Learning to Fuzz from Symbolic Execution with Application to Smart Contracts

Jingxuan
He

Mislav
Balunovic

Nodar
Ambroladze

Petar
Tsankov

Martin
Vechev

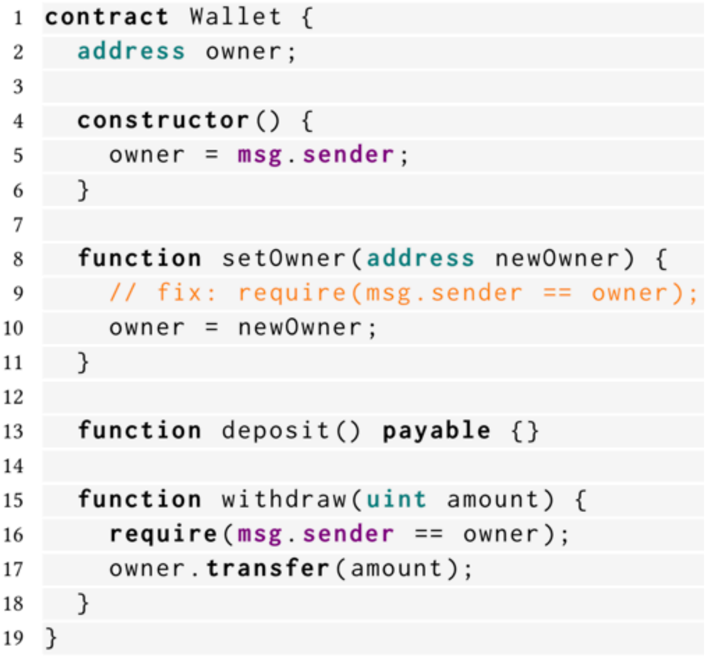
SRILAB

ETH zürich

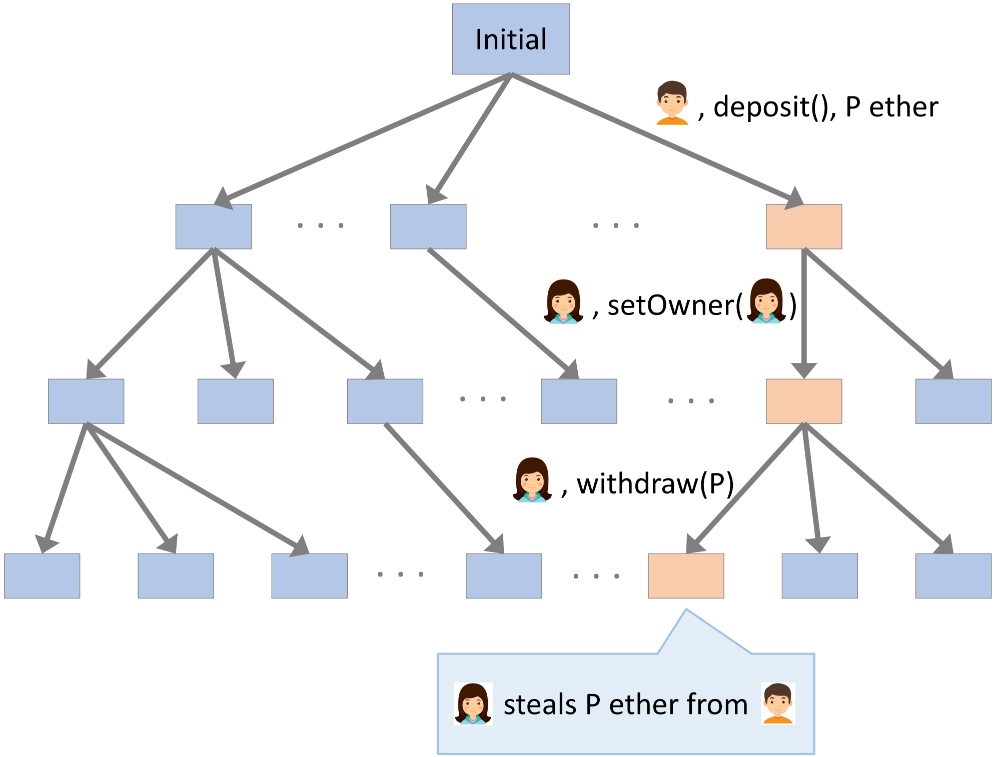
Random Fuzzing vs. Symbolic Execution

	Random Fuzzing	Symbolic Execution
Speed	✓ Fast	✗ Slow
Inputs	✗ Ineffective	✓ Effective
Coverage	✗ Low	✗ Low

Smart Contract Testing: Challenge

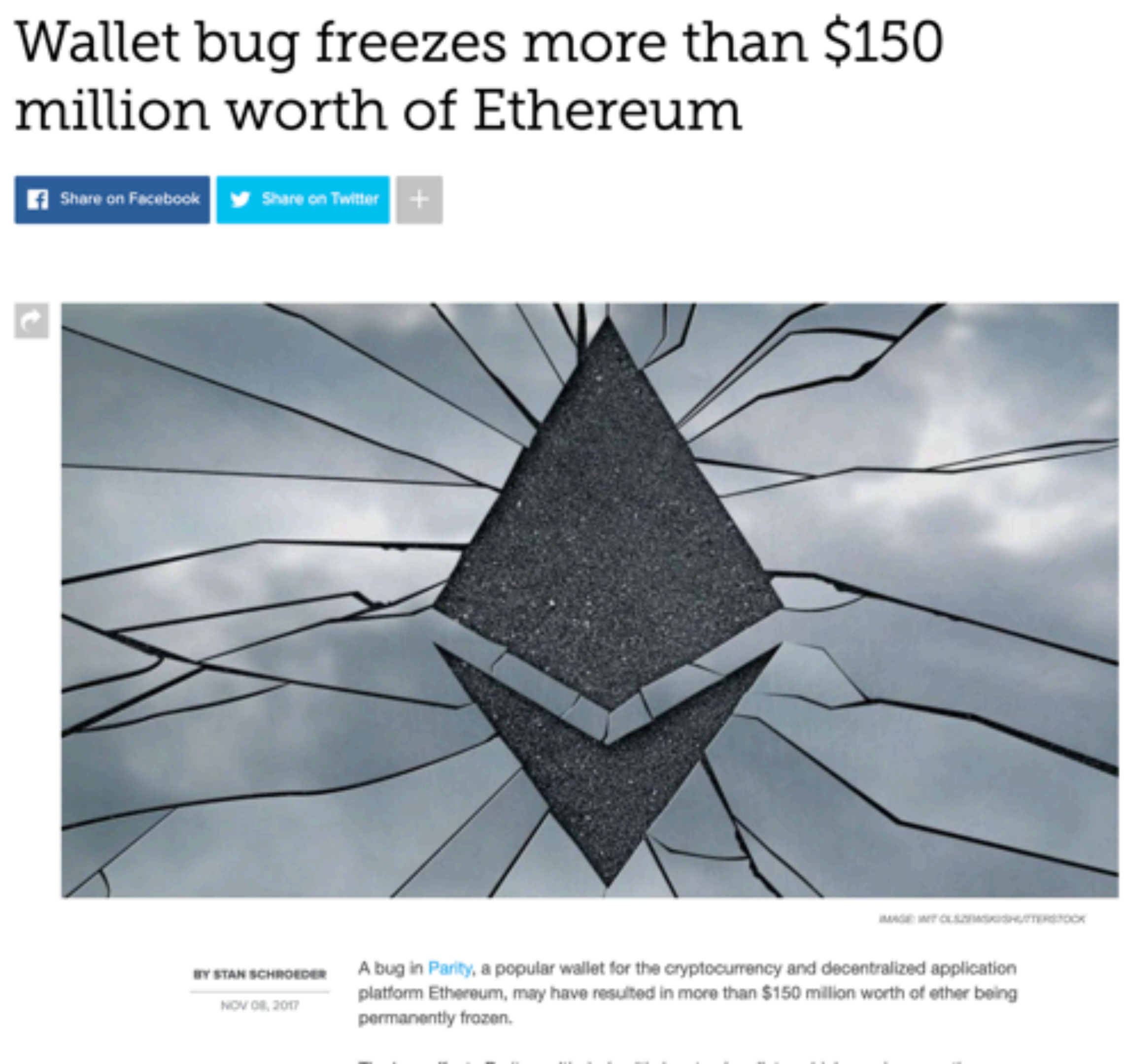


```
contract Wallet {
  address owner;

  constructor() {
    owner = msg.sender;
  }

  function setOwner(address newOwner) {
    // fix: require(msg.sender == owner);
    owner = newOwner;
  }

  function deposit() payable {}

  function withdraw(uint amount) {
    require(msg.sender == owner);
    owner.transfer(amount);
  }
}
```



Smart Contract Testing: Challenge

Wanted: Transaction sequences that thoroughly explore the state space



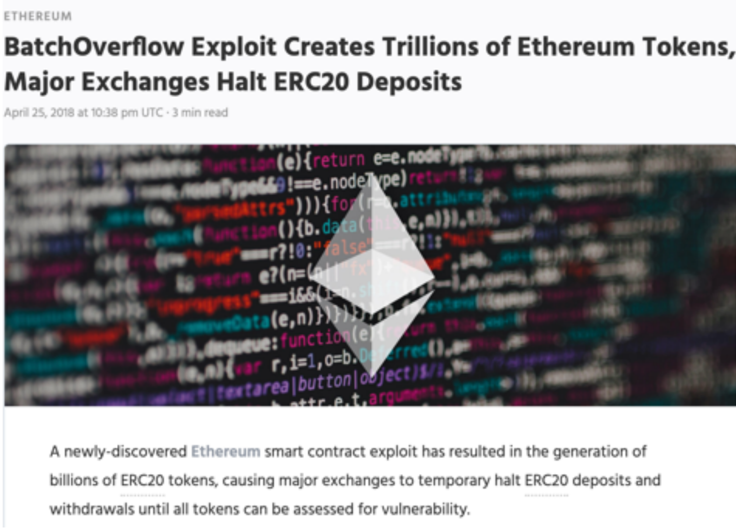
Wallet bug freezes more than $150 million worth of Ethereum

IMAGE: WIT OLSZEWSKI/SHUTTERSTOCK

BY STAN SCHROEDER

NOV 08, 2017

A bug in Parity, a popular wallet for the cryptocurrency and decentralized application platform Ethereum, may have resulted in more than $150 million worth of ether being permanently frozen.

