



Universidade de Brasília
Departamento de Ciência da Computação



DogeFuzz: A Simple Yet Efficient Grey-box Fuzzer for Ethereum Smart Contracts

Ismael Medeiros, Fausto Carvalho, Alexandre Ferreira, Rodrigo Bonifácio, Fabiano Cavalcanti
Fernandes

18/09/2024

Cryptonews • Blockchain News

Ethereum Suffers Most Hacks Among Blockchains in 2024

Ethereum Hacks



Crypto Reporter
Shalini Nagarajan

Last updated:

16 de abril de 2024 às 06:37 BRT

Forbes

FORBES > MONEY > INVESTING

BREAKING

More Than \$600 Million Stolen In Ethereum And Other Cryptocurrencies—Marking One Of Crypto’s Biggest Hacks Ever

Jonathan Ponciano Former Staff

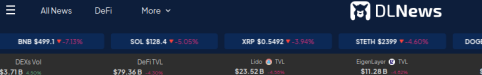
1

Aug 10, 2021, 11:10am EDT

O que é a Hyperledger Besu e por que o BC a escolheu para o Drex

Plataforma blockchain empresarial é baseada em Ethereum

Por Juliana Stell, Valor — São Paulo
07/12/2023 09h03 - Atualizado há 8 meses



BNB	SOL	XRP	STETH	DOGE
\$499.1	\$128.4	\$0.5492	\$2399	
-7.12%	-5.05%	-3.94%	-4.60%	

DEX Vol	DeFiTVL	Lido	SpotLayer
\$3.71 B	\$79.36 B	\$23.52 B	\$11.28 B
+1.0%	+1.0%	+1.0%	+1.0%

Markets

North Korean hackers eye Bitcoin, Ethereum ETFs, FBI warns

Estatísticas Ethereum - 1º Semestre 2024

- ▶ Valor Total Bloqueado (TVL) em Ethereum: **\$49B** (56% do mercado).
- ▶ TVL em SC implementados em Solidity: **\$126B**.
- ▶ Ataques na Rede Ethereum: **222** ataques **\$315B**.
- ▶ Exploração de vulnerabilidades em código de SC: **105** ataques.

Potencializadores de ataques

- ▶ **Imutabilidade** dos Smart Contracts.
- ▶ Possibilidade de ganhos **econômicos** imediatos e enormes.
- ▶ **Fragilidade** de projeto da linguagem Solidity.
- ▶ Natureza **pública** e **anônima** em blockchains.

Resultantes de **práticas inadequadas** de programação ou do **desconhecimento** da tecnologia blockchain.

Tipos de vulnerabilidades mais comuns:

- ▶ Reentrancy.
- ▶ Mishandled Exception.
- ▶ Integer Overflow and Underflow.
- ▶ Insecure Randomness (Number & Timestamp).

Técnicas de detecção:

- ▶ Análise Estática.
- ▶ **Análise Dinâmica.**
- ▶ Execução simbólica.
- ▶ Aprendizado de Máquina.
- ▶ Verificação formal.

Blockchain pode ser visto como um **sistema transacional**, uma máquina de estados.

Estado da arte em Smart Contracts fuzzing:

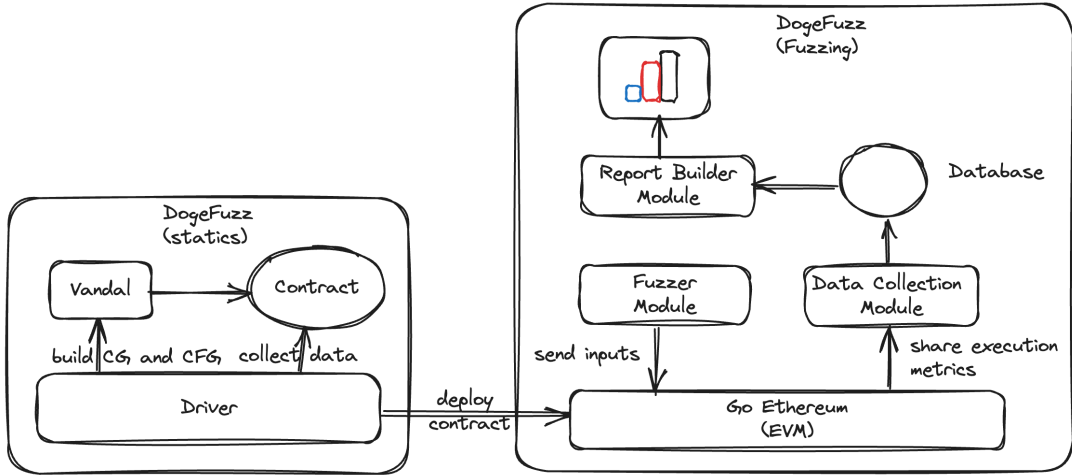
- ▶ Geração de sementes de transações e argumentos mais promissores.
- ▶ Exploração do contexto de estado e código fonte.
- ▶ Instrumentação de Ethereum Virtual Machine (EVM) leves.
- ▶ Ferramentas: ILF (ML), sFuzz (GA), Smartian (PA).

Contribuições do DogeFuzz

1. Uma **infraestrutura extensível** de código aberto para experimentar estratégias de fuzzing para smart contracts.
2. Experimentos que **demonstram** que as **estratégias mais simples de fuzzing** podem superar fuzzers de última geração.

Solução Proposta

Arquitetura DogeFuzz



Estratégias de fuzzing implementadas

- ▶ **DogeFuzz-B**: um blackbox fuzzer.
- ▶ **DogeFuzz-G**: um greybox fuzzer guiado a cobertura de código.
- ▶ **DogeFuzz-DG**: um directed greybox fuzzer guiado por métricas de distância a OPCODEs perigosos.

Descrição da estratégia guiada a cobertura

1. Construir **Control Flow Graph** (CFG) do bytecode do contrato.
2. Coletar dados de execução e de ambiente por meio **instrumentação da EVM**.
3. DogeFuzz-G: mapeia blocos executados em blocos da CFG.

Descrição da estratégia guiada a distância

1. Construir **Control Flow Graph** (CFG) do bytecode do contrato.
2. Coletar dados de execução e de ambiente por meio **instrumentação da EVM**.
3. DogeFuzz-DG: calcular distância para atingir **OPCODEs** perigosos usando o CFG.

Benchmarks

Id	Source	N. of Contracts	Used for
BENCH72	Smartbugs	82 labeled vulnerable	RQ1
BENCH500	Etherscan	500 real and popular	RQ2

RQ1: Comparação do DogeFuzz com outros fuzzers

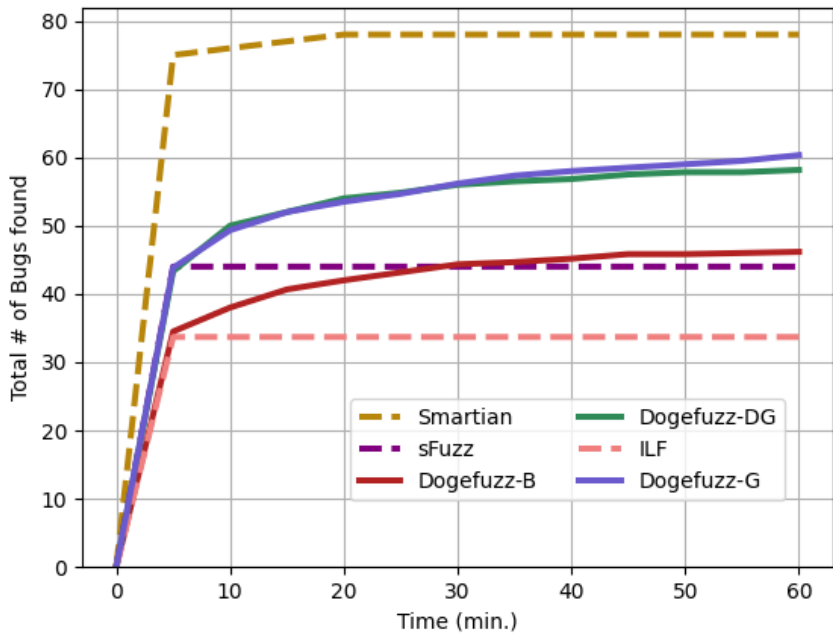
- ▶ 5 execuções de 1h cada por contrato por ferramenta.

