How to do *something* to *some* state in *some* contract

"oh look! something happened!"

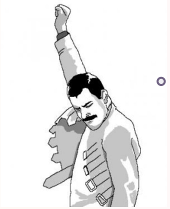
José Pedro Sousa | zpedro.eth
DevRel Engineer

Aztec Labs

Is this the real life?

Is this just fantasy?

MAMAAAA



OK, that's enough

YOU CAN'T REPRESENT THE REAL LIFE IN A GLOBAL LEDGER BECAUSE REAL LIFE CAUSALITY IS PRIVATE
SURE ZÉ PEDRO LETS GET YOU TO BED
imgflip.com

Microsoft®
Windows® xp ™

How to represent the *real life*

Using the world's most expensive clock

José Pedro Sousa | zpedro.eth
DevRel Engineer

Aztec Labs

Agenda

(look ma, I even have an **agenda!**)

01 The secret to success

02 Who are you

03 The world's most expensive timestamp machine

04 How to keep your secrets but shout them out loud

Aztec Labs

The secret to

Success and Happiness

I know the secret to your success and happiness.

I will give it to you for free, anon.

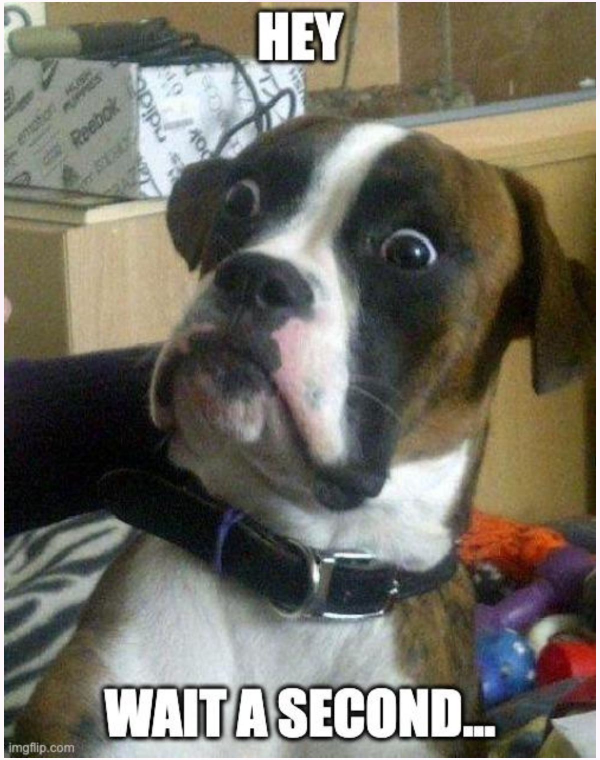
Because I like you ❤

Two simple steps

01

Trojan yourself

Track every interaction between citizens by bringing all the real-world data into an immutable, undeniable, public ledger.



Two simple steps

01

Trojan yourself

Track every interaction between citizens by bringing all the real-world data into an immutable, undeniable, public ledger.

02

Become a dictator

Two simple steps

02

Become a dictator

Be happy and successful.

Rule as you wish, terrorize people, and make your opponents have an irresistible urge to fall out of windows 👌

Aztec Labs

So if you don’t want to **be a dictator**...

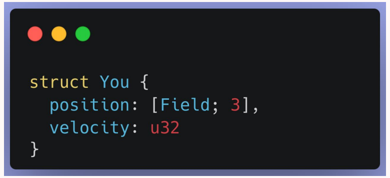
Who are you?

I asked world-class scientists* about that.

Physicists said:

You have a deterministic position and velocity.

If we agree on a common time, this information can be private and **I can still see you.**

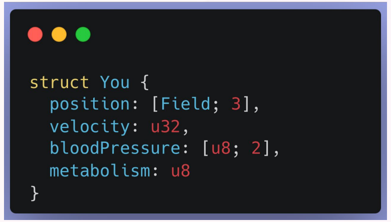


```
struct You {
  position: [Field; 3],
  velocity: u32
}
```

Biologists said:

Your blood pressure is 120/80. You’re burning 1.2kcal per minute.

