TACEO

[Don‘t] share your data.

TACEO.IO

TACEO

How to participate in the Workshop

TACEO

MPC meets circom and Noir

What are co-SNARKs?

Millionaires Problem

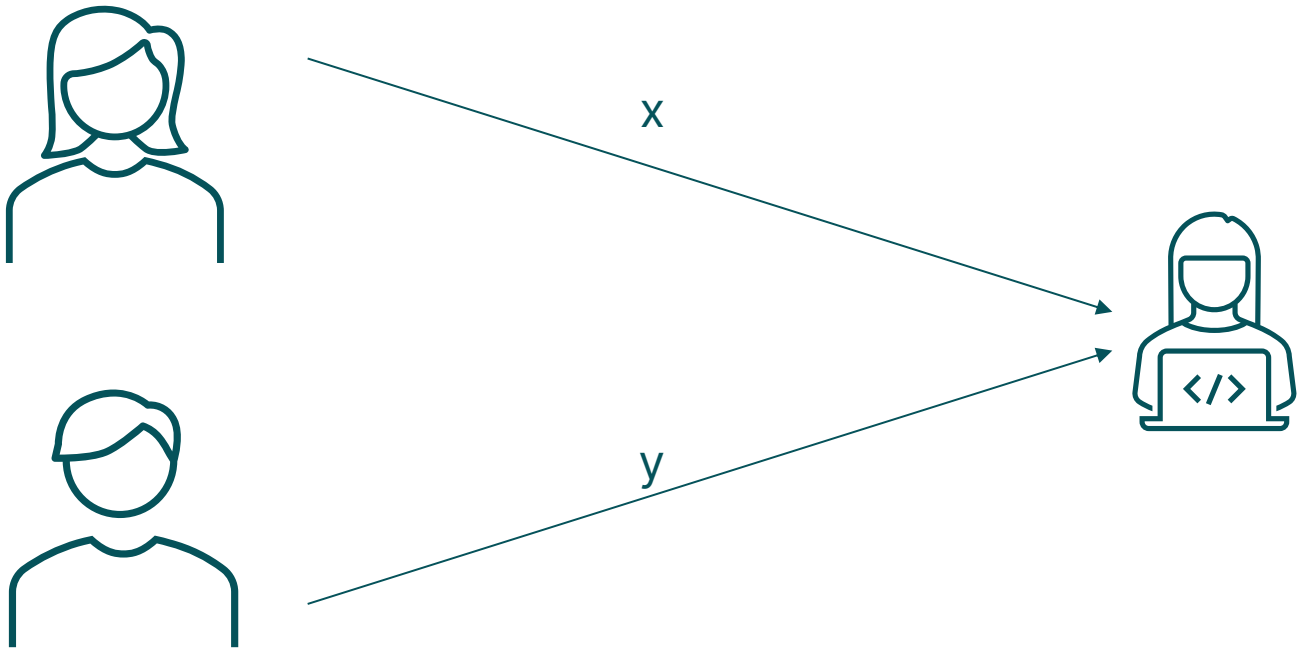
Millionaires Problem

Who is richer?

Millionaires Problem

Millionaires Problem

Millionaires Problem



Millionaires Problem

Millionaires Problem

How to share a secret?

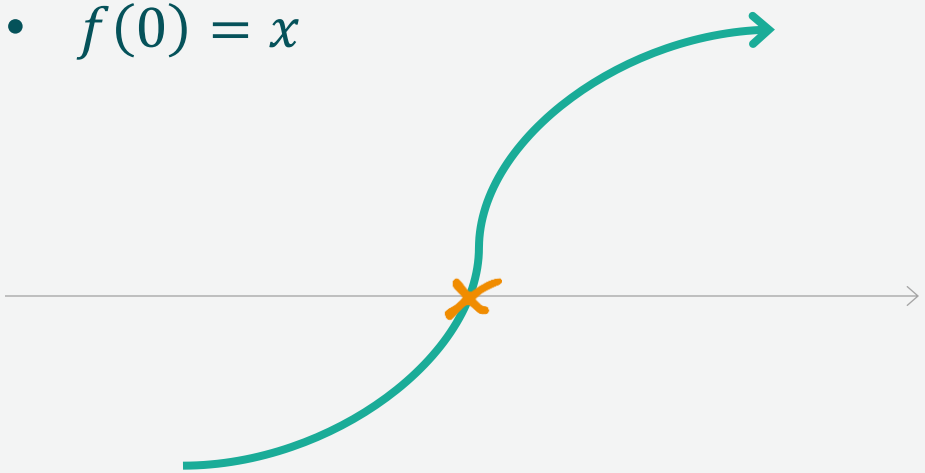
MPC

TACEO

How to share a secret?

Shamir Secret Sharing

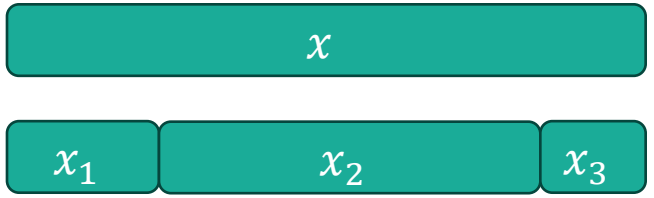
- Polynomial $f(x)$ of degree d
- Sample n points
- $f(0) = x$



