

Universal Composable Transaction Serialization with Order Fairness

Michele Ciampi

The University of Edinburgh

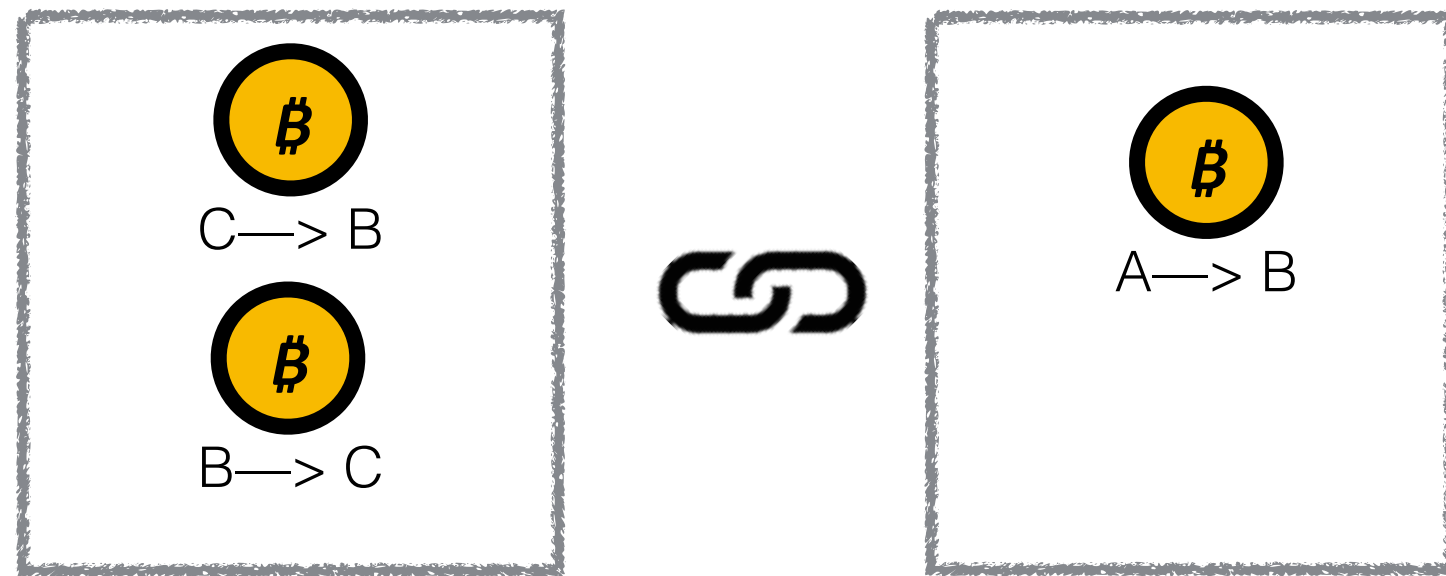
Aggelos Kiayias

University of Edinburgh
and IOG

Yu Shen

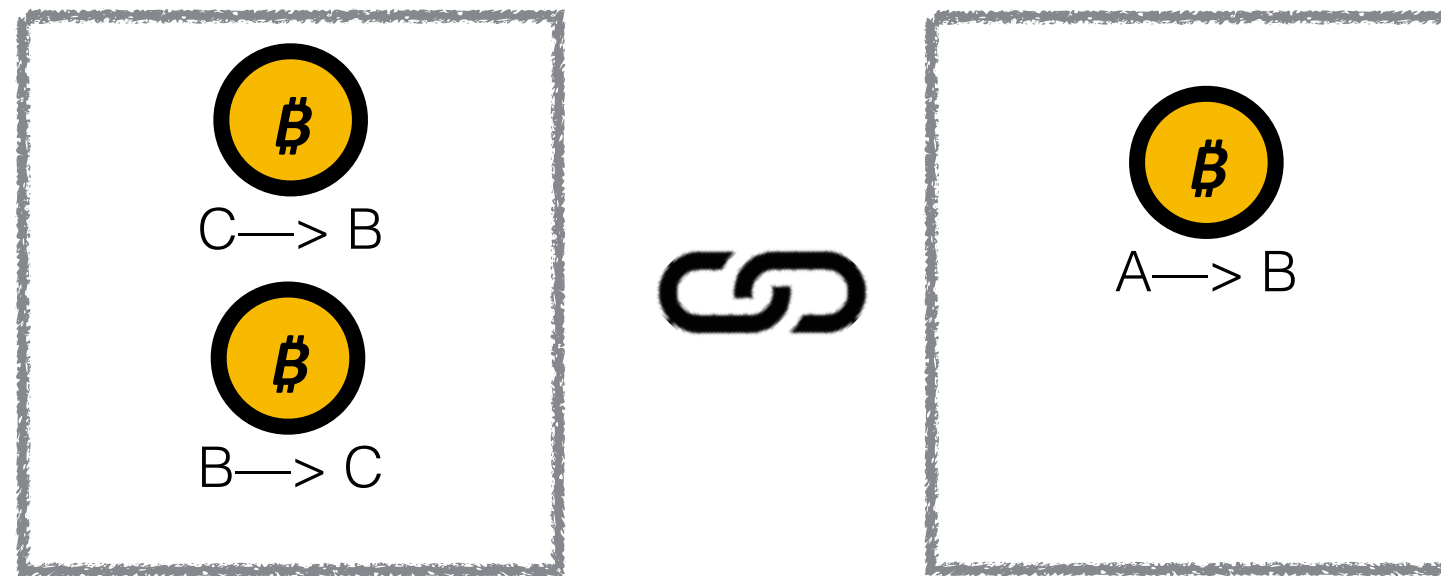
University of Edinburgh


Ledger consensus



Liveness
Consistency

Ledger consensus

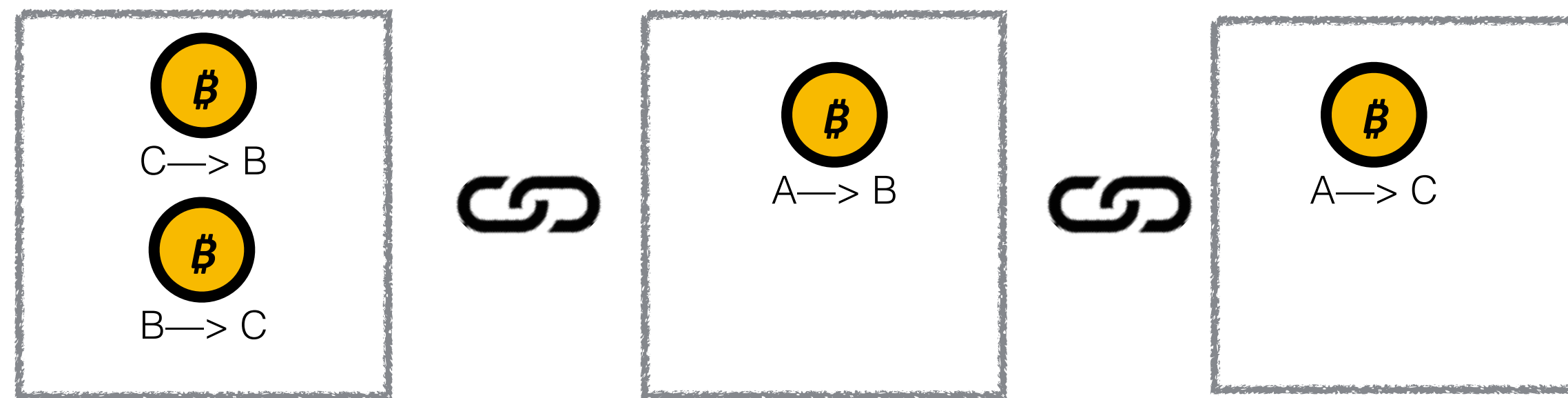




 $A \rightarrow C$



Liveness
Consistency

Ledger consensus

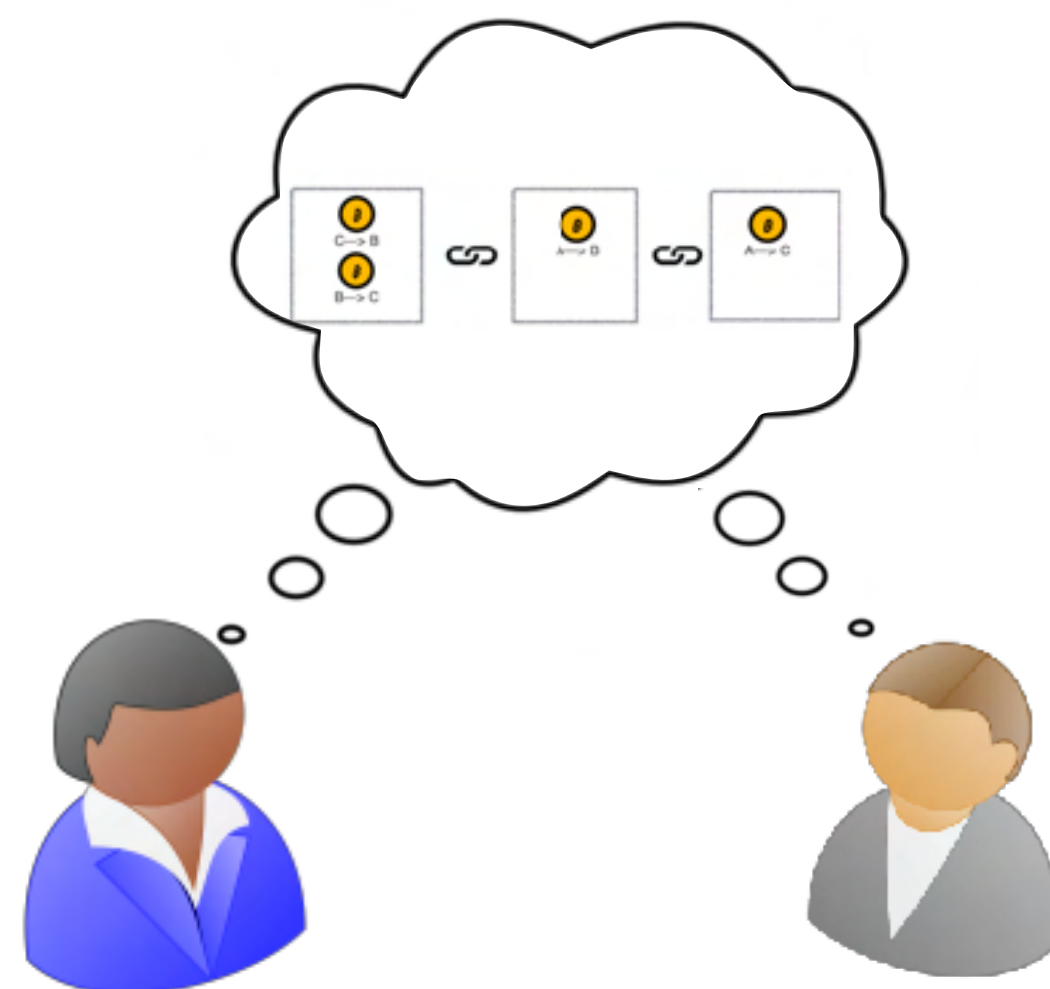
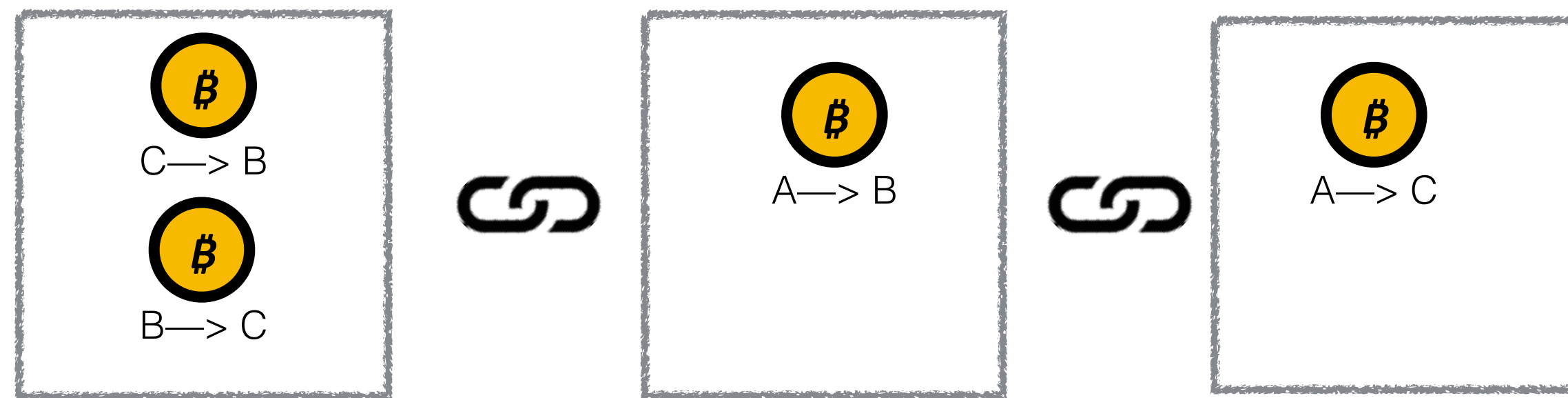



 $A \rightarrow C$



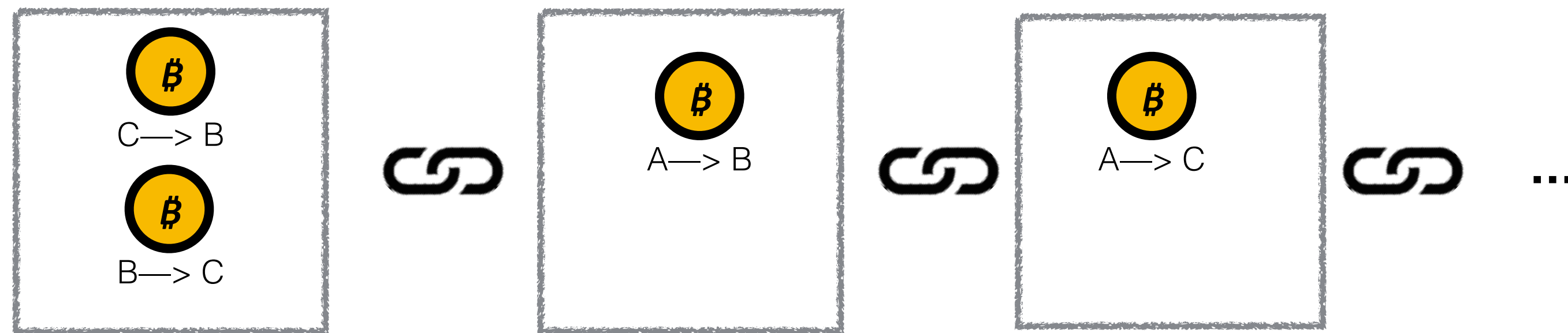
Liveness
Consistency


Ledger consensus




Liveness
Consistency

Ledger consensus



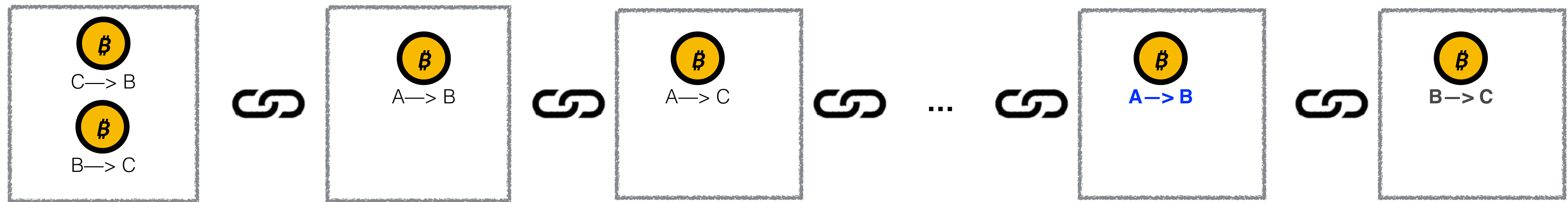
t_A 
 $A \rightarrow B$




t_B 
 $B \rightarrow C$




Ledger consensus



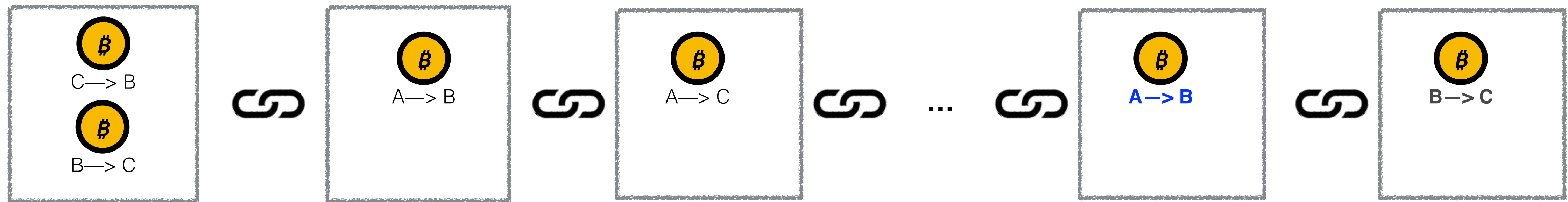
t_A 
A to B




t_B 
B to C




Ledger consensus




t_A




A → B




t_B




B → C

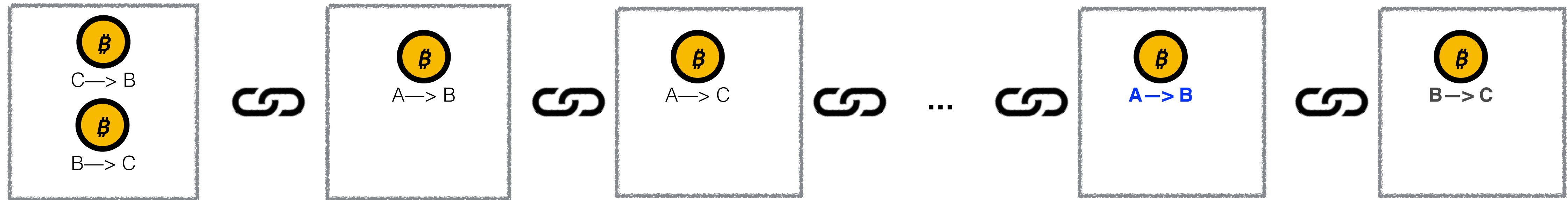



Dream property

If $t_A < t_B$ then  A → B


appears before  B → C

Ledger consensus




t_A 
A → B




t_B 
B → C

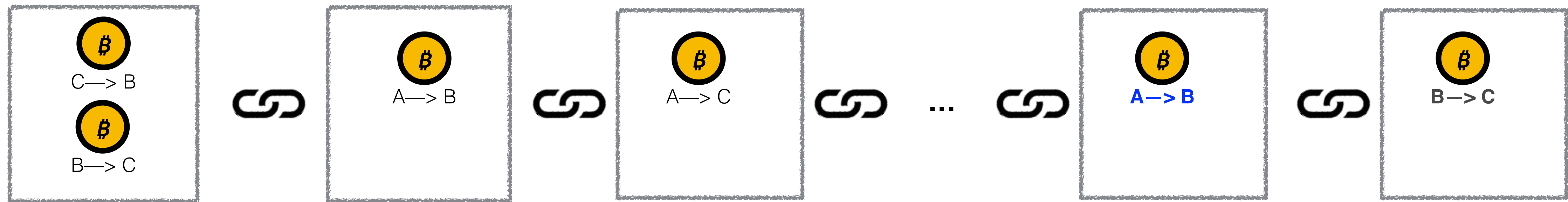



Dream property

If $t_A < t_B$ then 
A → B


appears before 
B → C

Ledger consensus



t_A 
A -> B



t_B 
B -> C

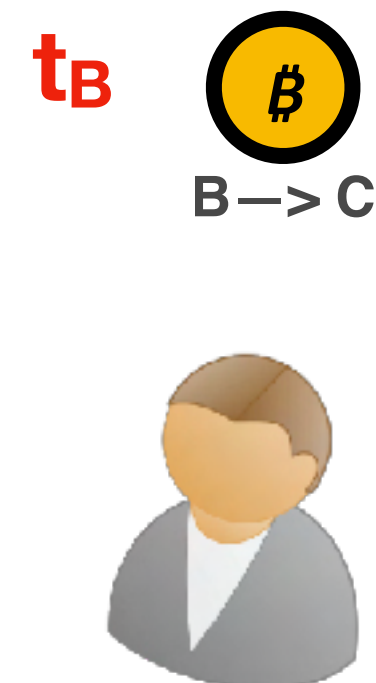
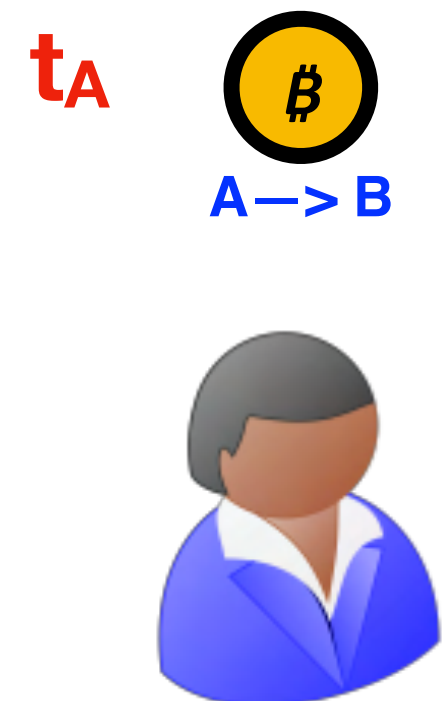
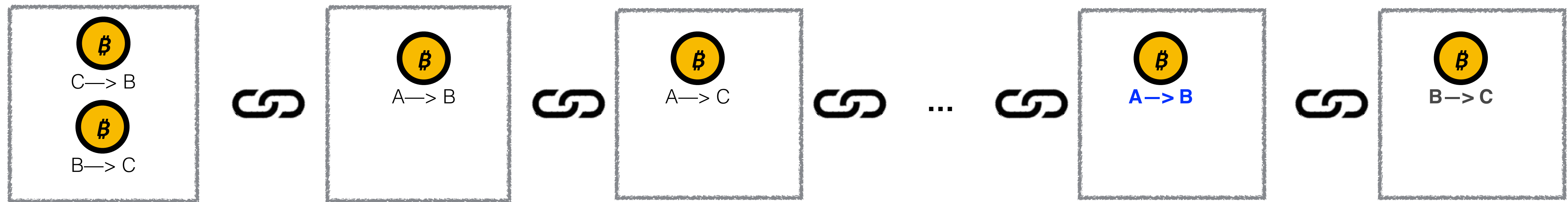


Dream property

If $t_A < t_B$ then 
A -> B
appears before 
B -> C

- Maximal Extractable Value (MEV)
- Critical issue in DeFi

Ledger consensus



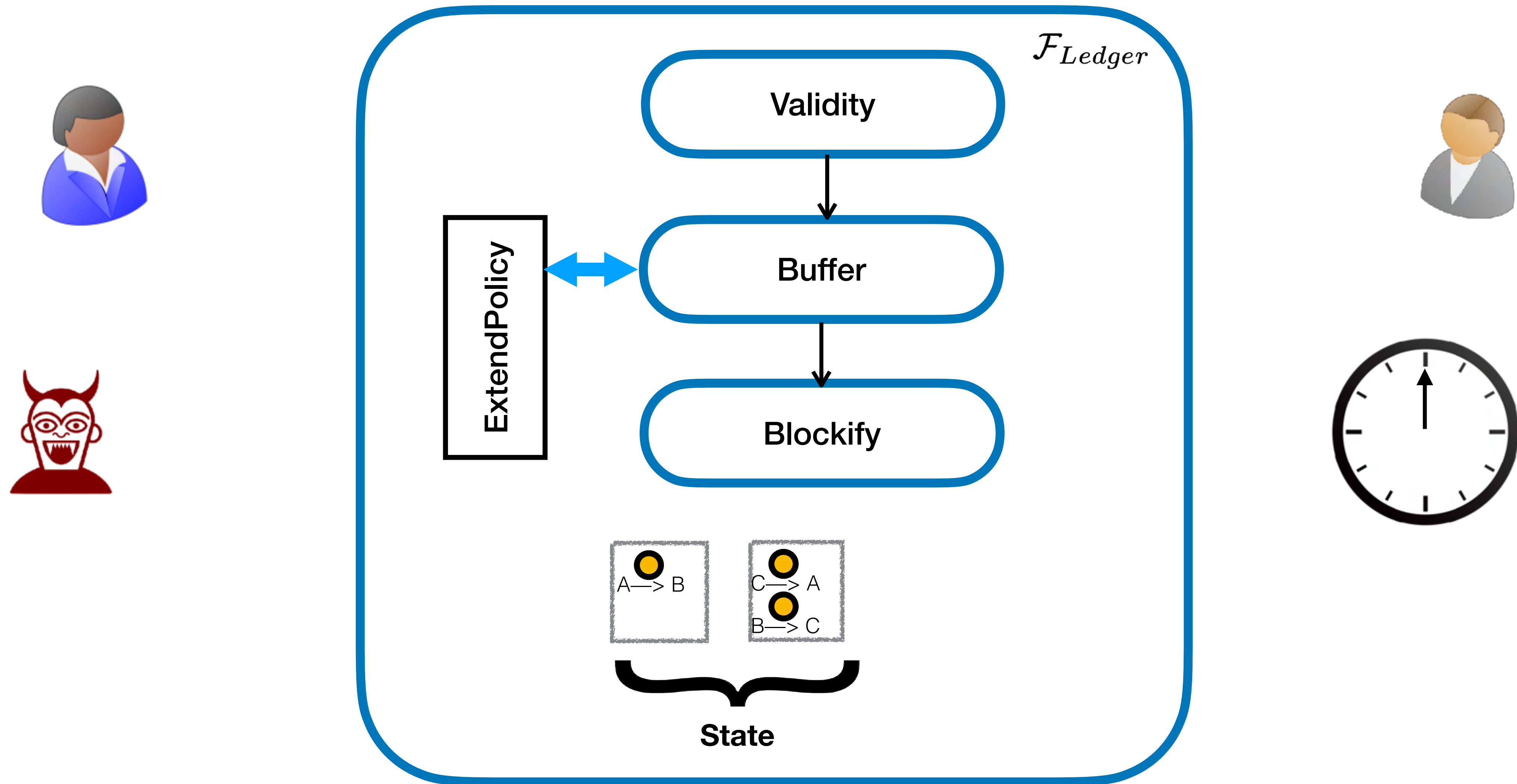
Dream property

If $t_A < t_B$ then  $A \rightarrow B$
appears before  $B \rightarrow C$

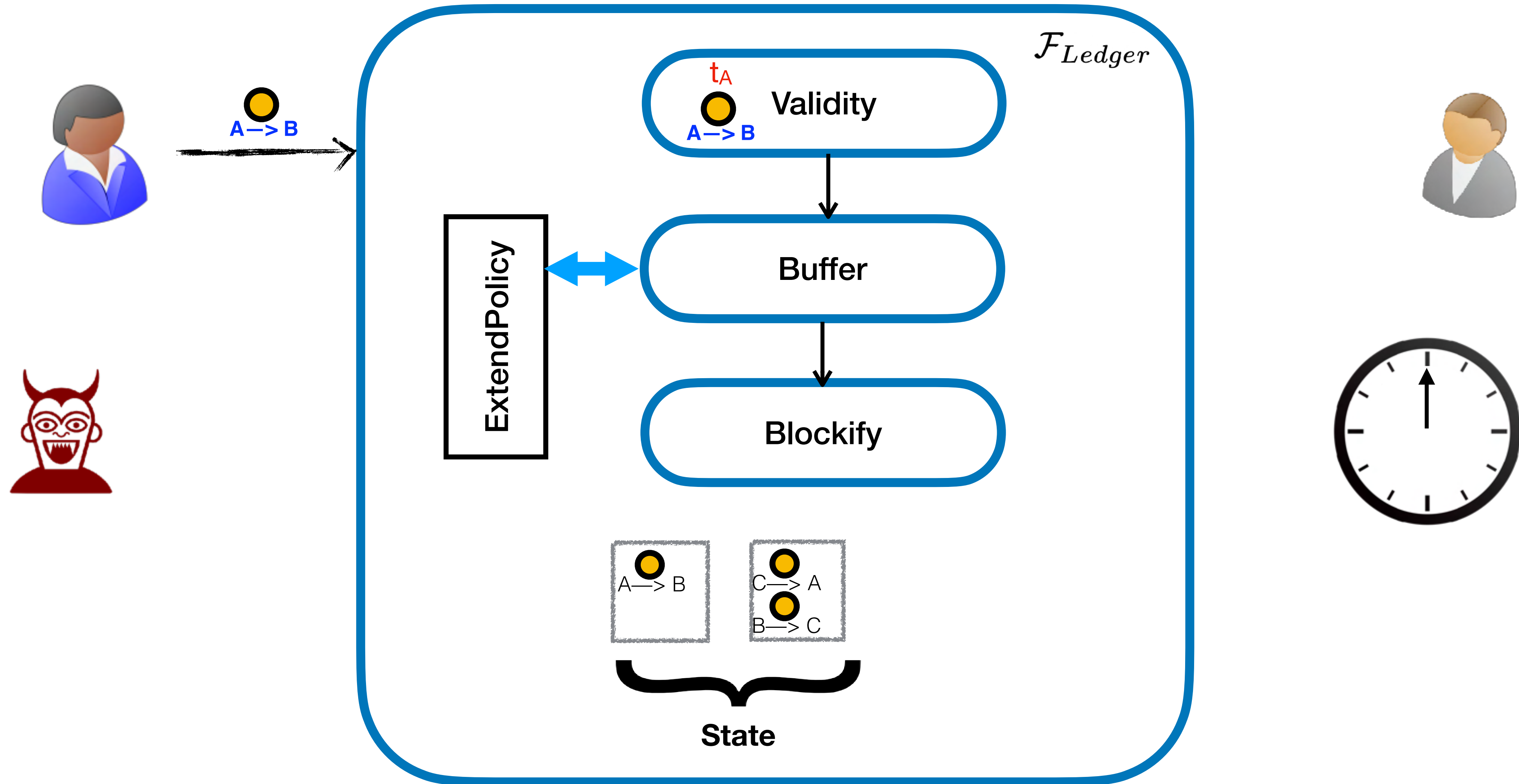
- Maximal Extractable Value (MEV)
- Critical issue in DeFi

- How do we formalize this property in UC?
- Can we live the dream?
- What can we realistically achieve?

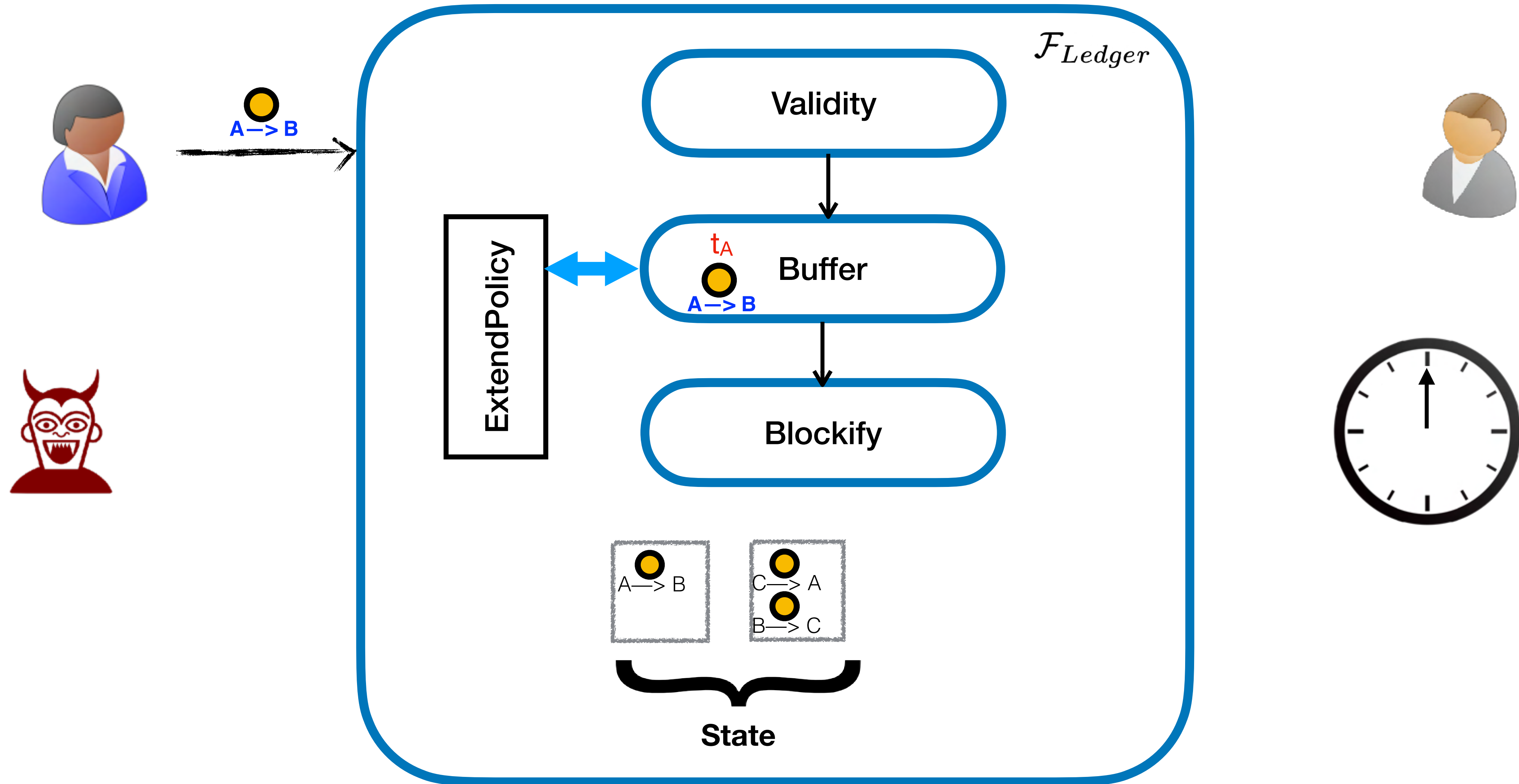
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



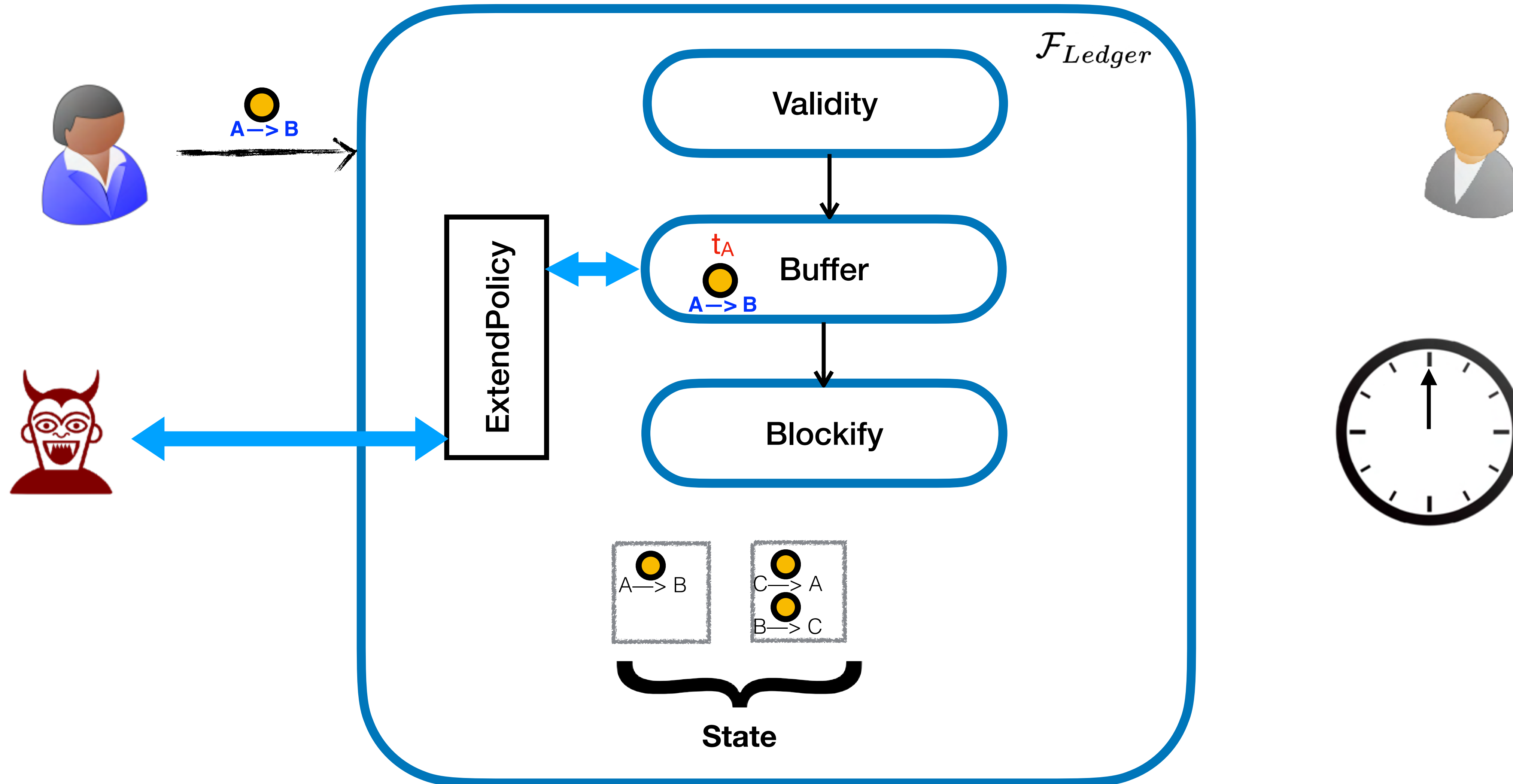
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



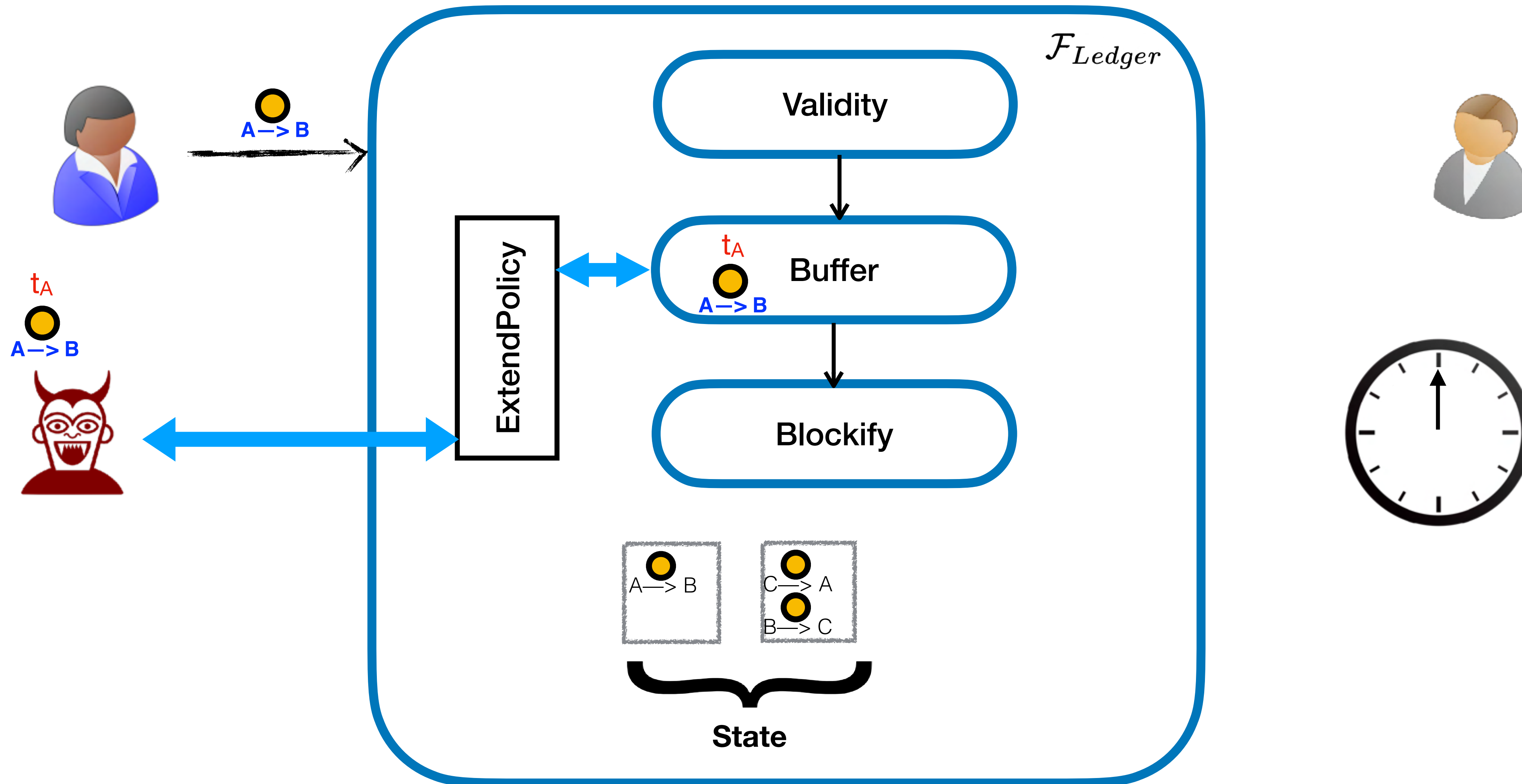
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



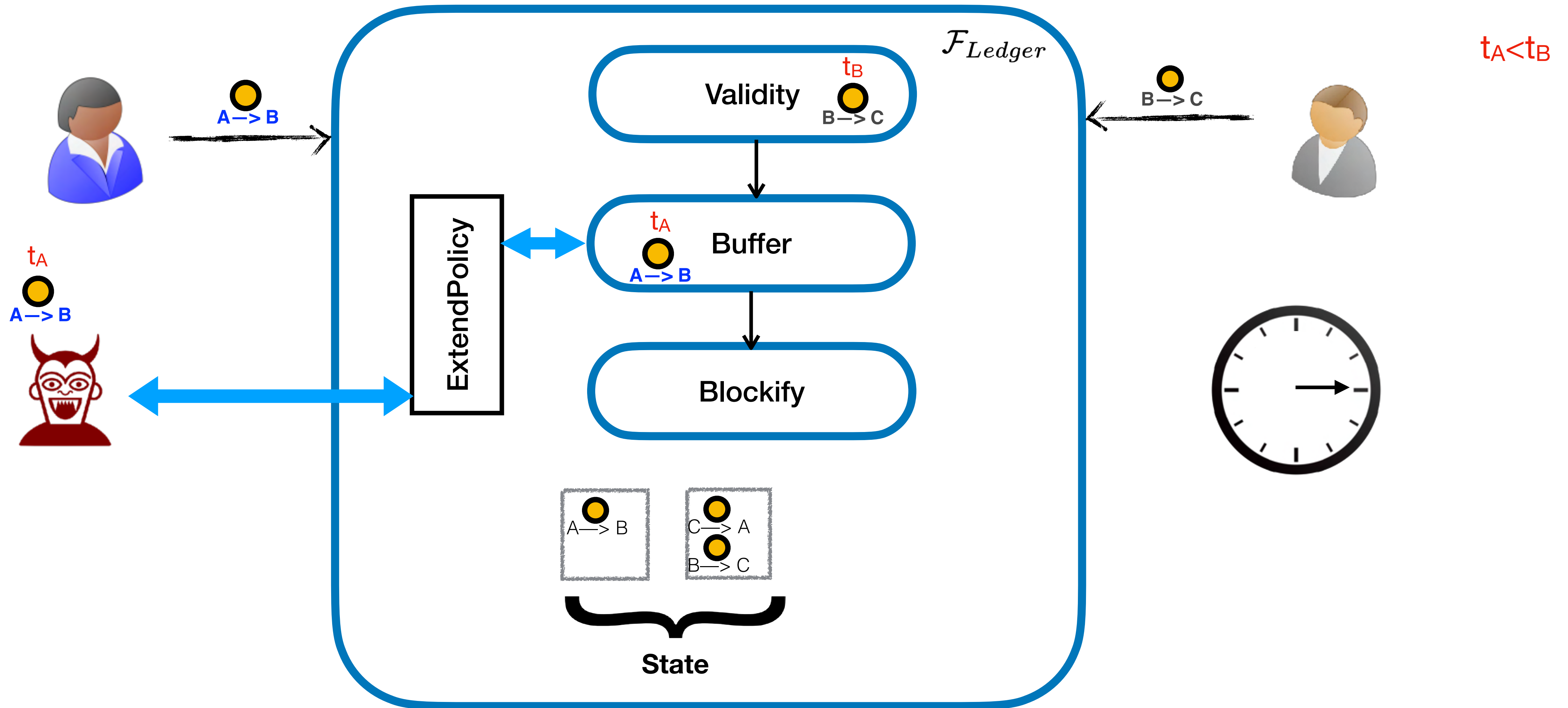
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



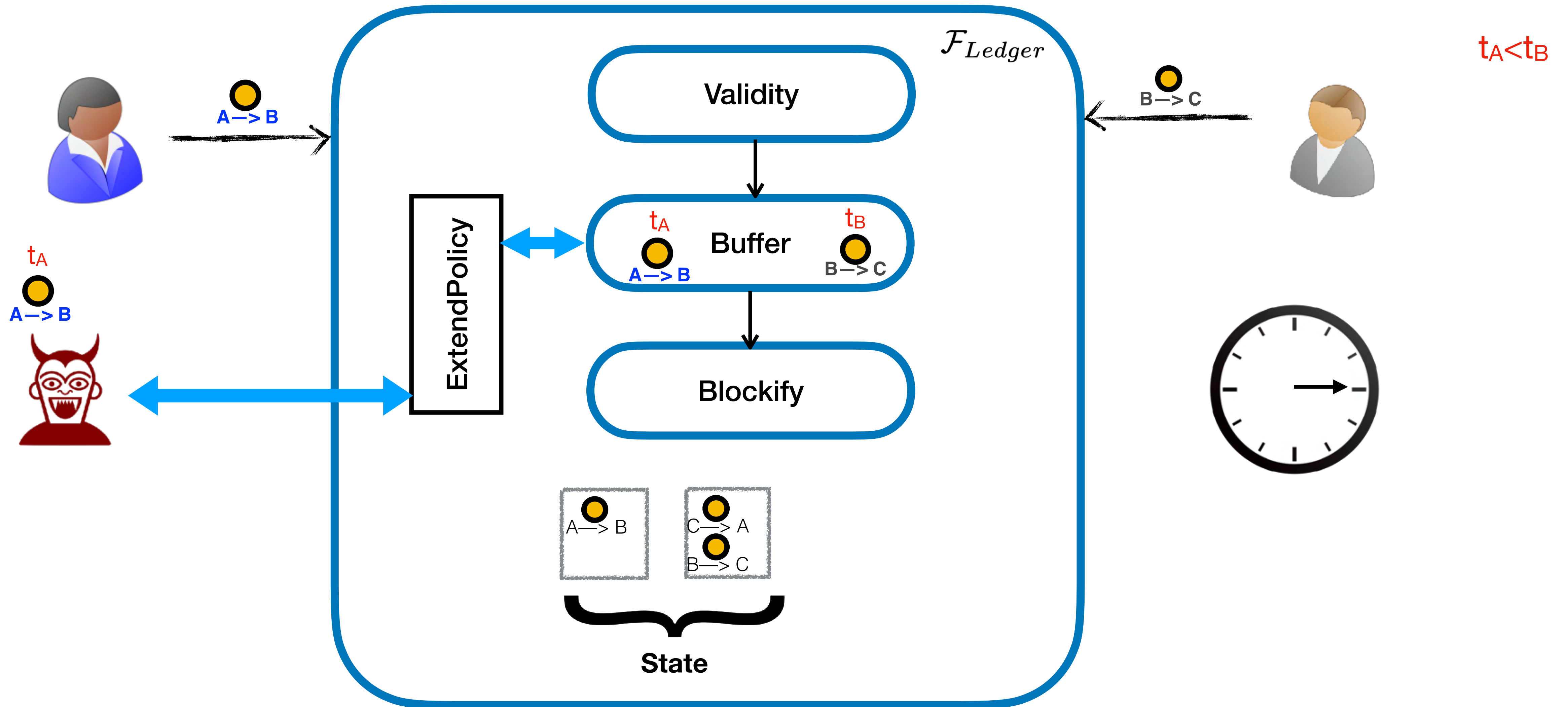
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



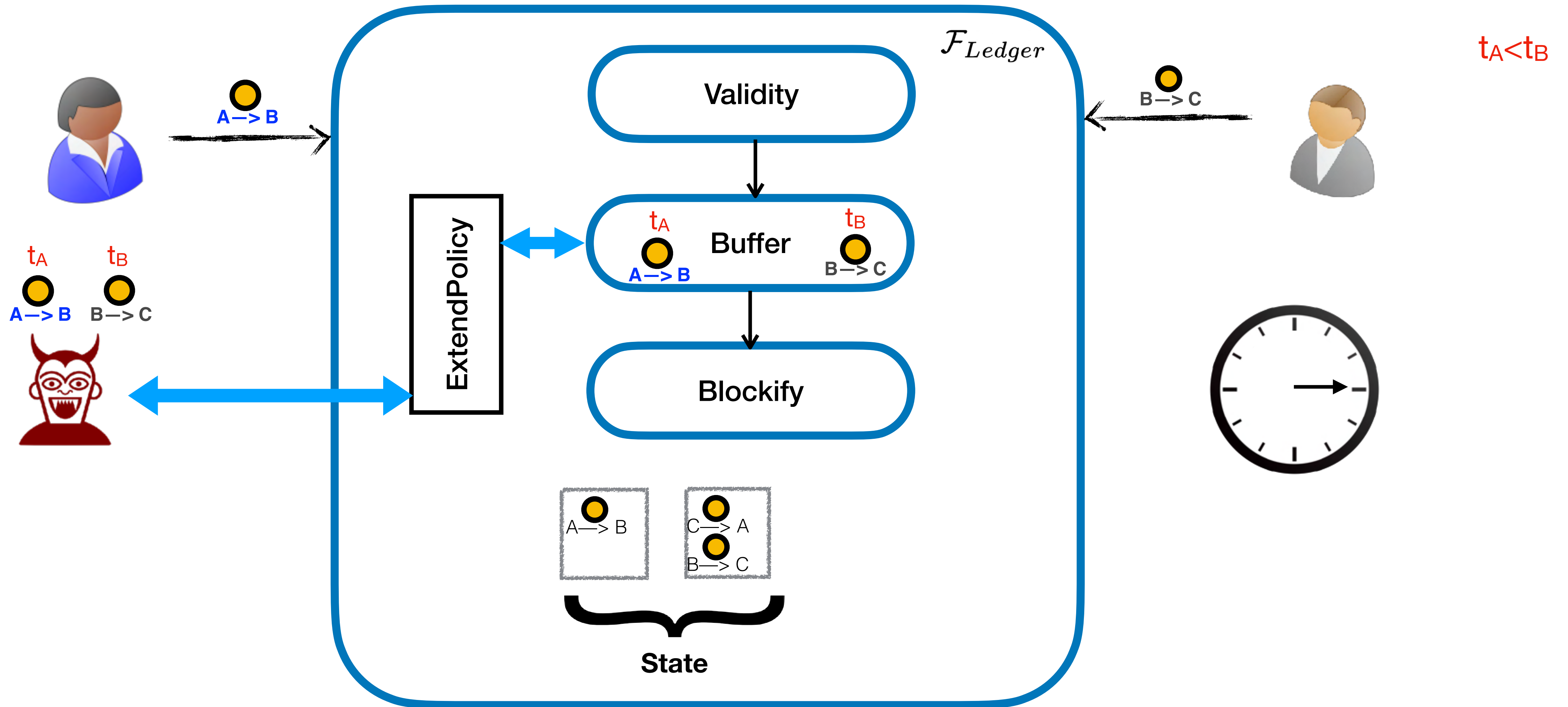
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