If we agree on a common time, this information can be private and **I can see you are alive.**

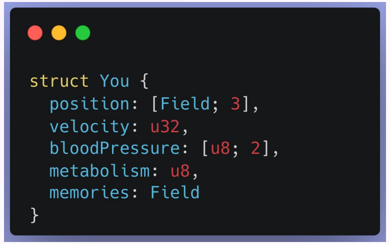


```
struct You {
  position: [Field; 3],
  velocity: u32,
  bloodPressure: [u8; 2],
  metabolism: u8
}
```

Psychologists said:

Your brain holds a ton of memories and knowledge.

If we agree on a common time, this information can be private and **I can see how your social presence affects our environment.**



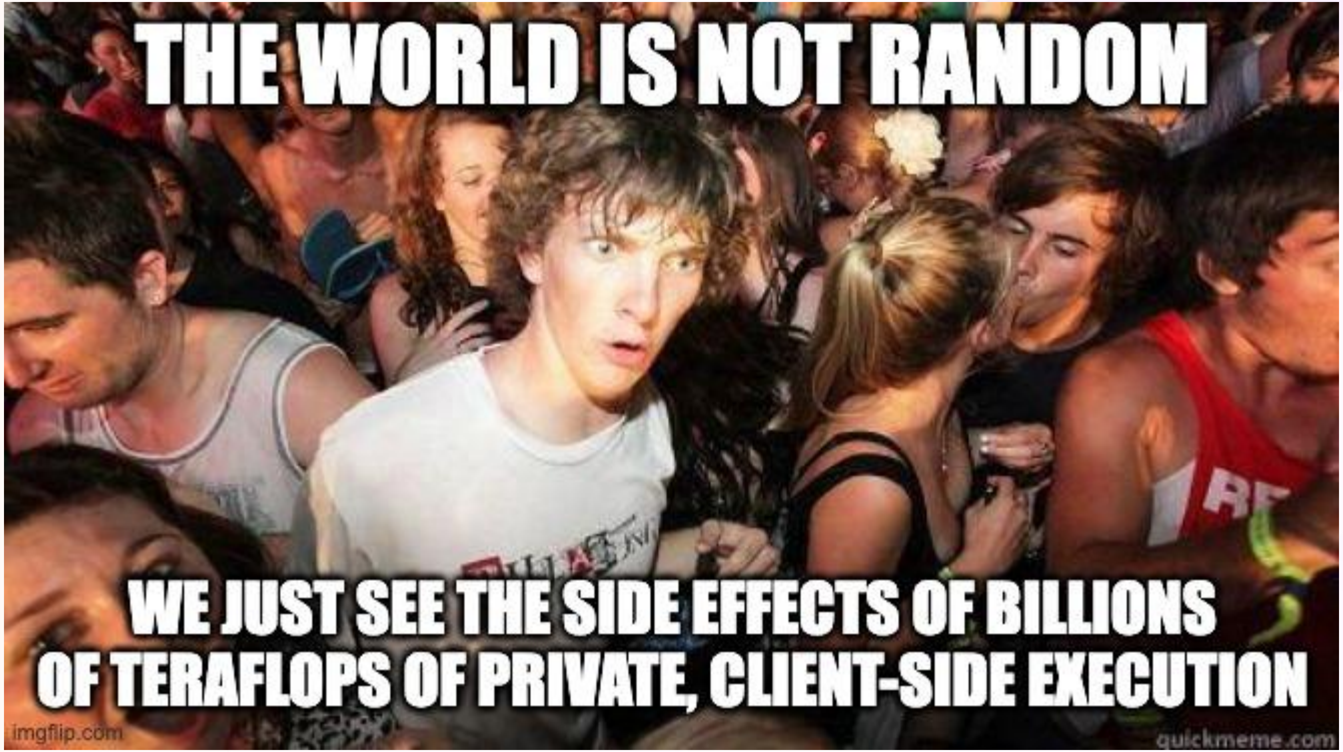
```
struct You {
  position: [Field; 3],
  velocity: u32,
  bloodPressure: [u8; 2],
  metabolism: u8,
  memories: Field
}
```

You say:

What the hell does this have to do with Aztec?