Additive Secret Sharing

- Split x in n parts

$$\sum_{n} x_i = x$$

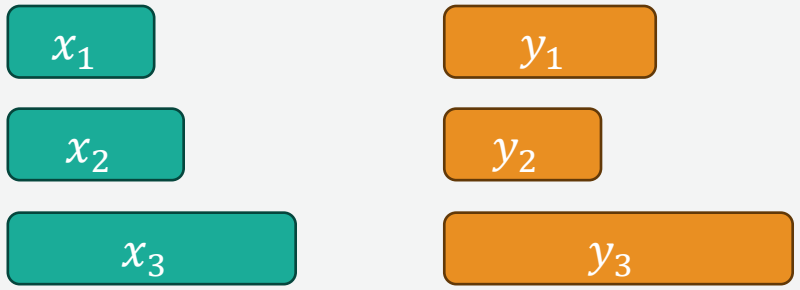


TACEO

Computing on secrets

Addition

Two secrets x and y

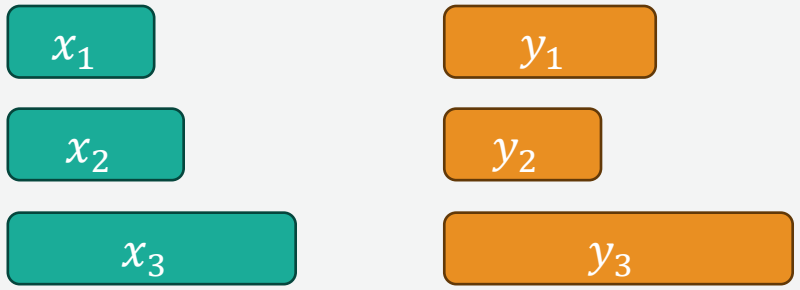


TACEO

Computing on secrets

Addition

Two secrets x and y



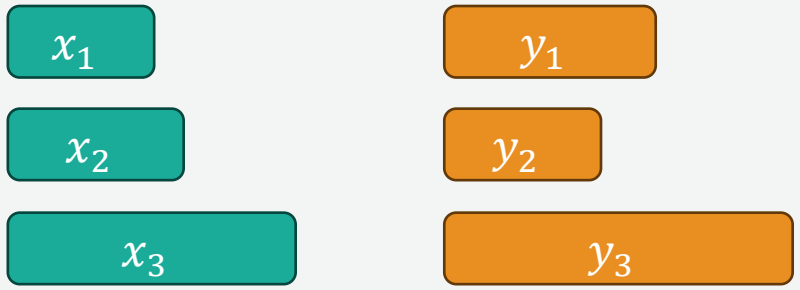
$$\begin{matrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{matrix} \quad = x + y$$

TACEO

Computing on secrets

Addition

Two secrets x and y



$$\begin{matrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{matrix} \quad = x + y$$

Multiplication

?

TACEO

Non-linear Operations

- Beaver triples
  - Generate helper triples $([\mathrm{a}], [\mathrm{b}], [c])$ and $ab = c$
  - Open $[a + x] = A$ and $[b + y] = B$
  - Compute $Ay + (-B)[a] + [c] = [xy]$

Non-linear Operations

- Beaver triples
  - Generate helper triples $([a],[b],[c])$ and $ab = c$
  - Open $[a + x] = A$ and $[b + y] = B$
  - Compute $Ay + (-B)[a] + [c] = [xy]$
- Replicated Secret Sharing (2 out of 3 sharing)
  - Parties hold two shares instead of one
  - Every party computes $x_a y_a + x_a y_b + x_b y_a + m$, where $m = [0]$
  - Reshare result

TACEO

Key take away

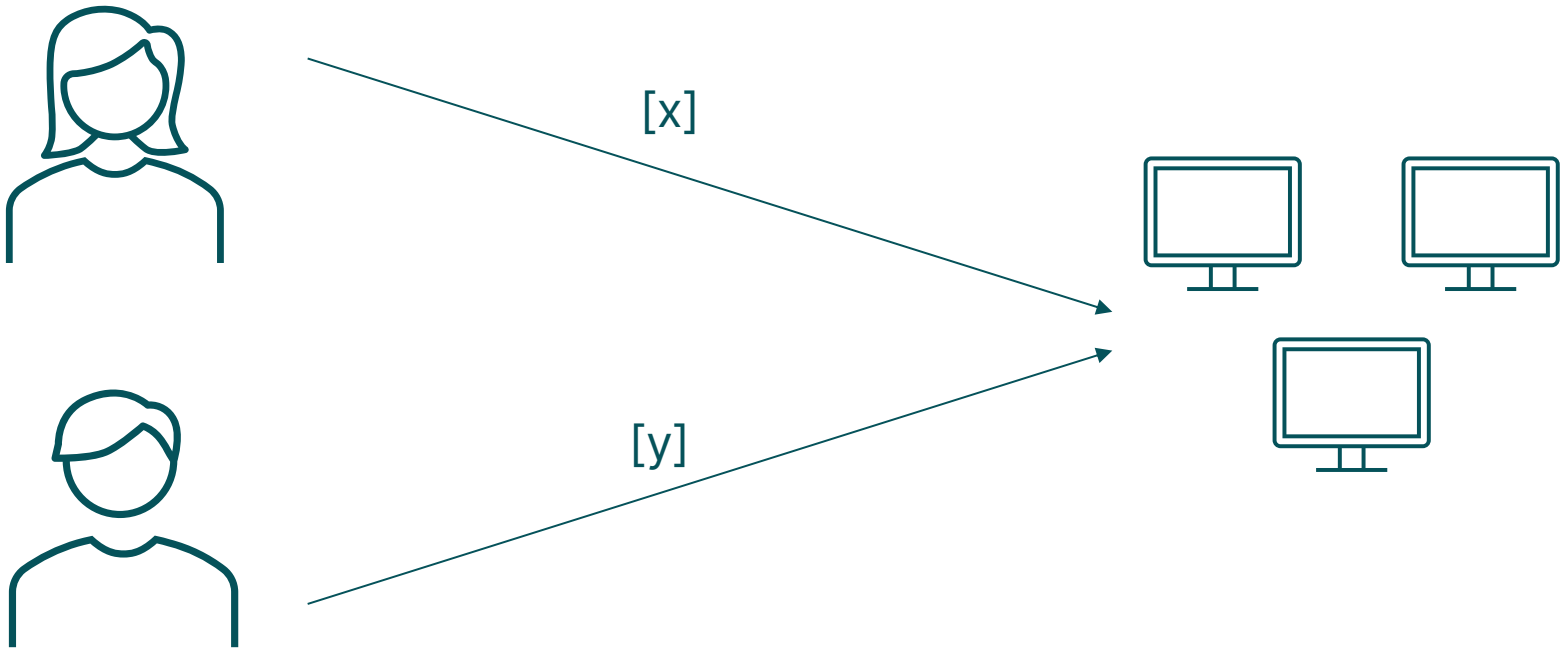
Linear operations (+)

- Parties compute locally on shares

Non-linear operations (*)