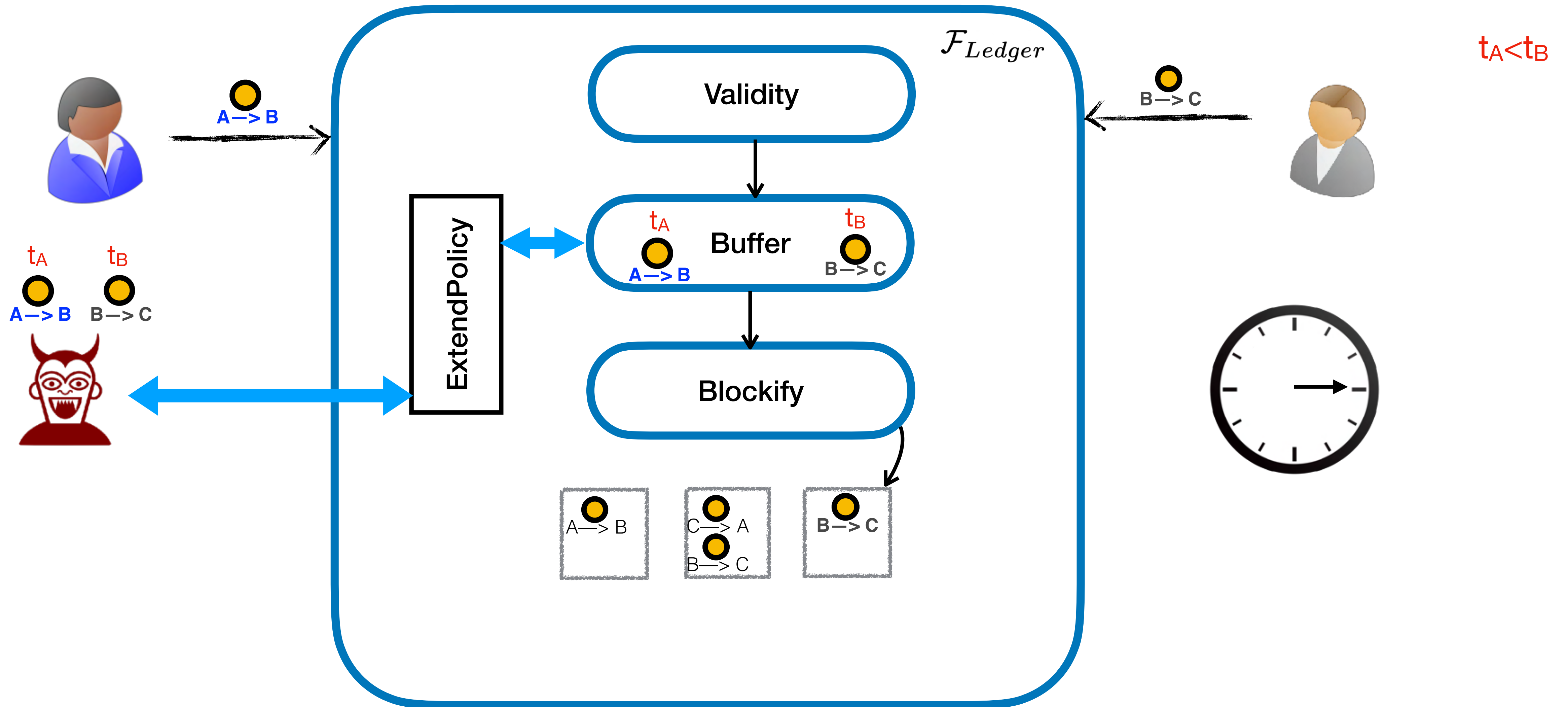
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



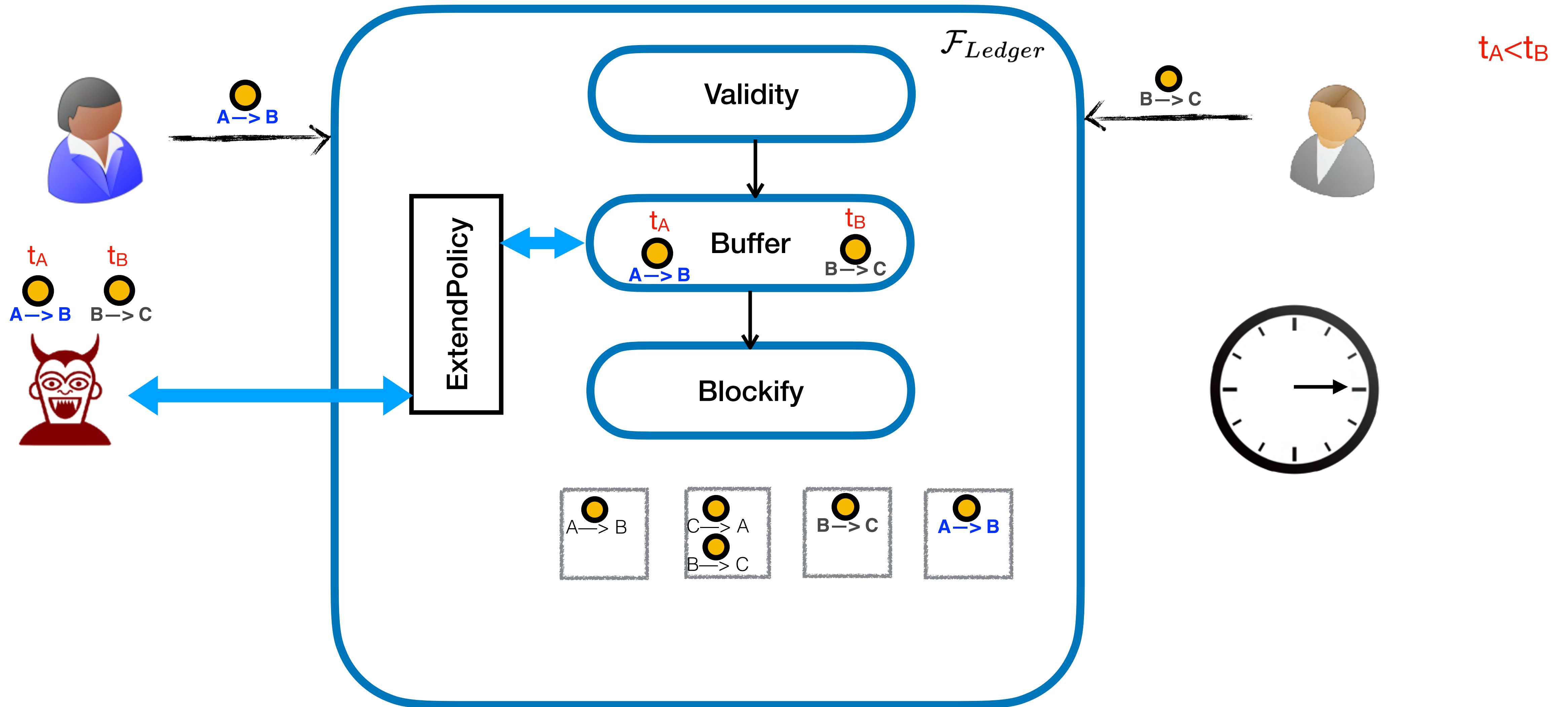
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



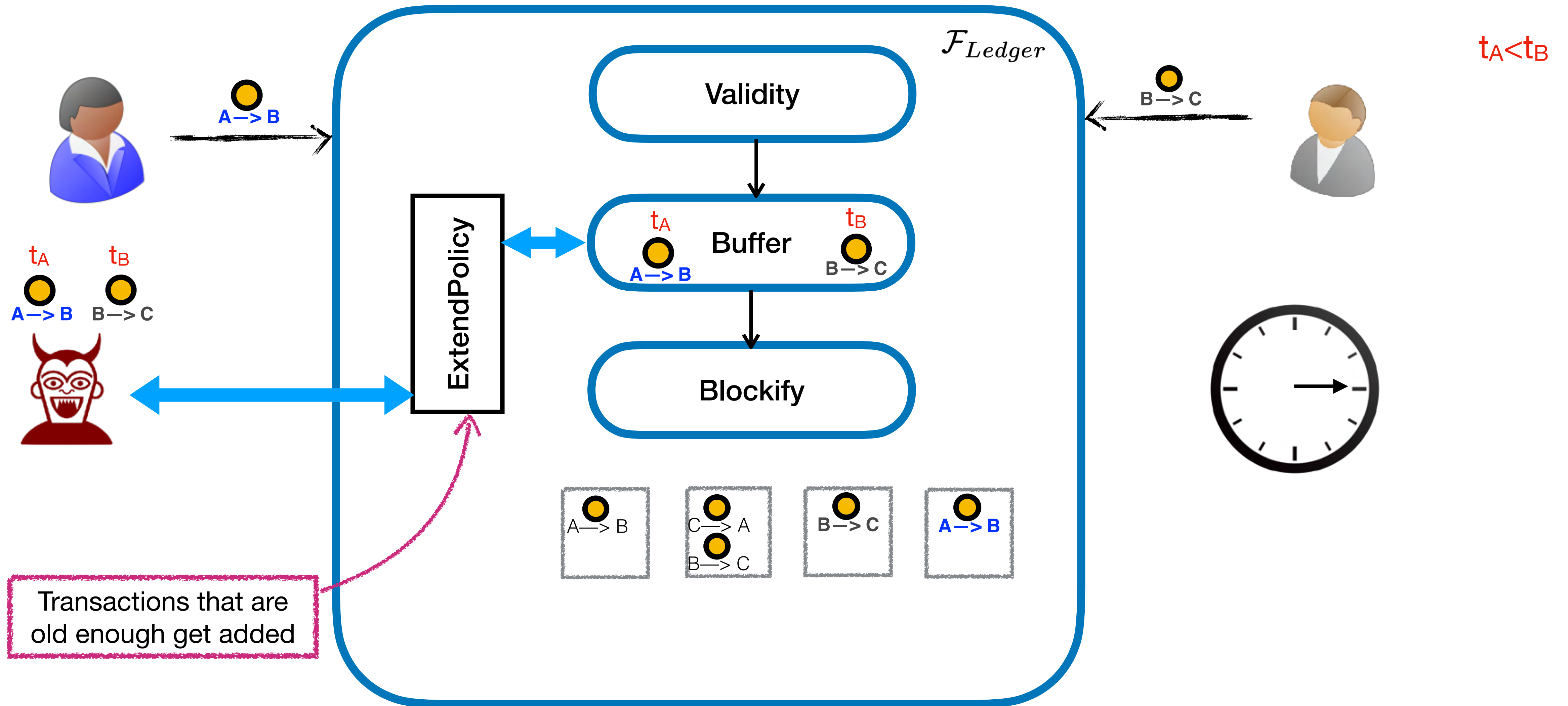
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



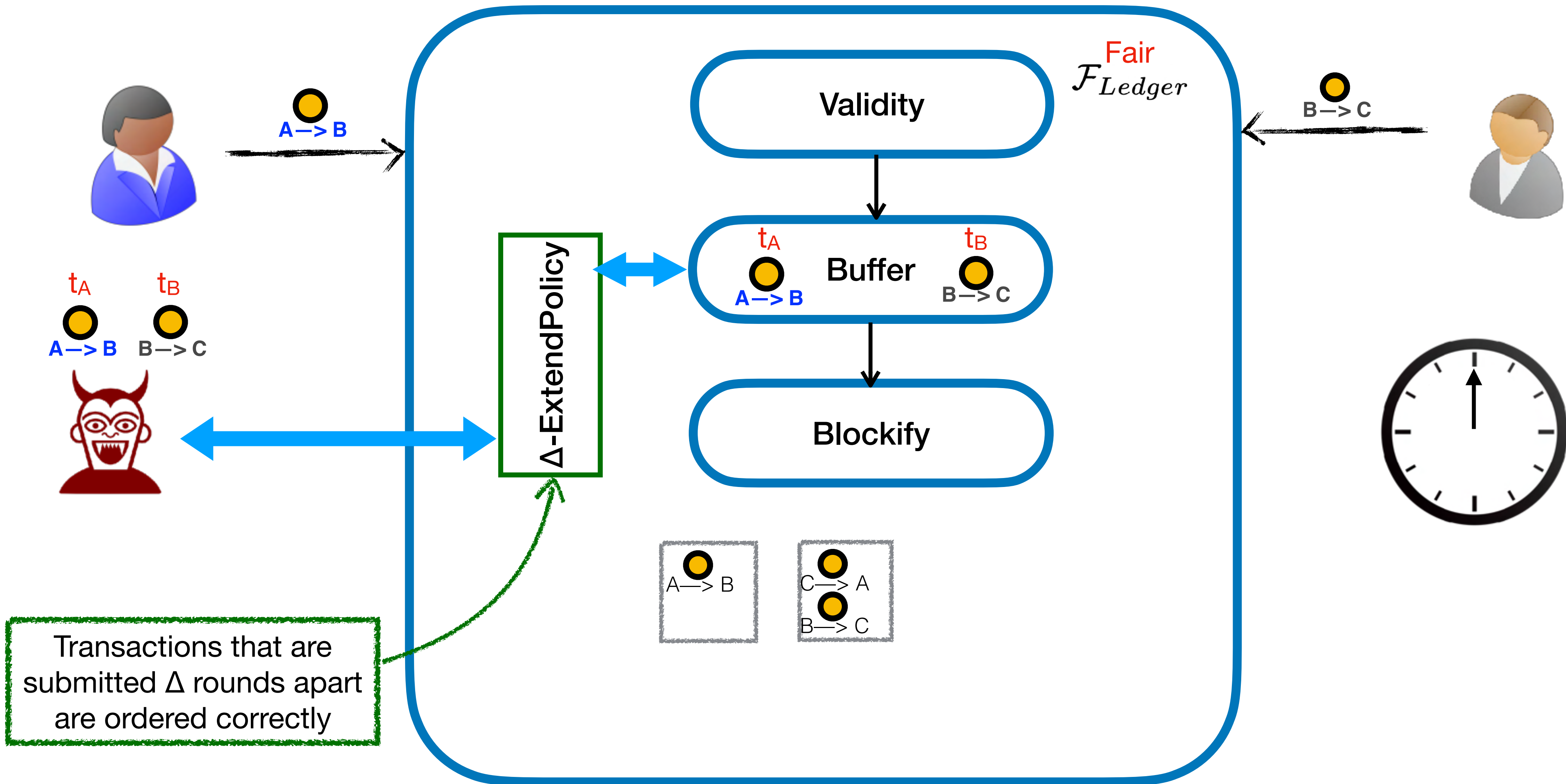
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



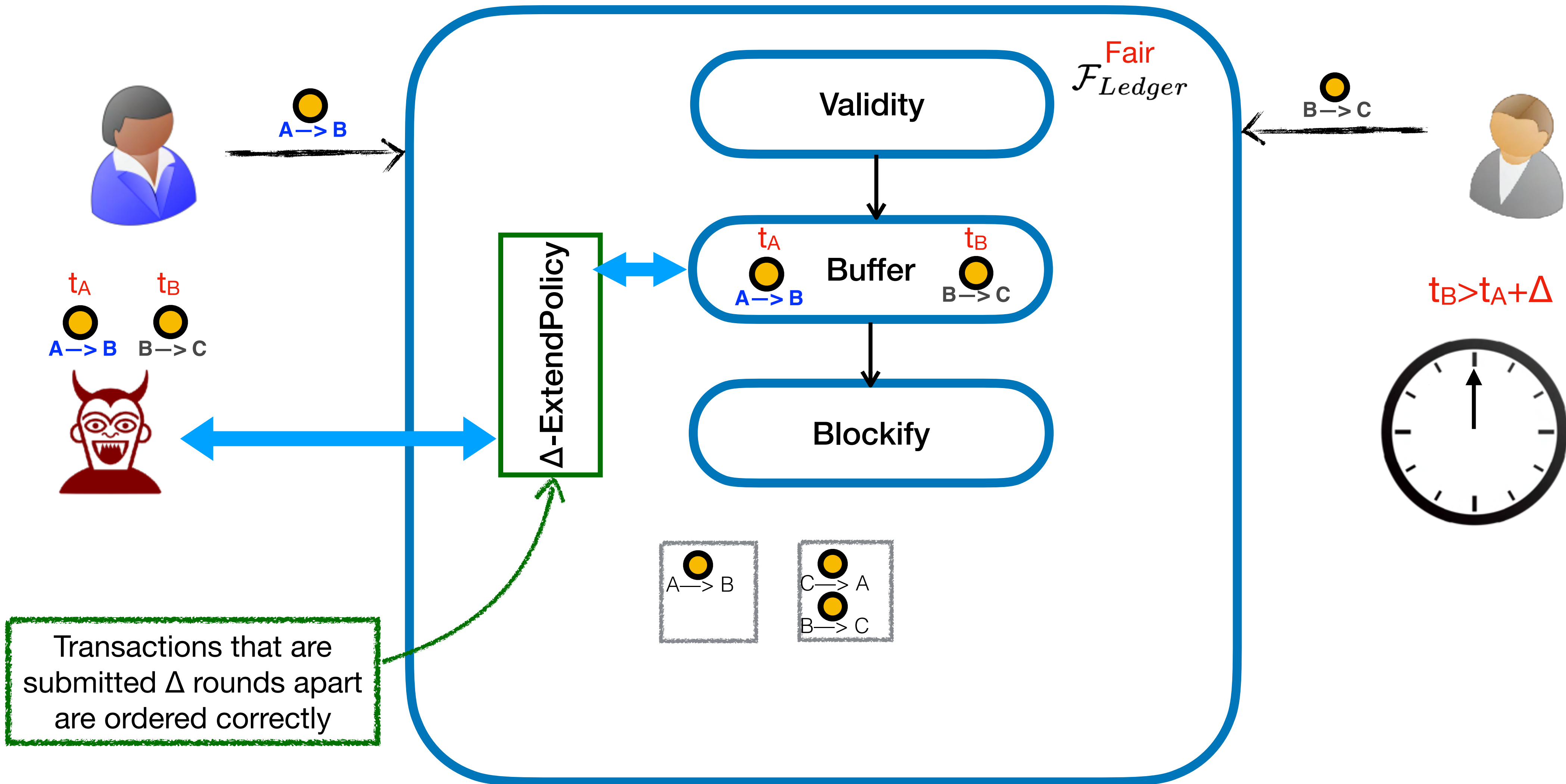
Starting Point: Ledger Functionality \mathcal{F}_{Ledger} [BMTZ17]



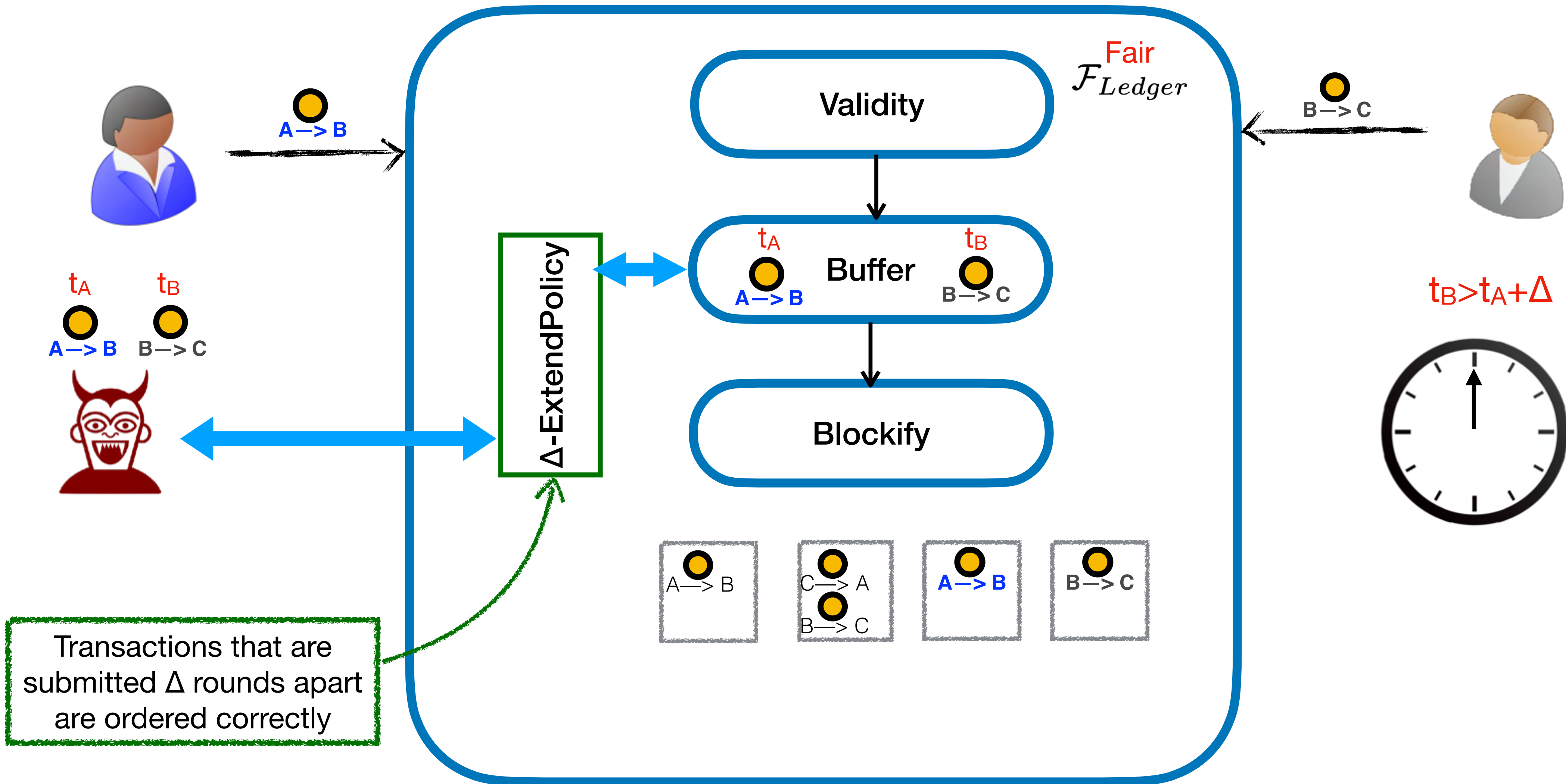
New Ledger Functionality $\mathcal{F}_{Ledger}^{Fair}$



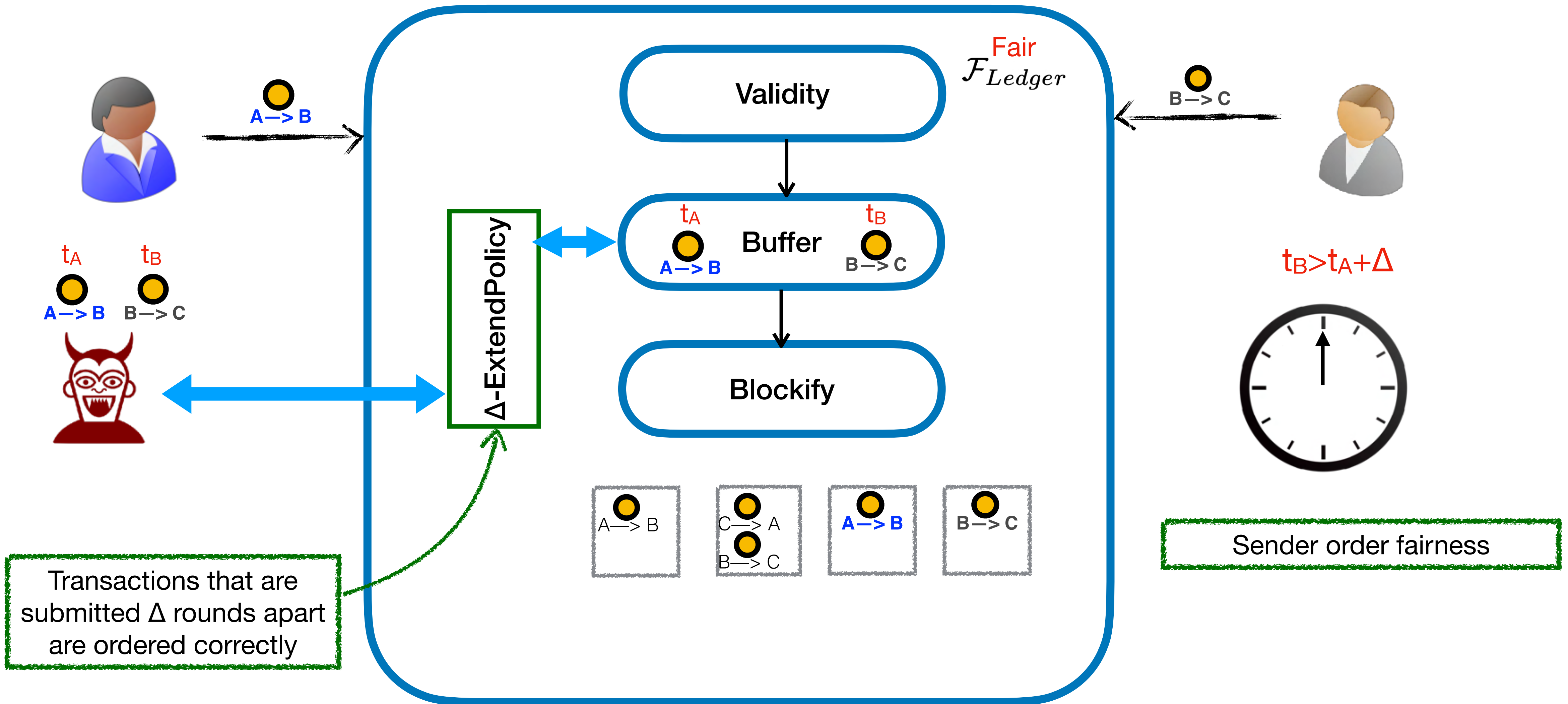
New Ledger Functionality $\mathcal{F}_{Ledge}^{Fair}$



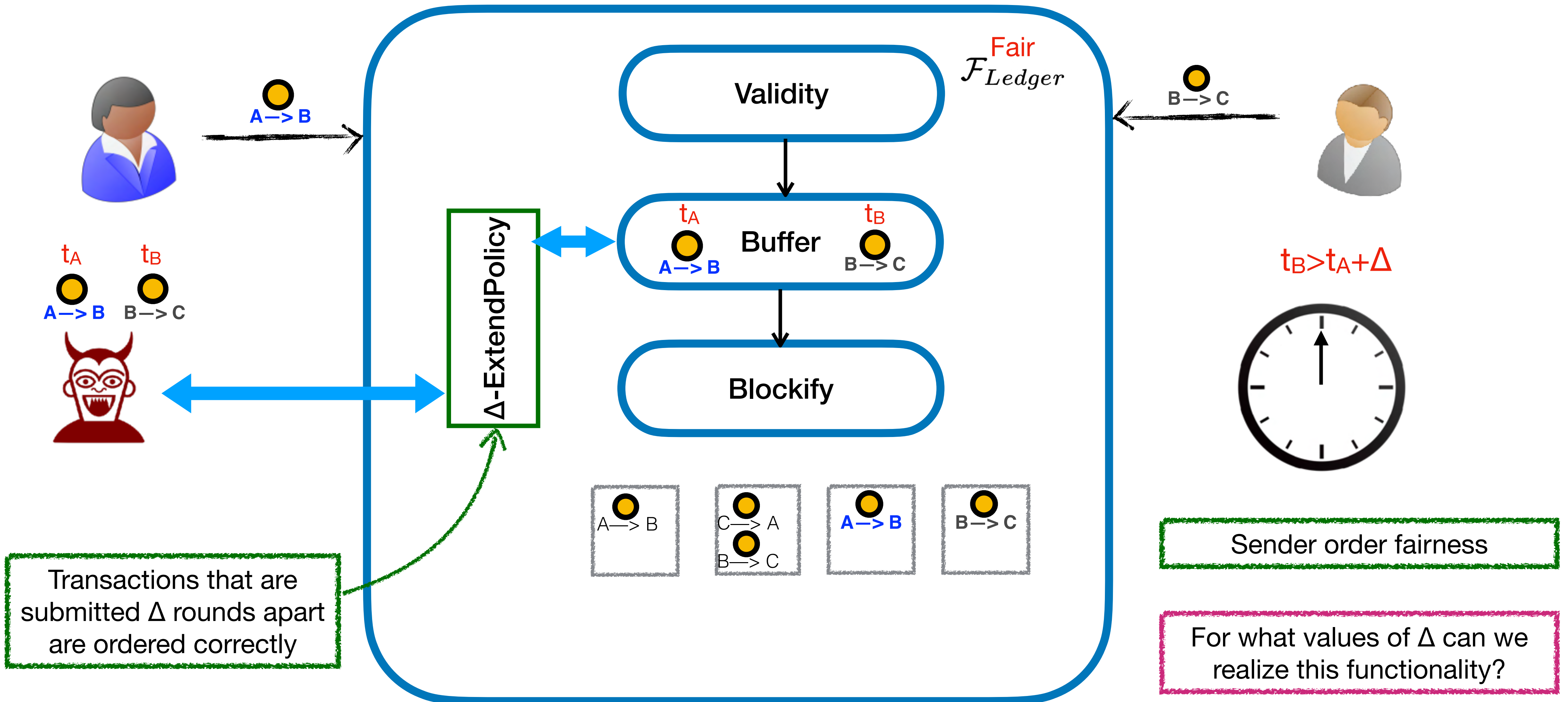
New Ledger Functionality $\mathcal{F}_{Ledger}^{Fair}$



New Ledger Functionality $\mathcal{F}_{Ledger}^{Fair}$

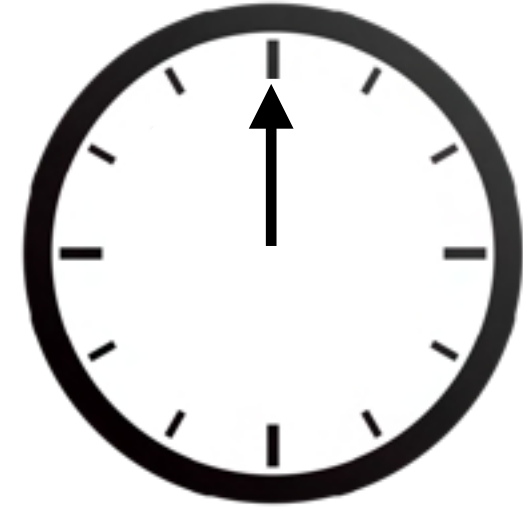


New Ledger Functionality $\mathcal{F}_{Ledger}^{Fair}$



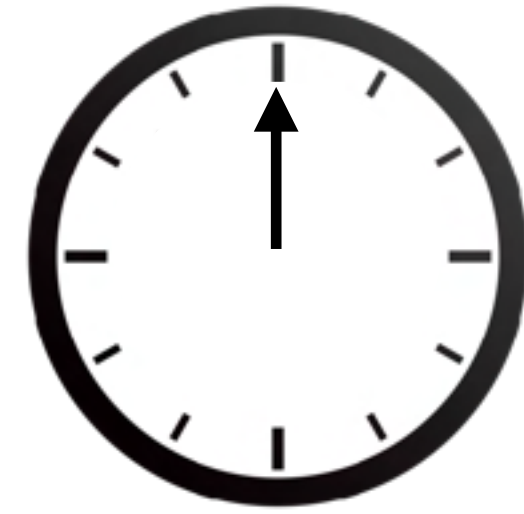
Communication network

$\mathcal{F}_{\text{Diffuse}}^K$



Communication network

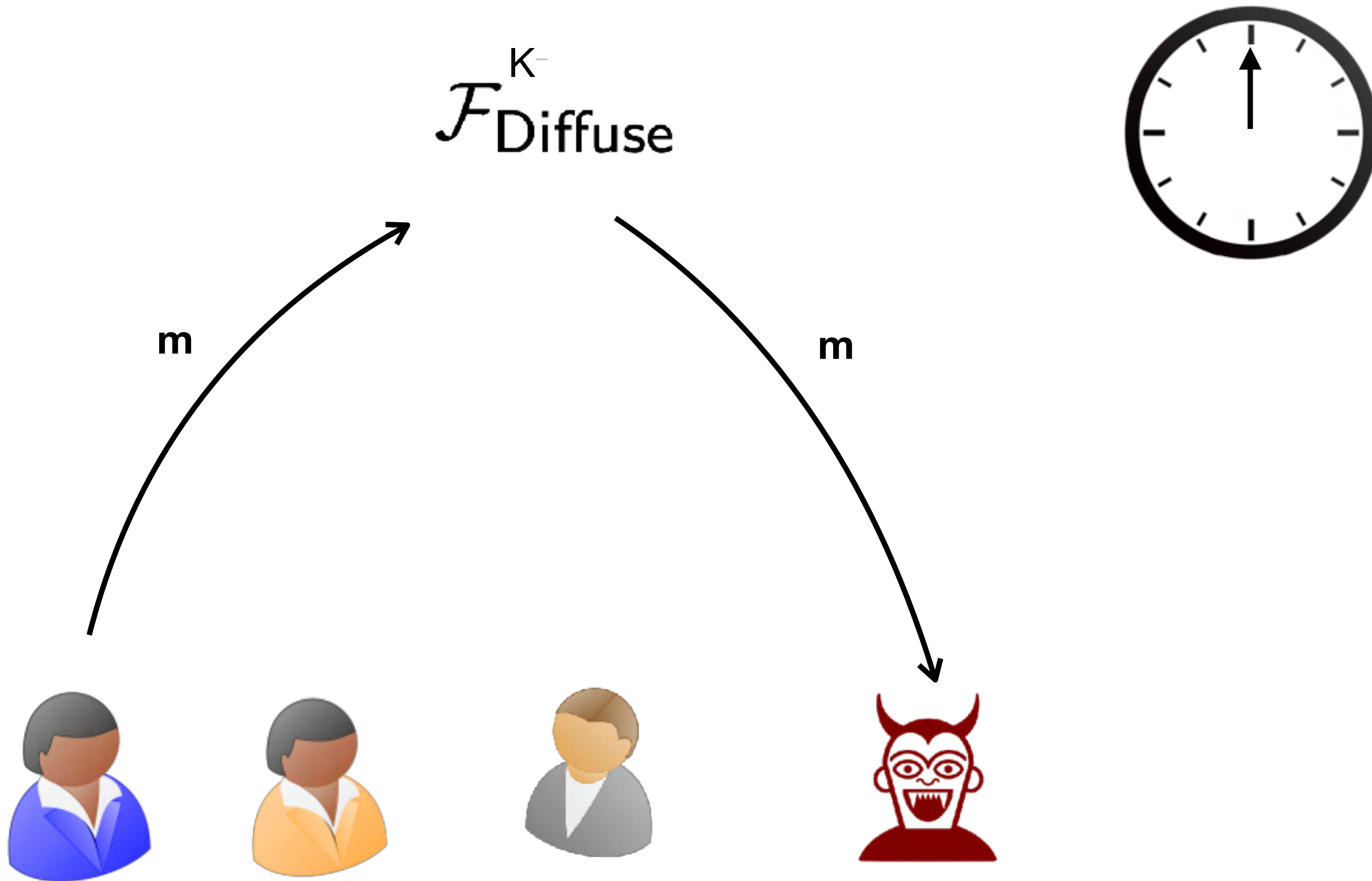
$\mathcal{F}_{\text{Diffuse}}^K$



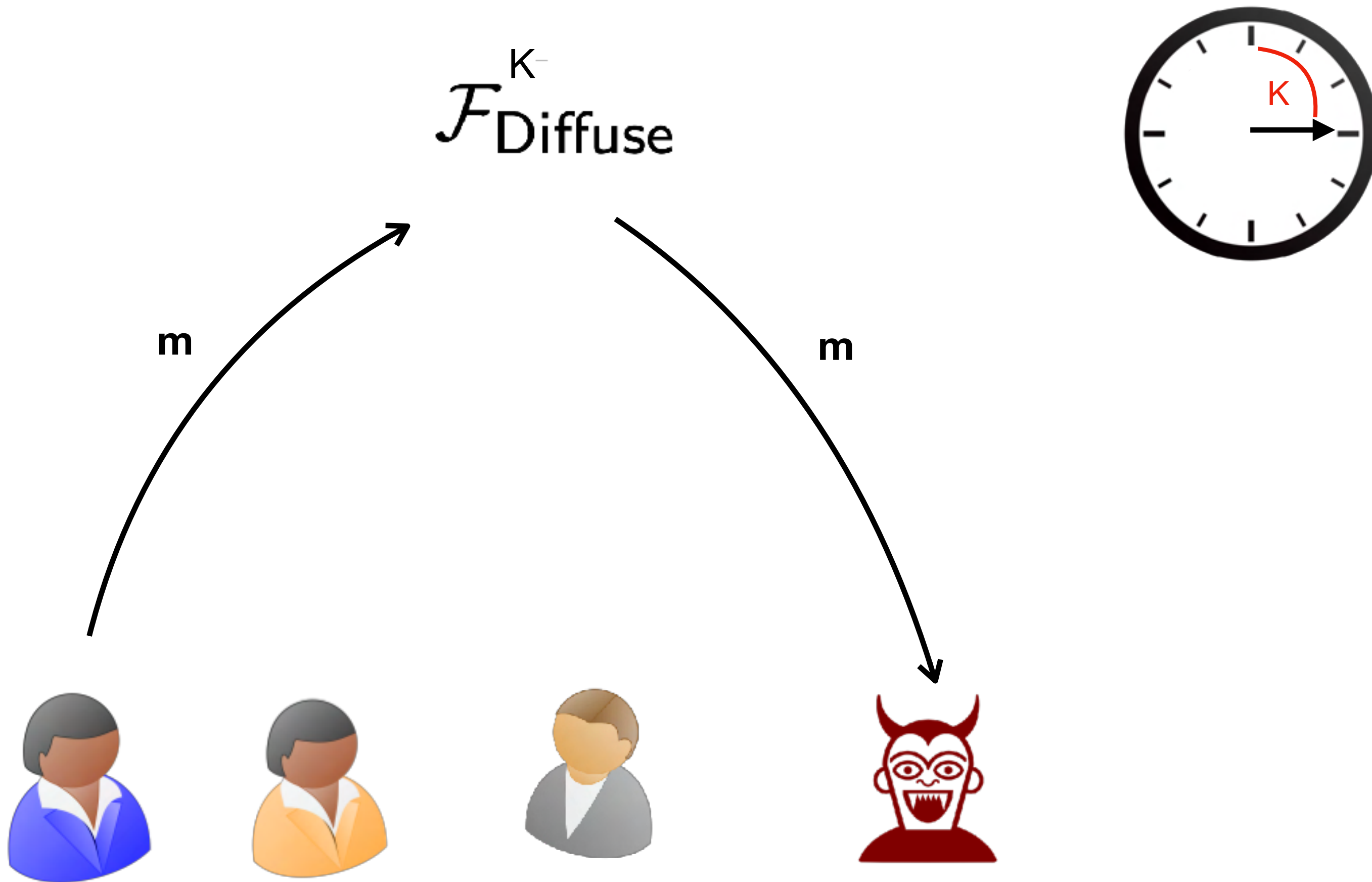
m



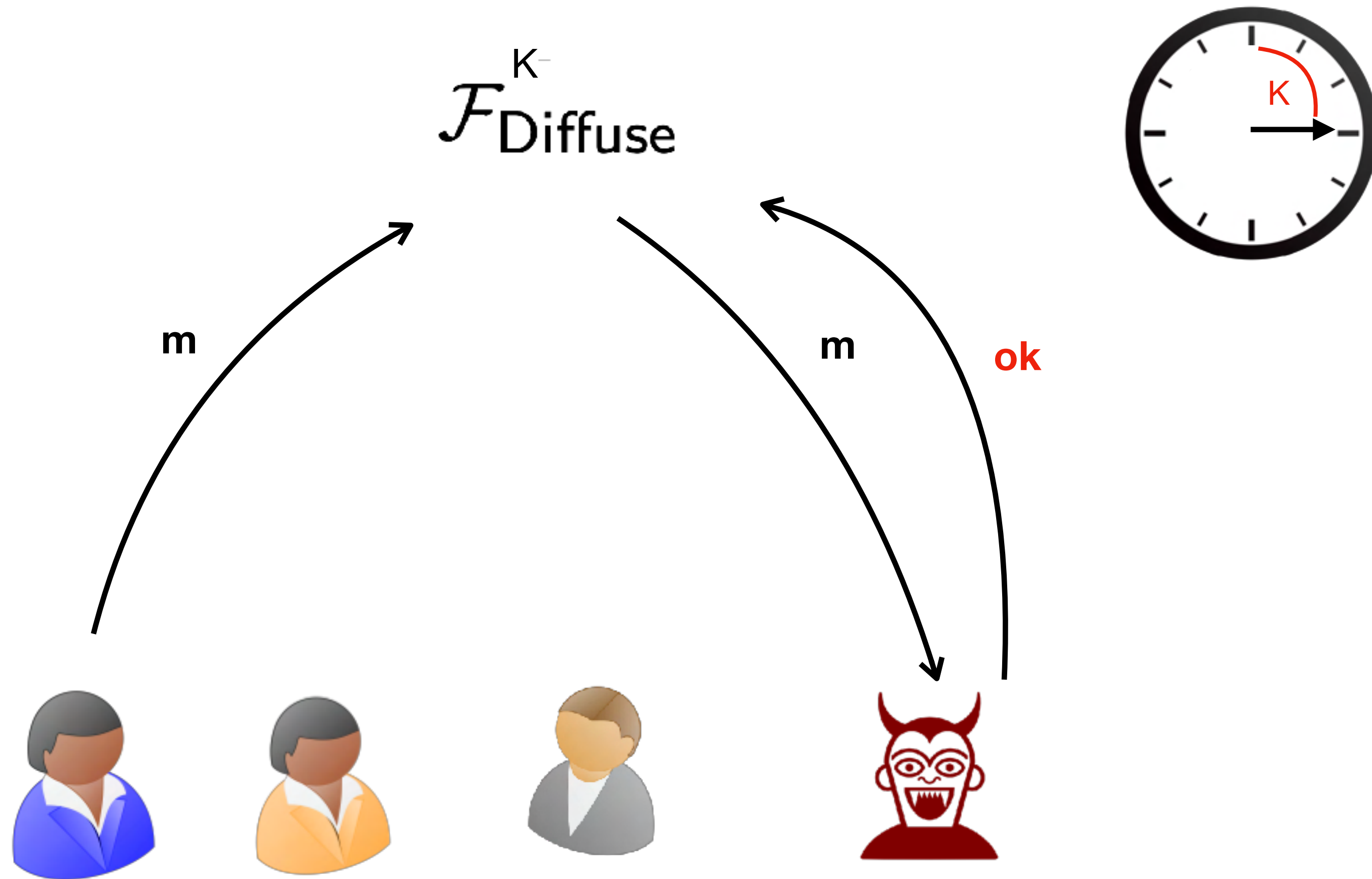
Communication network



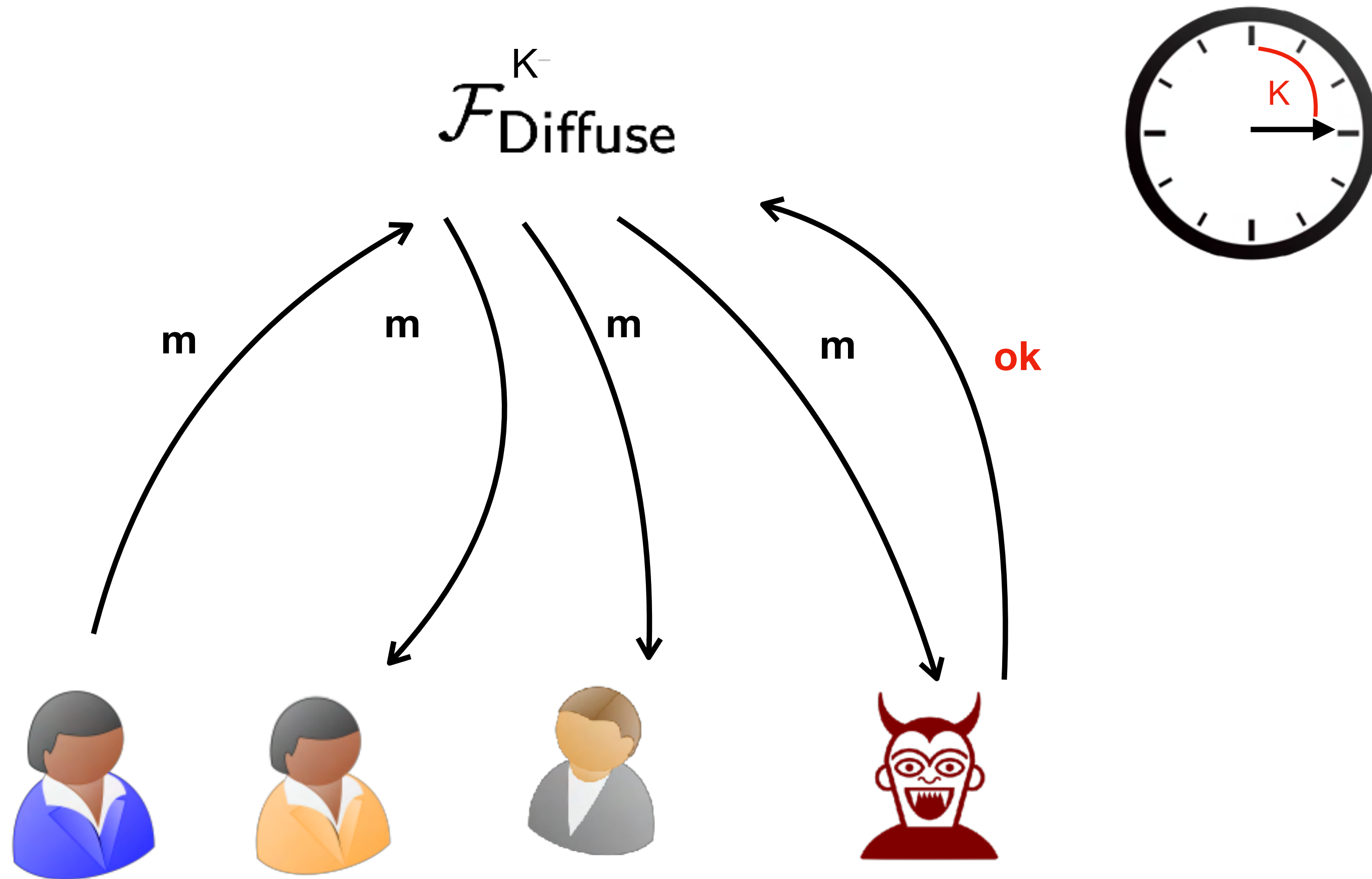
Communication network



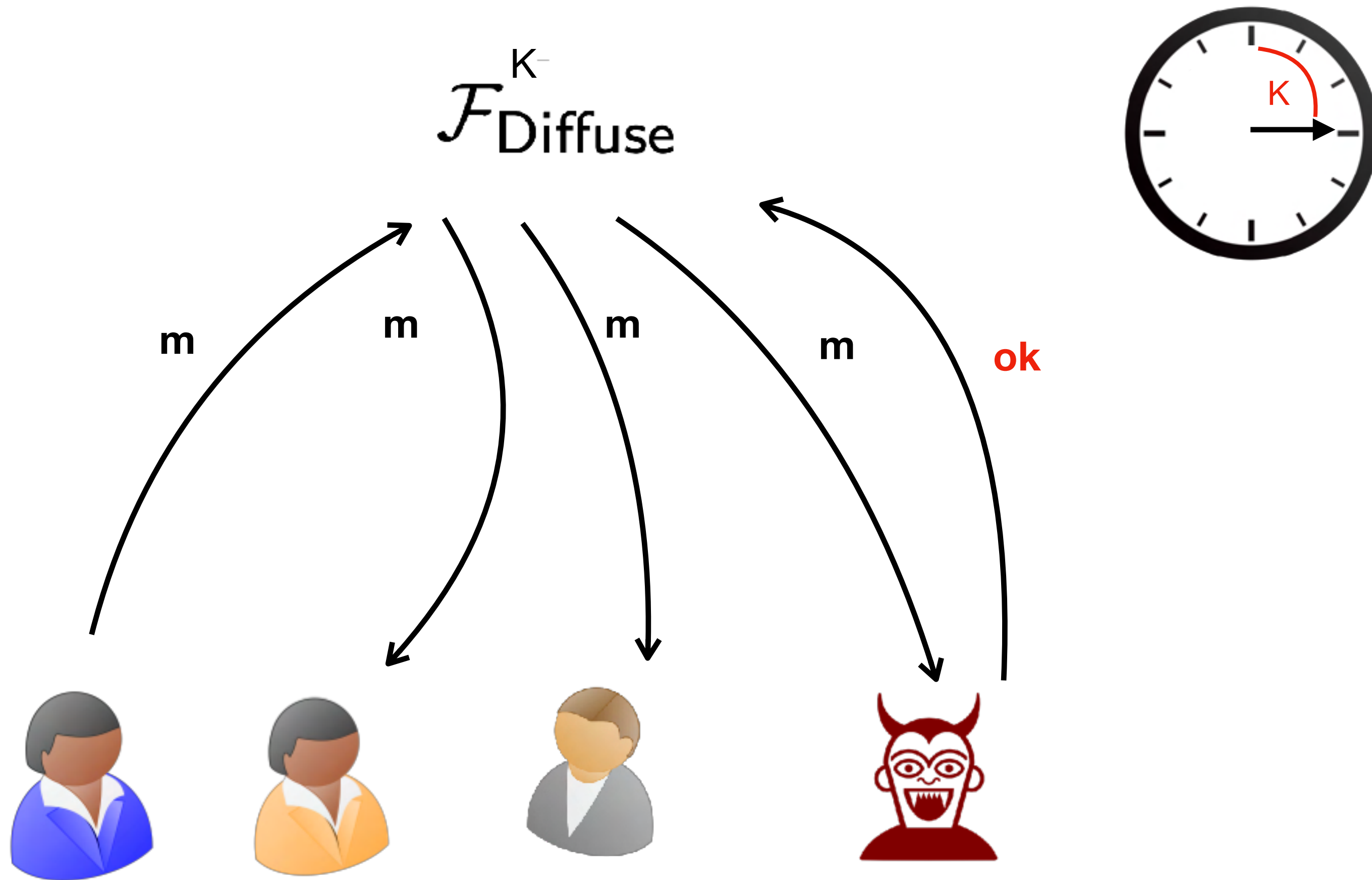
Communication network



Communication network

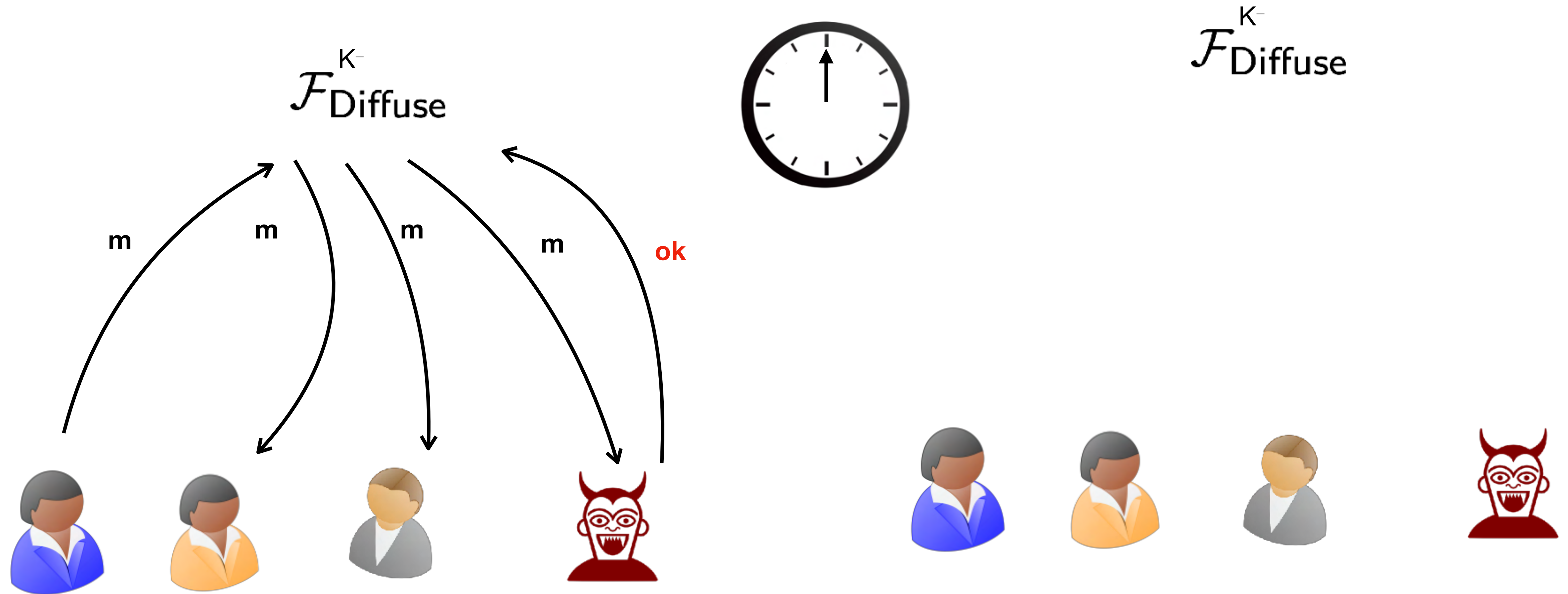


Communication network



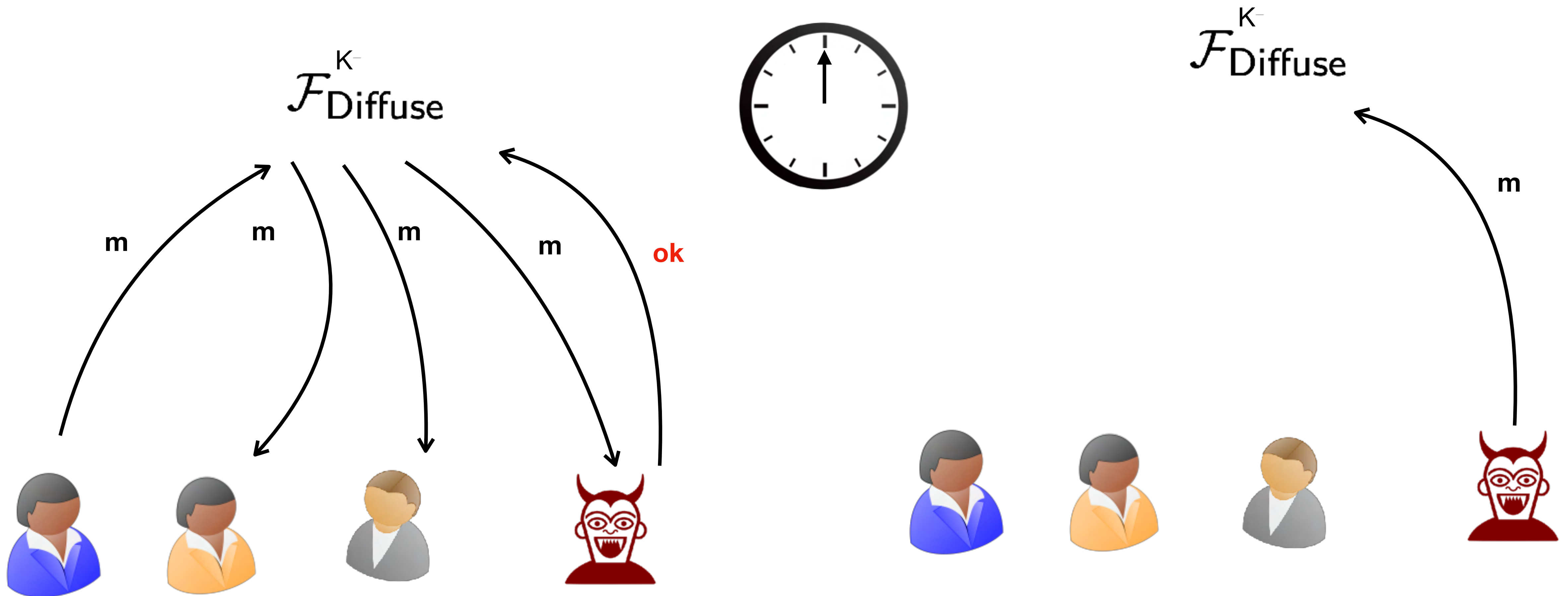
The adversary can always delay honest parties messages