Because so far, all blockchains imply full knowledge of causality. **Everyone knows everything and agrees on the same state.**

* my dad, my sister, and me 👌


THE WORLD IS NOT RANDOM
WE JUST SEE THE SIDE EFFECTS OF BILLIONS OF TERAFLOPS OF PRIVATE, CLIENT-SIDE EXECUTION
imgflip.com
quickmeme.com

In a nutshell

Aztec Labs

Ooooh ok... so privacy is quite the big deal, isn’t it?

It is also a human right, dummy!

No one shall be subjected to arbitrary interference with his ***privacy****, family, home or* ***correspondence*** *[...]*

Article 12 of the Universal Declaration of The Human Rights

You cannot

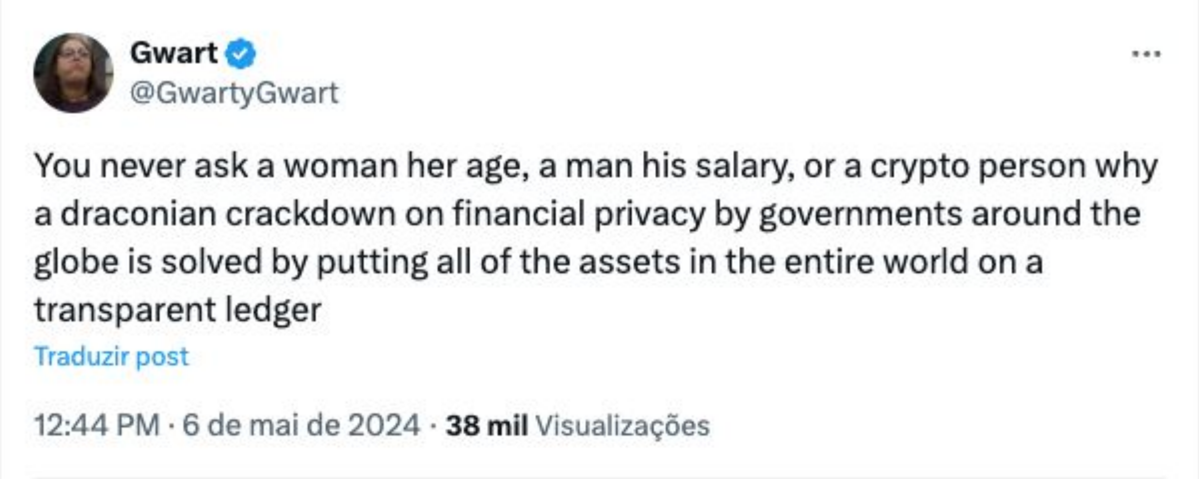
- Ignore privacy
- Ask someone to keep it
    - Pinky promises don’t work either
    - (nor GDPR)

You cannot

- Ignore privacy
- Ask someone to keep it
    - Pinky promises don’t work either
    - (nor GDPR)
- Trust that your password won’t be logged on some non-sanitized AWS lambda output because that junior dev just joined and he’s not used to this, we will make sure this won’t ever happen again, now please understand we’re the victims here from a very sophisticated attack involving the said junior dev writing a script to auto accept 2FA authentications because he was bored now please just change your password, but let me just `ufw allow all` because all that tunneling thing is too complicated for me but im...

I'VE FINALLY FOUND IT... AFTER 15 YEARS
THE SCROLL OF TRUTH!
Robotatertotcomics
blockchain without privacy is an orwellian nightmare
NYEHHH
WEB3
imgflip.com

Aztec Labs



Gwart
@GwartyGwart

You never ask a woman her age, a man his salary, or a crypto person why a draconian crackdown on financial privacy by governments around the globe is solved by putting all of the assets in the entire world on a transparent ledger

12:44 PM · 6 de mai de 2024 · **38 mil** Visualizações

TL;DR

We are encoded with our secrets IRL

Eg. I hate broccoli 🥦 I can add that *private input* to my Aztec representation.

