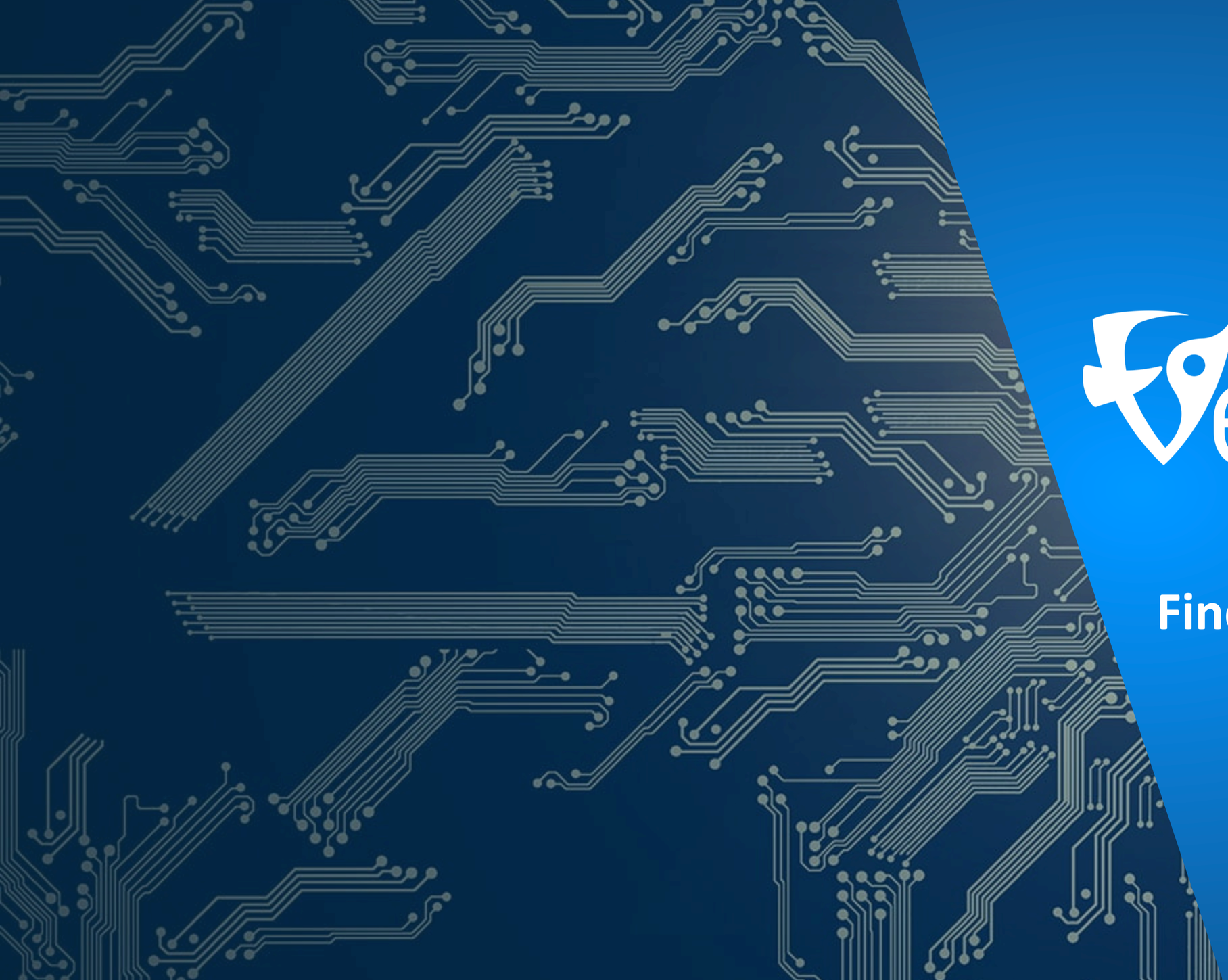
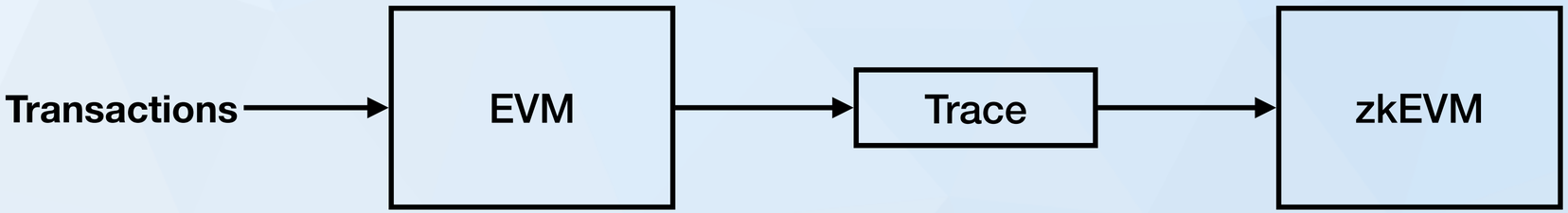