Communication network



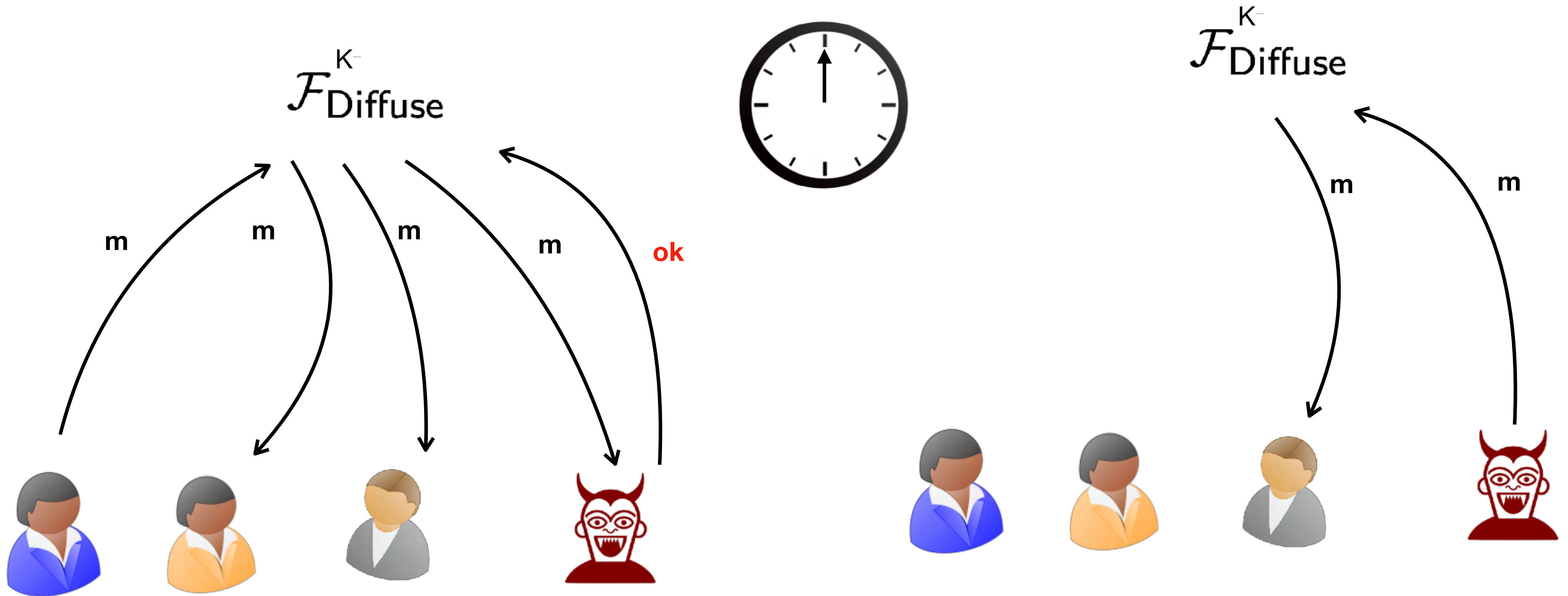
The adversary can always delay honest parties messages

Communication network



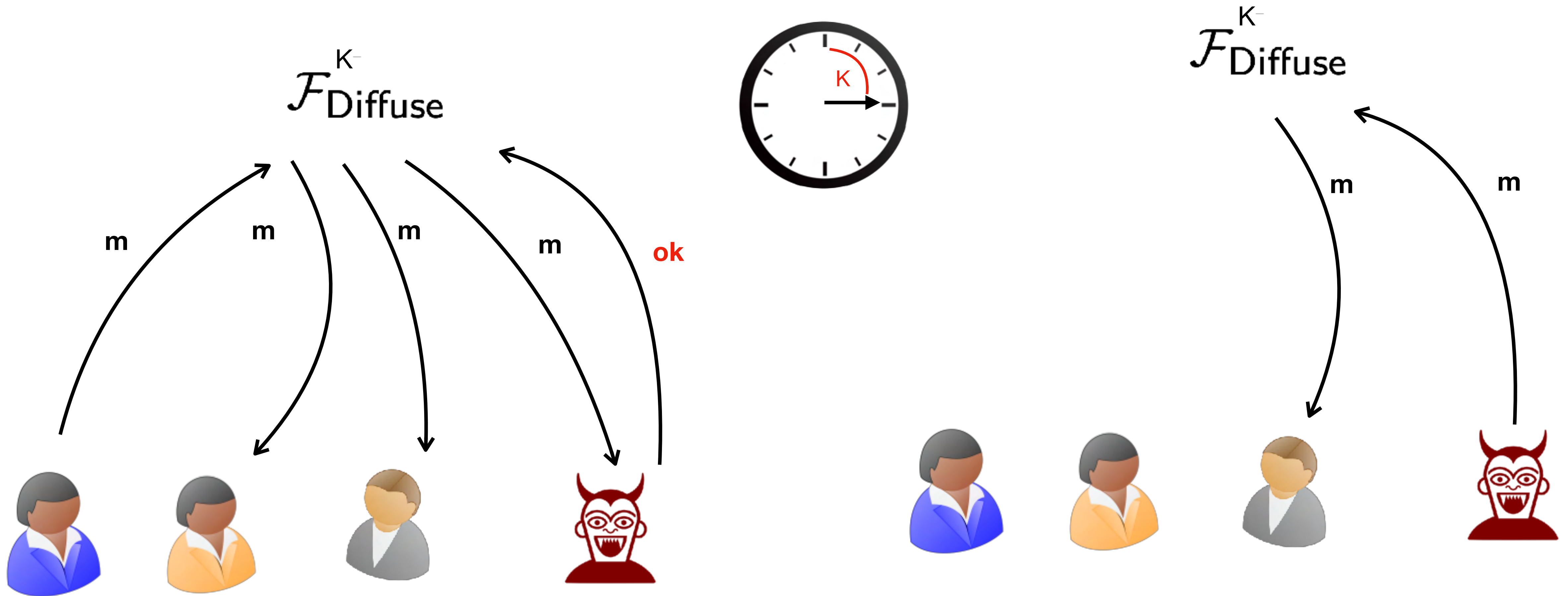
The adversary can always delay honest parties messages

Communication network



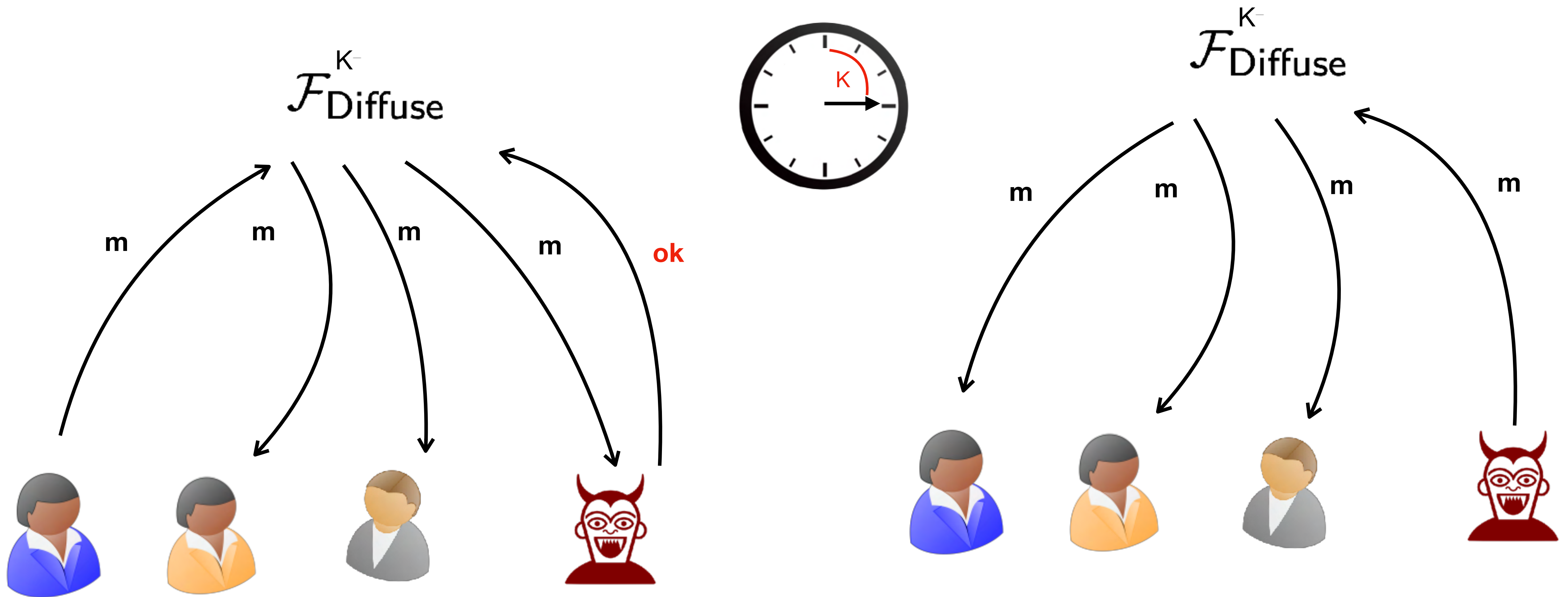
The adversary can always delay honest parties messages

Communication network



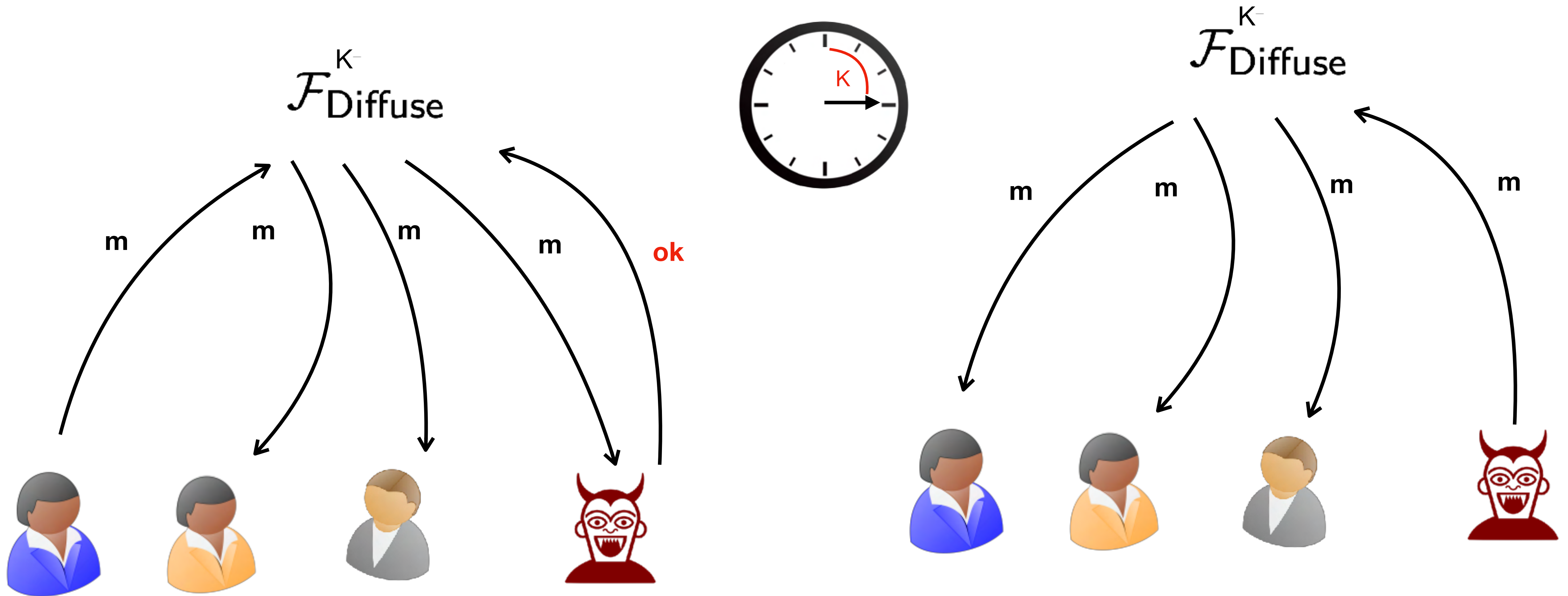
The adversary can always delay honest parties messages

Communication network



The adversary can always delay honest parties messages

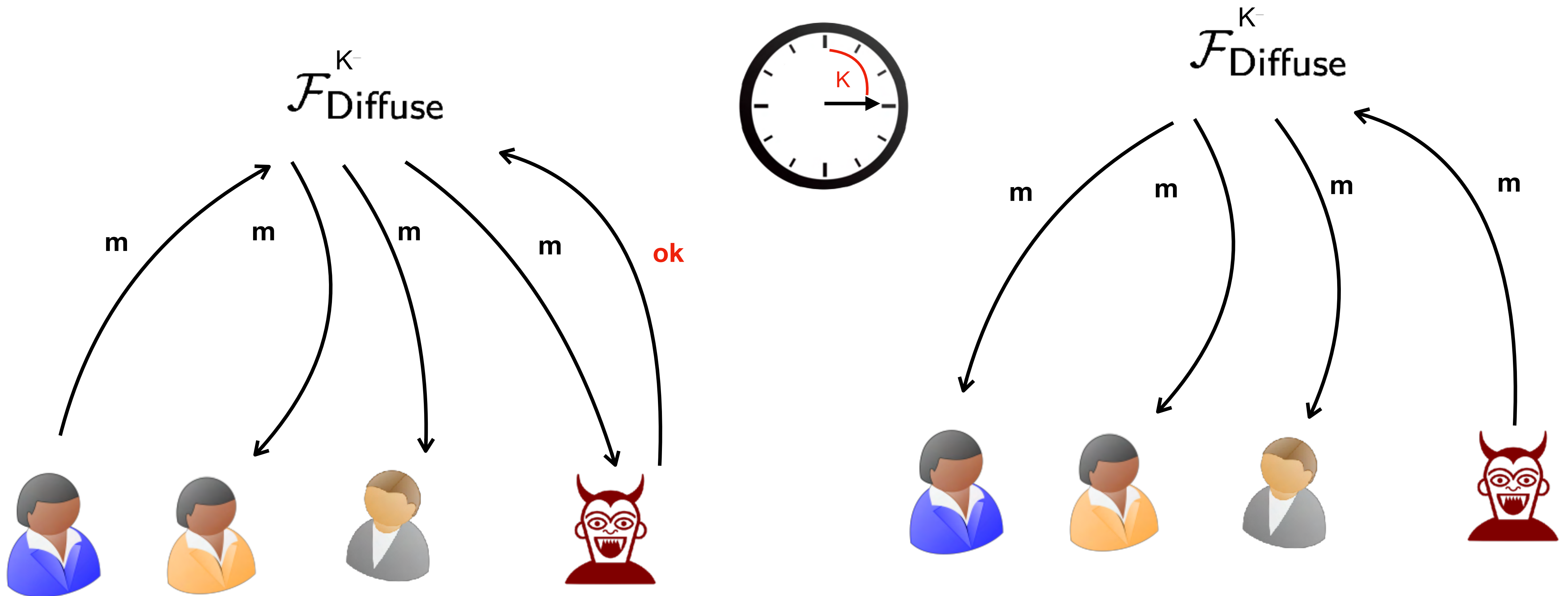
Communication network



The adversary can always delay honest parties messages

The adversary can deliver his own messages without delay

Communication network



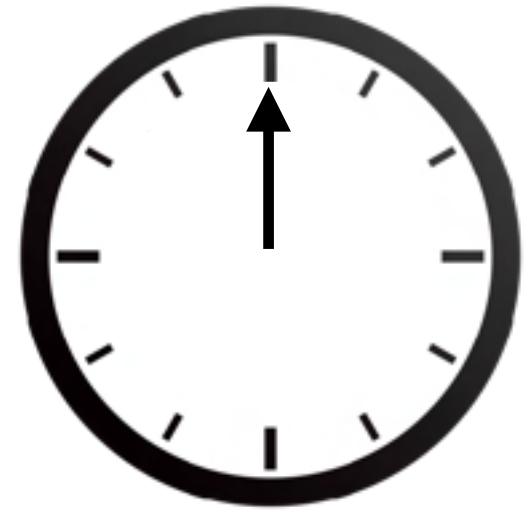
Even if Alice and a corrupt party send a transaction at the same time, Alice's transaction will be received with a K -round delay

Impossibility result

Real

Ideal

$\mathcal{F}_{\text{Diffuse}}^K$

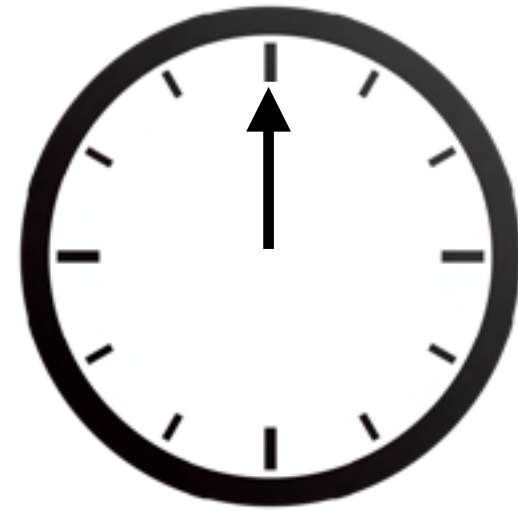


Impossibility result

Real

Ideal

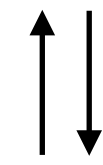
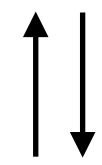
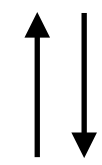
$\mathcal{F}_{\text{Diffuse}}^K$



\mathcal{F}_{aux}

\mathcal{F}_{aux}

\mathcal{F}_{aux}

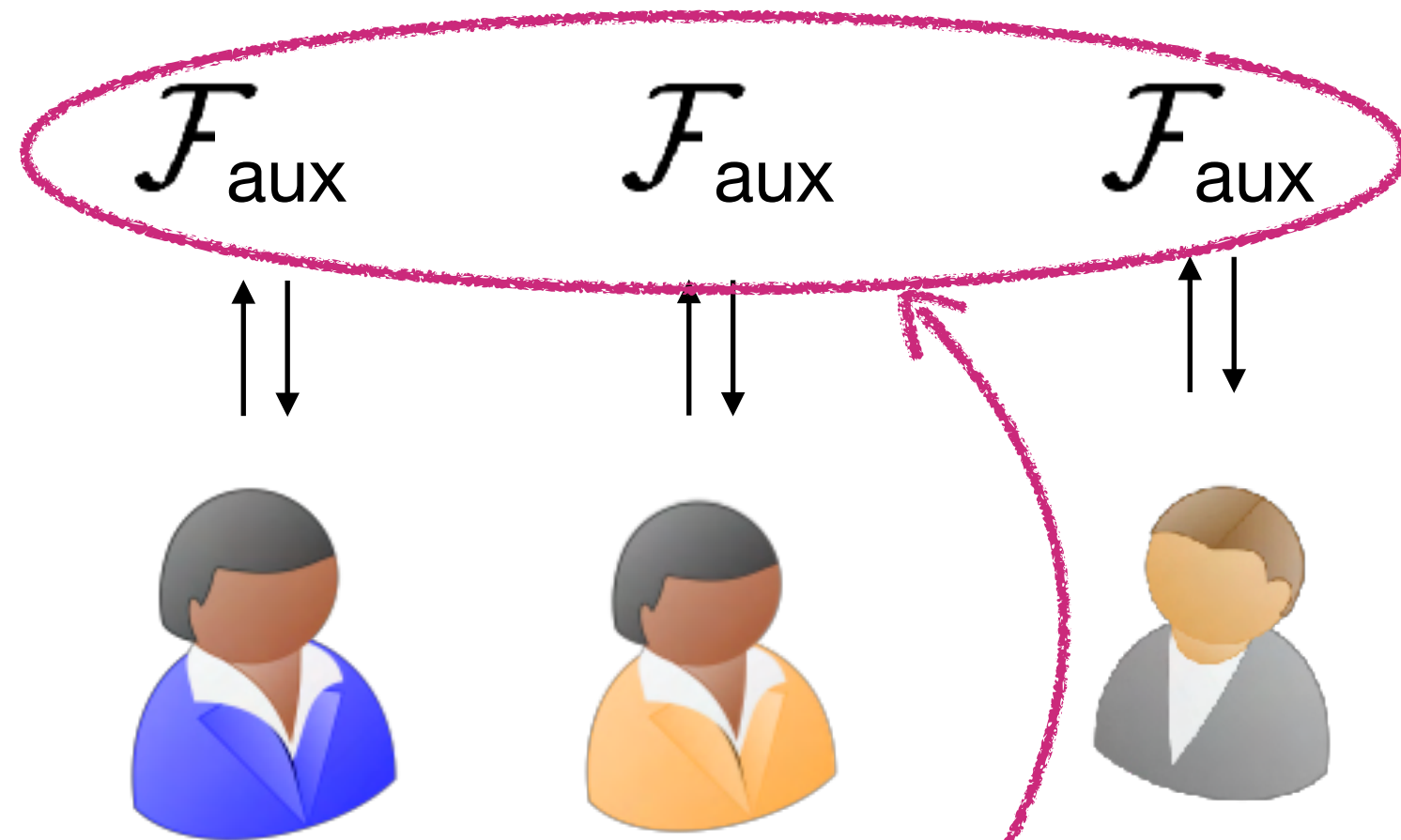
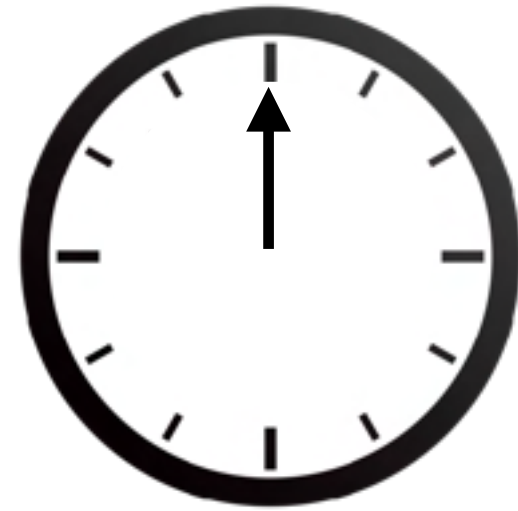


Impossibility result

Real

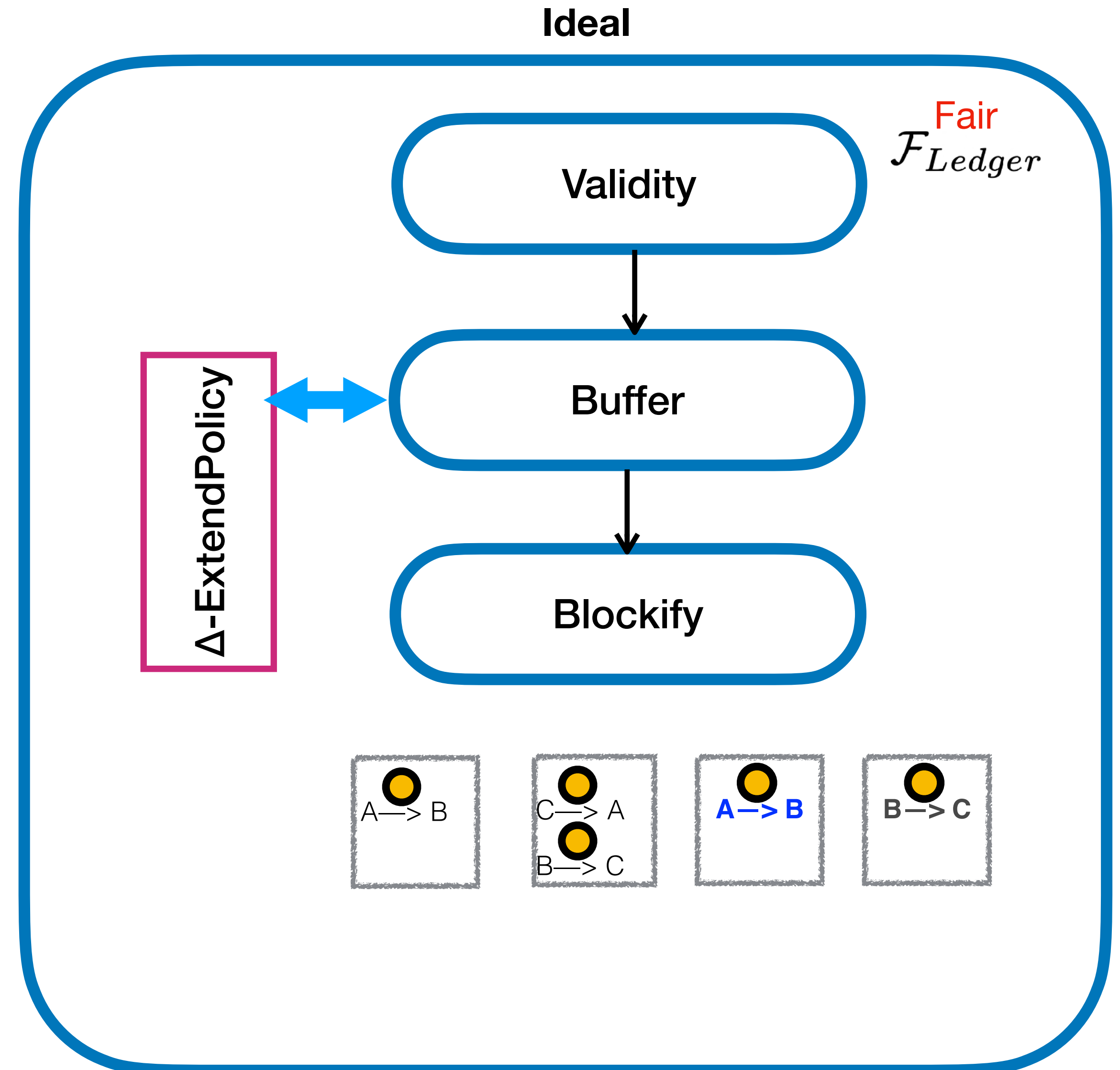
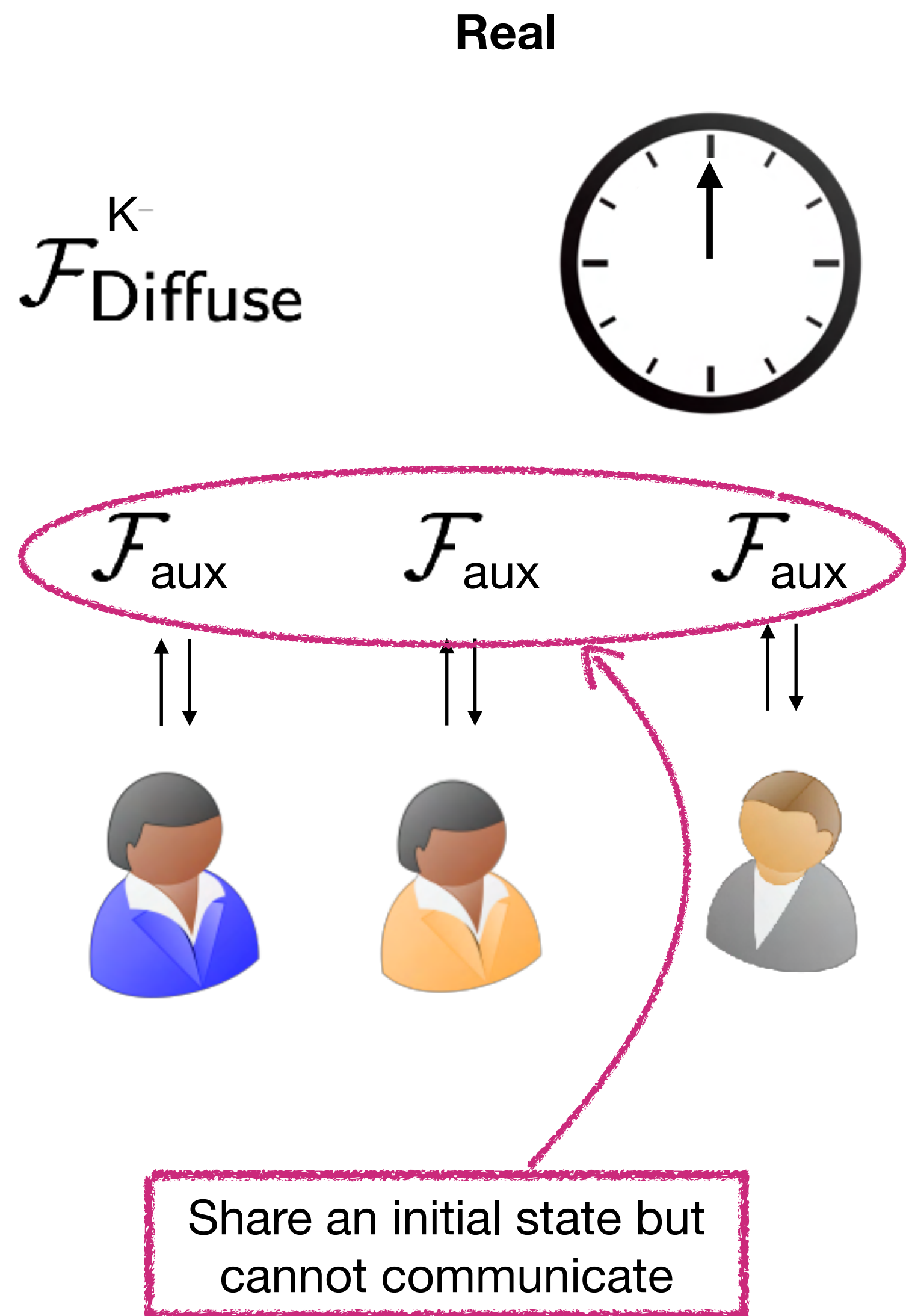
Ideal

$\mathcal{F}_{\text{Diffuse}}^K$

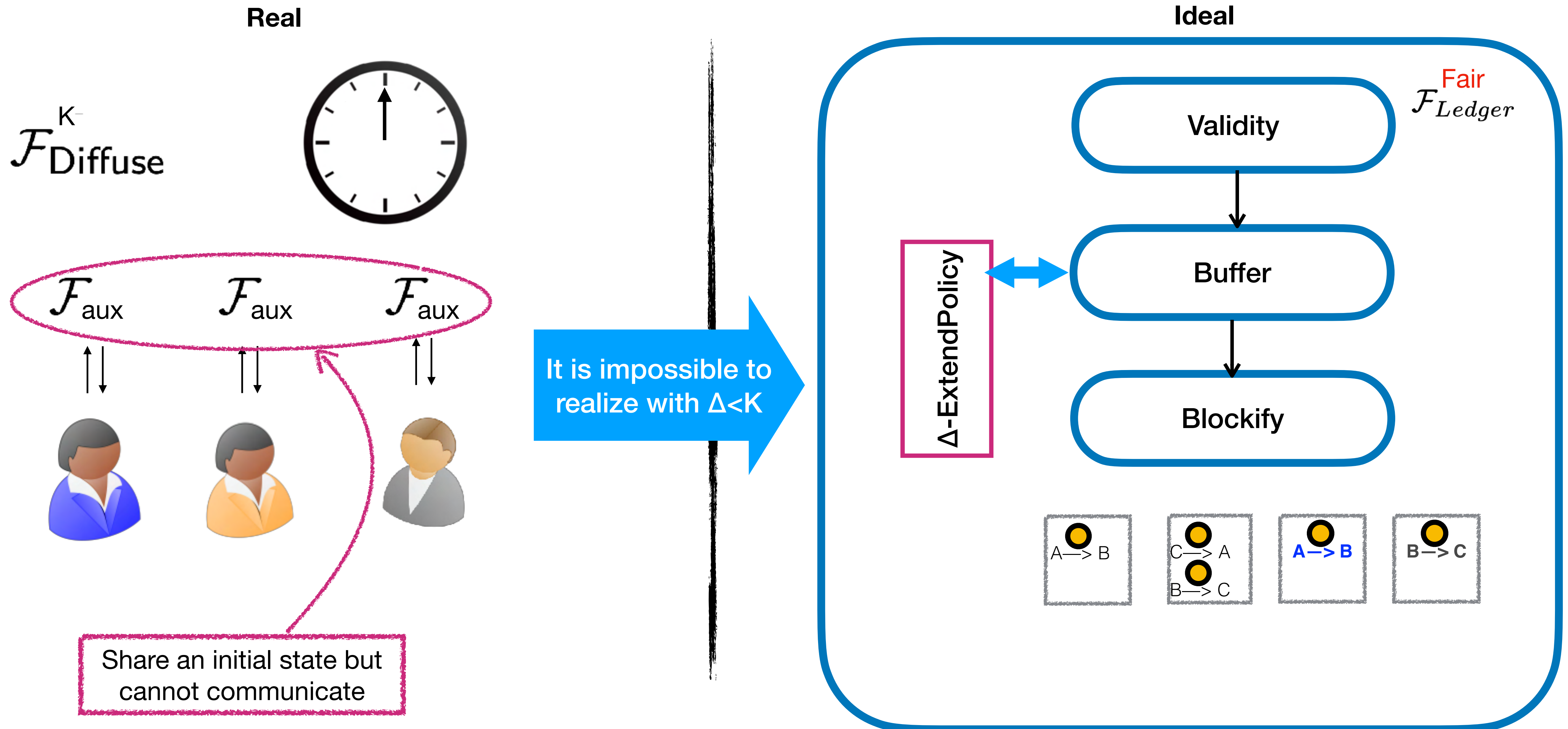


Share an initial state but
cannot communicate

Impossibility result



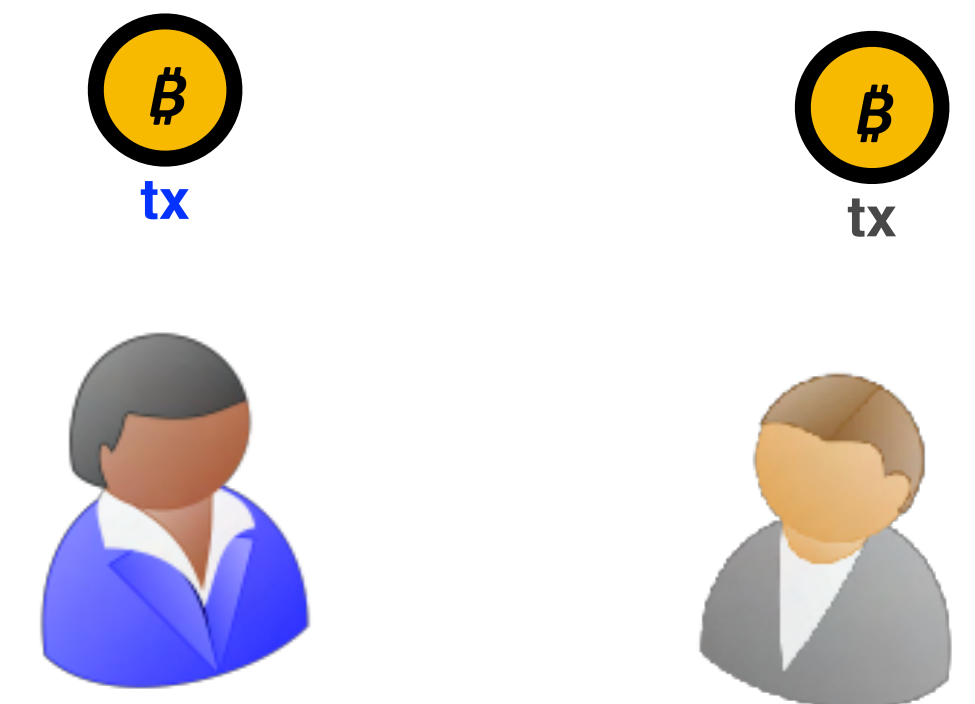
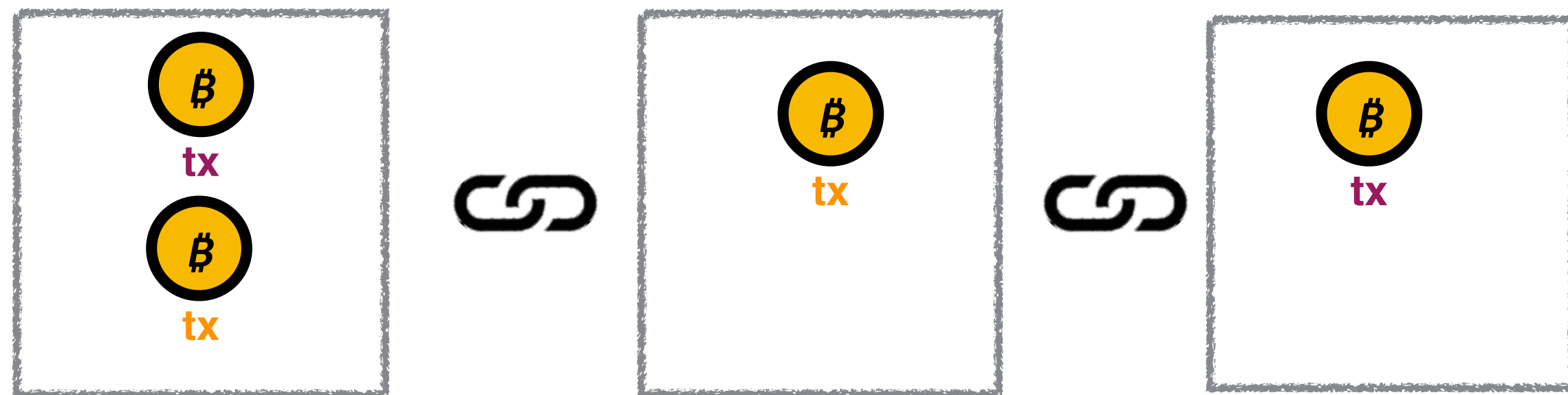
Impossibility result



How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



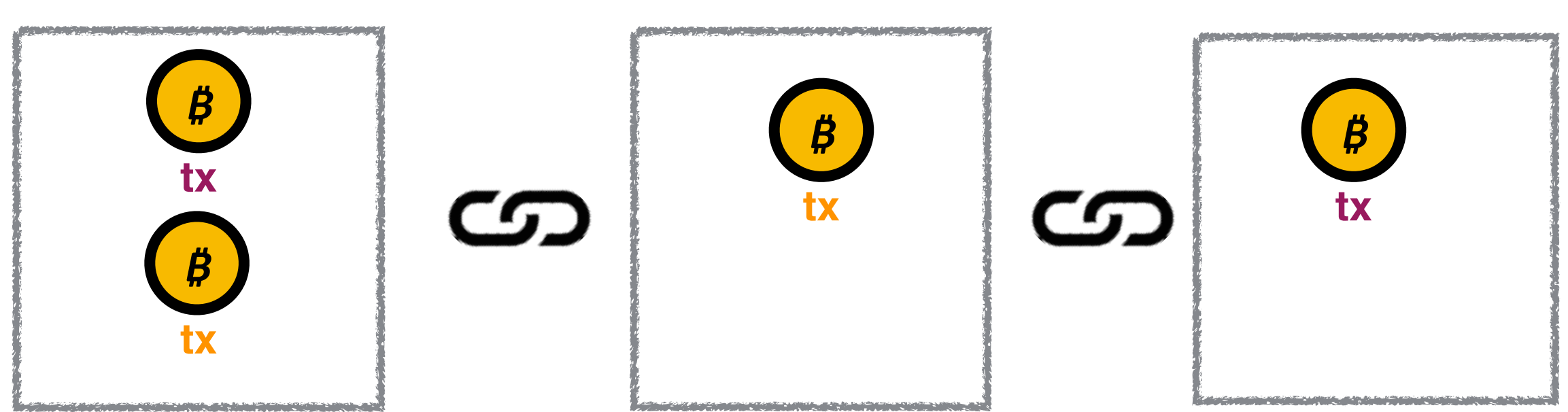
$\mathcal{F}_{Diffuse}^{K-}$



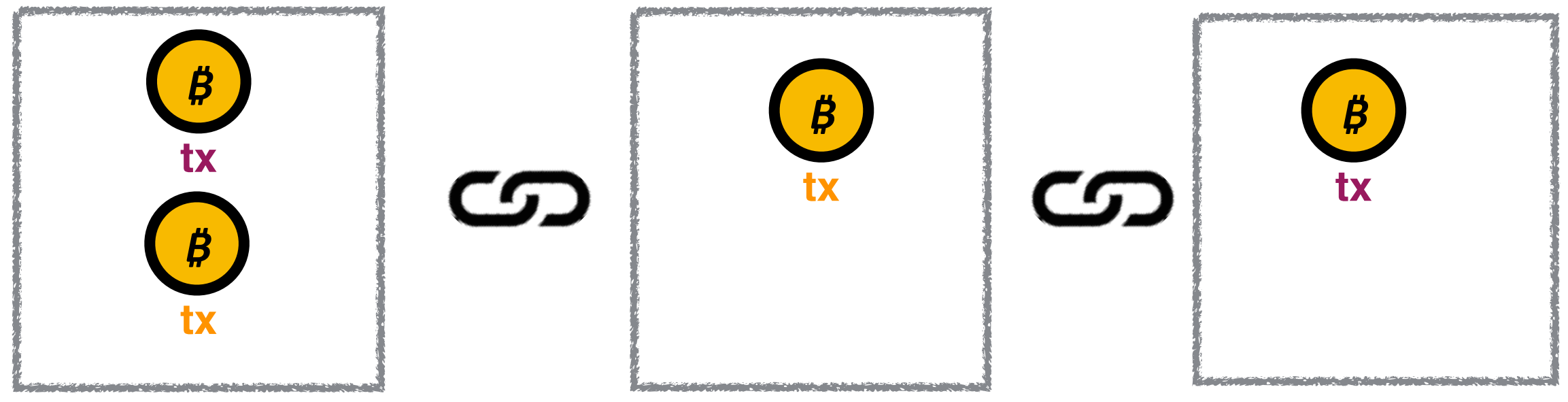
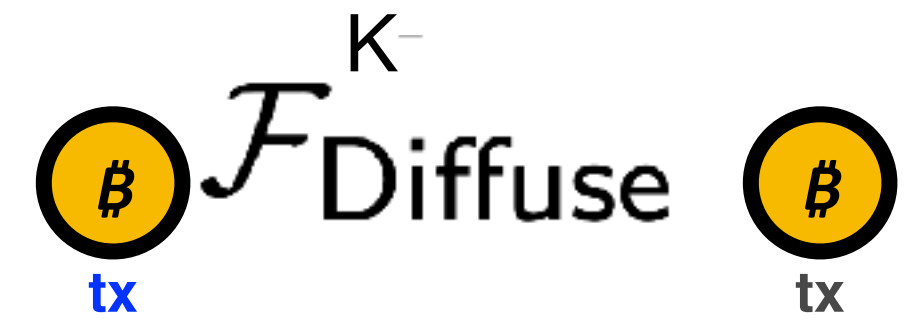
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



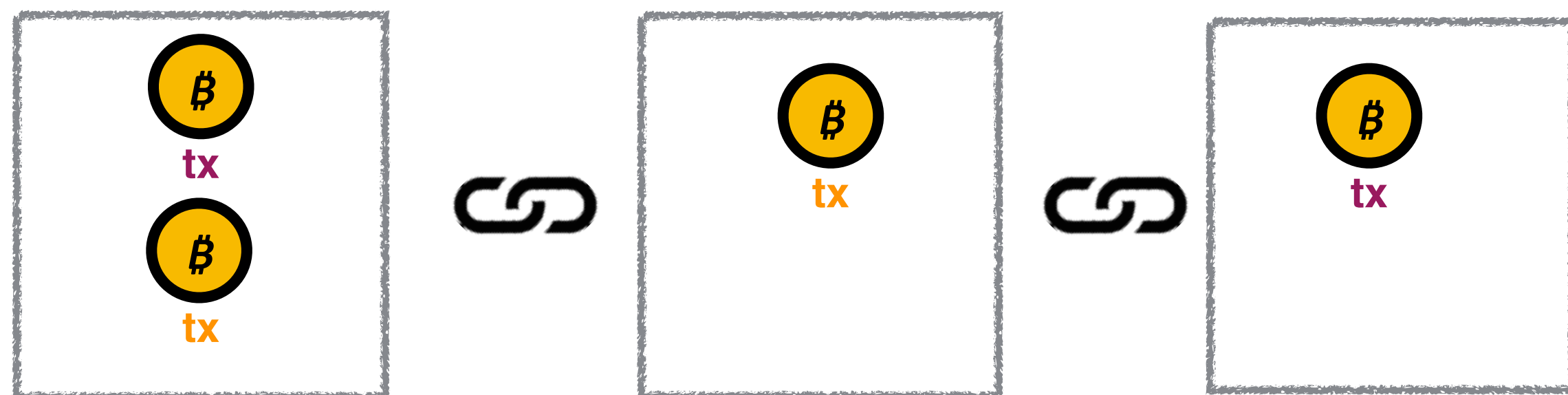
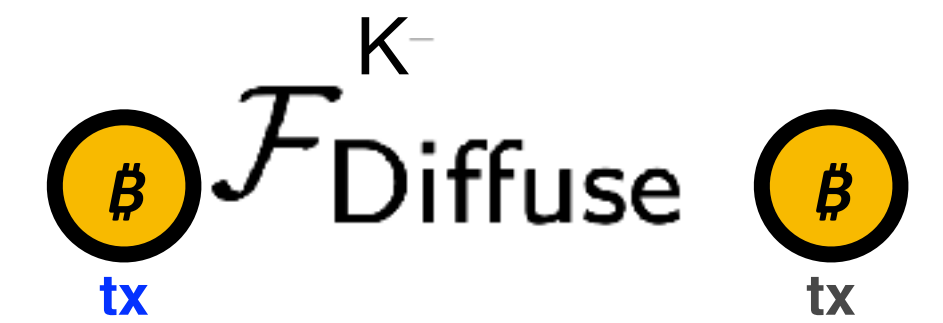
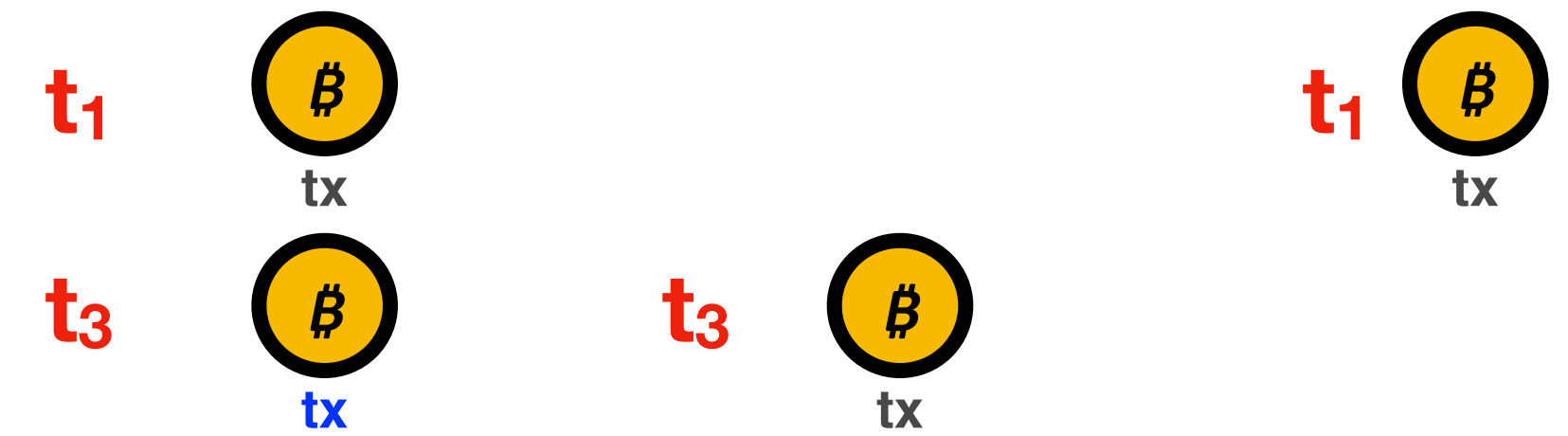
$\mathcal{F}_{Diffuse}^{K-}$

Two Bitcoin symbols, each with a 'tx' label below it, representing transactions.