We need to advance state by shouting

Eg. If we go to a restaurant, the fact that i hate brocolli *will influence my decision*, and has a verifiable side-effect (maybe you would follow the suggestion and choose broccoli too!)

Ta-da! I just shouted a new state without revealing my private inputs. No leaking.

Aztec Labs

Please shut up

Let’s do something

Agenda

(just pretending this is a respectable workshop)

01 Boot up the world's most expensive clock

02 Write programmable privacy

03 Run it 😈

Agenda

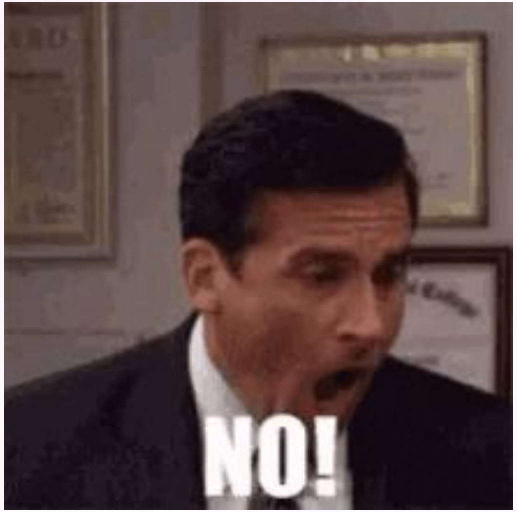
(just pretending this is a respectable workshop)

Agenda

(ok here's the actual plan)

01 Set up a development environment

02 Generating useful TS bindings



Agenda

(ok here's the actual plan)

01 Set up a development environment

02 Deploying with the glorious CLI wallet

Agenda

(ok here's the actual plan)

01 Set up a development environment

02 Deploying with the glorious CLI wallet

03 Can't run away from TS bindings (you can leave now, no questions asked)

Agenda

(ok here’s the actual plan)

01 Set up a development environment

02 Deploying with the glorious CLI wallet

03 Can’t run away from TS bindings (you can leave now, no questions asked)

04 Writing our deployer

05 Writing a contract

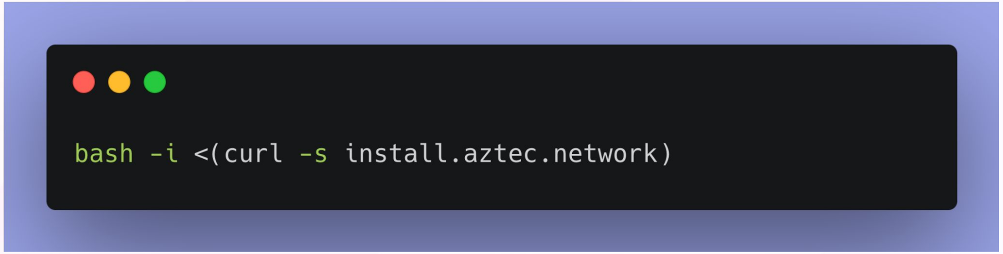
06 Bonus points for testing

Aztec Labs

Step 1. How to...

Run the clock

Run this. Done.



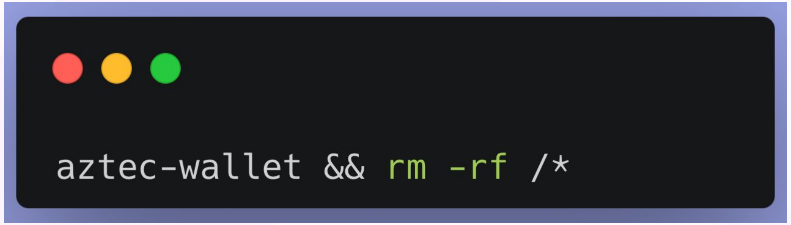
```
bash -i <(curl -s install.aztec.network)
```

Aztec Labs

Step 2. How to...

