FORMAL LAND

OUR WORK FOR MORE SECURITY ON SMART CONTRACTS

JULY 2024

contact@formal.land

ISSUE

Program testing can be used to show the **presence** of bugs, but never to show their **absence**!

— Edsger W. Dijkstra

contact@formal.land

COST

Hundreds of millions of dollars are **stolen** every year from smart contract bugs

Risk for the **credibility** of the Web3

contact@formal.land

OUR SOLUTION

What we are developing!

We are currently funded by the Aleph Zero blockchain, who we thank for that.

contact@formal.land

1 FORMAL VERIFICATION

Show the absence of bugs/attacks

- **Mathematical** analysis of the code
- Using **interactive** theorem provers (Coq, ...)
- To verify **any security properties**

contact@formal.land

2 WORKFLOW

1. **Translate** the code to a proof system
2. Write **specifications** (no assets creation, ...)
3. **Prove** that the specifications are always true
4. Code generation/AI crucial for **automation**

contact@formal.land

3 MAINTENANCE

1. Prove the **synchronization** with the source
2. Only verify the **updated code**
3. **Gain time** compared to manual audits

Simple changes should be simple to verify!

contact@formal.land

4 UPCOMING DEVELOPMENTS

- **General primitives** to specify smart contracts
- Definition of account, identity, rounding, ...
- Handle the **most common** use cases

contact@formal.land

LINK

- https://github.com/formal-land/solidity
- Open-source, ready-to-use
- Contact us for more!
- We provide formal verification as a service

contact@formal.land

BUSINESS MODEL

- **Predictable price** on the number of lines
- **Full refund** on medium/high/critical bug

contact@formal.land

BUSINESS MODEL

An audit should be viewed as a **loan** to a security company, **reimbursed at the next bug.**

contact@formal.land

THANKS!

contact@formal.land