Finding Bugs in zkEVMs

Amber Huang
BD, Veridise

zkEVM Model

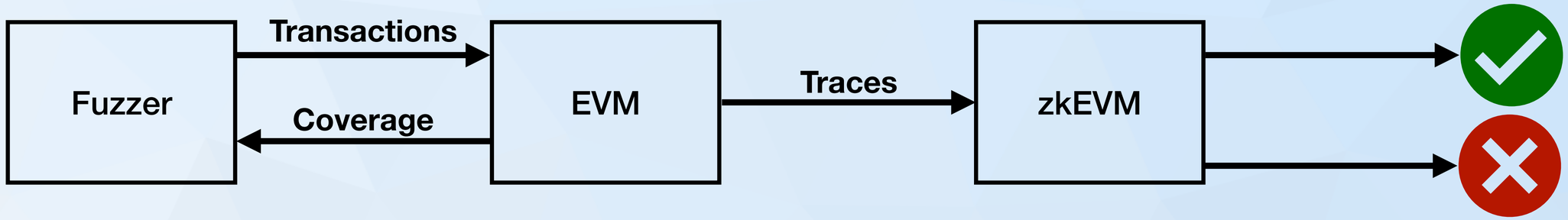
Simplified Model of a zkEVM



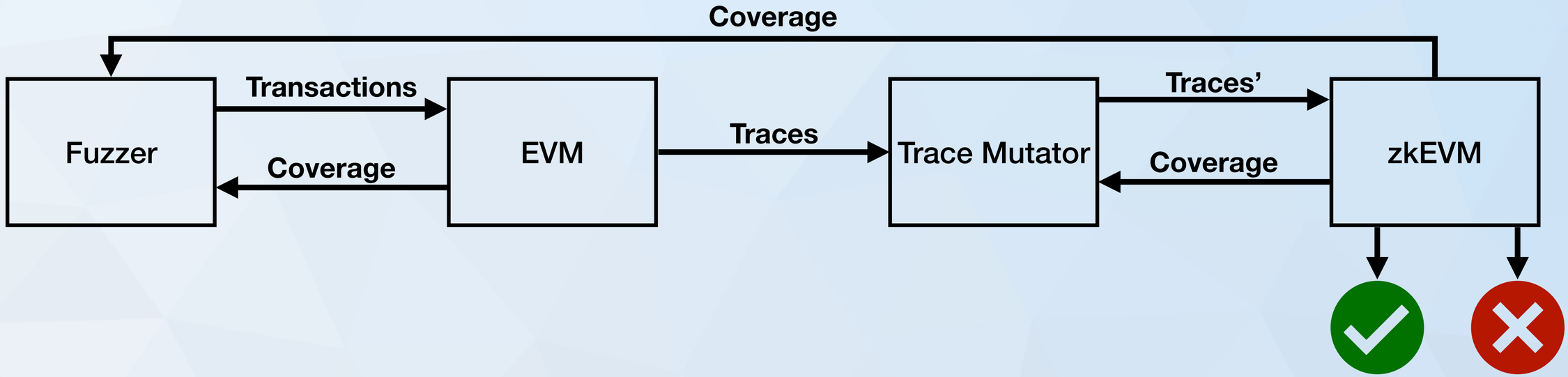
Goal: Find bugs in zkEVM's circuits

Veridise. | zkEVM Fuzzing Plan

1. Whole System Fuzzing