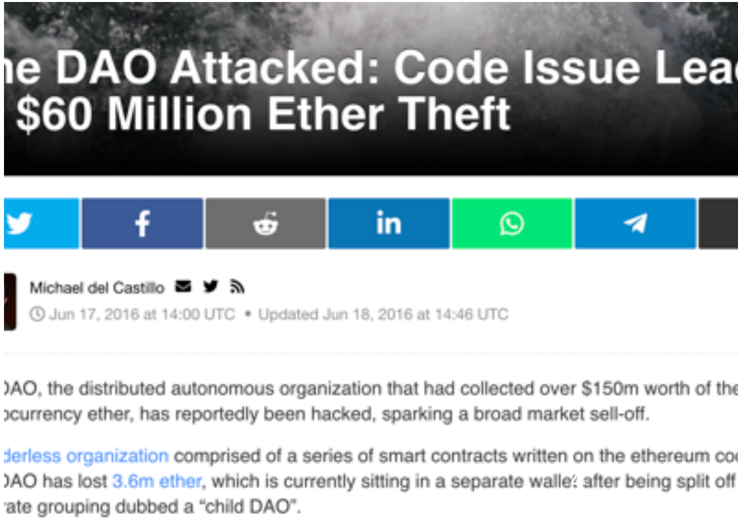


ETHEREUM

BatchOverflow Exploit Creates Trillions of Ethereum Tokens, Major Exchanges Halt ERC20 Deposits

April 25, 2018 at 10:38 pm UTC · 3 min read

A newly-discovered Ethereum smart contract exploit has resulted in the generation of billions of ERC20 tokens, causing major exchanges to temporary halt ERC20 deposits and withdrawals until all tokens can be assessed for vulnerability.



›e DAO Attacked: Code Issue Lea $60 Million Ether Theft

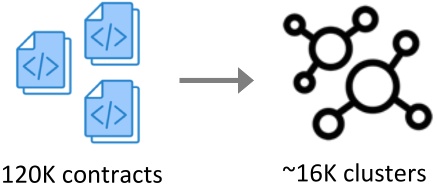
Michael del Castillo

Jun 17, 2016 at 14:00 UTC • Updated Jun 18, 2016 at 14:46 UTC

›AO, the distributed autonomous organization that had collected over $150m worth of the ›ocurrency ether, has reportedly been hacked, sparking a broad market sell-off.

›derless organization comprised of a series of smart contracts written on the ethereum coc ›AO has lost 3.6m ether, which is currently sitting in a separate walle after being split off ›ate grouping dubbed a “child DAO”.

Random Fuzzing vs. Symbolic Execution

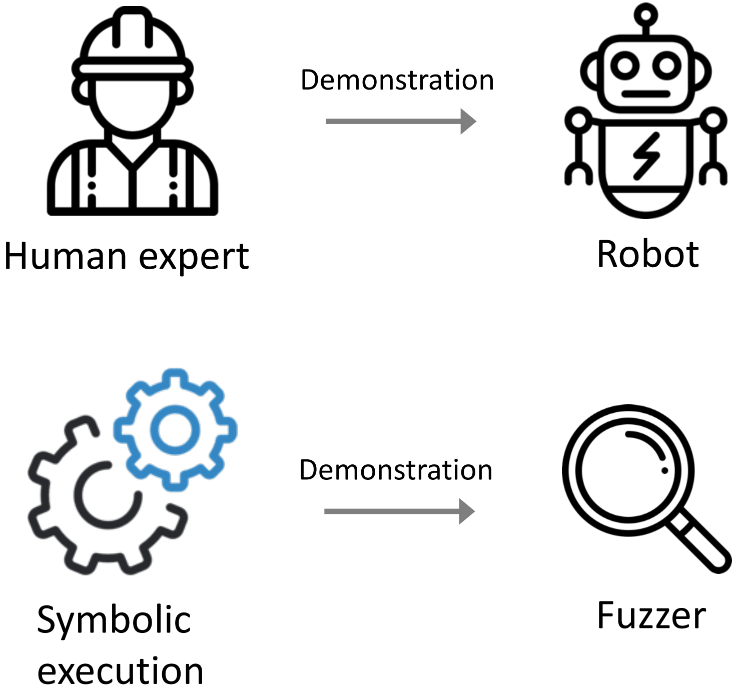


- Analyzing Ethereum’s Contract Topology. Kiffer et al.. IMC ’18

Imitation Learning based Fuzzer

	Random Fuzzing	Symbolic Execution	ILF (this work)
Speed	✓ Fast	✗ Slow	✓ Fast
Inputs	✗ Ineffective	✓ Effective	✓ Effective
Coverage	✗ Low	✗ Low	✓ High

