Disciplina sobre Blockchain

Arlindo F. da Conceição (arlindo.conceicao@unifesp.br)

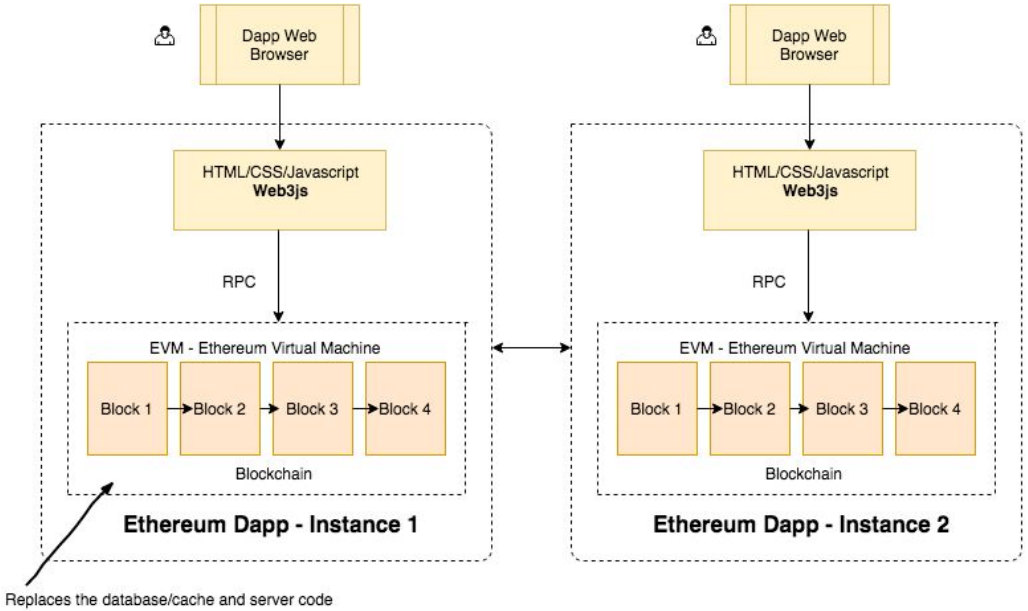
Mais sobre contratos inteligentes

O crescimento do GAS é não linear

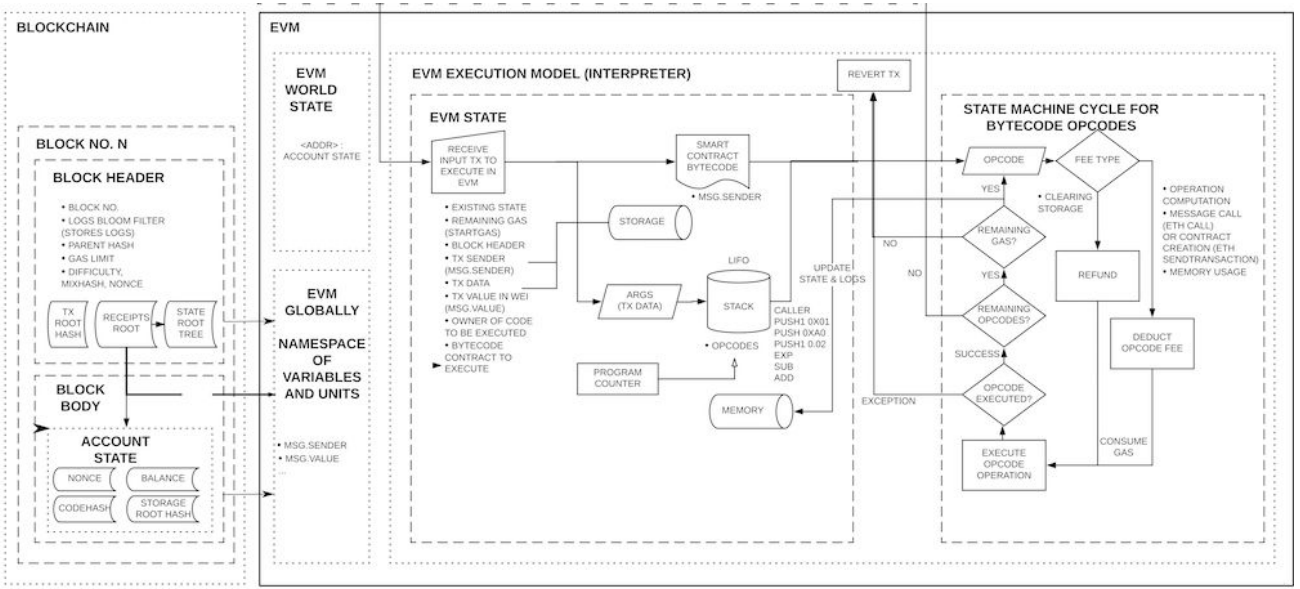
Erro: Contract code size exceeds 24576 bytes