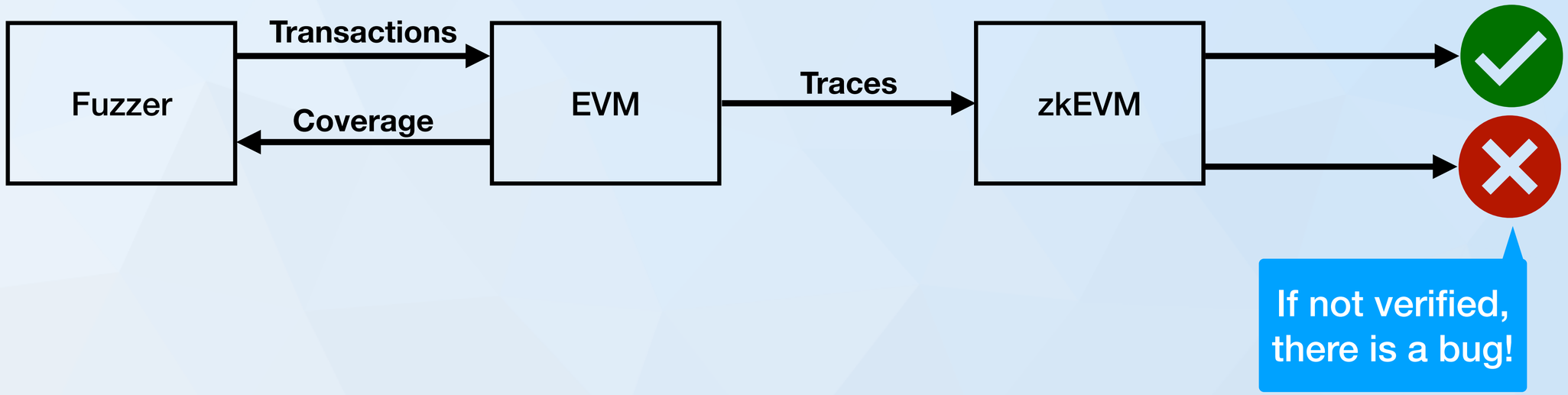


2. Trace Mutation Fuzzing



Veridise. | Whole System Fuzzing

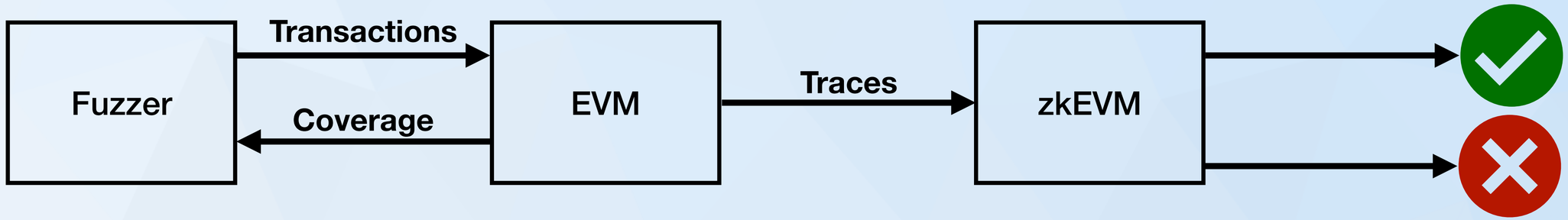
Looks for possible DoS Bugs in zkEVM



Unlikely to identify interesting bugs in ZK-Circuits

Veridise. | Results

Found 11 DoS bugs in a ZK EVM!