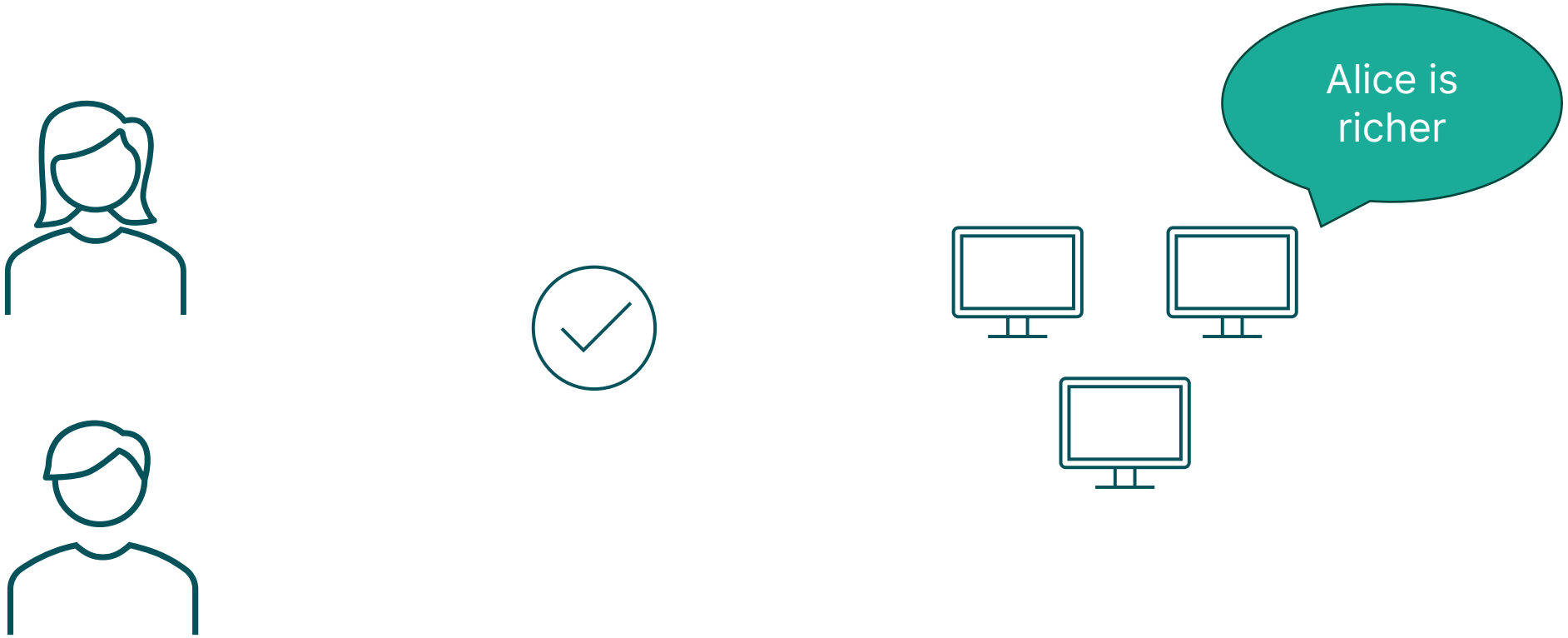
- Parties need to communicate

Millionaires Problem



Millionaires Problem

Millionaires Problem



Millionaires Problem

- Alice and Bob are two distrusting parties
- They have private information (their net worth)
  - Engage in an MPC protocol to compute who is richer

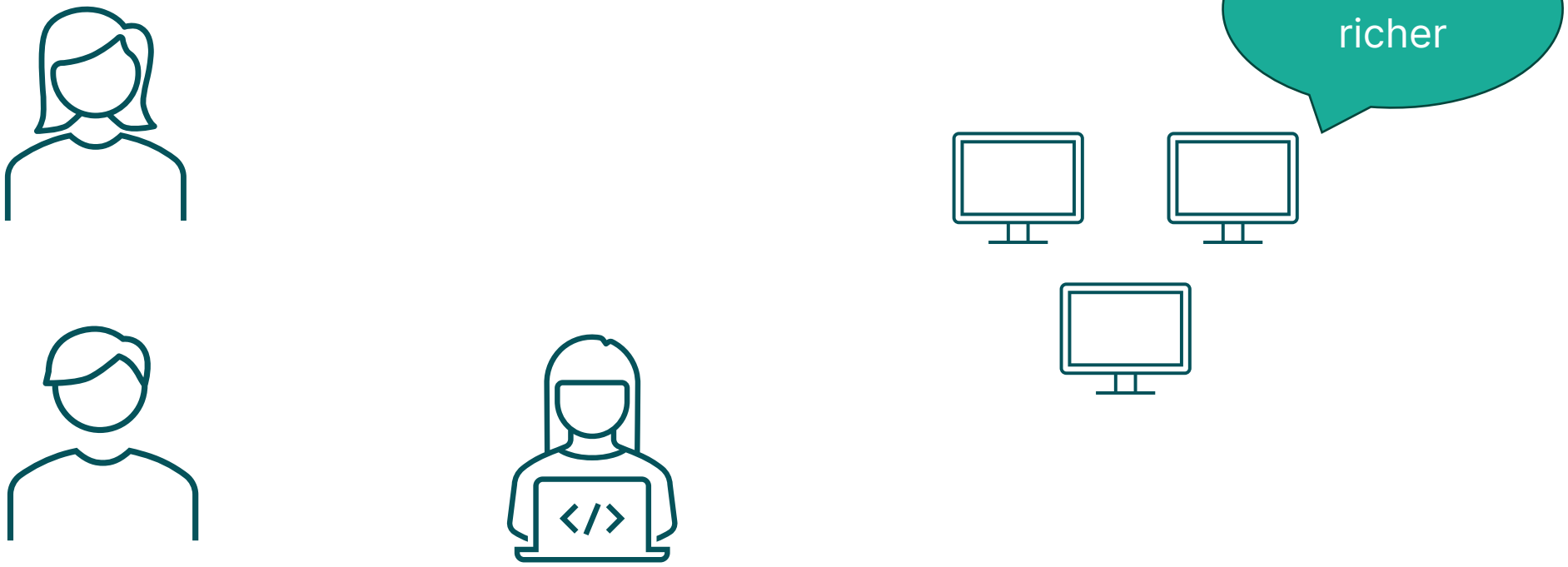
TACEO

Millionaires Problem

- Alice and Bob are two distrusting parties
- They have private information (their net worth)
  - Engage in an MPC protocol to compute who is richer