Imitation Learning



Human expert

Demonstration

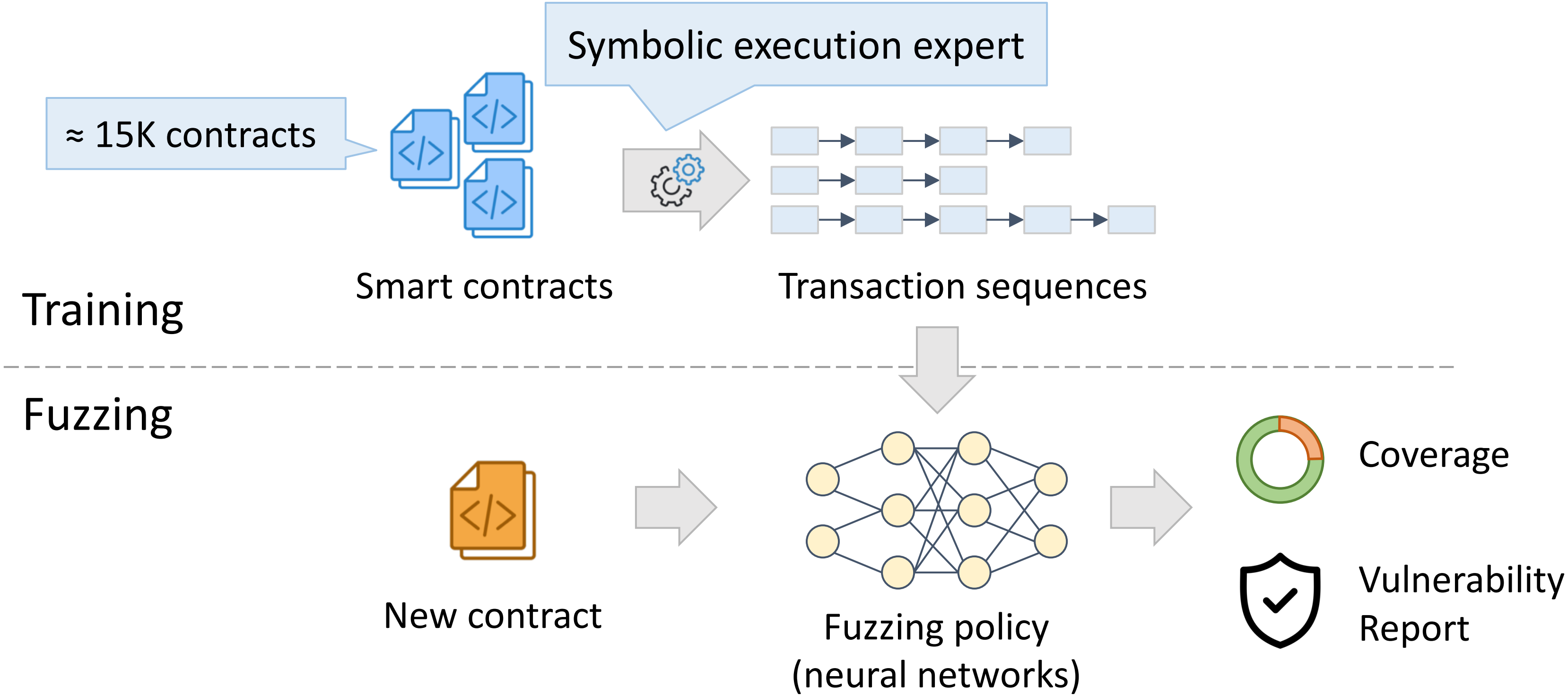
Robot

Symbolic execution

Demonstration

Fuzzer

Learning to Fuzz from Symbolic Execution



≈ 15K contracts

Symbolic execution expert

Smart contracts

Transaction sequences

Training

Fuzzing

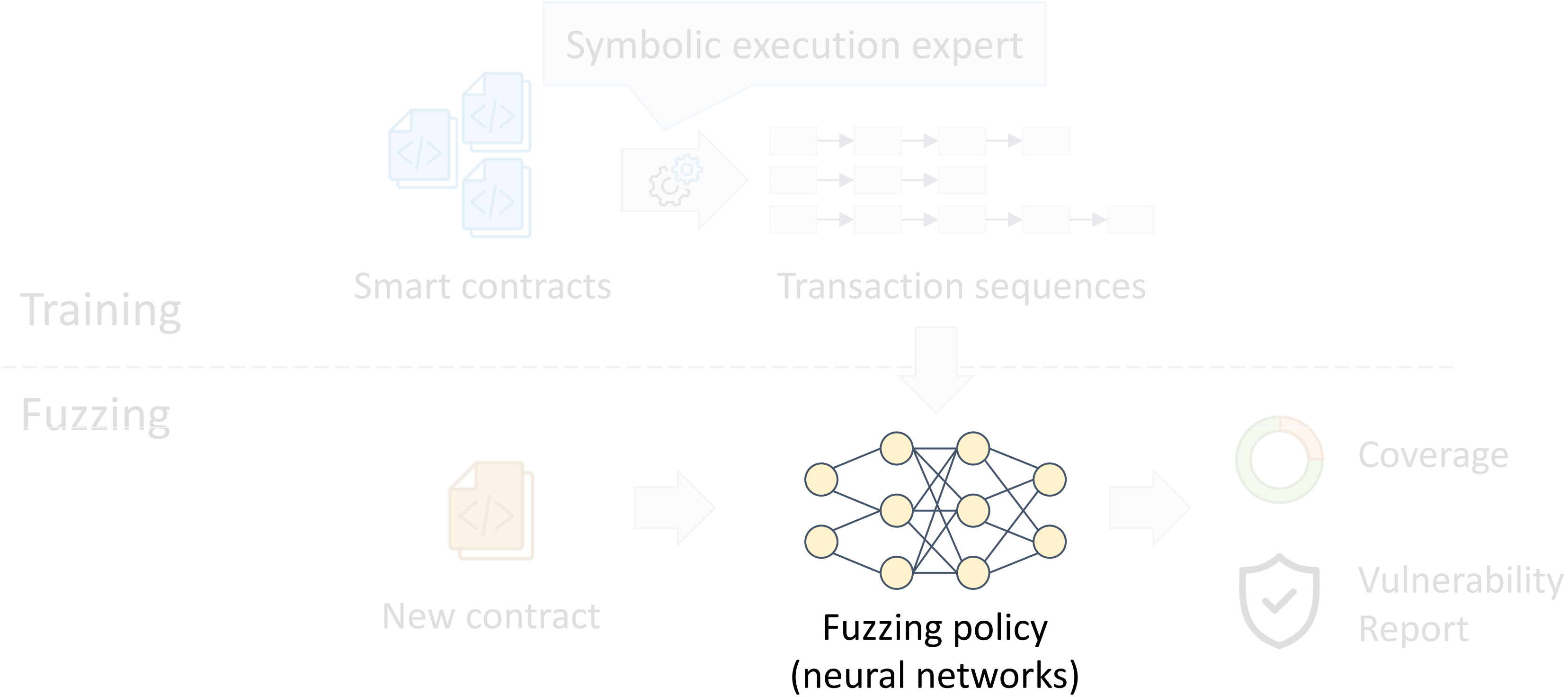
New contract

Fuzzing policy
(neural networks)

Coverage

Vulnerability
Report

Learning to Fuzz from Symbolic Execution



Symbolic execution expert

Smart contracts

Transaction sequences

Training

Fuzzing

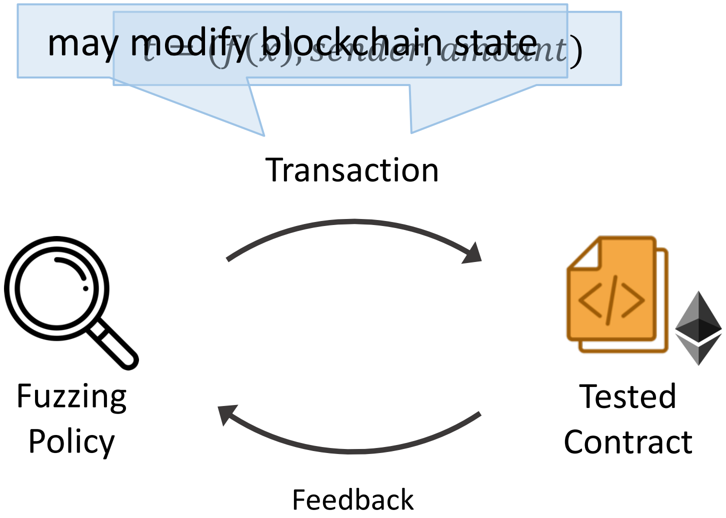
New contract

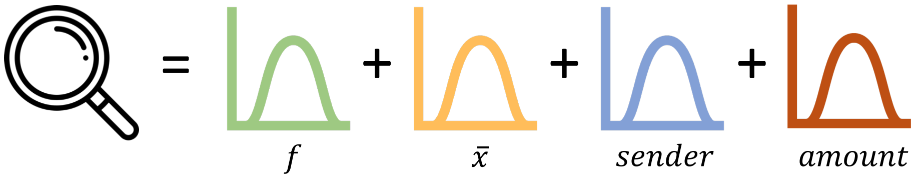
Coverage

Vulnerability Report

Fuzzing policy (neural networks)

Smart Contract Fuzzing Policy

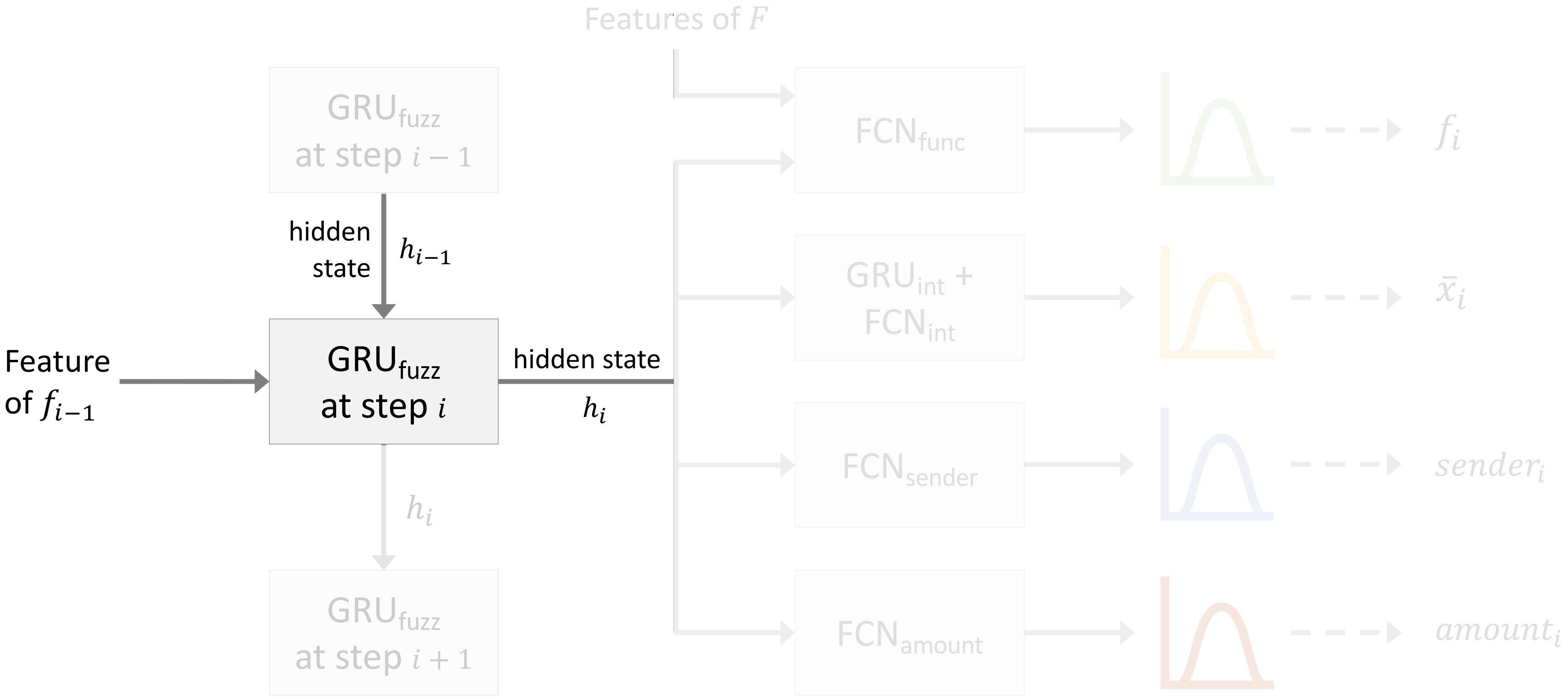

may modify blockchain state
$t = (f(\bar{x}), sender, amount)$
Transaction
Fuzzing Policy
Tested Contract
Feedback



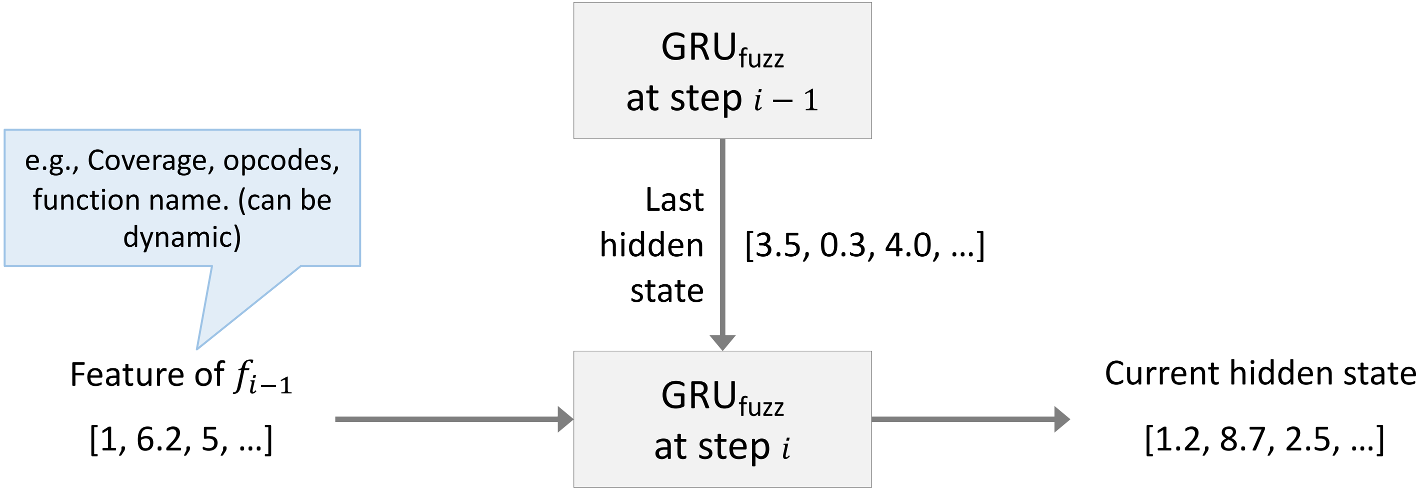
Example: a Uniformly Random Policy

- 🟩 : $Uniform(F)$
- 🟧 : $Uniform(Signature(f))$
- 🟦 : $Uniform(SENDERS)$
- 🟥 : $\begin{cases} Uniform([0, MA]) & f \text{ is payable} \\ P(0) = 1 & \text{otherwise} \end{cases}$

