



Circom

October 22, 2024

Distributed Lab

 [zndl-camp.github.io](https://github.com/zndl-camp)

 github.com/ZKDL-Camp

Plan

1 Introduction

2 Circom

3 Practice

Introduction
●○○○

Circom
○○○

Practice
○○

Introduction

Why ZK?

Why ZK?

Why do we need ZK?

1. Solution to privacy
2. Solution to scalability

Why ZK?

Why do we need ZK?

1. Solution to privacy
2. Solution to scalability

Example

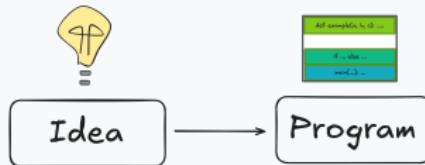
1. *I know the private key that corresponds to this public key*
2. *I know a private key that corresponds to a public key from this list*
3. *I know the preimage of this hash value*
4. *This is the hash of a blockchain block that does not produce negative balances*

Using ZKP

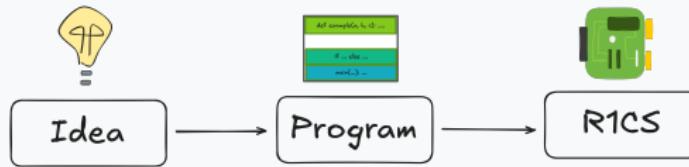
Using ZKP



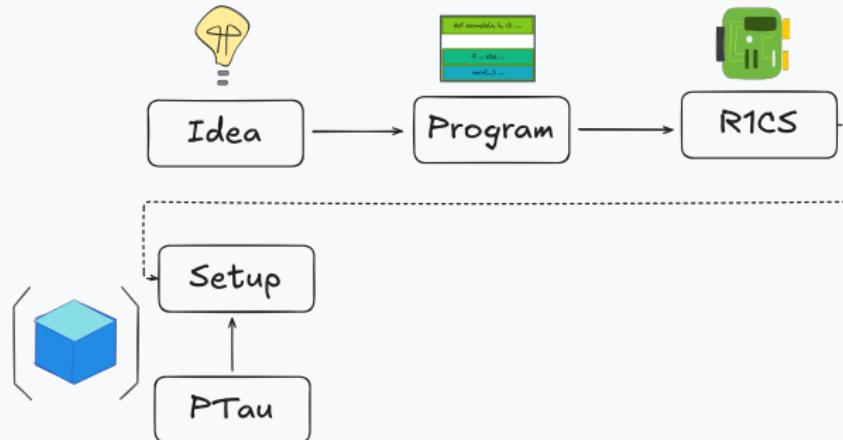
Using ZKP



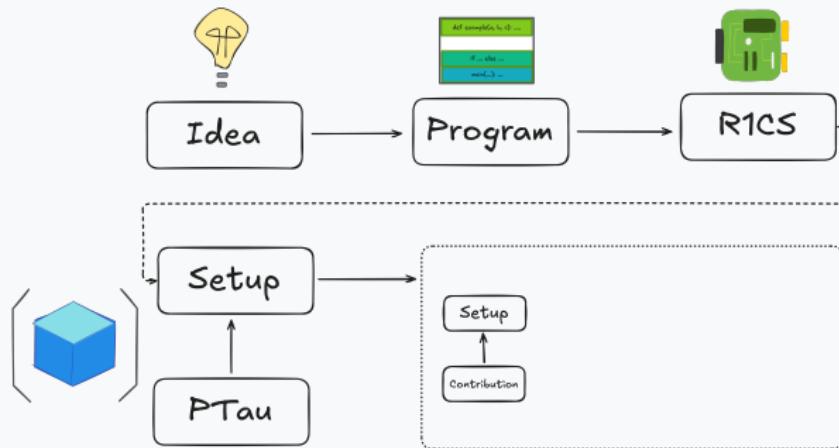
Using ZKP



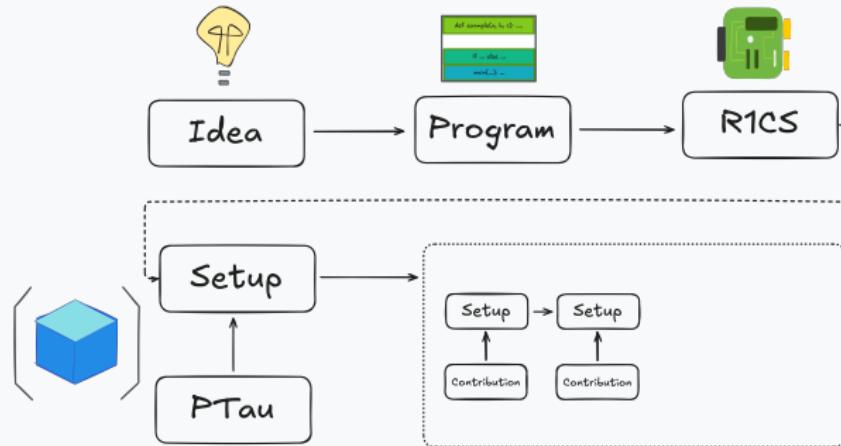
