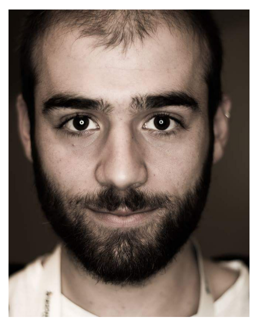
The security of Mimblewimble

Georg Fuchsbauer

joint work with

Michele Orrù



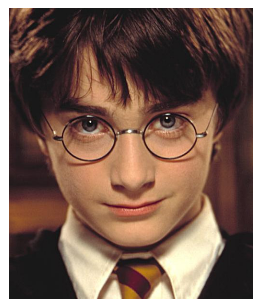
and Yannick Seurin

F, Orrù, Seurin: **Aggregate cash systems: A cryptographic investigation of Mimblewimble.** EUROCRYPT'19

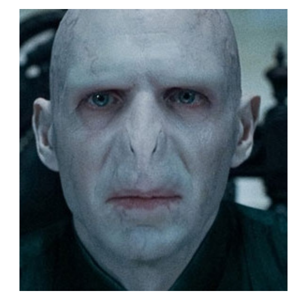
F, Orrù: **Non-interactive Mimblewimble transactions, revisited.** (eprint 2022/265)

What is it?

- **Cryptocurrency scheme**
  - **Privacy** (all amounts hidden; input/output relation blurred)
  - **Scalability** (forget about spent tx's)



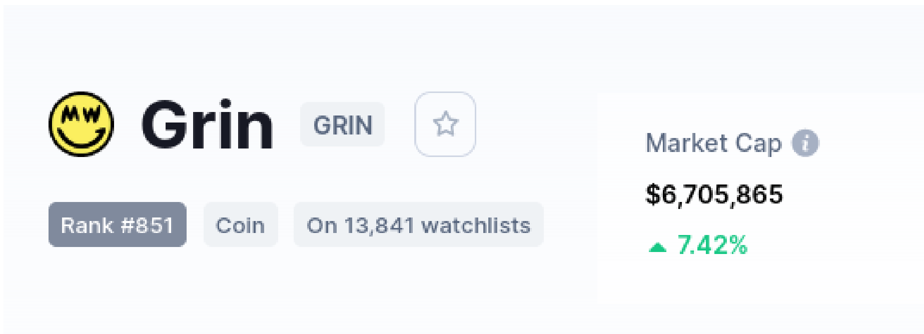
- proposed by
  "Tom Elvis Jedusor"
  in 2016

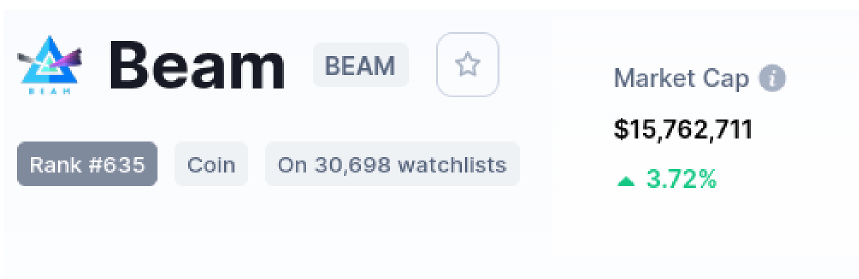


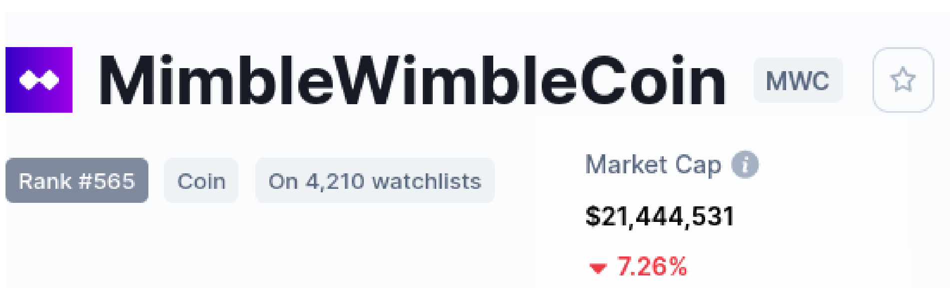
- uses ideas from Gregory Maxwell
- further developed by Andrew Poelstra

Applications

Implemented by several cryptocurrencies (. . . 2021):







Non-interactive TXs

Main **drawback**: transactions are *interactive*

2020: David Burkett, Gary Yu:
Non-interactive transactions

2021: Fixed by Burkett, F, Orrù

Analyzed by F, Orrù

2022: Implemented in

Litecoin

Non-interactive TXs

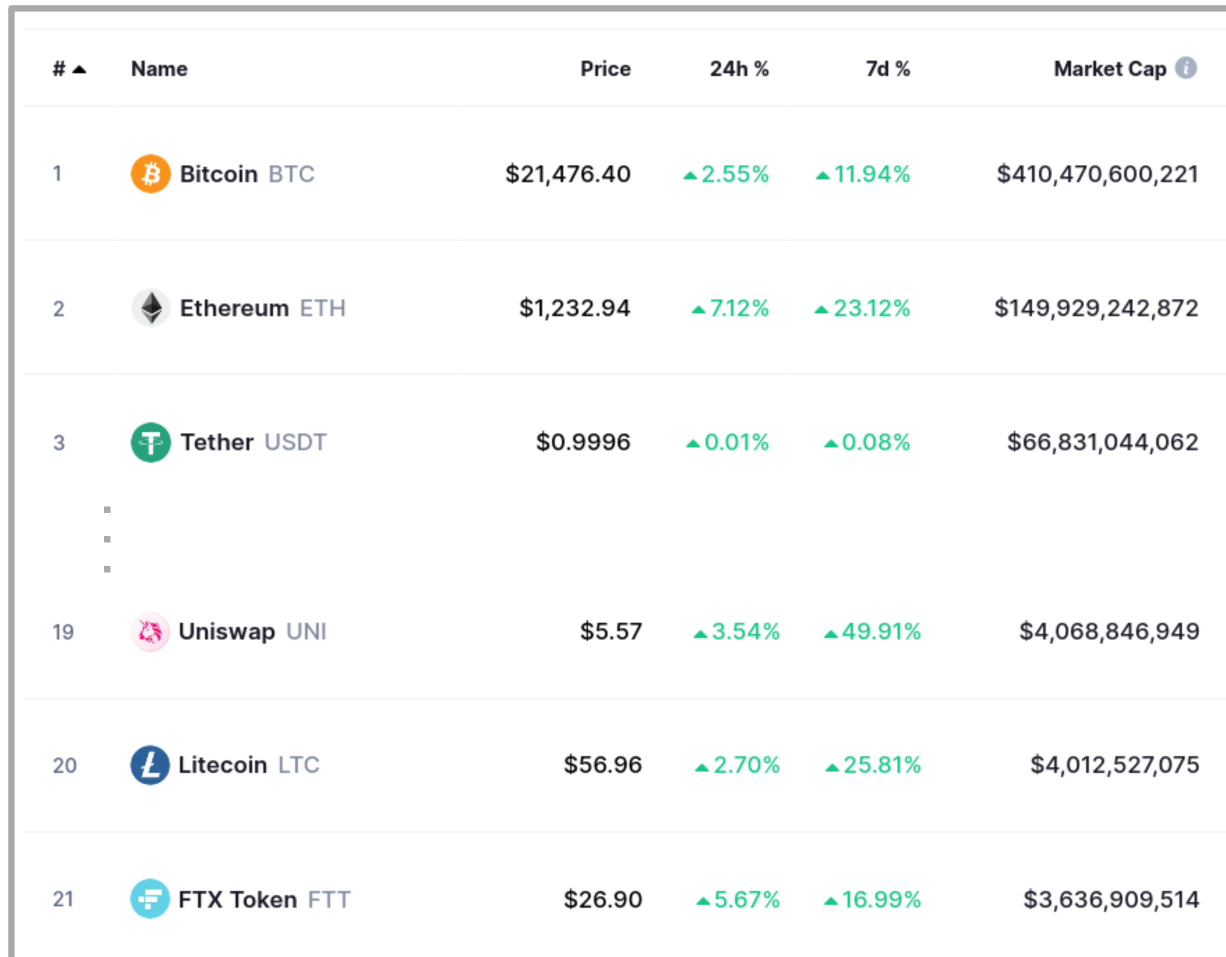
Main **drawback**: transactions are *interactive*

2020: David Burkett, Gary Yu:
Non-interactive

2021: Fixed by Burkett

Analyzed by F, C

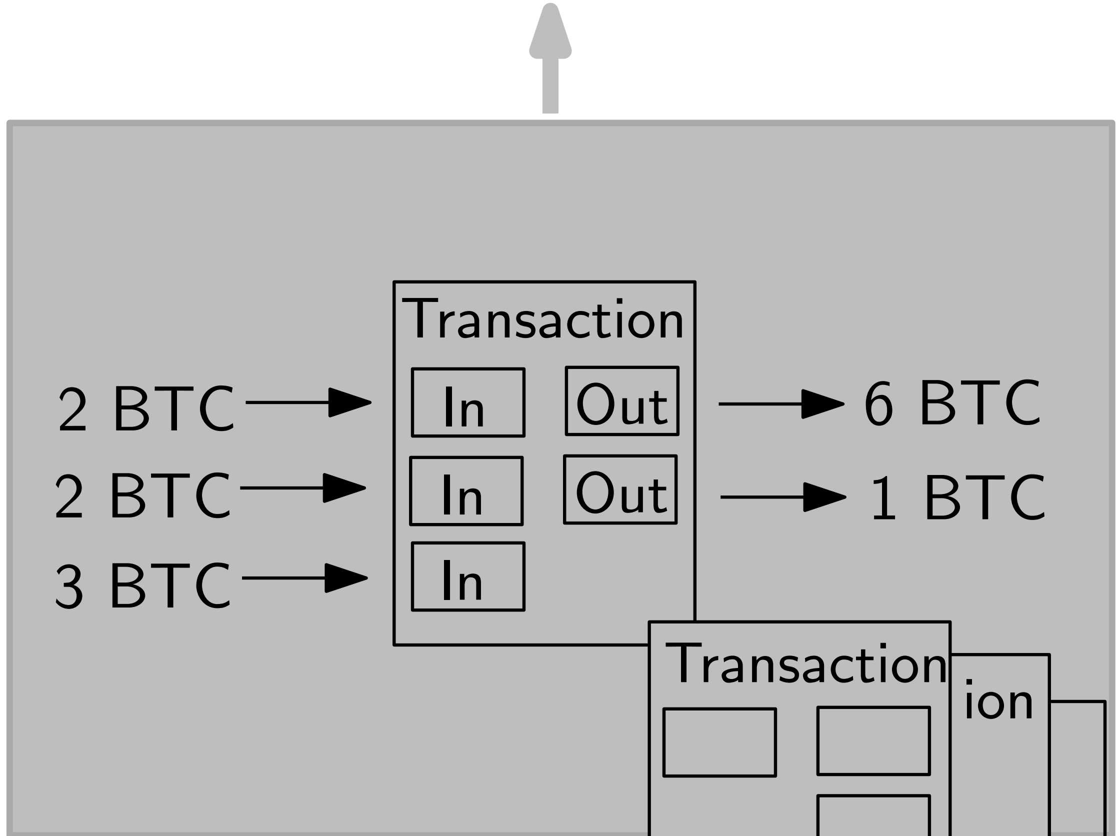
2022: Implemented in
Litecoin



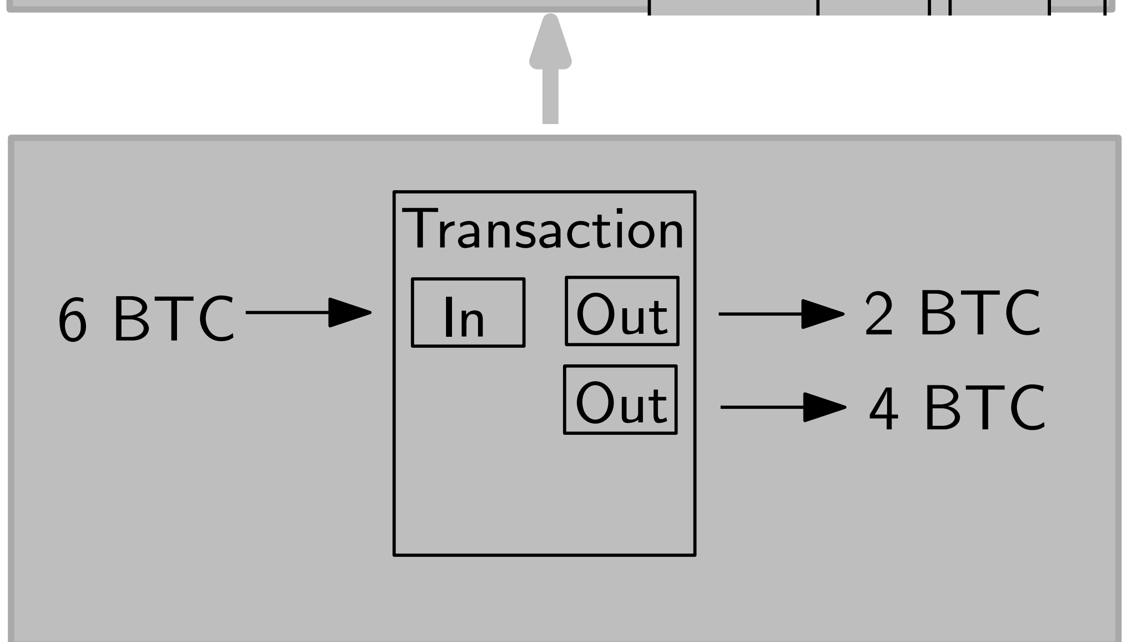
#	Name	Price	24h %	7d %	Market Cap
1	Bitcoin BTC	$21,476.40	2.55%	11.94%	$410,470,600,221
2	Ethereum ETH	$1,232.94	7.12%	23.12%	$149,929,242,872
3	Tether USDT	$0.9996	0.01%	0.08%	$66,831,044,062
⋮					
19	Uniswap UNI	$5.57	3.54%	49.91%	$4,068,846,949
20	Litecoin LTC	$56.96	2.70%	25.81%	$4,012,527,075
21	FTX Token FTT	$26.90	5.67%	16.99%	$3,636,909,514