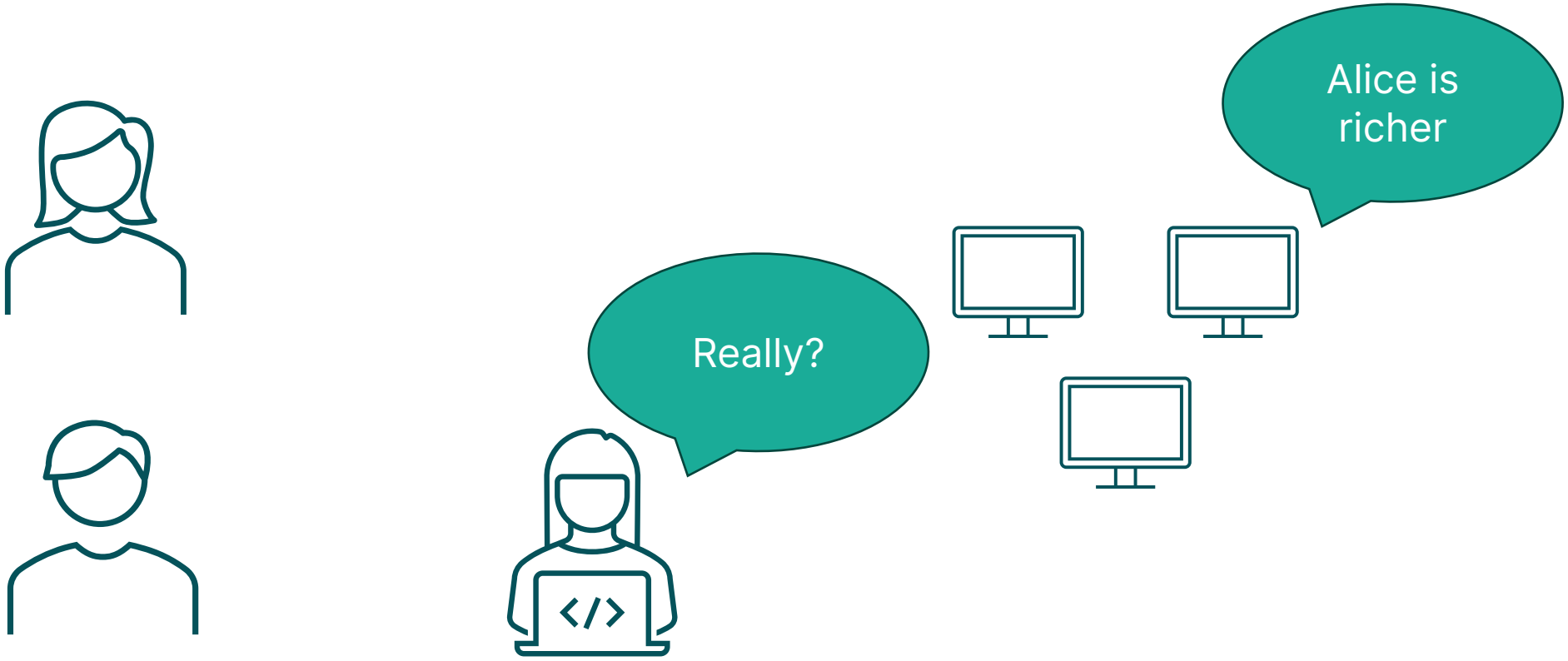
What is the problem?

Millionaires Problem



TACEO

Millionaires Problem



TACEO

Millionaires Problem

- Only involved parties know
  - whether they behaved honest (depending on MPC protocol)
  - what they computed
- If Charlette also wants to know who is richer, she must trust Alice and Bob

TACEO

What now?

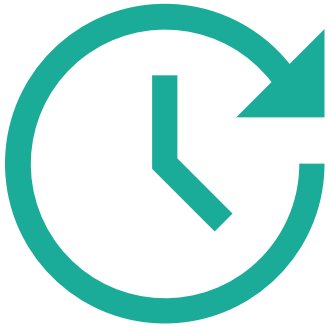
TACEO

zk-SNARKs 101

zk-SNARKs 101

TACEO

zk-SNARKs 101



Succinct proof for computational integrity

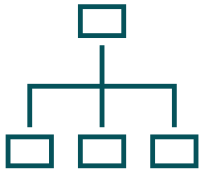
Keeping secret input hidden (potentially)

TACEO

What are co-SNARKs?

Zero-Knowledge

MPC

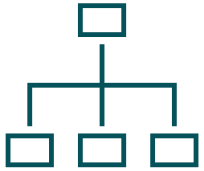


TACEO

What are co-SNARKs?

Zero-Knowledge

MPC

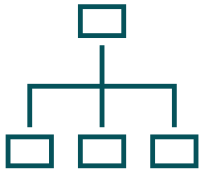


TACEO

What are co-SNARKs?

Zero-Knowledge

MPC



co-SNARKs

TACEO

ZK + MPC = ❤

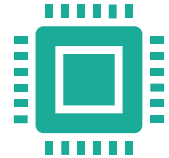
co-SNARKs

TACEO

Collaborative zk-SNARKs

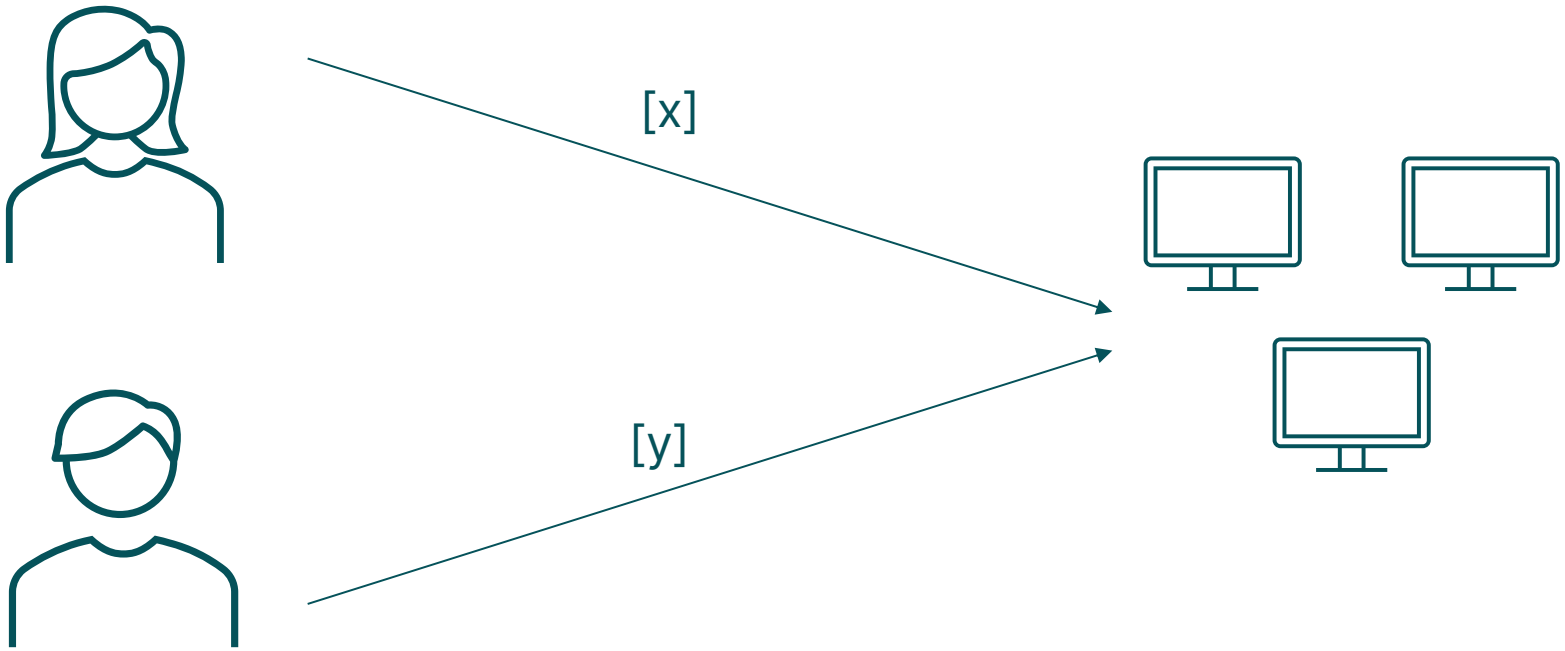
Allows multiple distrusting parties to jointly compute a proof