Using ZKP



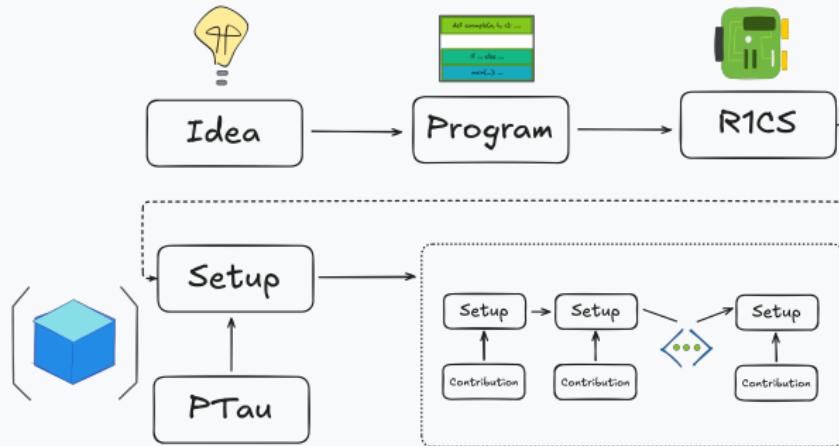
Using ZKP



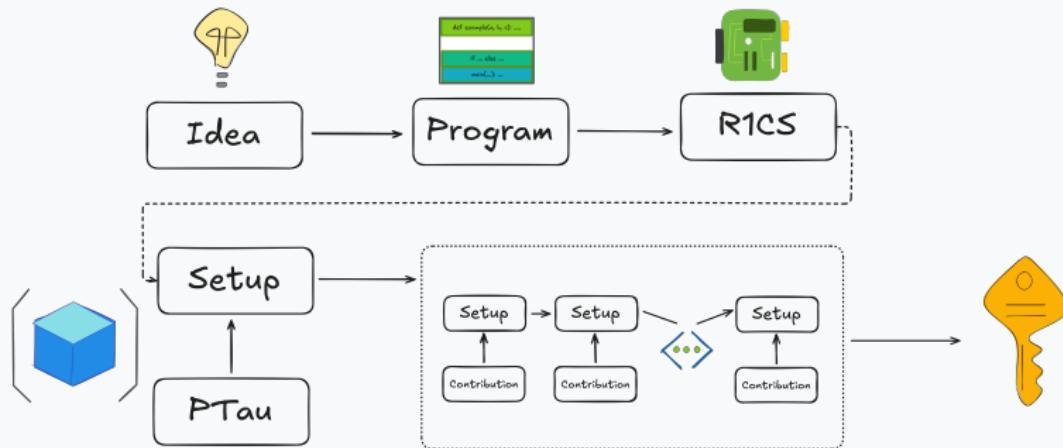
Using ZKP



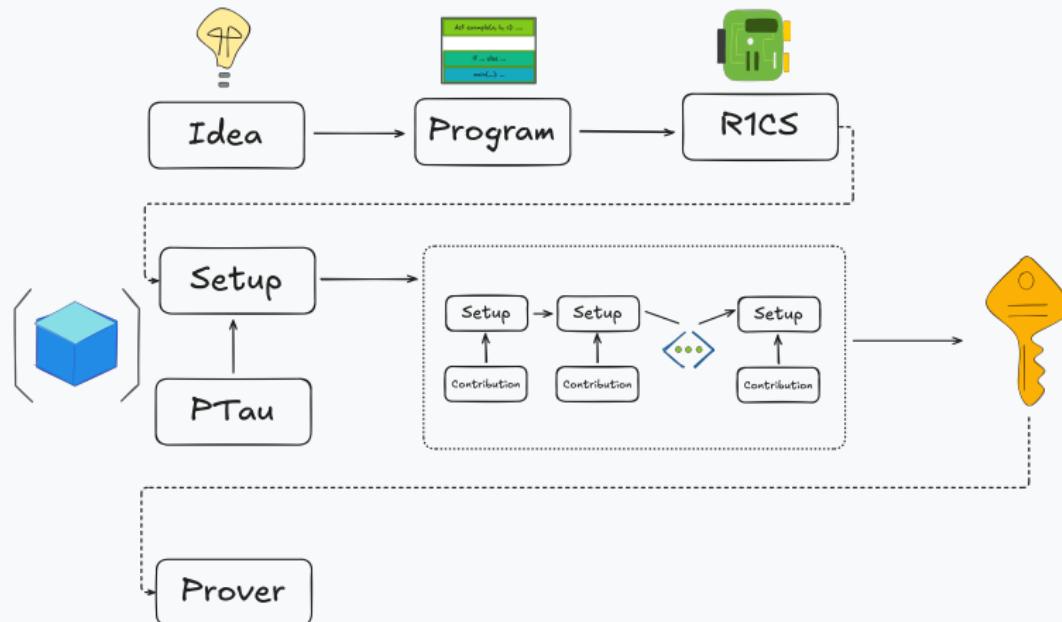
Using ZKP



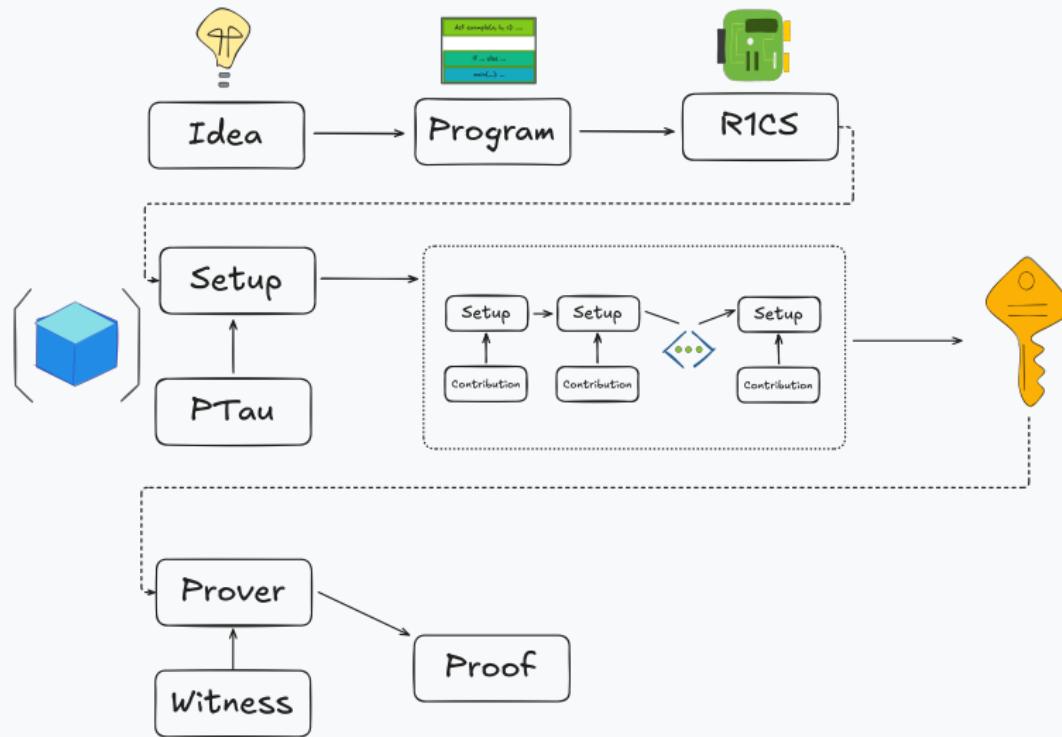
Using ZKP