Bitcoin

- **Transactions**

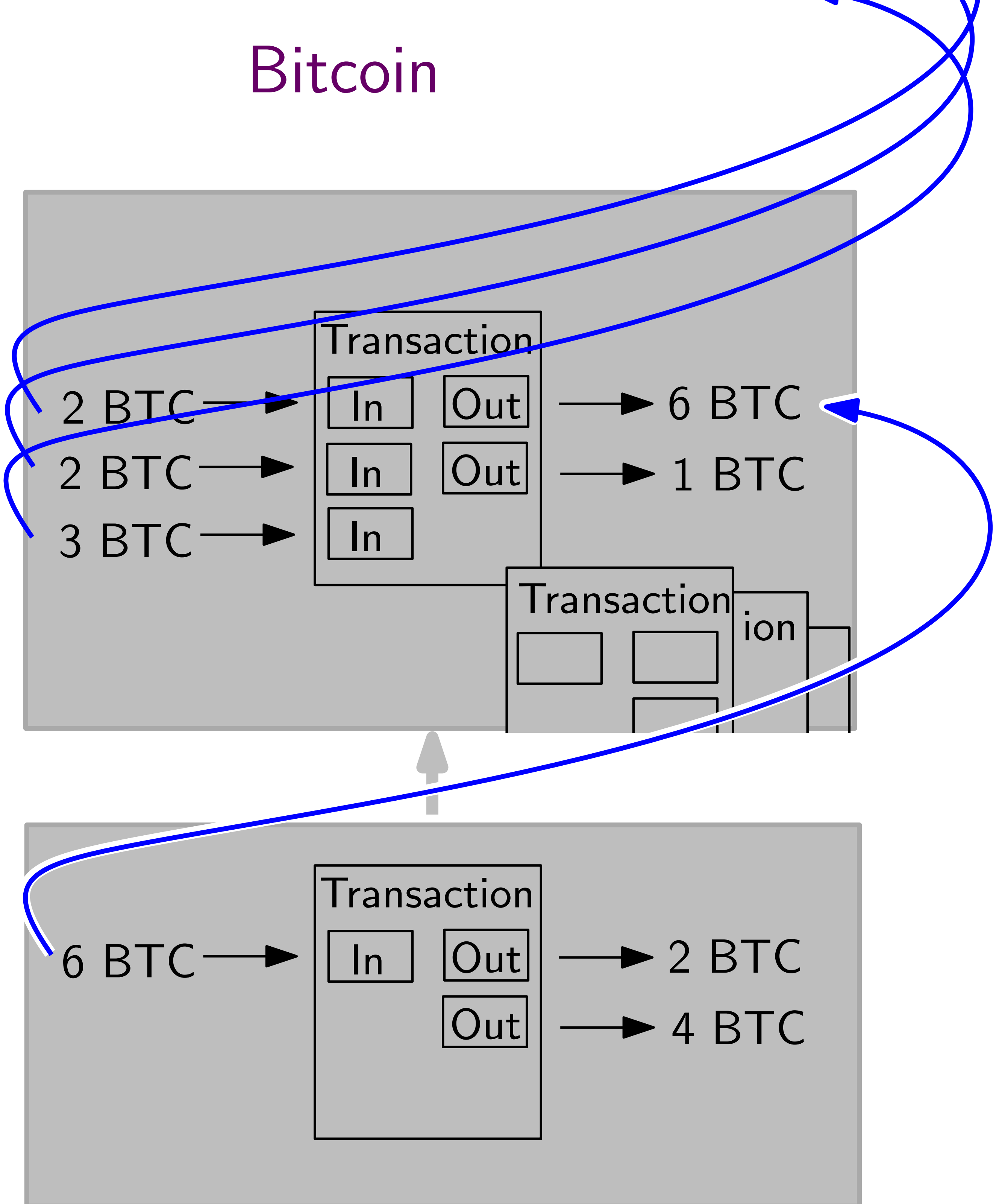


- **Blockchain**

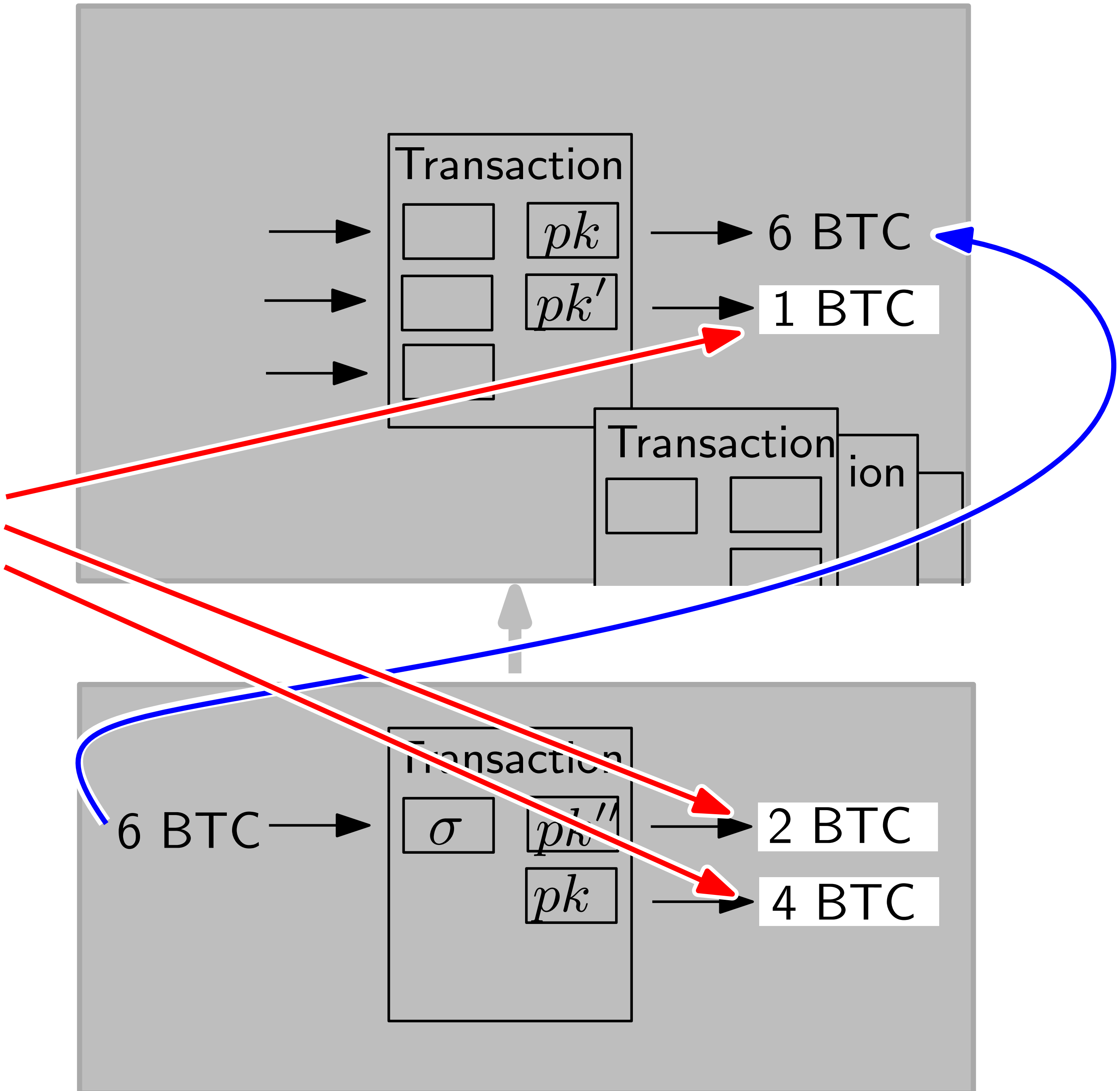


Bitcoin

- Reference to previous output



Bitcoin

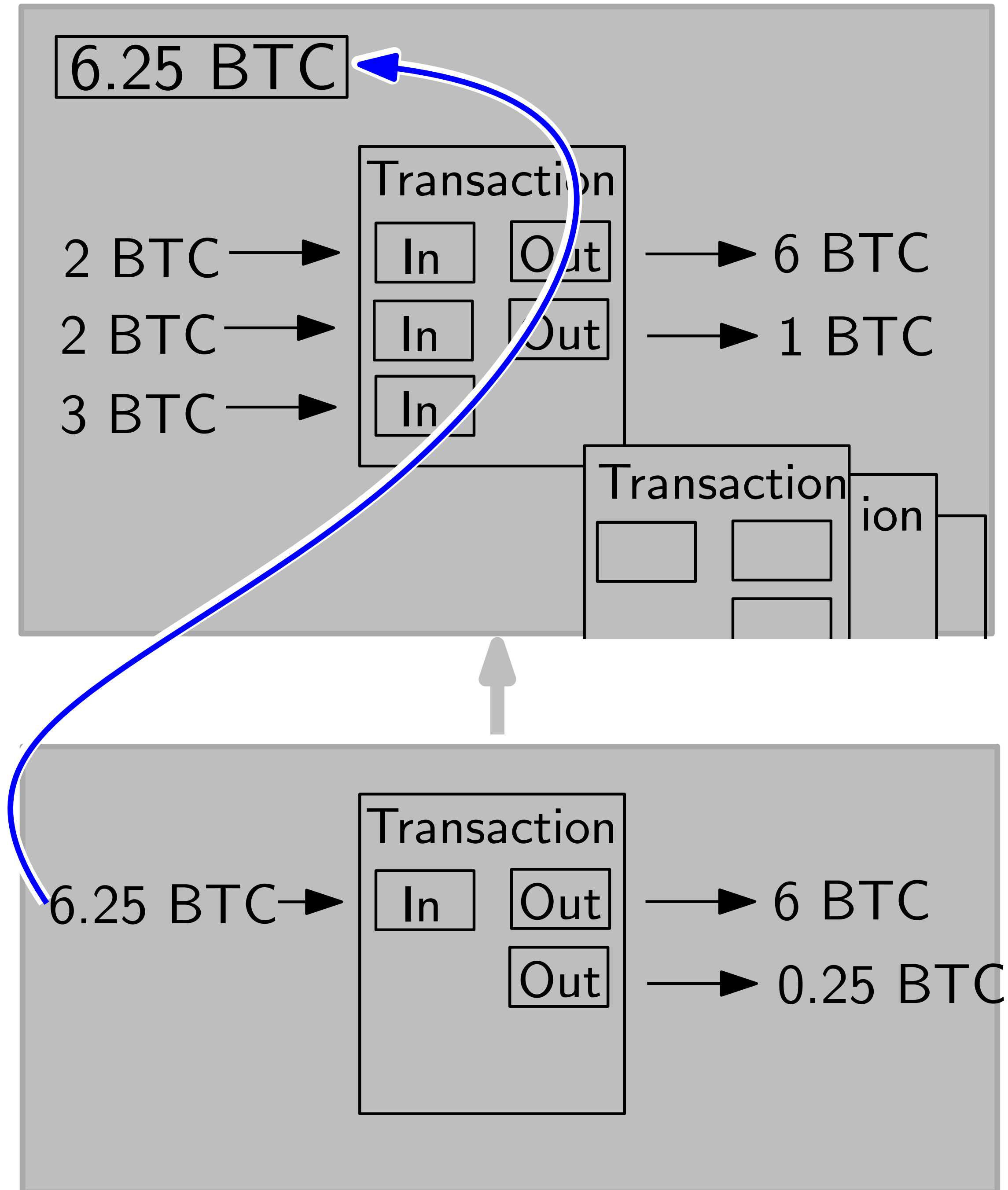


Unspent transaction outputs (UTXO's)

