Circom

November 28, 2024

Distributed Lab

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

Plan

Introduction

Why do we need ZK?

Why do we need ZK?

Option

Solution to privacy

Why do we need ZK?

Option

Solution to privacy

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*

Why do we need ZK?

Option

Solution to privacy

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*

Option

Solution to scalability

Why do we need ZK?

Option

Solution to privacy

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*

Option

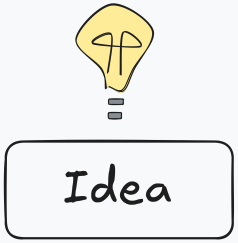
Solution to scalability

Example

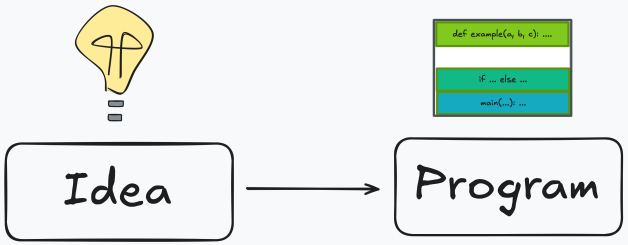
This is the hash of a blockchain block that does not produce negative balances

Using ZKP

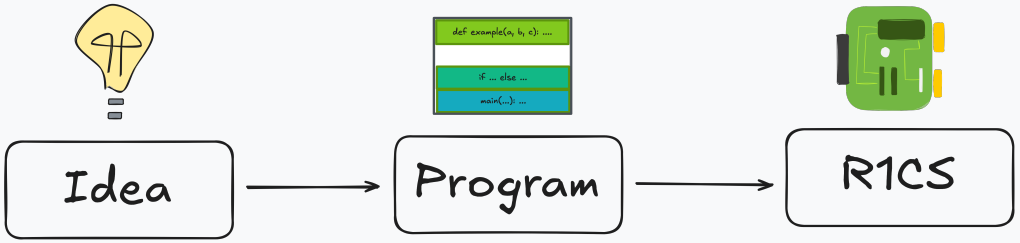
Using ZKP



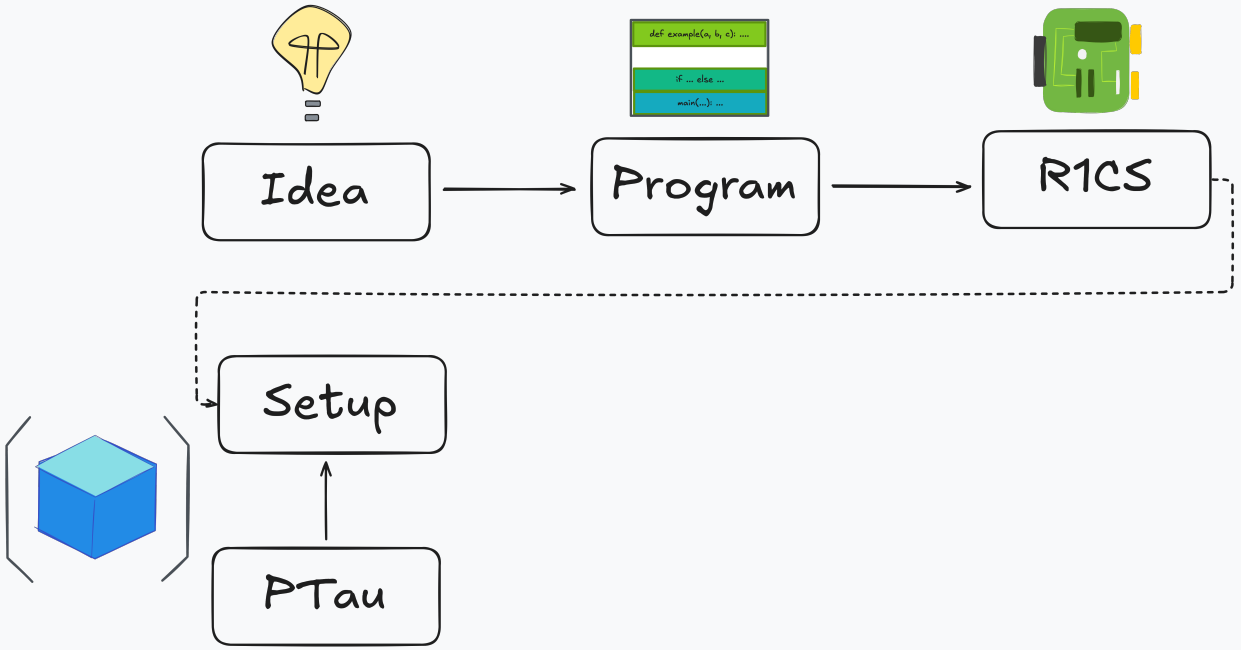
Using ZKP



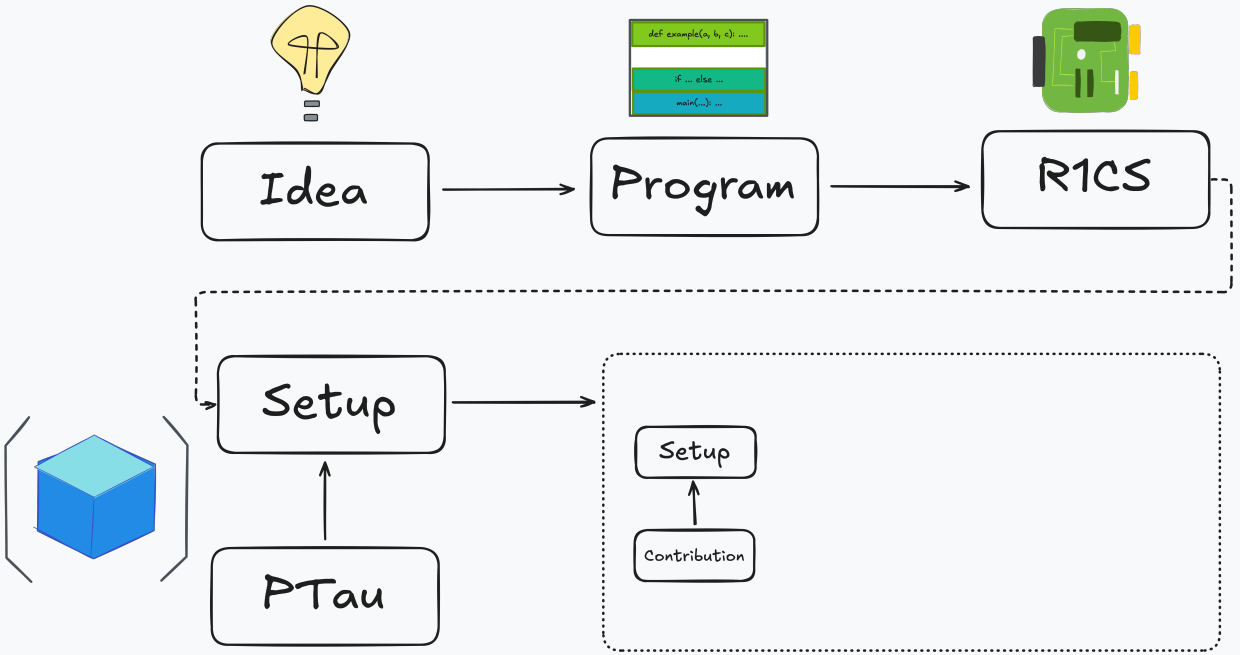