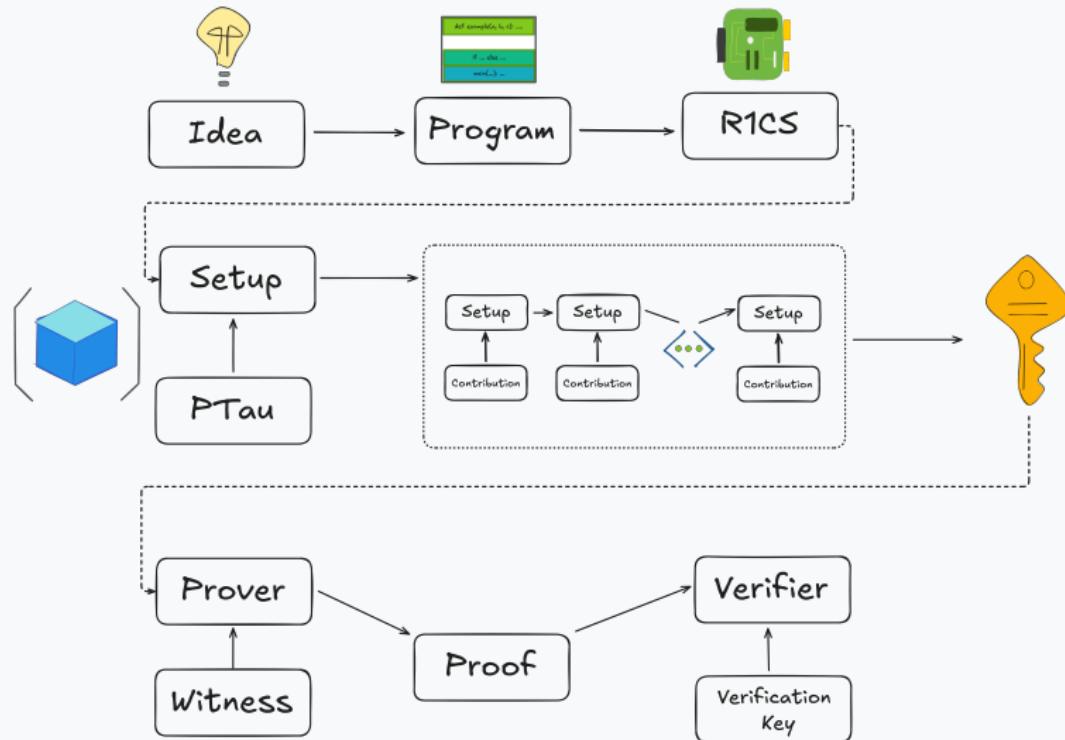
Using ZKP



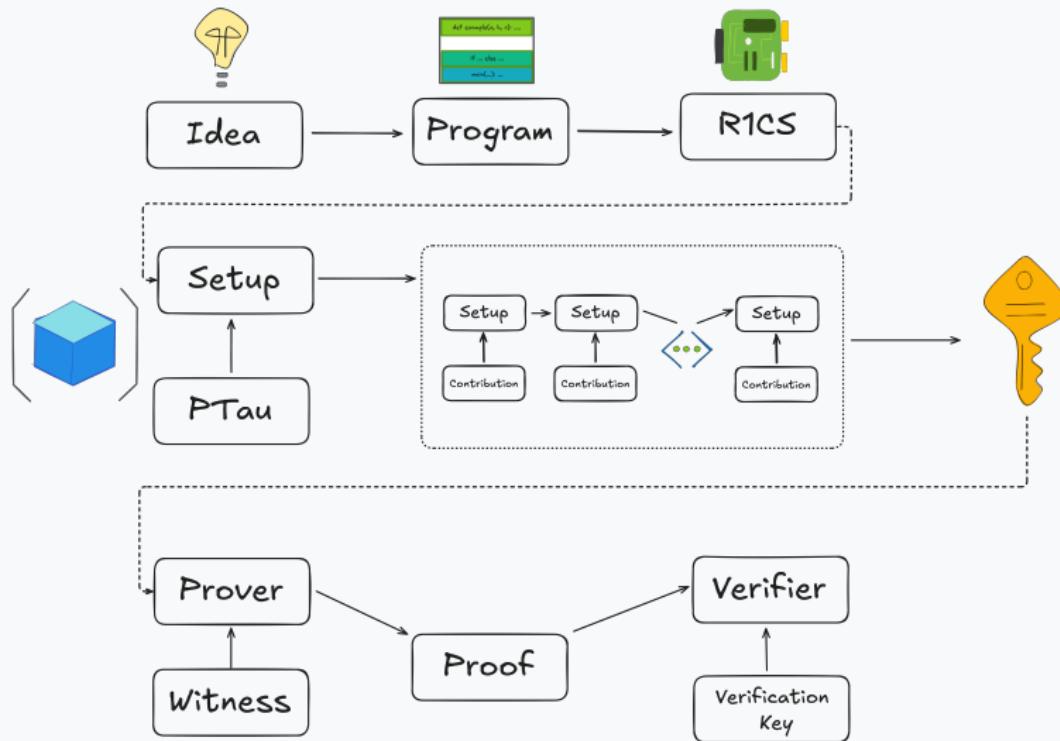
Using ZKP



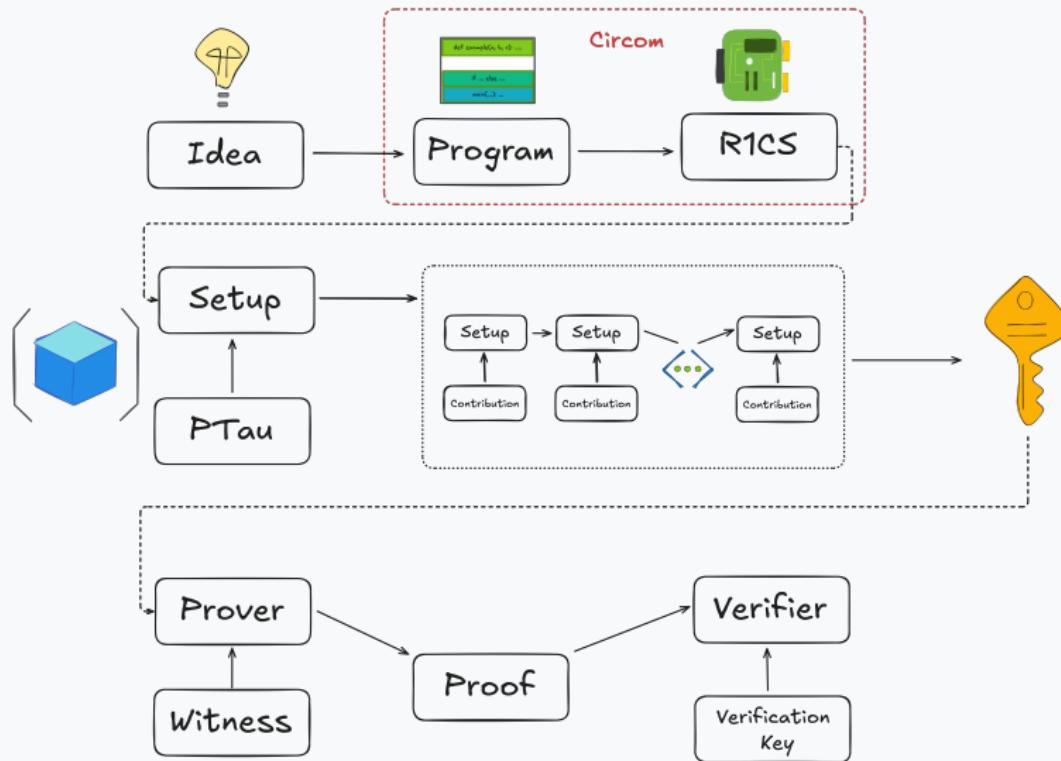
Using ZKP



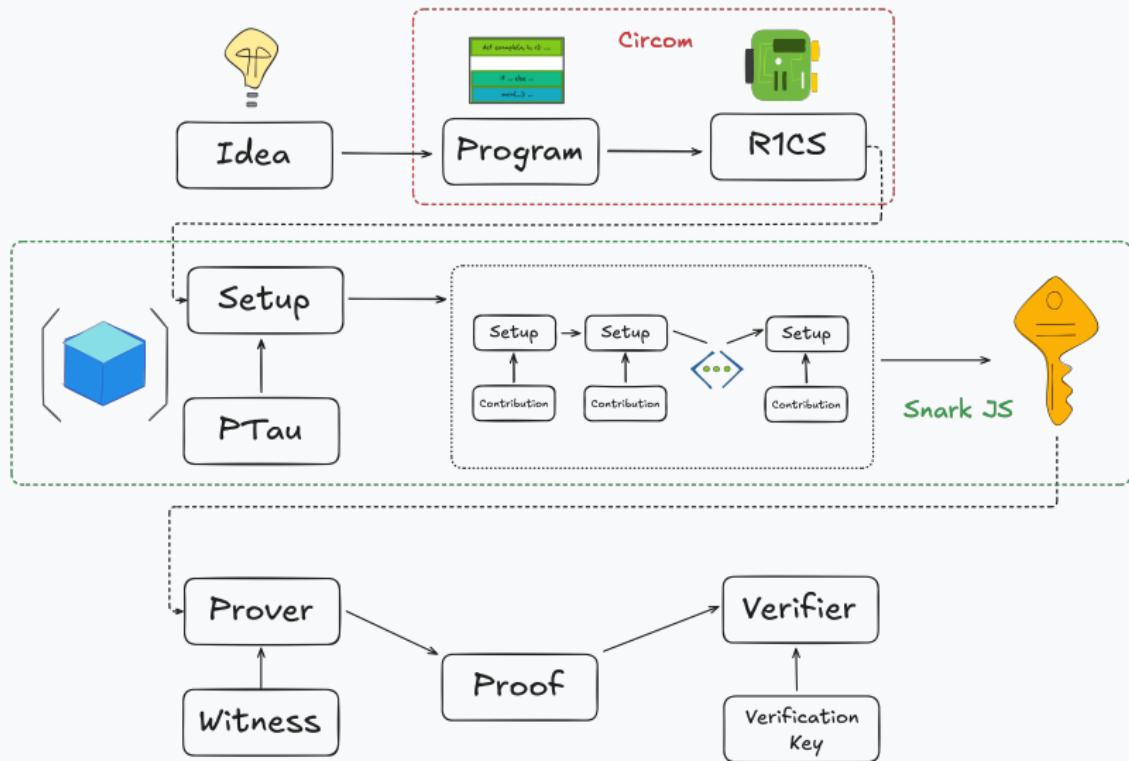
Toolchain