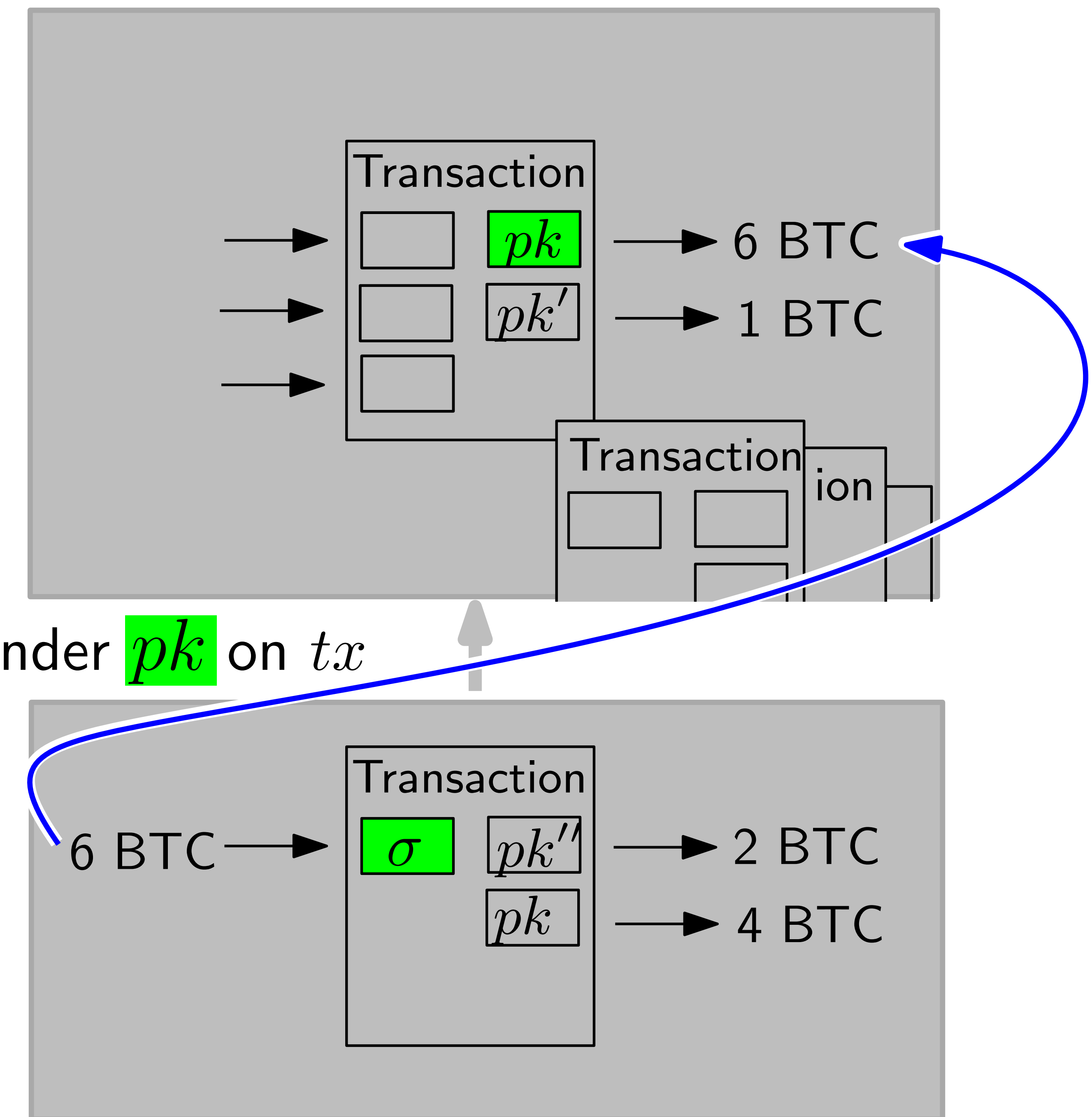
= existing money in system

Bitcoin

- **Coinbase transaction**



Bitcoin



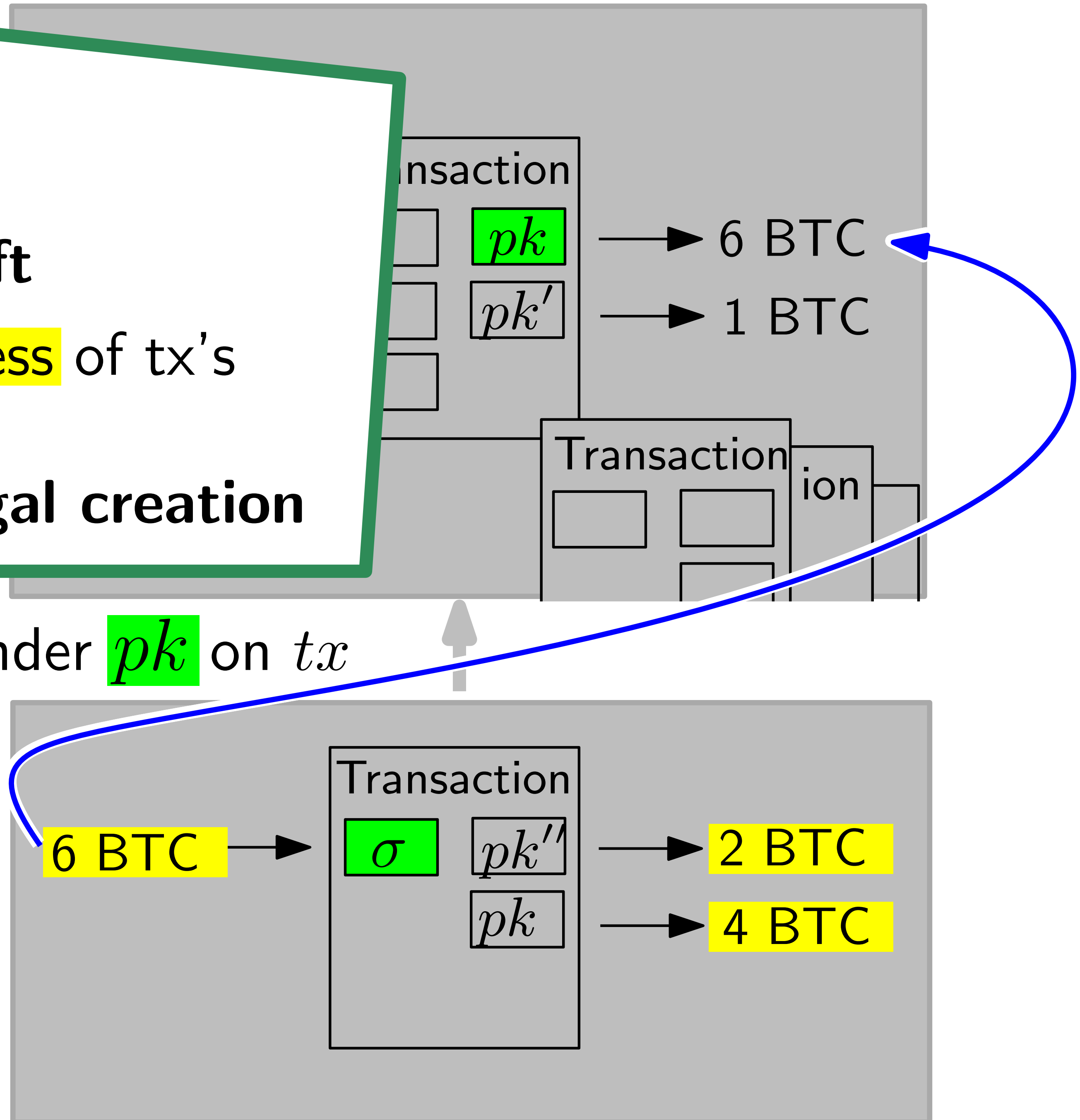
σ is **signature** under pk on tx

Bitcoin

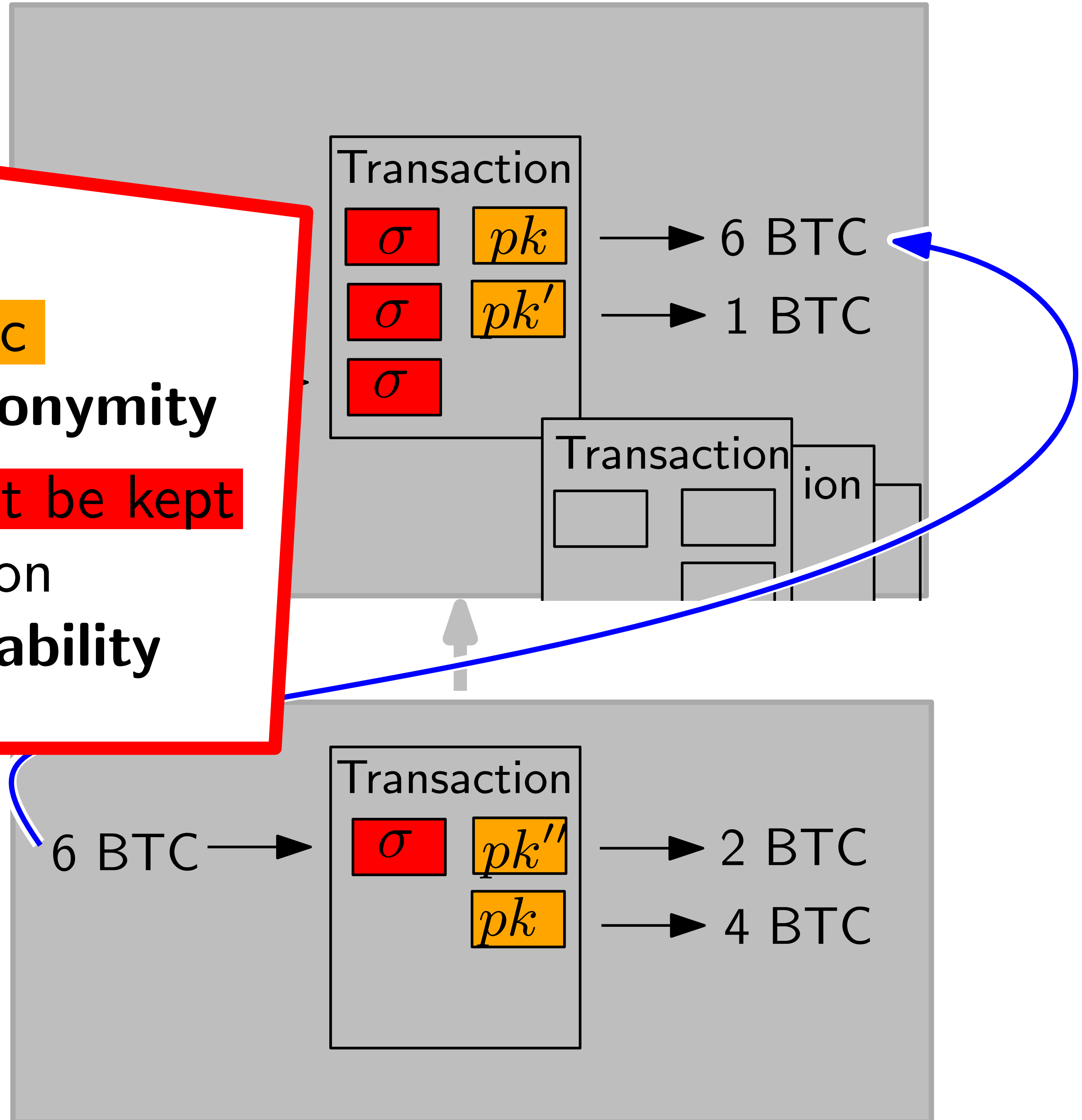
Security

- signatures
  $\Rightarrow$ **no theft**
- balancedness of tx's checkable
  $\Rightarrow$ **no illegal creation**

σ is **signature** under pk on tx



Bitcoin

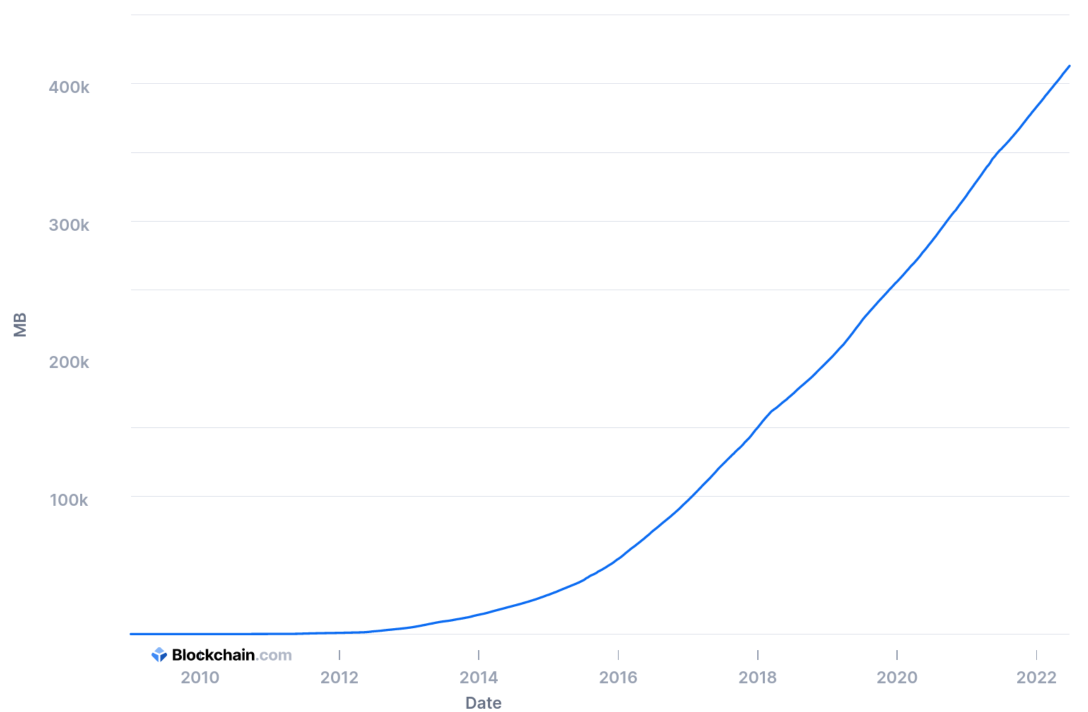


Drawbacks

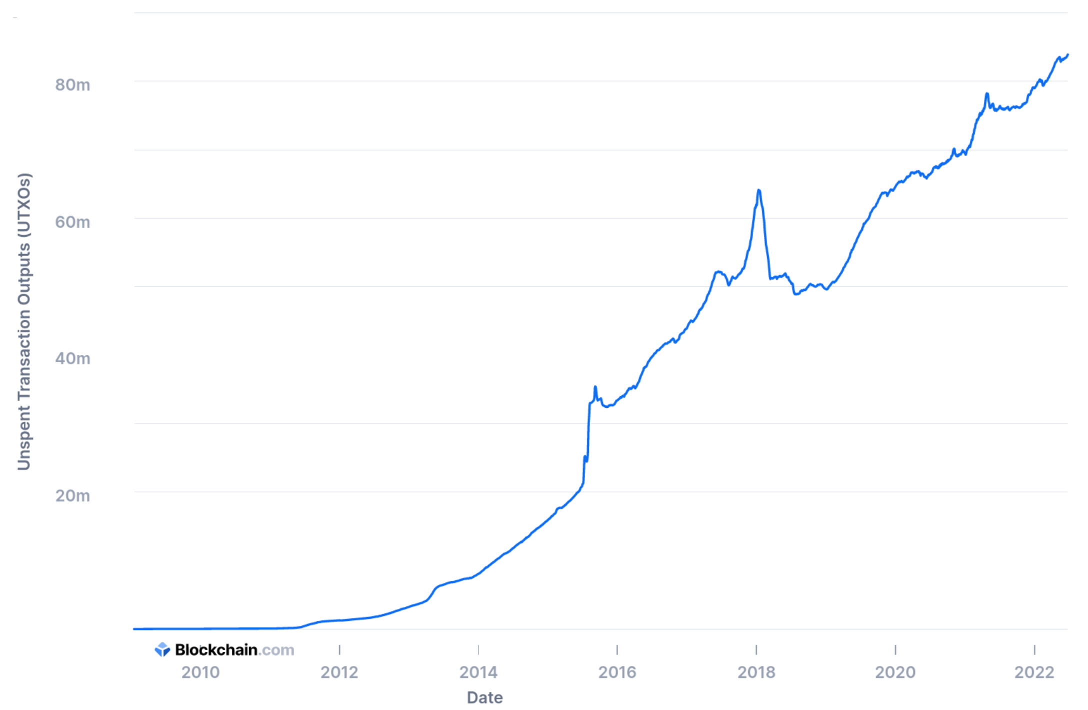
- all tx's public
  $\Rightarrow$ **weak anonymity**
- all data must be kept for verification
  $\Rightarrow$ **bad scalability**

