Non-interactive Mimblewimble transactions, revisited

Michele Orrù (UC Berkeley)

Joint work with Georg Fuchsbauer (TU Wien)

ia.cr/2022/265

MimbleWimble

MimbleWimble is the spell that does not let the Blockchain babble out user information.




Core ideas:

- Confidential transactions [Back, Maxwell]
- CoinJoin [Maxwell]
- Transaction cut-through [Maxwell]
- Stealth Addresses [Todd, van Saberhagen]

Our Contribution

1. Strengthen the model of [FOS19]
   - Inflation-resistance
   - Theft-resistance
   - Transaction Binding
   - Transaction Privacy

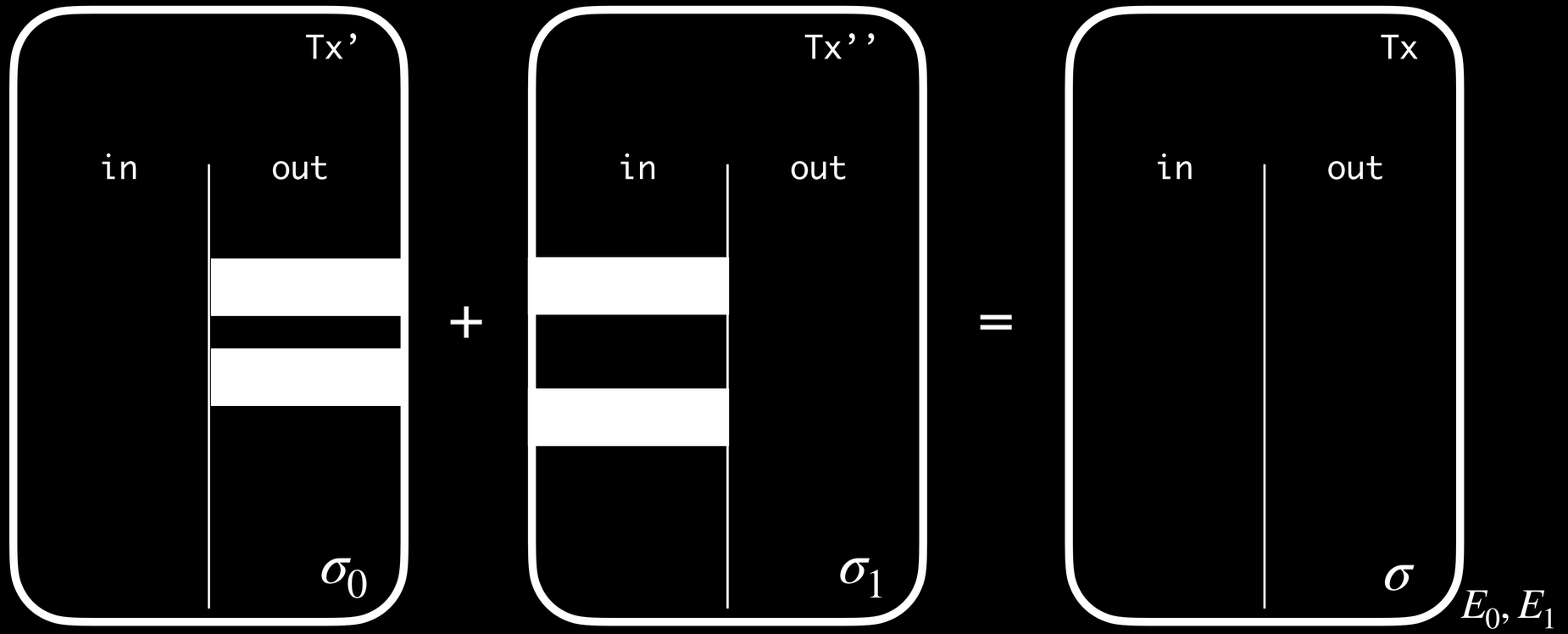
Stronger security!
Stronger anonymity!