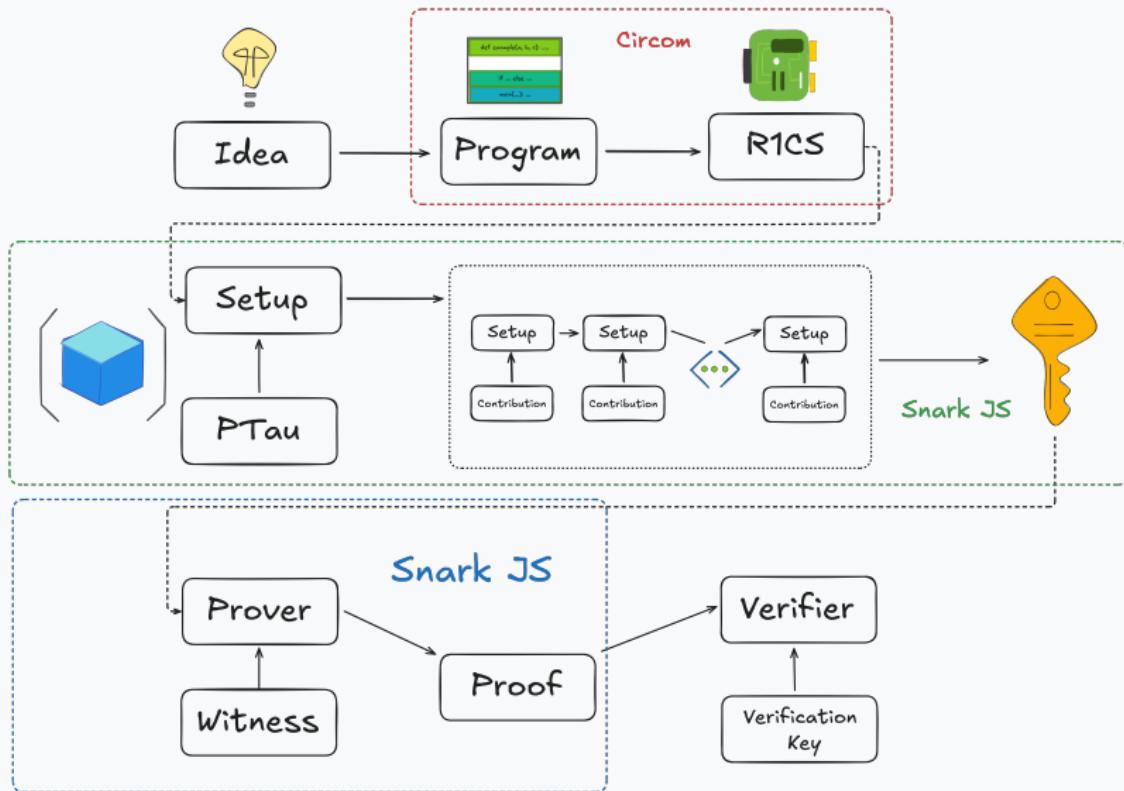
Toolchain



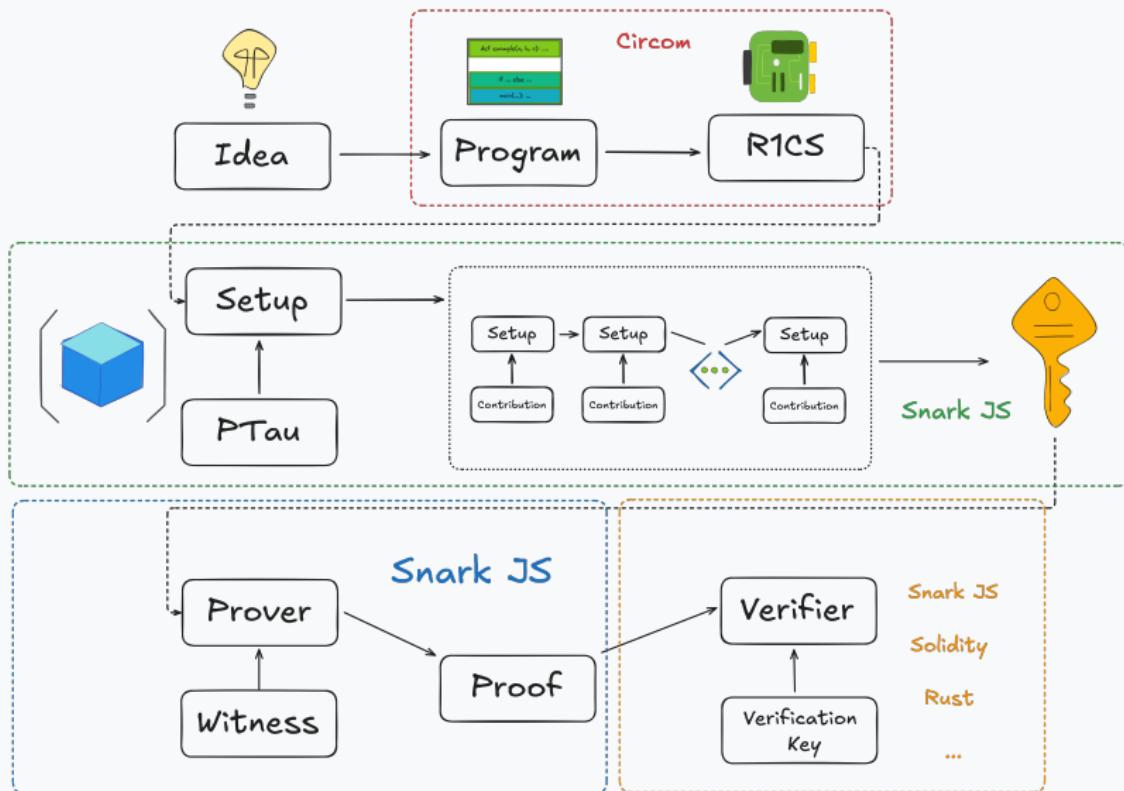
Toolchain



Toolchain



Toolchain



Introduction
○○○○

Circom
●○○

Practice
○○

Circom

It looks good, as long as all I need is to look at it.