Scalability

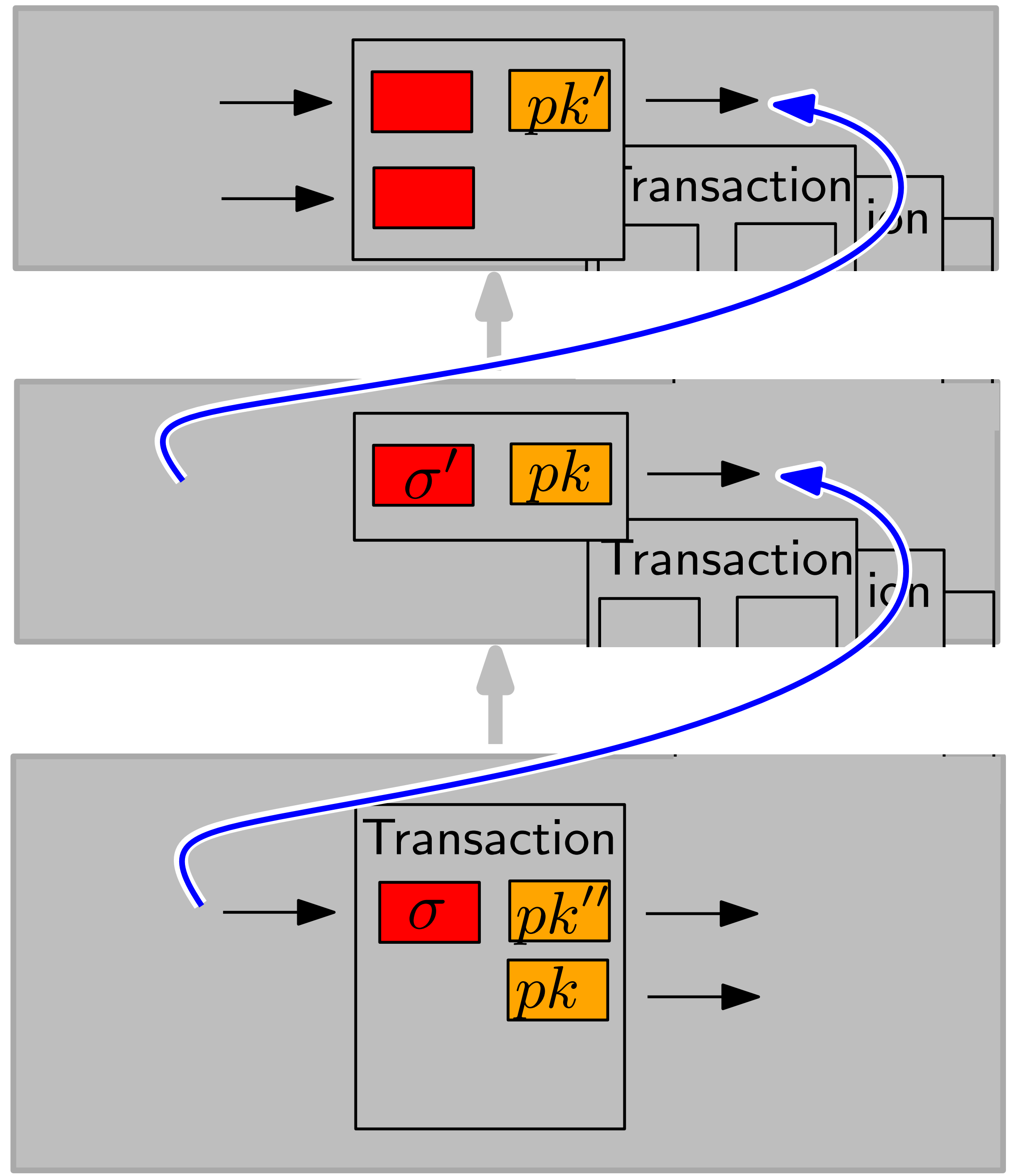
Blockchain size:
> 400 GB



Size of UTXO set:
< 5 GB



Scalability



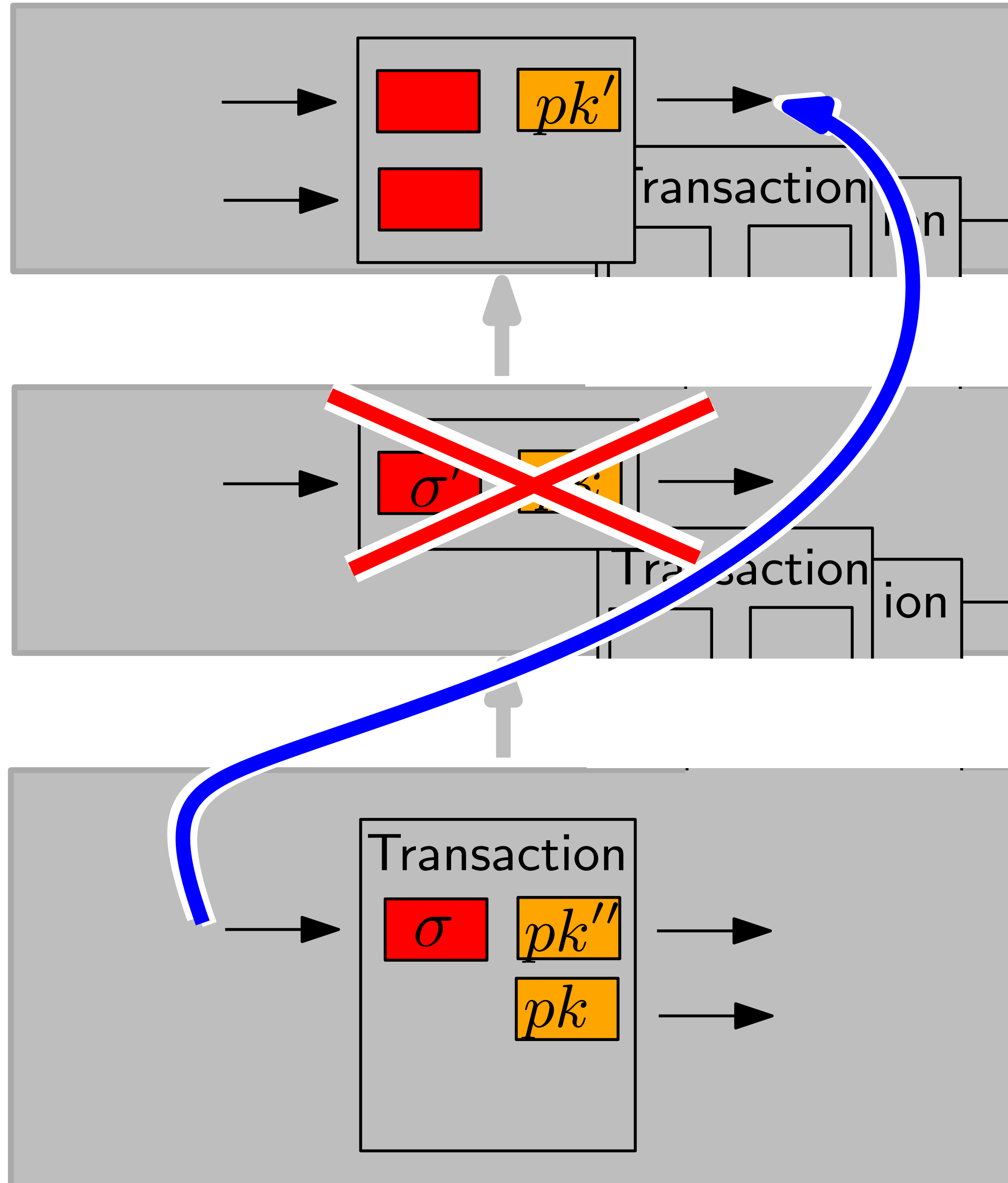
Scalability

“cut-through”

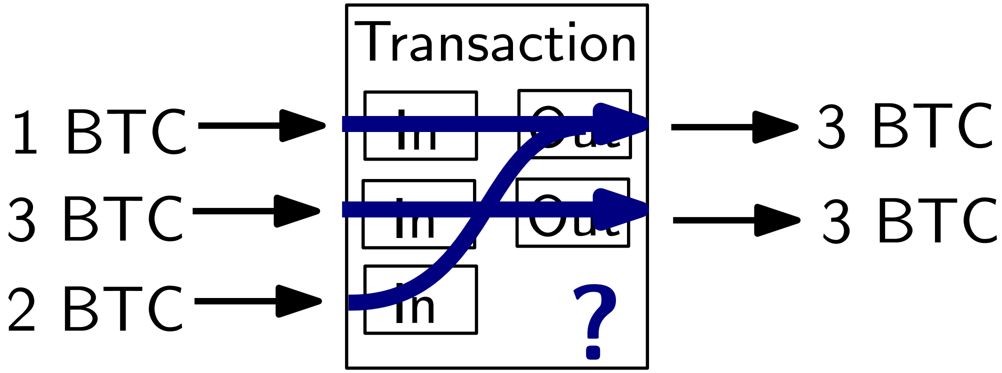
not possible
in Bitcoin:

σ' is needed
to verify validity

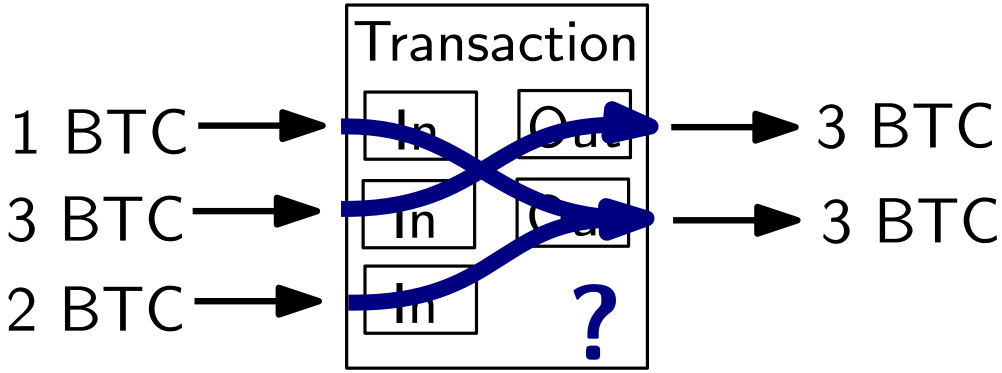
$\Rightarrow$ **Mimblewimble**



Anonymity

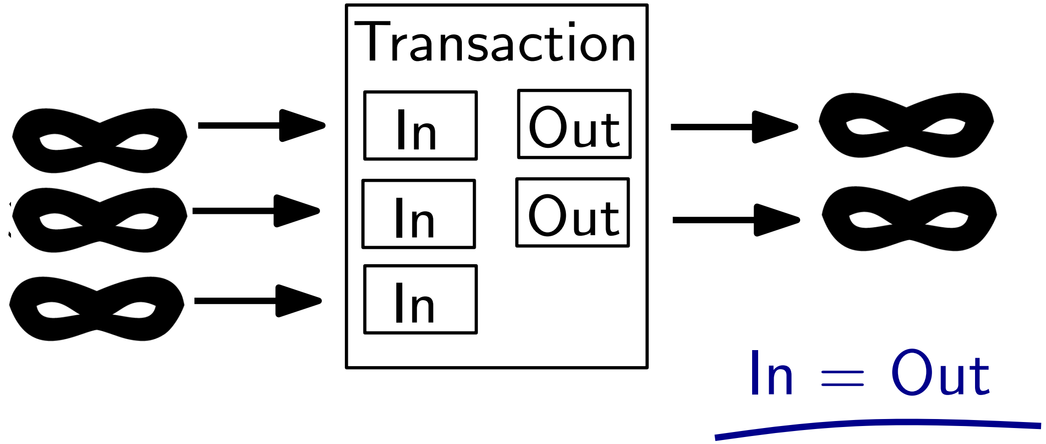


Anonymity



- **CoinJoin** [Maxwell'13]
  - no *link* between inputs and outputs
  - join many transactions?
  - in Bitcoin: only interactively, since all inputs must sign tx

Anonymity



- **Confidential Transactions** [Maxwell]
  - hide the input and output *amounts*
  - not compatible with Bitcoin system
  - balancedness verifiable?

(by default in MONERO)

Anonymity

How can we get

- **Confidential transactions**
  (check balancedness)
- **Coin-join**
  (non-interactively)
- **Cut-through**
  (post-confirmation)

while **maintaining verifiability?**

- **Confider**
  - hide tł
  - not co
  - balanc

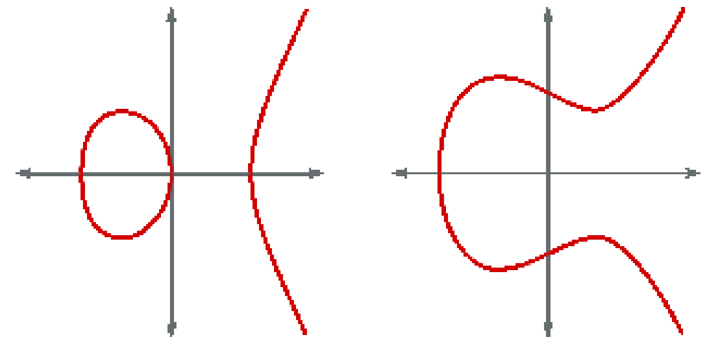
Anonymity

- **Confider**
  - hide tl
  - not co
  - balanc

Mimblewimble

Discrete logarithms

- Finite group (of prime order) $(\mathbb{G}, +)$
  - generator G
  - $xG := \underbrace{G + \ldots + G}_{x \text{ times}}$



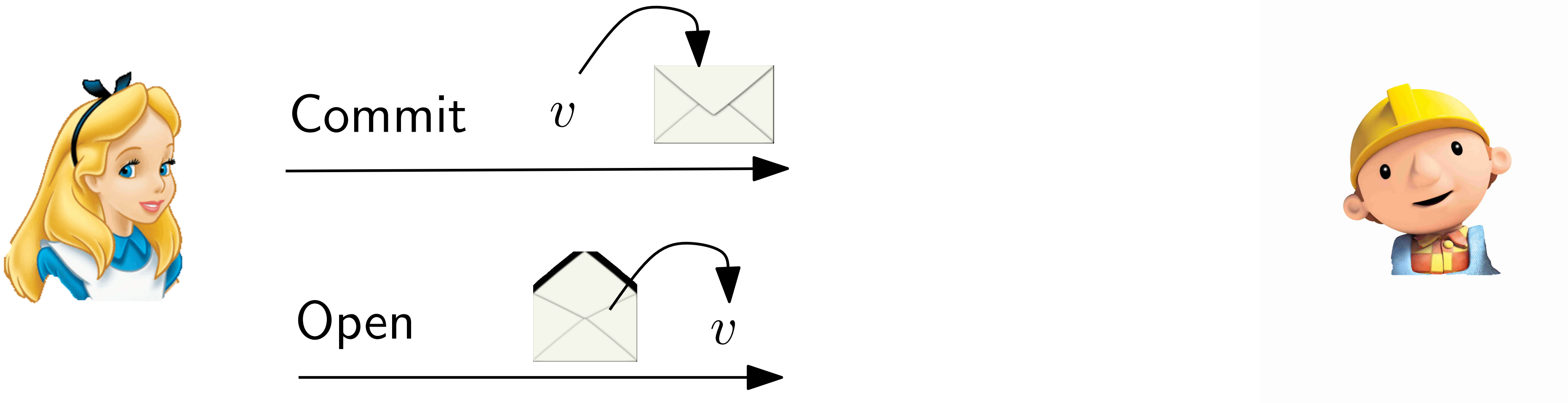
- **Discrete logarithm** problem:
  - given $G, H \in \mathbb{G}$
  - find x such that $H = xG$

- used in **signature schemes**
  (e.g. ECDSA ,
  Schnorr)
  - secret key: x
  - public key: $X = xG$

Pedersen commitment

Commitment

- "digital envelope"



- **hiding:** commitment hides v
- **binding:** Alice can open commitment only to one value

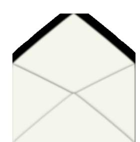
Pedersen commitment

Commitment

- "digital envelope"

Commit v

Open



Pedersen

$G, H \in \mathbb{G}$

pick random r

$C := vH + rG$

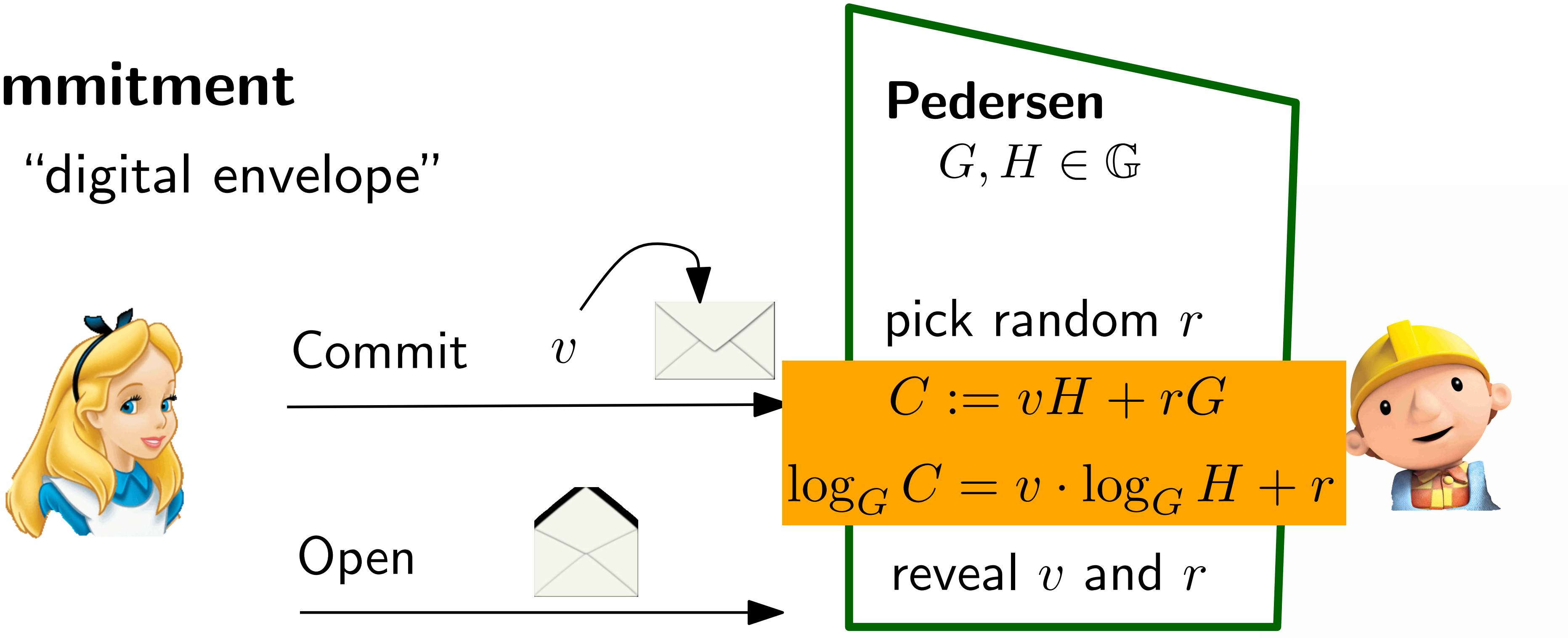
reveal v and r

- **hiding:** for any v exists r so that C commits v

Pedersen commitment

Commitment

- "digital envelope"



- **hiding:** for any v exists r so that C commits v:

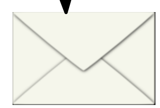
$$(r = \log_G C - v \cdot \log_G H)$$

Pedersen commitment

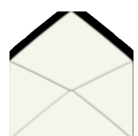
Commitment

- "digital envelope"

Commit v



Open



Pedersen

$G, H \in \mathbb{G}$

pick random r

$C := vH + rG$

reveal v and r

- **binding:** assume Alice finds $v \neq v', r, r'$ with

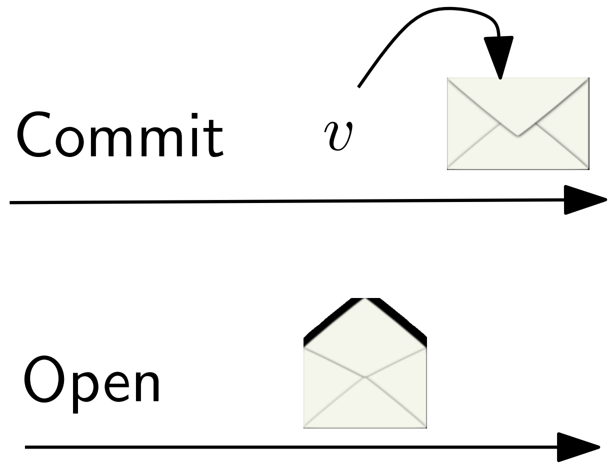
$$vH + rG = C = v'H + r'G, \quad \text{then } \frac{r'-r}{v-v'}G = H$$

$\Rightarrow$ Alice solved discrete log problem!