Arquitetura Ethereum

https://medium.com/@mvmurthy/ethereum-for-web-developers-890be23d1d0c



Arquitetura da EVM



Fonte: https://fullstacks.o

UNIFESP
Universidade Federal de São Paulo
1933

Problemas

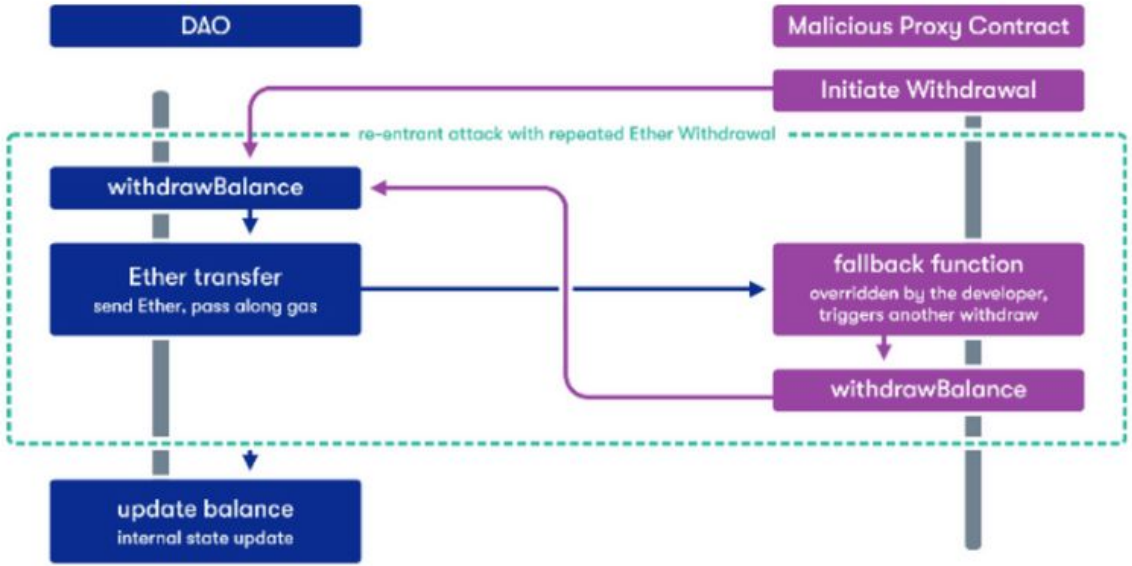
Verification of smart contracts: A survey

Mouhamad Almakhour [a,b,*], Layth Sliman [c], Abed Ellatif Samhat [b], Abdelhamid Mellouk [a]

- Verificação formal
  - Mas a especificação precisa estar certa!
- Teste de vulnerabilidades
  - Reexecução
  - *Overflow* de inteiros
  - Endereço errado
  - Código morto