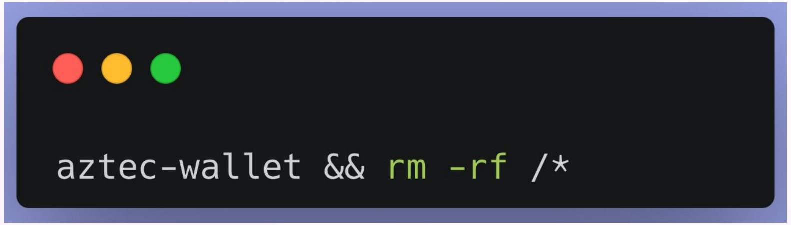
Use the CLI wallet

Run this. Done.



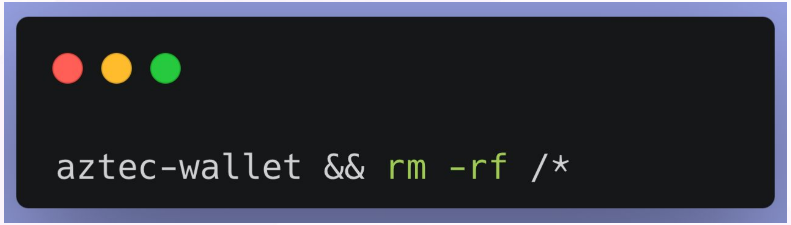
```
aztec-wallet && rm -rf /*
```

~~Run this. Done.~~



```
aztec-wallet && rm -rf /*
```

Don’t run this.
Or you’re Done.



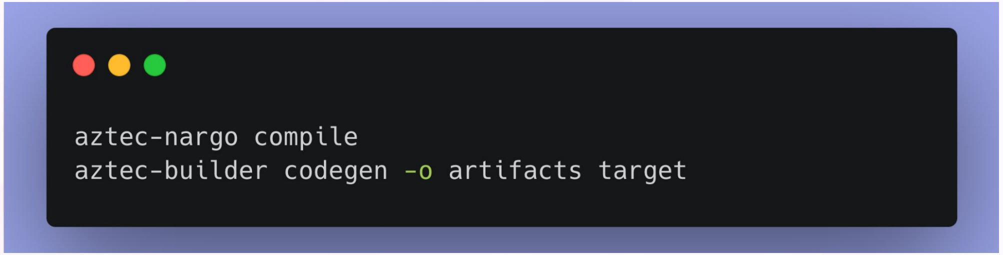
```
aztec-wallet && rm -rf /*
```

Aztec Labs

Step 3. I smell Javascript in the horizon...

RUN NOW

See, not so bad.



```
aztec-nargo compile
aztec-builder codegen -o artifacts target
```