Pedersen commitment

Commitment

- "digital envelope"



Pedersen

$G, H \in \mathbb{G}$

pick random r

$\textbf{Com}(v; r) := vH + rG$

reveal v and r

- commitments are **homomorphic**:

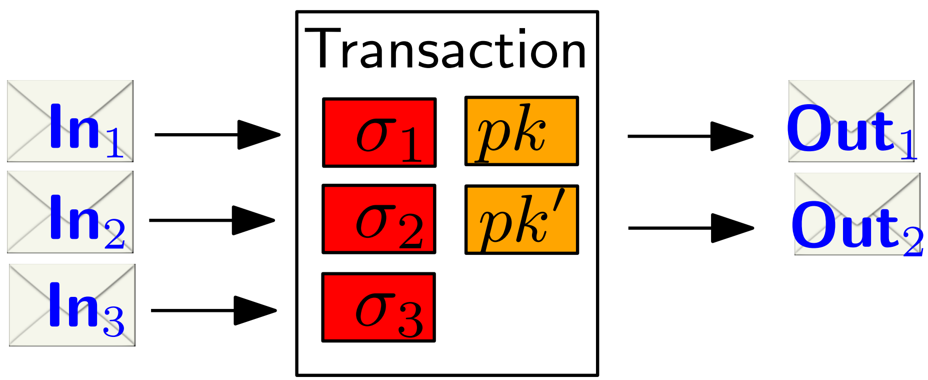
$$\begin{aligned}\textbf{Com}(v_1; r_1) + \textbf{Com}(v_2; r_2) &= (v_1 H + r_1 G) \ + \ (v_2 H + r_2 G) \\ &= (v_1 + v_2)H + (r_1 + r_2)G \\ &= \textbf{Com}(v_1 + v_2; r_1 + r_2)\end{aligned}$$

e.g.: $\textbf{Com}(1; 5) + \textbf{Com}(1; 10) - \textbf{Com}(2, 15) = \mathbf{0}$

Confidential Transactions

[Back, Maxwell '13–'15]

- use *commitments* to amounts
- ensure that transactions do not create money?



$$C = vH + rG$$

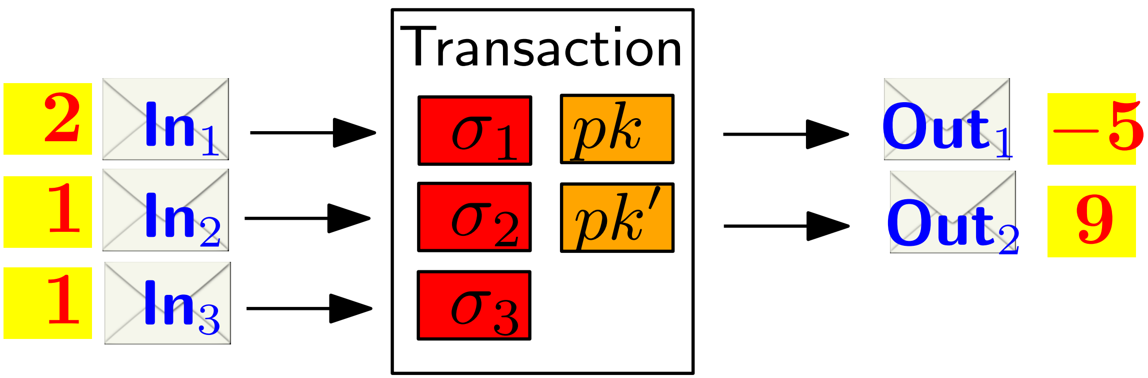
$$\boxed{\textstyle\sum \mathbf{Out} - \sum \mathbf{In} = 0}$$

$$\begin{aligned}
&\textstyle\sum C_i^{\text{out}} - \sum C_i^{\text{in}} \\
&= \textstyle\sum (v_i^{\text{out}} H + r_i^{\text{out}} G) - \sum (v_i^{\text{in}} H + r_i^{\text{in}} G) \\
&= \underbrace{\textstyle(\sum v_i^{\text{out}} - \sum v_i^{\text{in}})}_{\stackrel{!}{=}0} H + \underbrace{\textstyle(\sum r_i^{\text{out}} - \sum r_i^{\text{in}})}_{\stackrel{!}{=}0} G
\end{aligned}$$

Confidential Transactions

[Back,Maxwell '13–'15]

- use *commitments* to amounts
- ensure that transactions do not create money?



$C = vH + rG$ π

$$\boxed{\sum \mathbf{Out} - \sum \mathbf{In} = \mathbf{0}}$$

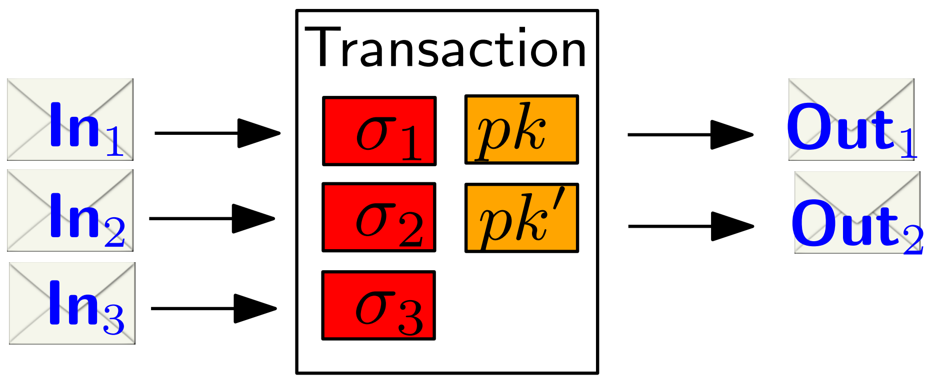
- negative amounts!

Range proofs

– add proofs that committed values are in $\in [0, 2^{64}]$

Confidential Transactions

Confidential transaction



$$C = vH + rG, \quad \pi$$

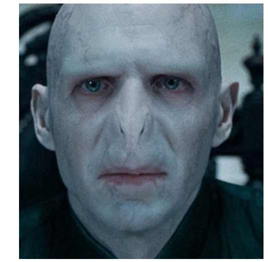
$$\sum \textbf{Out} - \sum \textbf{In} = 0$$

Signatures $\Rightarrow$

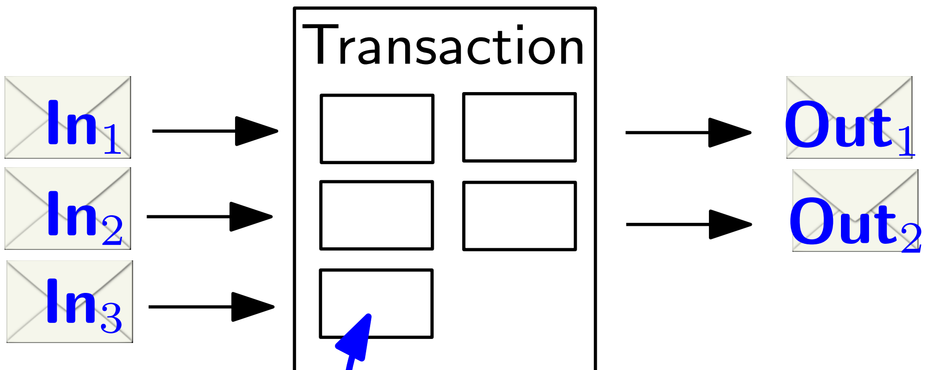
- no non-interactive CoinJoin
- no Cut-Through

Mimblewimble

[Jedusor '16]



secret key!



$$C = vH + rG, \quad \pi$$

$$\sum \mathbf{Out} - \sum \mathbf{In} = 0$$

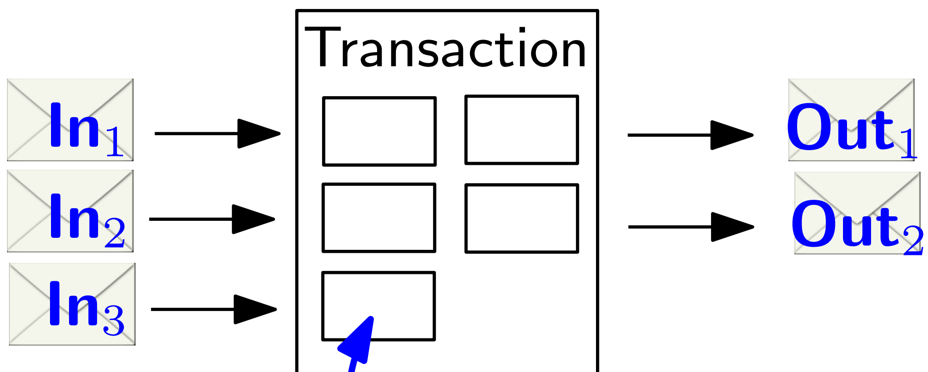
no more signatures!

But: sender knows sum of output r's

Mimblewimble

[Jedusor '16]

secret key!



$$C = vH + rG, \quad \pi$$

$$\sum \mathbf{Out} - \sum \mathbf{In} = 0H + xG$$

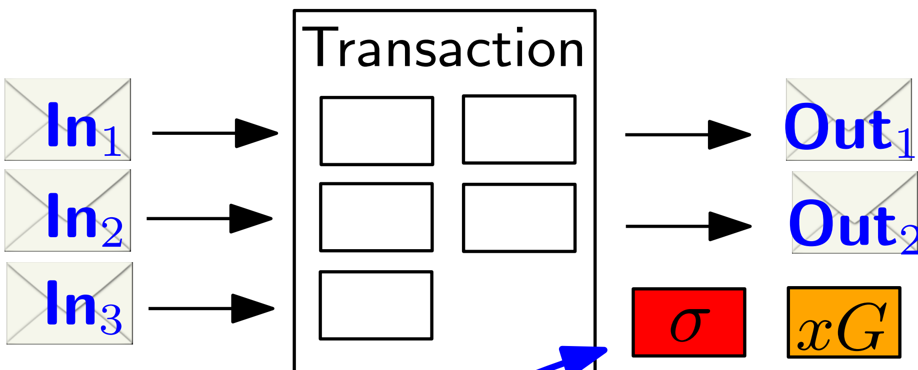
no more signatures!

$$\sum C_i^{\text{out}} - \sum C_i^{\text{in}}$$
$$= \sum (v_i^{\text{out}} H + r_i^{\text{out}} G) - \sum (v_i^{\text{in}} H + r_i^{\text{in}} G)$$
$$= (\underbrace{\sum v_i^{\text{out}} - \sum v_i^{\text{in}}}_{\stackrel{!}{=} 0}) H + (\underbrace{\sum r_i^{\text{out}} - \sum r_i^{\text{in}}}_{=: x}) G$$

Mimblewimble

[Jedusor '16]

secret key!



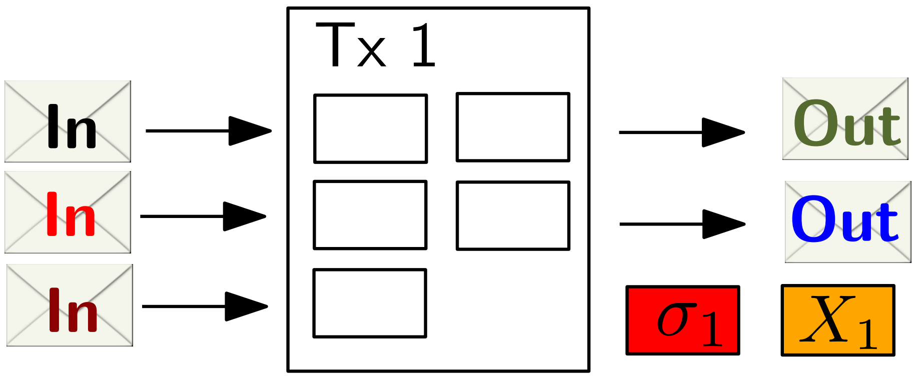
$C = vH + rG, \quad \pi$

$$\boxed{\sum \mathbf{Out} - \sum \mathbf{In} = 0H + xG}$$

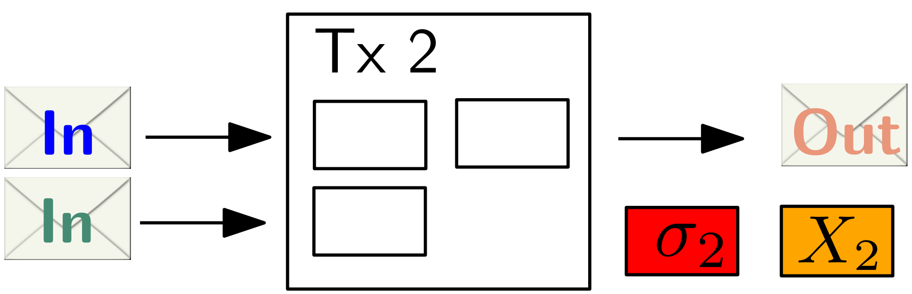
one signature

"proves" that $\overbrace{\sum \mathsf{Out} - \sum \mathsf{In}}$ is commitment to 0

Mimblewimble



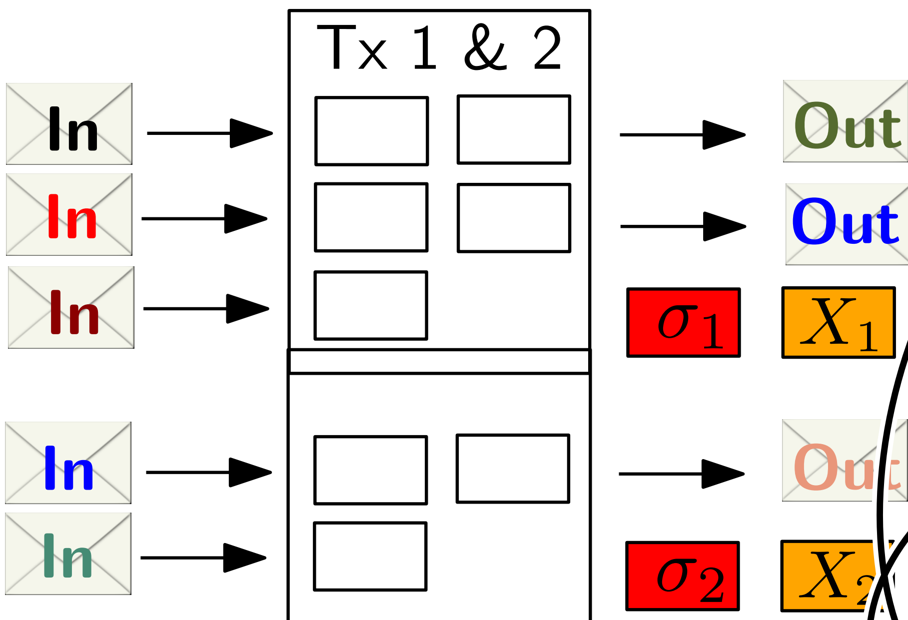
- $\sum \textbf{Out}_1 - \sum \textbf{In}_1 = X_1$
- σ_1 valid for X_1