Execute the ZK prover in an MPC circuit



TACEO

Millionaires Problem



Millionaires Problem

TACEO

Millionaires Problem

TACEO

Performance

Linear operations (+)

Non-linear operations (*)

TACEO

Performance

Linear operations (+)

- FFTs
- MSMs

Non-linear operations (*)

TACEO

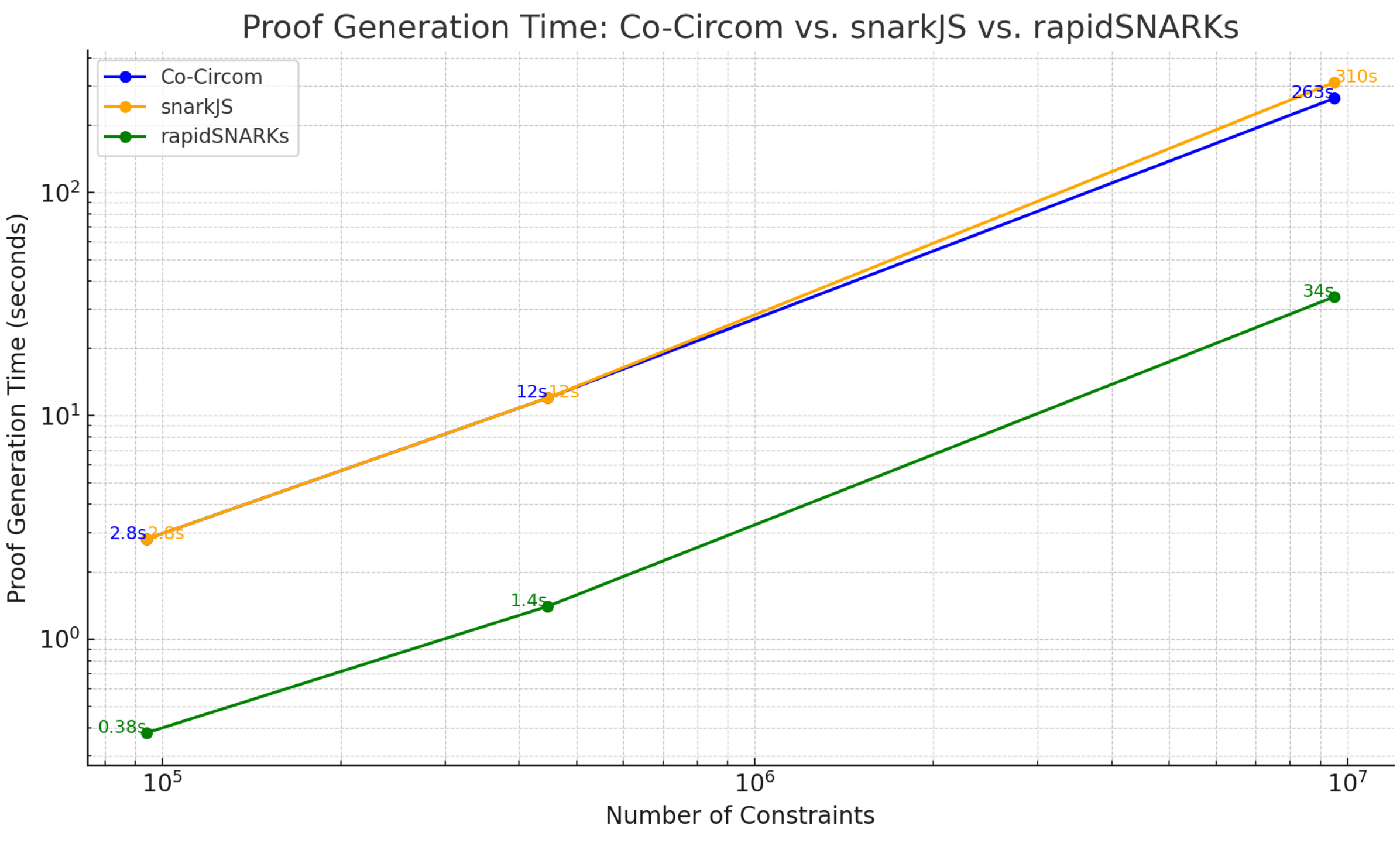
Performance

Linear operations (+)

- FFTs
- MSMs

Non-linear operations (*)

- Large multiplications
- Hash based commitment schemes (STARKs)


Proof Generation Time: Co-Circom vs. snarkJS vs. rapidSNARKs
Co-Circom
snarkJS
rapidSNARKs
Proof Generation Time (seconds)
Number of Constraints
10^2
10^1
10^0
10^5
10^6
10^7
263s
310s
12s
12s
2.8s
2.8s
34s
1.4s
0.38s

TACEO

Use Cases

Private Shared State

- Compute on multiple private states
- Roll computation on-chain
  - All benefits of succinct proofs

TACEO

Use Cases

Private Shared State

- Compute on multiple private states
- Roll computation on-chain
  - All benefits of succinct proofs