Neural Network Fuzzing Policy

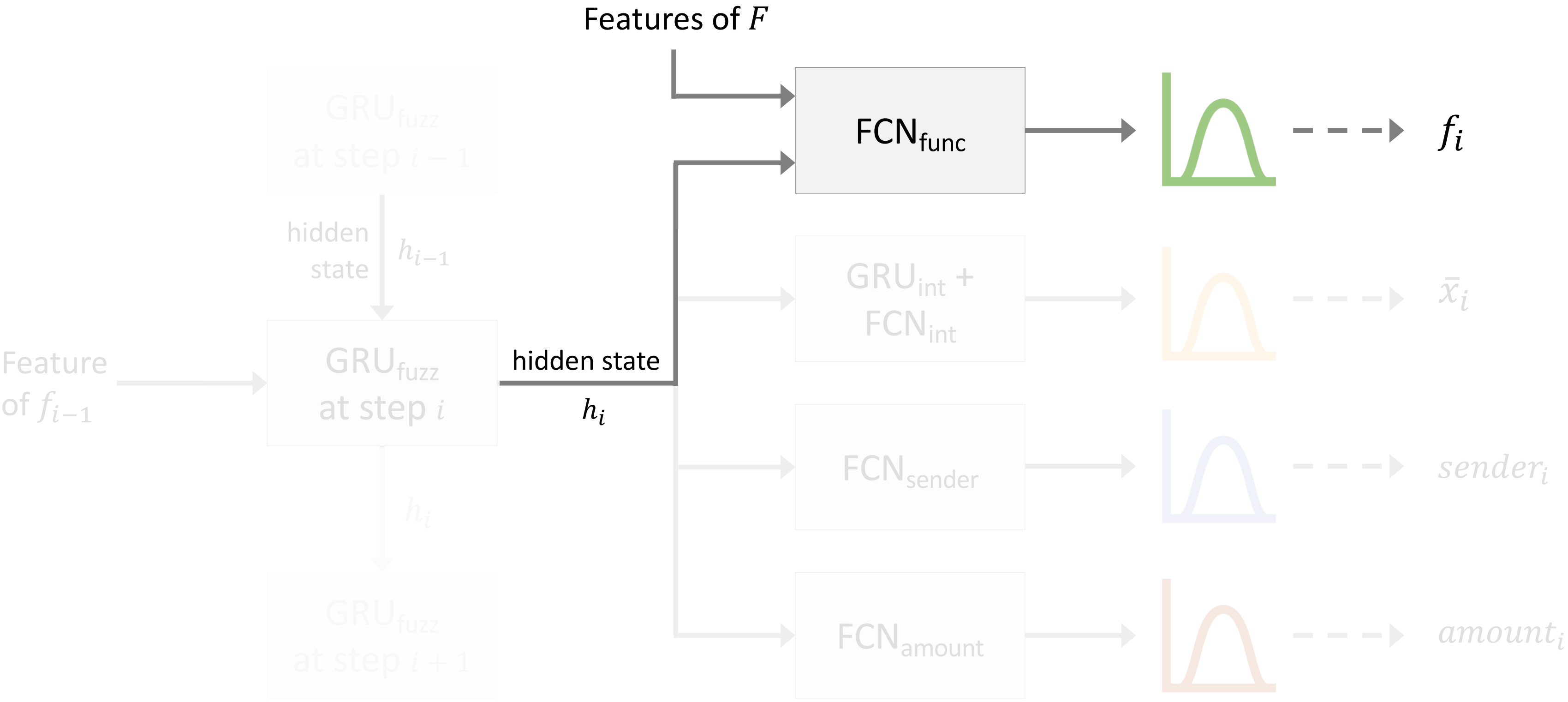


Neural Network Fuzzing Policy – Fuzzing State

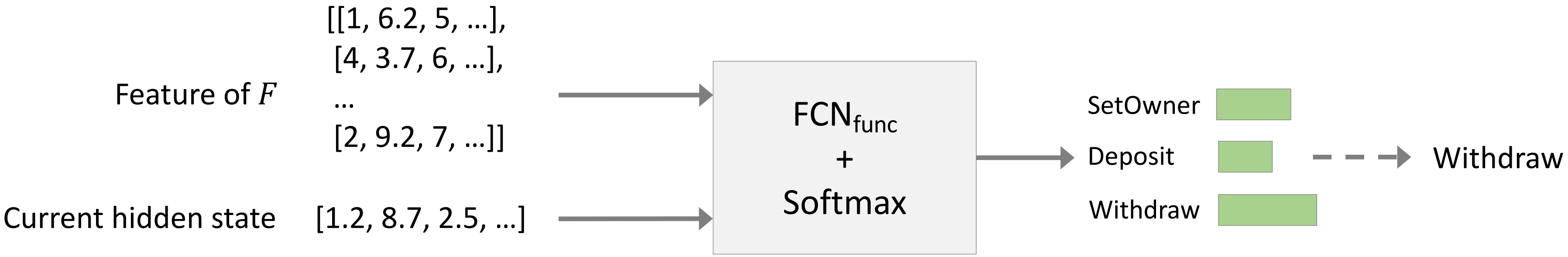


e.g., Coverage, opcodes, function name. (can be dynamic)

Neural Network Fuzzing Policy



Neural Network Fuzzing Policy – Function



Feature of F

[[1, 6.2, 5, …],
[4, 3.7, 6, …],
…
[2, 9.2, 7, …]]

Current hidden state

[1.2, 8.7, 2.5, …]