- $\sum \textbf{Out}_2 - \sum \textbf{In}_2 = X_2$
- σ_2 valid for X_2

Mimblewimble

Non-interactive CoinJoin

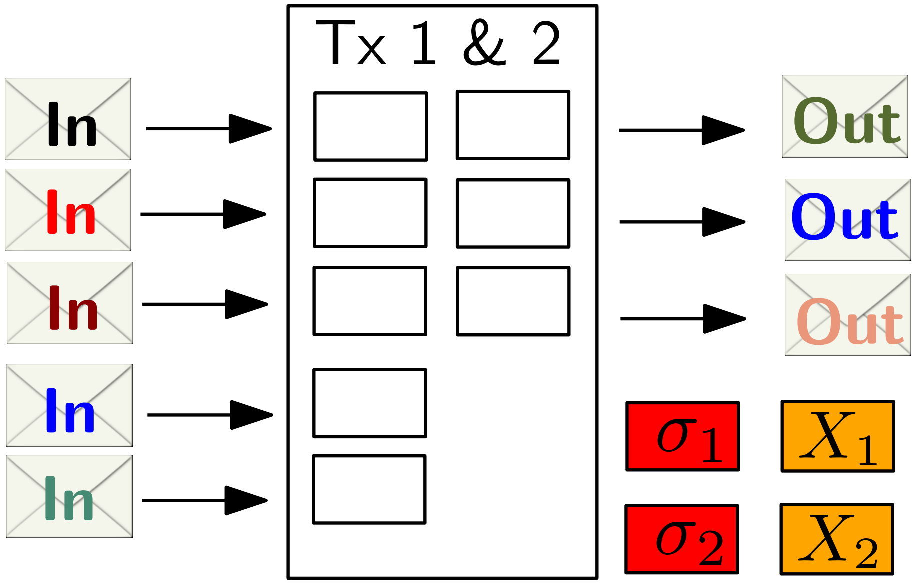


- $\sum \textbf{Out}_1 - \sum \textbf{In}_1 = X_1$
- σ_1 valid for X_1

- $\sum \textbf{Out}_2 - \sum \textbf{In}_2 = X_2$
- σ_2 valid for X_2

- $\sum \textbf{Out} - \sum \textbf{In} = X_1 + X_2$
- σ_1 valid for X_1
- σ_2 valid for X_2

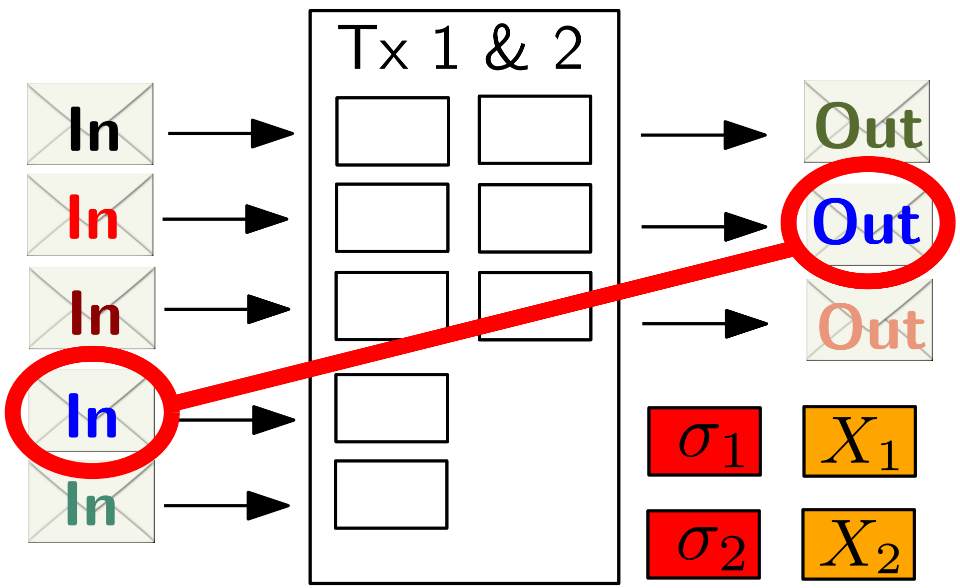
Mimblewimble



- $\sum$ **Out** $-\sum$ **In** $= X_1 + X_2$
- σ_1 valid for X_1
- σ_2 valid for X_2

Mimblewimble

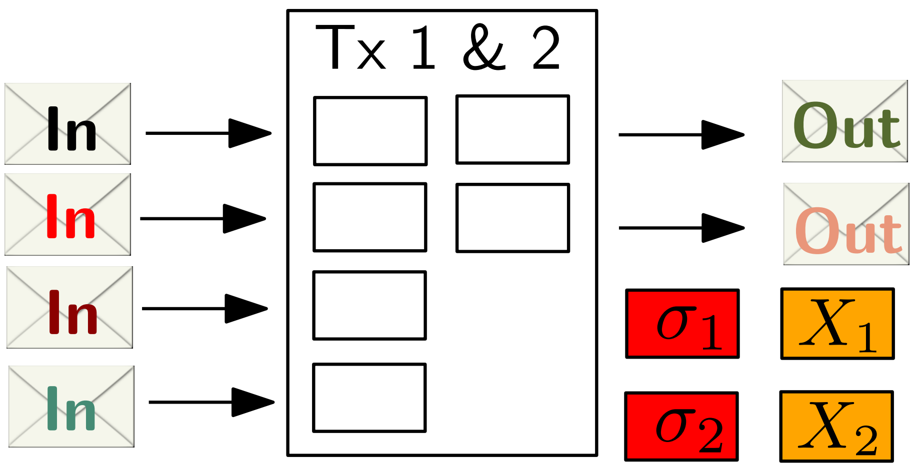
Post-confirmation Cut-Through



- $\sum$ **Out** $-\sum$ **In** $= X_1 + X_2$
- σ_1 valid for X_1
- σ_2 valid for X_2

Mimblewimble

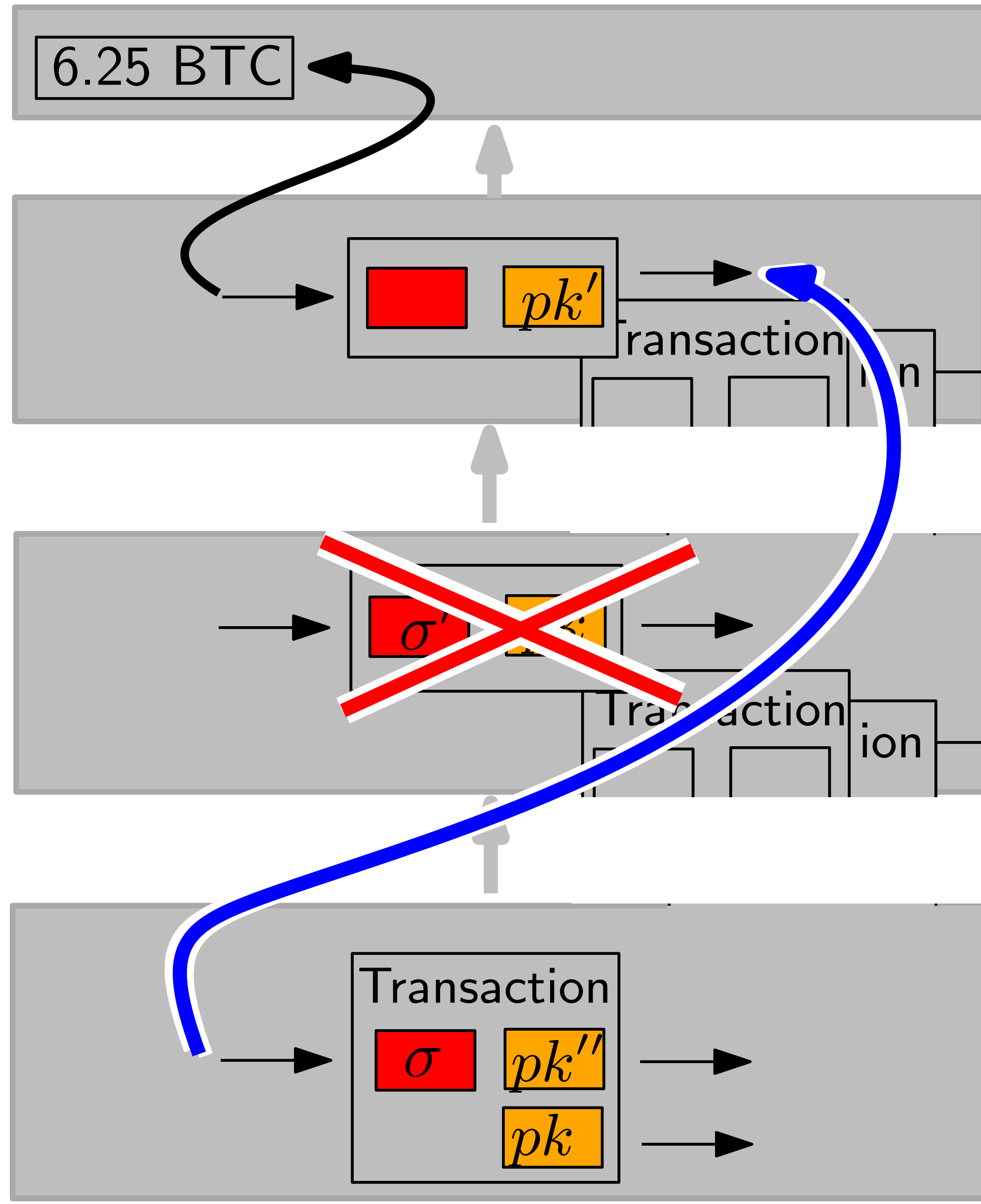
Post-confirmation Cut-Through



- $\sum \mathbf{Out} - \sum \mathbf{In} = X_1 + X_2$
- σ_1 valid for X_1
- σ_2 valid for X_2

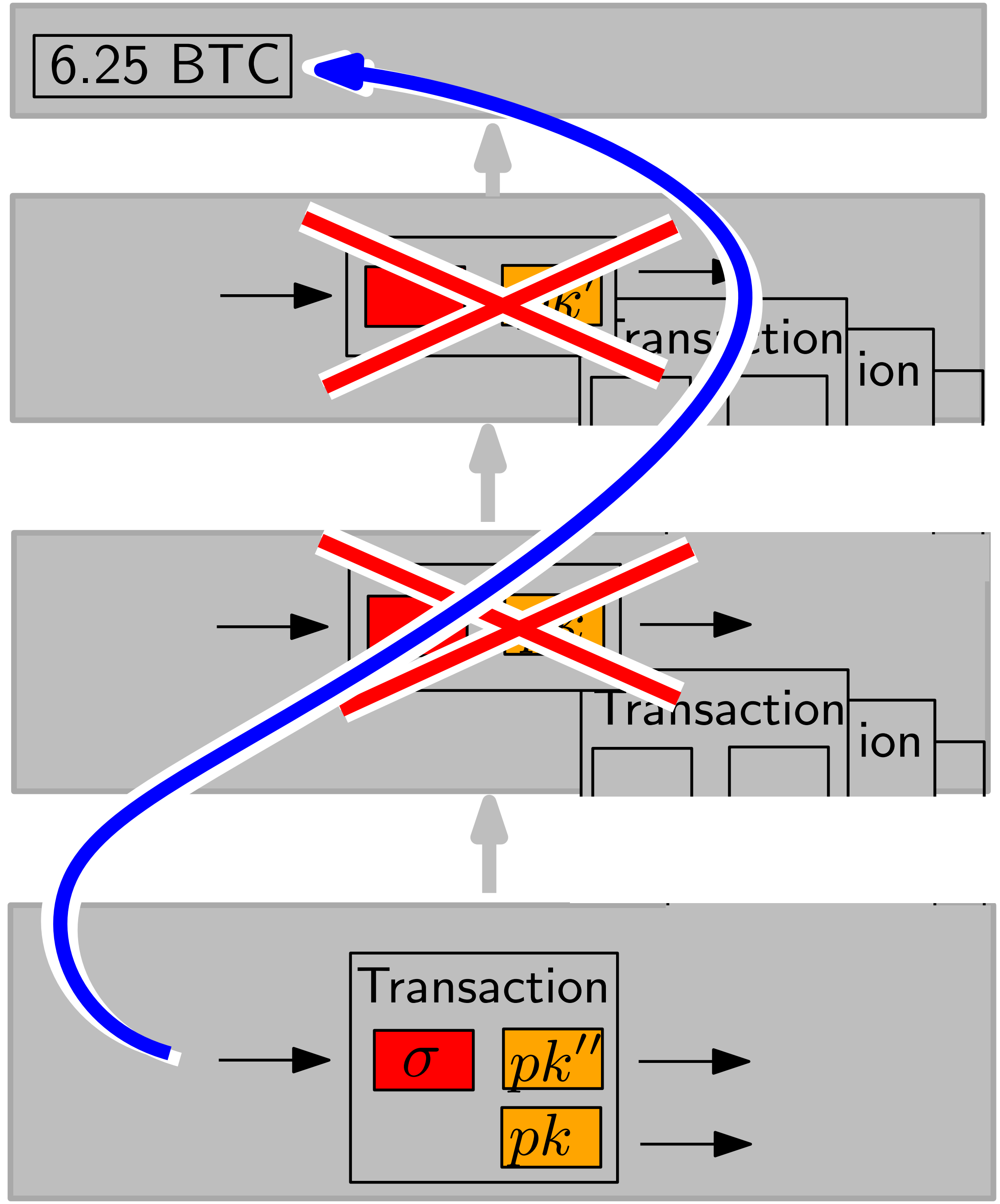
Scalability

“cut-through”



