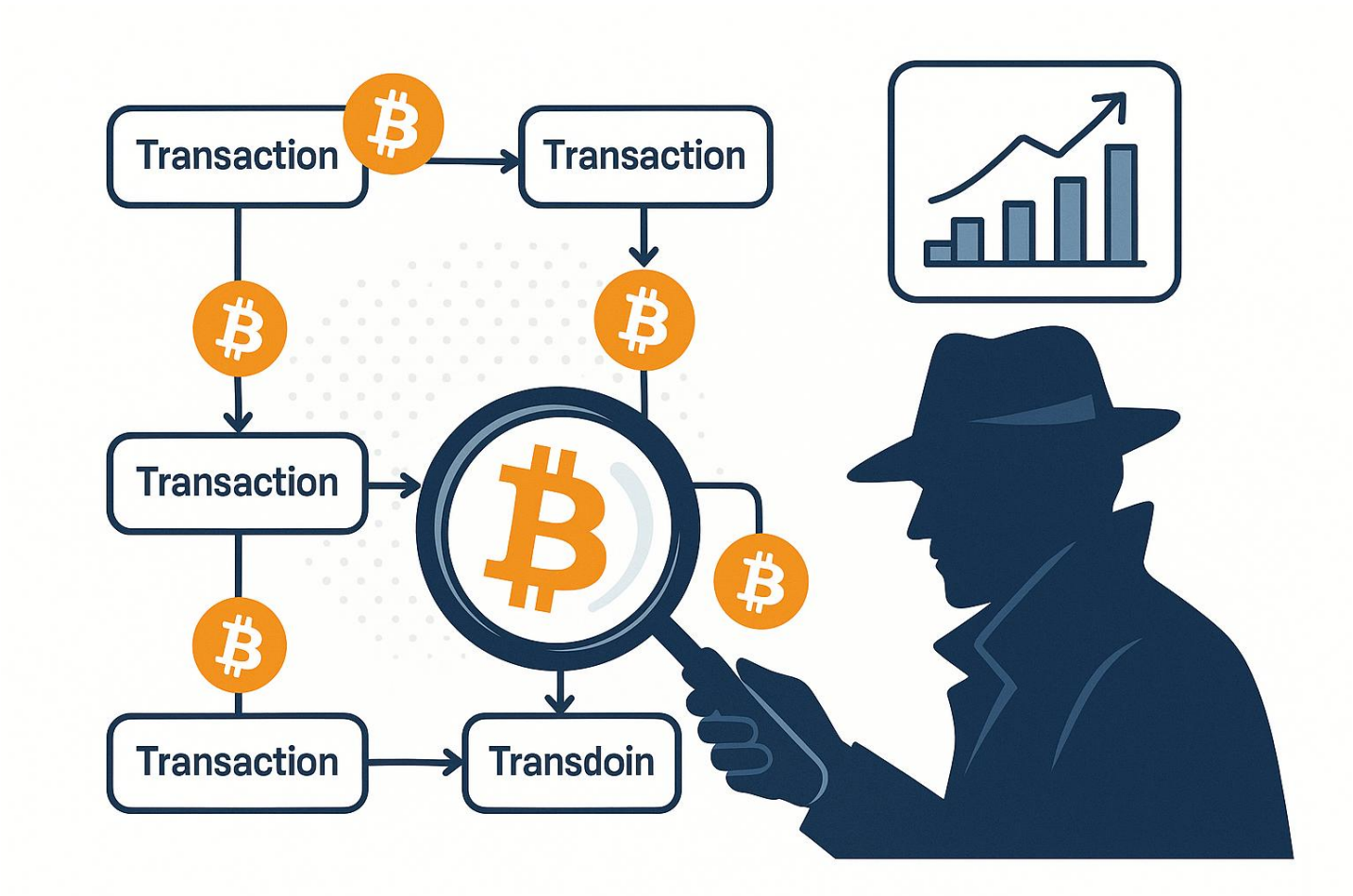
- Operazione che **unisce più UTXO piccoli** in uno più grande.
- Conviene farlo **quando le fee sono basse**.
- Riduce il numero di input futuri → **transazioni più leggere e rapide**.

Dust limit

- È la **soglia minima** sotto cui un UTXO non conviene più spendere (costo > valore).
- Serve a evitare la creazione di "polvere" inutile nella blockchain.

Analisi della blockchain

- Tutte le transazioni Bitcoin sono **pubbliche e tracciabili**.
- Analisti e aziende usano tecniche di **clustering** per collegare UTXO e identità.
- Anche piccoli errori di gestione possono **rivelare connessioni** tra indirizzi.



Buone pratiche di privacy

Etichettatura UTXO

- Gli UTXO possono essere associati a **fonti note** (exchange, servizi, wallet).
- Usare sempre **portafogli separati** per scopi diversi (risparmio, spesa, donazioni).
- Evitare di mescolare fondi “pubblici” e “privati”.

Coin Control

- Funzione che permette di **scegliere manualmente** quali UTXO spendere.
- Utile per mantenere la **separazione tra identità on-chain**.
- Aiuta anche a gestire consolidamenti e fee in modo mirato.

Riuso degli indirizzi

- Evitare di **ricevere più volte sullo stesso indirizzo**.
- Ogni pagamento dovrebbe usare **un indirizzo nuovo**.
- Il riuso facilita la **ricostruzione delle relazioni** tra transazioni.

Tecniche per rompere le euristiche di chain analysis

CoinJoin

- Transazioni collaborative che **mescolano input di più utenti**.
- Rompono il collegamento diretto tra input e output.
- Implementazioni comuni: **Whirlpool**, **JoinMarket**, **Wasabi**.
- Migliore efficacia con uso ricorrente e post-mix gestito correttamente.

Swap tra layer e protocolli

- **On-chain ↔ Lightning Network ↔ Liquid**
- Ogni passaggio genera **interruzioni di tracciabilità** (“break in heuristics”).
- Gli swap atomici (*atomic swaps*) consentono di spostare fondi **senza terze parti fidate**.
- Gli scambi LN o Liquid appaiono come semplici output on-chain, rendendo difficile seguirne l’origine.

PayJoin (P2EP)

- Transazione cooperativa tra mittente e destinatario.
- Entrambi forniscono input, **confondendo l’analisi del flusso di denaro**.
- Appare come una normale transazione ma rompe le euristiche comuni.

Altre strategie anti-analisi

- **Evitare consolidamenti automatici** di UTXO.
- Usare **wallet diversi** per categorie di fondi.
- **Variare orari e importi** per non creare pattern ripetitivi.


?
Q
&
A
!