Using ZKP



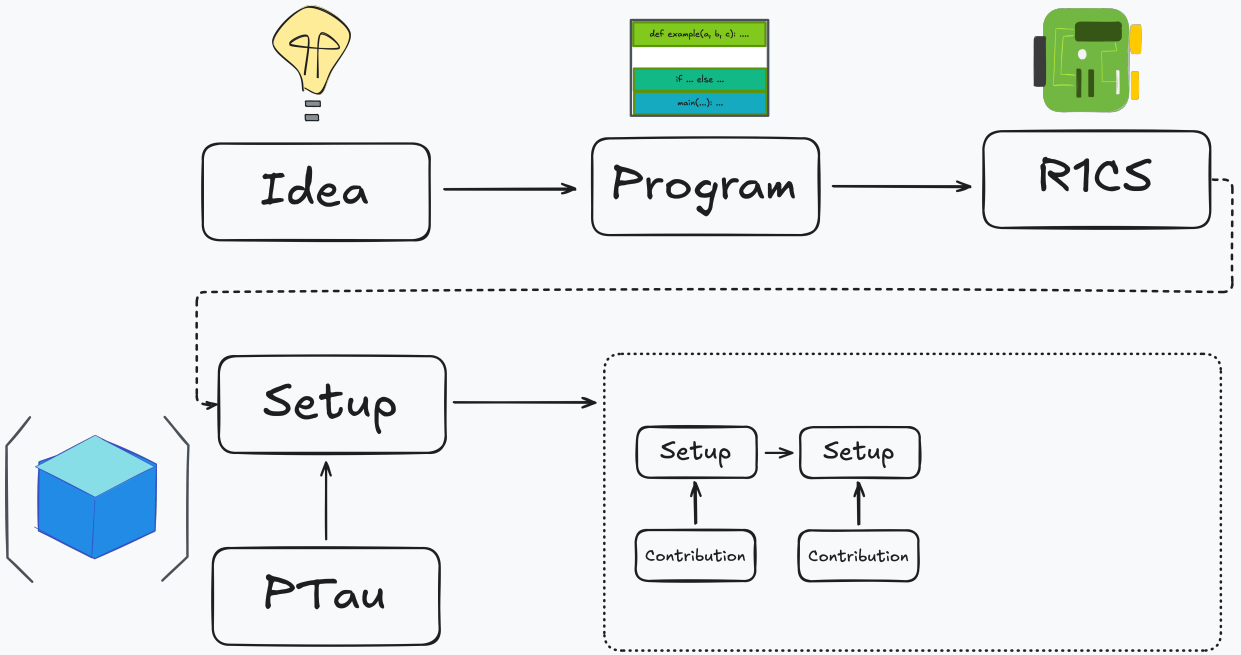
Using ZKP



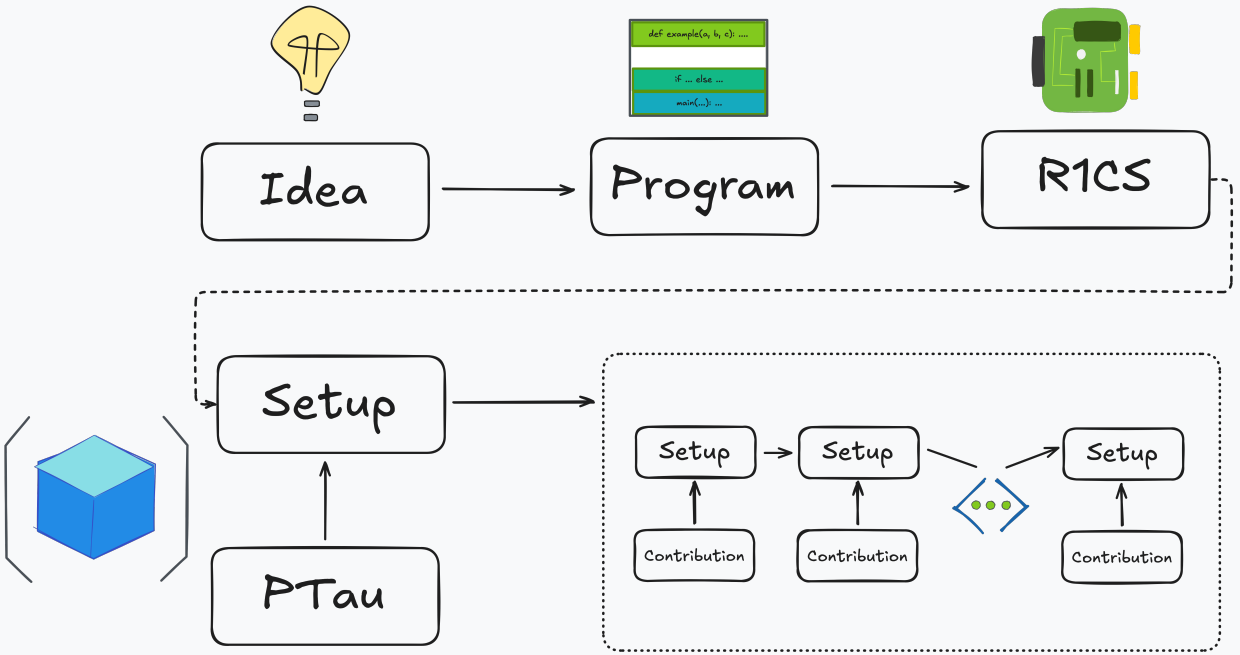
Using ZKP



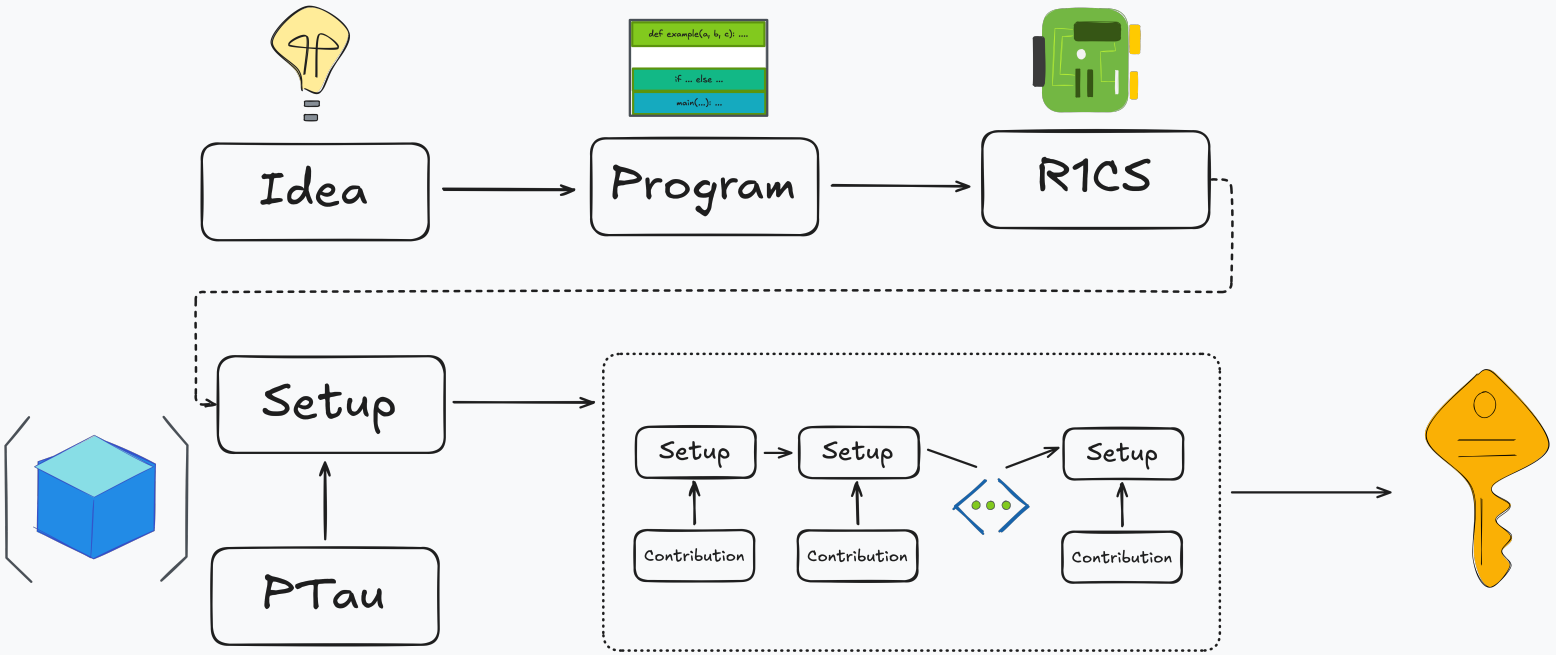
Using ZKP


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Contribution
Contribution

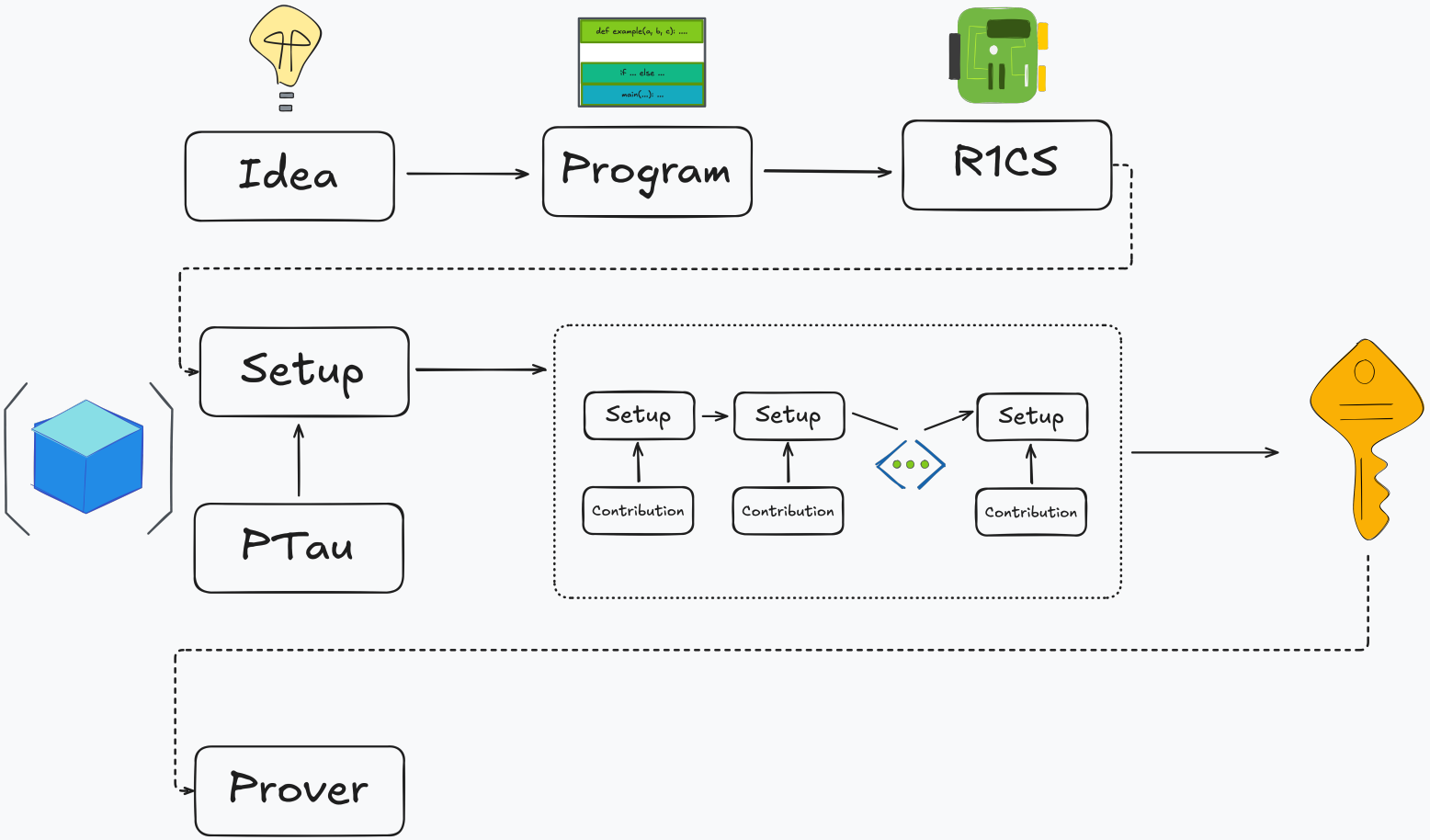