FCN$_{\text{func}}$
+
Softmax

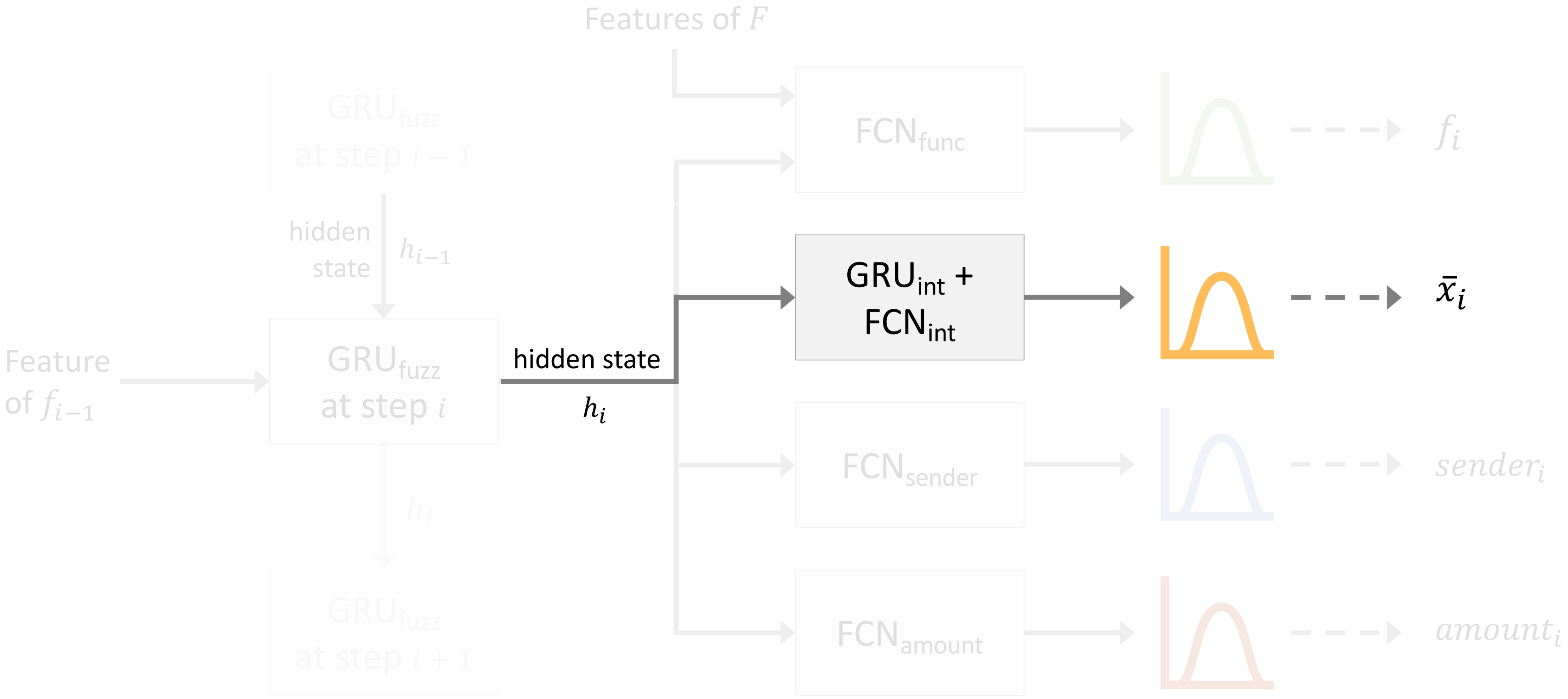
SetOwner

Deposit

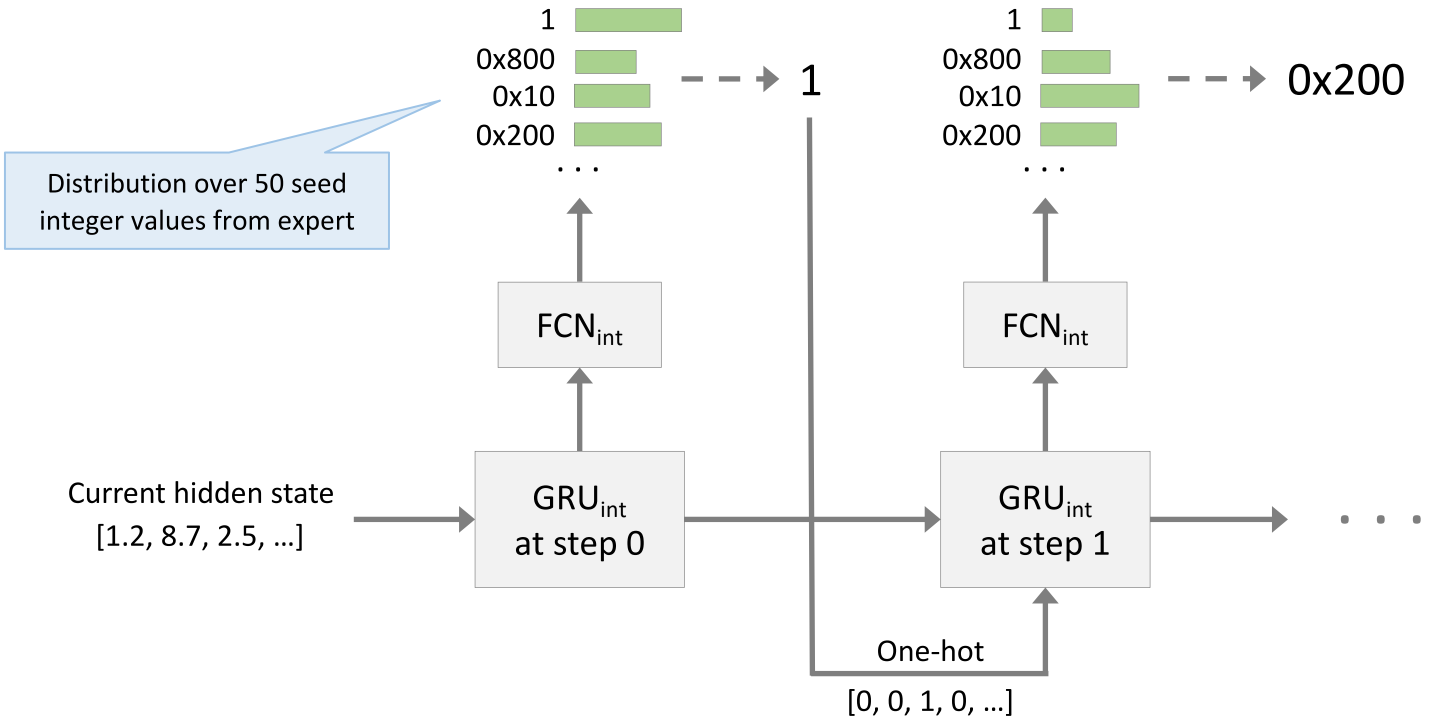
Withdraw

Withdraw

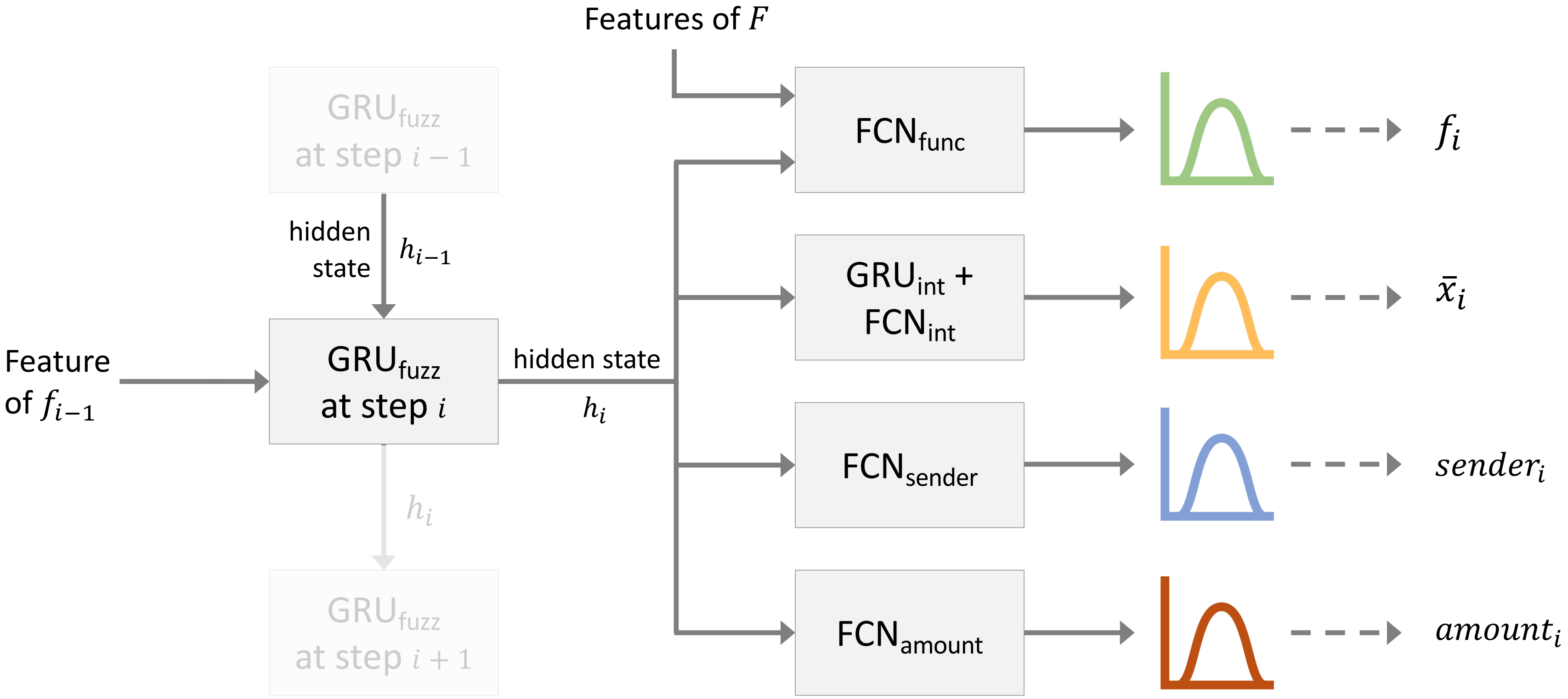
Neural Network Fuzzing Policy


Features of F
GRU_{fuzz} at step $i-1$
hidden state
h_{i-1}
Feature of f_{i-1}
GRU_{fuzz} at step i
hidden state
h_i
h_i
GRU_{fuzz} at step $i+1$
FCN_{func}
GRU_{int} + FCN_{int}
$\text{FCN}_{\text{sender}}$
$\text{FCN}_{\text{amount}}$
f_i
$\bar{x}_i$
$sender_i$
$amount_i$

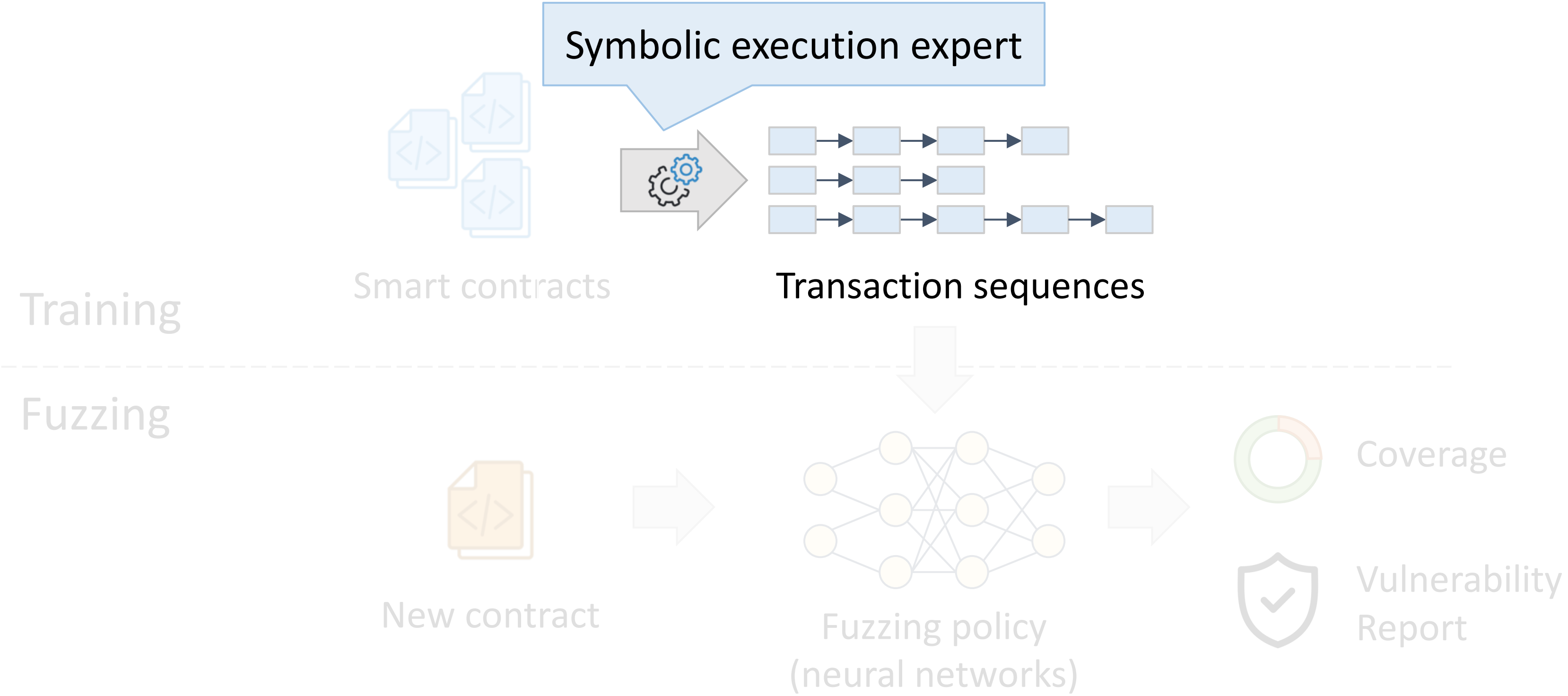
Neural Network Fuzzing Policy – Arguments



Neural Network Fuzzing Policy


Features of F
GRU_{fuzz} at step $i-1$
hidden state
h_{i-1}
Feature of f_{i-1}
GRU_{fuzz} at step i
hidden state
h_i
h_i
GRU_{fuzz} at step $i+1$
FCN_{func}
GRU_{int} + FCN_{int}
$\text{FCN}_{\text{sender}}$
$\text{FCN}_{\text{amount}}$
f_i
$\bar{x}_i$
$sender_i$
$amount_i$