2. Provide a non-interactive Aggregate Cash System

Small variants are now in use by and by

Aggregate Transactions

Non-Interactive CoinJoin and Cut-Through

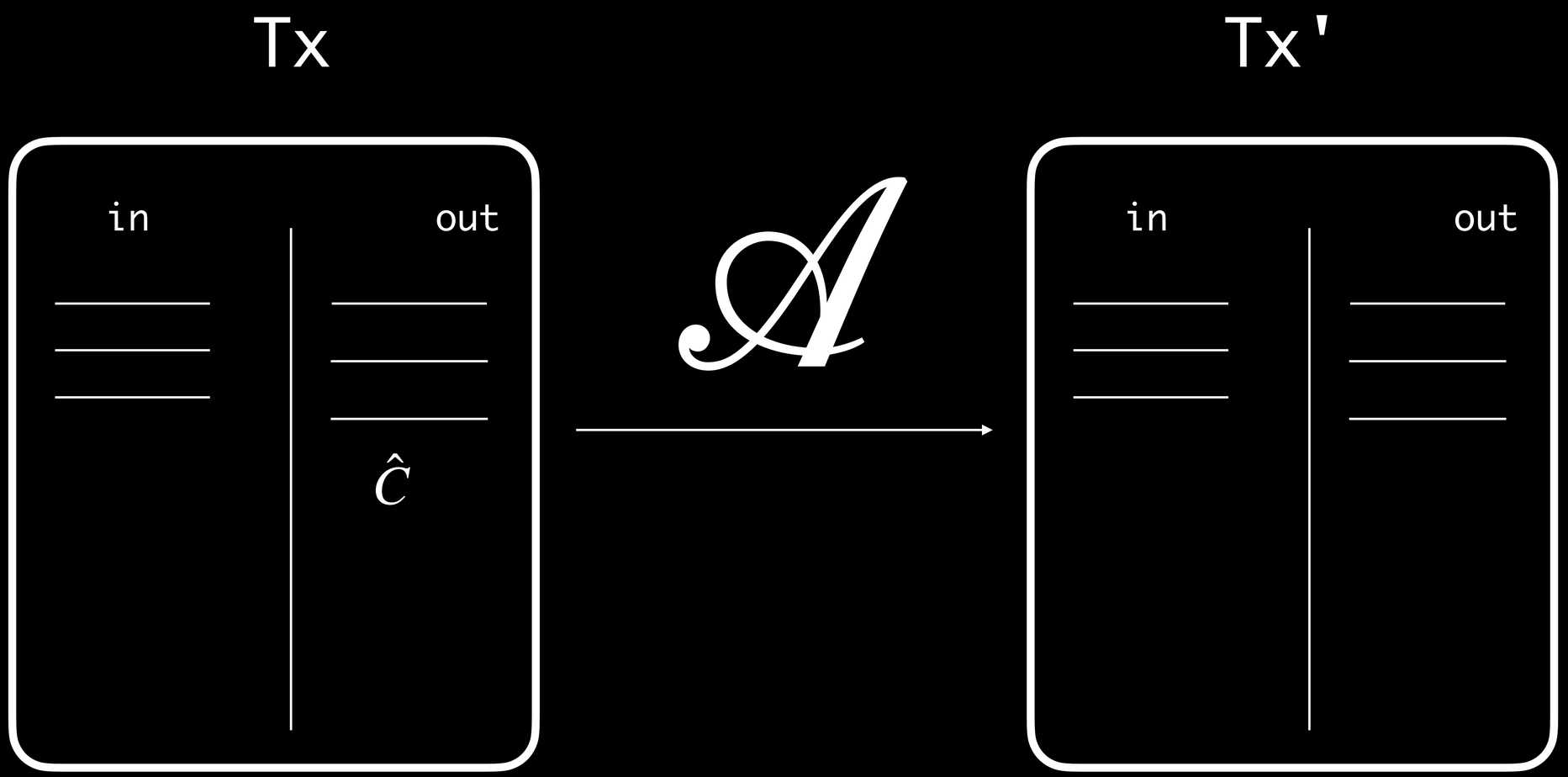