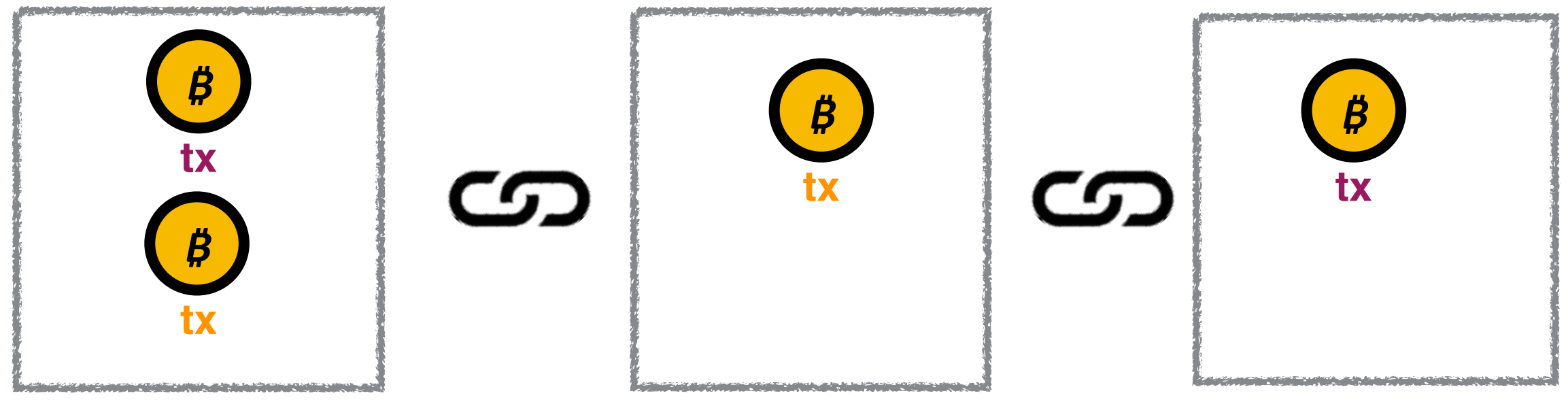
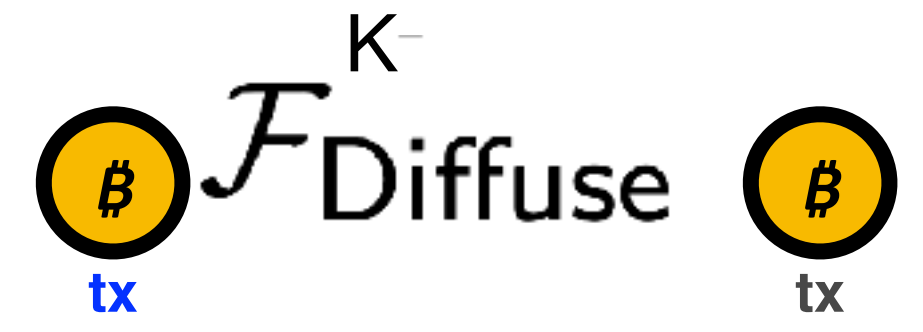
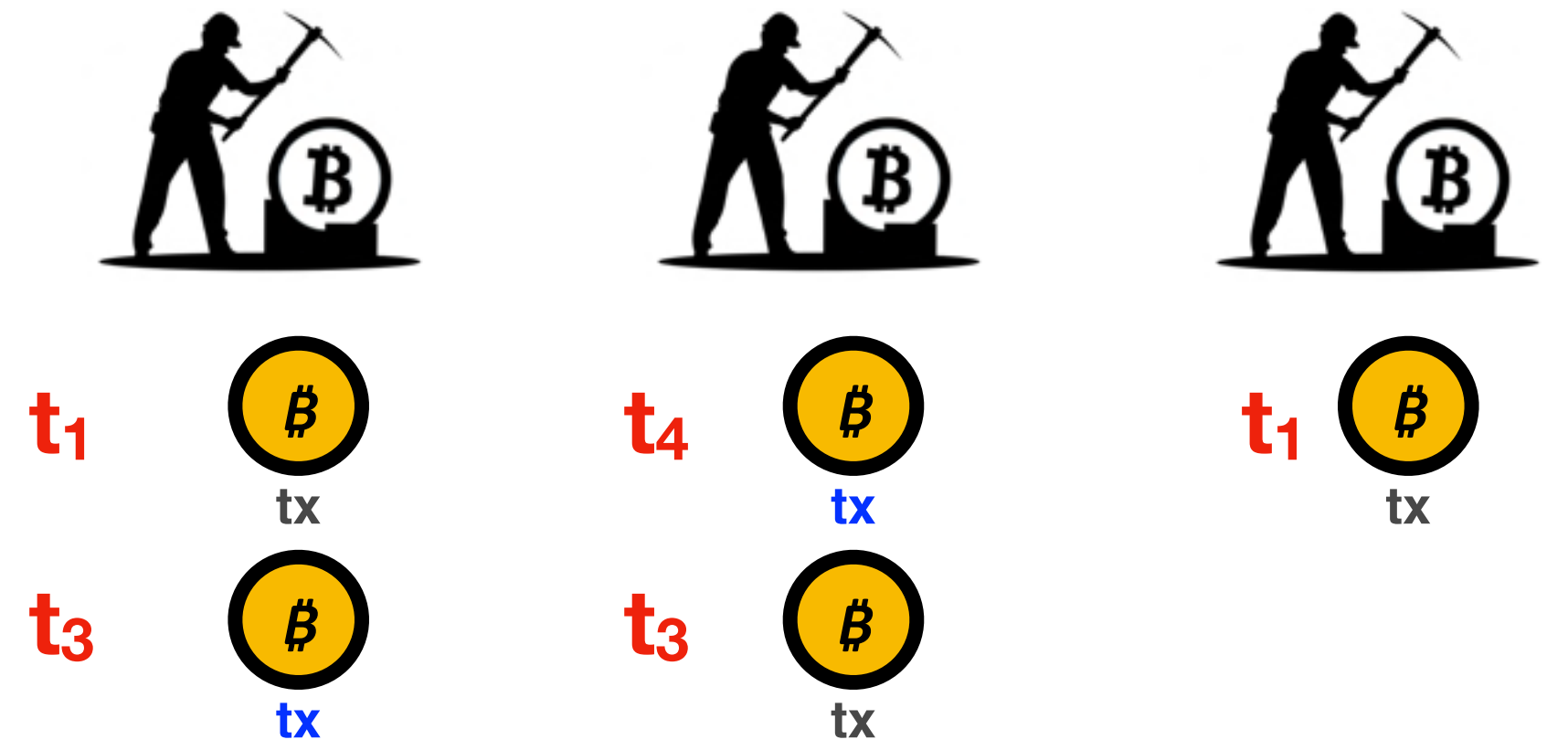
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



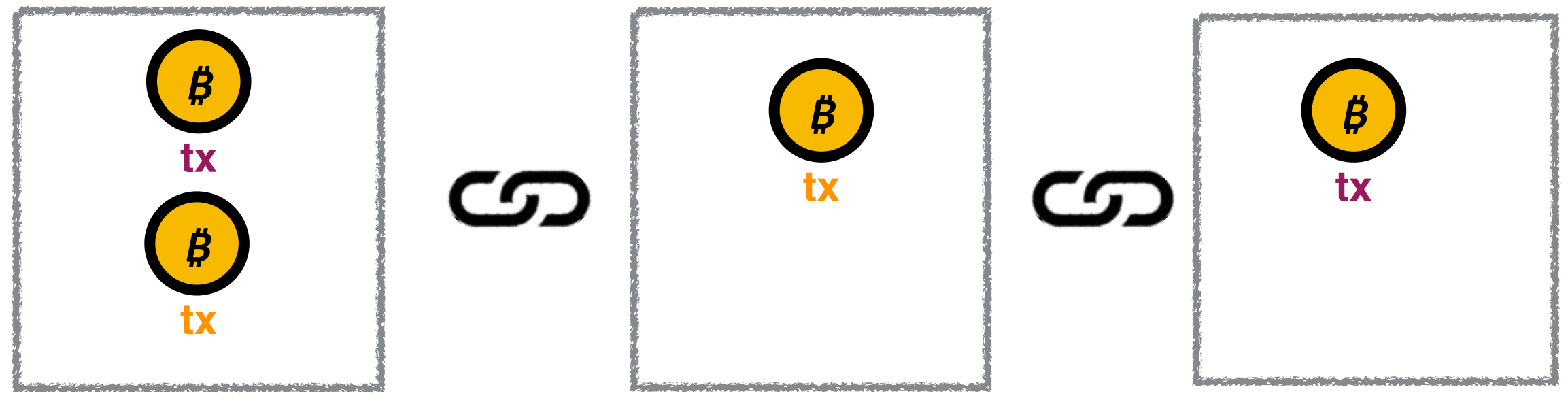
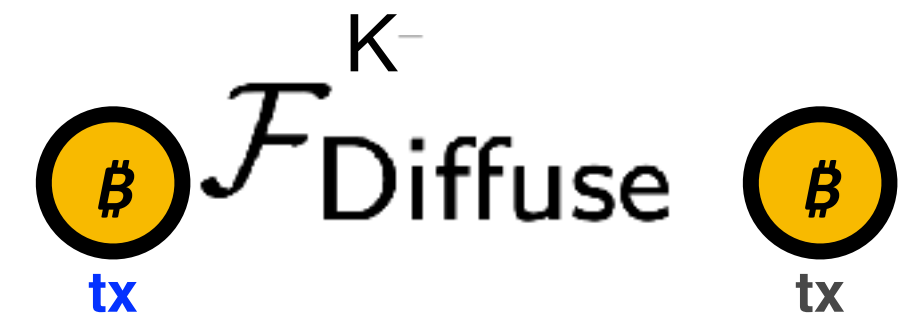
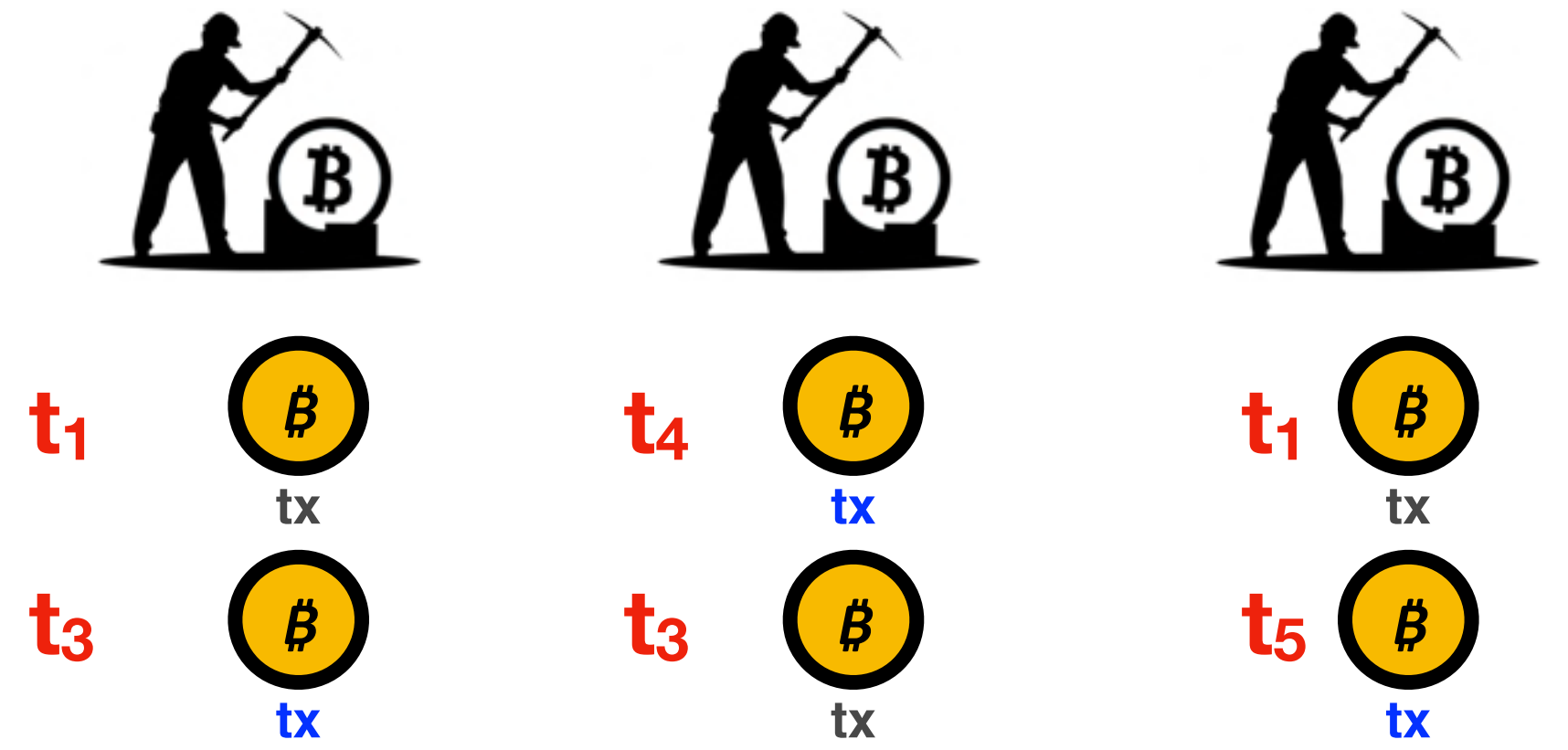
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



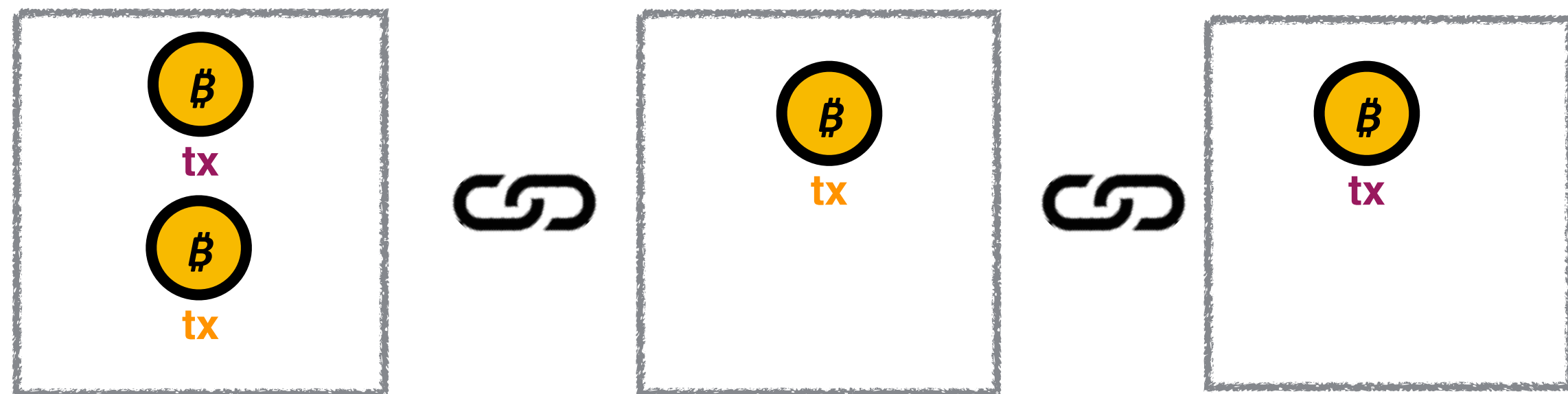
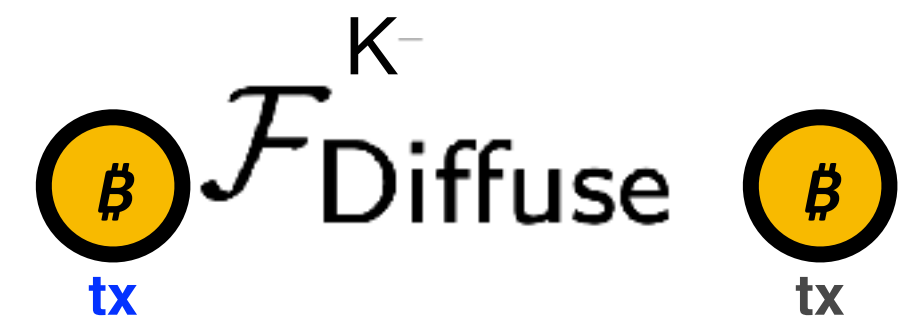
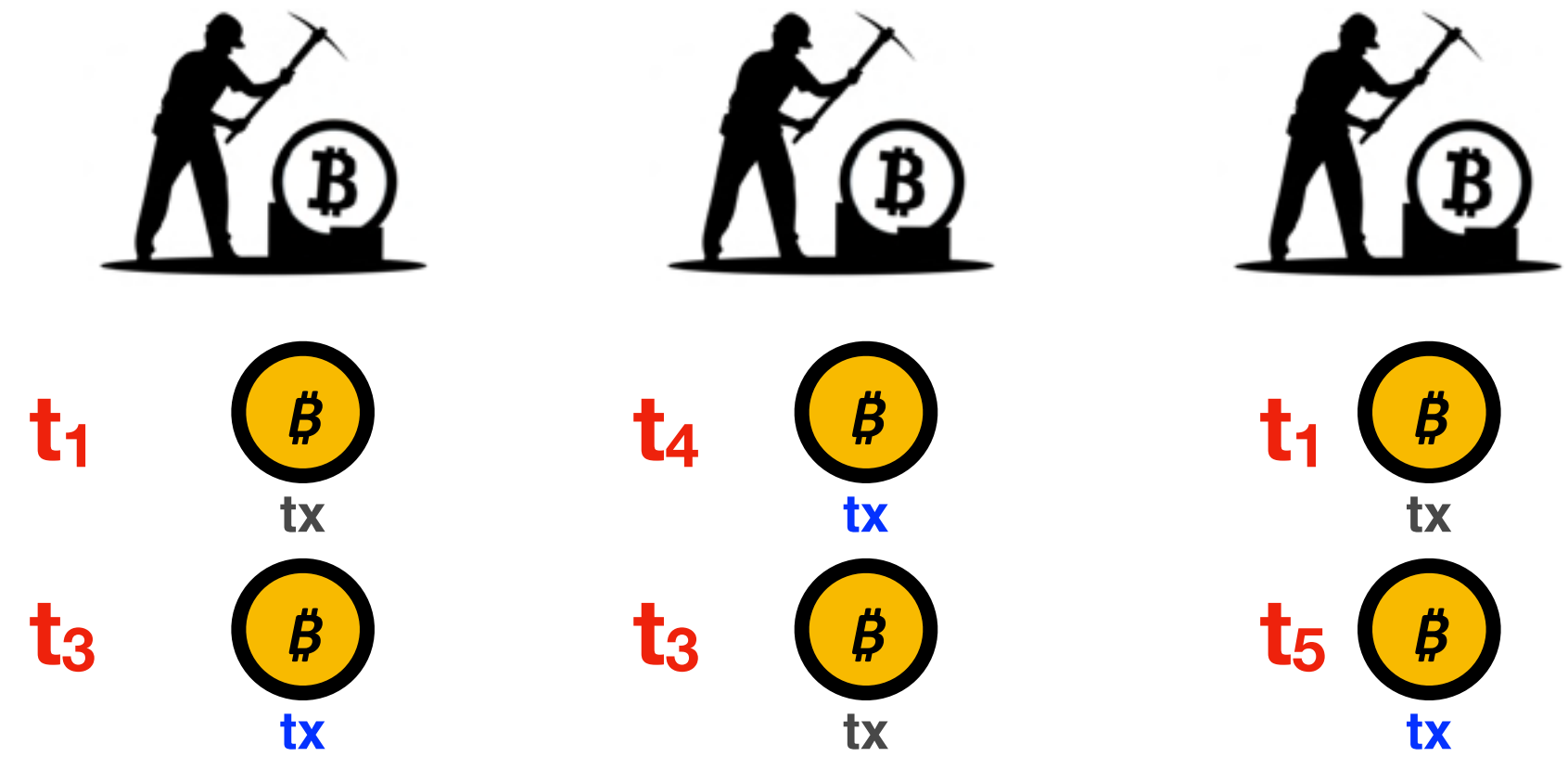
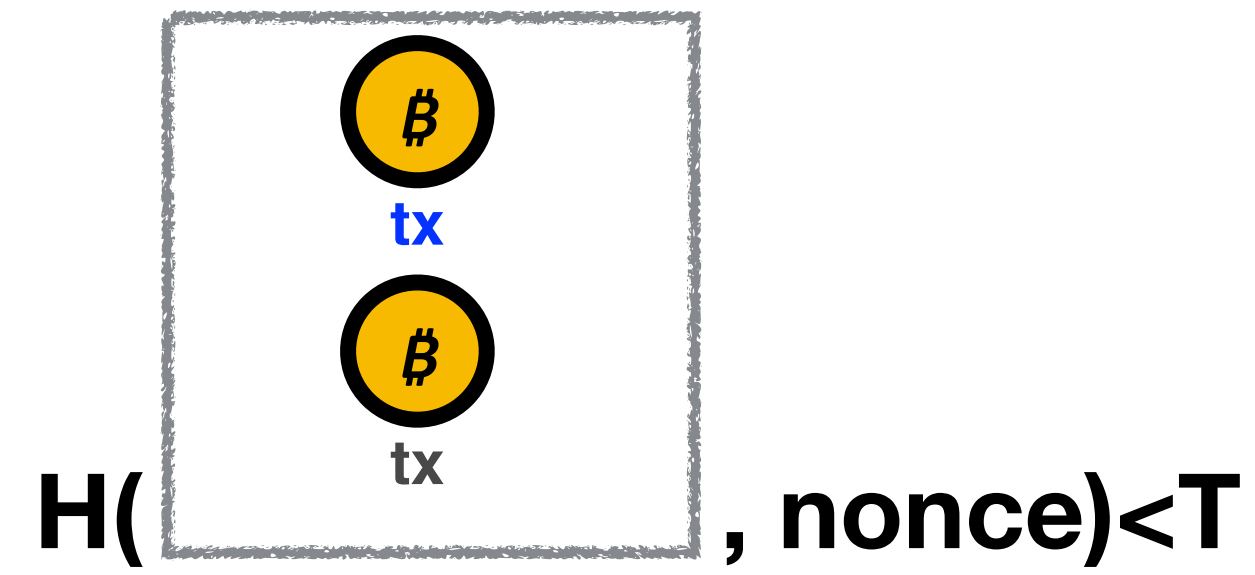
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



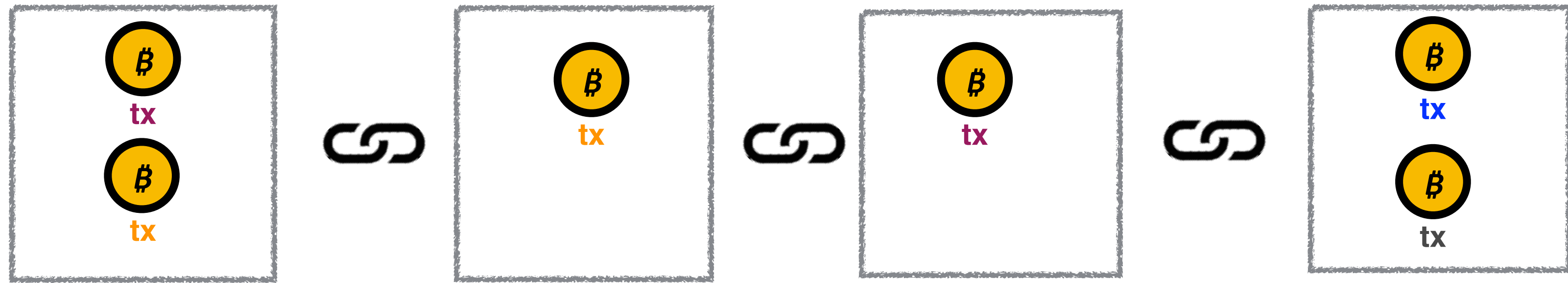
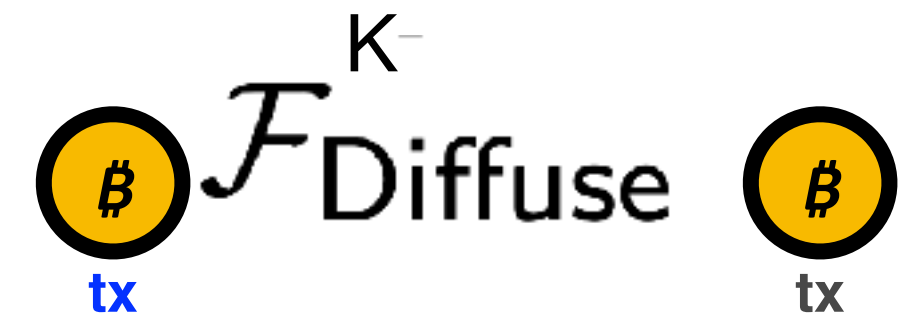
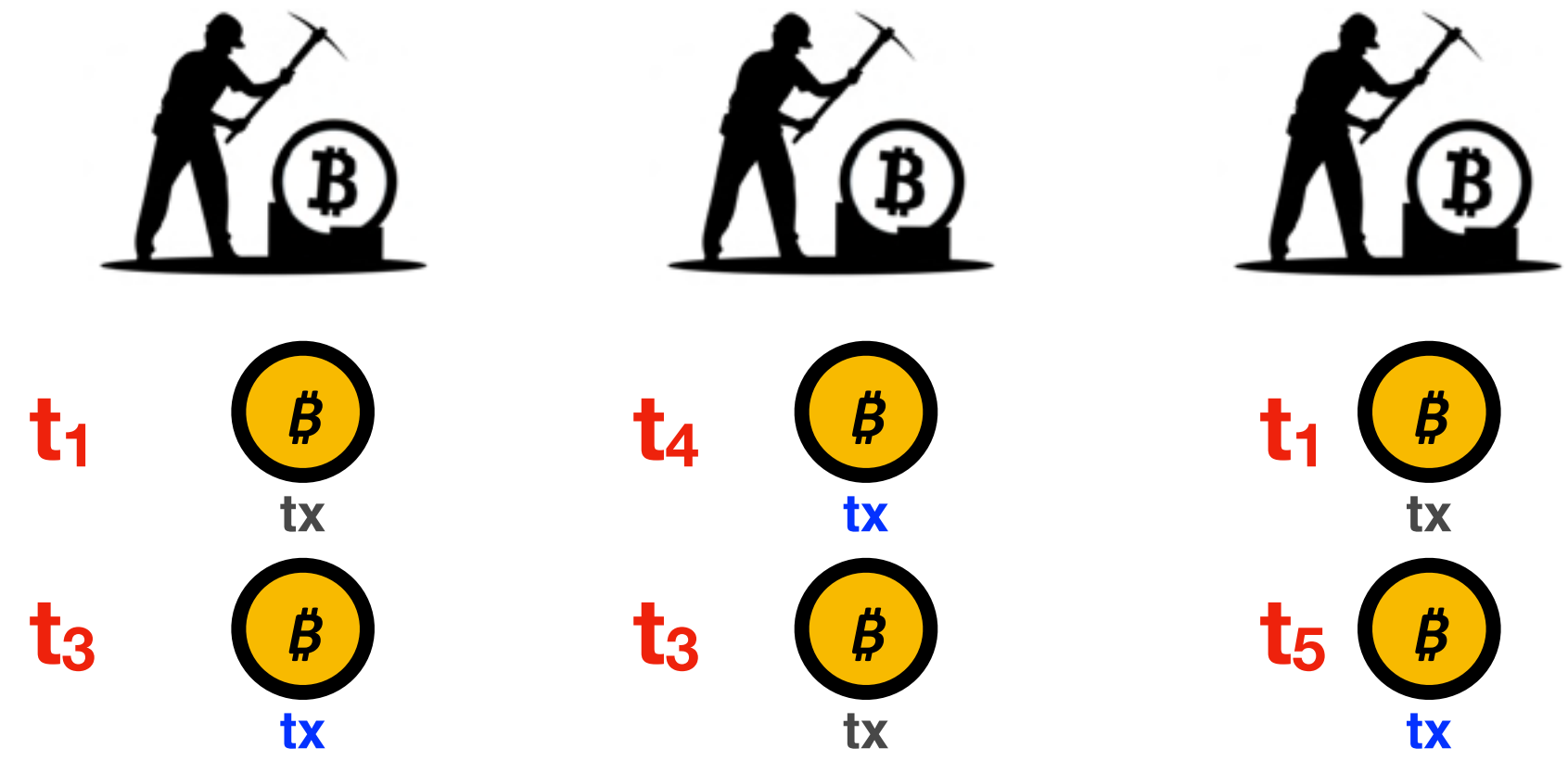
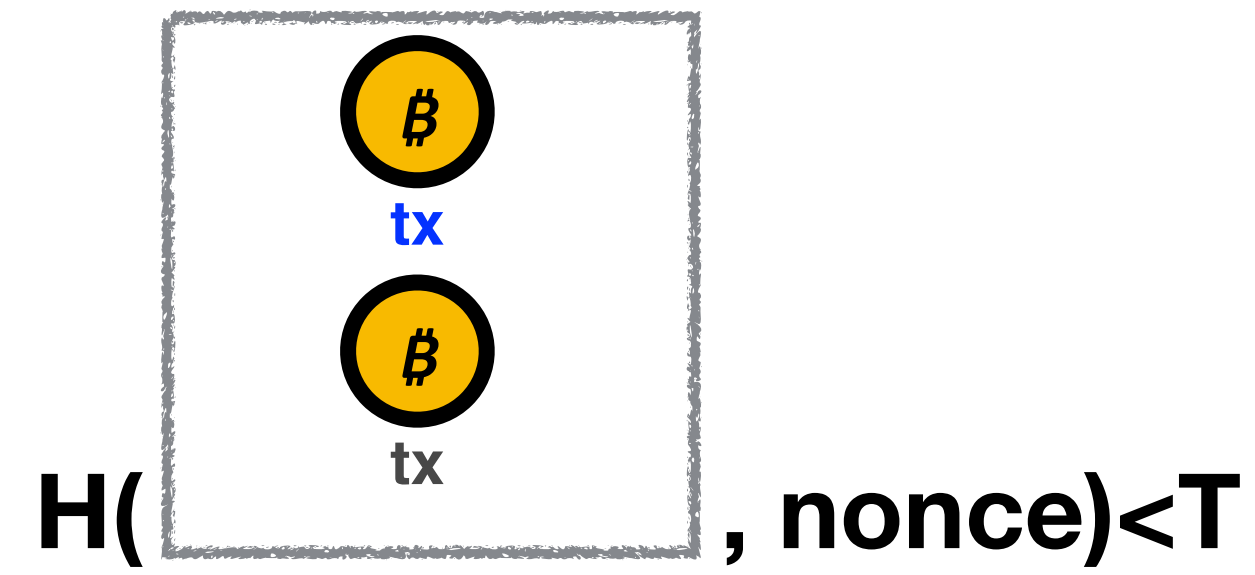
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



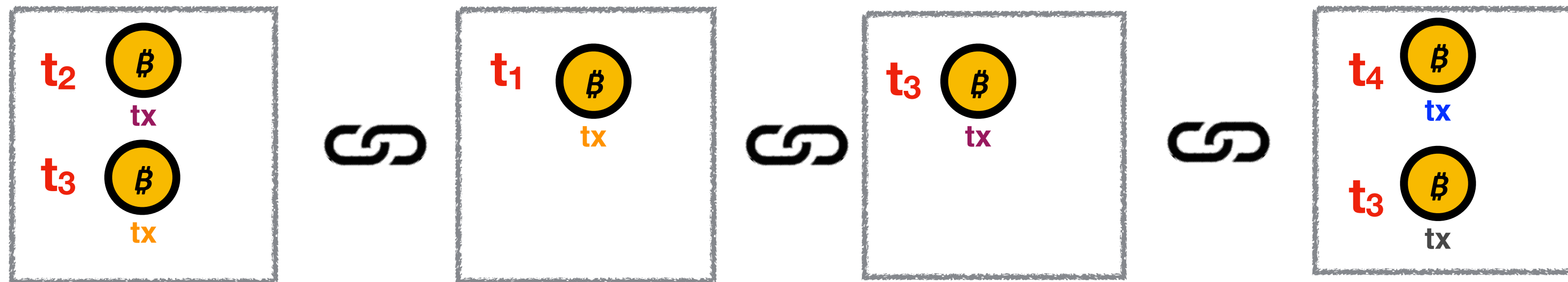
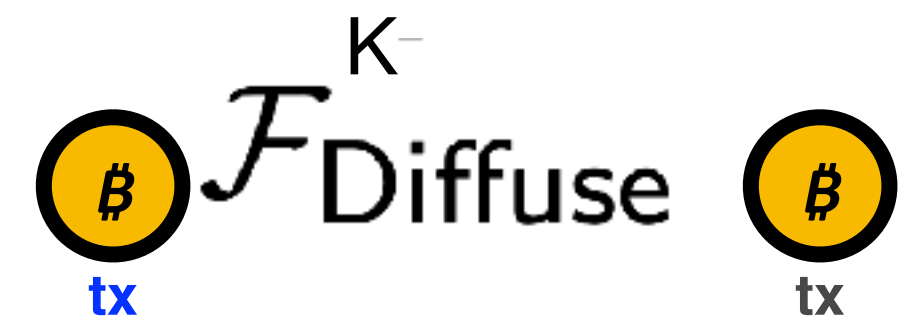
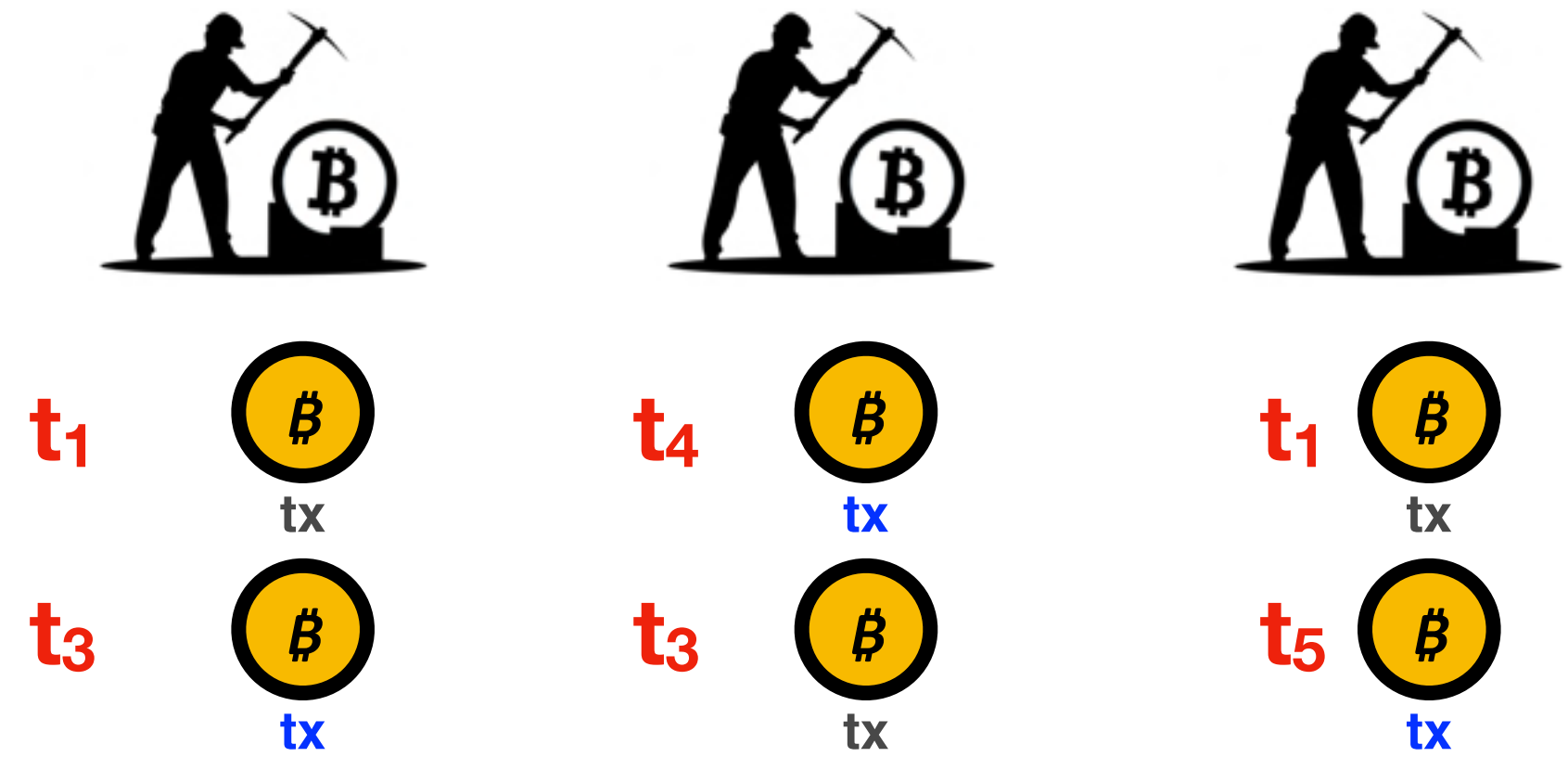
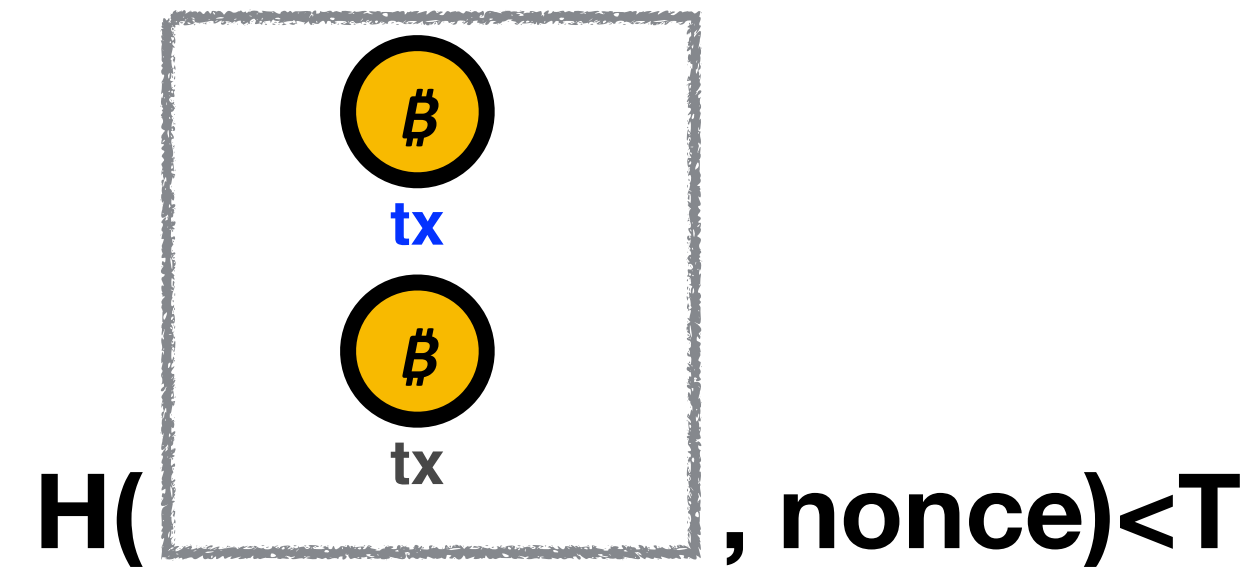
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



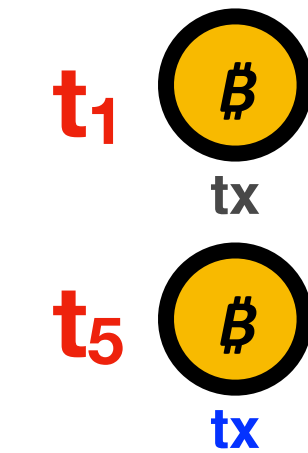
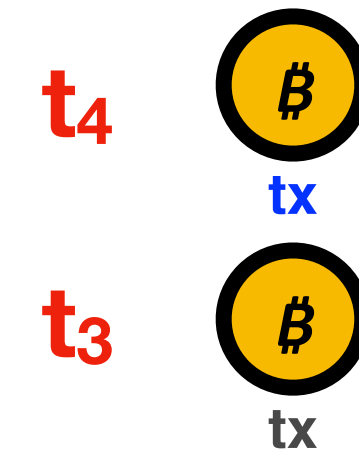
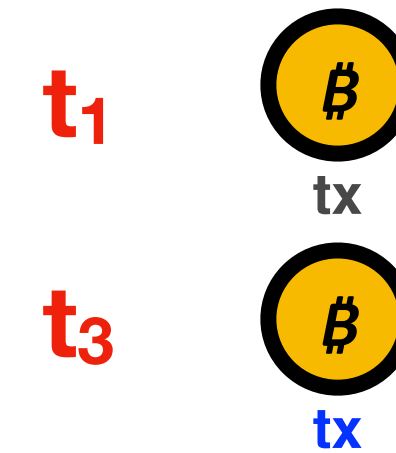
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



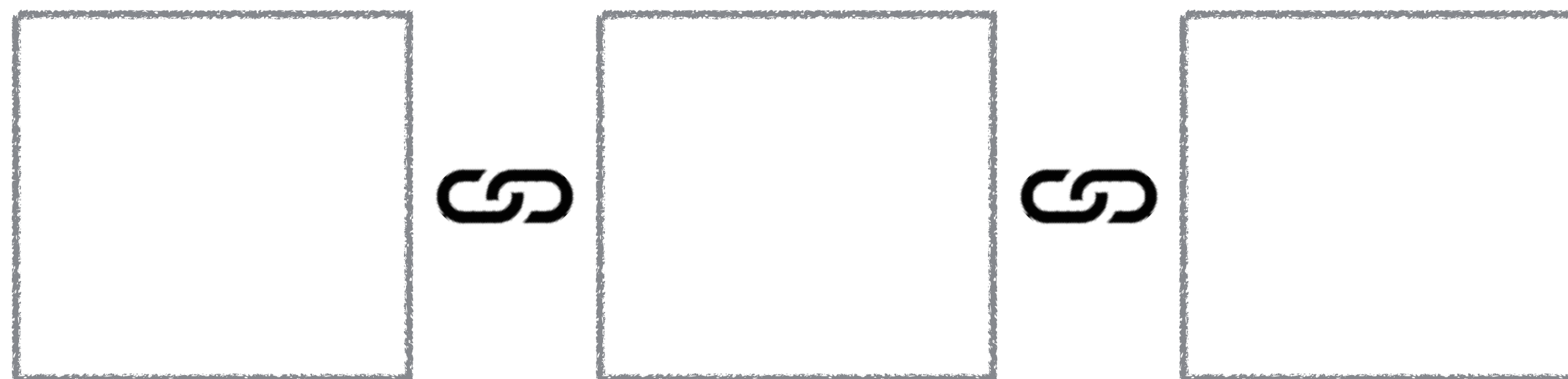
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$

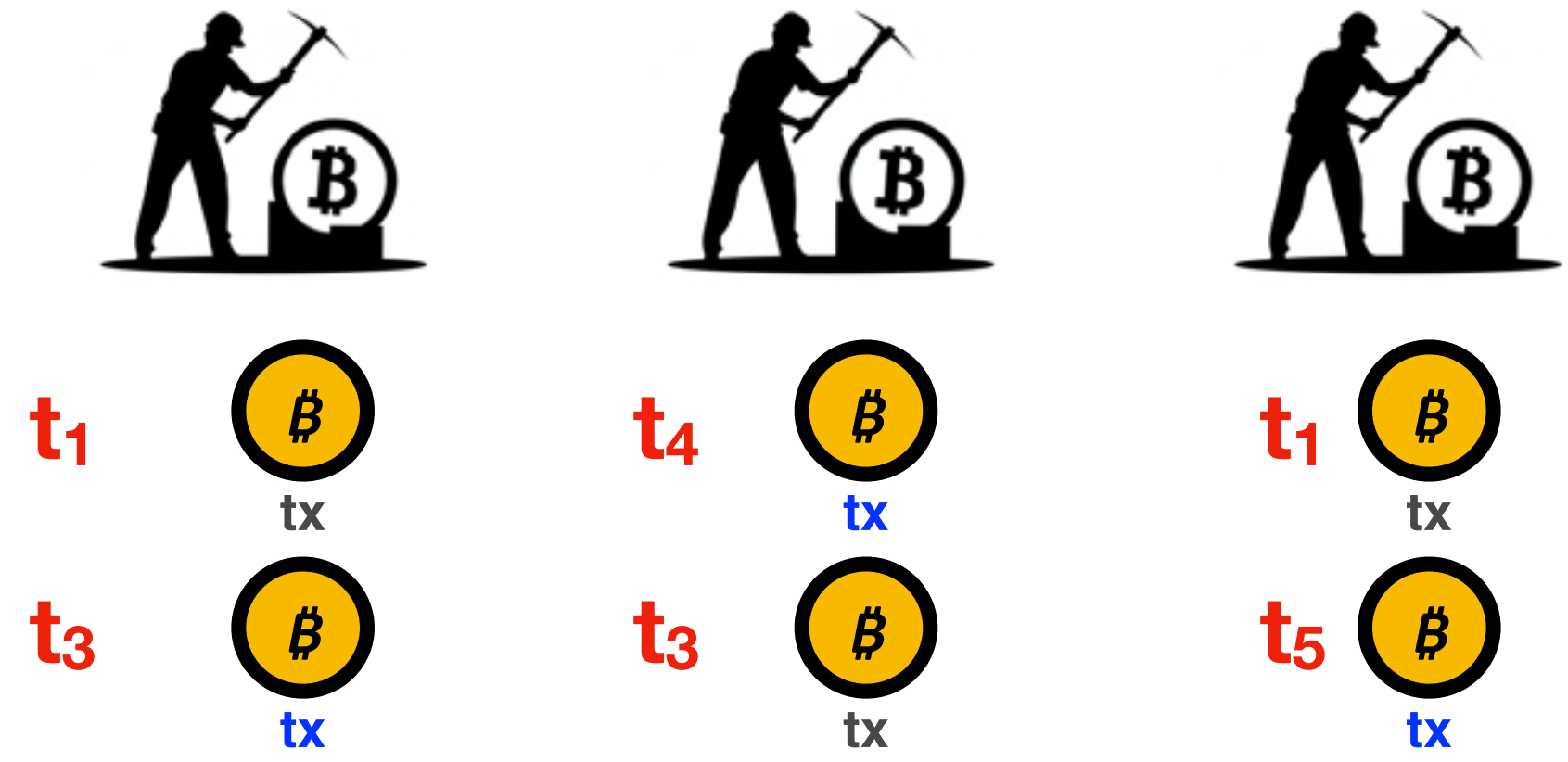


$\mathcal{F}_{Diffuse}^{K-}$

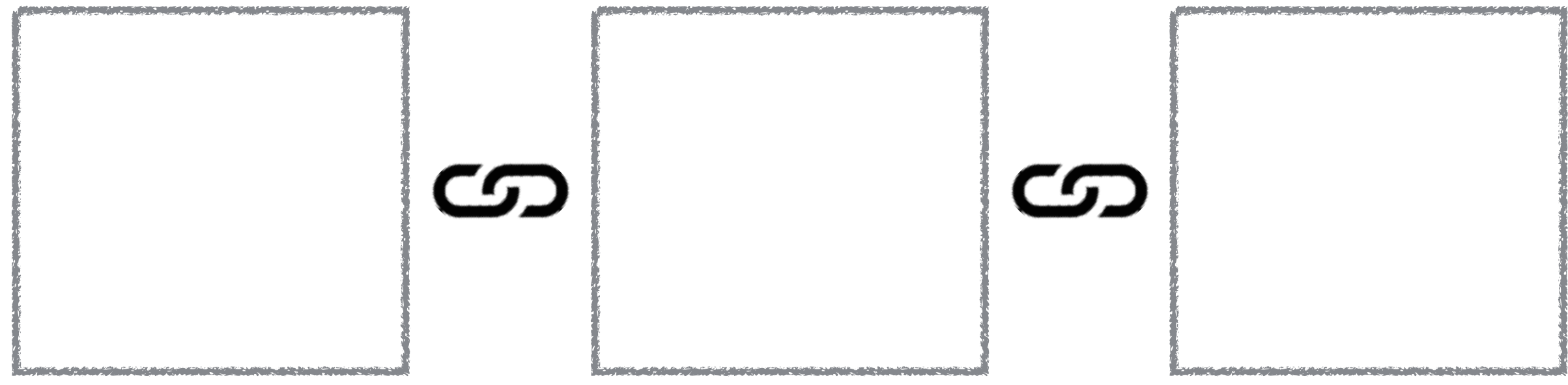
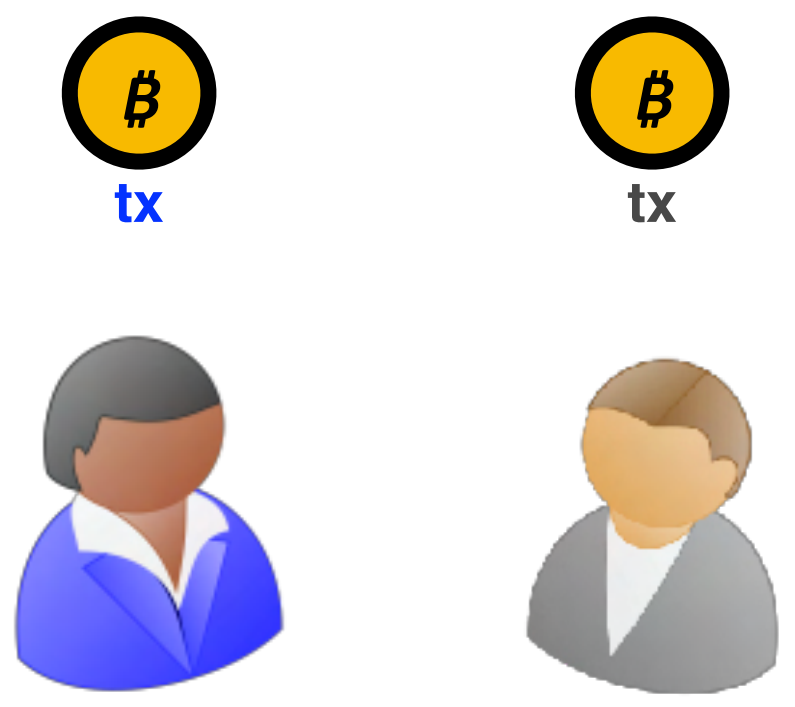


How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$

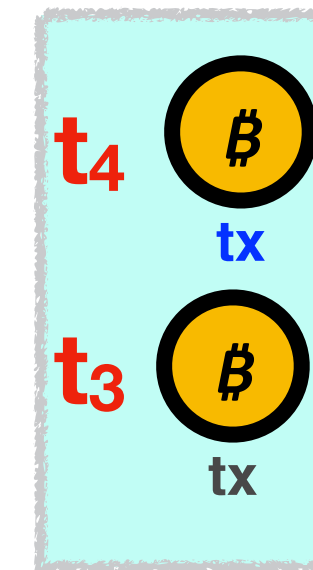
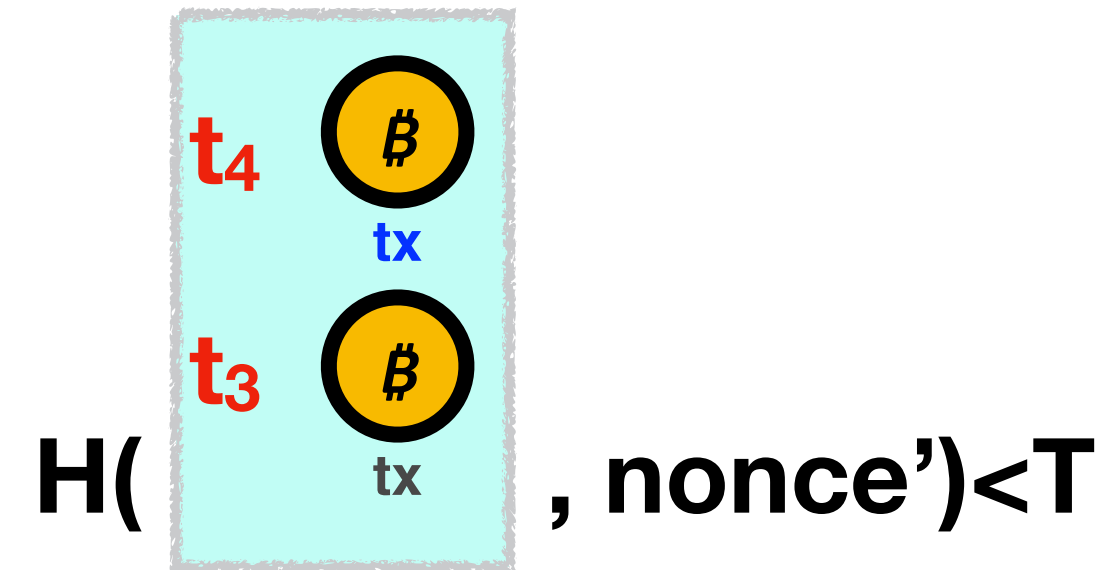
$$H(\text{[} \begin{array}{c} t_4 \text{ } \textcircled{\text{B}} \\ \text{tx} \\ t_3 \text{ } \textcircled{\text{B}} \\ \text{tx} \end{array} \text{, nonce}') < T$$



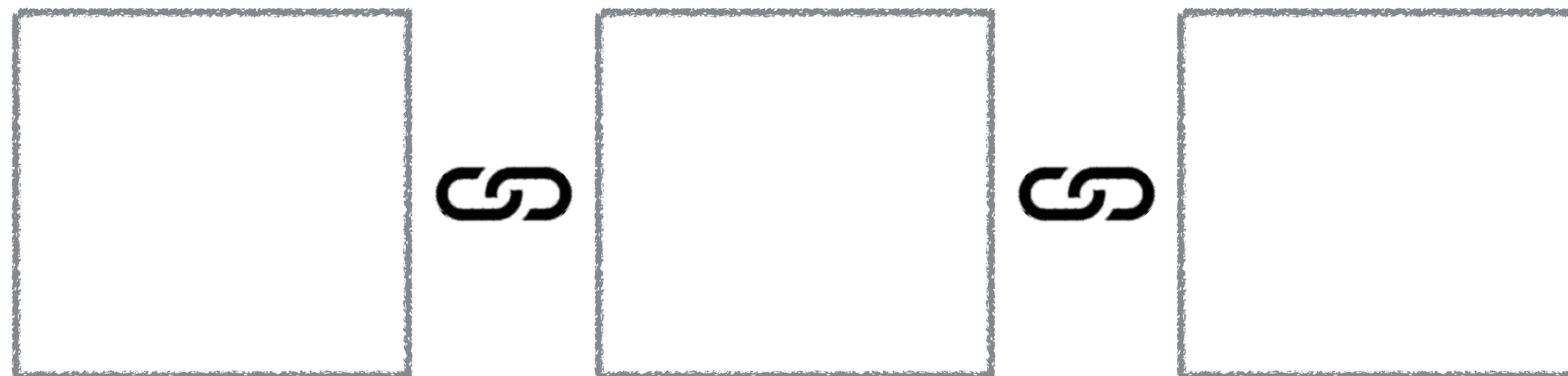
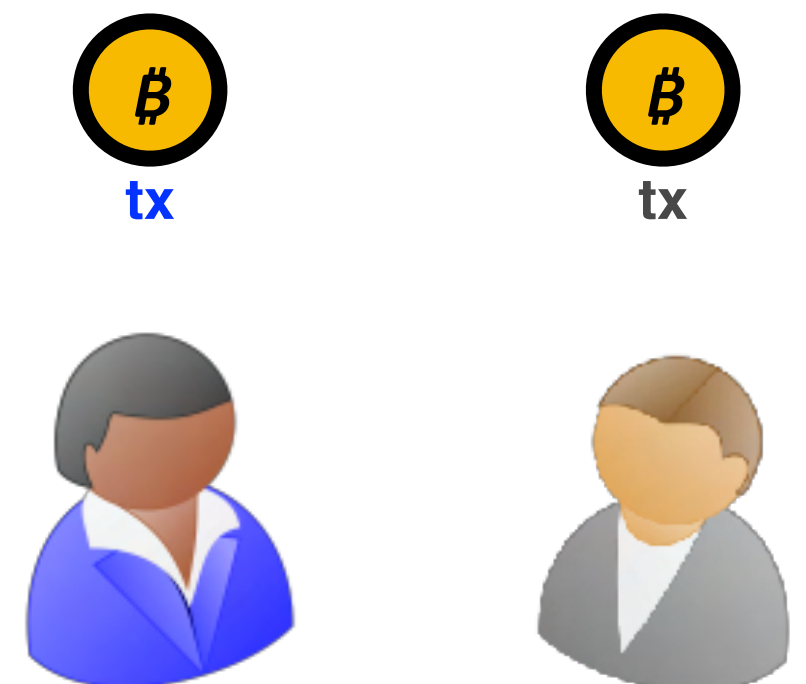
$\mathcal{F}_{Diffuse}^{K-}$



