Affordable Security
Or
Big Guy vs. Small Guy

Does the depth of your pockets impact your protocols?

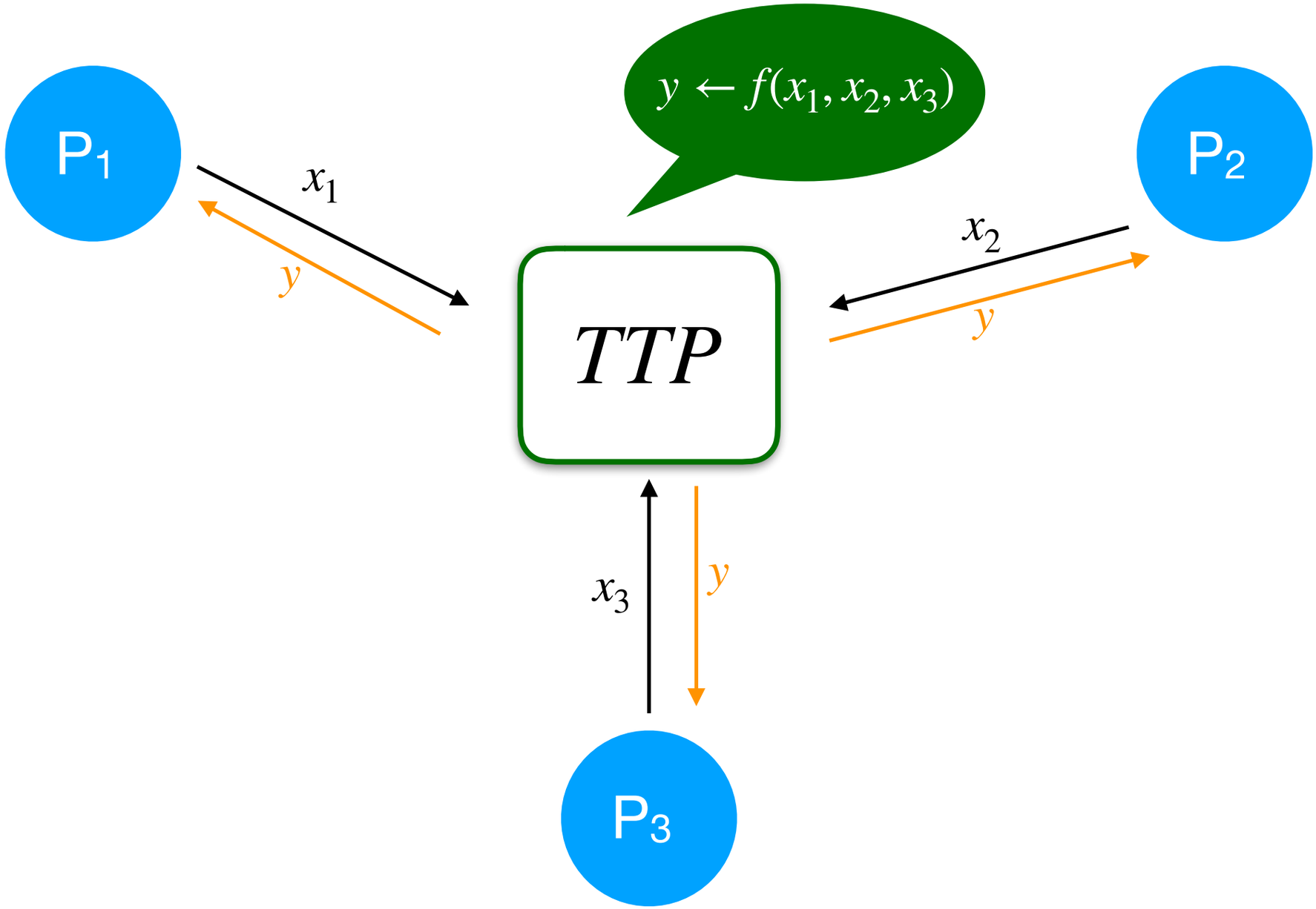
Daniele Friolo

Università di Roma La Sapienza

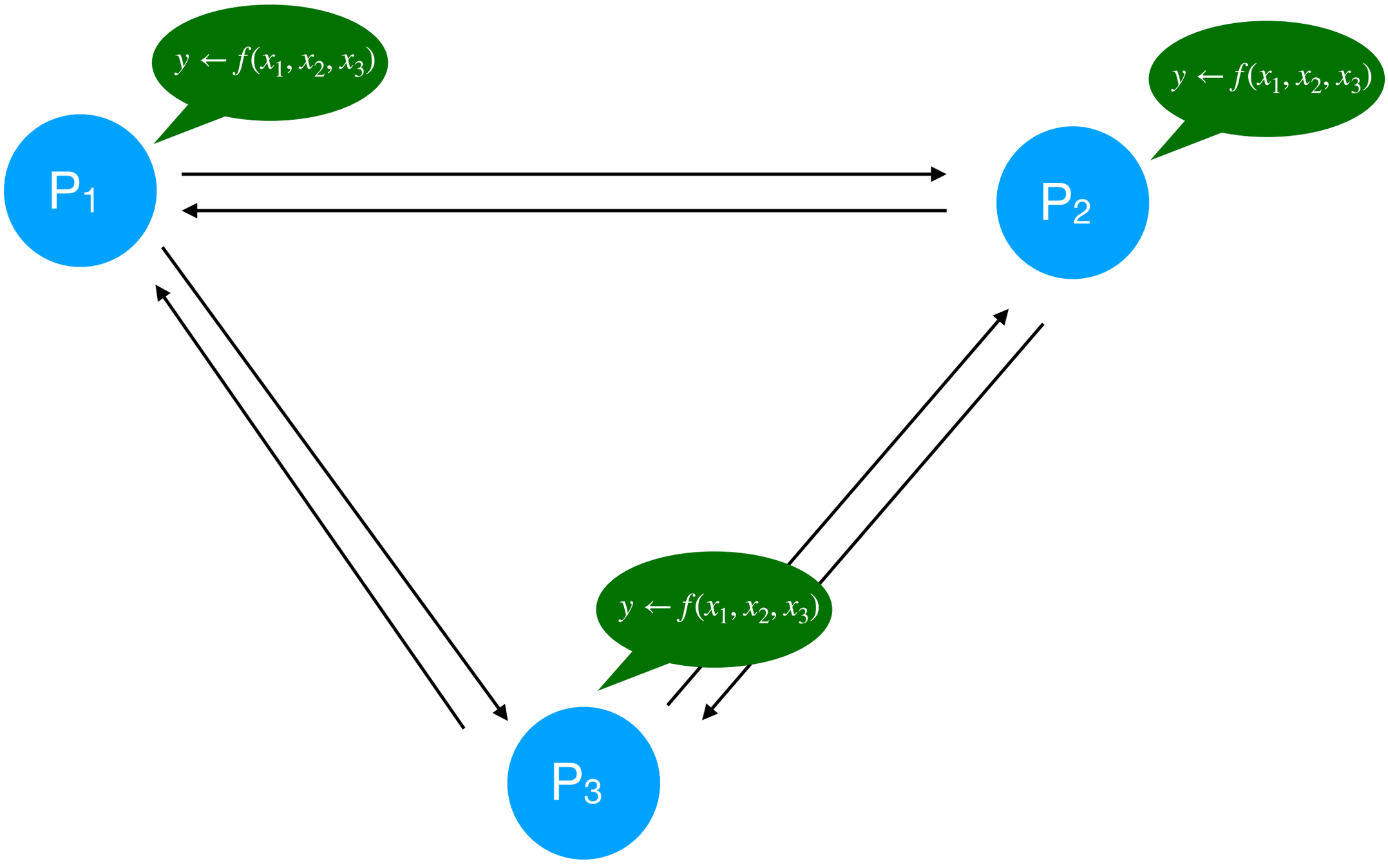
joint work with Daniele Venturi[1], Chan Nam Ngo[2], Fabio Massacci[2]