Aztec Labs

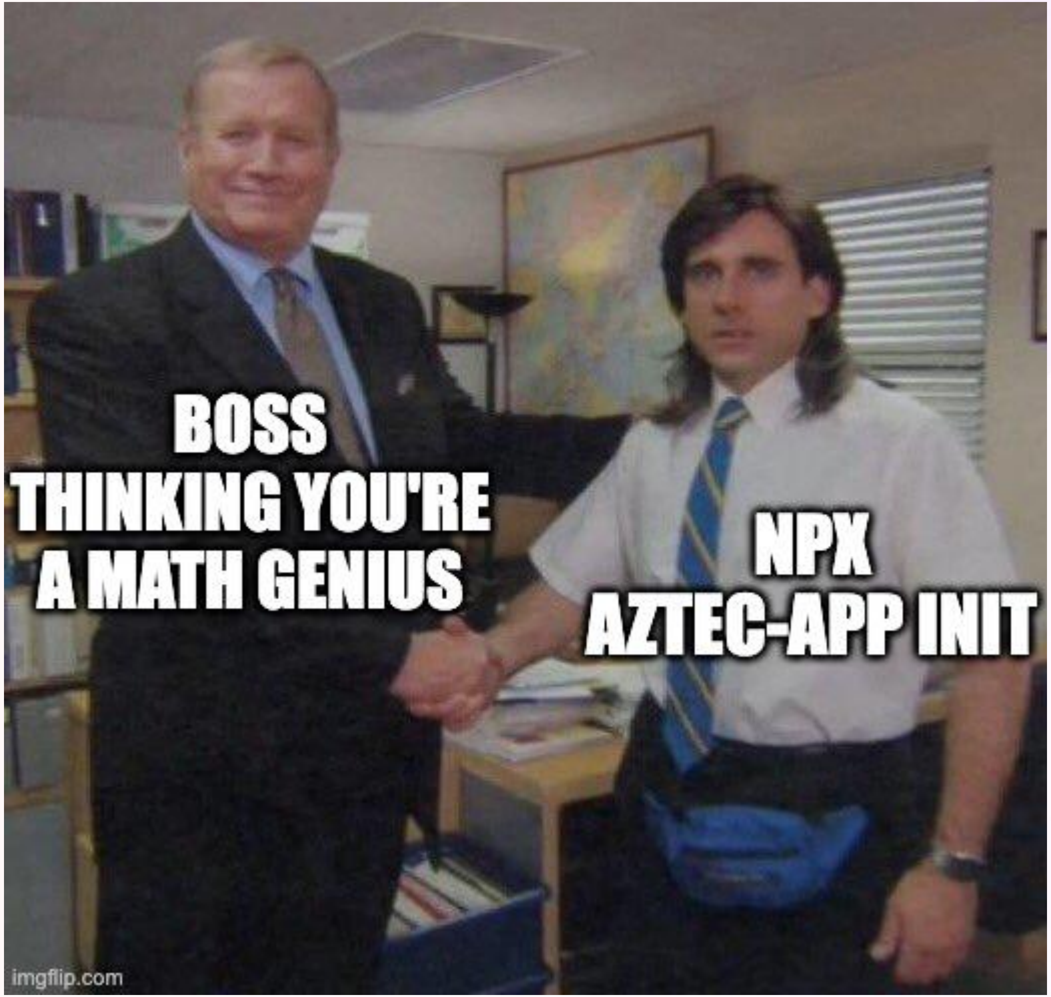
Step 4. How to write a deployer... In Typescript 🫠