Private Proof Delegation

- Outsource proving
- Privacy not compromised
- Limited hardware

TACEO

How to participate in the Workshop

(and co-Noir, we need to change the name)

co-circom

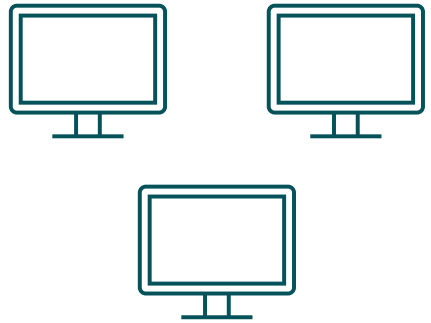
TACEO

co-circom

- Build co-SNARKs based on
  - Circom
  - Noir
- Support for Groth16/PLONK
- Leverage the existing toolchain
  - Verifier cannot distinguish between coSNARK and zkSNARK

Max Pick Challenge

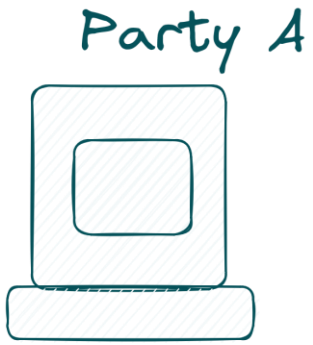
- Game written with co-circom
- Highest Unique Guess wins
  - ⇒ keep guess secret
- Fully deployed on Optimism