[1]Università di Roma La Sapienza [2]Università di Trento

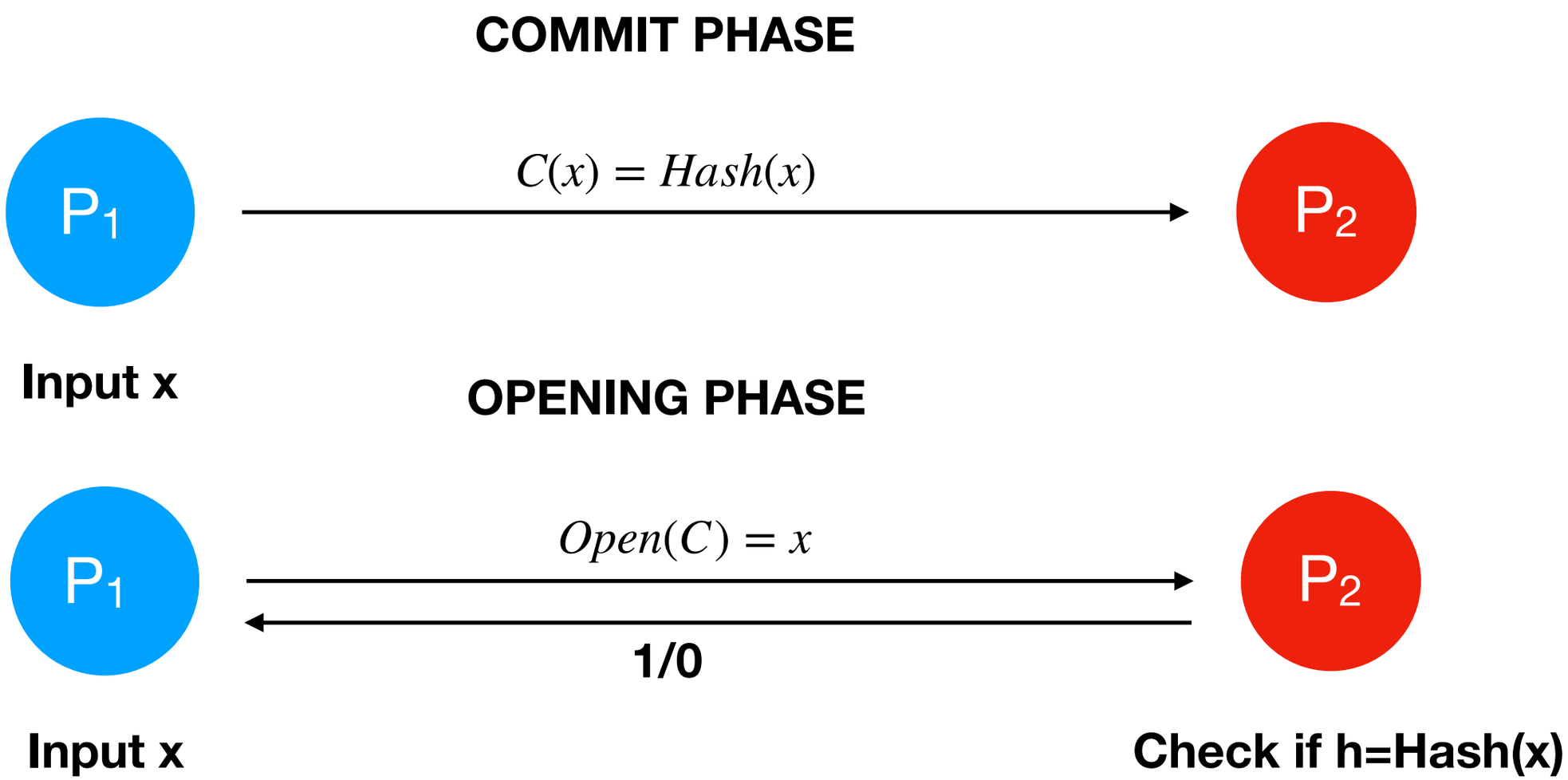
Multi-party Computation



Multi-party Computation



Commitment Schemes



- Security properties: **Binding** and **Hiding**

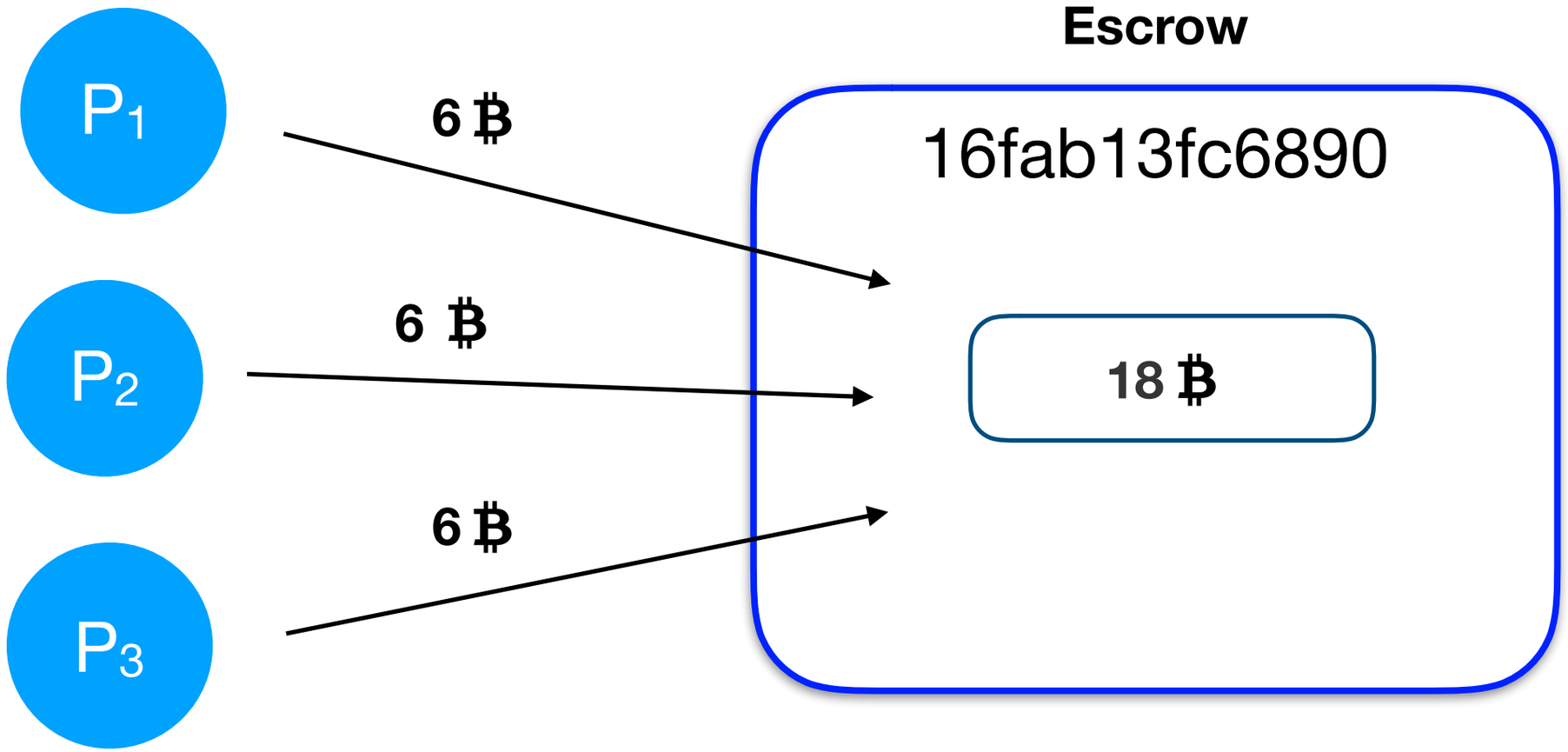
Penalties as solution to unfairness

- Security guarantees of MPC
  - Privacy, correctness, independence of inputs, guaranteed output delivery,..
  - **Fairness:** corrupted parties receive the output if and only if the honest parties do as well

- Big issue in digital *auctions, digital exchanges, on-line gambling (Poker, lottery)*
- Impossible to achieve for dishonest majority
  [Cleve86]
    - Achieved for specific functionalities, relaxing security definitions, using public bulletin board..
    - **Penalties using Bitcoin**
      [ADMM14] [KB14] [KVV16] …