RQ2: Avaliação do DogeFuzz em contratos reais

- ▶ 5 execuções de 15m cada por contrato por ferramenta.

Baselines

- ▶ ILF (ML)
- ▶ sFuzz (GA)
- ▶ Smartian (DFA)
- ▶ DogeFuzz



Resultados RQ1

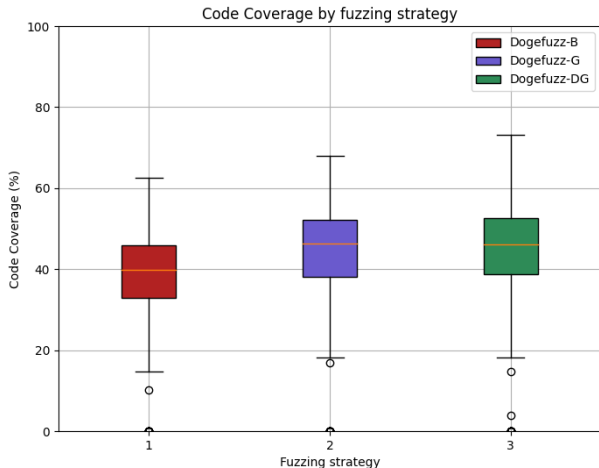
RQ1: Matriz de avaliação de desempenho



	TP	FP	FN	Precision	Recall	F_1 score
BlockDependency						
ILF	5	0	8	1	0.38	0.56
sFuzz	10	0	3	1	0.77	0.87
Smartian	11	0	2	1	0.85	0.92
Dogefuzz-G	9	1	4	0.90	0.69	0.78
Dogefuzz-DG	9	1	4	0.90	0.69	0.78
Dogefuzz-B	8	0	5	1	0.62	0.76
MishandledException						
ILF	11	0	39	1	0.22	0.36
sFuzz	29	6	21	0.83	0.58	0.68
Smartian	48	0	2	1	0.96	0.98
Dogefuzz-G	39	9	11	0.81	0.78	0.80
Dogefuzz-DG	35	7	15	0.83	0.70	0.76
Dogefuzz-B	31	4	19	0.89	0.62	0.73
Reentrancy						
ILF	18	2	1	0.90	0.94	0.92
sFuzz	5	20	14	0.20	0.26	0.26
Smartian	19	0	0	1	1	1
Dogefuzz-G	16	4	3	0.80	0.84	0.82
Dogefuzz-DG	14	4	5	0.78	0.74	0.76
Dogefuzz-B	7	4	12	0.64	0.37	0.47

Average	ILF	0.96	0.51	0.61
	sFuzz	0.67	0.53	0.59
	Smartian	1	0.93	0.92
	Dogefuzz-G	0.83	0.77	0.80
	Dogefuzz-DG	0.83	0.71	0.76
	Dogefuzz-B	0.84	0.53	0.65

- ▶ DogeFuzz-G e DG: 48%
- ▶ DogeFuzz-B: 40%
- ▶ Smart Contracs 6x maiores que RQ1.



- ▶ Estratégias de fuzzing orientadas por métricas (cobertura e instruções críticas) **demonstram boa efetividade** em relação a estratégias mais complexas.
- ▶ DogeFuzz como **framework moderno para experimentações** de fuzzing de smart contracts.