Learning to Fuzz from Symbolic Execution



Symbolic execution expert

Smart contracts

Transaction sequences

Training

Fuzzing

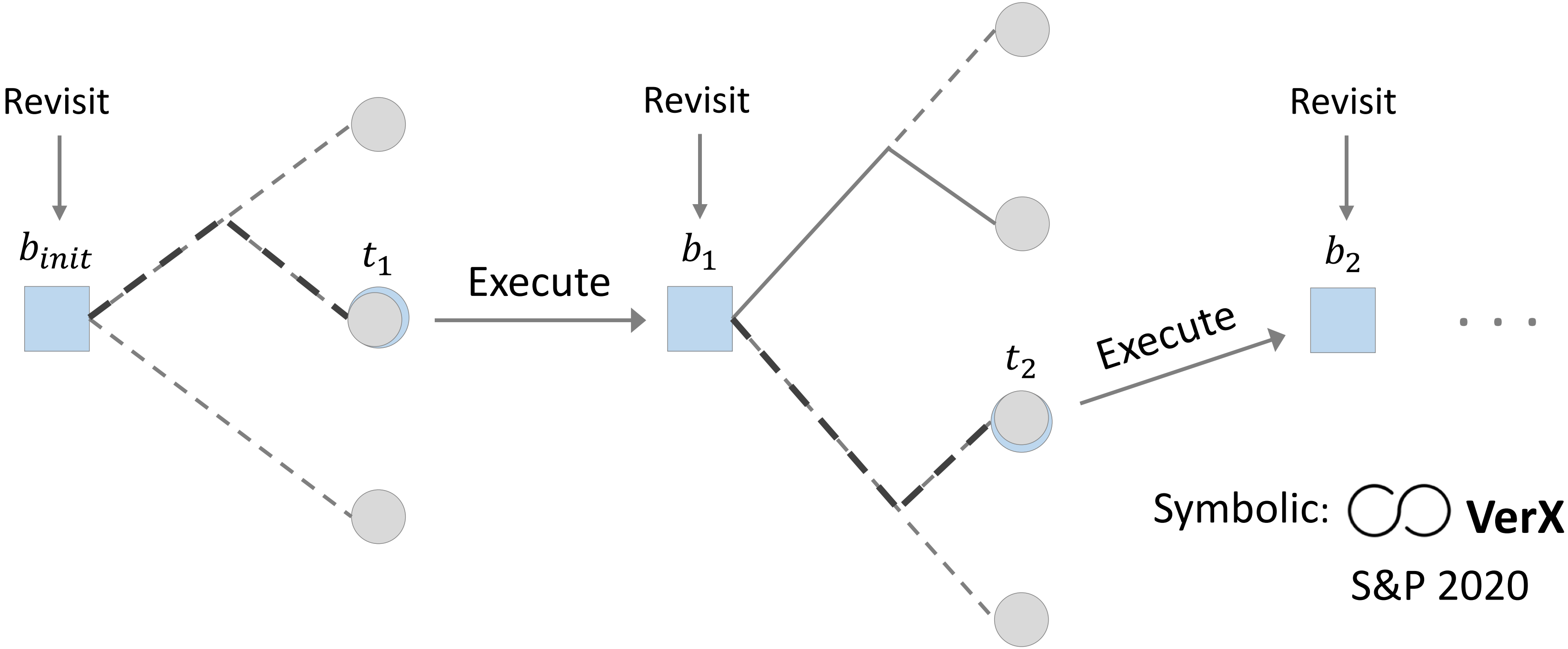
New contract

Fuzzing policy
(neural networks)