UNIFESP
UNIVERSIDADE FEDERAL DE SÃO PAULO
1933

Reentrância



Fonte: https://quantstamp.com/blog/what-is-a-re-entrancy-attack

Ferra-mentas

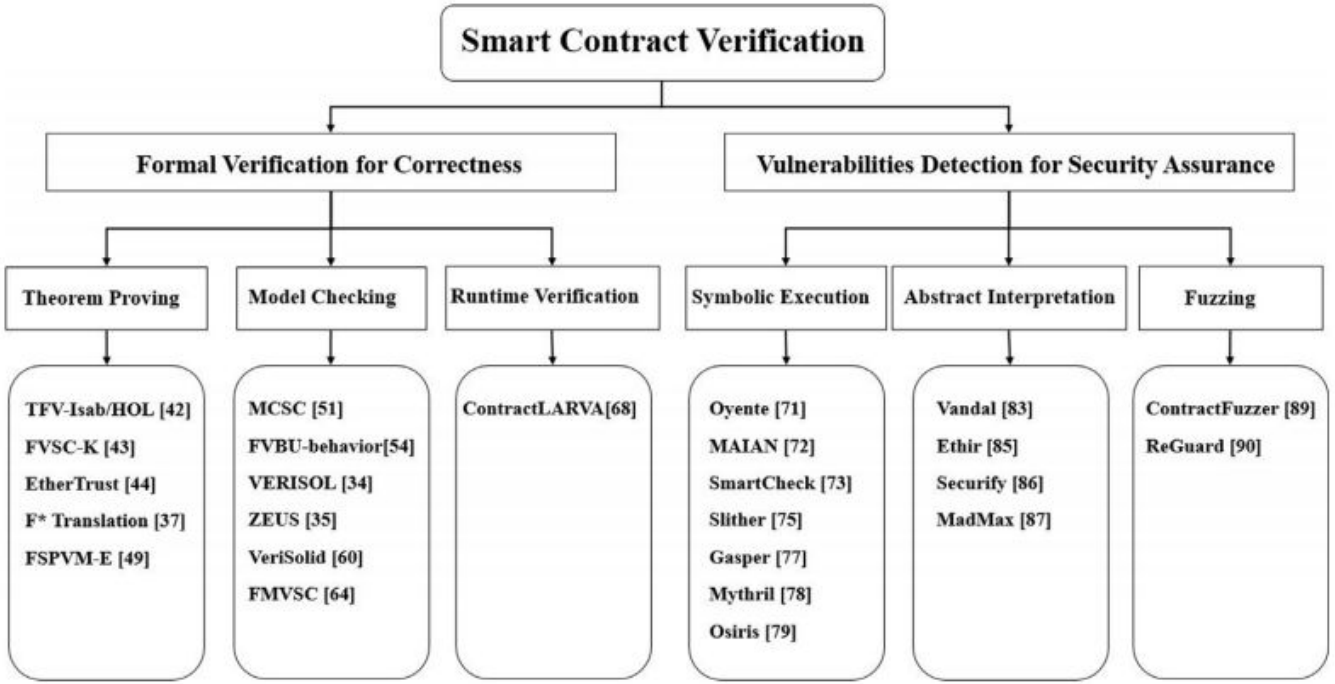


Fig. 1. Taxonomy of the smart contract verification's tools.

Ethereum

- https://www.ethernodes.org/network/1

Projetos

- Pitch de projetos:
- Grupos de 03 estudantes
  - Preencher e manter atualizado: https://docs.google.com/spreadsheets/d/1tbDra87Cdpzqnec4ho2OtUaRzY1AyfxT00RVmqHzrsE/edit?usp=sharing
- Apresentação do projeto em **10m + 5m de perguntas**
  - Problema
  - Por que Blockchain é necessário? (Indispensável?)
    - Qual Blockchain usou? Por que?
  - Solução
  - Benefícios
  - Demo
- Documentação do projeto em um site e código no github

- Apresentações de 29/05 a 24/06