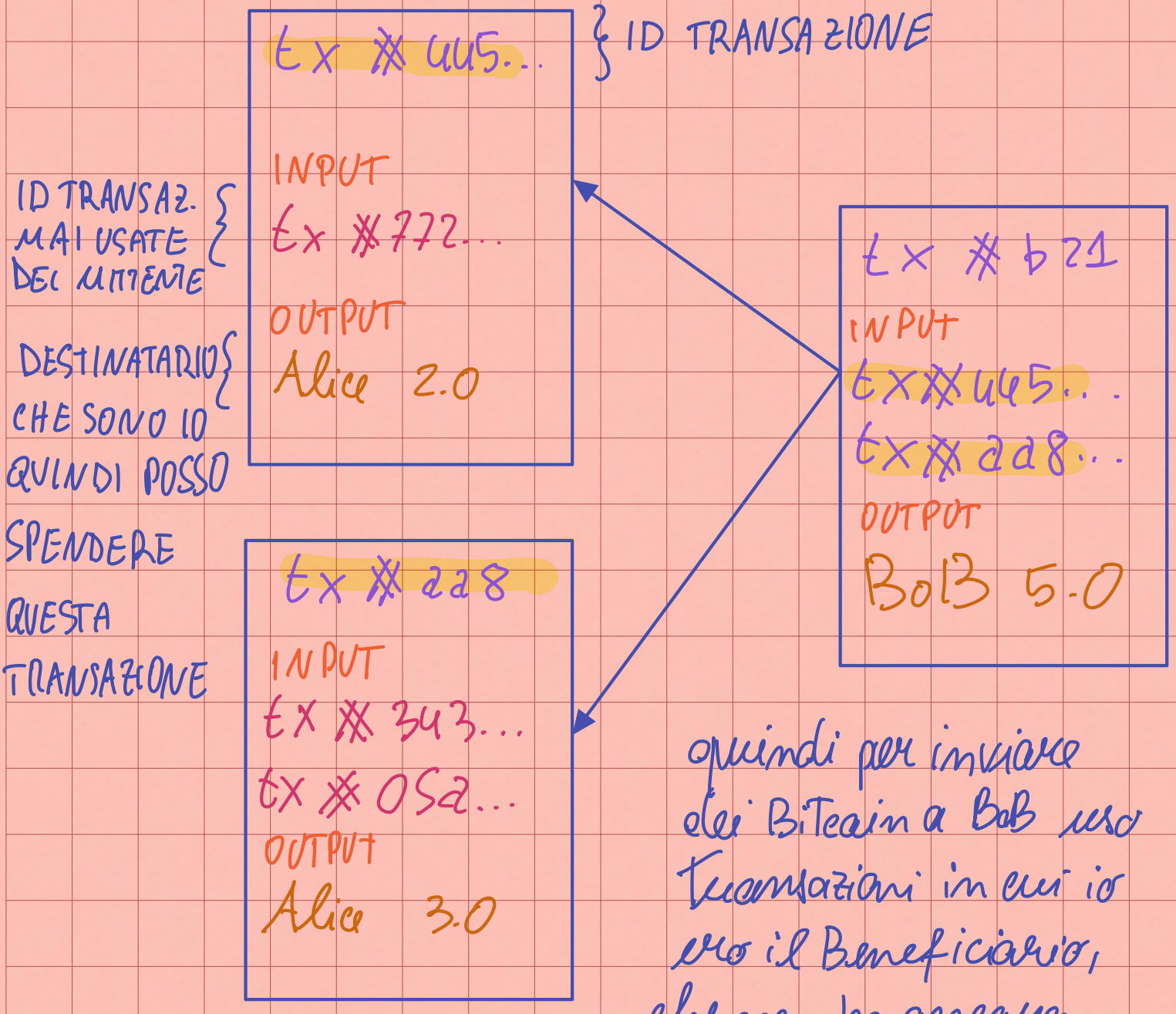
UTXO
Unspent transaction output

Le transazioni in bitcoin sono codificate secondo il modello UTXO. Esso ci consente di:

Rendere impossibile recuperare il saldo di un utente: per ricostruire il saldo di un utente si dovrebbe andare a trovare tutte quelle transazioni che hanno l'indirizzo di quel determinato utente come output. Dato però che ogni utente può generare quanti indirizzi vuole questo rende impossibile tenere traccia del patrimonio complessivo.

Nota: Un indirizzo Bitcoin è composto da 26-35 caratteri.

COME FUNZIONA



quindi per inviare dei Bitcoin a Bob uso transazioni in cui io ero il Beneficiario, che non ho ancora usato.

Se voglio ottenere il "resto" dalla transazione, metto anche me stesso (Alice) come output in tx #b21 e scrivo la quantità che voglio mi venga restituita.

Ex #445...