Penalties as the universal cure

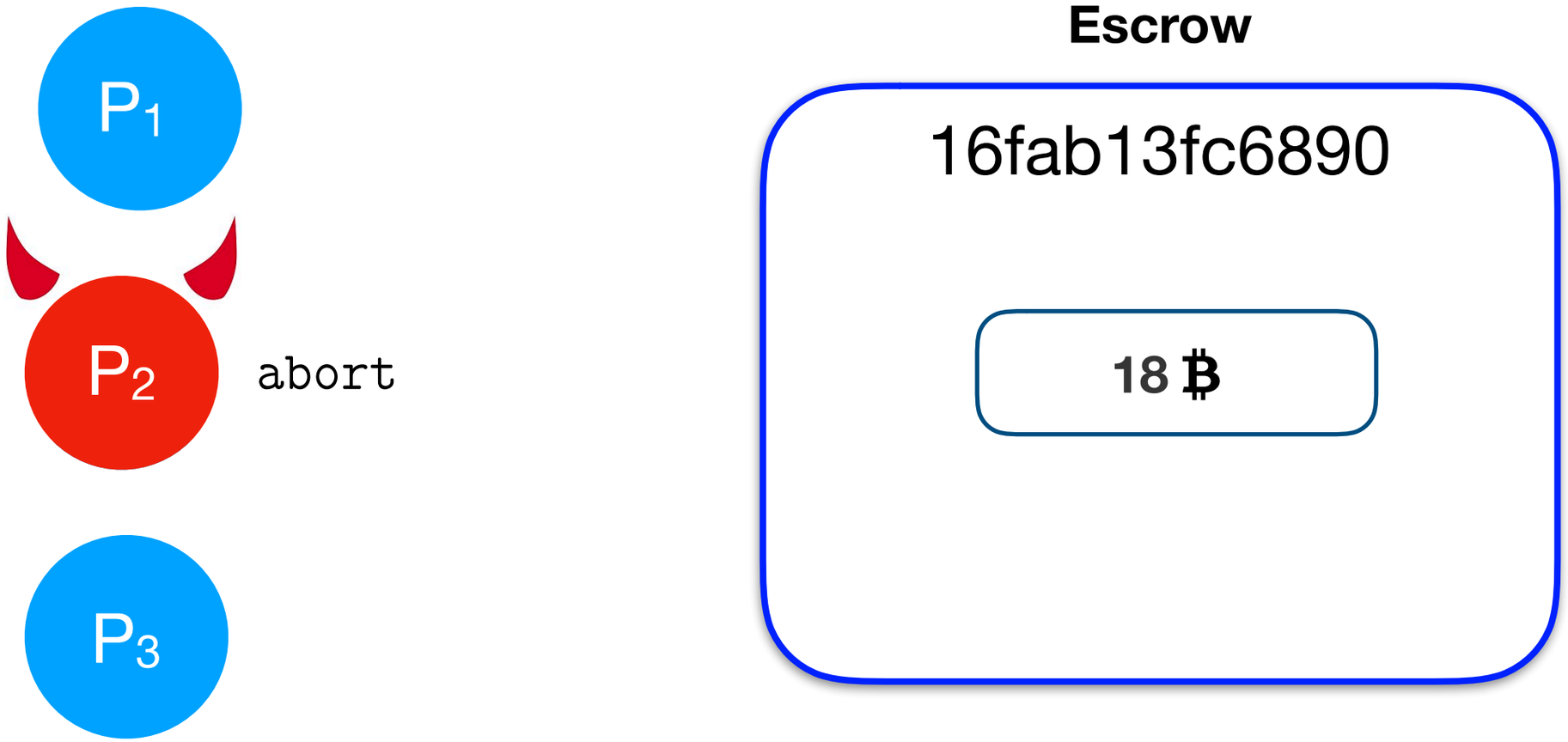
- Idea originated by Andrychowicz *et al.* [ADMM14] implemented in *Bitcoin* (only for lottery functionality)



- Extended by Bentov *et al.* to general purpose MPC with penalties

Penalties as the universal cure

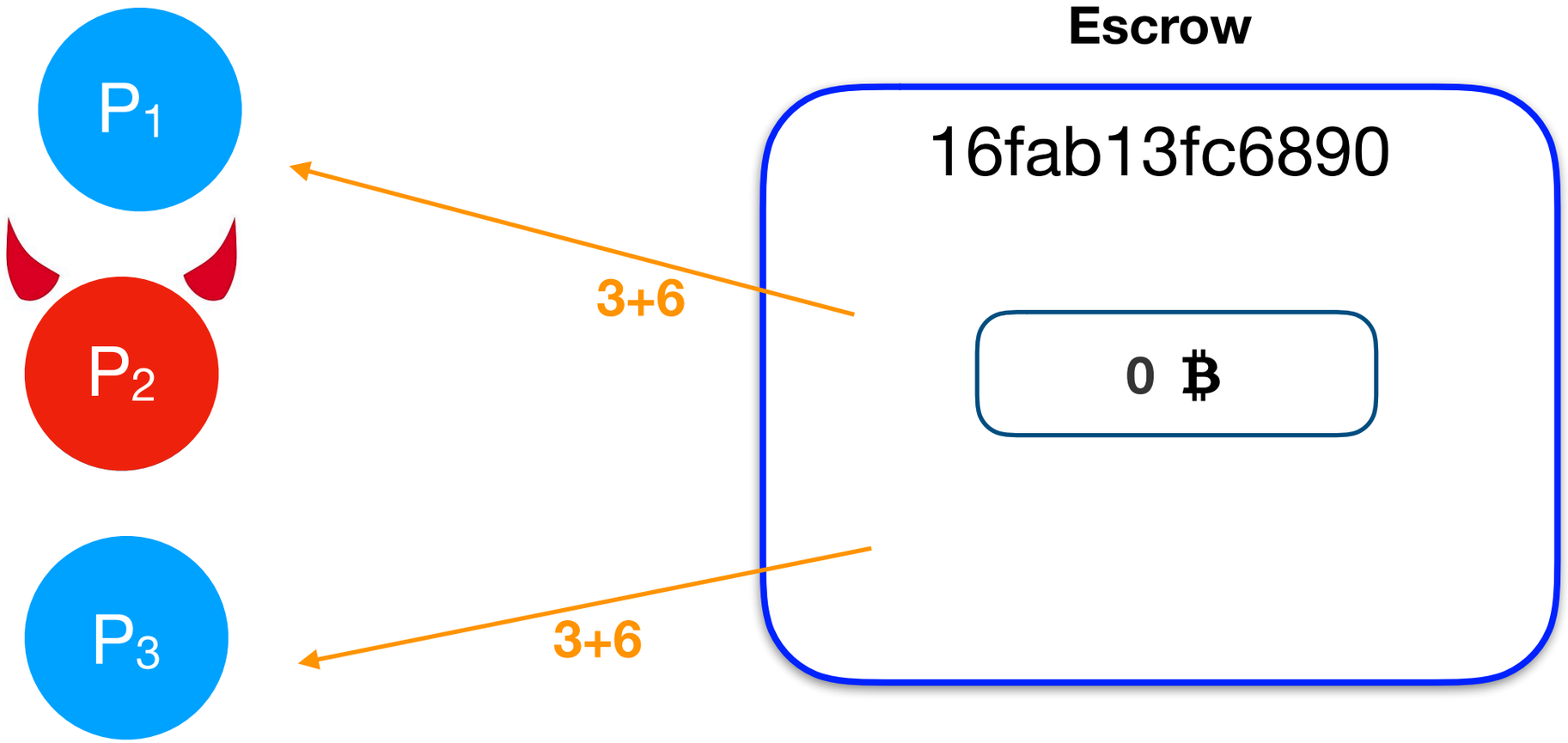
- Idea originated by Andrychowicz *et al.* [ADMM14] implemented in *Bitcoin* (only for lottery functionality)