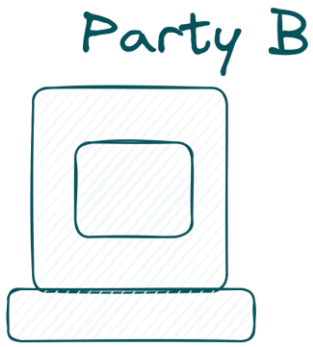


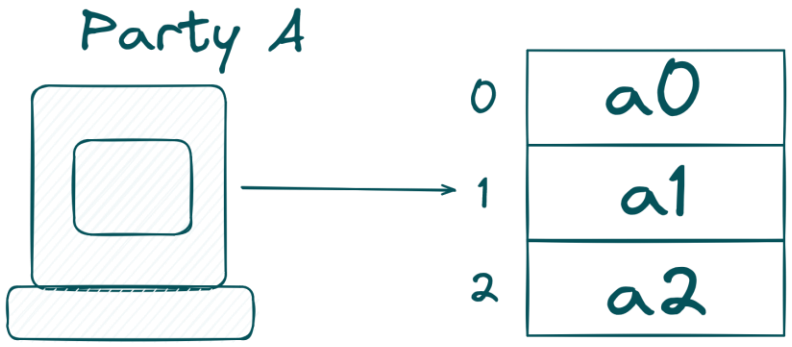
How to participate in the Workshop

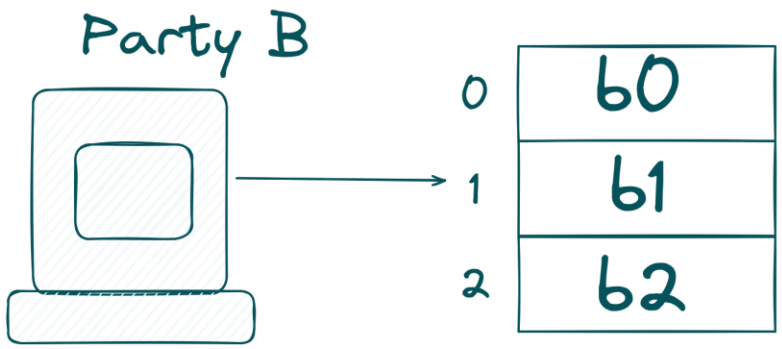
TACEO

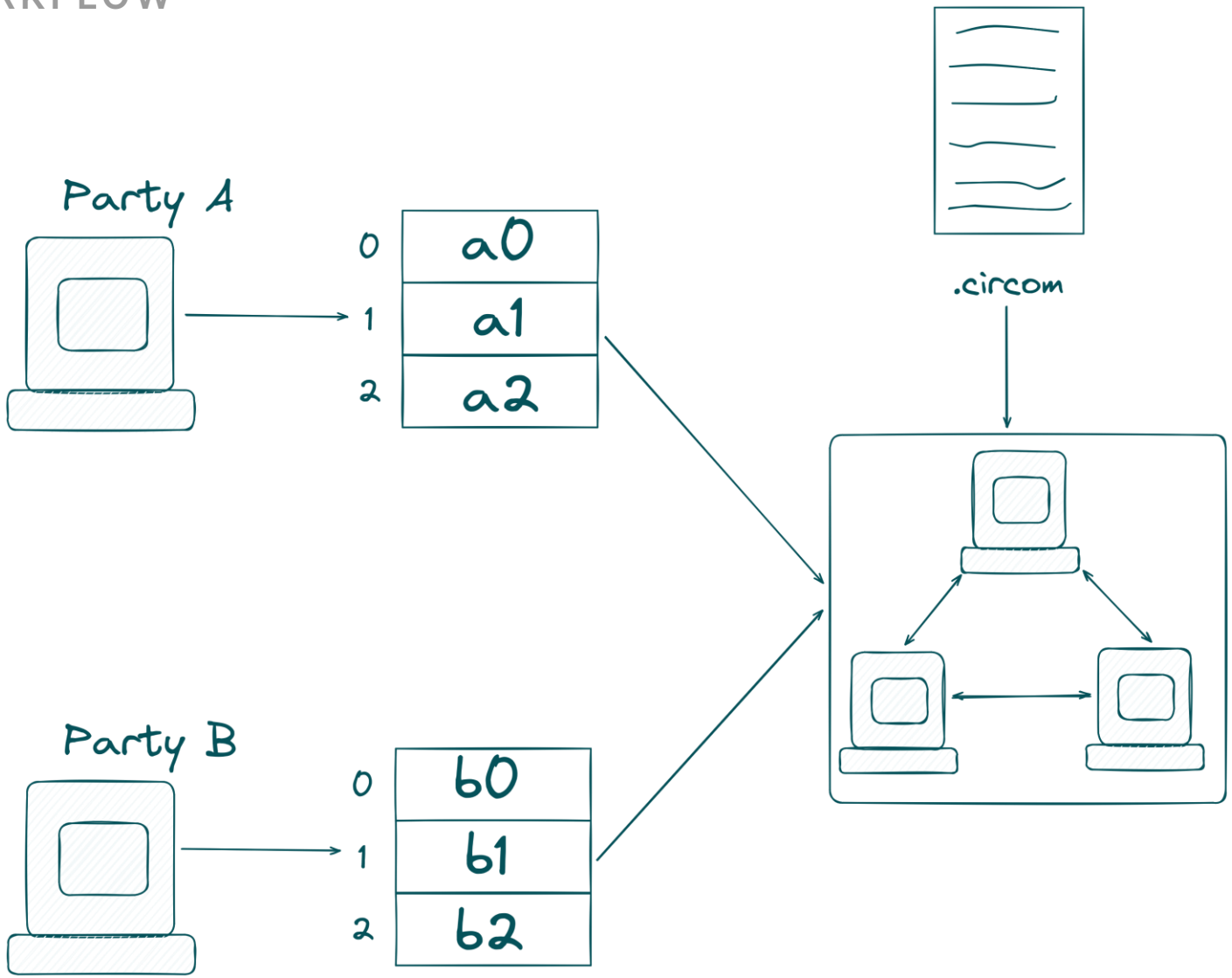
Workflow

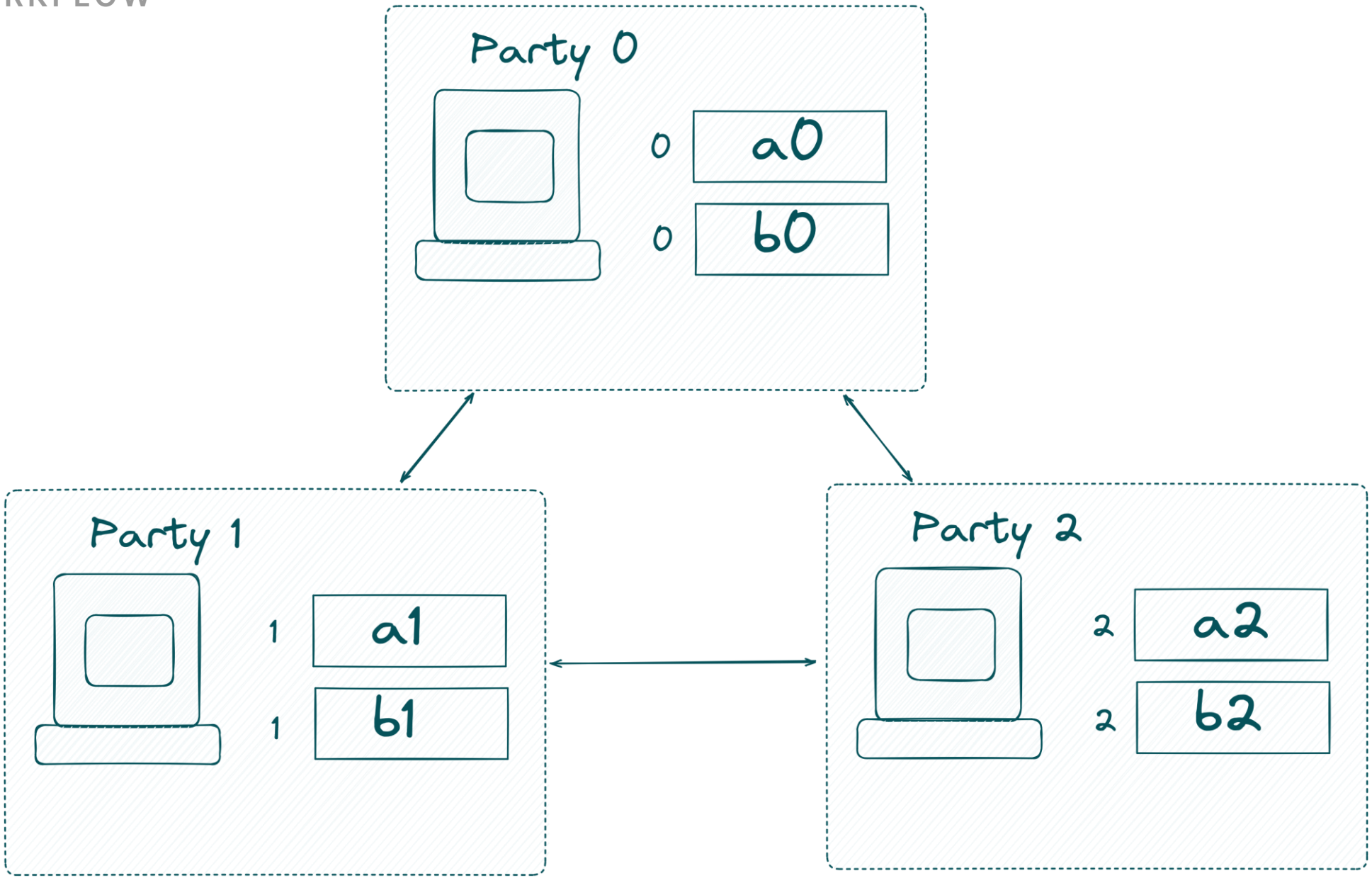

Party A


Party B

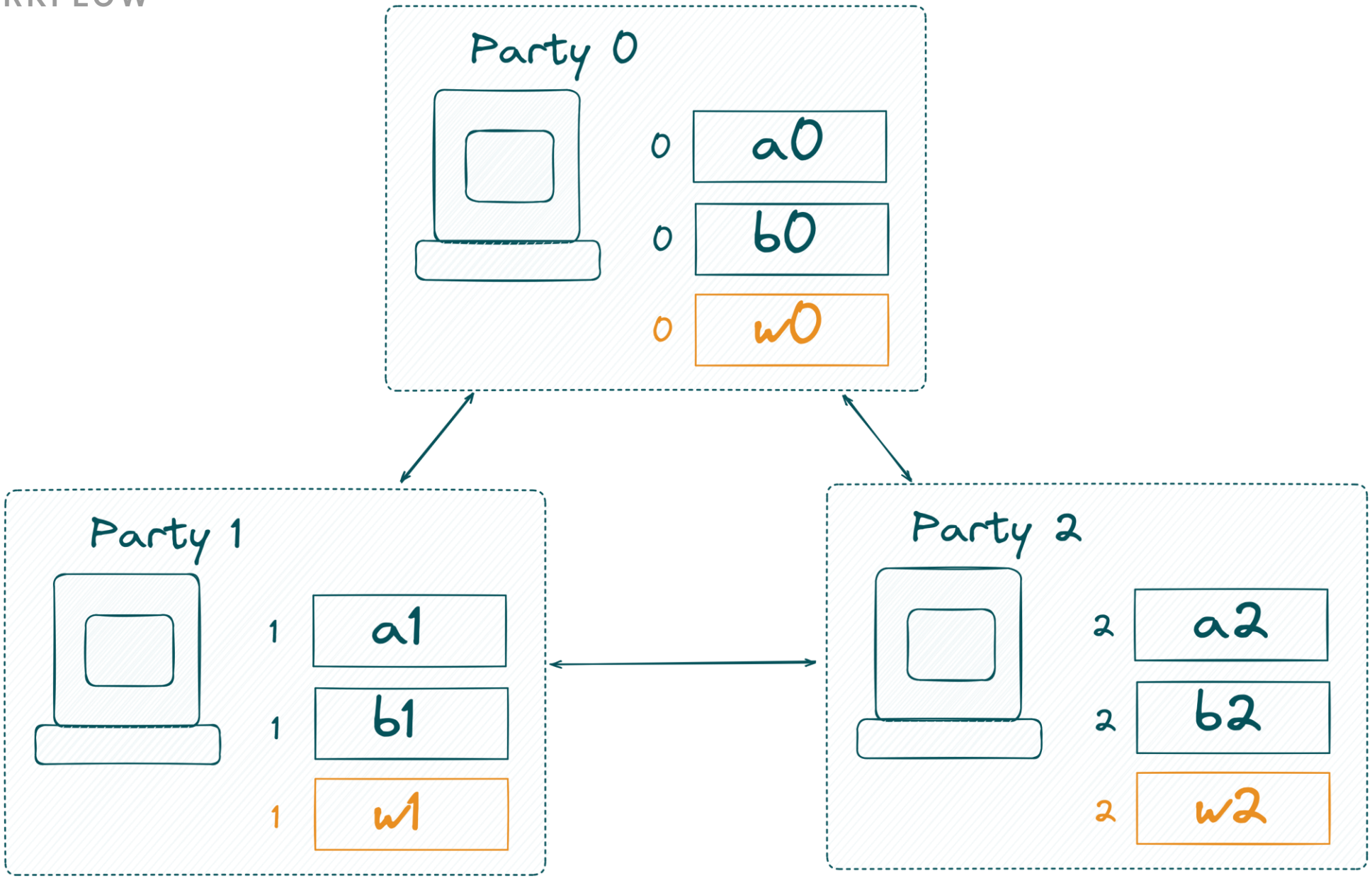