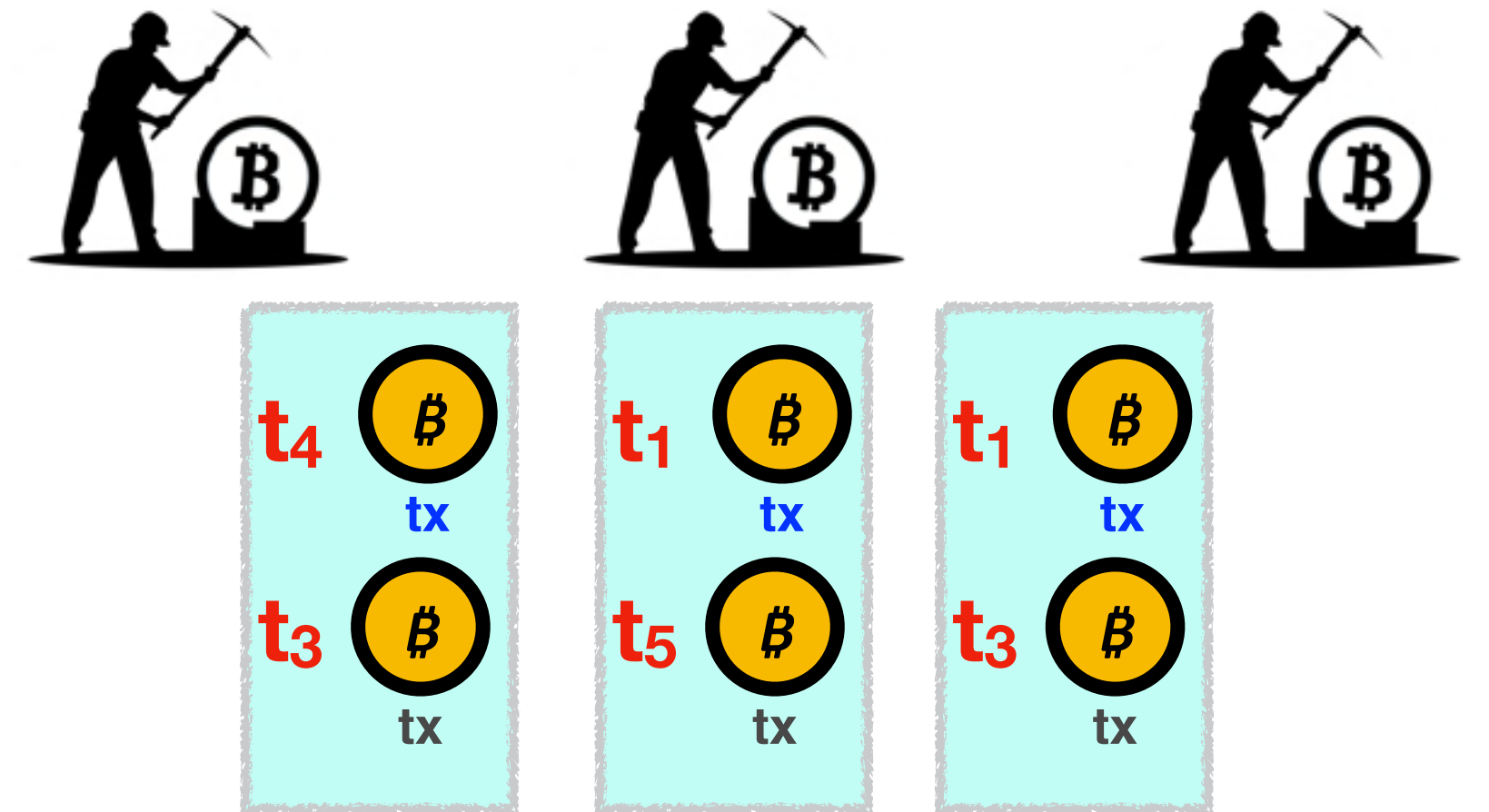
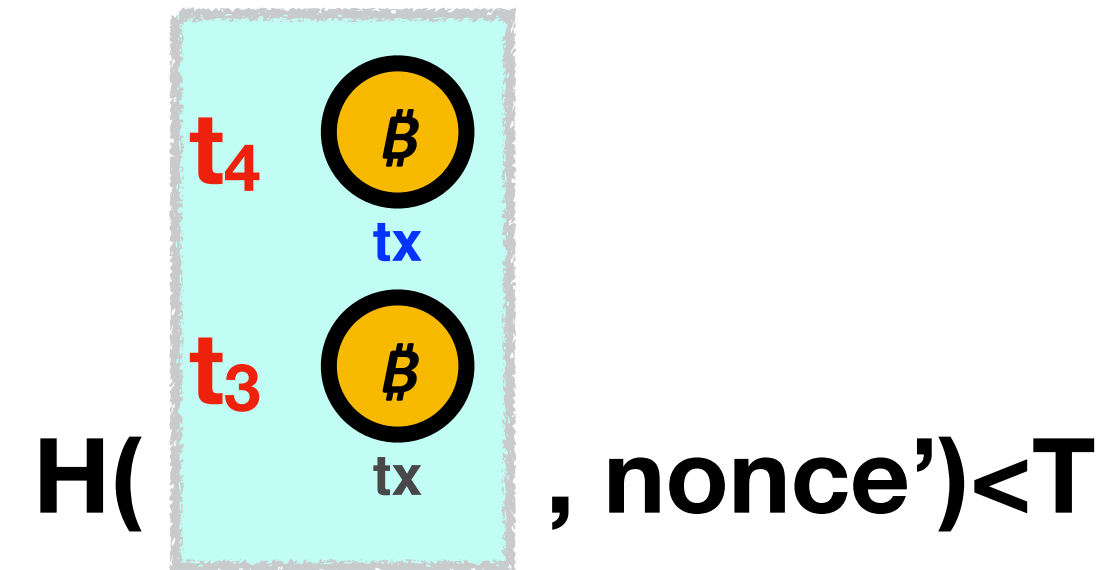
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



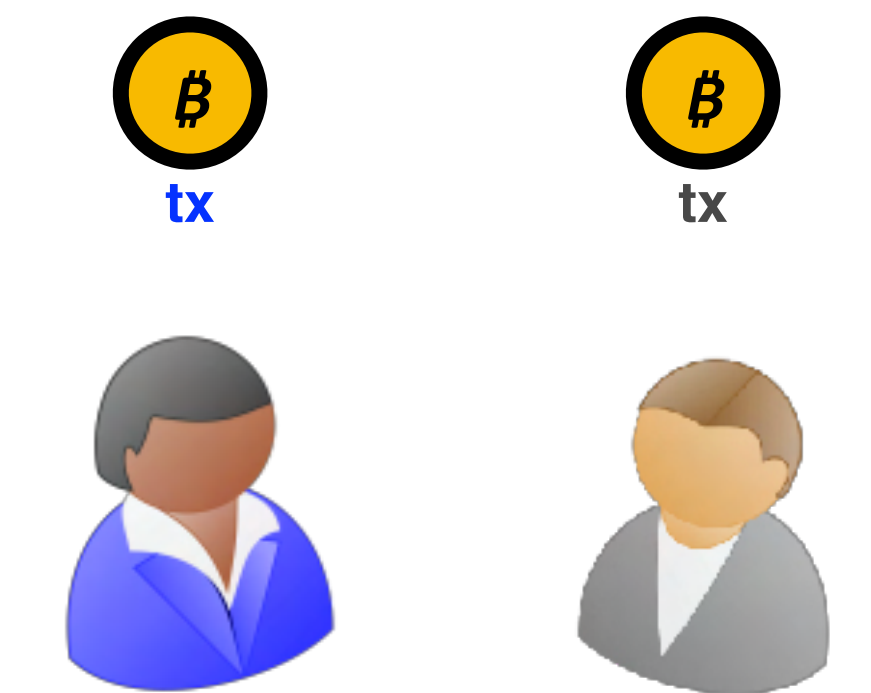
$\mathcal{F}_{Diffuse}^{K-}$



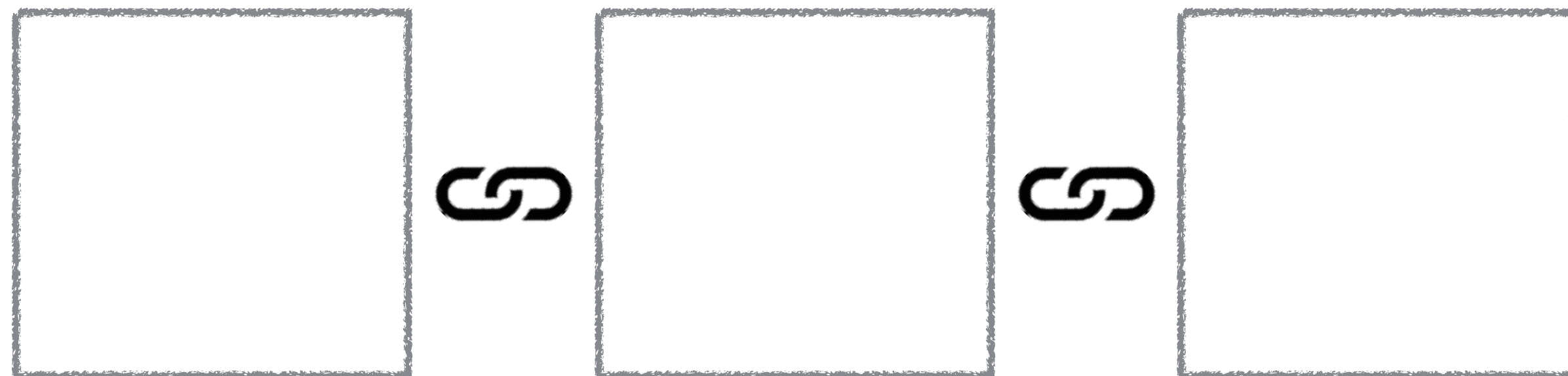
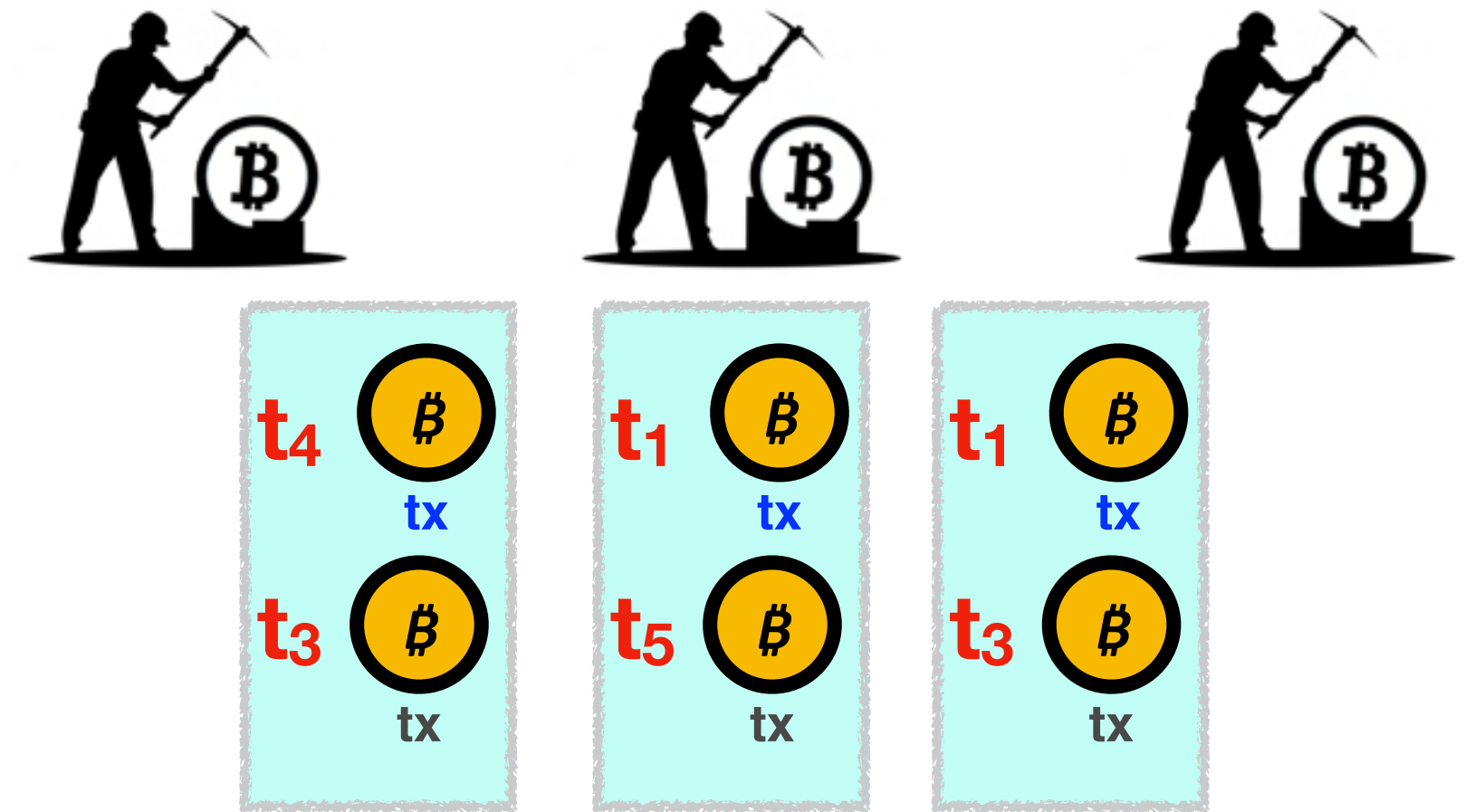
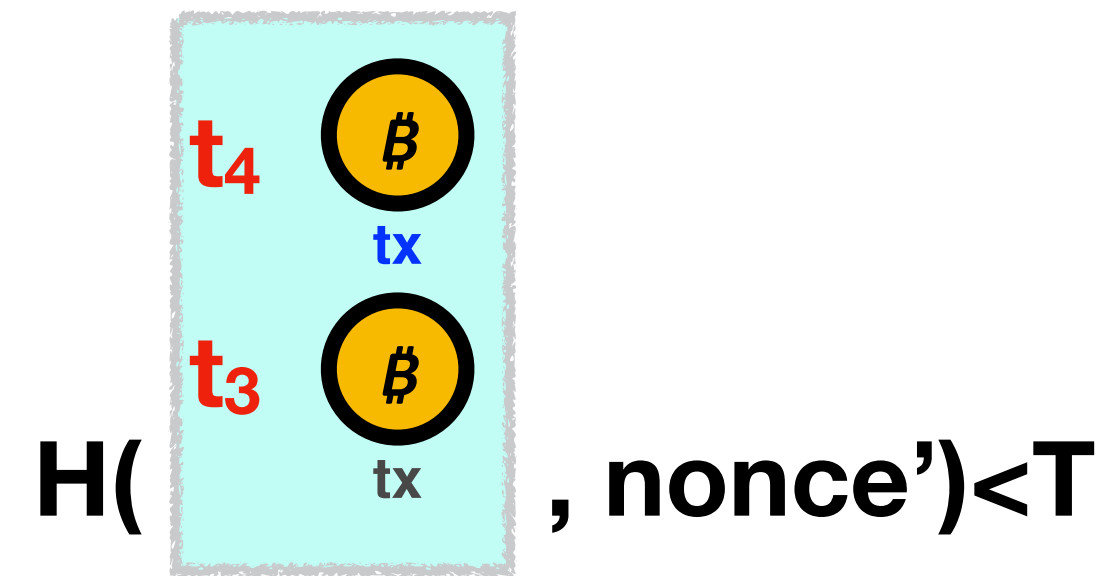
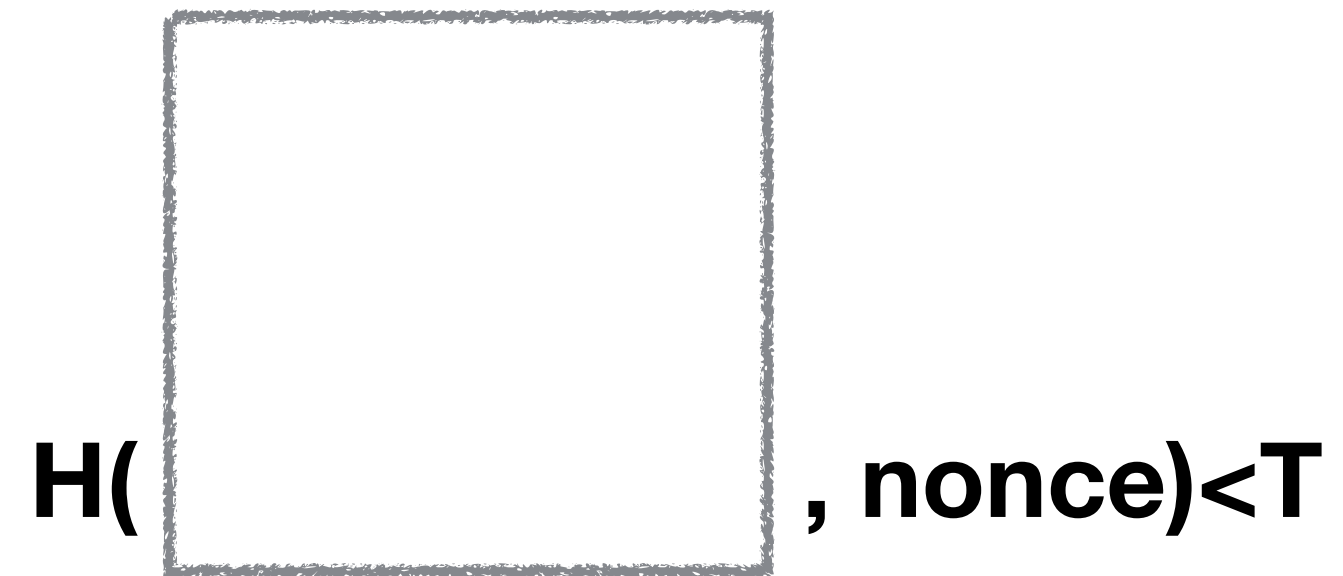
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



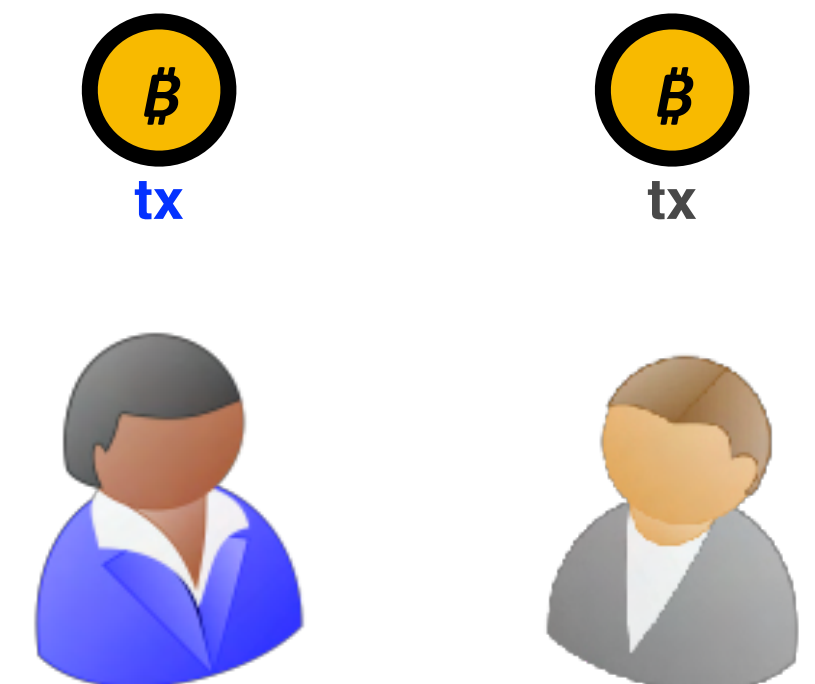
$\mathcal{F}_{Diffuse}^{K-}$



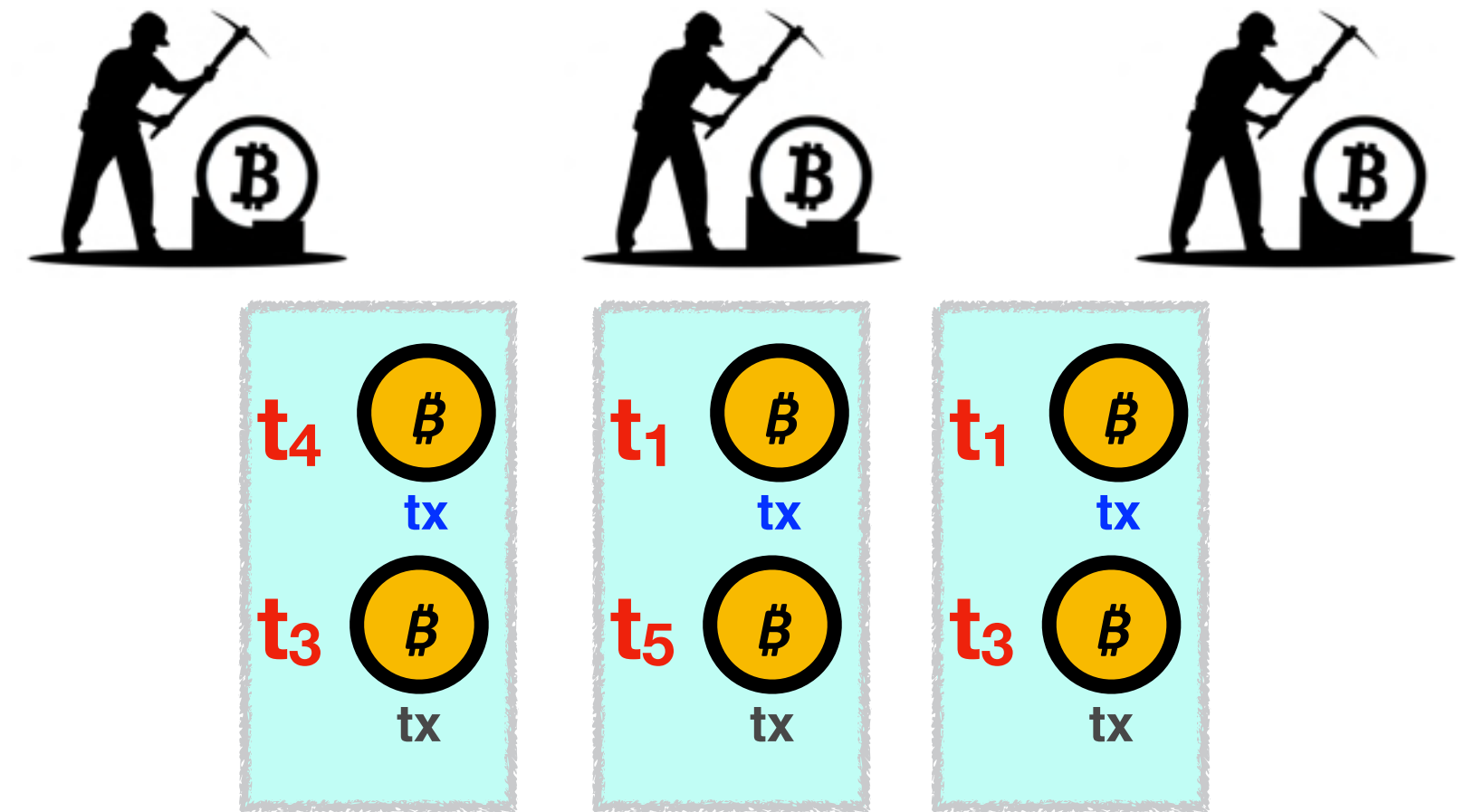
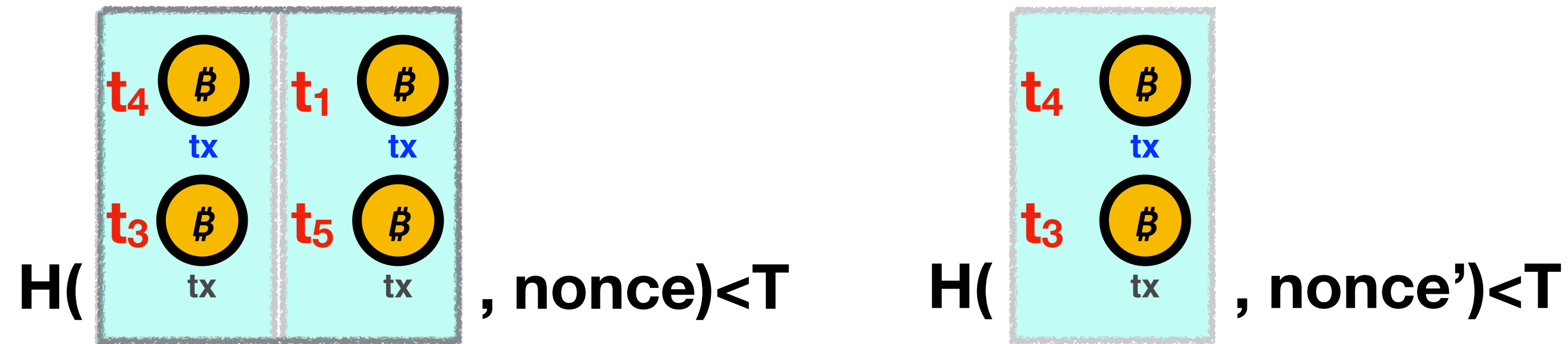
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



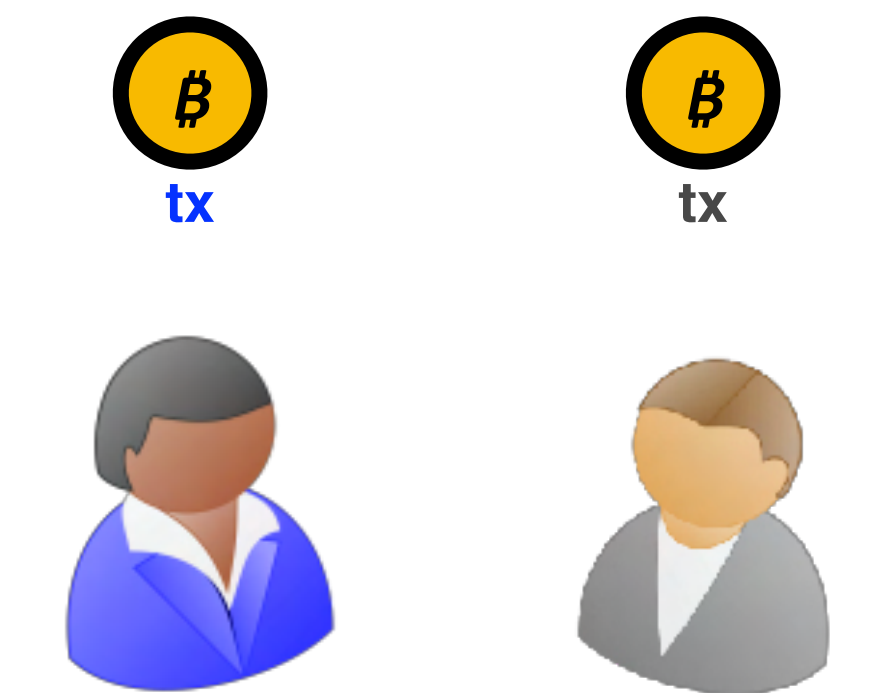
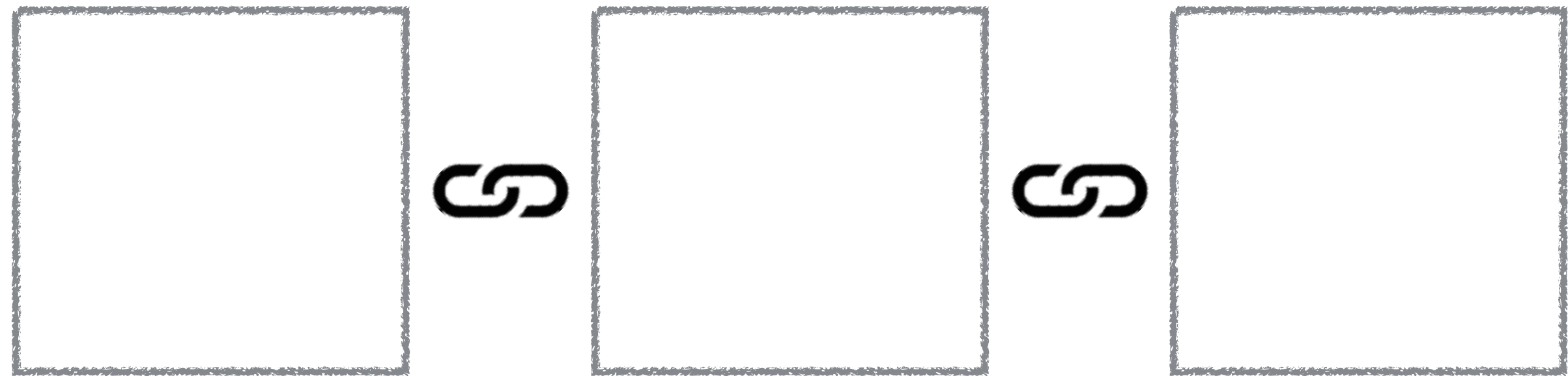
$\mathcal{F}_{Diffuse}^{K-}$



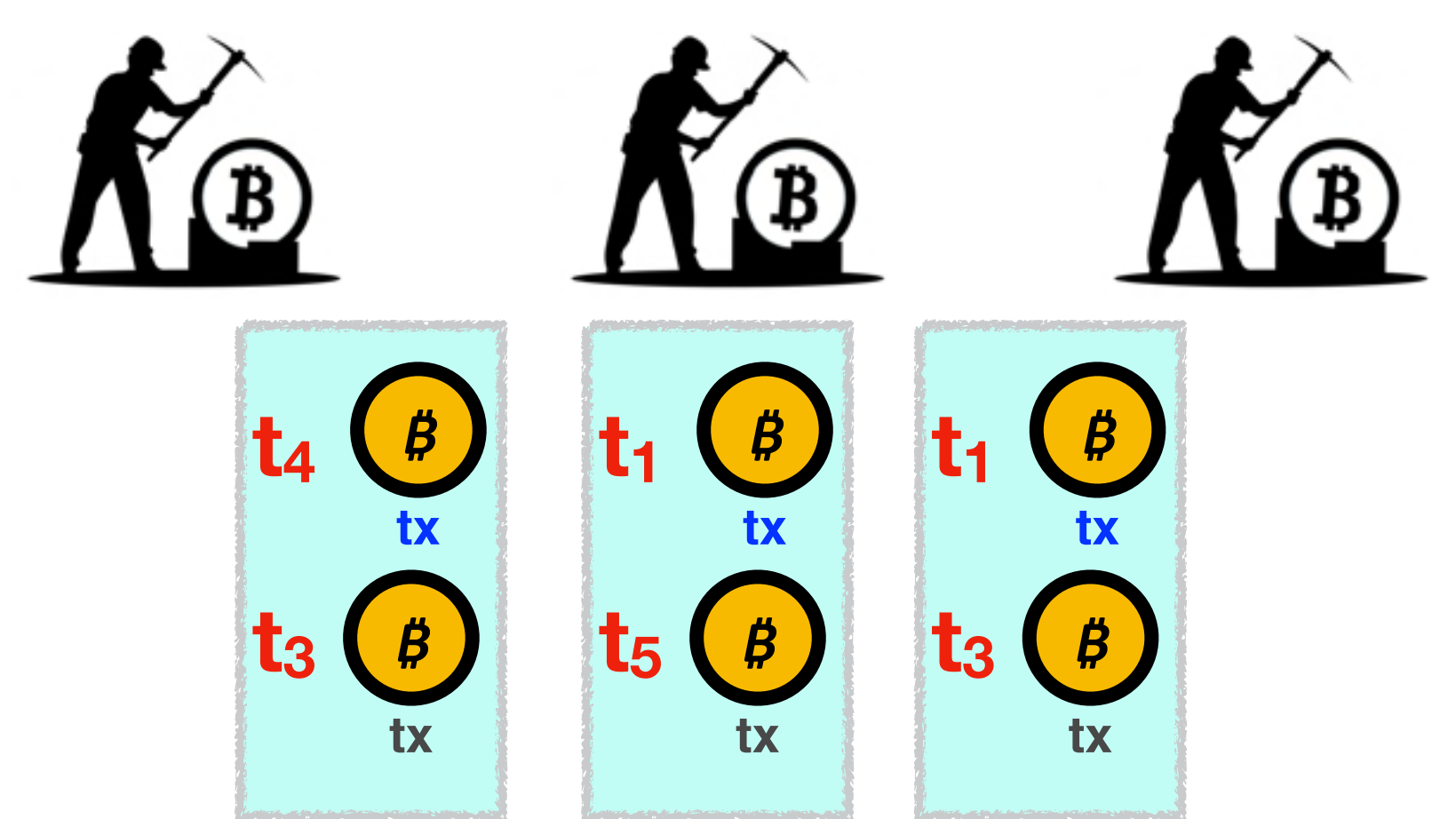
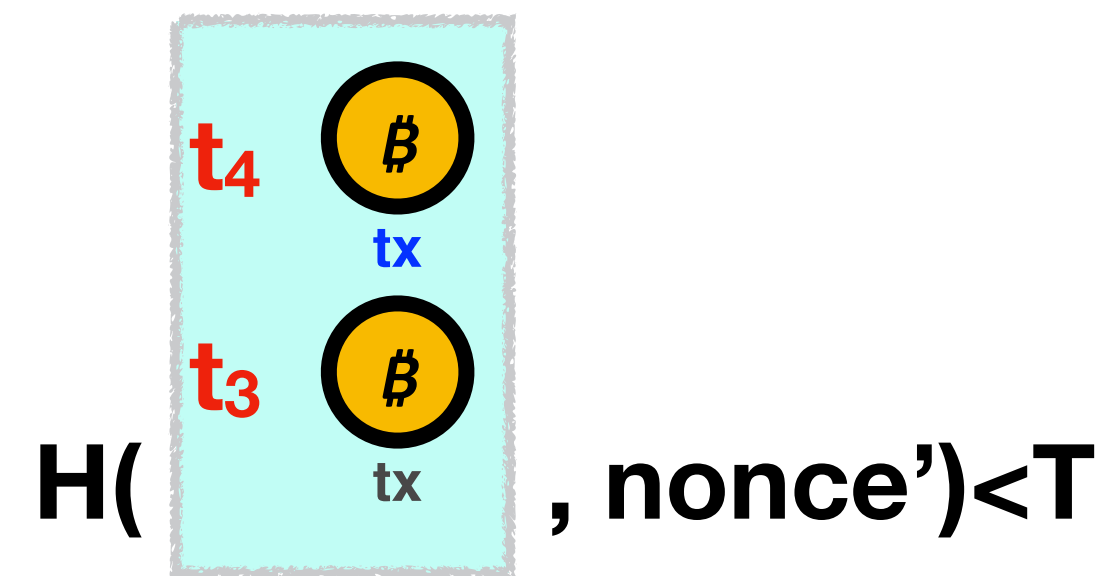
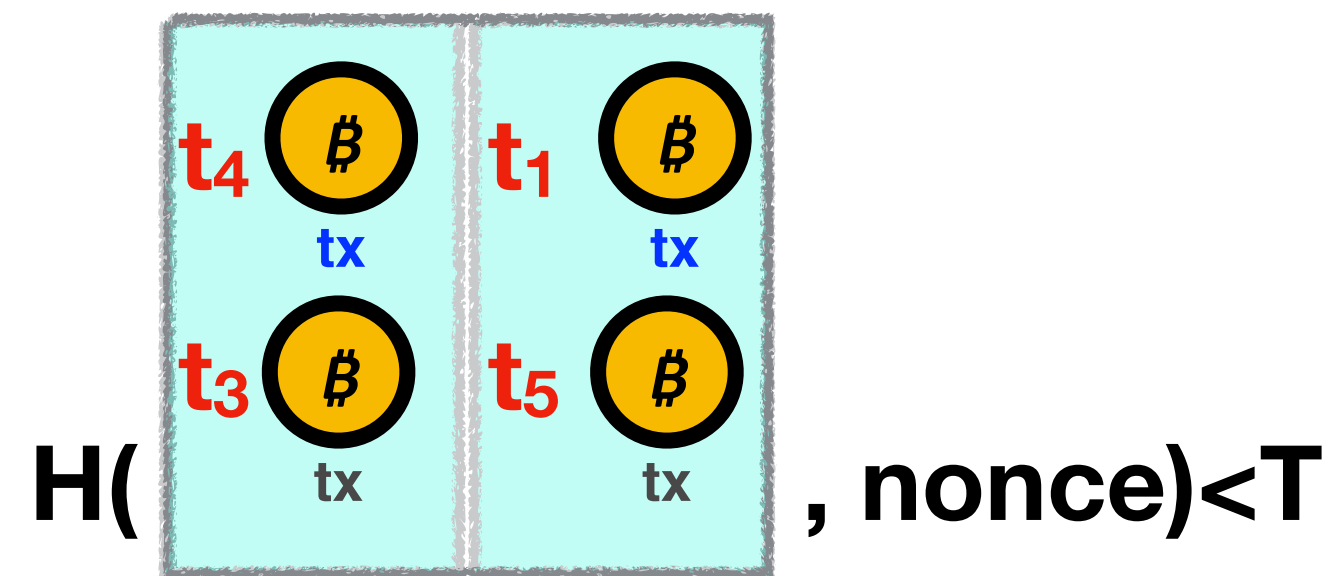
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



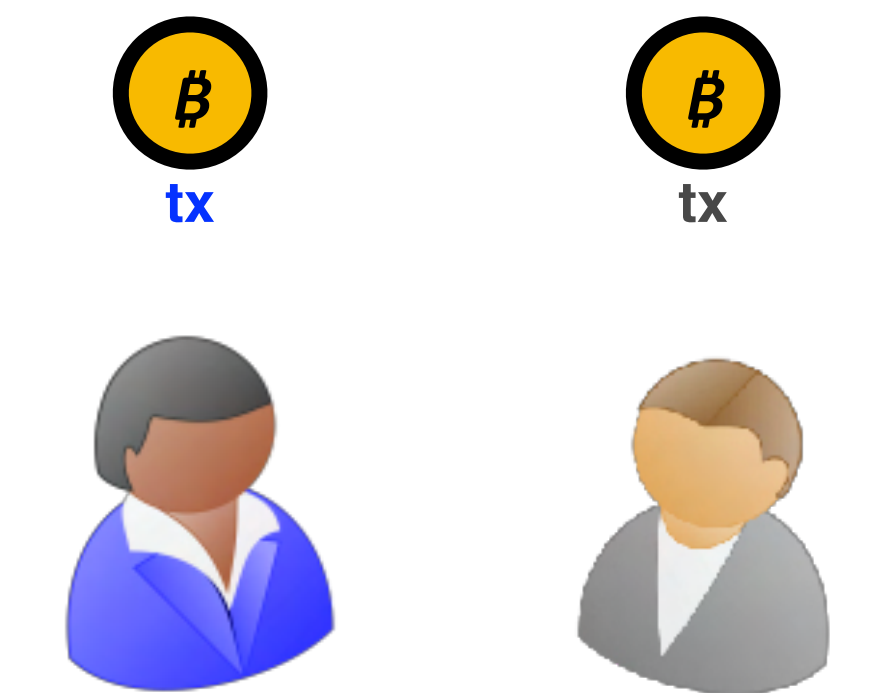
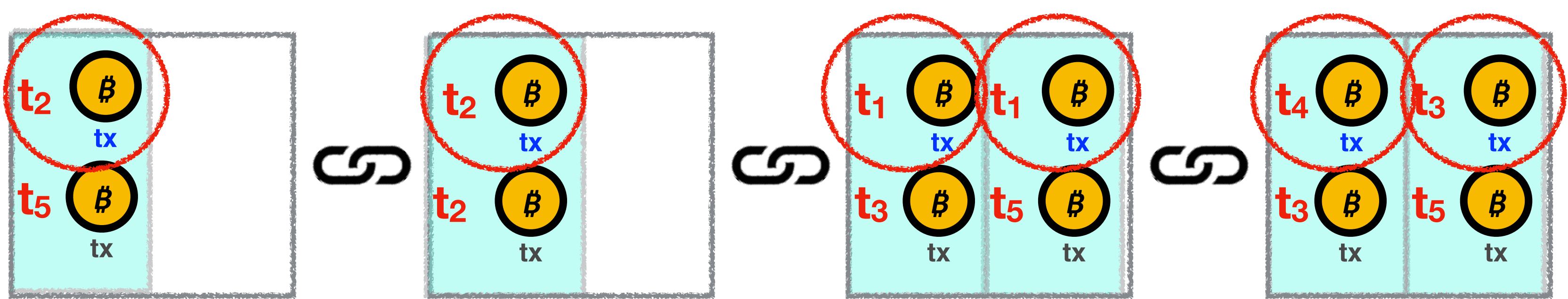
$\mathcal{F}_{Diffuse}^{K-}$



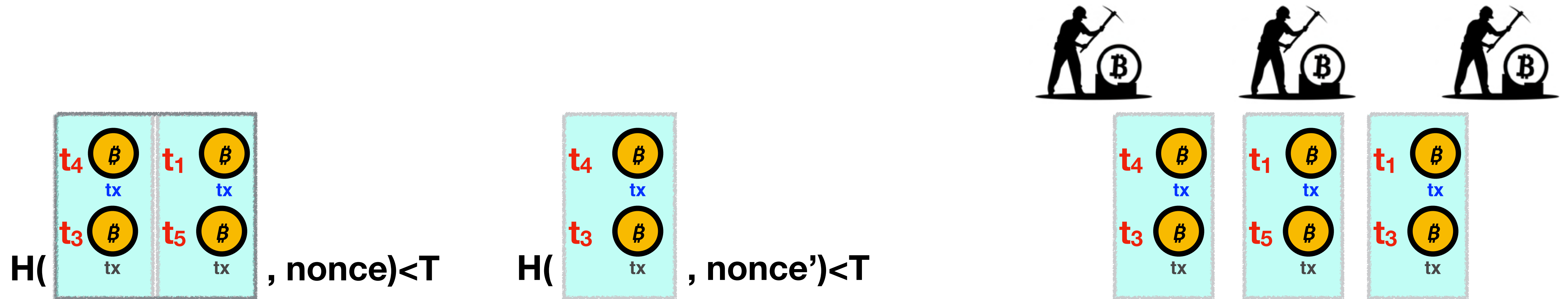
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



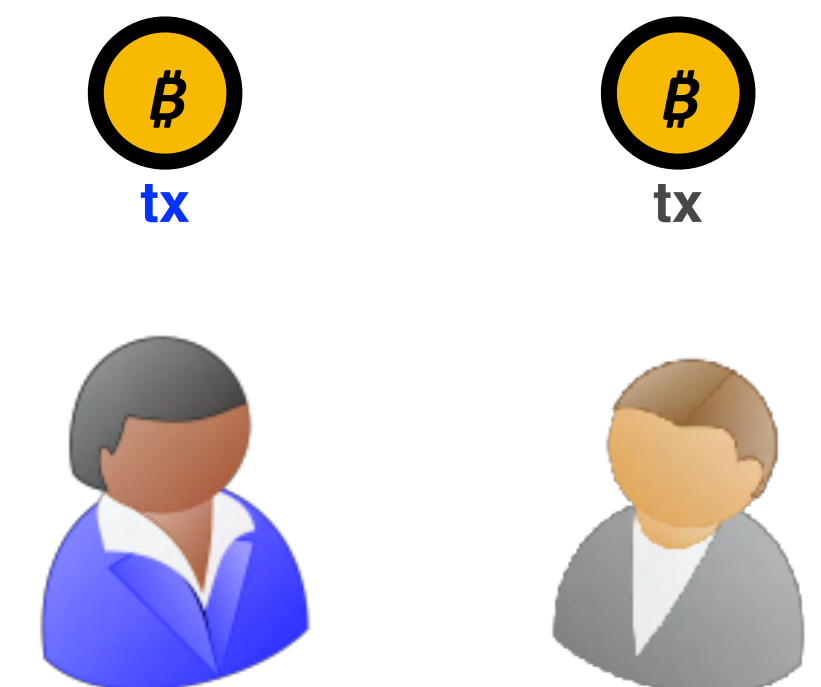
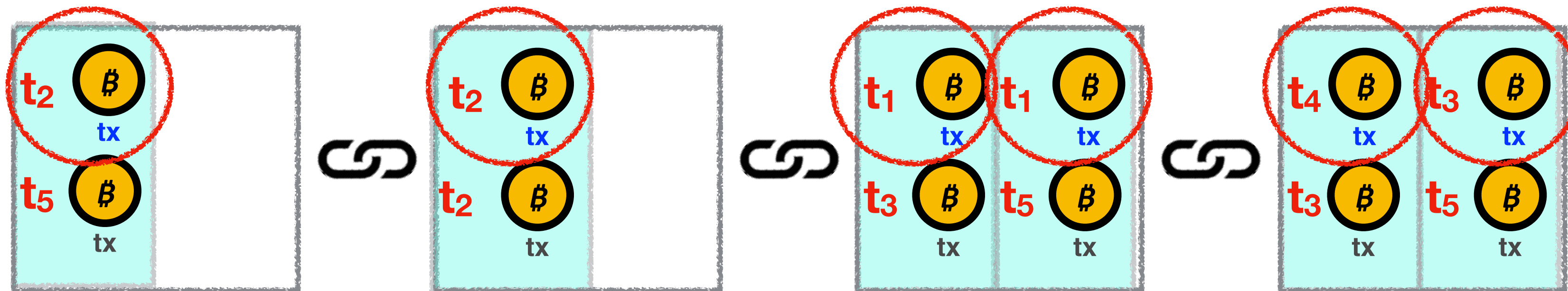
$\mathcal{F}_{Diffuse}^{K-}$



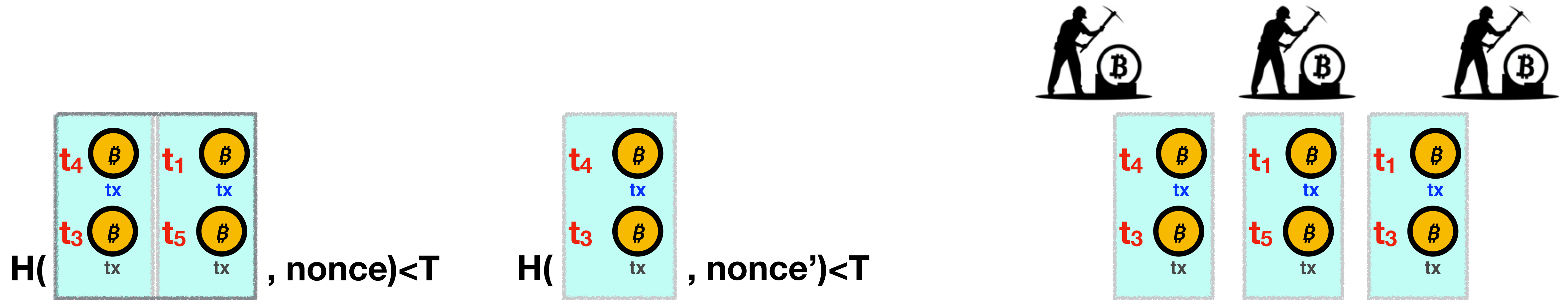
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



$\text{Median}\{t_1, t_1, t_2, t_2, t_3, t_4\} = t_2$



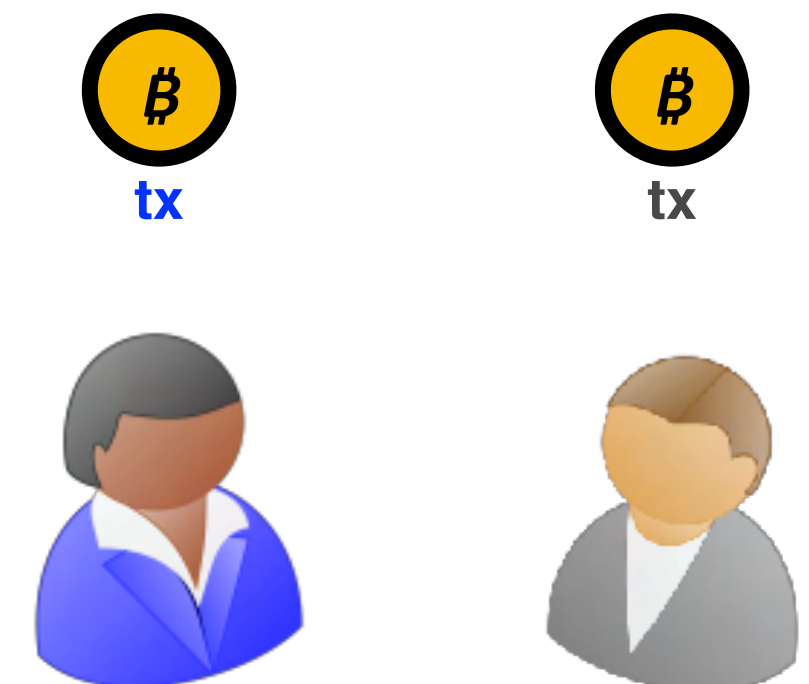
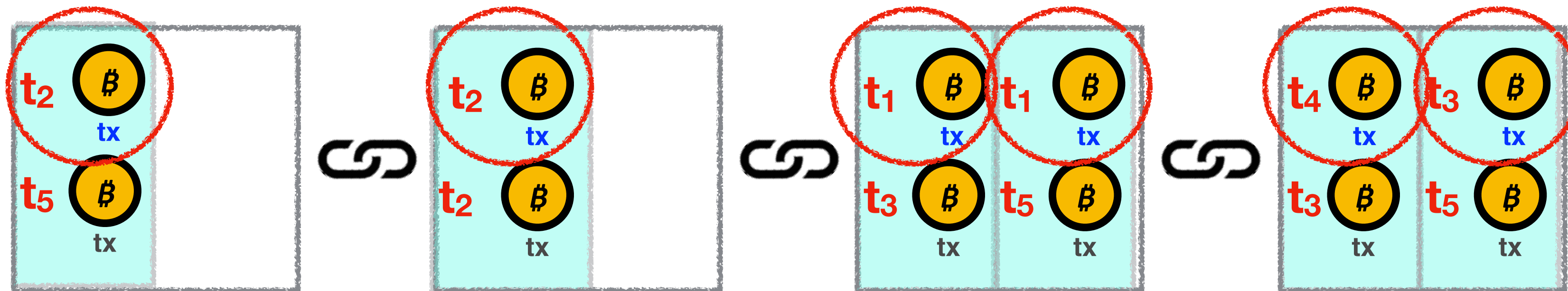
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



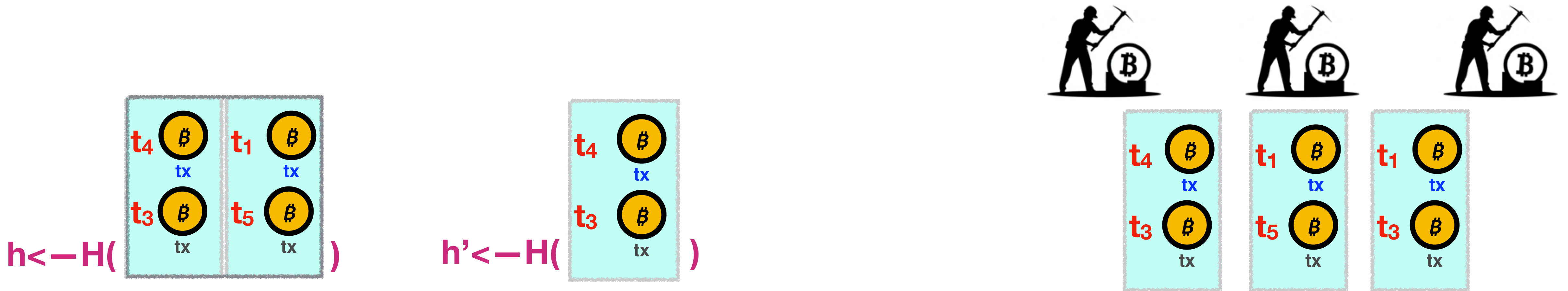
$\text{Median}\{t_1, t_1, t_2, t_2, t_3, t_4\} = t_2$

 has timestamp t_2

$\mathcal{F}_{Diffuse}^{K-}$



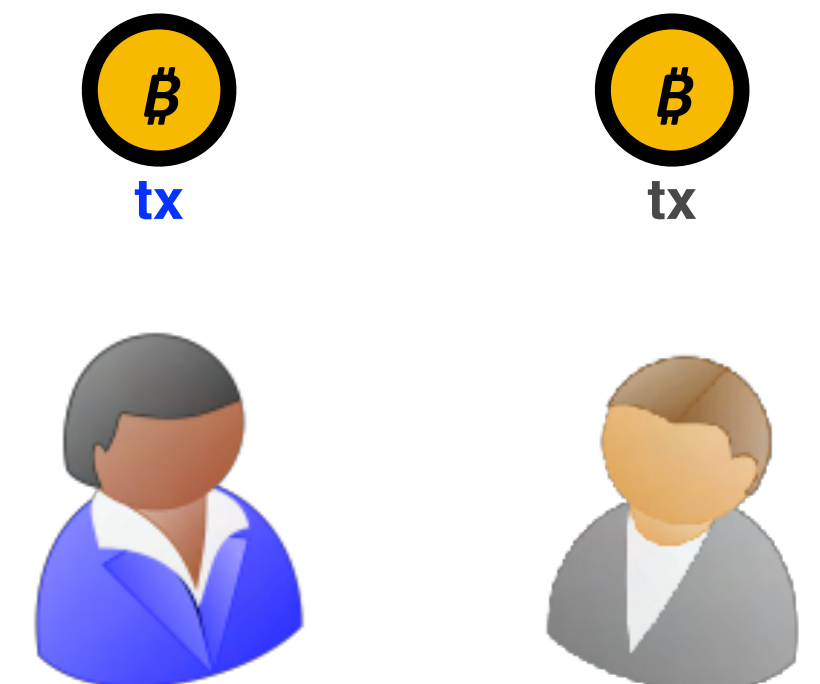
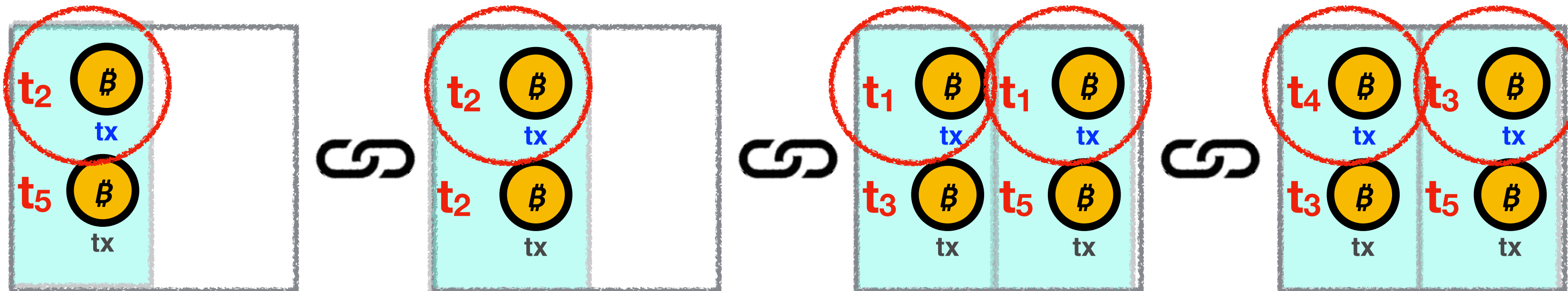
How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