INPUT
Ex #772...

OUTPUT
Alice 2.0

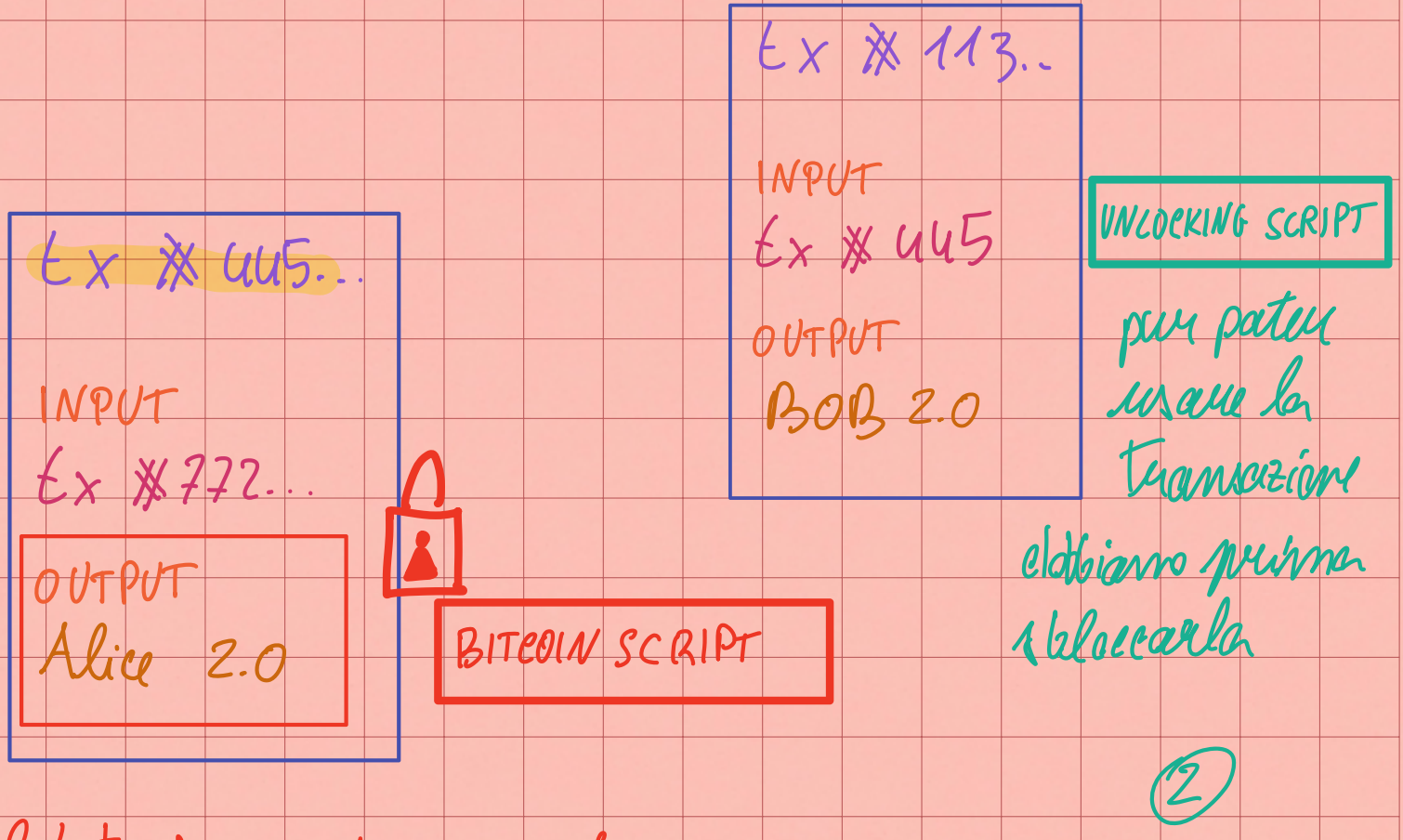
dato che l'identificativo delle Transazioni è pubblico, un modo per non permettere l'utilizzo da utenti malevoli è usare il sistema di scripting di BiTcoin per garantire autenticazione.

SCRIPTING DI BITCOIN: Basato su stack ed elaborato da sinistra a destra. Esso:

- associato ad ogni Transazione
- determina tramite l'esecuzione di un insieme di istruzioni, se possiamo spendere la Transazione oppure no.
- se alla fine dell'esecuzione dello script, in cima allo STACK CI' TRUE, allora possiamo spendere la Transazione.

Uno script bitcoin può contenere solo due tipi di istruzioni:

1. Un dato
2. Un OP CODE. Operazione predeterminata che esegue l'operazione sui valori in cima allo stack e mette il risultato sempre in cima allo stack.



il bitcoin script viene posto sull'output delle transazioni

1