Party A
0
a0
1
a1
2
a2

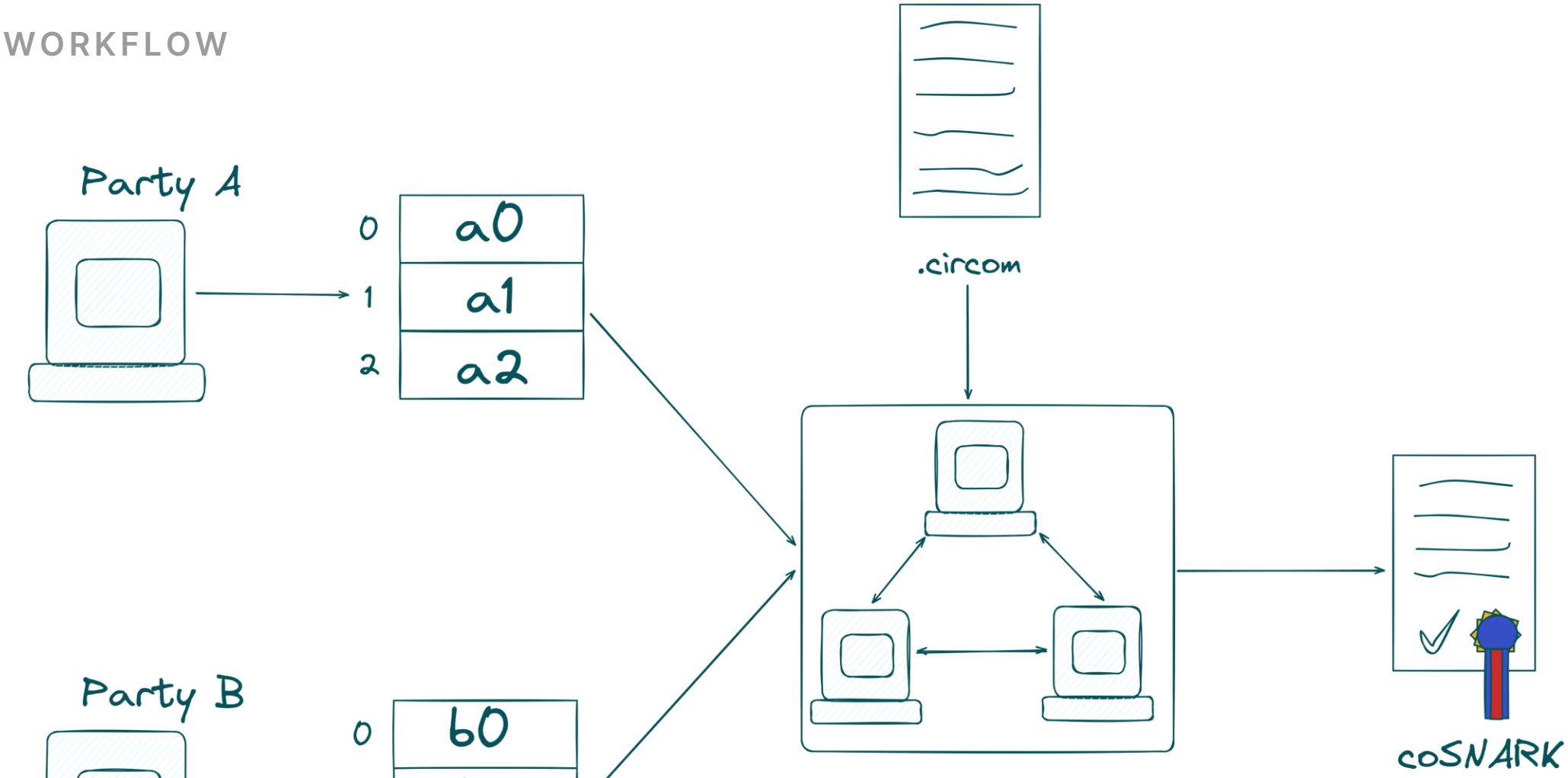

Party B
0
b0
1
b1
2
b2


Party A
0
a0
1
a1
2
a2
.circom
Party B
0
b0
1
b1
2
b2


Party 0
0
a0
0
b0
Party 1
1
a1
1
b1
Party 2
2
a2
2
b2

TACEO




Party A
0
1
2
a0
a1
a2
.circom
Party B
0
1
2
b0
b1
b2
coSNARK

TACEO

Please leave a start ♥