Using ZKP


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution

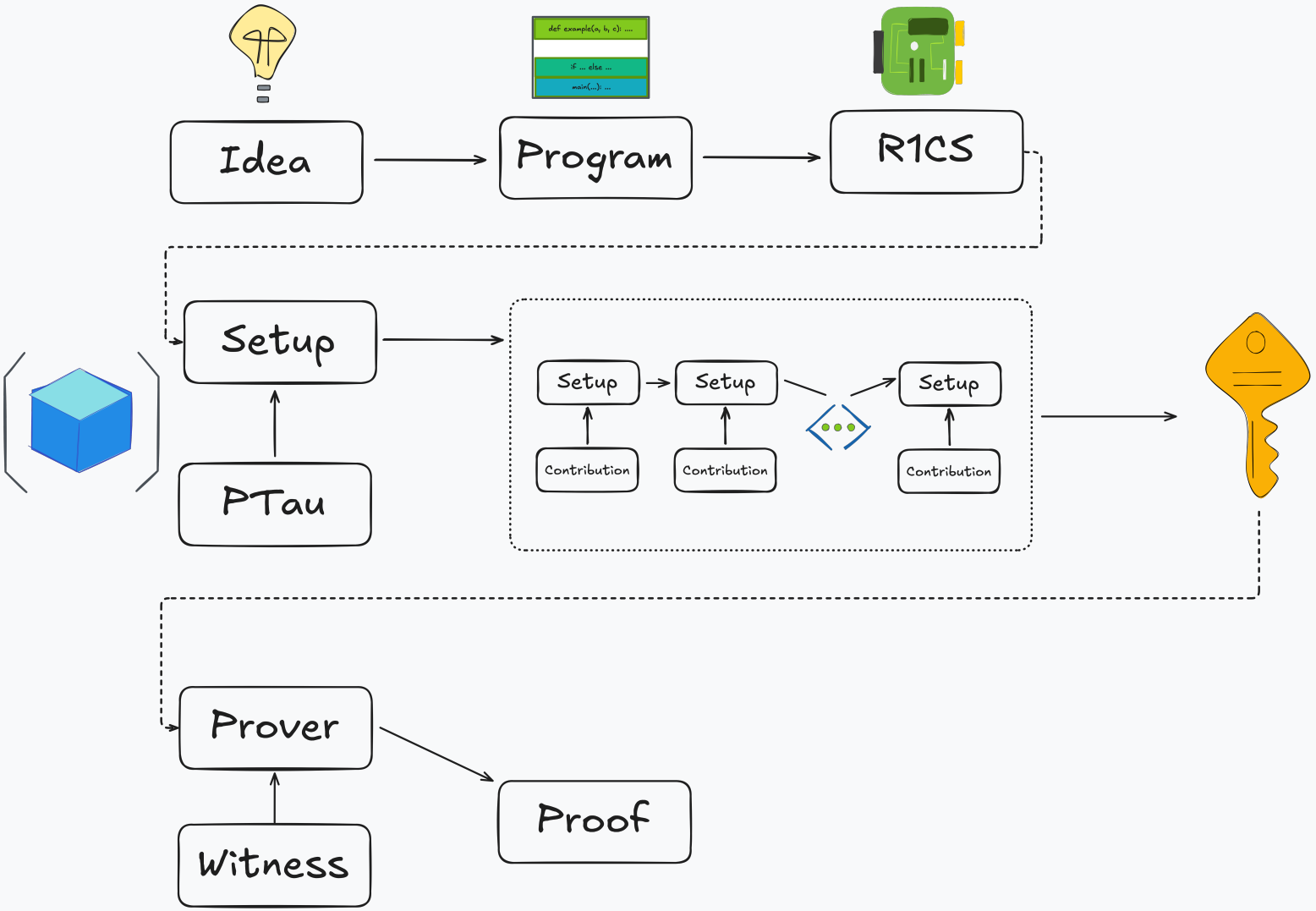
Using ZKP


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution

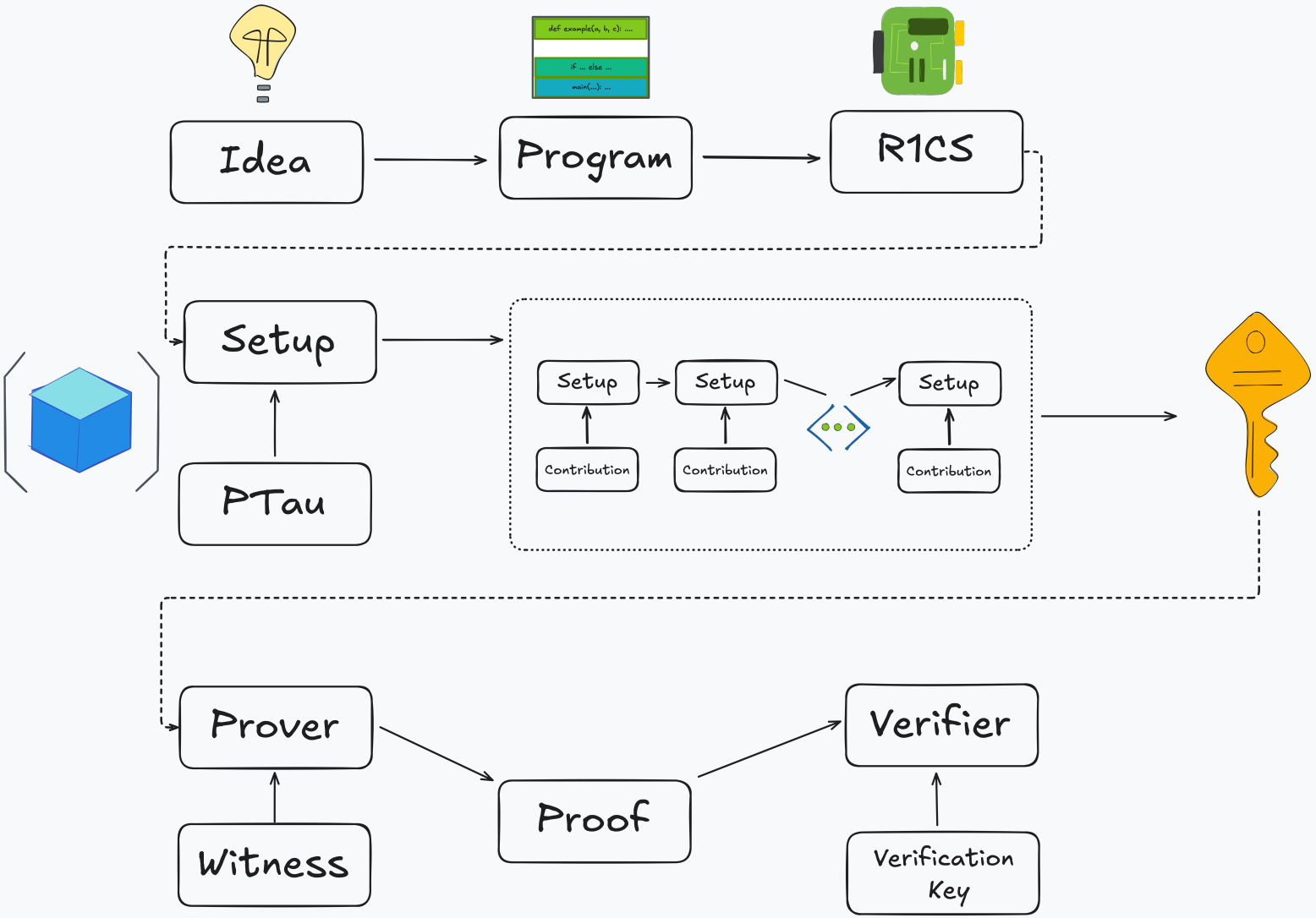
Using ZKP


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Prover