$$E_0 := \sum \text{out}_0 - \sum \text{in}_0$$

$$E_1 := \sum \text{out}_1 - \sum \text{in}_1$$

$$E_0 + E_1 = \sum \text{out} - \sum \text{in}$$

Transaction Binding

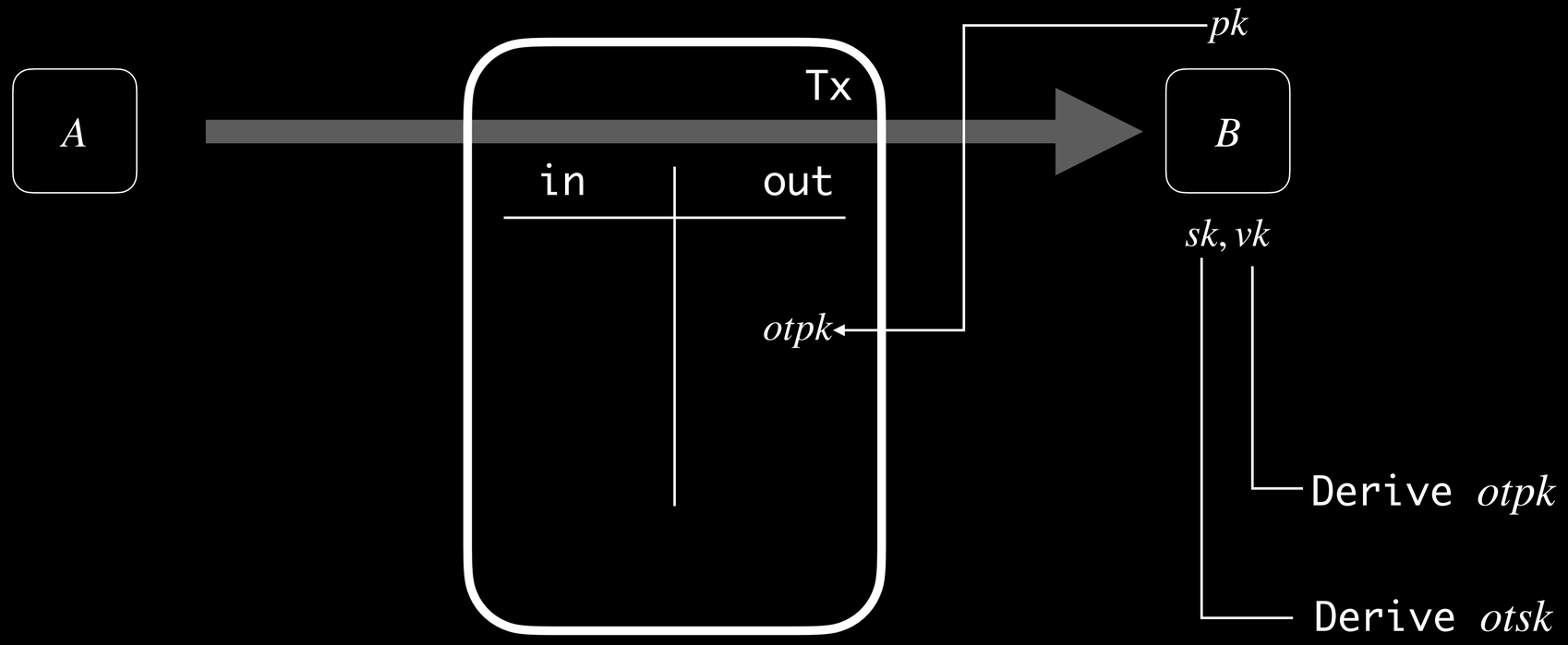