- Extended by Bentov *et al.* to general purpose MPC with penalties

Penalties as the universal cure

- Idea originated by Andrychowicz *et al.* [ADMM14] implemented in *Bitcoin* (only for lottery functionality)



- Extended by Bentov *et al.* to general purpose MPC with penalties

Pocket depth's and financial fairness

- D*iscount rate.* Measure dependent on
  - the level of risk aversions
  - the confidence in the certainty of future payments
    - life expectancy.
- Say that **q** is the penalty amount, δ a measure of the discount rate, and assume that Pi deposits at time 0, then the loss of Pi at time t is defined as

$$\Delta_i = d_i - d_i(1 - \delta(t))$$

- A protocol with a common reward is financially fair iff for every pair of parties i,j $\Delta_i = \Delta_j$ at the end of the protocol

Ladder mechanism of Kumaresan *et al. vs other constructions*

- Kumaresan et al. for MPC with penalties, using the *ladder mechanism* to achieve fairness.
  - iq deposit for player player Pi
  - O(n) rounds of communication
  - **Not financially fair.**

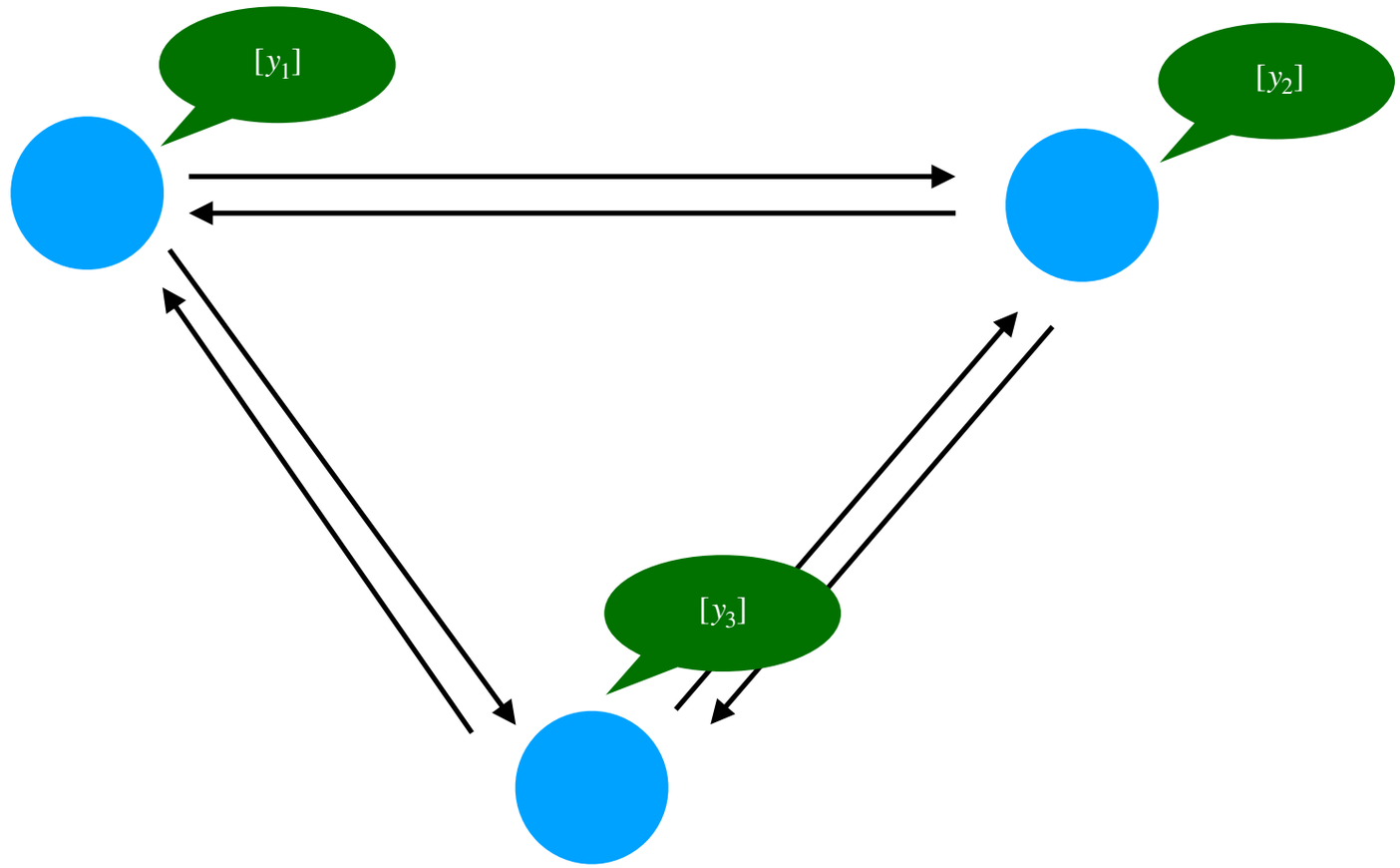
- Andrychowicz et al. for secure MPC lottery and Bentov et. al. for secure MPC with penalties
  - Each party deposits q(n-1)
  - O(1) rounds of communication
  - **Financially Fair.**