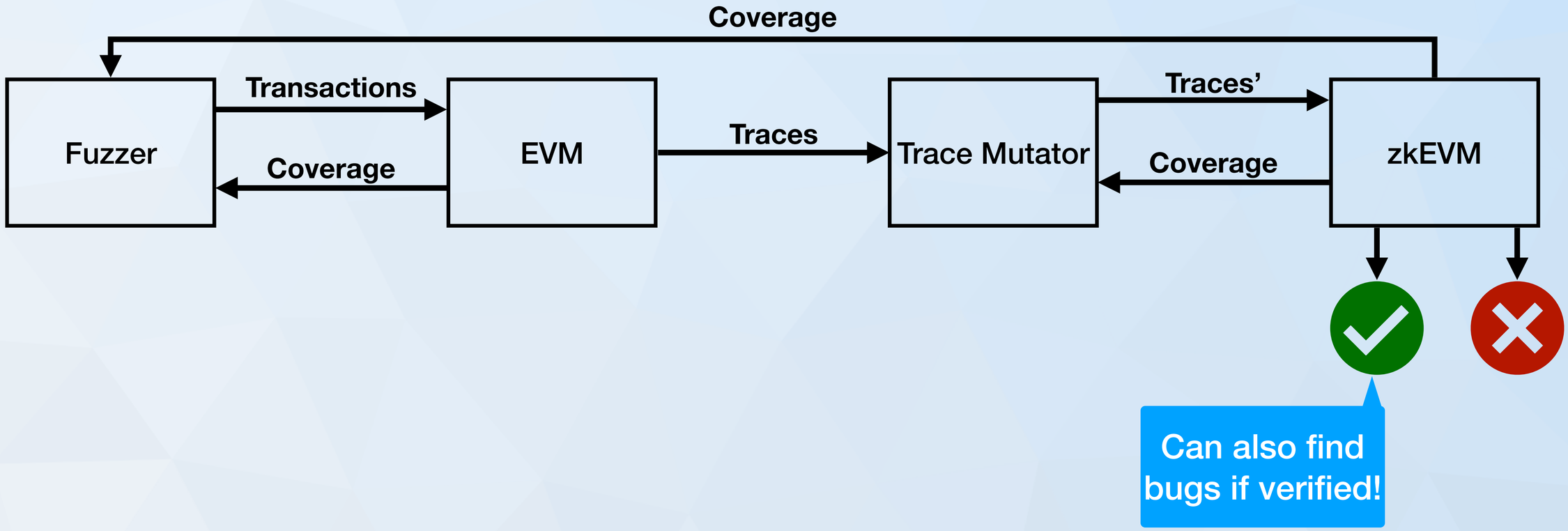


Bugs Found:

- 1 Verification Failed (State Circuit)
- 1 Invalid Call (TX Circuit)
- 3 Index Out of Bounds (EVM Circuit)
- 2 Integer Overflow (EVM Circuit)
- 2 Assertion Violation (EVM Circuit)
- 2 Invalid Calls (EVM Circuit)

Veridise. | Trace Mutation Fuzzing

Can identify complex bugs like under-constrained circuits using the trace mutator!



Veridise. | Finding bugs in the circuits

zkVanguard

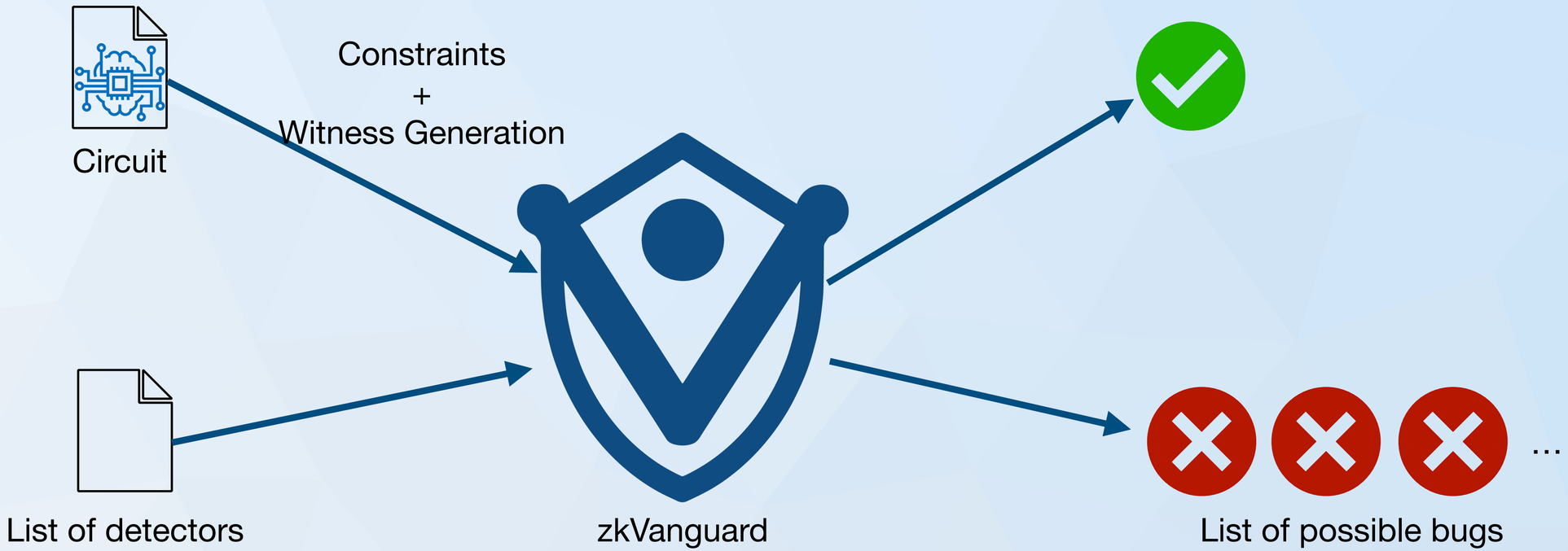
Static analysis for common bugs in ZK circuits