Transaction Privacy

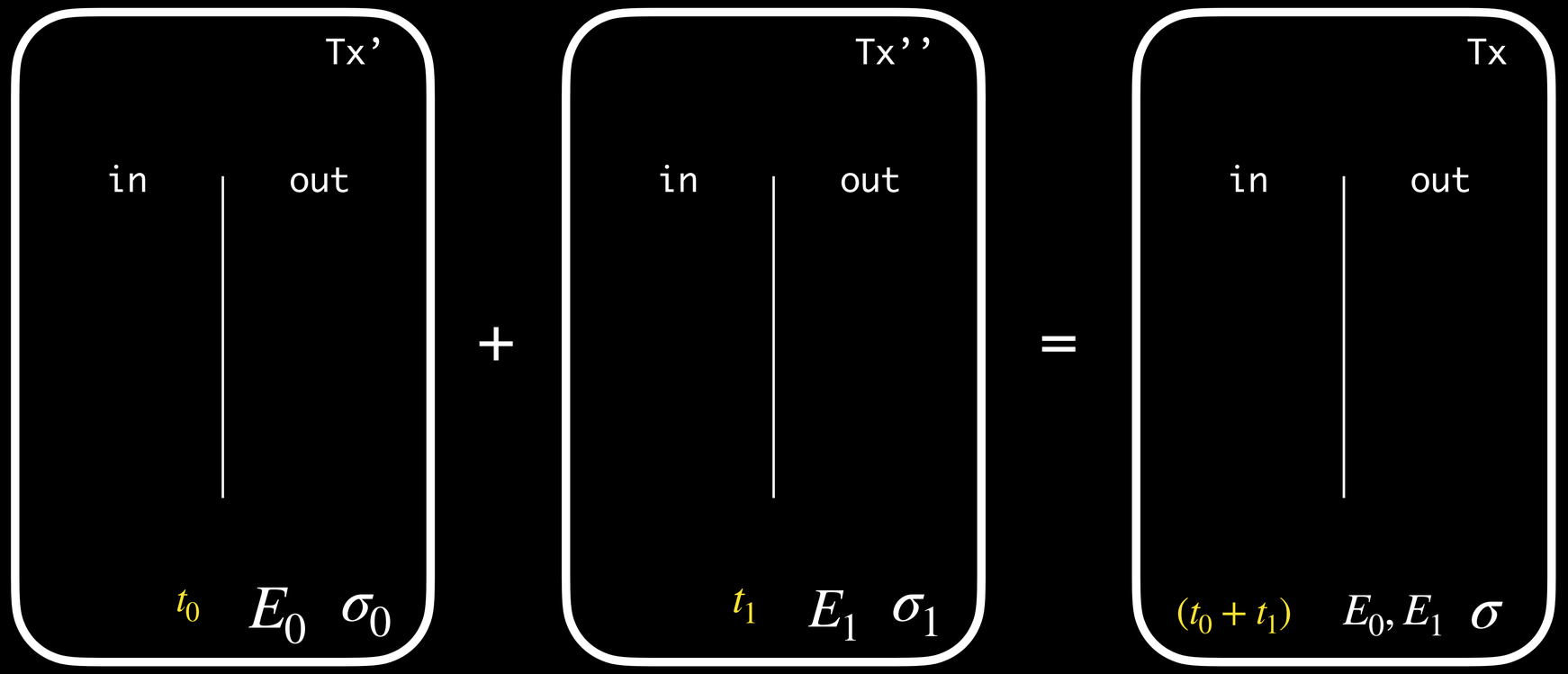
- Transaction amounts are hidden
- Recipients of a transaction are hidden
- It is not possible to de-compose transactions