Coverage

Vulnerability
Report

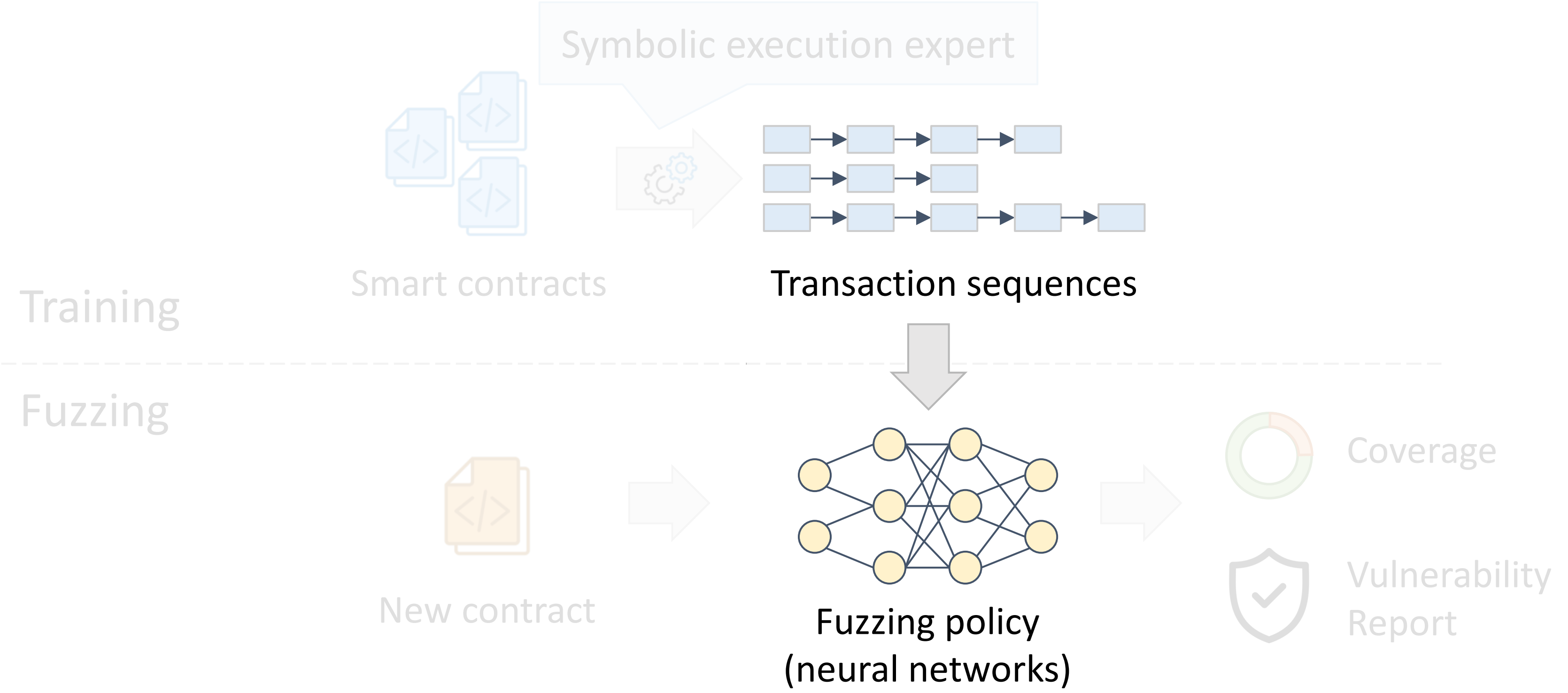
Symbolic Execution Expert



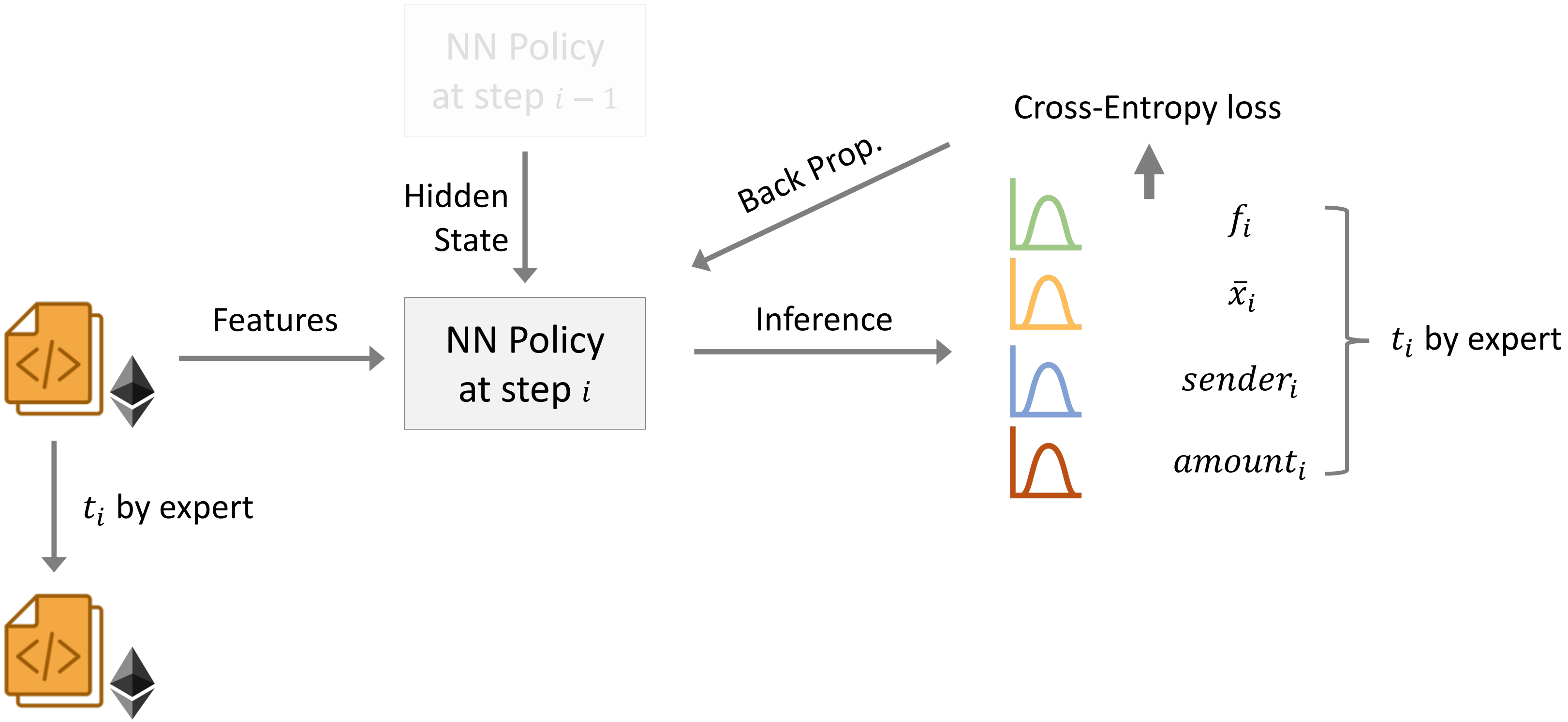
Symbolic: VerX

S&P 2020

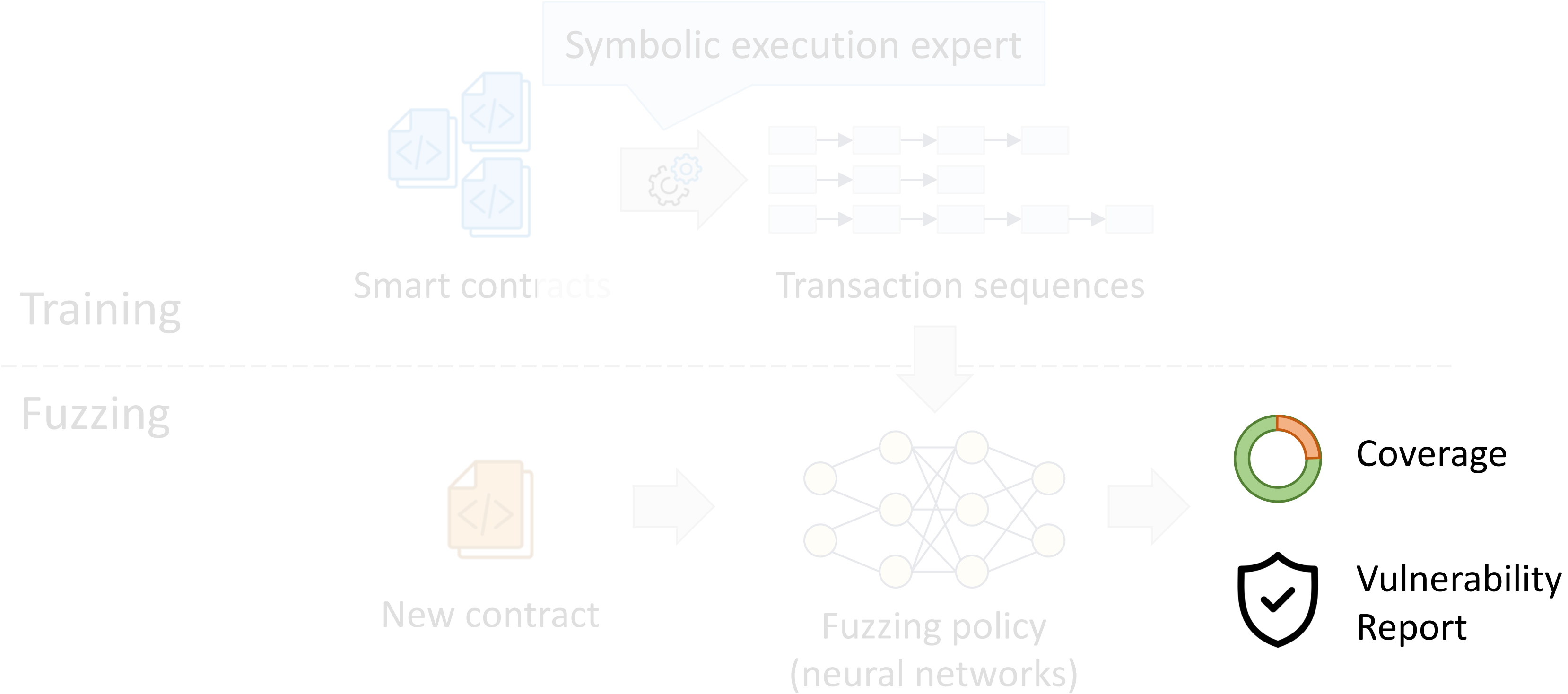
Learning to Fuzz from Symbolic Execution



Training Neural Network Fuzzing Policy



Learning to Fuzz from Symbolic Execution



Symbolic execution expert

Smart contracts

Transaction sequences

Training

Fuzzing

New contract

Fuzzing policy (neural networks)

Coverage

Vulnerability Report

ILF System: Coverage & Vulnerability Detection

- **Instruction** coverage.
- **Basic block** coverage.

- **Locking**: The contract cannot send out but can receive ether.
- **Leaking**: An attacker can steal ether from the contract.
- **Suicidal**: An attacker can deconstruct the contract.
- **Block Dependency**: Ether transfer depends on block state variables.
- **Unhandled Exception**: Root call does not catch exceptions from child calls.
- **Controlled Delegatecall**: Transaction parameters explicitly flow into arguments of a *delegatecall* instruction.

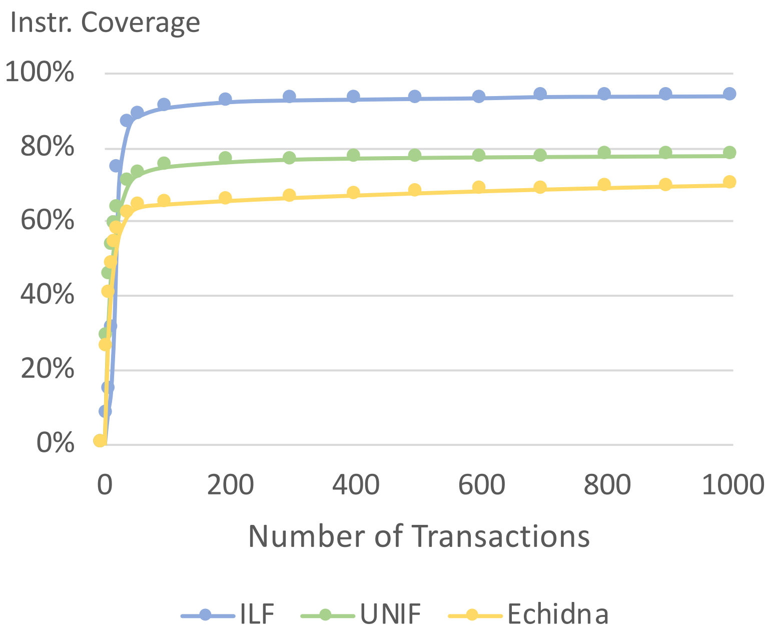
Evaluation

- 18,496 Contracts (5,013 Large & 13,483 Small)
- 5-fold Cross Validation

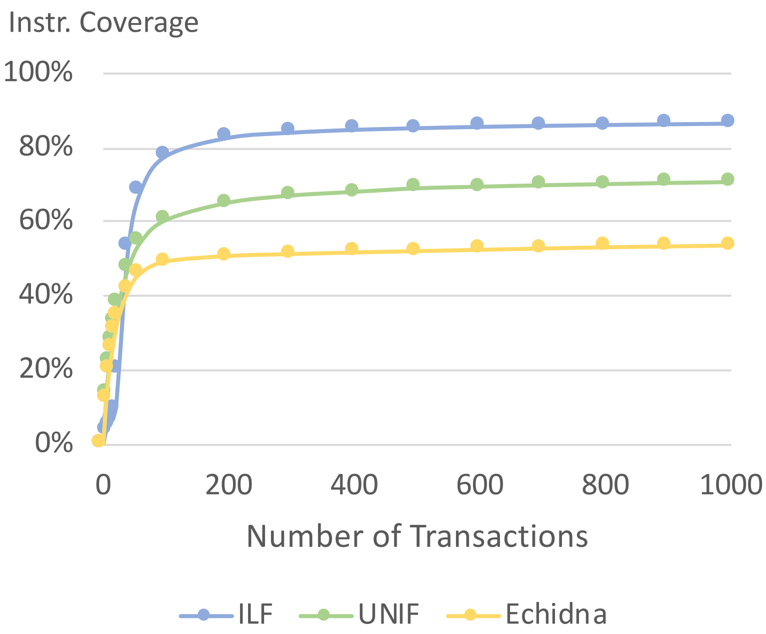
- UNIF ◔ 🛡
- EXPERT ◔
- Echidna ◔
- MAIAN 🛡
- ContractFuzzer 🛡