Picus

Proving whether or not ZK circuits are properly constrained

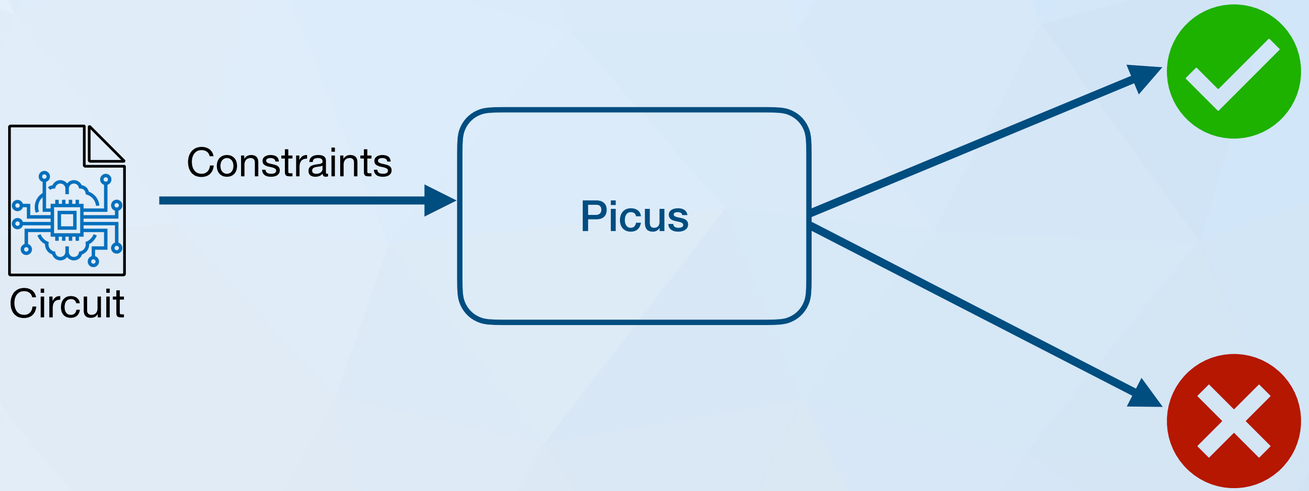
Finding common bugs with ZK Vanguard

ZK Vanguard has a set of detectors that search for common buggy patterns in Circuits



Veridise. | Verify that circuits are properly constrained

Picus formally proves that a circuit is deterministic



Veridise. | Helping auditors in ZK audits

We actively use Picus and zkVanguard in our audits

- Rate Limiting Nullifier (PSE)
- HydraS2 (Sismo)
- Manta Network
- Telepathy (Succinct Labs)
- Unirep (PSE)
- Scroll zkEVM
- CircomLib

...

https://veridise.com/audits/

Veridise. | Our ZK Research

https://medium.com/veridise

Automated Detection of Under-Constrained Circuits in Zero-Knowledge Proofs

SHANKARA PAILOOR*, Veridise, USA
YANJU CHEN*, Veridise, USA
FRANKLYN WANG, Harvard University/0xparc, USA
CLARA RODRÍGUEZ, Complutense University of Madrid, Spain
JACOB VAN GEFFEN, Veridise, USA
JASON MORTON, ZKonduit, USA
MICHAEL CHU, 0xparc, USA
BRIAN GU, 0xparc, USA
YU FENG, Veridise, USA
IŞIL DILLIG, Veridise, USA

Veridise. | Conclusion

Picus

zkVanguard

Trusted By:

Semaphore

succinct

MANTA NETWORK

Light Protocol

Scroll

Aleo

CircomLib

https://github.com/Veridise/Picus

Medium https://veridise.medium.com/

https://veridise.com/

@VeridiseInc