- ▶ Modelo de sementes baseados em sequências de transações.
- ▶ Incorporação de um *solver* de condições/restrições.
- ▶ Implementação de estratégias multi-objetivos.



Dúvidas?

Obrigado!

Contato:

faustocarva@gmail.com



University of Brasília
Department of Computer Science



DogeFuzz: A Simple Yet Efficient Grey-box Fuzzer for Ethereum Smart Contracts

Ismael Medeiros, Fausto Carvalho, Alexandre Ferreira, Rodrigo Bonifácio, Fabiano Cavalcanti
Fernandes

18/09/2024

Cryptonews • Blockchain News

Ethereum Suffers Most Hacks Among Blockchains in 2024

Ethereum Hacks



Crypto Reporter
Shalini Nagarajan

Last updated:

16 de abril de 2024 às 06:37 BRT

Forbes

FORBES > MONEY > INVESTING

BREAKING

More Than \$600 Million Stolen In Ethereum And Other Cryptocurrencies—Marking One Of Crypto's Biggest Hacks Ever

Jonathan Ponciano Former Staff

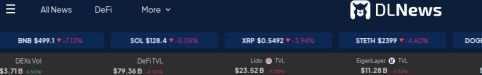
1

Aug 10, 2021, 11:10am EDT

O que é a Hyperledger Besu e por que o BC a escolheu para o Drex

Plataforma blockchain empresarial é baseada em Ethereum

Por Juliana Steil, Valor — São Paulo
07/12/2023 05h03 - Atualizado há 8 meses



BNB	SOL	XRP	STETH	DOGE
\$499.1	\$128.4	\$0.5492	\$2399	
-7.12%	-5.00%	-3.94%	-4.60%	

DEX Vol	DeFiTVL	Lido	Tvl	Spot Layer	Tvl
\$3.71 B	\$79.36 B	\$23.52 B	\$11.28 B		
+60%	+30%	+20%	+10%		

North Korean hackers eye Bitcoin, Ethereum ETFs, FBI warns



Ethereum Statistics - 1st Semester 2024

- ▶ Total Value Locked (TVL) in Ethereum: **\$49B** (56% of the market).
- ▶ TVL in SC implemented in Solidity: **\$126B**.
- ▶ Attacks on the Ethereum Network: **222** attacks **\$315B**.
- ▶ Exploitation of vulnerabilities in SC code: **105** attacks.

Attack Enablers

- ▶ Immutability of Smart Contracts.
- ▶ Possibility of immediate and enormous economic gains.
- ▶ Design weaknesses of the Solidity language.
- ▶ Public and anonymous nature in blockchains.



Resulting from **inadequate programming practices** or **lack of knowledge** about blockchain technology.

Most common types of vulnerabilities:

- ▶ Reentrancy.
- ▶ Mishandled Exception.
- ▶ Integer Overflow and Underflow.
- ▶ Insecure Randomness (Number & Timestamp).



Detection techniques:

- ▶ Static Analysis.
- ▶ Dynamic Analysis (fuzzing)
- ▶ Symbolic Execution.
- ▶ Machine Learning.
- ▶ Formal Verification.



Blockchain can be seen as a transactional system, a state machine.

State of the art in Smart Contracts fuzzing:

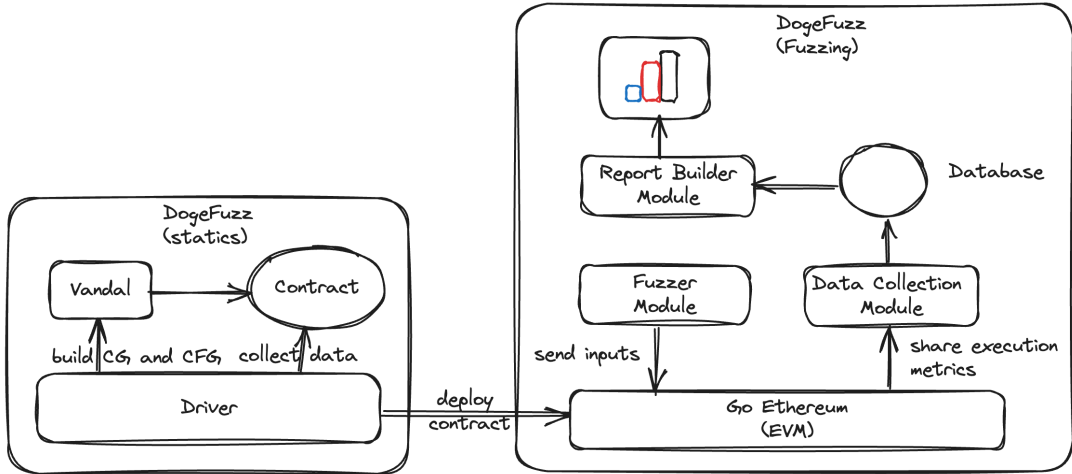
- ▶ Generation of more promising transaction seeds and arguments.
- ▶ Exploration of state context and source code.
- ▶ Lightweight instrumentation of the Ethereum Virtual Machine (EVM).
- ▶ Tools: ILF (ML), sFuzz (GA), Smartian (PA).

DogeFuzz Contributions

1. An extensible open-source infrastructure for experimenting with fuzzing strategies for smart contracts.
2. Experiments demonstrating that simpler fuzzing strategies can outperform state-of-the-art fuzzers.

Proposed Solution

DogeFuzz Architecture



Implemented Fuzzing Strategies

- ▶ DogeFuzz-B: a blackbox fuzzer.
- ▶ DogeFuzz-G: a greybox fuzzer guided by code coverage.
- ▶ DogeFuzz-DG: a directed greybox fuzzer guided by distance metrics to dangerous OPCODEs.

Description of Coverage-Guided Strategy

1. Build Control Flow Graph (CFG) of the contract's bytecode.
2. Collect execution and environment data through EVM instrumentation.
3. DogeFuzz-G: maps executed blocks to CFG blocks.

Description of Distance-Guided Strategy

1. Build Control Flow Graph (CFG) of the contract's bytecode.
2. Collect execution and environment data through EVM instrumentation.
3. DogeFuzz-DG: calculate distance to reach dangerous OPCODEs using the CFG.

Benchmarks

Id	Source	N. of Contracts	Used for
BENCH72	Smartbugs	82 labeled vulnerable	RQ1
BENCH500	Etherscan	500 real and popular	RQ2

RQ1: Comparison of DogeFuzz with other fuzzers

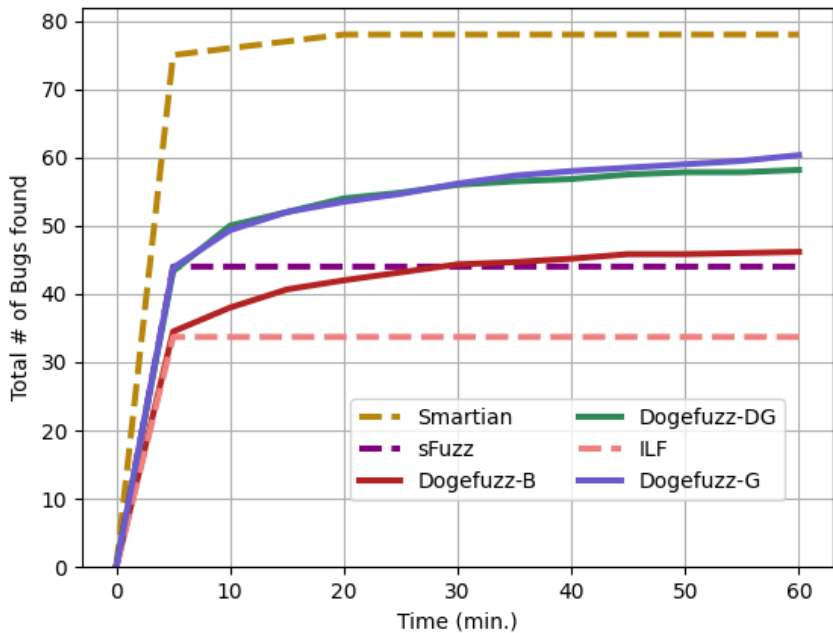
- ▶ 5 runs of 1 hour each per contract per tool.