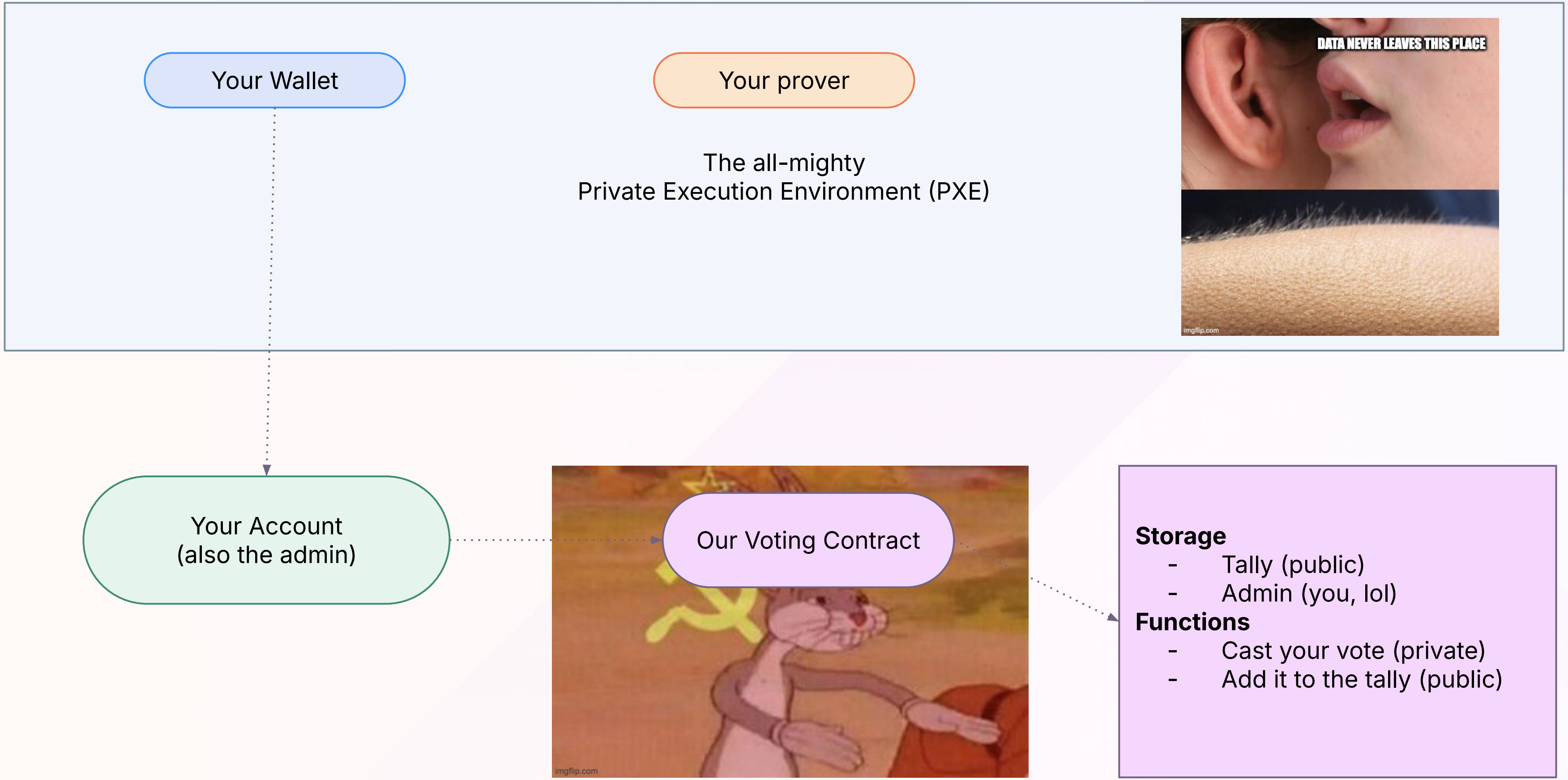
Please stay. Please.

Aztec Labs

Step 5. How to...

Write a contract 😈


BOSS THINKING YOU'RE A MATH GENIUS
NPX AZTEC-APP INIT
imgflip.com



Your Wallet

Your prover

The all-mighty
Private Execution Environment (PXE)

Your Account
(also the admin)