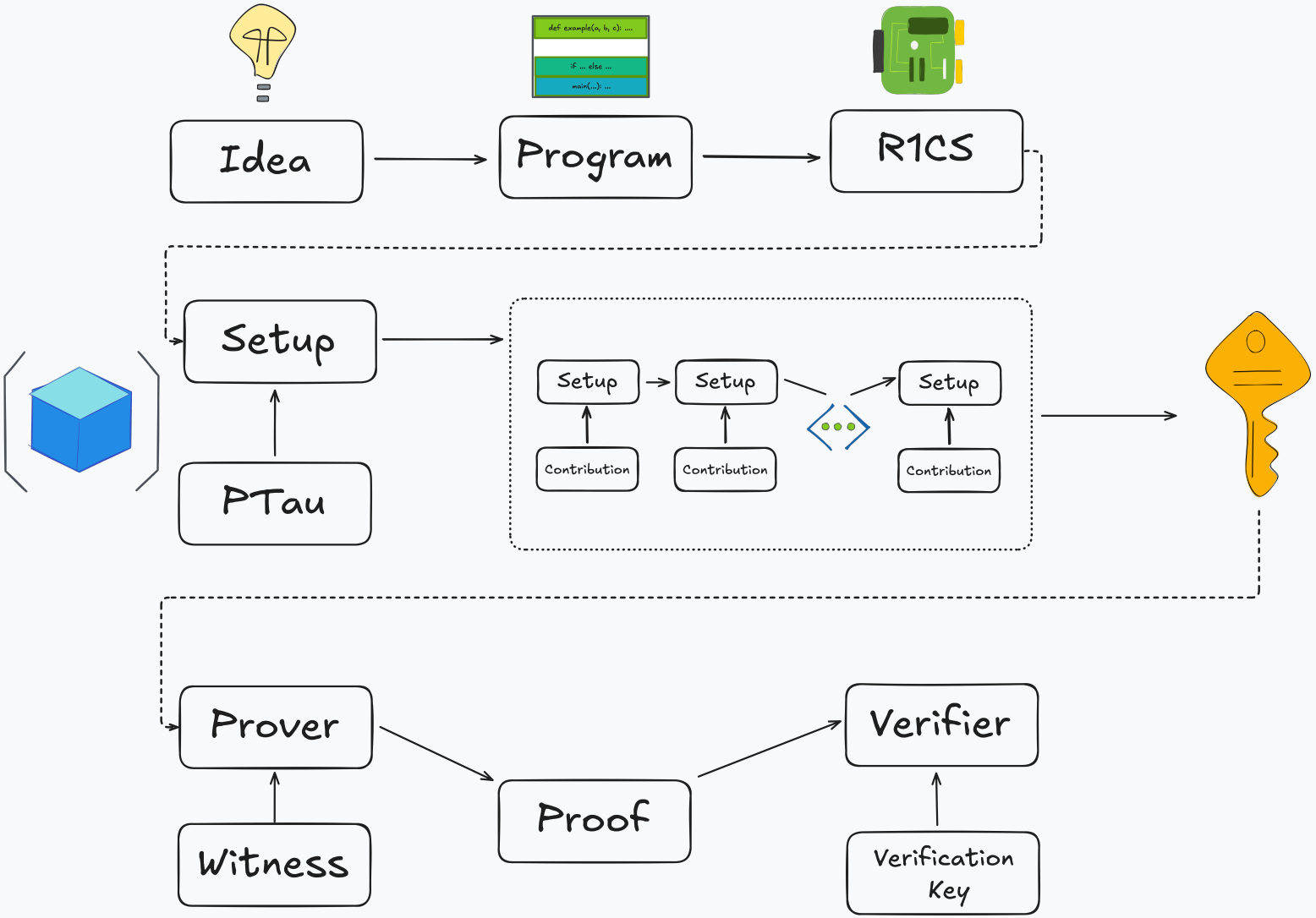
Using ZKP


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Prover
Witness
Proof

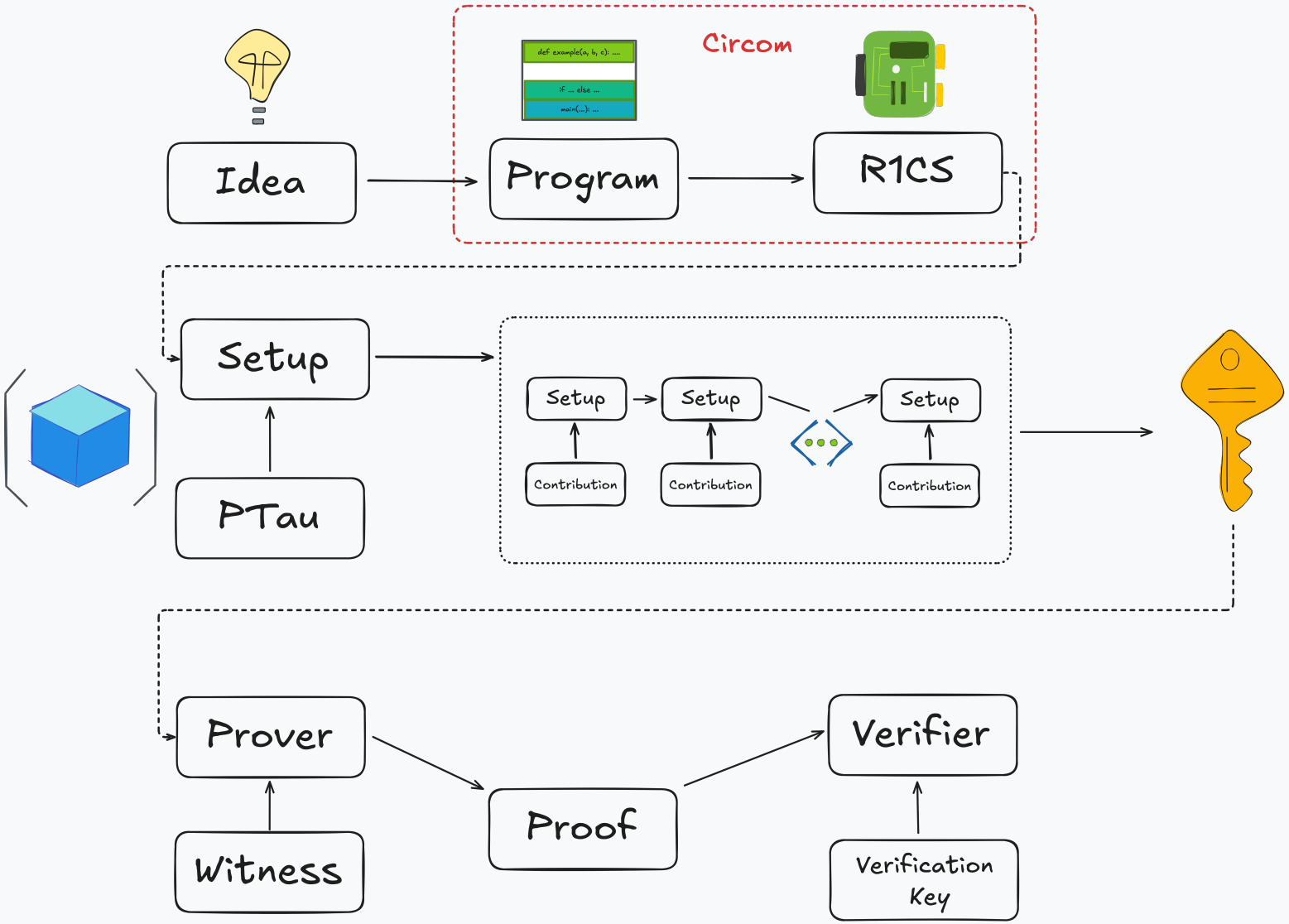
Using ZKP


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Prover
Witness
Proof
Verifier
Verification Key