Share reconstruction protocol (Kumaresan et al) First step: unfair MPC

- N-out-of-N secret sharing: an attacker learns no information about y if he possess less than N shares

$$(y_1, \ldots, y_n) \leftarrow Share(y)$$

$$y \leftarrow Recon(y_1, \ldots, y_n)$$



Claim-Or-Refund functionality

DEPOSIT PHASE

P_s

"Deposit coins(x) redeemable by P_r"

$(\texttt{deposit}, s, r, \phi_{s,r}, \tau, \texttt{coins}(x))$

$\mathcal{F}_{CR}$

CLAIM PHASE

P_r

"Claim that I possess a witness w for x"

$(\texttt{claim}, s, r, \phi_{s,r}, \tau, x, \mathbf{w})$

"if the check passes send coins(x) to the receiver"

$\mathcal{F}_{CR}$

REFUND PHASE

P_s

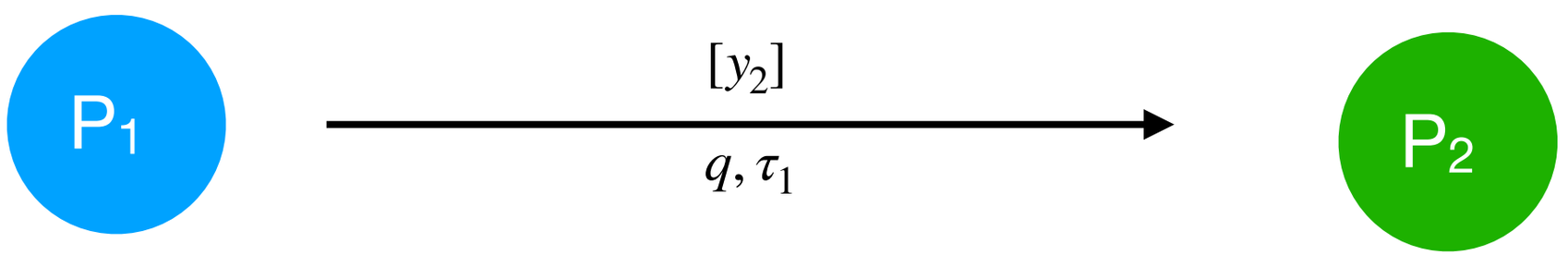
"If the deposit hasn't been claimed before τ refund coins(x) to P_s"