- Coverage & Speed
- Fuzzing Components
- Vulnerability Detection
- Case Study

Coverage: ILF vs. Fuzzers

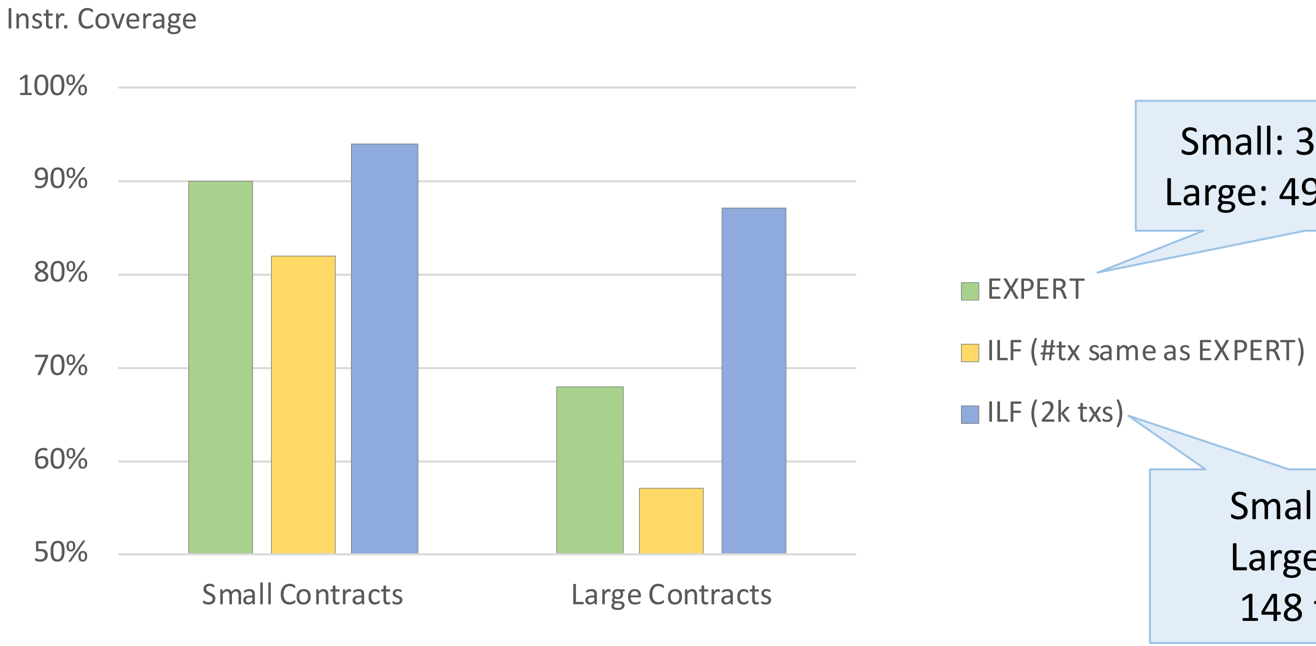


Small contracts



Large contracts

Coverage: ILF vs. Symbolic Expert

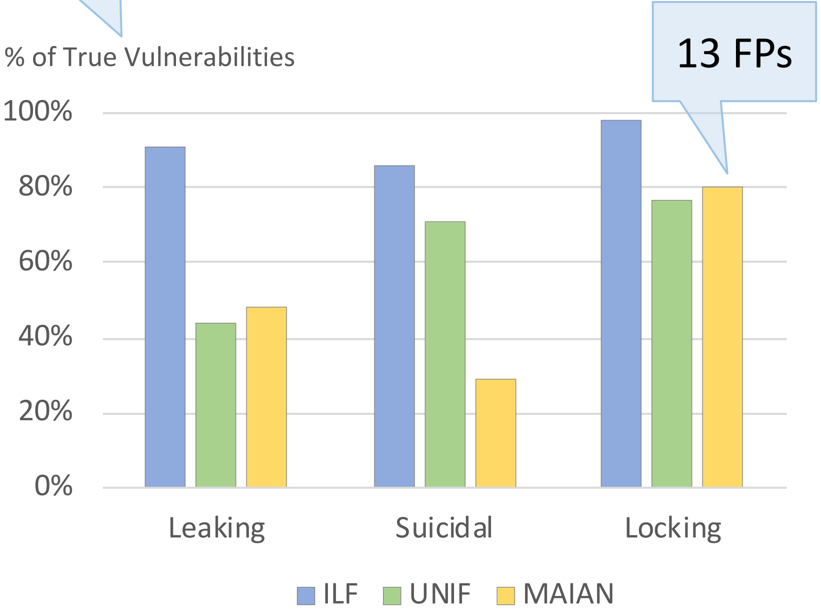


Small: 30 txs, 547s
Large: 49 txs, 2,580s

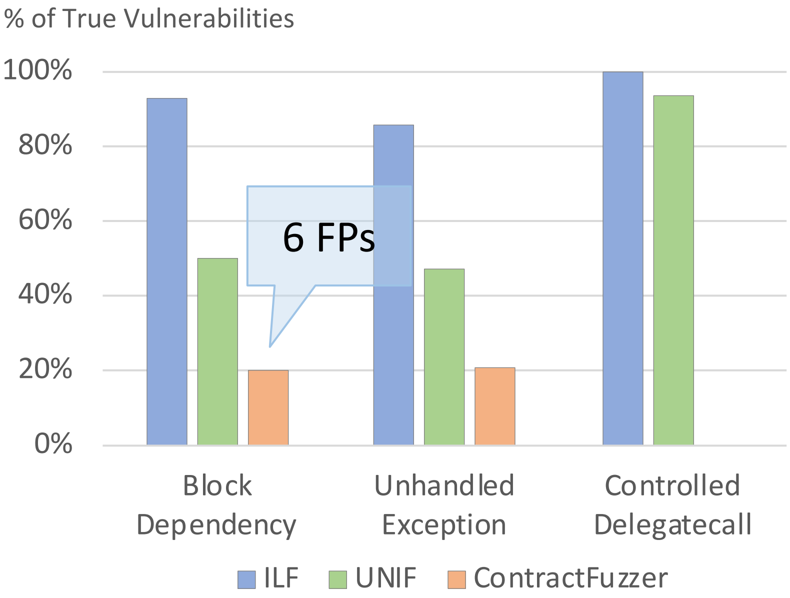
Small: 13s
Large: 17s
148 txs/s

Vulnerability Detection

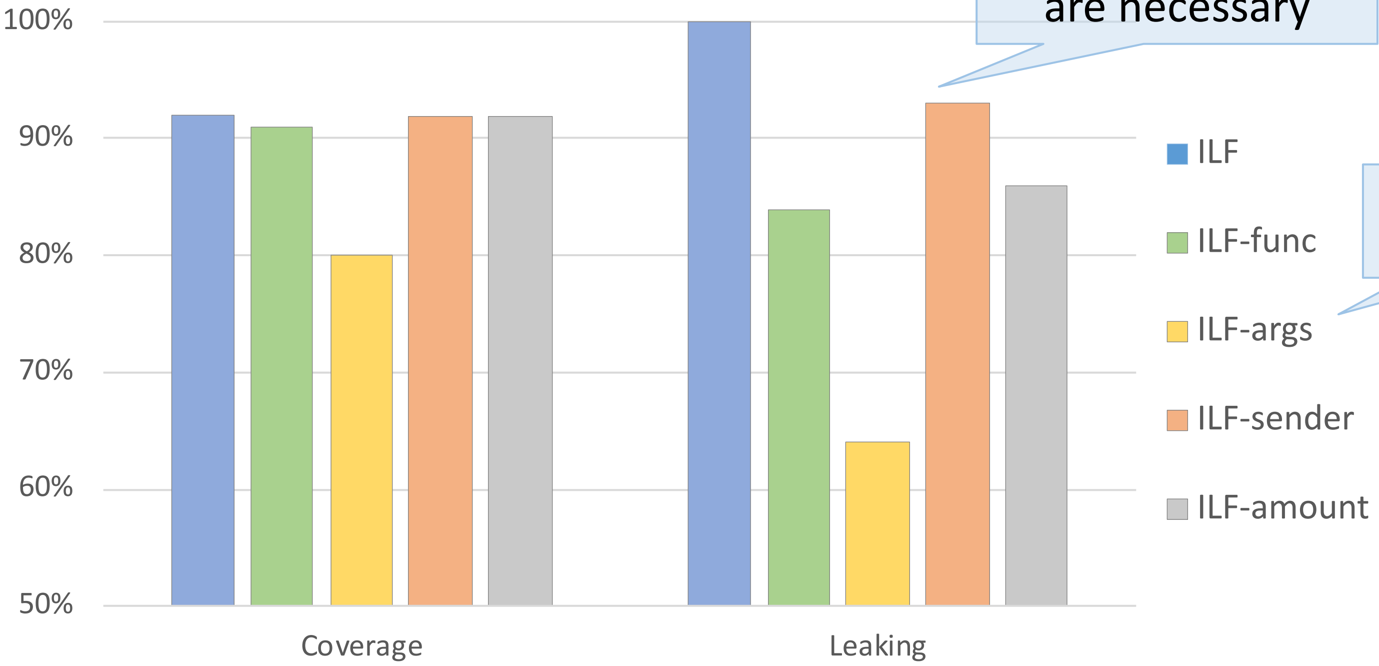
|🟦| / |🟦 ∪ 🟩 ∪ 🟨|



ILF: 0 FPs



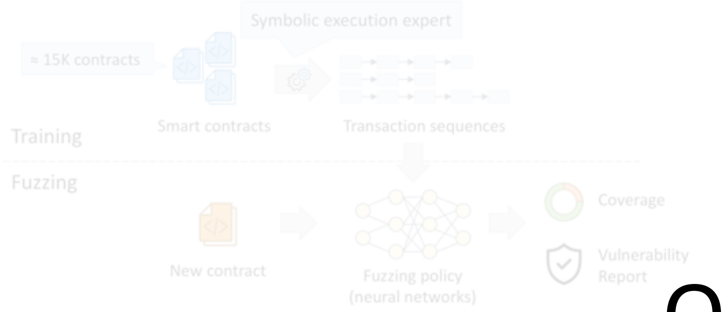
Importance of Policy Components

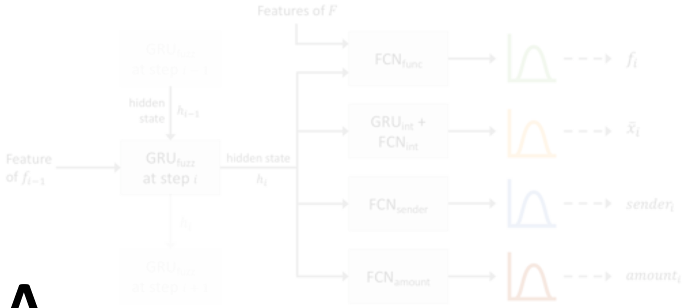


All components are necessary

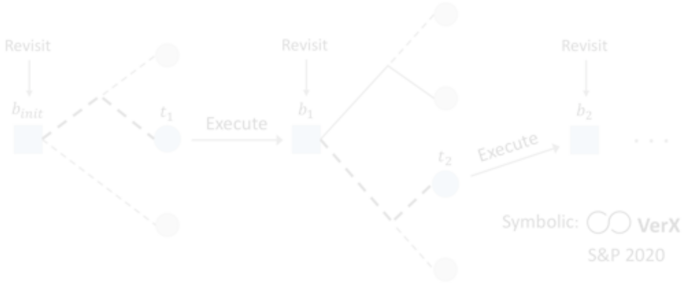
Most important

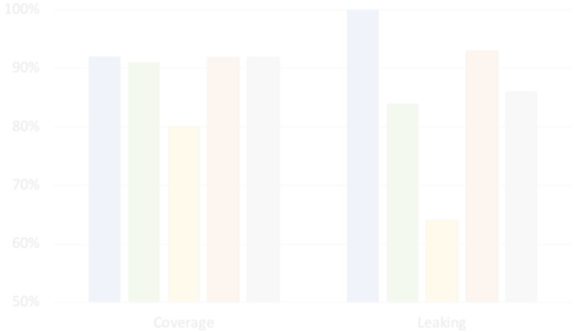
Summary


Symbolic execution expert
≈ 15K contracts
Smart contracts
Transaction sequences
Training
Fuzzing
New contract
Fuzzing policy
(neural networks)
Coverage
Vulnerability
Report


Features of F
GRU
at step $i-1$
hidden
state
h_{i-1}
Feature
of f_{i-1}
GRU_{fuzz}
at step i
hidden state
h_i
GRU
at step $i+1$
FCN_{func}
GRU_{int} +
FCN_{int}
FCN_{sender}
FCN_{amount}
f_i
$\bar{x}_i$
$sender_i$
$amount_i$

Q & A


Revisit
Revisit
Revisit
b_{init}
t_1
Execute
b_1
t_2
Execute
b_2
. . .
Symbolic: VerX
S&P 2020


100%
90%
80%
70%
60%
50%
Coverage
Leaking