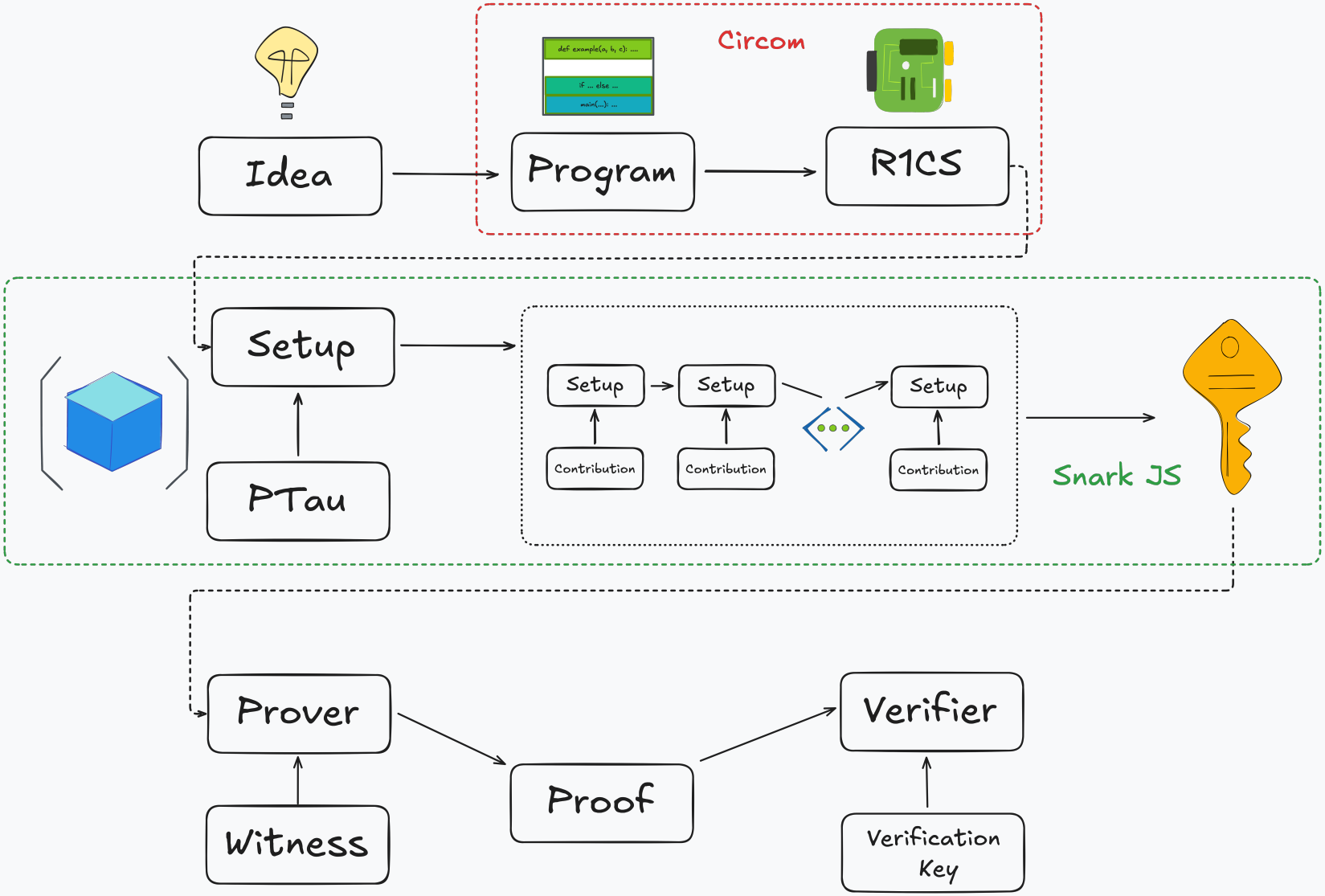
Toolchain


Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Prover
Witness
Proof
Verifier
Verification Key

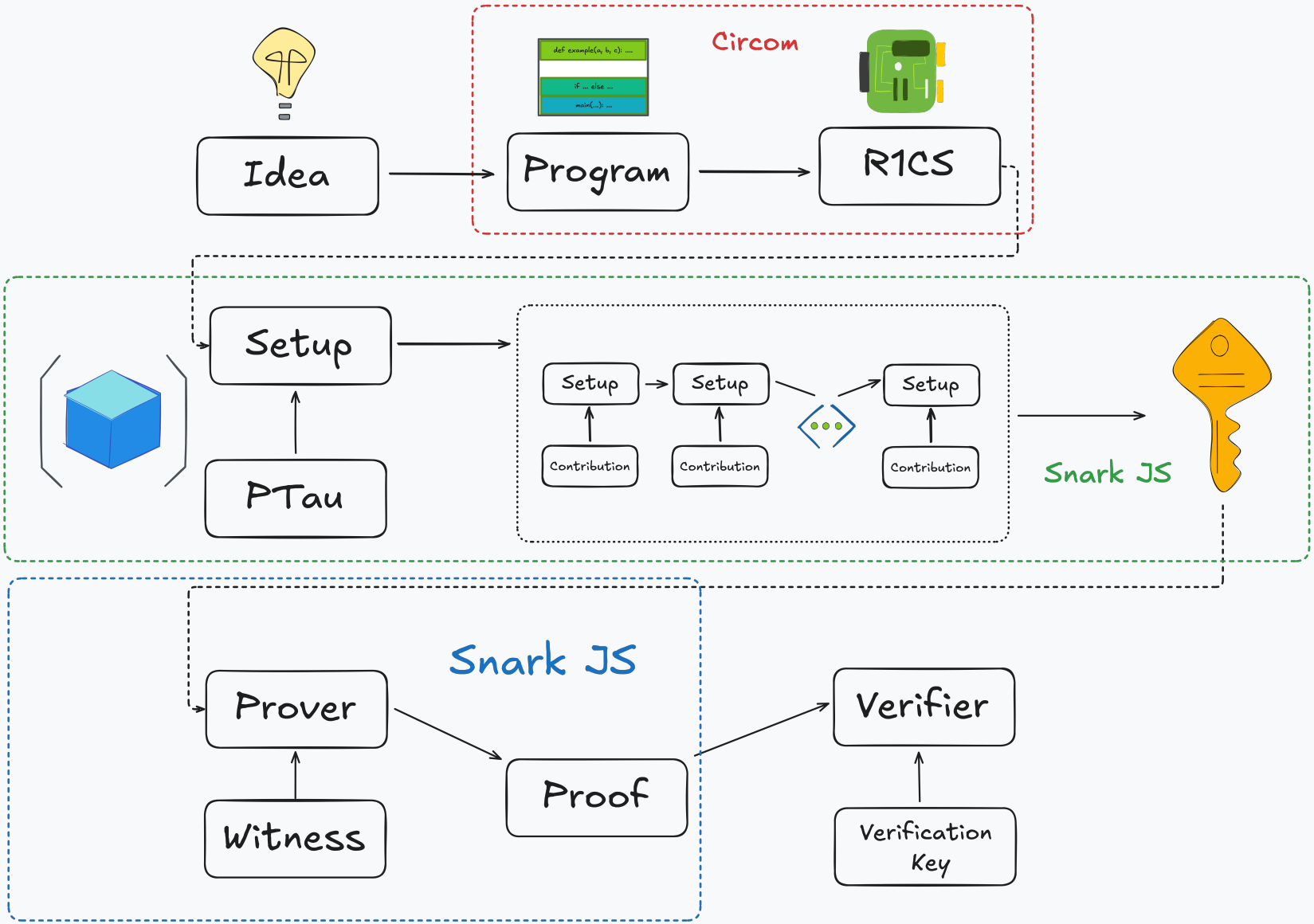
Toolchain


Circom
Idea
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Prover
Witness
Proof
Verifier
Verification Key