$(\texttt{refund}, s, r, \phi_{s,r}, \tau, \texttt{coins}(x))$

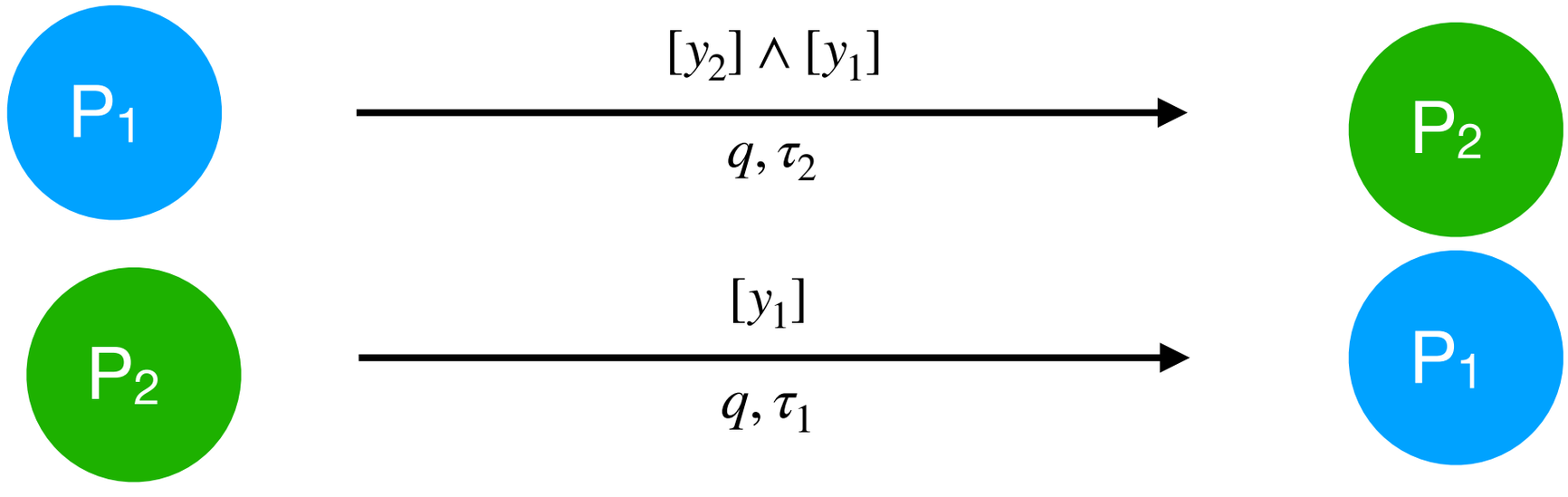
$\mathcal{F}_{CR}$

Share reconstruction ladder mechanism *for 2 parties:*

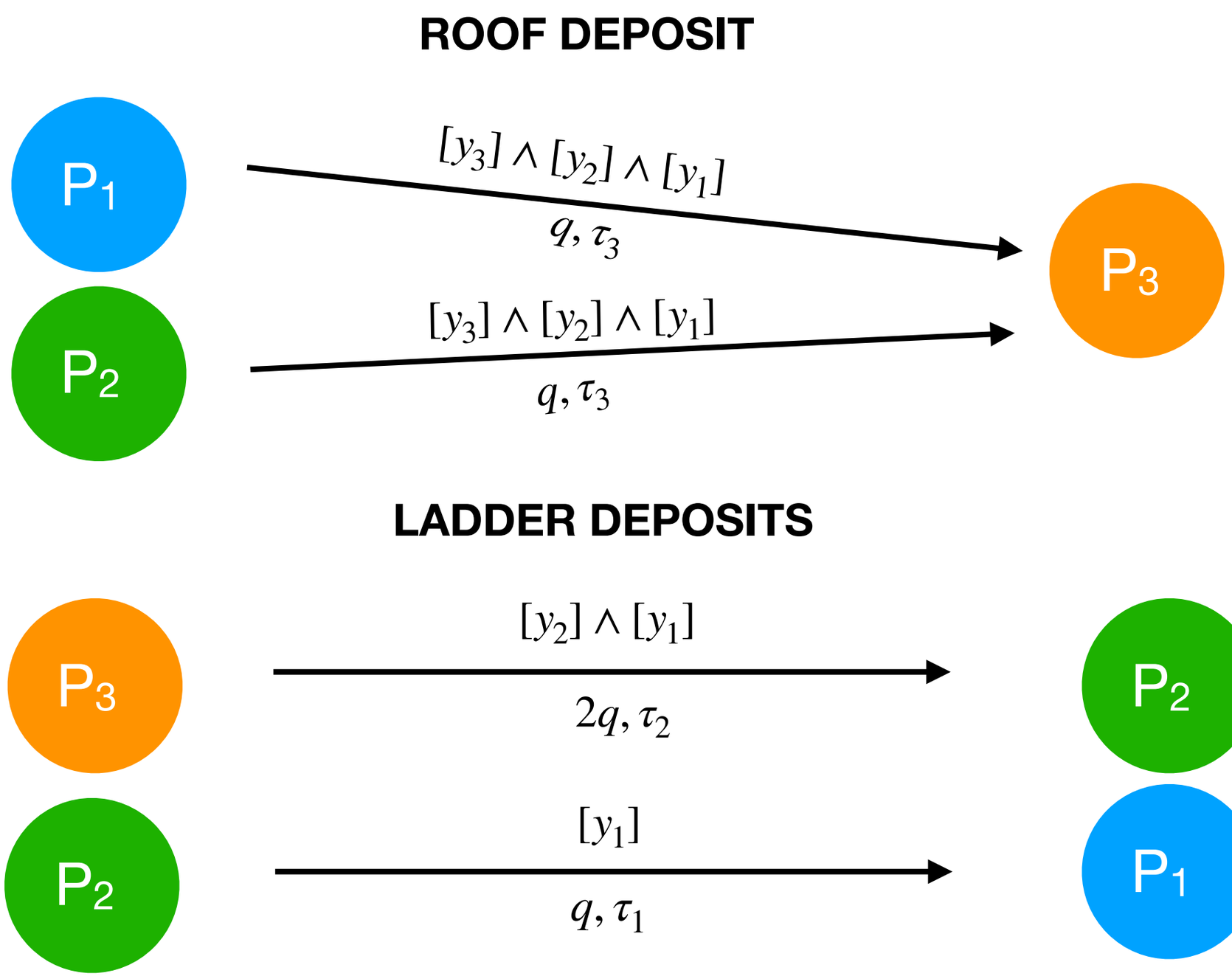
NAIVE IDEA



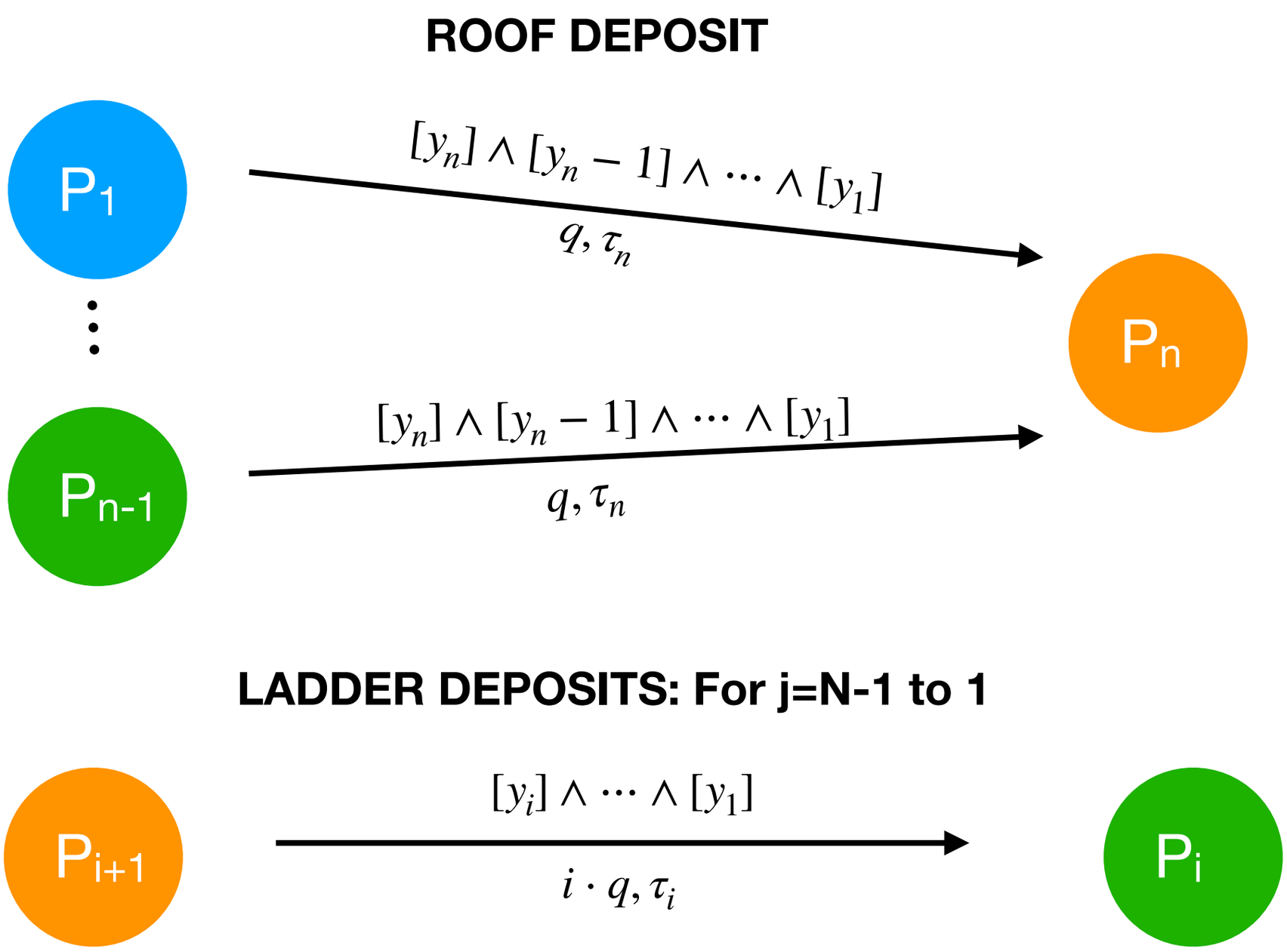
MODIFIED PROTOCOL



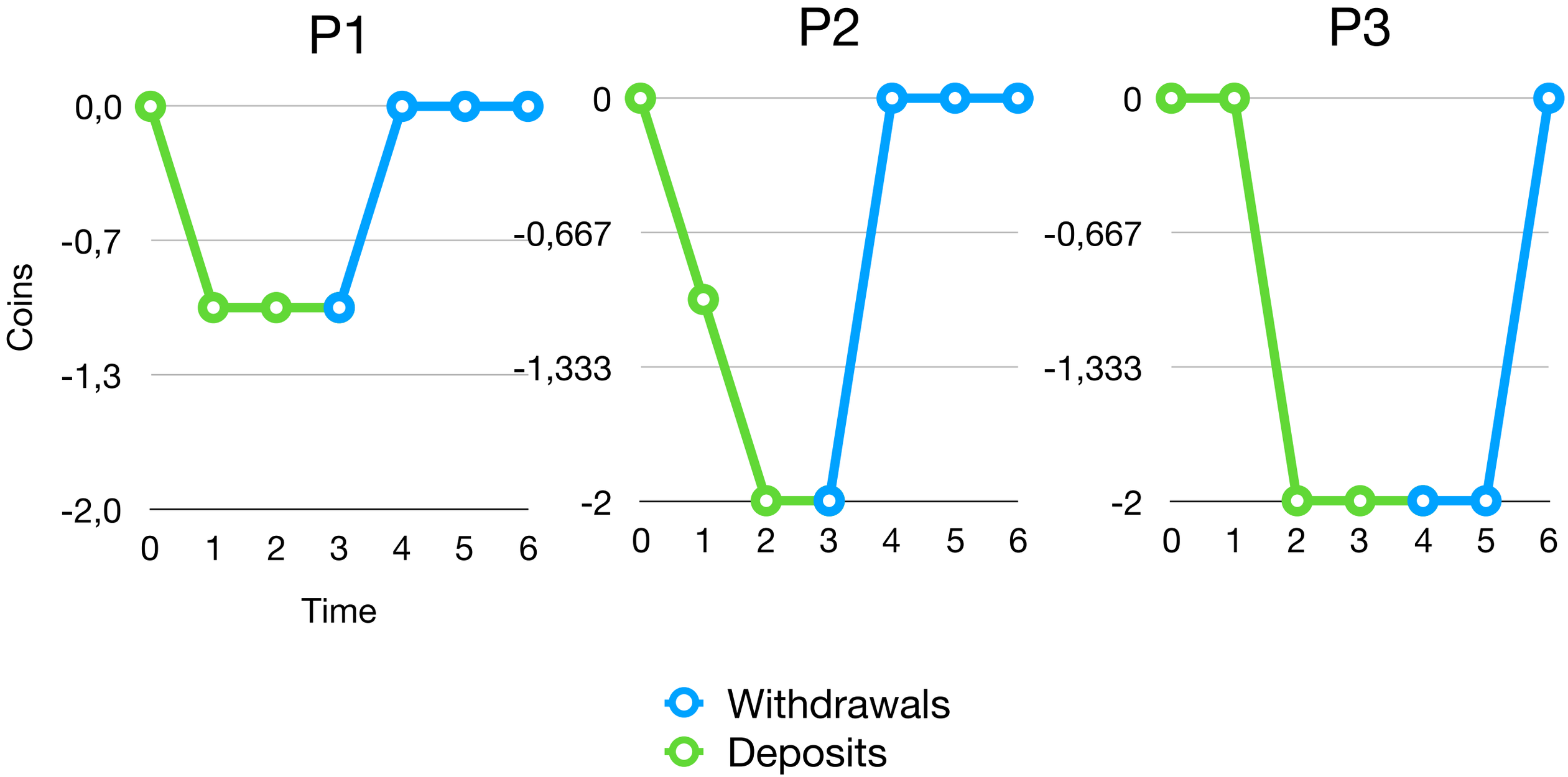
Share reconstruction ladder mechanism *for 3 parties:*



Share reconstruction ladder mechanism *for n parties:*



3-party ladder



Loss for each player in case of q = 100$ (3 parties)

Party	0%	0,1%	0,25%	0,75%	1%	3%
P_1	0$	-0,4$	-1,0$	-2,9$	-3,9$	-10,8$
P_2	0$	-1,2$	-3,0$	-8,7$	-11,4$	-31,3$
P_3	0$	-1,3$	-3,2$	-9,4$	-12,3$	-33,1$

Conclusions and ongoing work

- Kumaresan et al. ladder mechanism is not Financially Fair, while other protocols, and Andrychowicz et al for lottery is

- Defined a new measure to calculate money loss in escrow protocols

- Standard abstraction for every escrow protocol and loss function defined for more general cases

- Bentov *et al.* protocol for secure MPC with penalties proved in a stronger model and implemented more efficiently in Bitcoin