Stealth Addresses

One-time addresses to mask your public key



Transaction Offsets



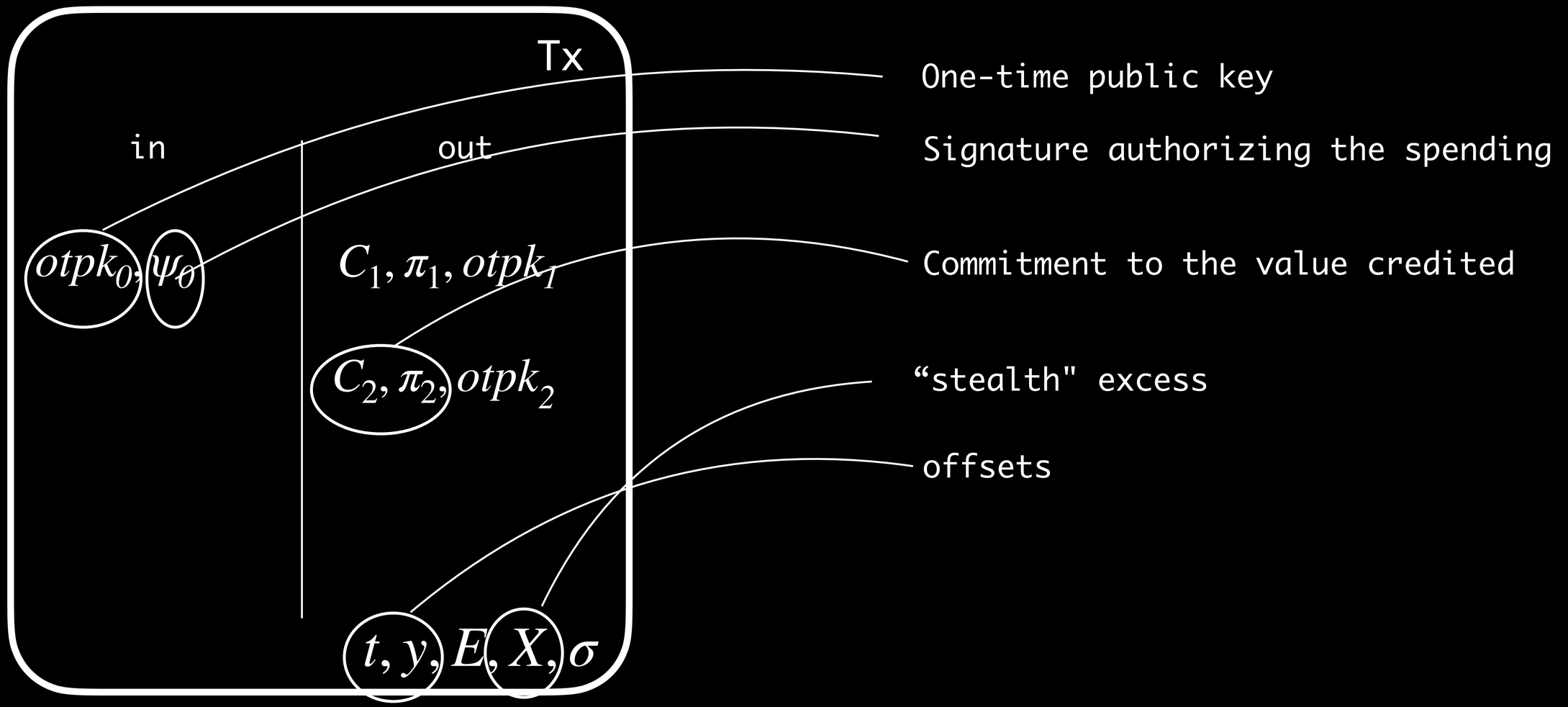
$$E_0 := \sum \text{out}_0 - \sum \text{in}_0 \; + t_0 G$$

$$E_1 := \sum \text{out}_1 - \sum \text{in}_1 \; + t_1 G$$

$$E_0 + E_1 = \sum \text{out} - \sum \text{in} \; + (t_0 + t_1) G$$

Non-Interactive Transactions

Original ideas from Burkett and Yu.



Wrapping up

We strengthen Aggregate Cash Systems [FOS19], and provide an ACS for non-interactive transactions now in use by and by