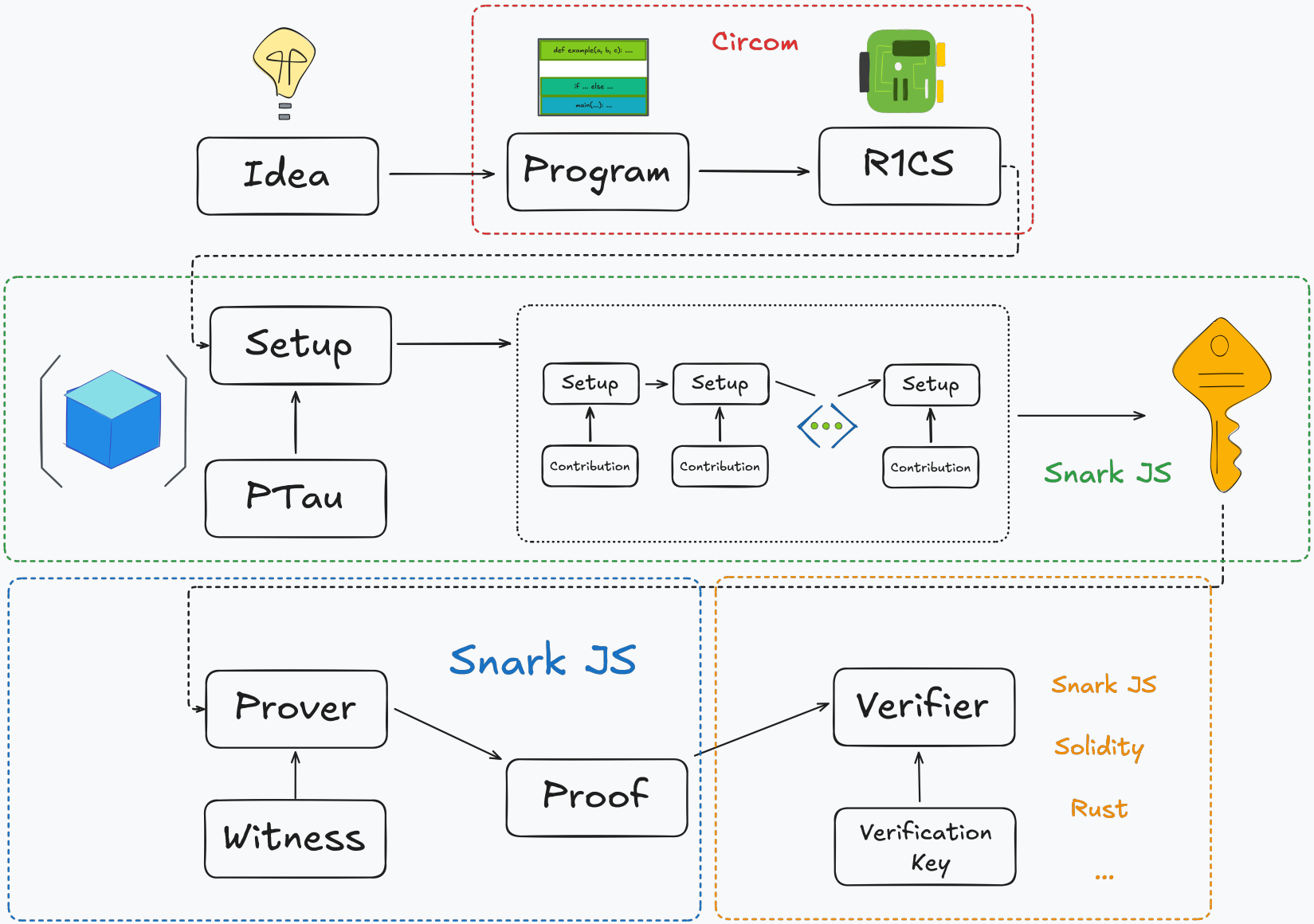
Toolchain


Idea
Program
Circom
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Snark JS
Prover
Witness
Proof
Verifier
Verification Key

Toolchain


Idea
Circom
def example(a, b, c): ....
if ... else ...
main(...): ...
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Snark JS
Snark JS
Prover
Witness
Proof
Verifier
Verification Key

Toolchain


Idea
Circom
Program
R1CS
Setup
PTau
Setup
Setup
Setup
Contribution
Contribution
Contribution
Snark JS
Snark JS
Prover
Witness
Proof
Verifier
Verification Key
Snark JS
Solidity
Rust
...

Circom

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

Trusted Setup:

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

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

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

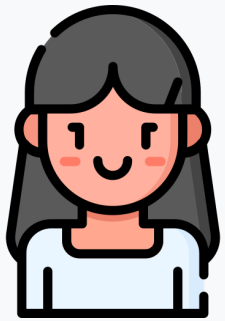
✓ Proof of Exponent:

$$e(\pi_L, g^\alpha) = e(\pi'_L, g),$$
$$e(\pi_R, g^\alpha) = e(\pi'_R, g),$$
$$e(\pi_O, g^\alpha) = e(\pi'_O, g),$$
$$e(\pi_H, g^\alpha) = e(\pi'_H, g).$$

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

Prover $\mathcal{P}$

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



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;

    a * (1 - a) === 0;

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

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

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

Practice

Thank you for your attention

zkdl-camp.github.io

github.com/ZKDL-Camp