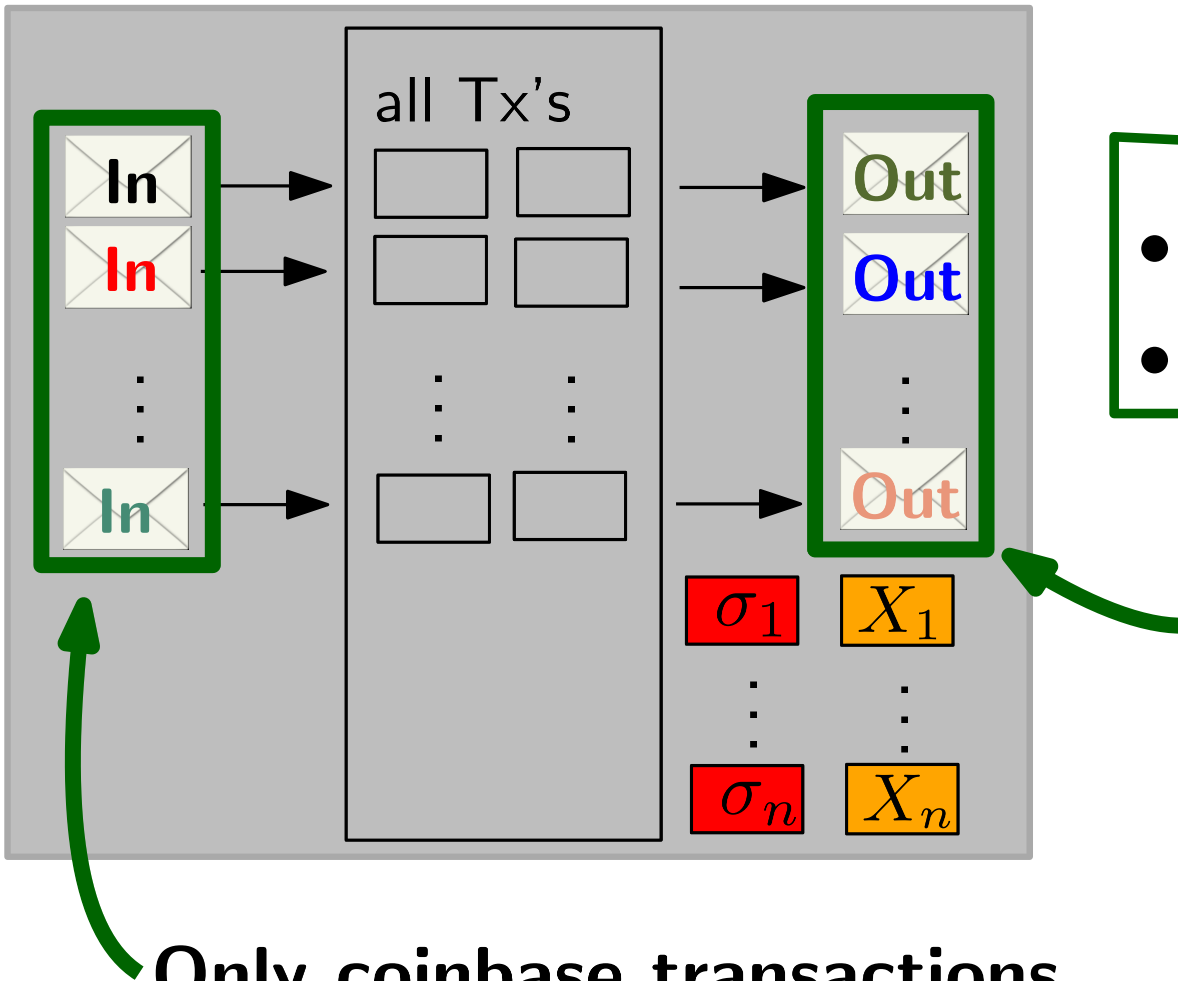
Scalability

“cut-through”



Mimblewimble

Cut through all transactions in blockchain



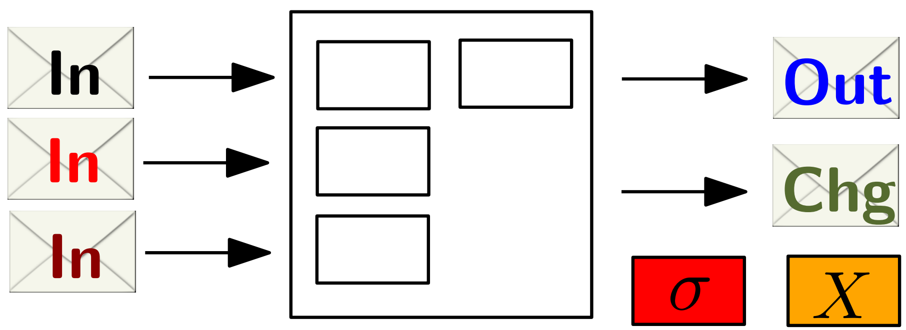
- $\sum$ **Out** $-\sum$ **In** $= \sum X_i$
- $\forall i : \sigma_i$ valid for X_i

UTXO set

Only coinbase transactions

Mimblewimble

How are transactions actually created?



- $\sum \textbf{Out} - \sum \textbf{In} = X$
- σ valid for X

signature under key $r_{\text{Out}} + r_{\text{Chg}} - \sum r_{In}$

known by sender

known by receiver

Use interactive protocol for signature under $X_1 + X_2$

Mimblewimble

[FOS19]

- **Formal security models:**
  - inflation-resistance
  - coin-theft-resistance
  - confidential amounts
- **Abstraction of Mimblewimble** from:
  - homomorphic commitments
  - compatible signatures

  ] . . . satisfying joint security
  - simulation-extractable NIZK range proofs
- **Proof** that abstraction satisfies model
- **Instantiations:** proof that
  - Pedersen + Schnorr
  - Pedersen + (aggregate) BLS

  ] . . . satisfy joint security

Non-interactive TXs

Mimblewimble: receiver needs to **interact** with sender

Bitcoin: knowing receiver's address, anyone can send money

Privacy? **Bitcoin:**

- use every address only once $\rightarrow$ *unlinkability*
- send address privately $\rightarrow$ requires *interaction*

Stealth addresses:

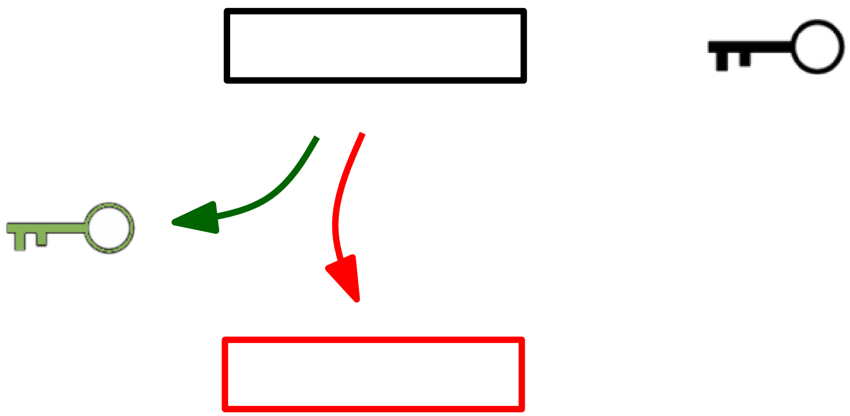
- publish **one** address
- receive **unlinkable** payments **non-interactively**

(by default in MONERO)

Stealth addresses

Stealth addresses:

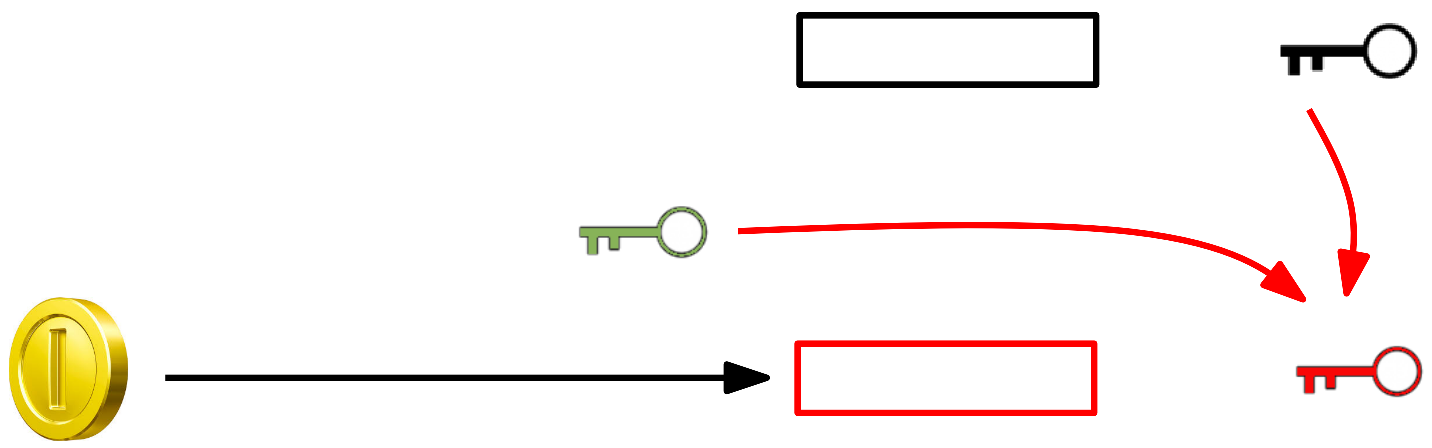
- publish **one** address



Stealth addresses

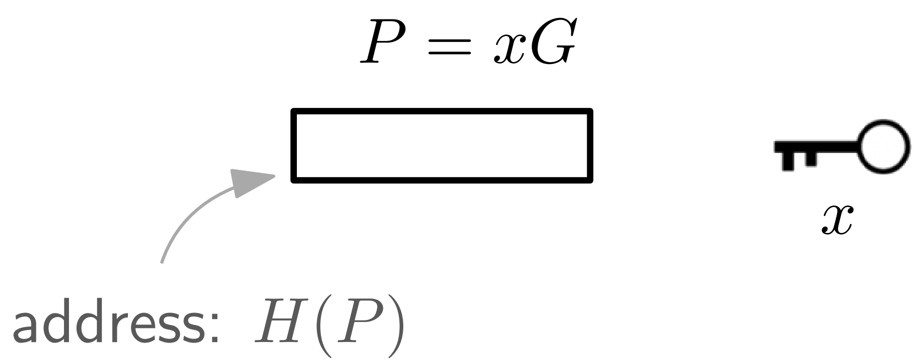
Stealth addresses:

- publish **one** address
- receive **unlinkable** payments



Stealth addresses

Bitcoin



Stealth addresses

$$(A, B) = (aG, bG)$$

- pick random r

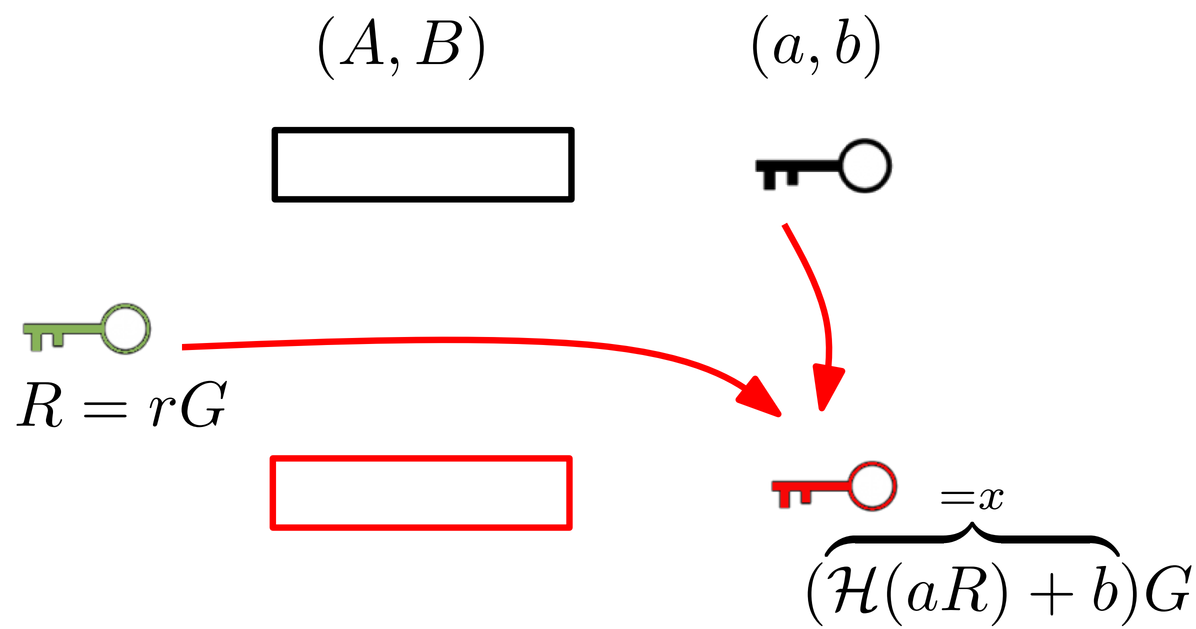
$$R = rG$$

$$P = \mathcal{H}(\underbrace{rA}_{= raG = aR})G + B = (\overbrace{\mathcal{H}(aR) + b}^{=x})G$$

Diffie-Hellman shared key between A and R

Stealth addresses

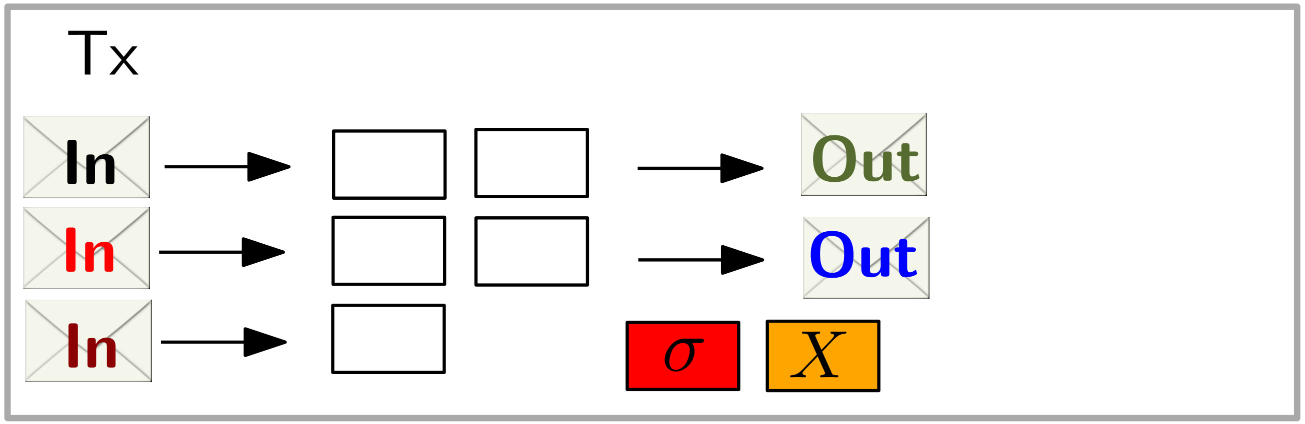
- pick random r



Non-interactive TXs

MW with non-interactive TXs

stealth addresses for outputs



(A_1, B_1)

(A_2, B_2)

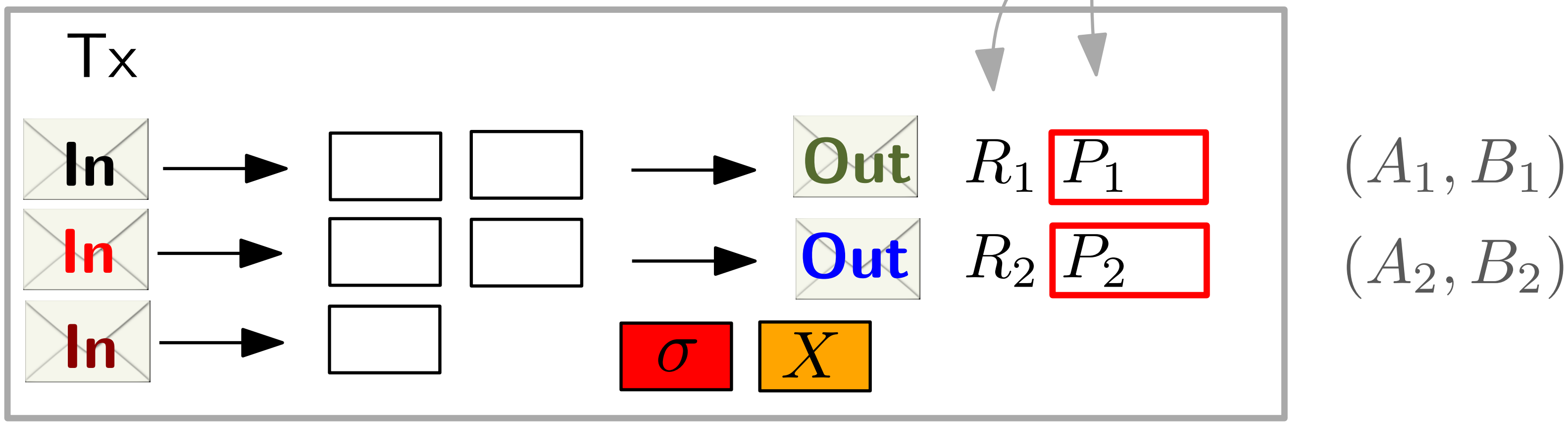
- $\sum$ **Out** $- \sum$ **In** $= X$
- σ valid for X
- rangeproofs valid