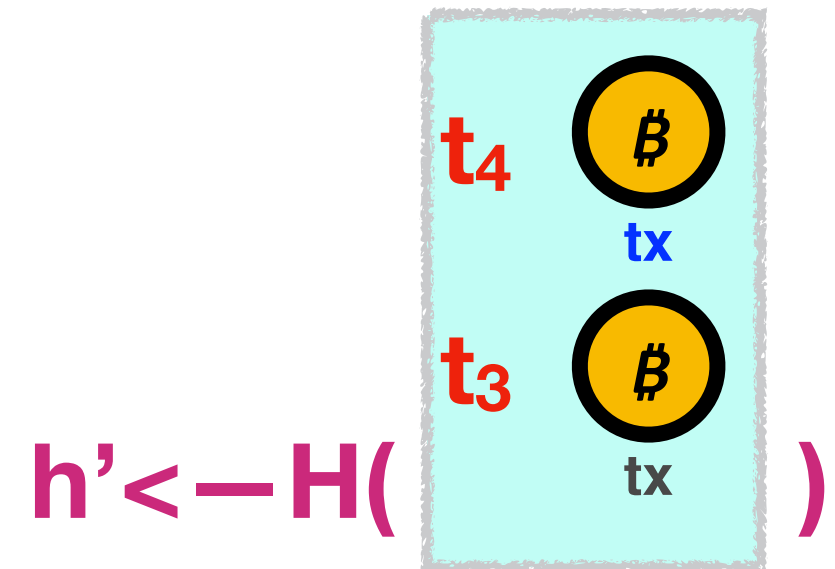
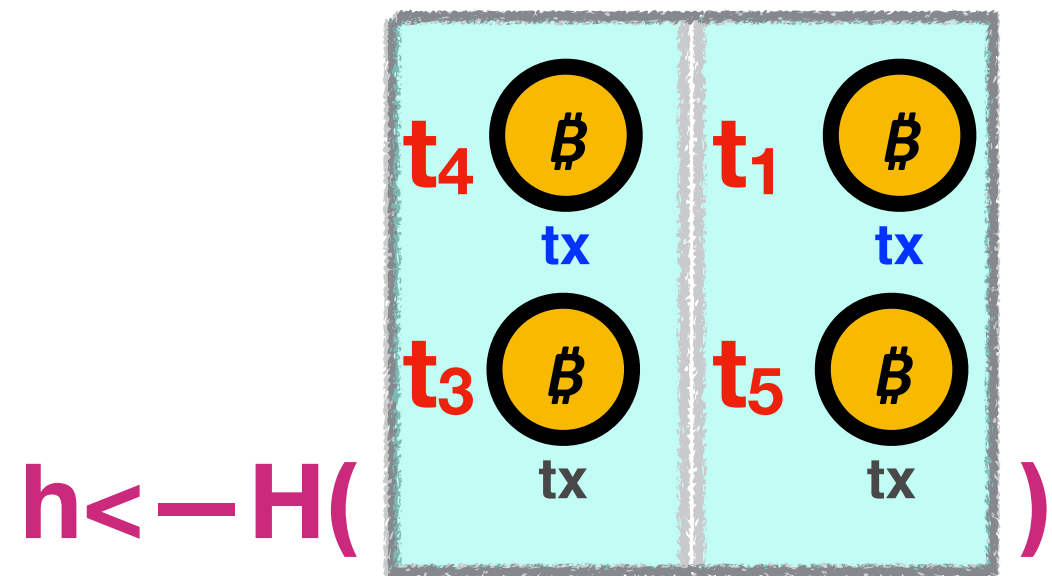
$\text{Median}\{t_1, t_1, t_2, t_2, t_3, t_4\} = t_2$

 has timestamp t_2

$\mathcal{F}_{Diffuse}^{K-}$



How to realize $\mathcal{F}_{Ledger}^{Fair}$ for $\Delta \geq K$



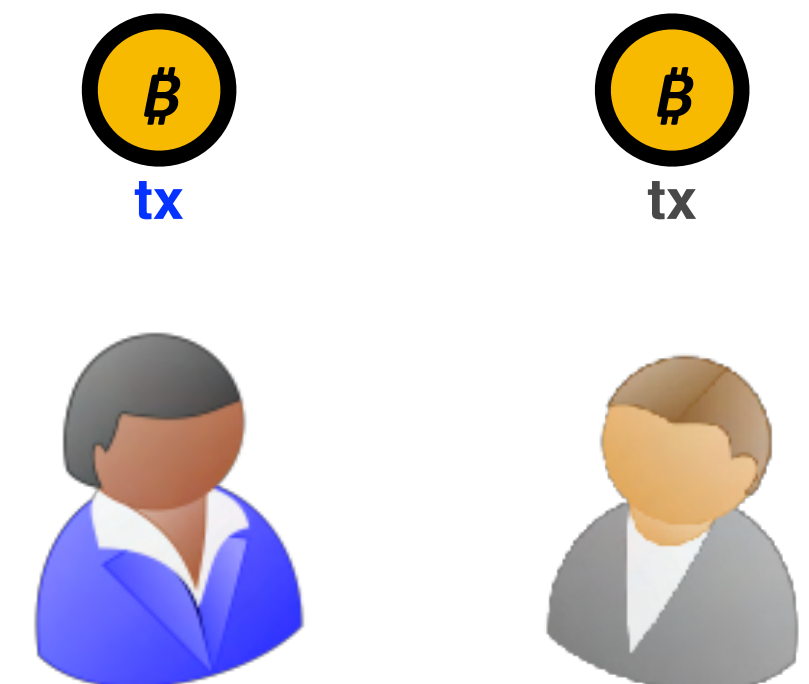
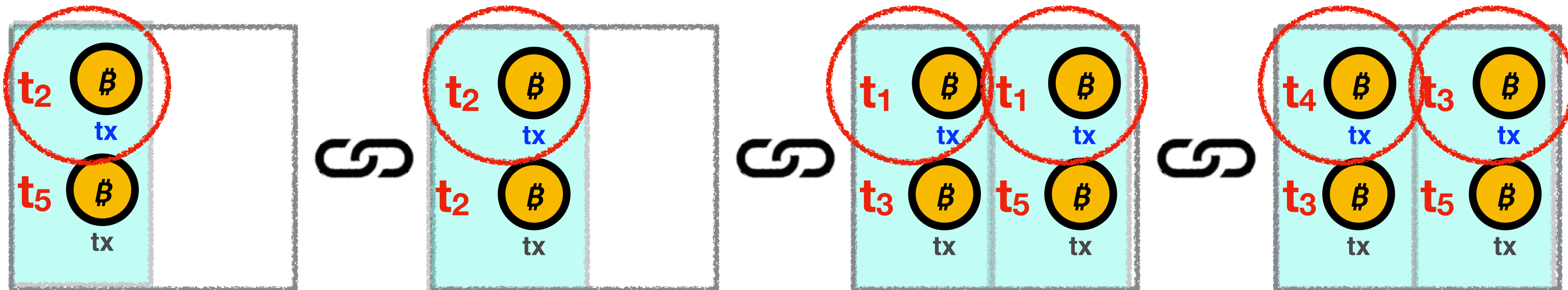
2-for-1 PoW [GKL15]

$w \leftarrow -H(h', h, \text{nonce})$
 If $w < T$ then standard block
 If $[w]^R < T$ then profile block

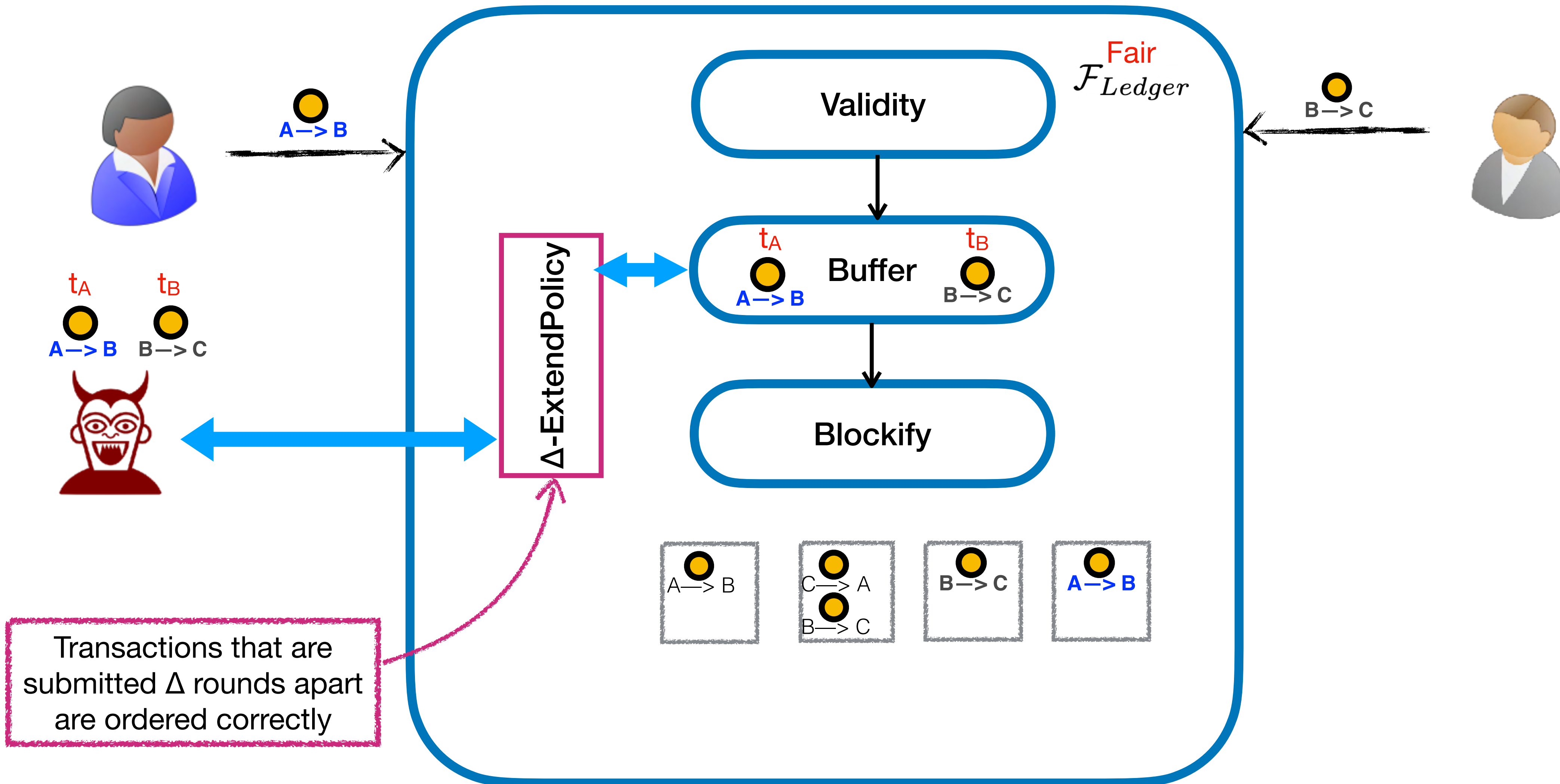
$\text{Median}\{t_1, t_1, t_2, t_2, t_3, t_4\} = t_2$



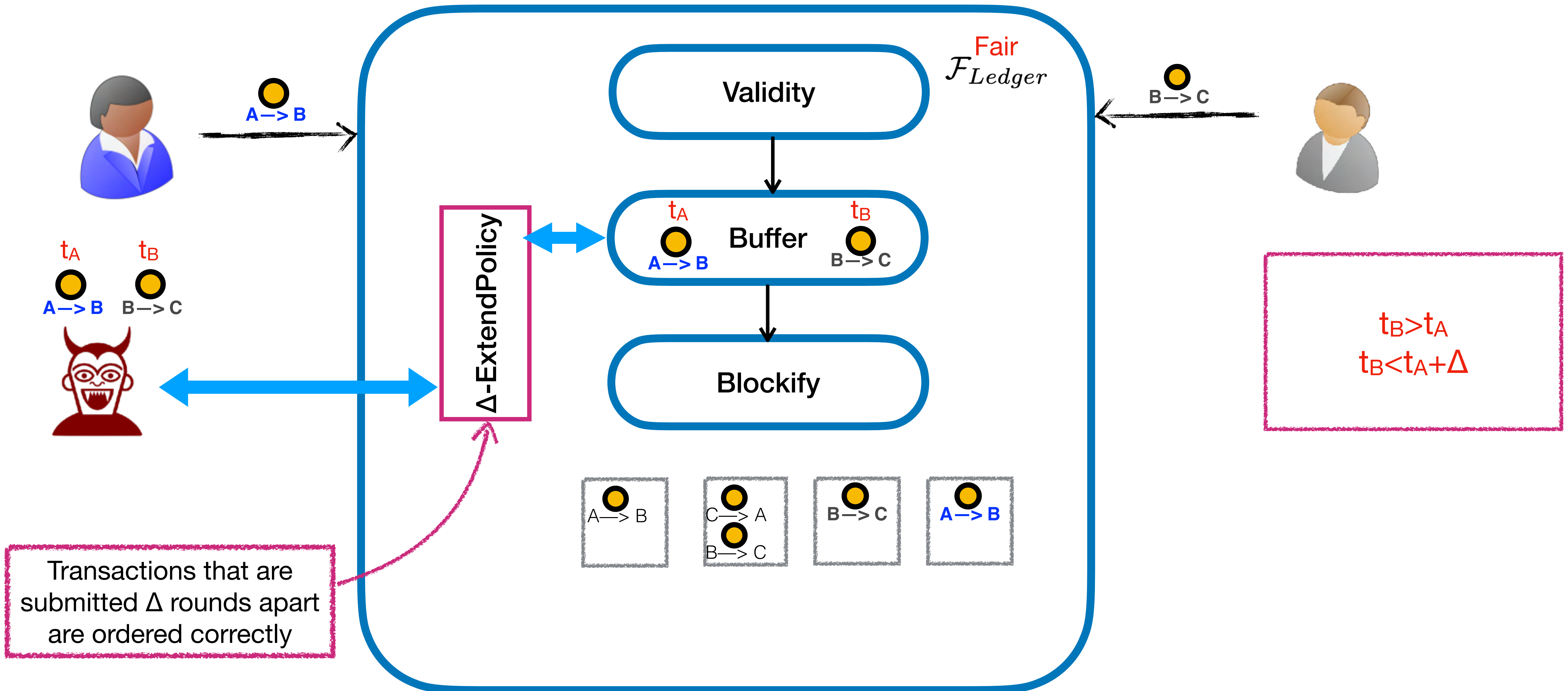
$\mathcal{F}_{Diffuse}^K$



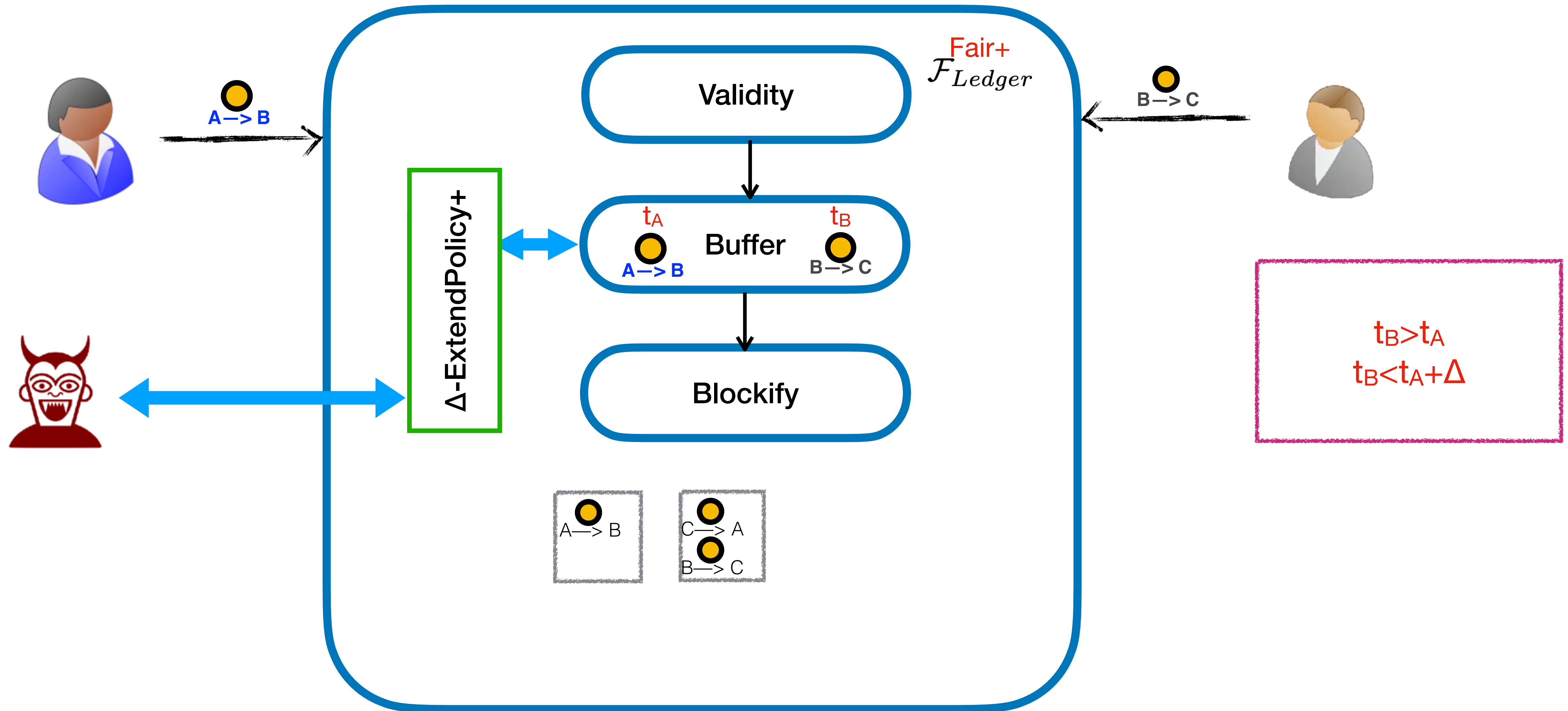
Can we do something for transactions submitted not much apart?



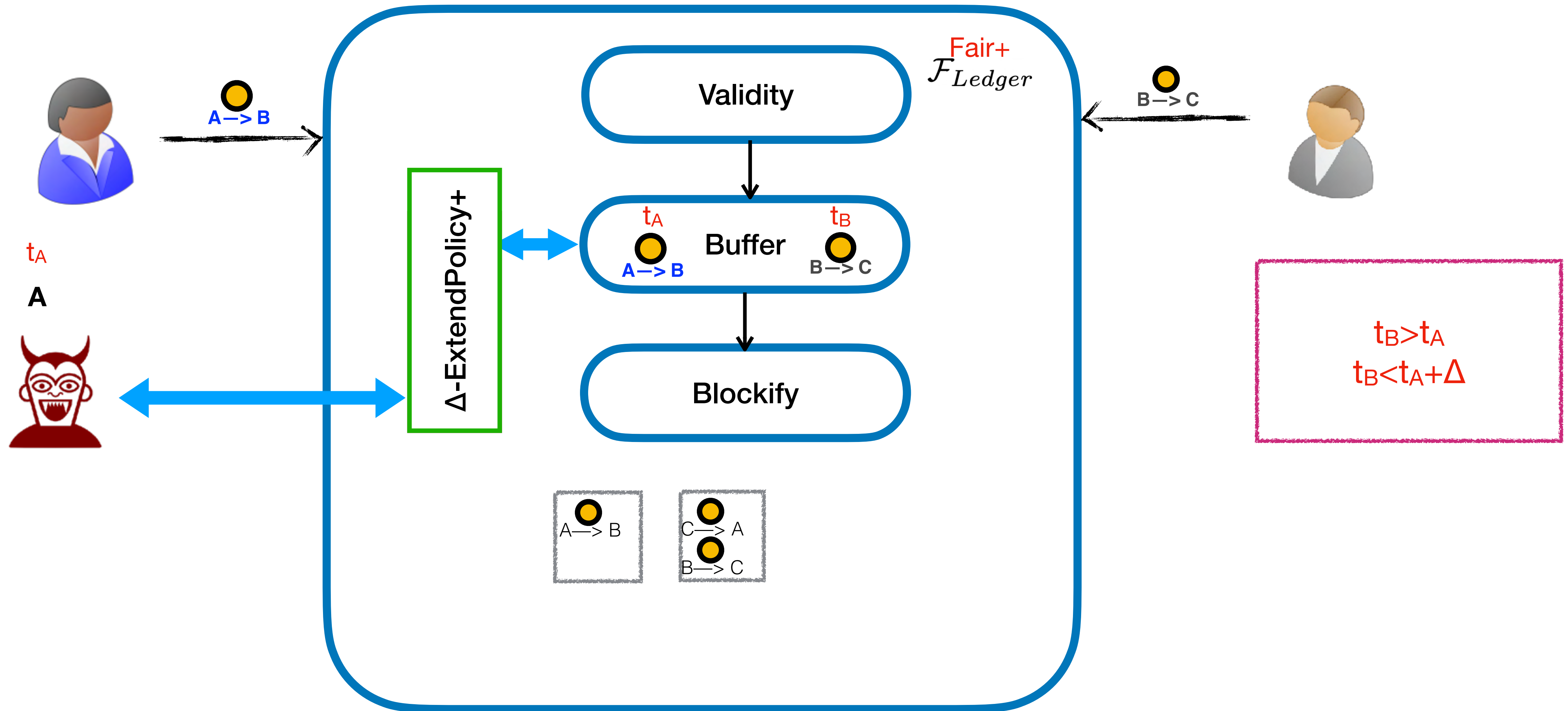
Can we do something for transactions submitted not much apart?



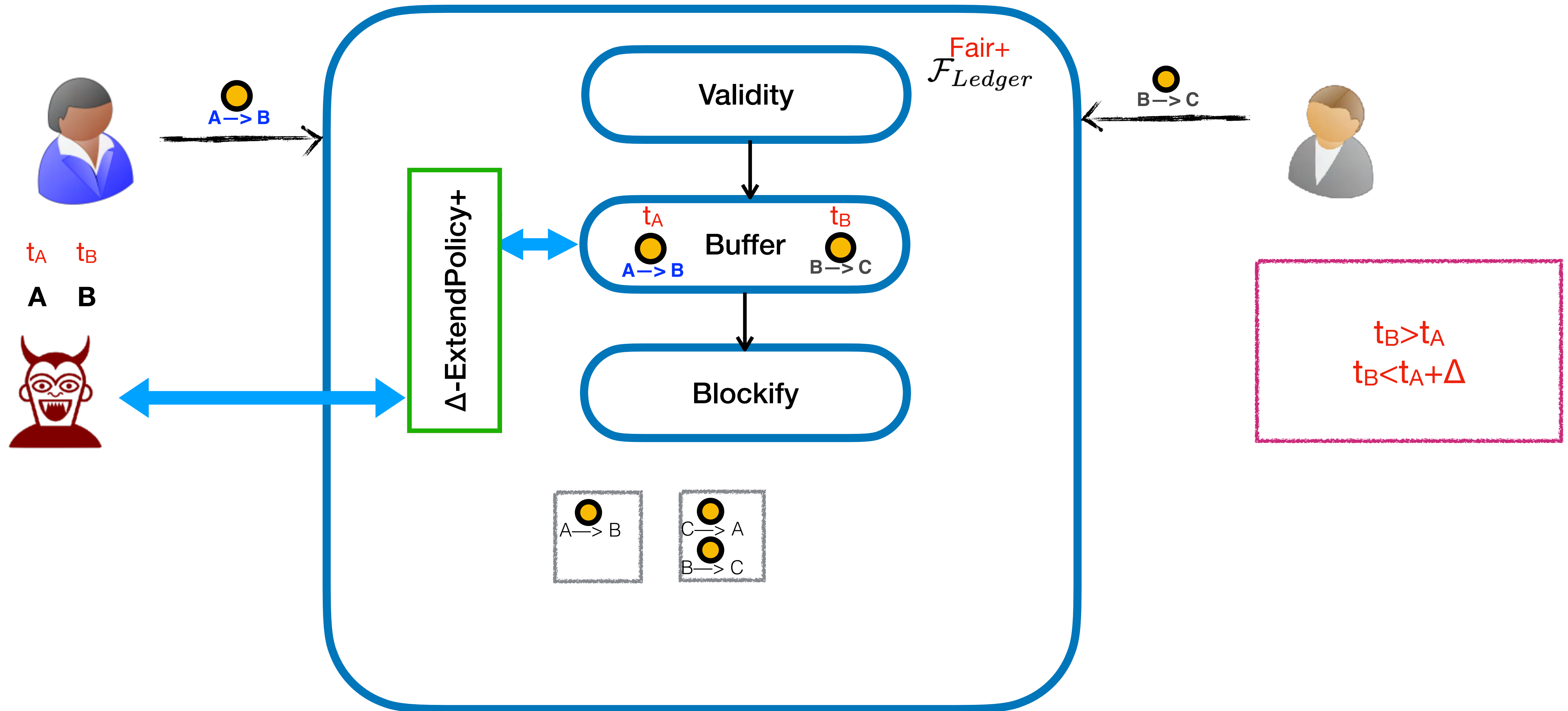
Can we do something for transactions submitted not much apart?



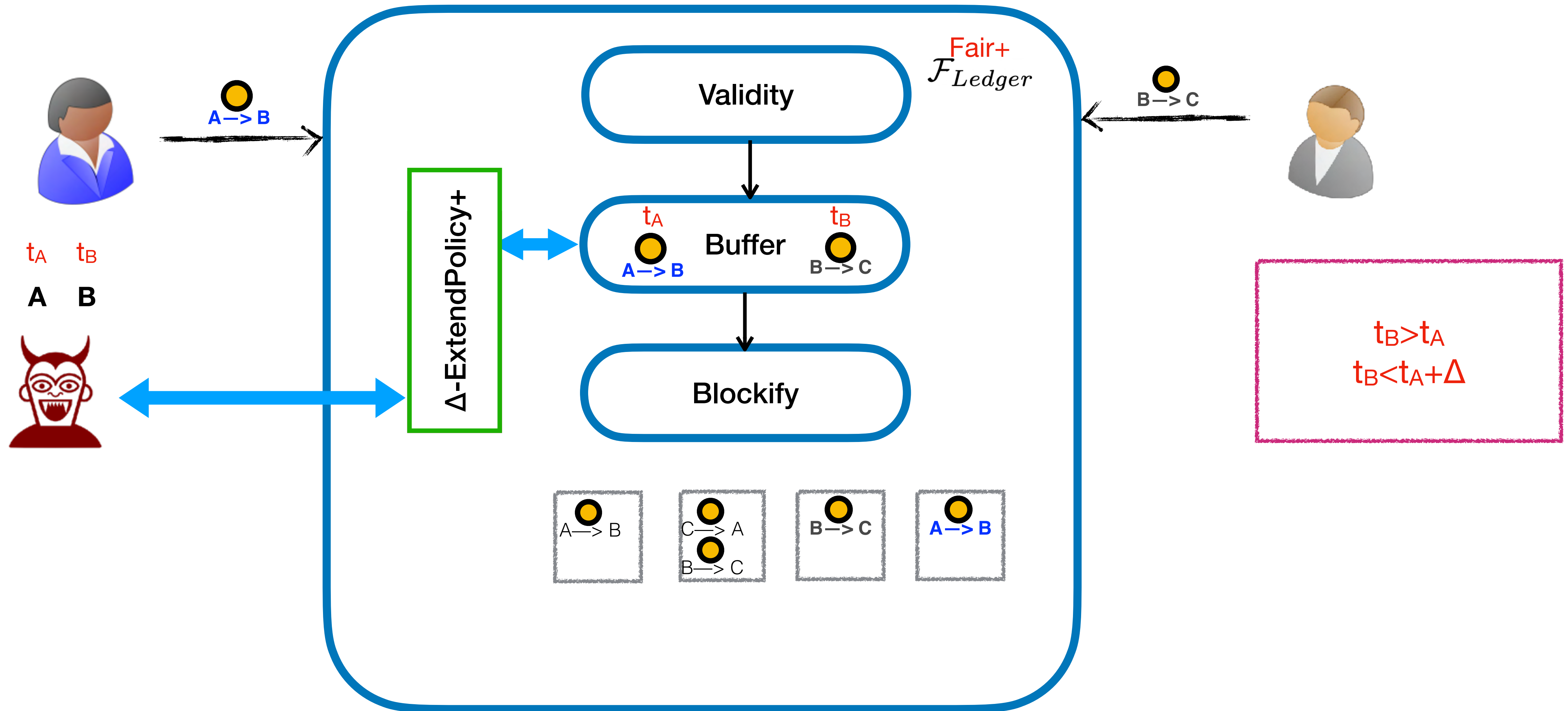
Can we do something for transactions submitted not much apart?



Can we do something for transactions submitted not much apart?



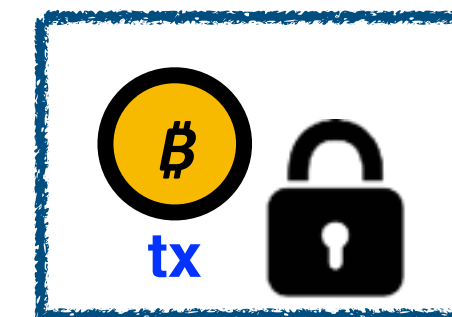
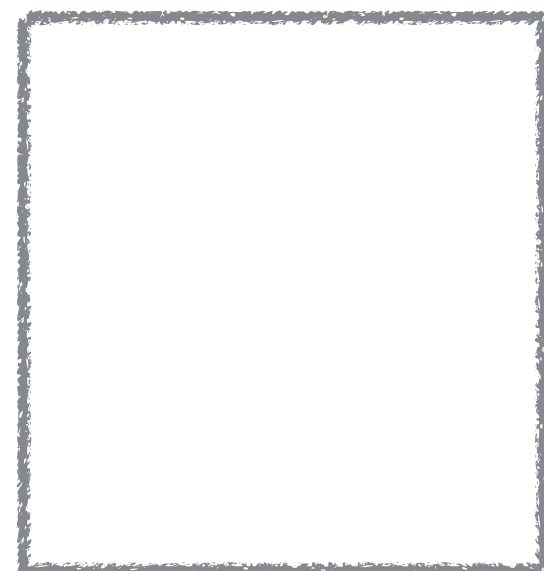
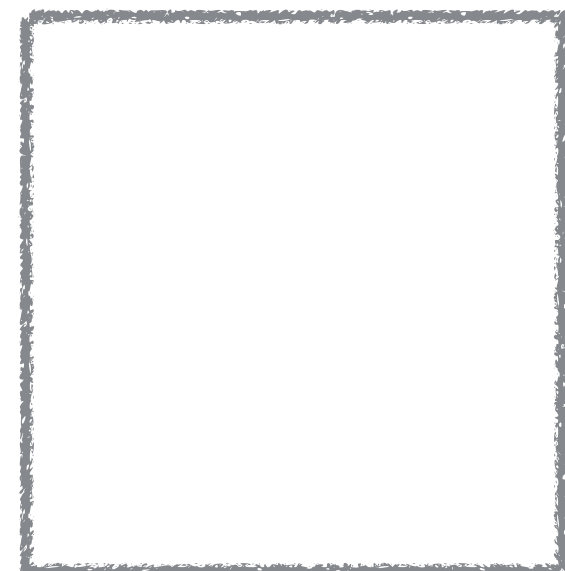
Can we do something for transactions submitted not much apart?



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



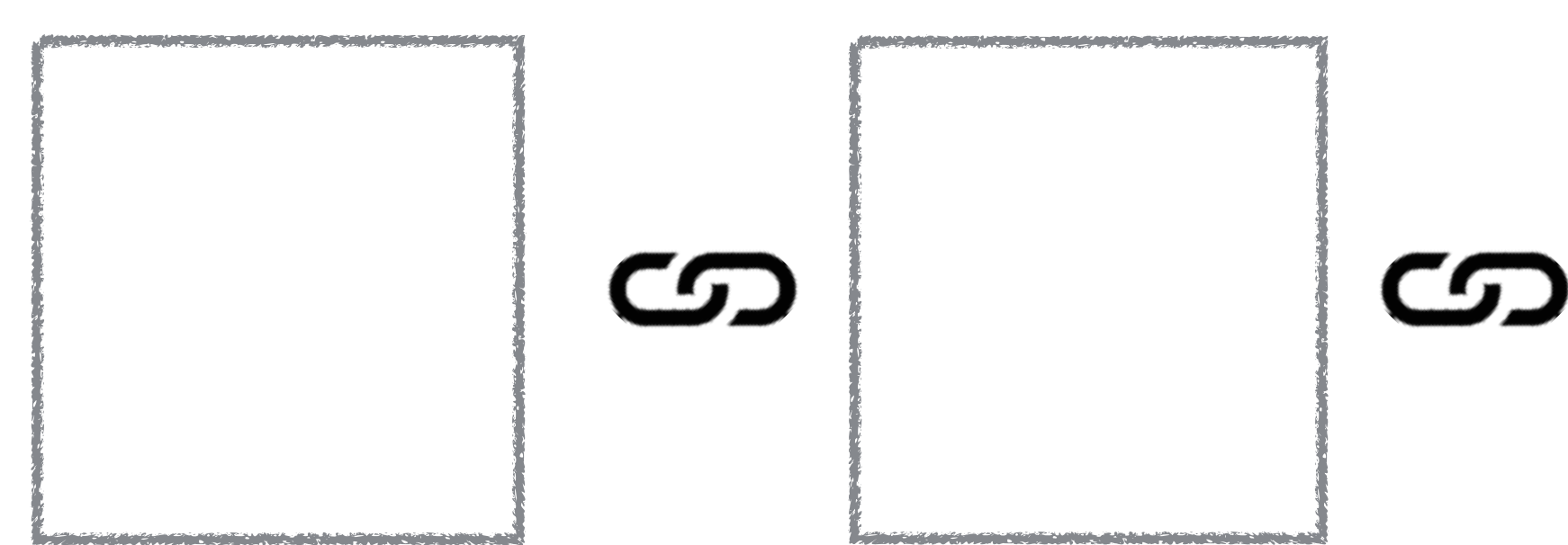
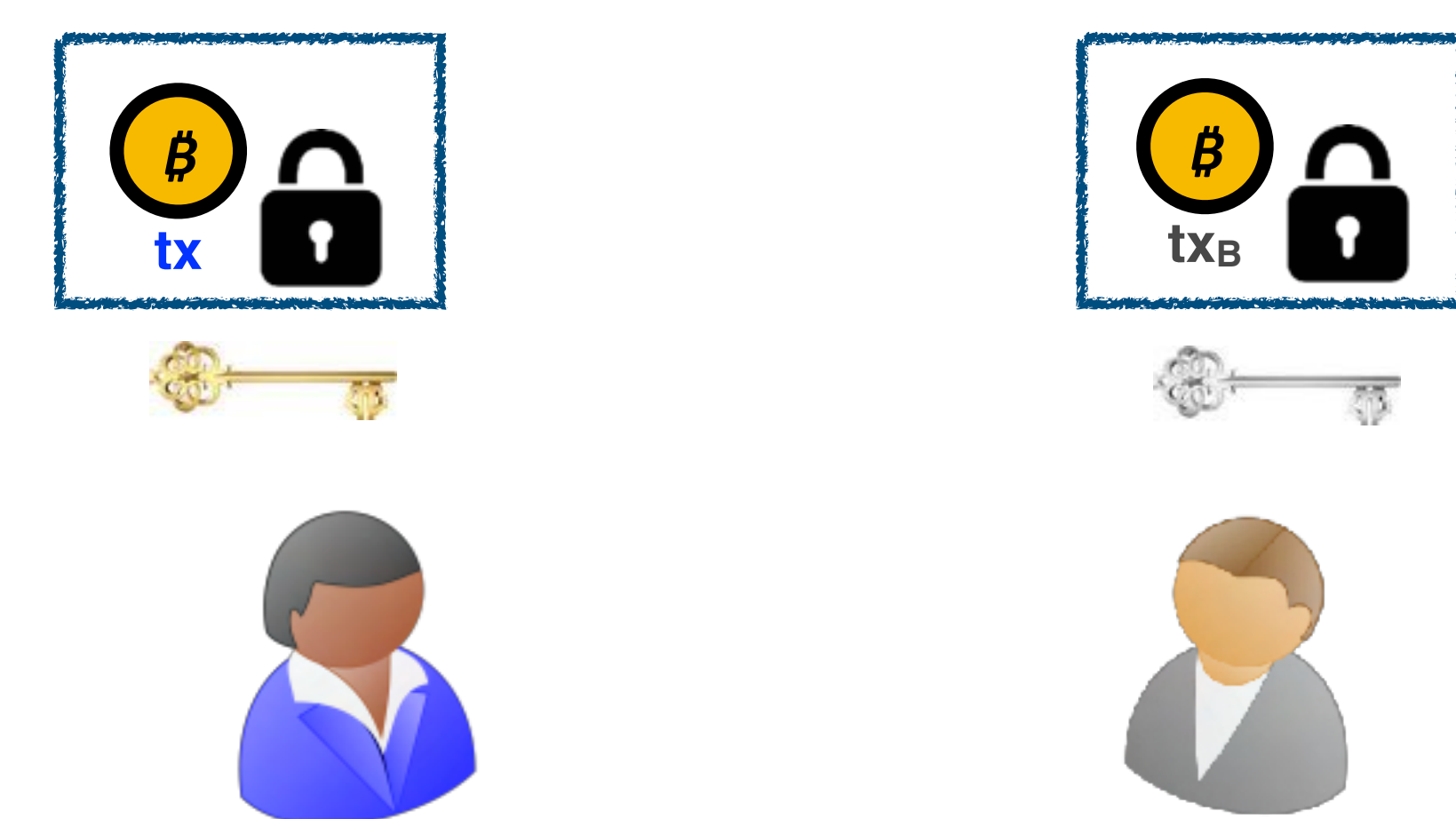
$\mathcal{F}_{Diffuse}^K$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



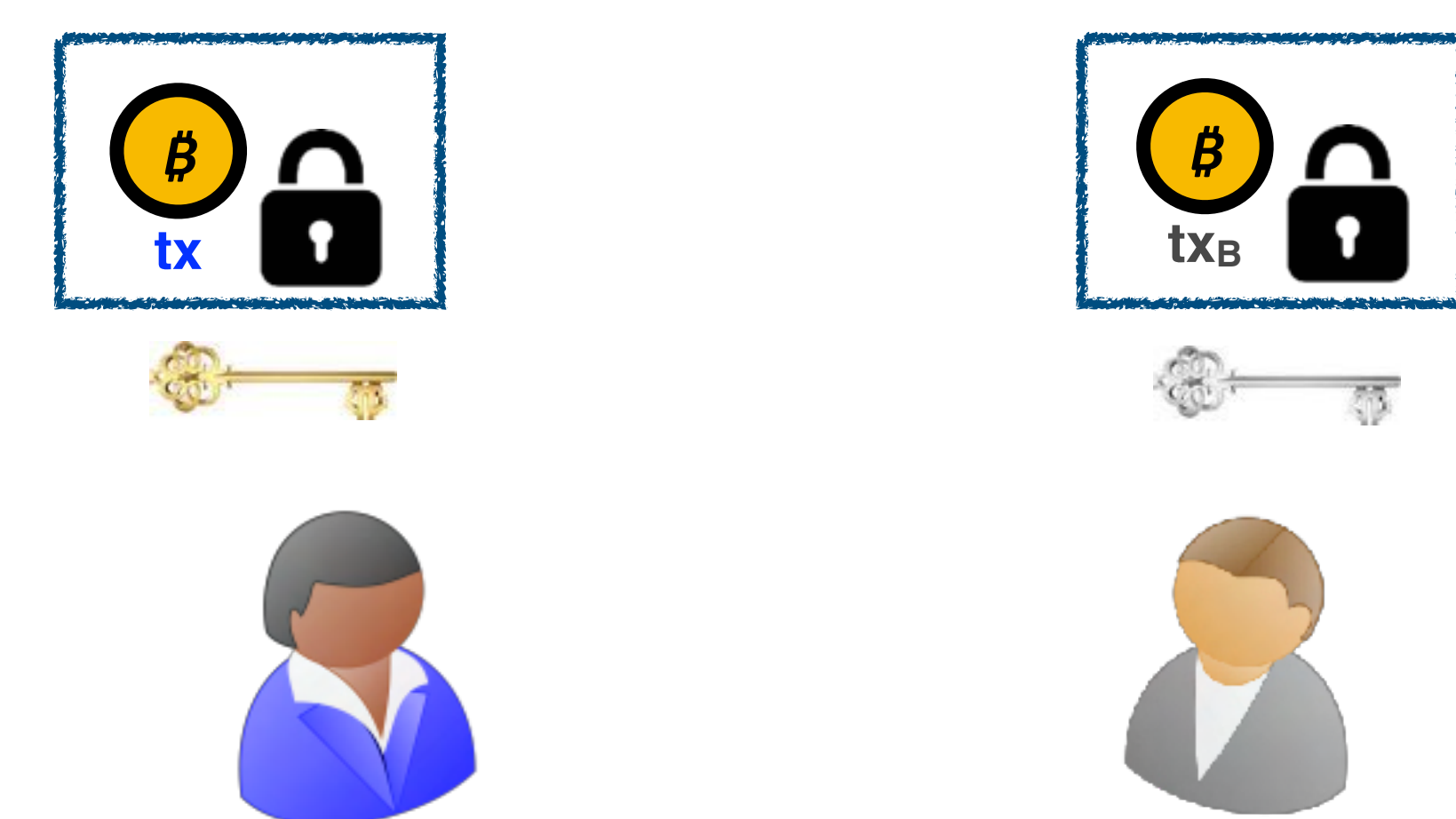
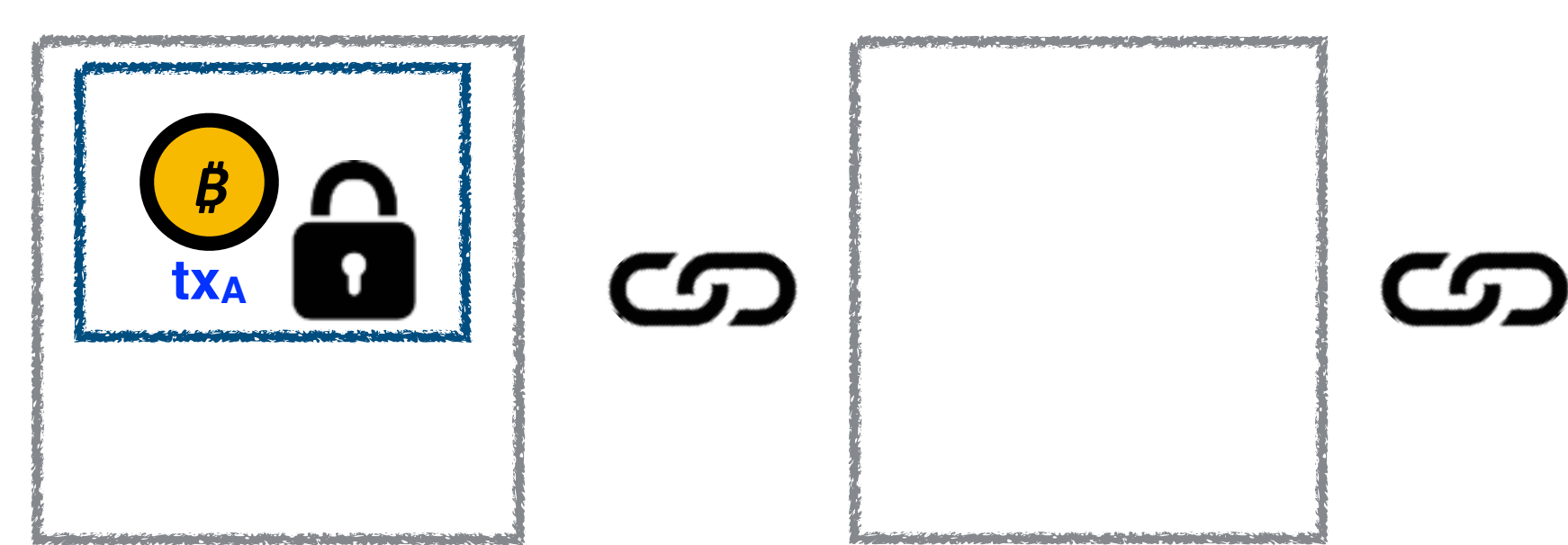
$\mathcal{F}_{Diffuse}^K$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



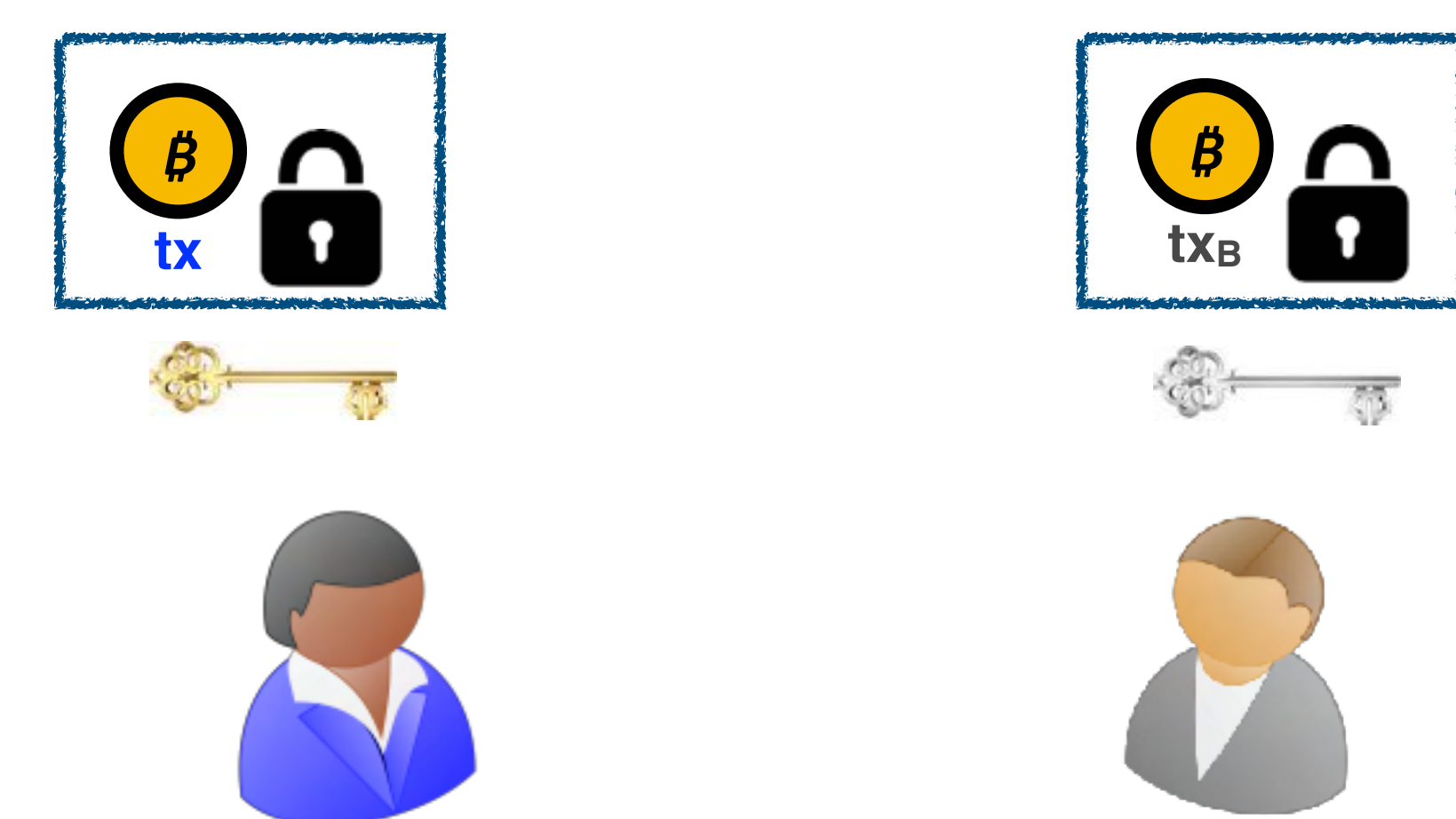
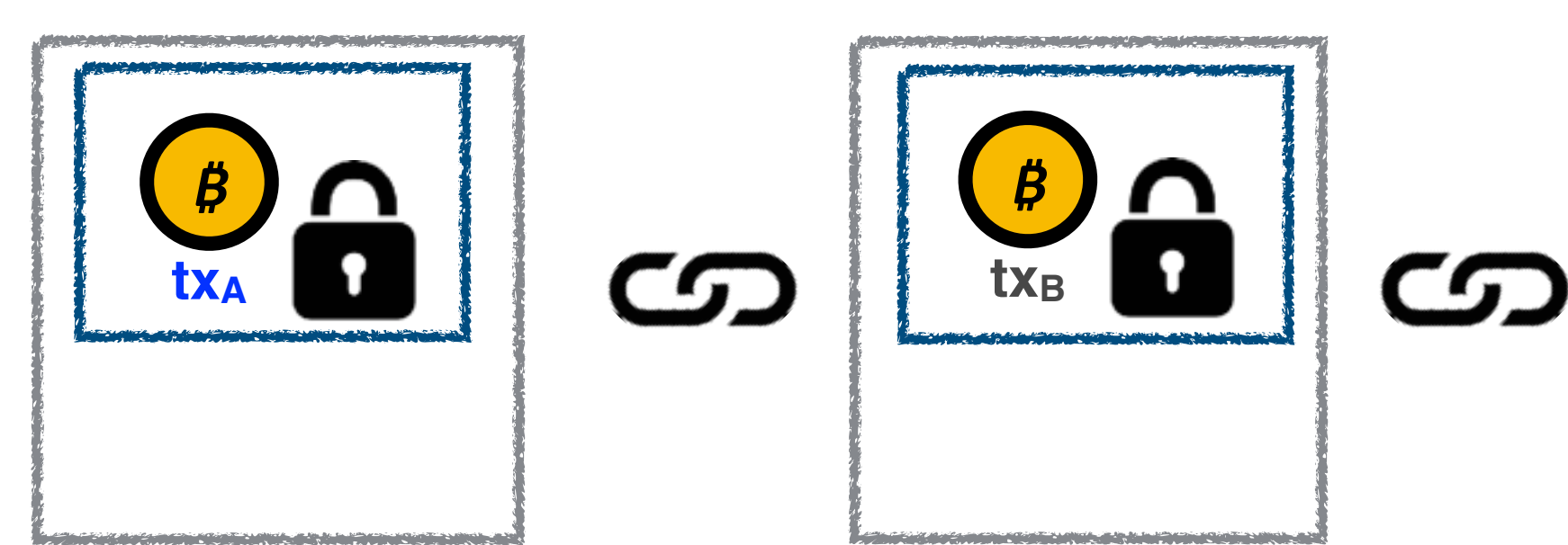
$\mathcal{F}_{Diffuse}^K$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



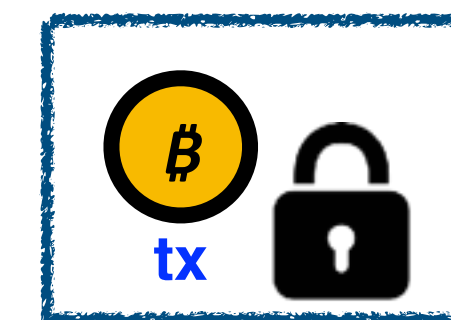
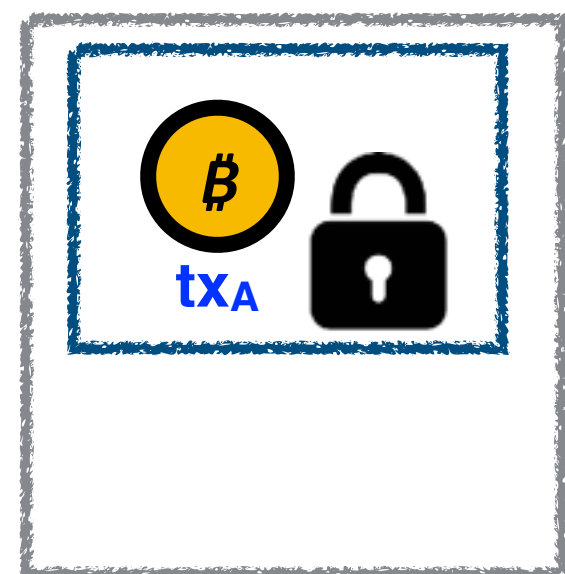
$\mathcal{F}_{Diffuse}^K$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