Trusted Setup:

$\tau, \alpha, \beta_L, \beta_R, \beta_O, \gamma \xleftarrow{R} \mathbb{F}, \quad \{\{g^{\tau^i}, g^{\alpha\tau^i}\}_{i \in [d]}, \quad \{g^{\beta_L L_i(\tau)}, g^{\beta_R R_i(\tau)}, g^{\beta_O O_i(\tau)}\}_{i \in [n]}\},$
 $\{g^{Z(\tau)}, g^\alpha, g^{\beta_L}, g^{\beta_R}, g^{\beta_O}, g^{\beta_L \gamma}, g^{\beta_R \gamma}, g^{\beta_O \gamma}, g^\gamma\}, \quad \text{delete}(\tau, \alpha, \beta_L, \beta_R, \beta_O, \gamma).$

✓ $H(x) = \frac{L(x) \times R(x) - O(x)}{Z(x)}.$

✓ Sample $\delta_L, \delta_R, \delta_O \xleftarrow{R} \mathbb{F}$, compute:

$$\begin{aligned} \pi_L &\leftarrow g^{L(\tau)}(g^{Z(\tau)})^{\delta_L}, \pi'_L \leftarrow g^{\alpha L(\tau)}(g^{\alpha Z(\tau)})^{\delta_L}, \\ \pi_R &\leftarrow g^{R(\tau)}(g^{Z(\tau)})^{\delta_R}, \pi'_R \leftarrow g^{\alpha R(\tau)}(g^{\alpha Z(\tau)})^{\delta_R}, \\ \pi_O &\leftarrow g^{O(\tau)}(g^{Z(\tau)})^{\delta_O}, \pi'_O \leftarrow g^{\alpha O(\tau)}(g^{\alpha Z(\tau)})^{\delta_O}, \\ \pi_H &\leftarrow g^{H(\tau)}(g^{\delta_O})(g^{R(\tau)})^{\delta_L}(g^{L(\tau)})^{\delta_R}(g^{Z(\tau)})^{\delta_L \delta_R} \\ \pi_\beta &= \dots \end{aligned}$$

✓ $e(\pi_L, \pi_R) \stackrel{?}{=} e(\text{com}(Z), \pi_H) \cdot e(\pi_O, g).$

✓ Proof of Exponent:

$$\begin{aligned} e(\pi_L, g^\alpha) &= e(\pi'_L, g), \\ e(\pi_R, g^\alpha) &= e(\pi'_R, g), \\ e(\pi_O, g^\alpha) &= e(\pi'_O, g), \\ e(\pi_H, g^\alpha) &= e(\pi'_H, g). \end{aligned}$$

✓ $e(\pi_L, g^{\gamma \beta_L}) \cdot e(\pi_R, g^{\gamma \beta_R}) \cdot e(\pi_O, g^{\gamma \beta_O}) = e(\pi_\beta, g^\gamma)$



Prover \mathcal{P}

$$\pi = (\pi_L, \pi_R, \pi_O, \pi_H, \pi'_L, \pi'_R, \pi'_O, \pi'_H, \pi_\beta)$$



Verifier \mathcal{V}

Something we can touch.

```
pragma circom 2.1.6;

template Math() {
    signal output res;

    signal input a;
    signal input b;
    signal input c;

    signal mul1 <== a * b;
    signal mul2 <== a * c;
    signal res1 <== mul1 * mul2;

    signal add1 <== (1 - a) * b;
    signal add2 <== (1 - a) * c;
    signal res2 <== add1 + add2;

    res1 + res2 ==> res;
}
```

Introduction
○○○○

Circom
○○○

Practice
●○

Practice

Thank you for your attention



 zkdl-camp.github.io
 github.com/ZKDL-Camp

