FORMAL LAND

FORMAL VERIFICATION OF RUST FOR THE EVM

SEPTEMBER 2024

TUM BLOCKCHAIN CONFERENCE

TABLE OF CONTENT

FORMAL LAND

WHAT IS FORMAL VERIFICATION?

Make sure a code has **no bugs** by making mathematical proofs on the code.

FORMAL LAND

POSSIBLE

- Reasoning by cases: **if**
- By induction: **for** loops
- By parts: **functions**

FORMAL LAND

EXAMPLES

- **Certora**: smart contracts
- **Coq**/**Lean**: general purposes
- **Z3**: automated

FORMAL LAND

EVM

- ***E**thereum **V**irtual **M**achine*
- **Go** Ethereum
- **Python** specification
- **Rust** revm for L2s

FORMAL LAND

RISKS

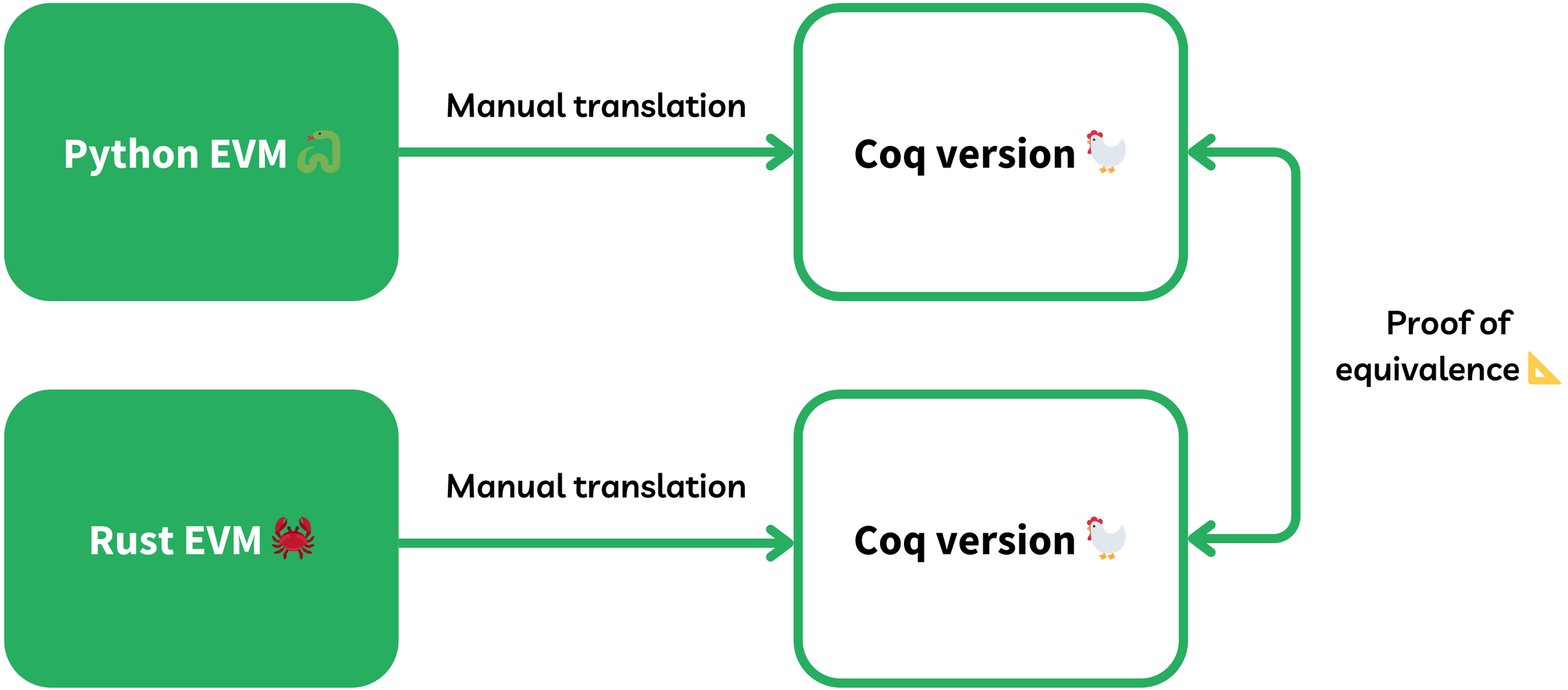
- Different behaviors
- => smart contract **attacks**
- => **fork** of the chain

FORMAL LAND

HOW WE DO

- Prove the equivalence Rust/Python EVM
- https://github.com/ethereum/execution-specs
- https://github.com/bluealloy/revm