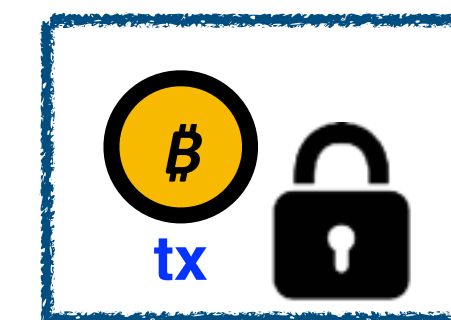
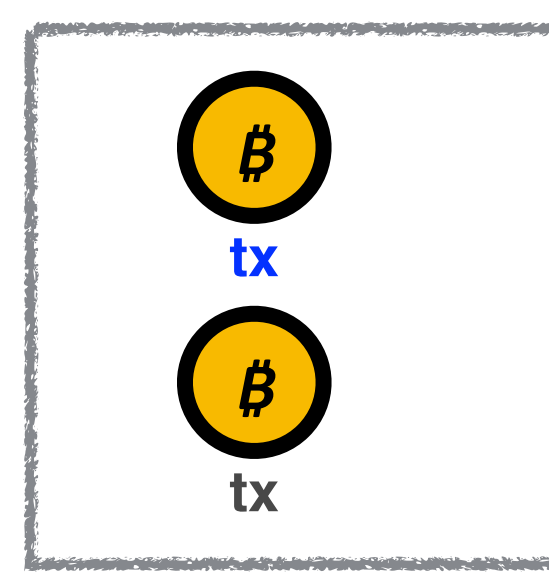
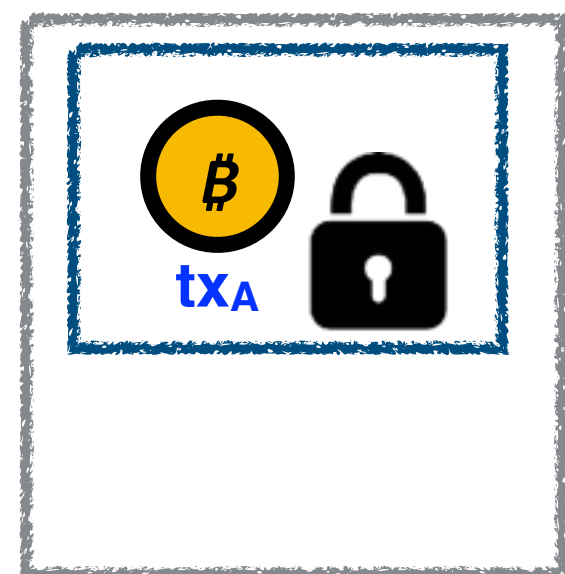
$\mathcal{F}_{Diffuse}^K$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



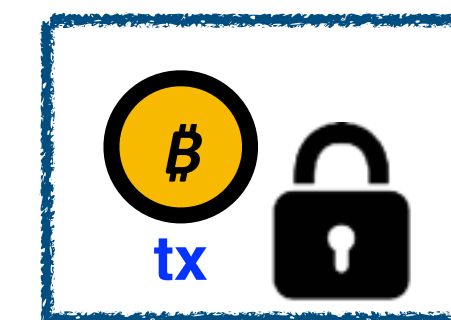
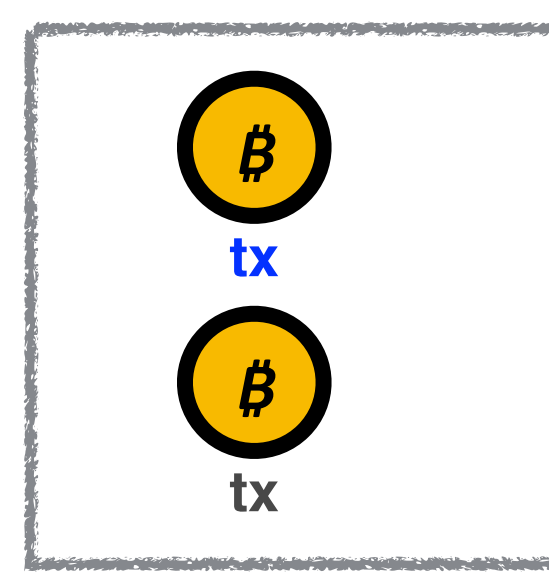
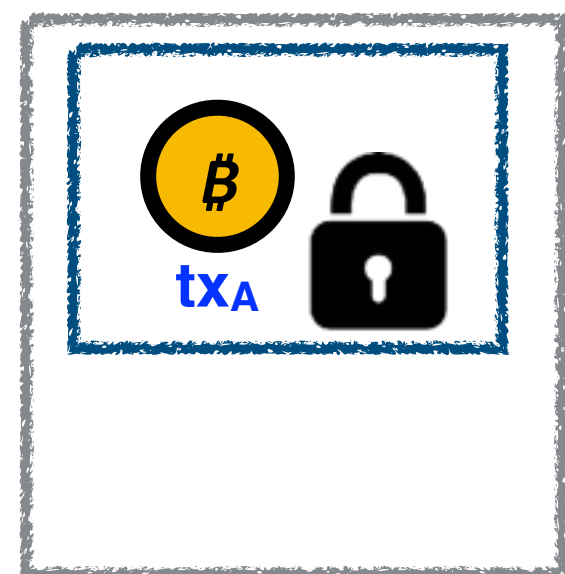
$\mathcal{F}_{Diffuse}^K$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



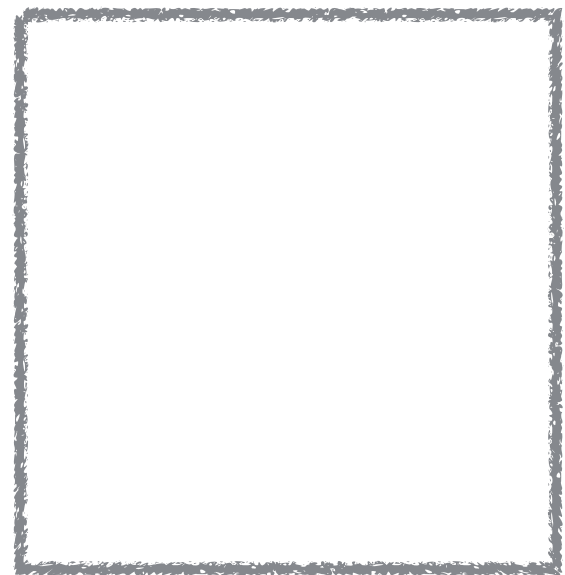
$\mathcal{F}_{Diffuse}^K$



How to realize $\overset{\text{Fair+}}{\mathcal{F}}_{\text{Ledger}}$



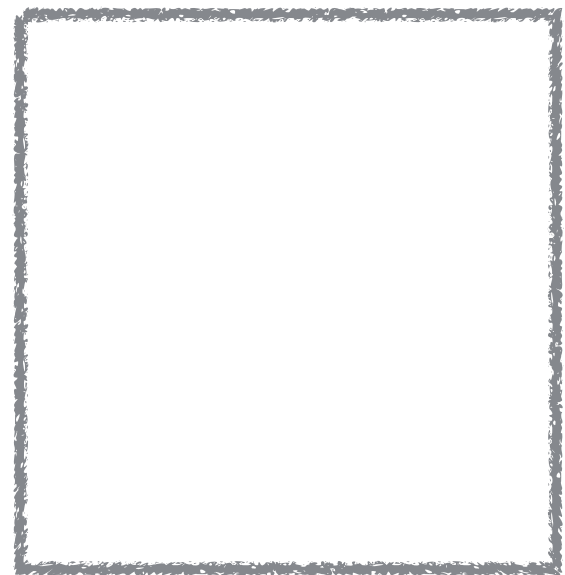
$\overset{\text{K-}}{\mathcal{F}}_{\text{Diffuse}}$



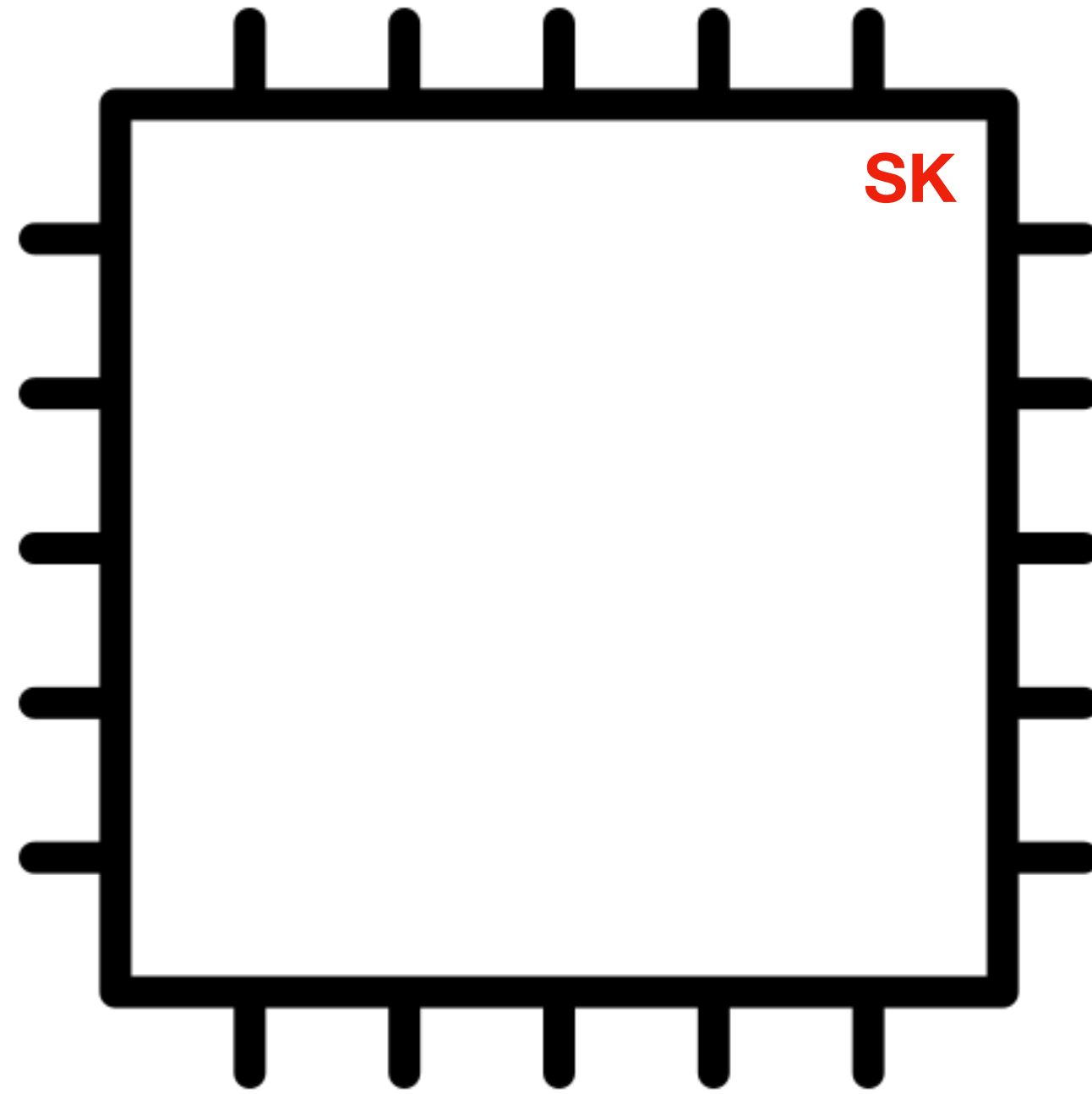
How to realize $\overset{\text{Fair+}}{\mathcal{F}}_{\text{Ledger}}$



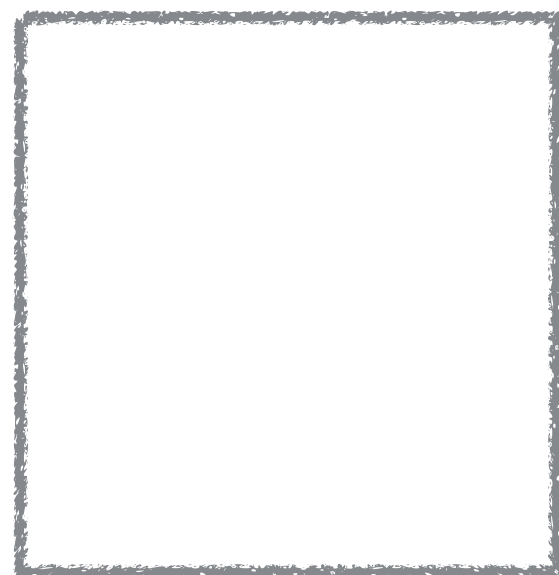
PK $\overset{\text{K-}}{\mathcal{F}}_{\text{Diffuse}}$



How to realize $\mathcal{F}_{Ledge}^{Fair+}$



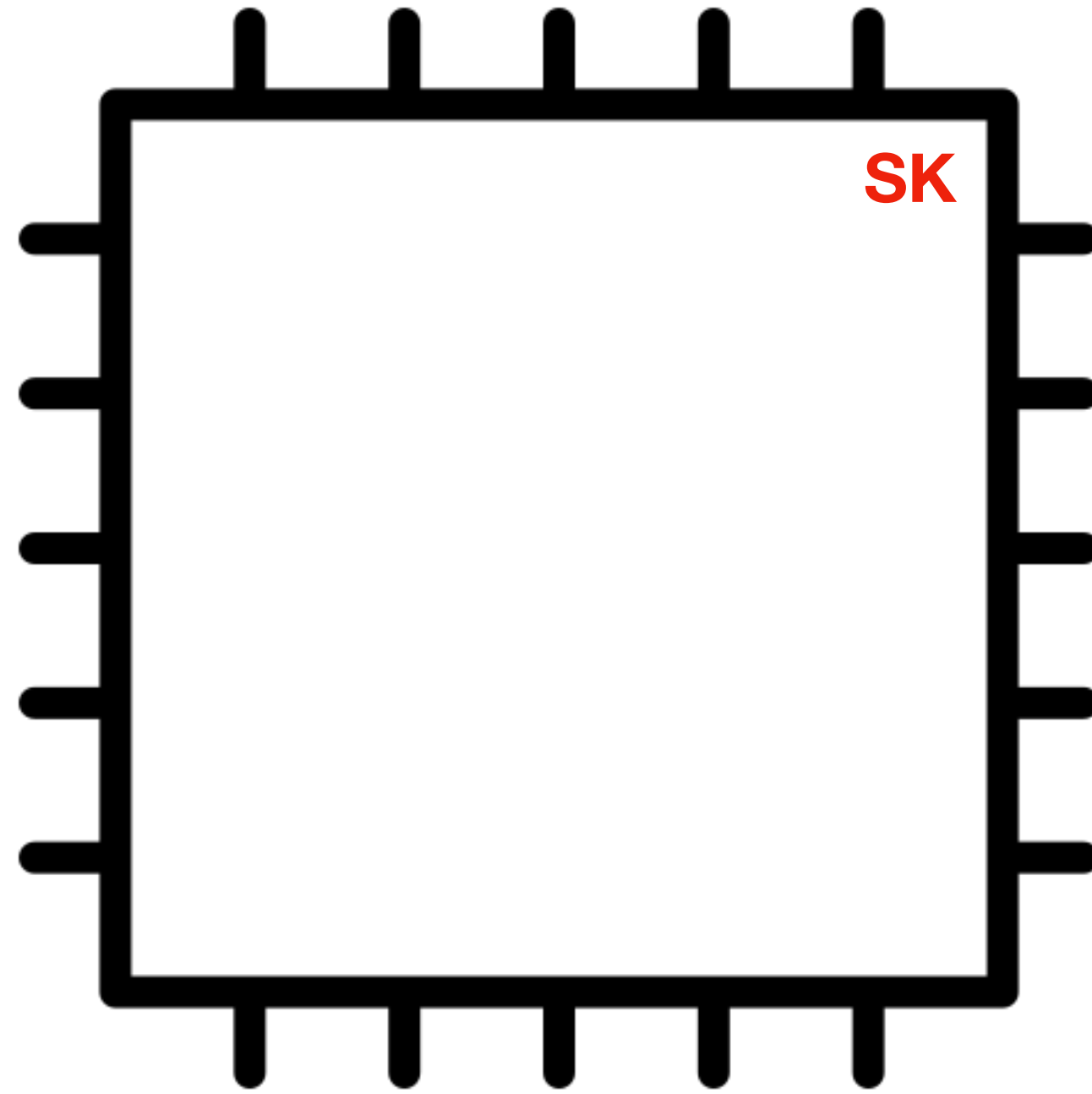
PK $\mathcal{F}_{Diffuse}^K$



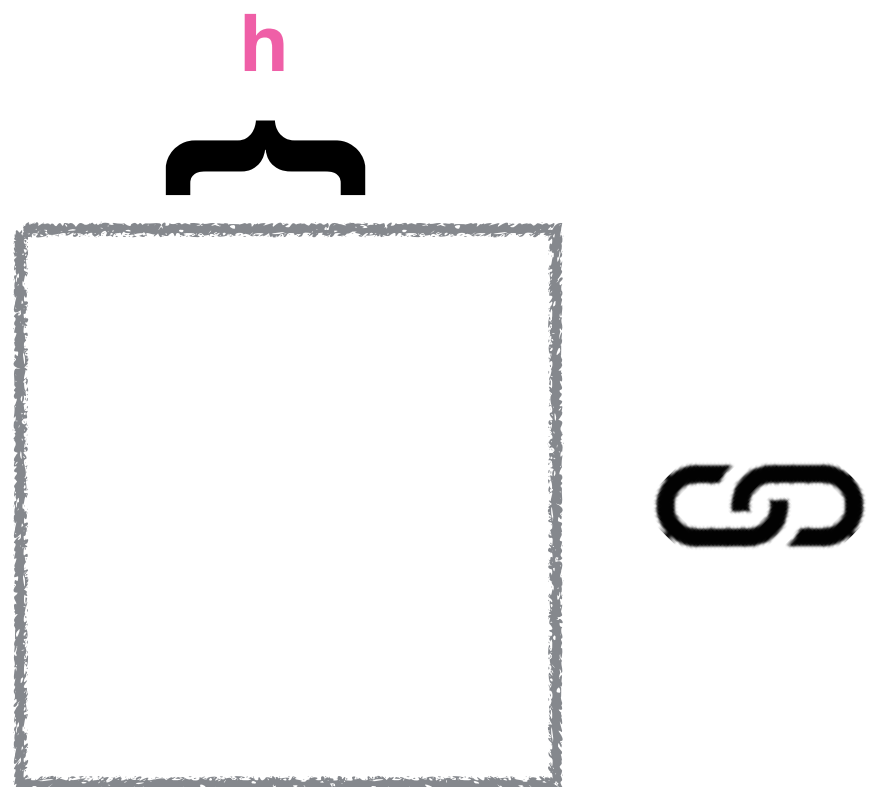
S



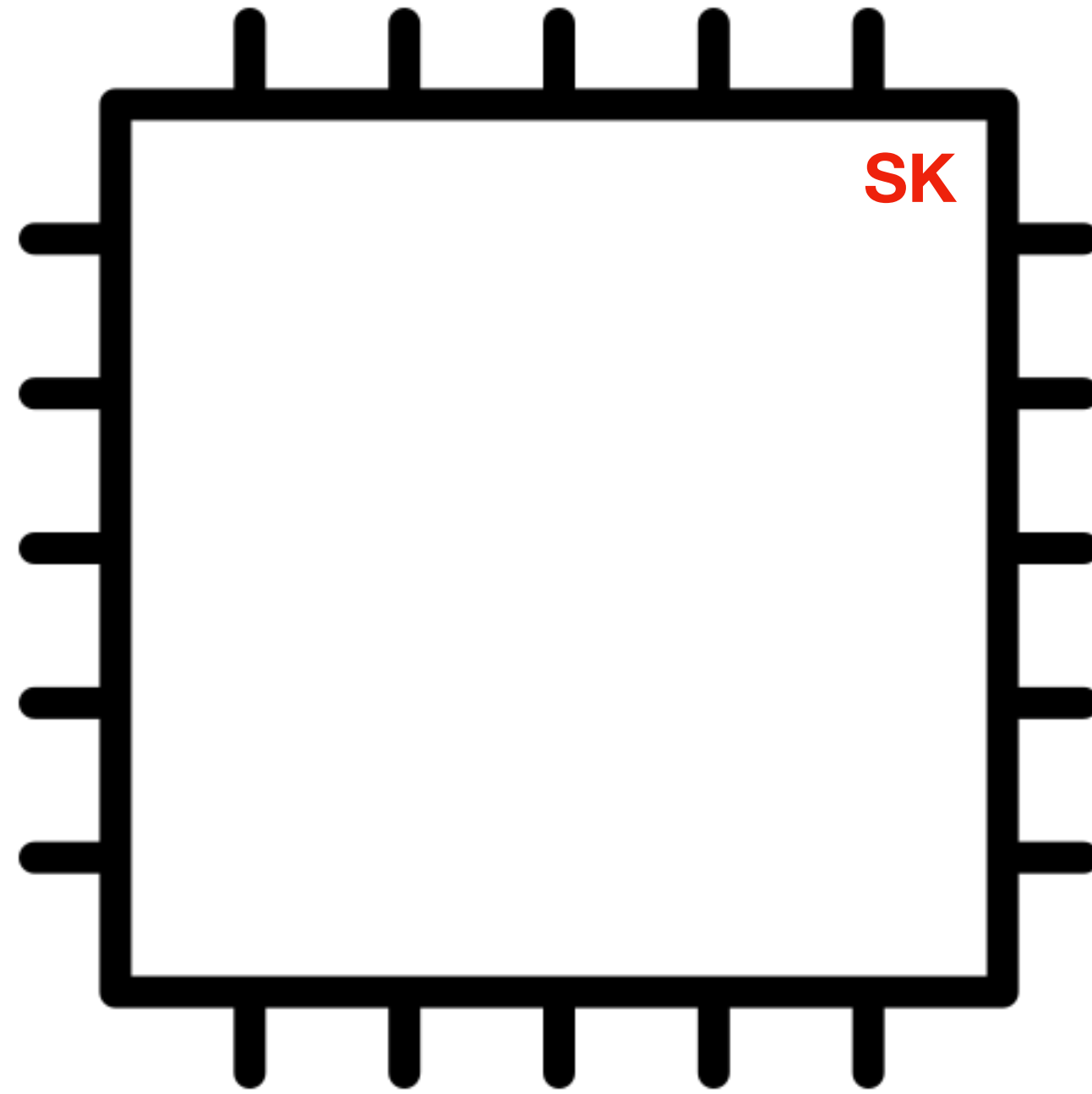
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



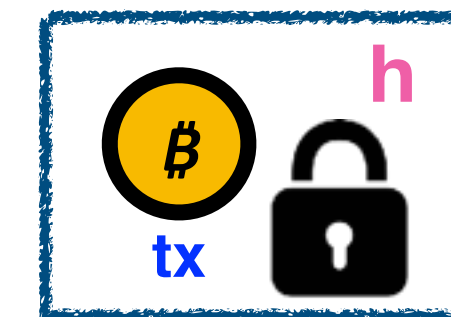
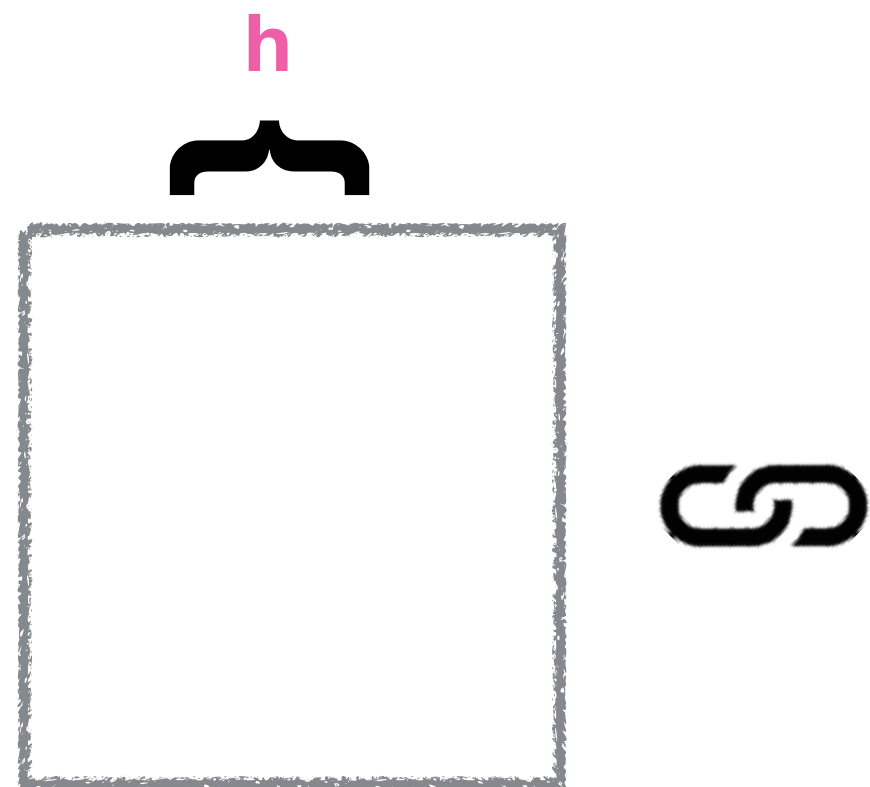
PK $\mathcal{F}_{Diffuse}^K$



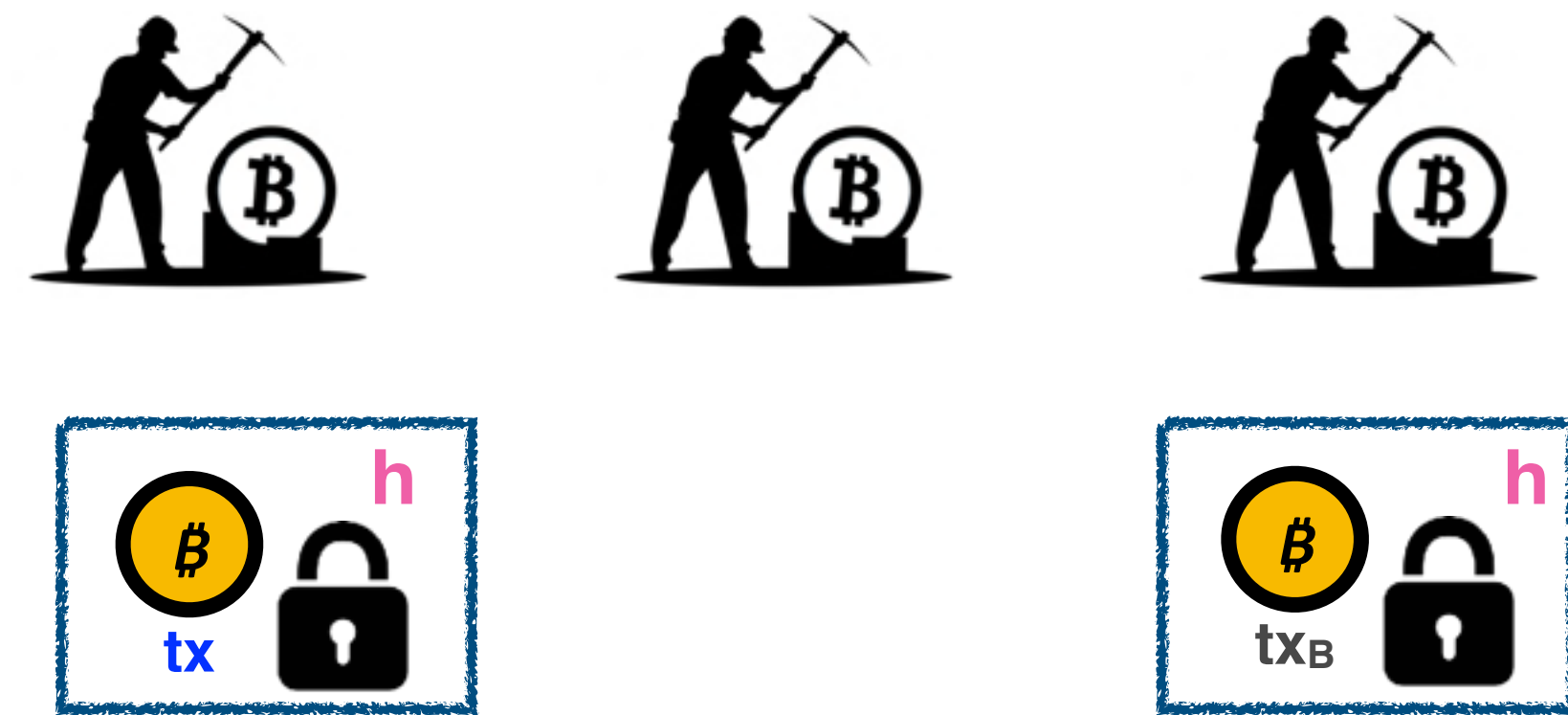
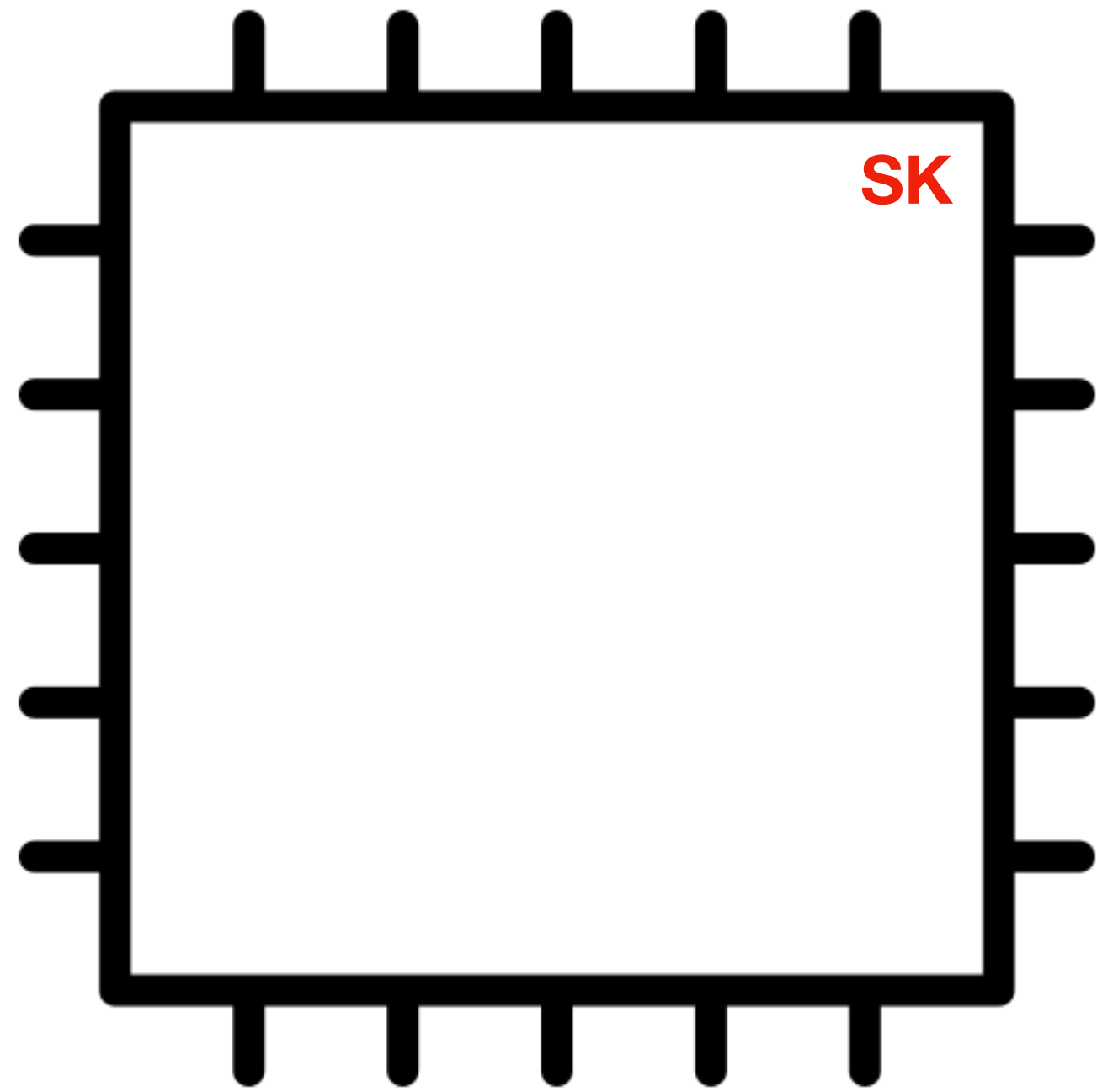
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



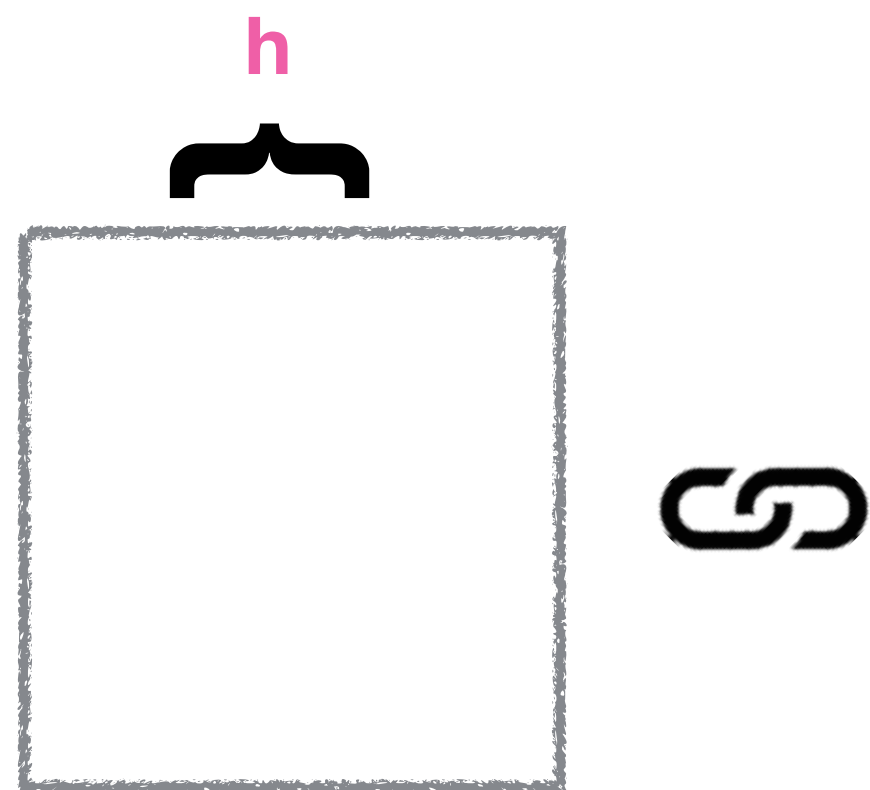
PK $\mathcal{F}_{Diffuse}^{K-}$



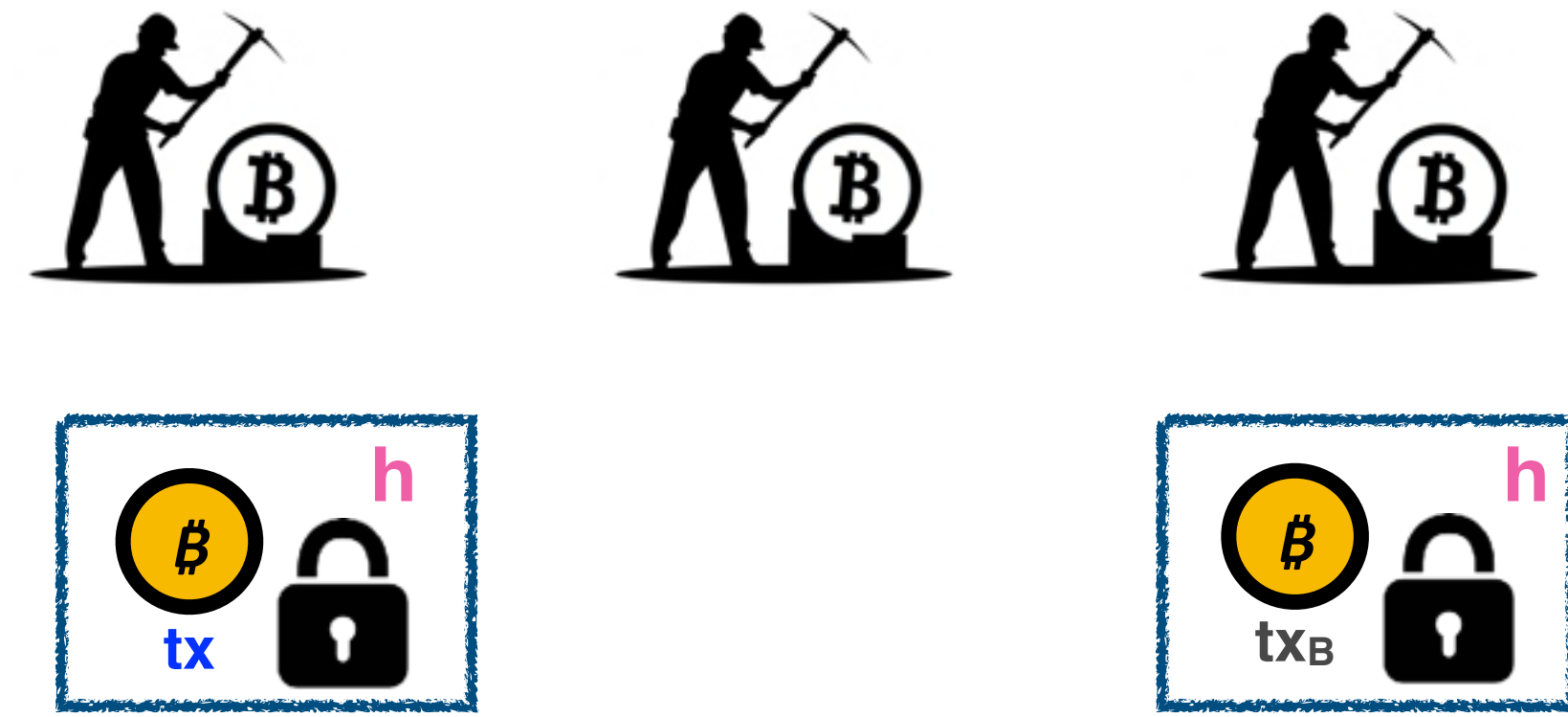
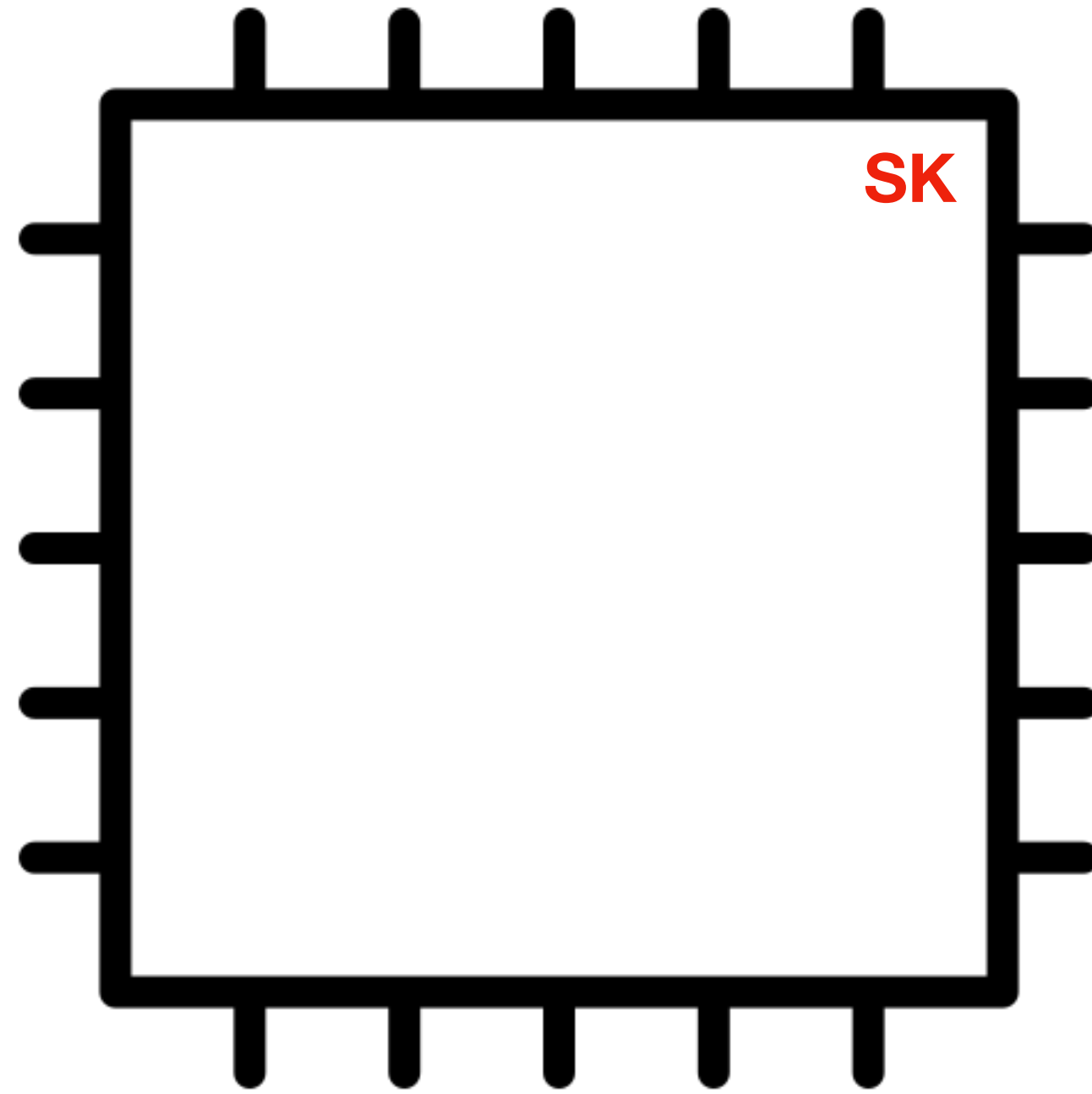
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



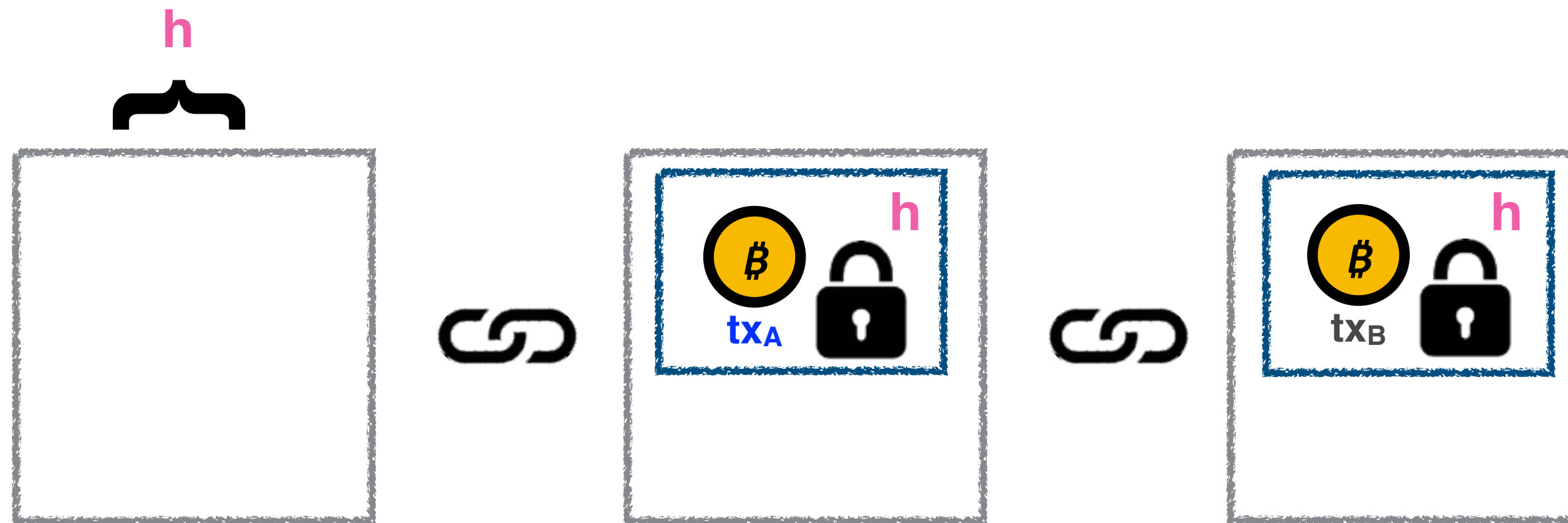
PK $\mathcal{F}_{Diffuse}^{K-}$



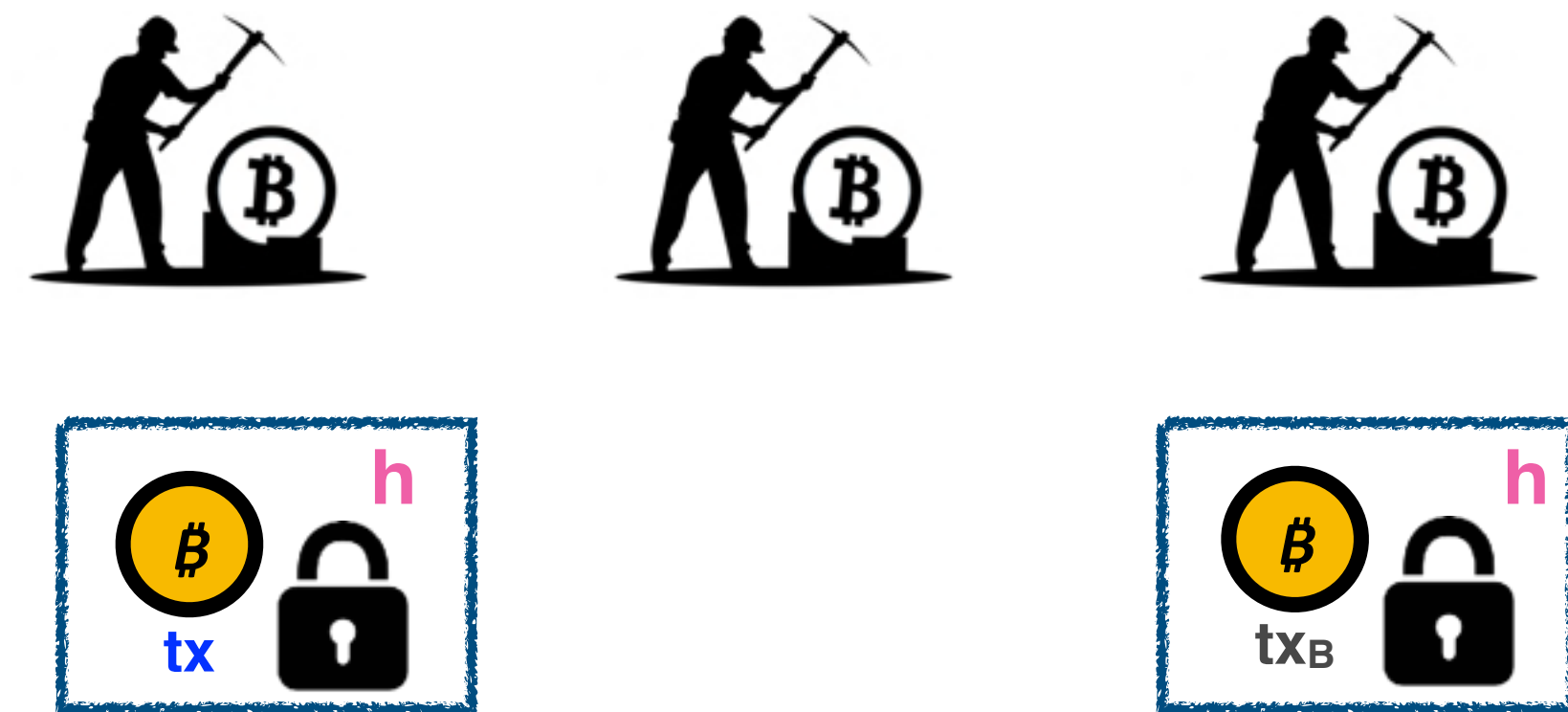
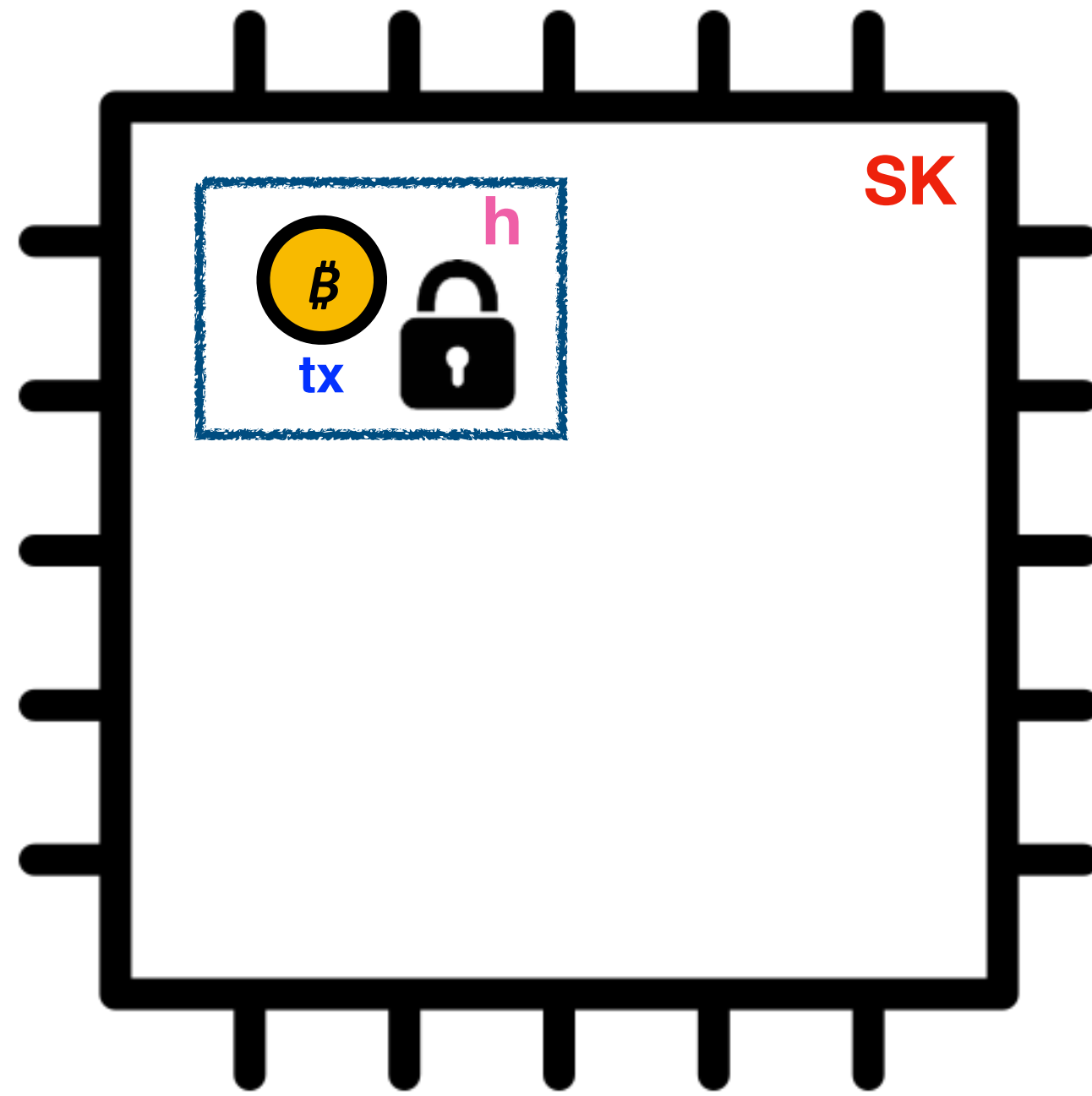
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