Non-interactive TXs

MW with non-interactive TXs

one-time addresses

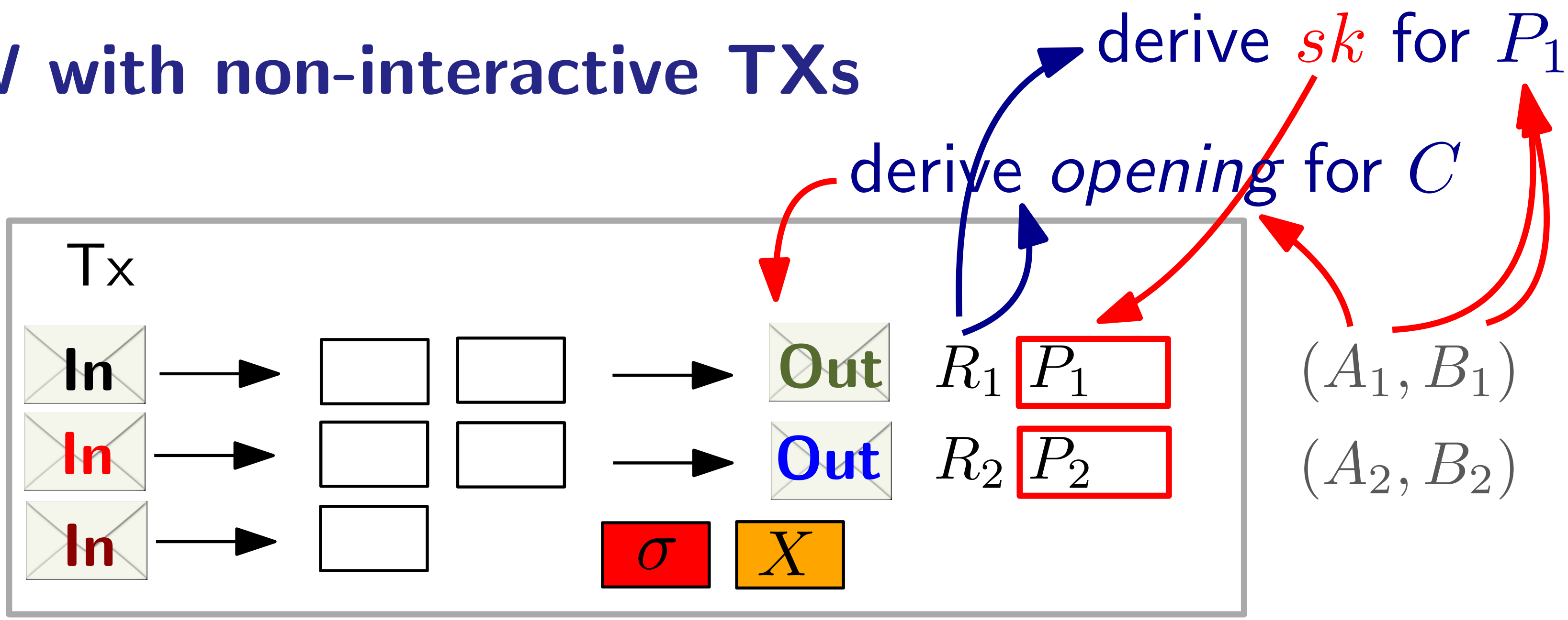
"transfer keys"



- $\sum$ **Out** $-\sum$ **In** $= X$
- σ valid for X
- rangeproofs valid

Non-interactive TXs

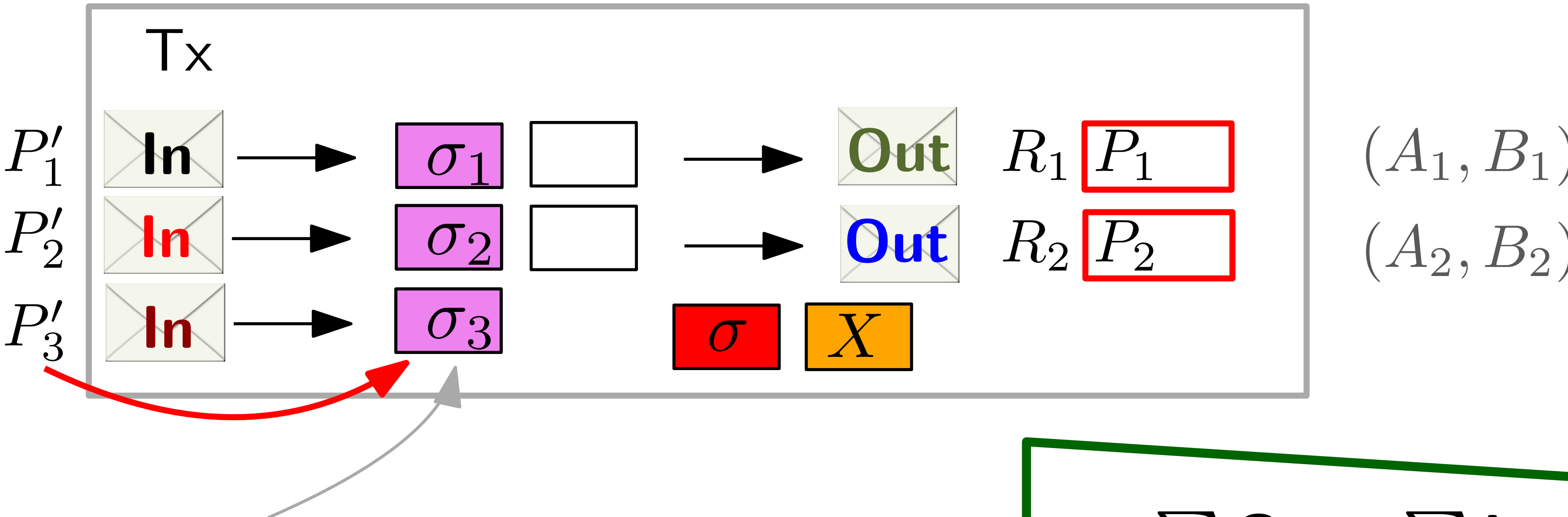
MW with non-interactive TXs



- $\sum$ **Out** $-\sum$ **In** $= \boxed{X}$
- $\boxed{\sigma}$ valid for $\boxed{X}$
- rangeproofs valid

Non-interactive TXs

MW with non-interactive TXs



sig under one-time key P_3'

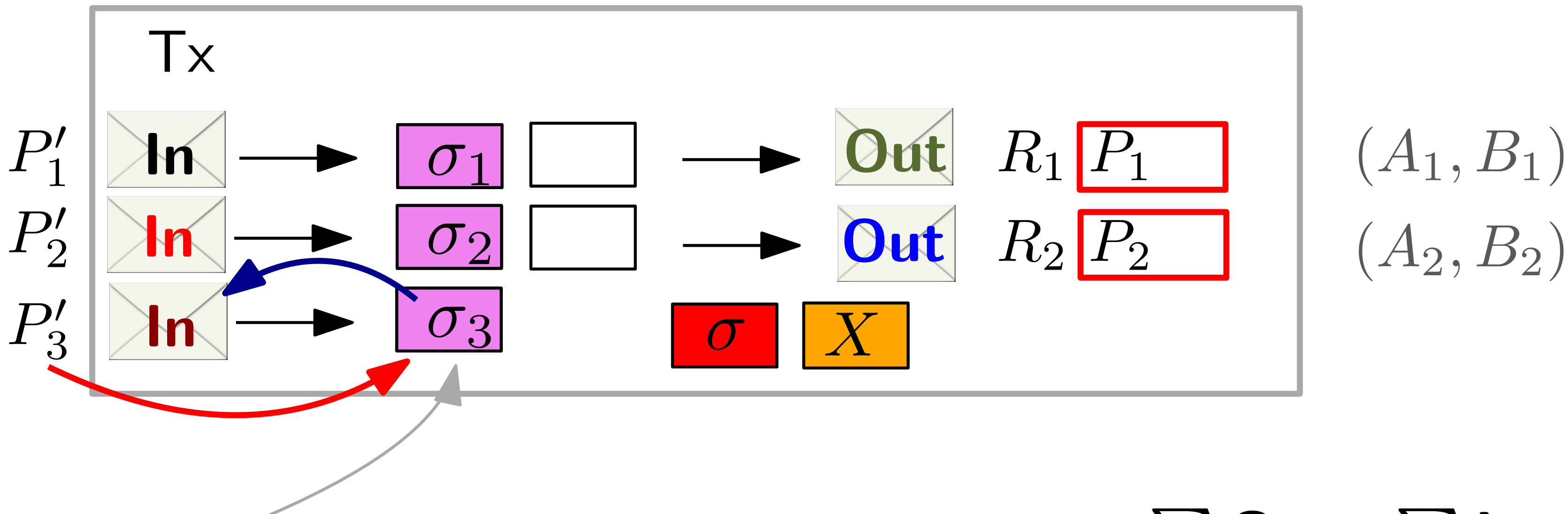
- $\sum$ **Out** $- \sum$ **In** $= X$
- σ valid for X
- rangeproofs valid

But: σ cannot sign Tx

$\leftarrow$ CoinJoin, anonymity

Non-interactive TXs

MW with non-interactive TXs



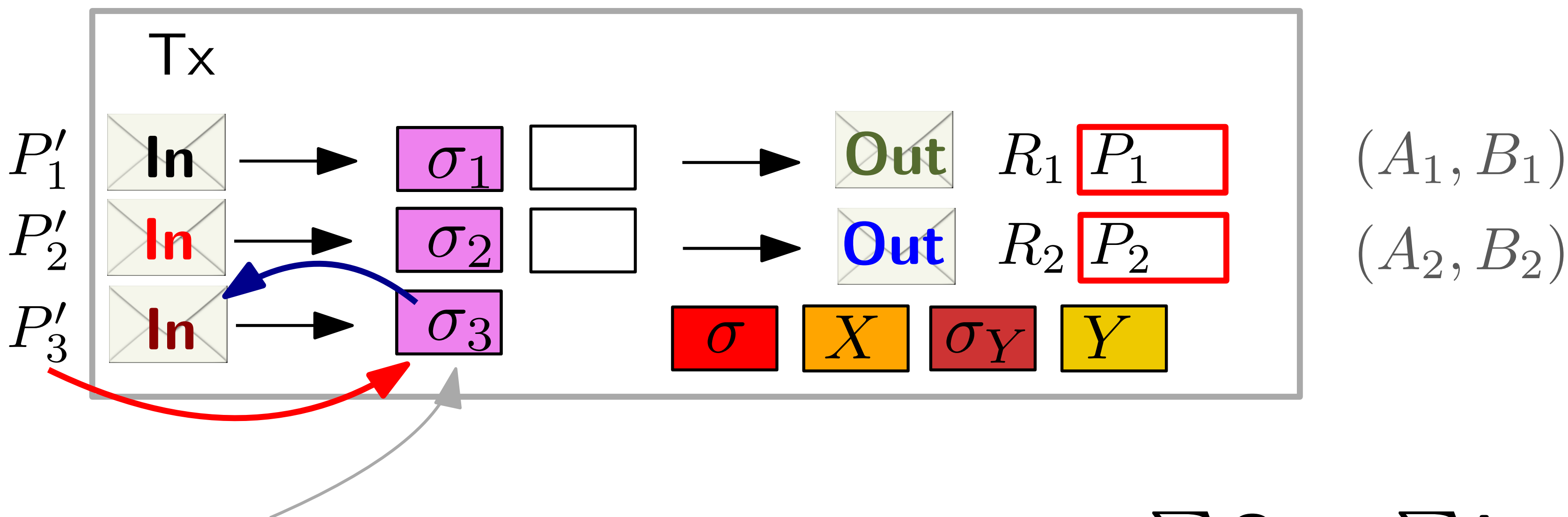
sig under one-time key P'_3 on input

- $\sum$ **Out** $- \sum$ **In** $= X$
- σ valid for X
- rangeproofs valid
- verify σ_i's

But: no "authentication" of outputs

Non-interactive TXs

MW with non-interactive TXs



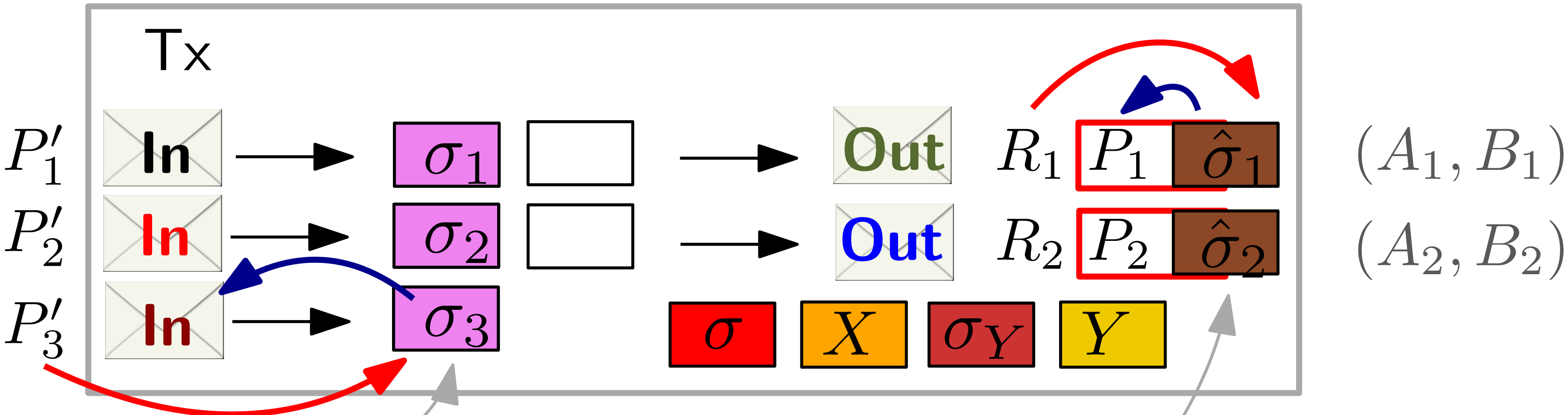
sig under one-time key P'_3 on input

- $\sum$ **Out** $- \sum$ **In** $= X$
- σ valid for X
- rangeproofs valid
- verify σ_i's
- $\sum R_i - \sum P'_i = Y$
- σ_Y valid for Y

But: miner could just change P

Non-interactive TXs

MW with non-interactive TXs



sig under one-time key P'_3 on input

sig under R_2 on P_2

- $\sum$ **Out** $- \sum$ **In** $= X$
- σ valid for X
- rangeproofs valid
- verify σ_i's
- $\sum R_i - \sum P'_i = Y$
- σ_Y valid for Y
- verify $\hat{\sigma}_i$'s

But: still subtle attacks

Non-interactive TXs

[FO22]

- **Fixing scheme with Burkett**
- **Prove properties**
  - inflation-resistance
  - coin-theft-resistance
  - **transaction-binding**
  - transaction-privacy

  assuming
  - hardness of computing discrete logarithms (and DDH for privacy)
  - range proofs are extractable (and zero-knowledge)
  - Schnorr is *simulation-sound* proof of knowledge of sk