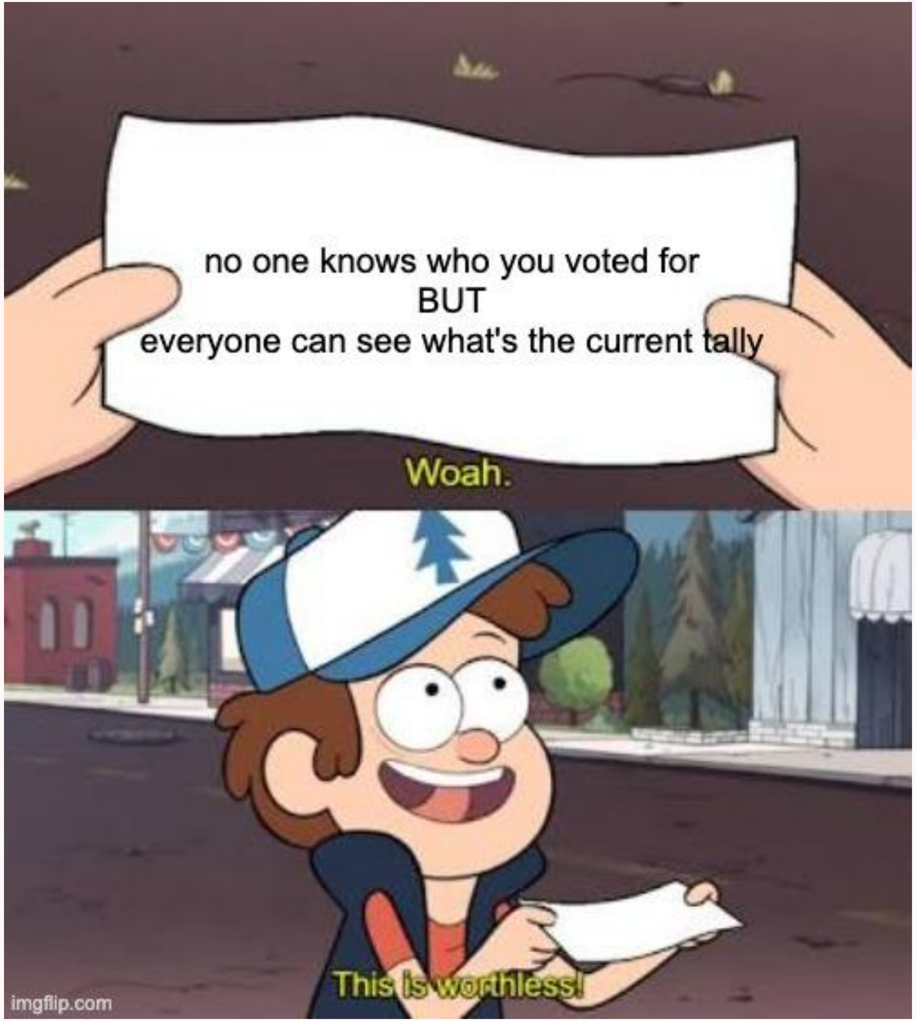
Our Voting Contract

Storage

- Tally (public)
- Admin (you, lol)

Functions

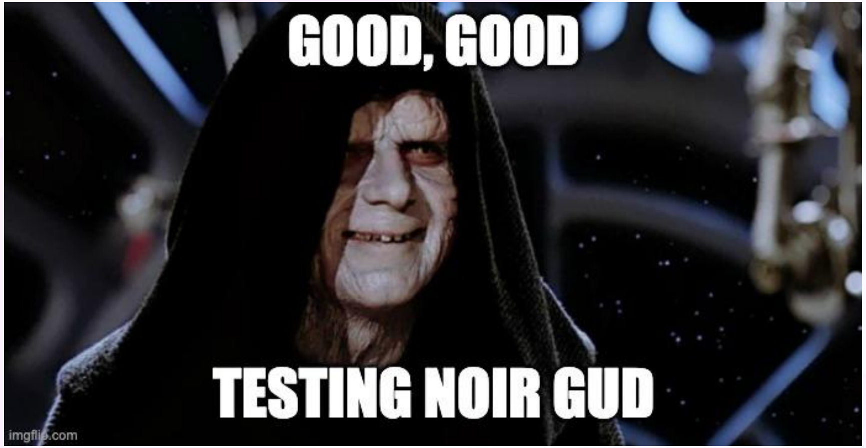
- Cast your vote (private)
- Add it to the tally (public)


no one knows who you voted for
BUT
everyone can see what's the current tally
Woah.
This is worthless!
imgflip.com

Aztec Labs

Step 6 if there's enough time. How to...

Test and see it's not dark magic



Then, the good stuff...

ACCOUNT ABSTRACTION
i sleep
NATIVE ACCOUNT ABSTRACTION
real shit
PRIVATE NATIVE ACCOUNT ABSTRACTION
Ascended
imgflip.com

Ok that’s good.
That’s… very good. But maybe
another day

Enough memes, let’s hack.

And remember 5h debugging can save you 5min reading docs

Some links

José Pedro Sousa | zpedro.eth

DevRel Engineer @ Aztec Labs

Aztec Discord

docs.aztec.network

linktr.ee/zpedro.eth

Workshop Resources