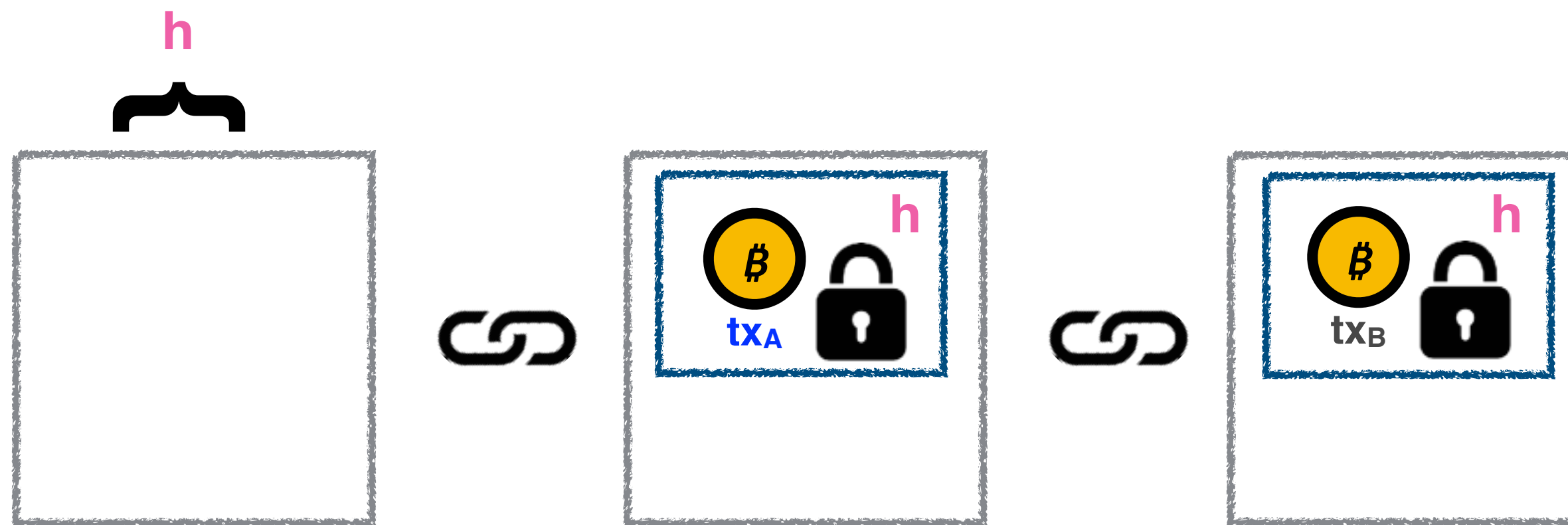
PK $\mathcal{F}_{Diffuse}^{K-}$



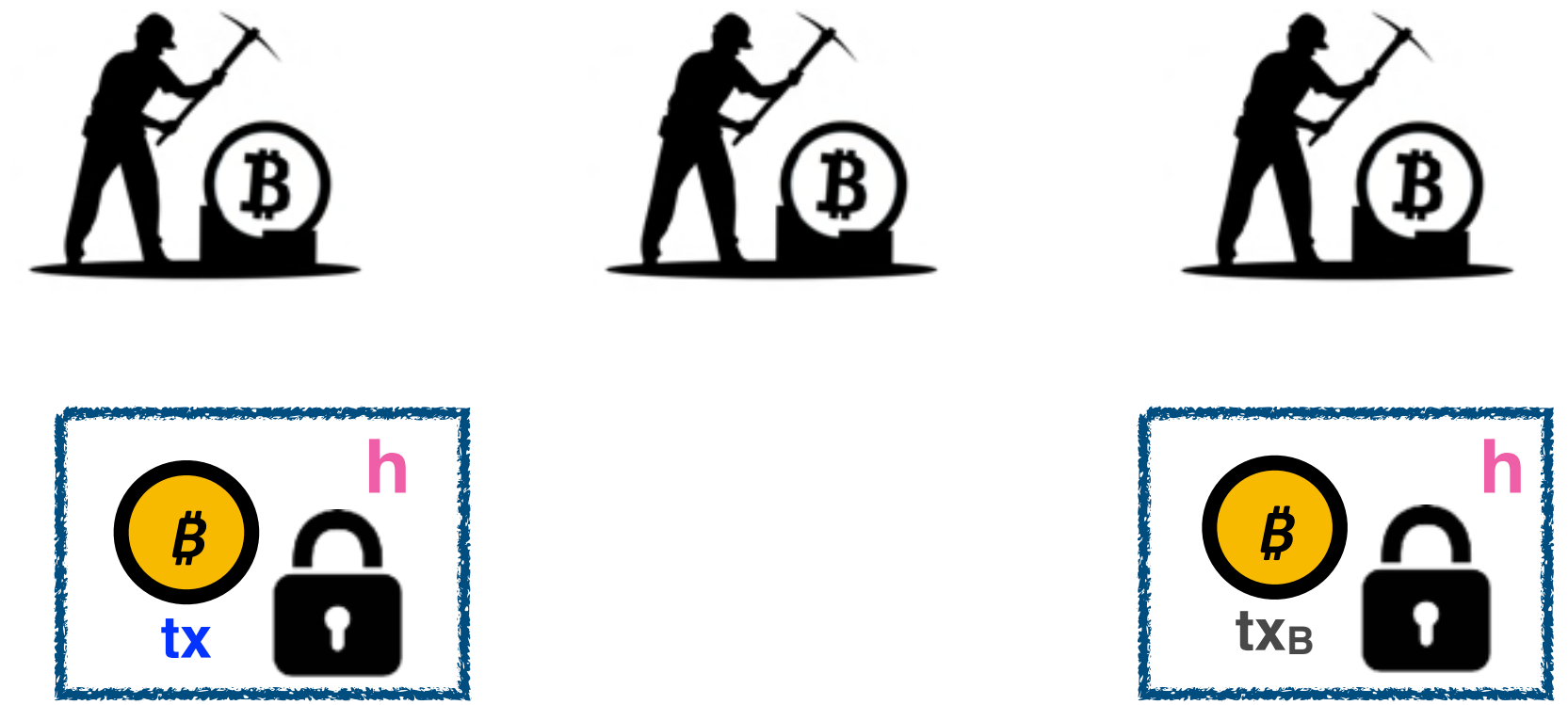
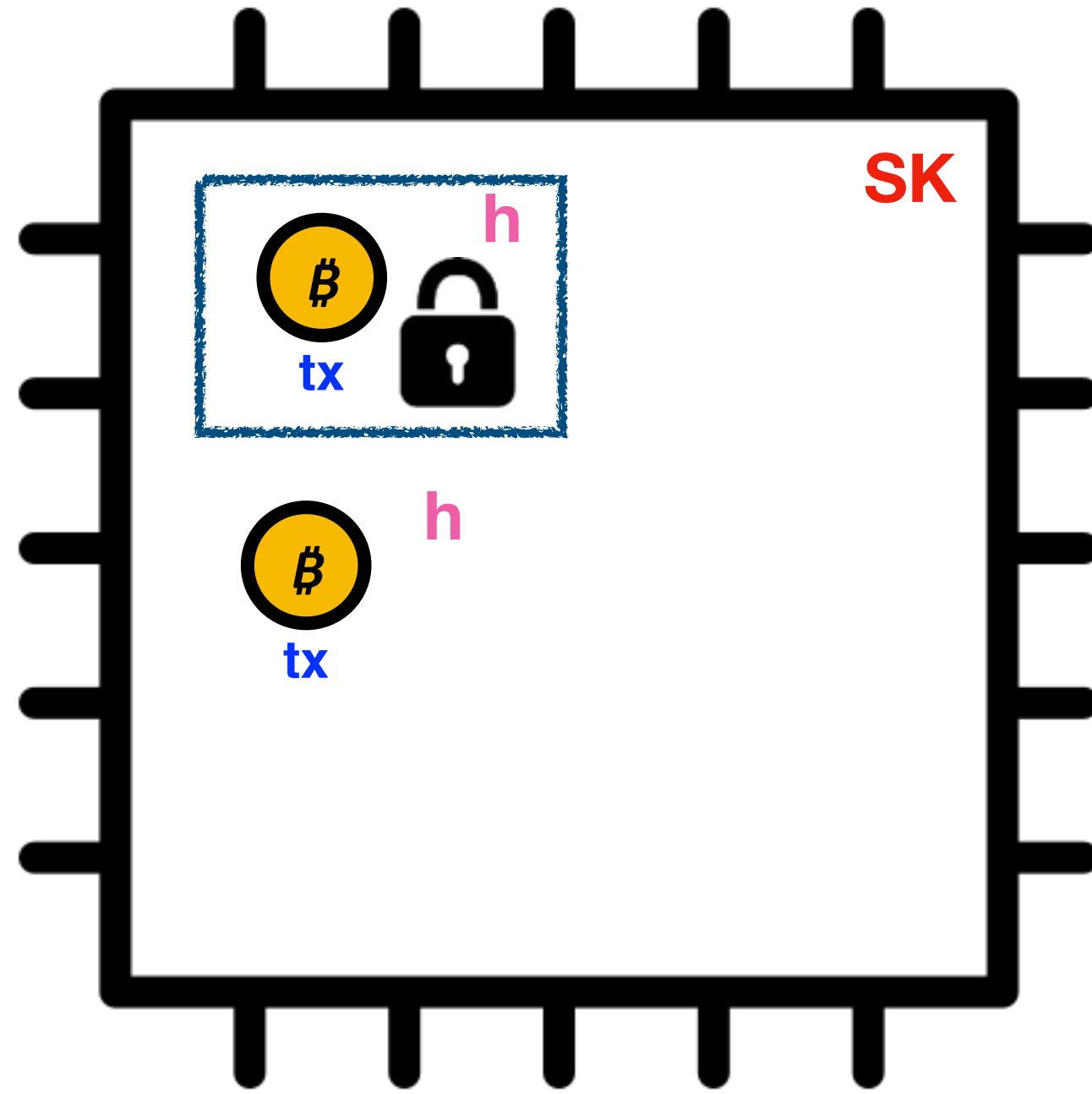
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



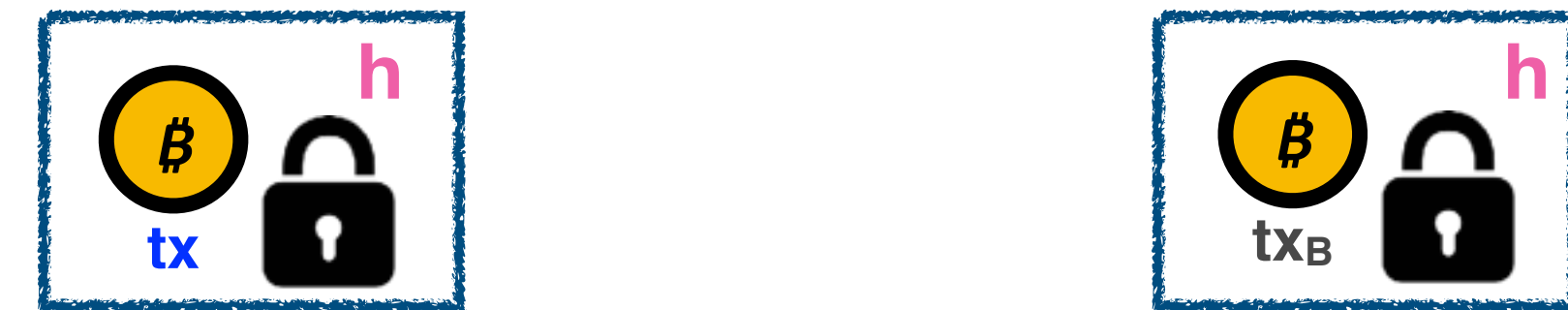
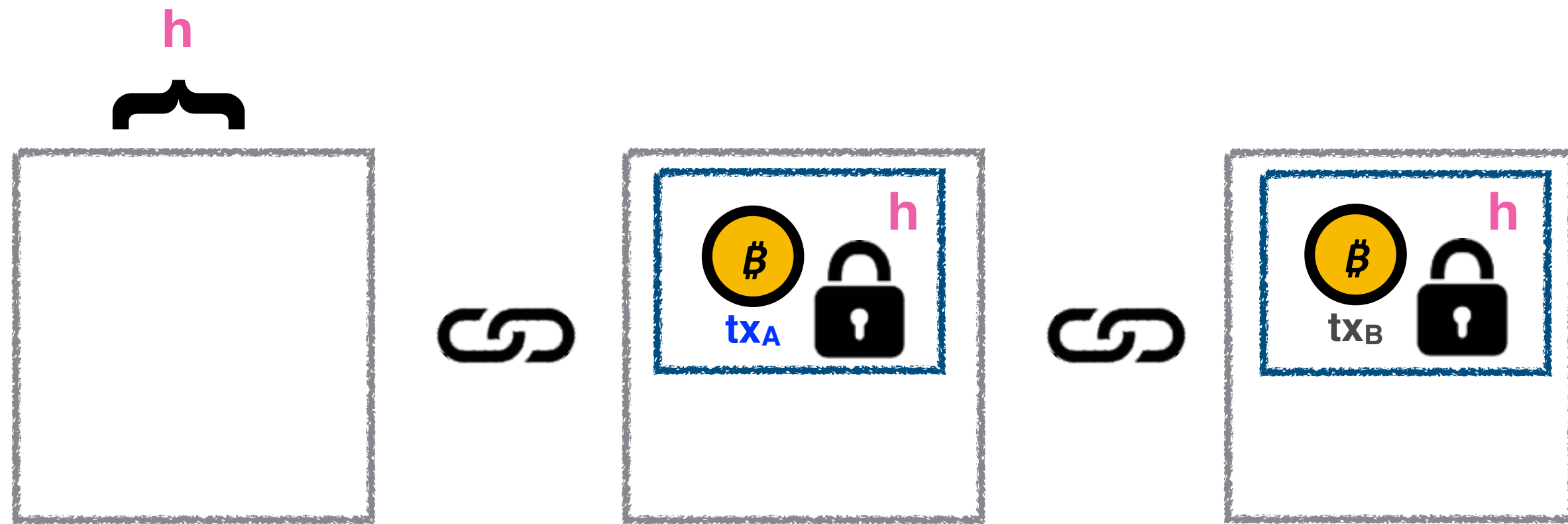
PK $\mathcal{F}_{Diffuse}^{K-}$



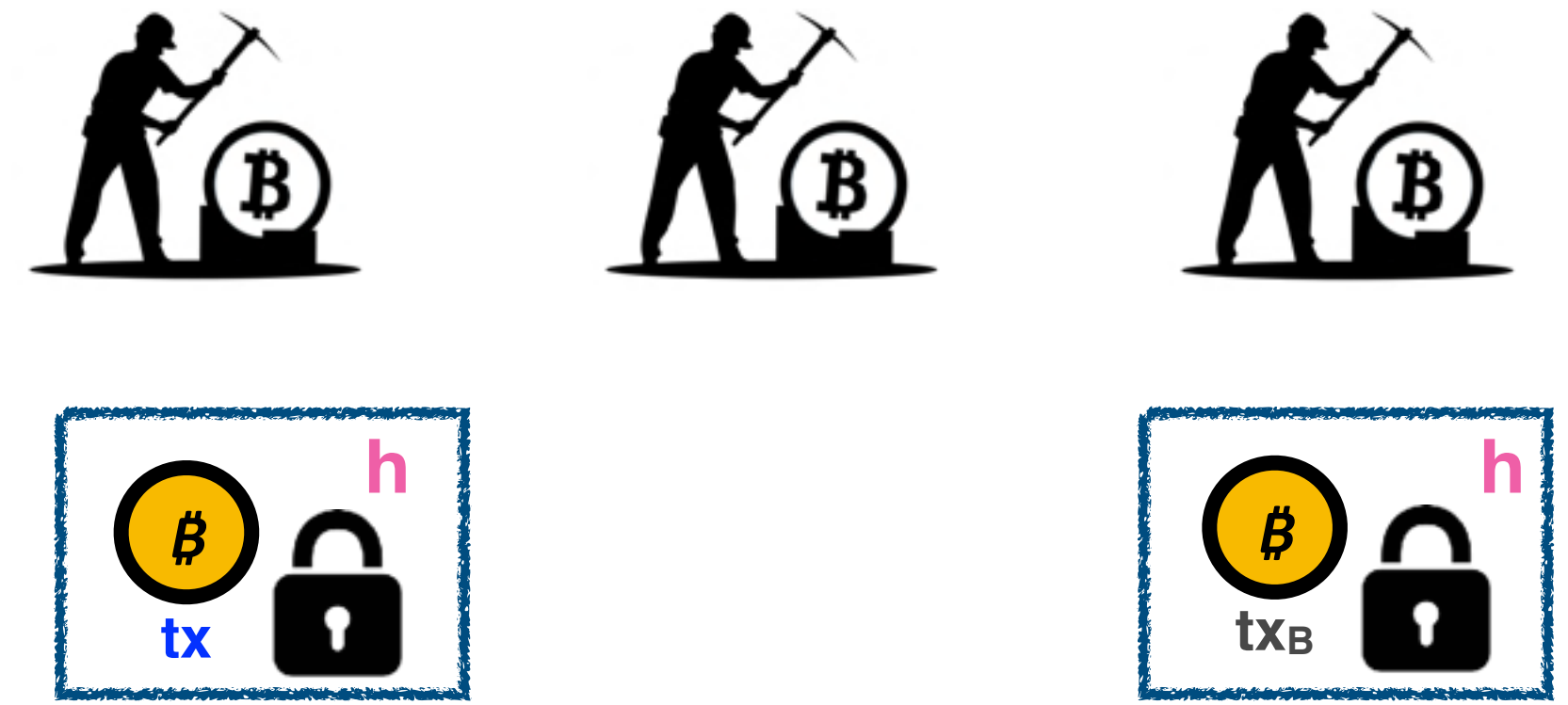
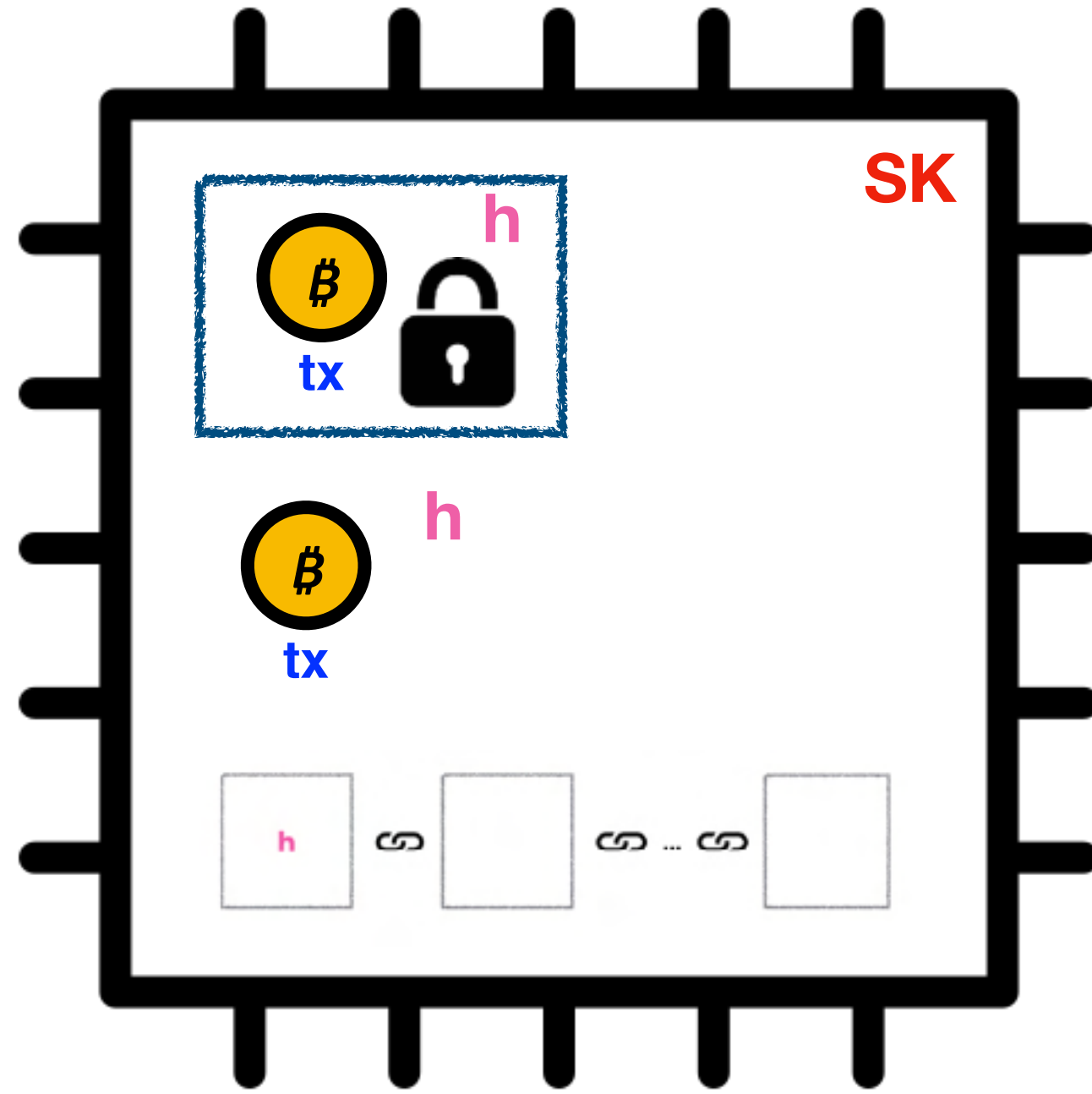
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



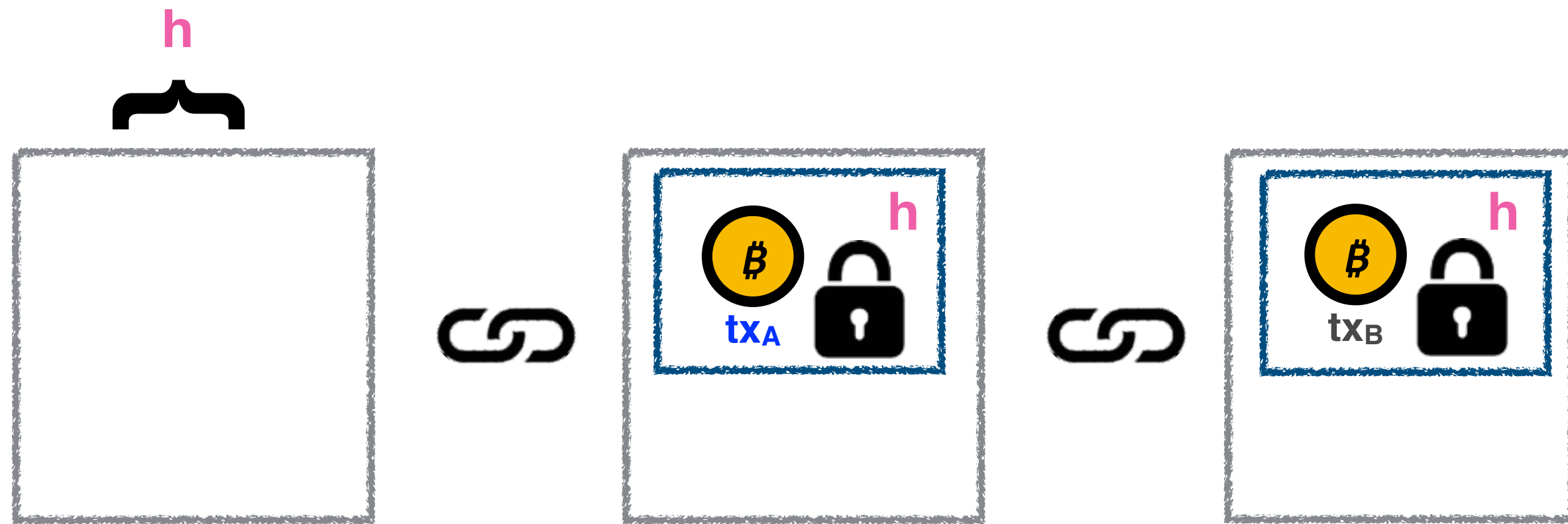
PK $\mathcal{F}_{Diffuse}^{K-}$



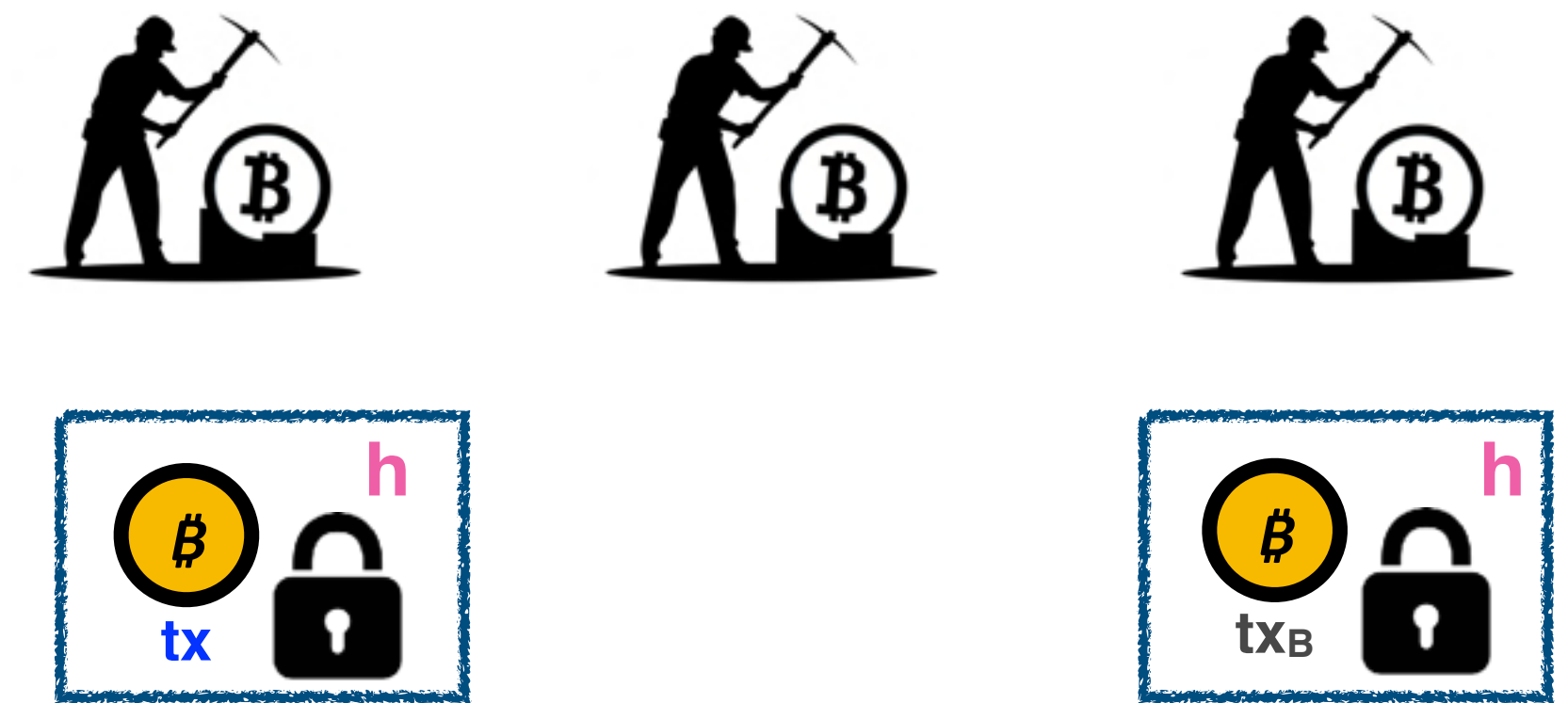
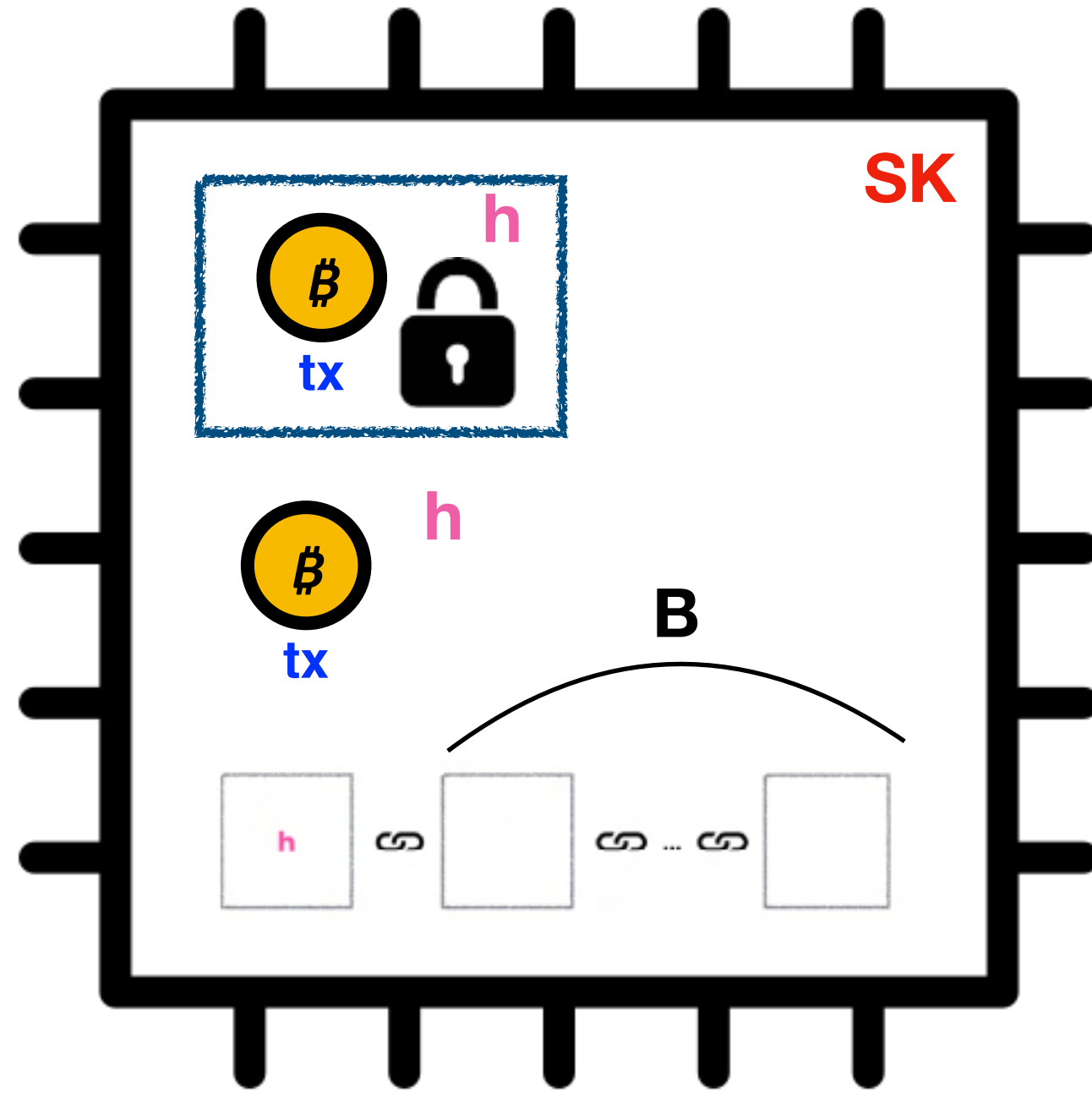
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



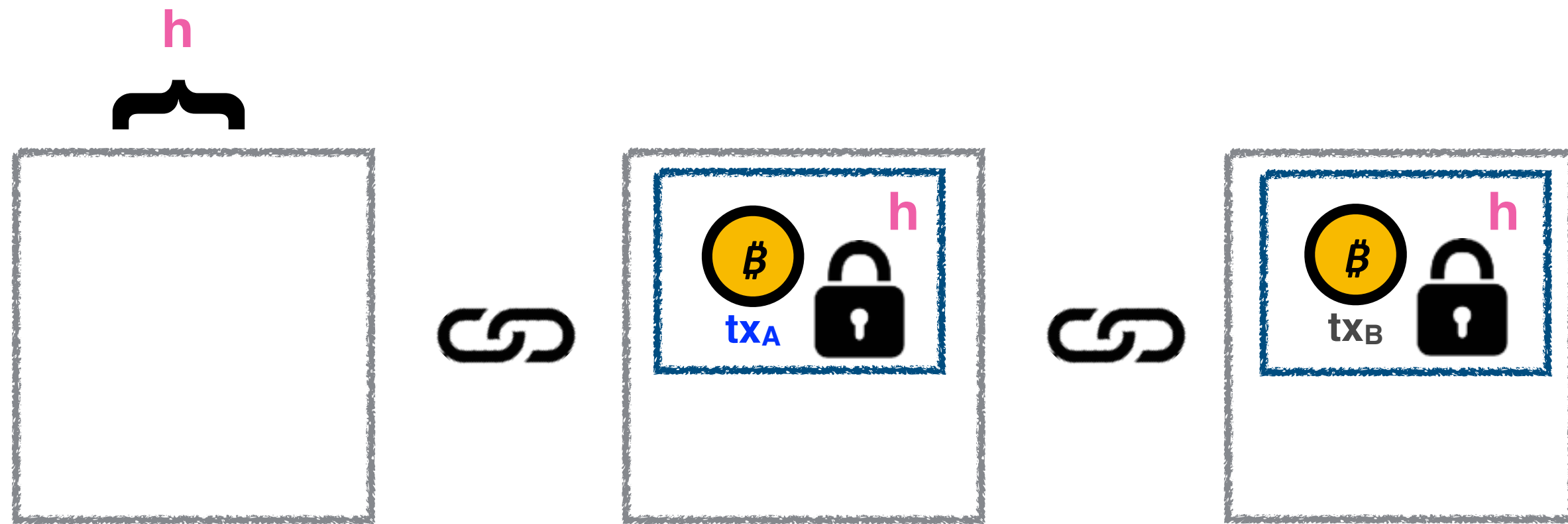
PK $\mathcal{F}_{Diffuse}^{K-}$



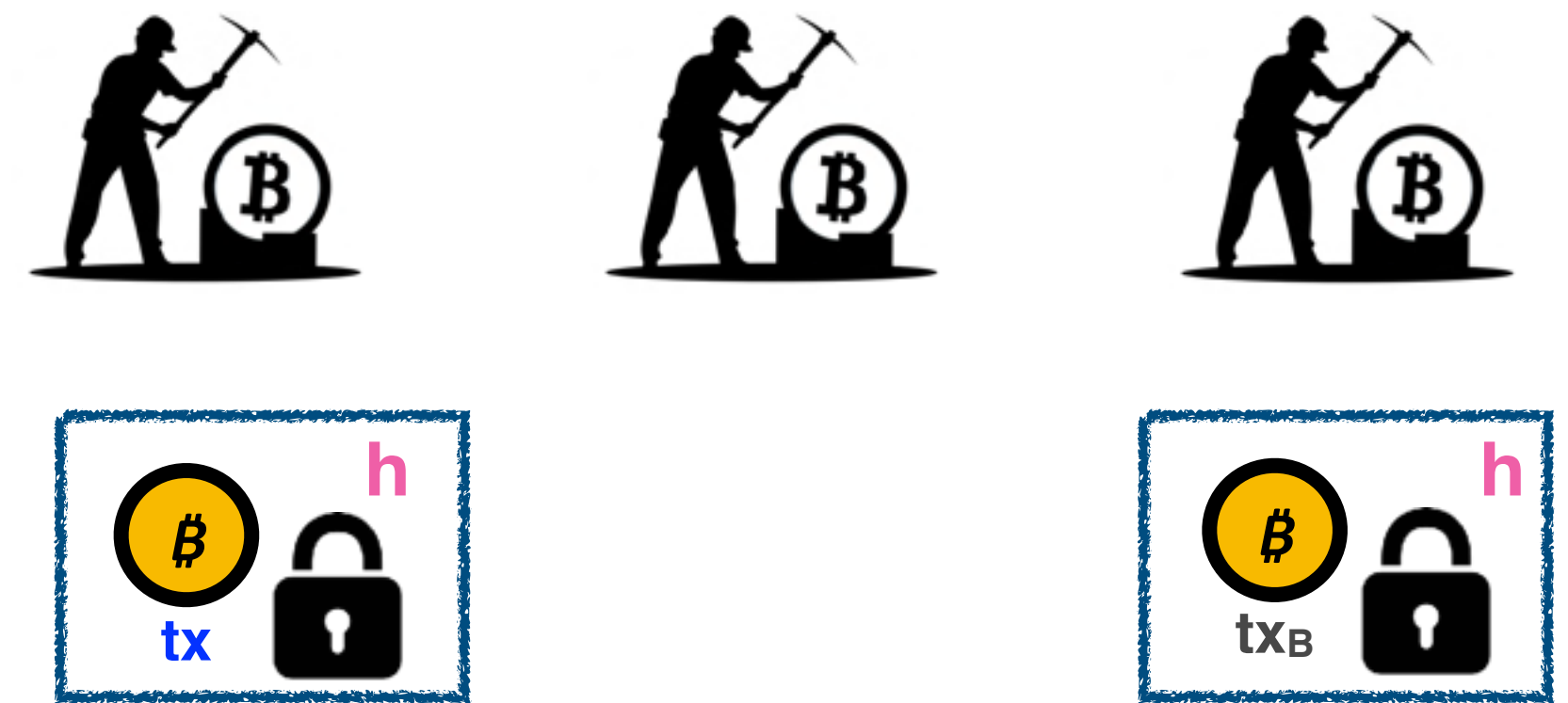
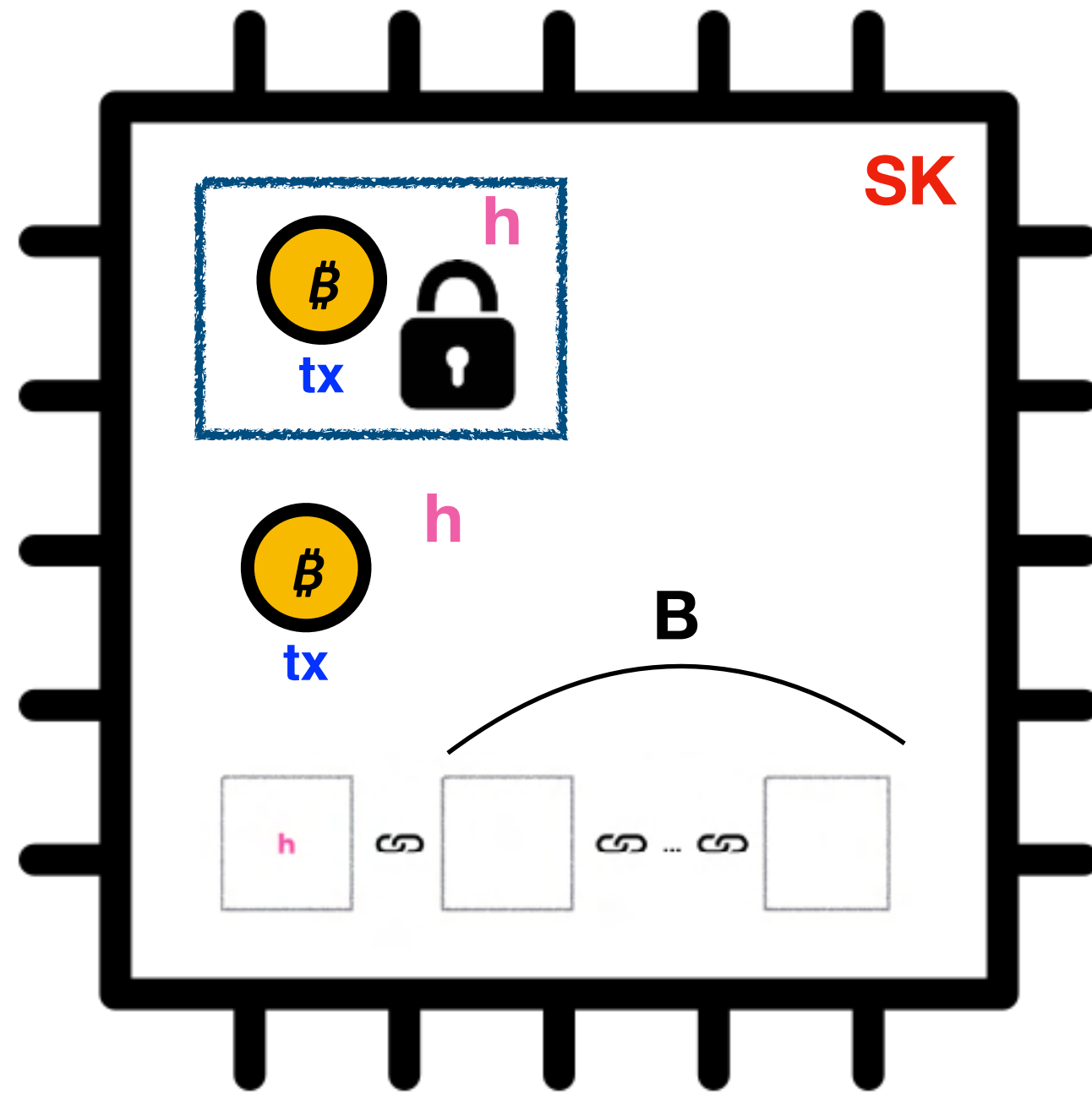
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



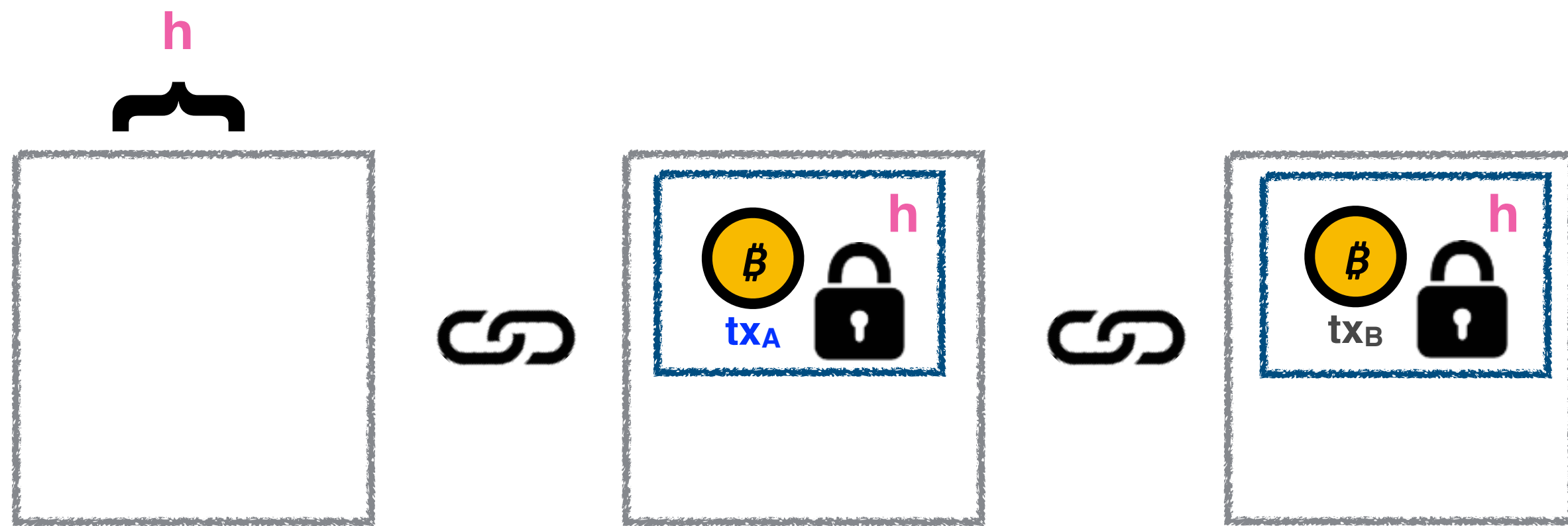
PK $\mathcal{F}_{Diffuse}^{K-}$



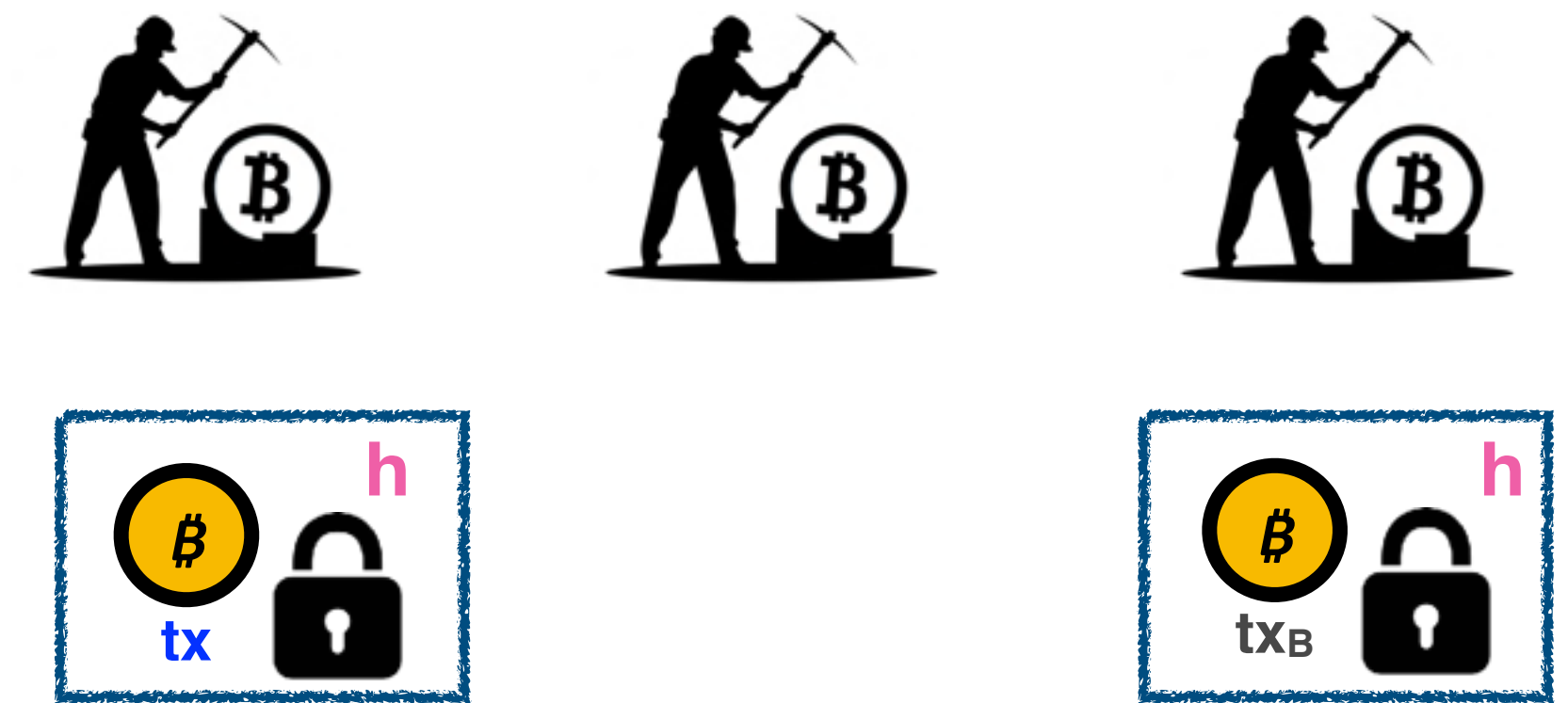
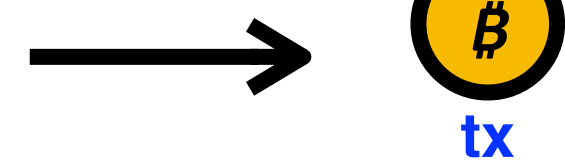
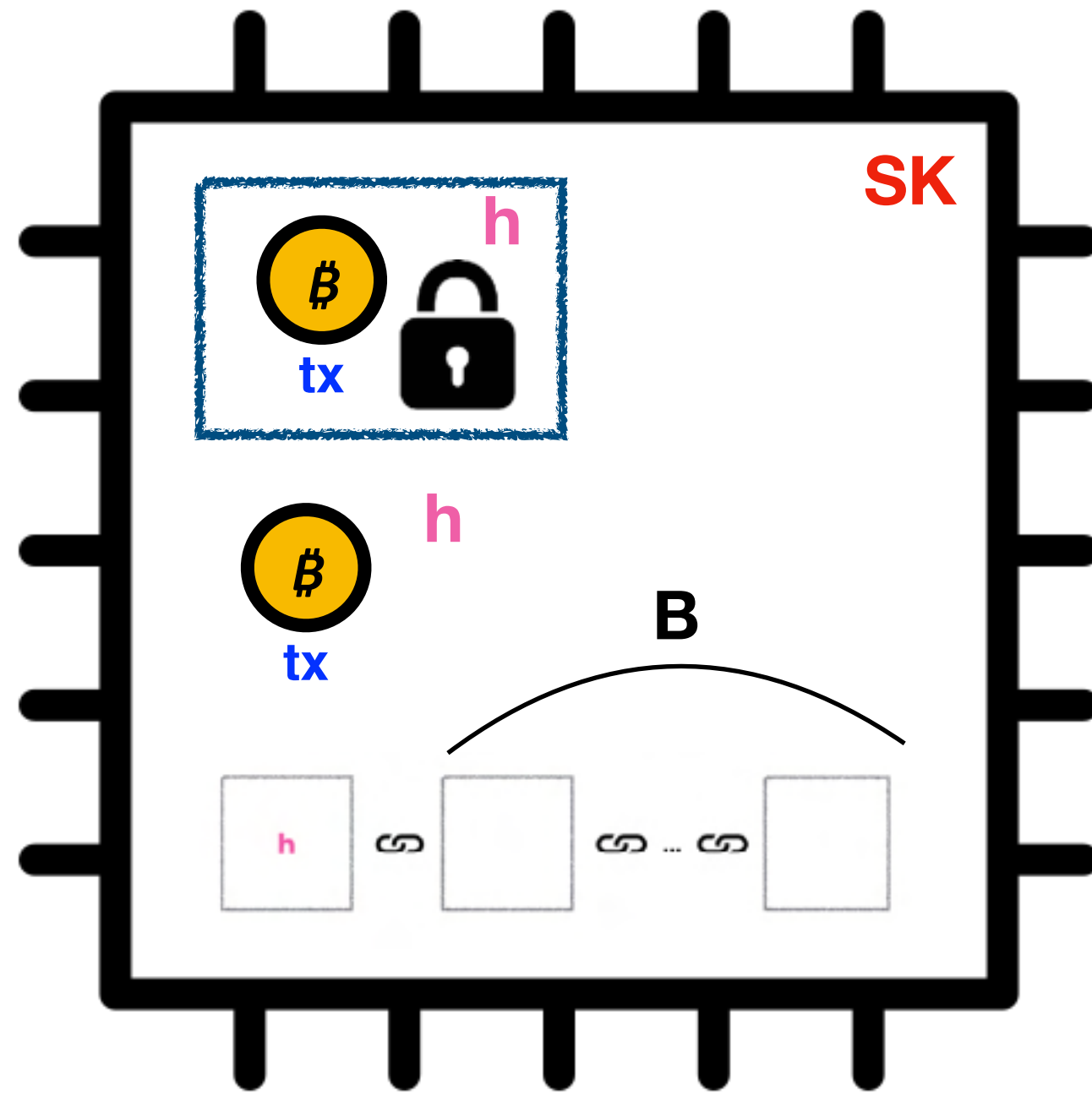
How to realize $\mathcal{F}_{Ledger}^{Fair+}$



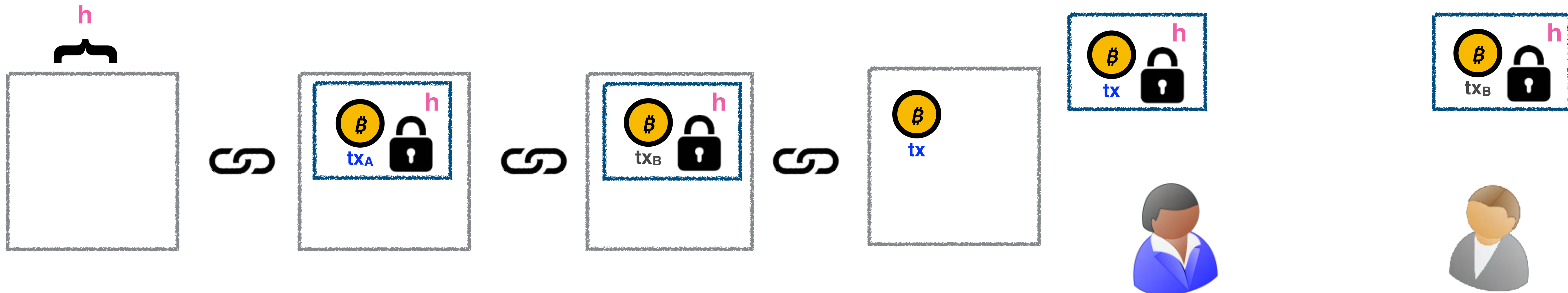
PK $\mathcal{F}_{Diffuse}^{K-}$



How to realize $\mathcal{F}_{Ledger}^{Fair+}$



PK $\mathcal{F}_{Diffuse}^{K-}$



Conclusions and Open Questions

Conclusions and Open Questions

- UC formalization of ledgers with a fair order

Conclusions and Open Questions

- UC formalization of ledgers with a fair order
- Construction based on global setups (global trusted execution enclaves)

Conclusions and Open Questions

- UC formalization of ledgers with a fair order
- Construction based on global setups (global trusted execution enclaves)
- Impossibility for sender order fairness

Conclusions and Open Questions

- UC formalization of ledgers with a fair order
- Construction based on global setups (global trusted execution enclaves)
- Impossibility for sender order fairness
- Extention to proof of stake blockchains

Conclusions and Open Questions

- UC formalization of ledgers with a fair order
- Construction based on global setups (global trusted execution enclaves)
- Impossibility for sender order fairness
- Extension to proof of stake blockchains
- Remove TEE while minimizing the communication complexity

Conclusions and Open Questions

- UC formalization of ledgers with a fair order
- Construction based on global setups (global trusted execution enclaves)
- Impossibility for sender order fairness
- Extension to proof of stake blockchains
- Remove TEE while minimizing the communication complexity
- Consider a different network functionality

Thanks