RQ2: Evaluation of DogeFuzz on real contracts

- ▶ 5 runs of 15 minutes each per contract per tool.

Baselines

- ▶ ILF (ML)
- ▶ sFuzz (GA)
- ▶ Smartian (DFA)
- ▶ DogeFuzz



Results RQ1

RQ1: Performance Evaluation Matrix

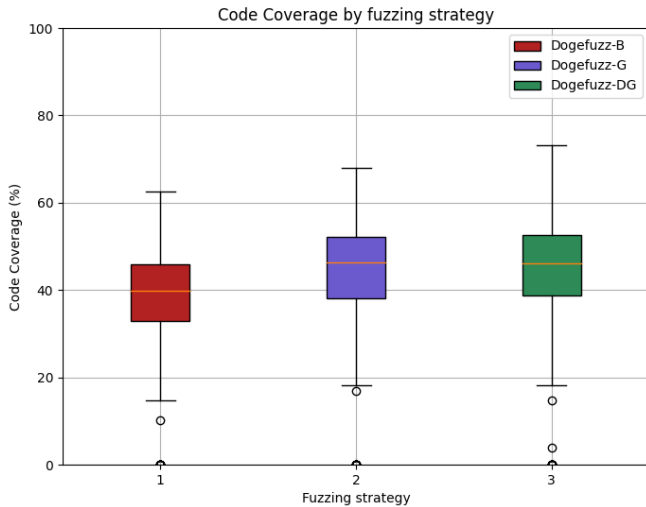


	TP	FP	FN	Precision	Recall	F_1 score
BlockDependency						
ILF	5	0	8	1	0.38	0.56
sFuzz	10	0	3	1	0.77	0.87
Smartian	11	0	2	1	0.85	0.92
Dogefuzz-G	9	1	4	0.90	0.69	0.78
Dogefuzz-DG	9	1	4	0.90	0.69	0.78
Dogefuzz-B	8	0	5	1	0.62	0.76
MishandledException						
ILF	11	0	39	1	0.22	0.36
sFuzz	29	6	21	0.83	0.58	0.68
Smartian	48	0	2	1	0.96	0.98
Dogefuzz-G	39	9	11	0.81	0.78	0.80
Dogefuzz-DG	35	7	15	0.83	0.70	0.76
Dogefuzz-B	31	4	19	0.89	0.62	0.73
Reentrancy						
ILF	18	2	1	0.90	0.94	0.92
sFuzz	5	20	14	0.20	0.26	0.26
Smartian	19	0	0	1	1	1
Dogefuzz-G	16	4	3	0.80	0.84	0.82
Dogefuzz-DG	14	4	5	0.78	0.74	0.76
Dogefuzz-B	7	4	12	0.64	0.37	0.47

Average	ILF	0.96	0.51	0.61
	sFuzz	0.67	0.53	0.59
	Smartian	1	0.93	0.92
	Dogefuzz-G	0.83	0.77	0.80
	Dogefuzz-DG	0.83	0.71	0.76
	Dogefuzz-B	0.84	0.53	0.65

Results RQ2

RQ2 Large-Scale Performance Coverage



- ▶ Fuzzing strategies guided by metrics (coverage and critical instructions) show good effectiveness and have similar rates.
- ▶ DogeFuzz as a modern framework for smart contract fuzzing experiments.

1. Seed models based on transaction sequences.
2. Incorporation of a constraint solver.
3. Implementation of multi-objective strategies.



Questions?

Thanks!

E-Mail:

faustocarva@gmail.com