FORMAL LAND


Python EVM
Manual translation
Coq version
Proof of equivalence
Rust EVM
Manual translation
Coq version

FORMAL LAND

PYTHON

```python
def div(evm: Evm) -> None:
    """
    Integer division of the top two elements of the stack. Pushes the result
    back on the stack.

    Parameters
    ----------
    evm :
        The current EVM frame.

    """
    # STACK
    dividend = pop(evm.stack)
    divisor = pop(evm.stack)

    # GAS
    charge_gas(evm, GAS_LOW)

    # OPERATION
    if divisor == 0:
        quotient = U256(0)
    else:
        quotient = dividend // divisor

    push(evm.stack, quotient)

    # PROGRAM COUNTER
    evm.pc += 1
```

COQ

```coq
Definition div : MS? Evm.t Exception.t unit :=
  (* STACK *)
  letS? divident := StateError.lift_lens Evm.Lens.stack pop in
  letS? divisor := StateError.lift_lens Evm.Lens.stack pop in

  (* GAS *)
  letS? _ := charge_gas GAS_LOW in

  (* OPERATION *)

  let division :=
    match (U256.to_Z divident) with
    | 0 =>
      U256.of_Z 0
    | _ =>
      U256.of_Z ((U256.to_Z divisor) / (U256.to_Z divident))
  end in

  let result := division in

  letS? _ := StateError.lift_lens Evm.Lens.stack (push result) in

  (* PROGRAM COUNTER *)
  letS? _ := StateError.lift_lens Evm.Lens.pc (fun pc =>
    (inl tt, Uint.__add__ pc (Uint.Make 1))) in

  returnS? tt.
```

FORMAL LAND

RUST

```rust
pub fn div<H: Host + ?Sized>(
    interpreter: &mut Interpreter
    _host: &mut H
) {
    gas!(interpreter, gas::LOW);
    pop_top!(interpreter, op1, op2);
    if *op2 != U256::ZERO {
        *op2 = op1.wrapping_div(*op2);
    }
}
```

COQ

```
Definition div :
    MS? Interpreter.t string unit :=
  letS? _ := gas_macro Gas.LOW in
  letS? '(op1, op2_ref) := pop_top_macro2 in
  liftS? Interpreter.Lens.stack (
    liftS?of!? op2_ref (
      letS? op2 := readS? in
      if U256.eq op2 U256.ZERO
      then returnS? tt
      else writeS? (U256.wrapping_div op1 op2)
    )
  ).
```

FORMAL LAND

ISSUE

- The code is **similar**
- But we can make **mistakes**
- Hard to follow **upgrades**

COQ-OF-RUST

- Tool to import **Rust code to Coq**
- Automatic
- https://github.com/formal-land/coq-of-rust

FORMAL LAND

HOW

- Representation of all the Rust syntax
- Connected to the Rust compiler

OUTPUT

- Very low-level
- Very verbose

EXAMPLE

```
Definition div (ε : list Value.t) (τ : list Ty.t) (α : list Value.t) : M :=
  match ε, τ, α with
  | [], [ H ], [ interpreter; _host ] ⇒
    ltac:(M.monadic
      (let interpreter := M.alloc (| interpreter |) in
      let _host := M.alloc (| _host |) in
      M.catch_return (|
        ltac:(M.monadic
          (M.read (|
            let~ _ :=
              M.match_operator (|
                M.alloc (| Value.Tuple [] |),
                [
                  fun γ ⇒
                    ltac:(M.monadic
                      (let γ :=
                        M.use
                          (M.alloc (|
                            UnOp.not (|
                              M.call_closure (|
                                M.get_associated_function (|
                                  Ty.path "revm_interpreter::gas::Gas",
                                  "record_cost",
                                  []
                                |),
                                [
                                  M.SubPointer.get_struct_record_field (|
                                    M.read (| interpreter |),
                                    "revm_interpreter::interpreter::Interpreter",
                                    "gas"
                                  |);
                                  M.read (|
                                    M.get_constant (| "revm_interpreter::gas::constants::LOW" |)
                                  |)
                                ]
                              |)
                            |)
                          |)) in
                      let _ :=
                        M.is_constant_or_break_match (| M.read (| γ |), Value.Bool true |) in
```

FORMAL LAND

USAGE

Showing the **equivalence** hand

translation/source Rust code.

FORMAL LAND

AUTOMATION

- Using “links” as an intermediate step
- Generated by Python script from the Rust AST
- Still a research work

FORMAL LAND

THANKS

FORMAL LAND