CHI23 Late-Breaking Work

Code Will Tell: Visual Identification of Ponzi Schemes on Ethereum

Xiaolin Wen[1,2] wenxiaolin@stu.scu.edu.cn
Kim Siang Yeo[2] ks.yeo.2021@mitb.smu.edu.sg
Yong Wang[2] yongwang@smu.edu.sg
Ling Cheng[2] lingcheng.2020@phds.smu.edu.sg
Feida Zhu[2] fdzhu@smu.edu.sg
Min Zhu[1] zhumin@scu.edu.cn

1. Sichuan University
2. Singapore Management University

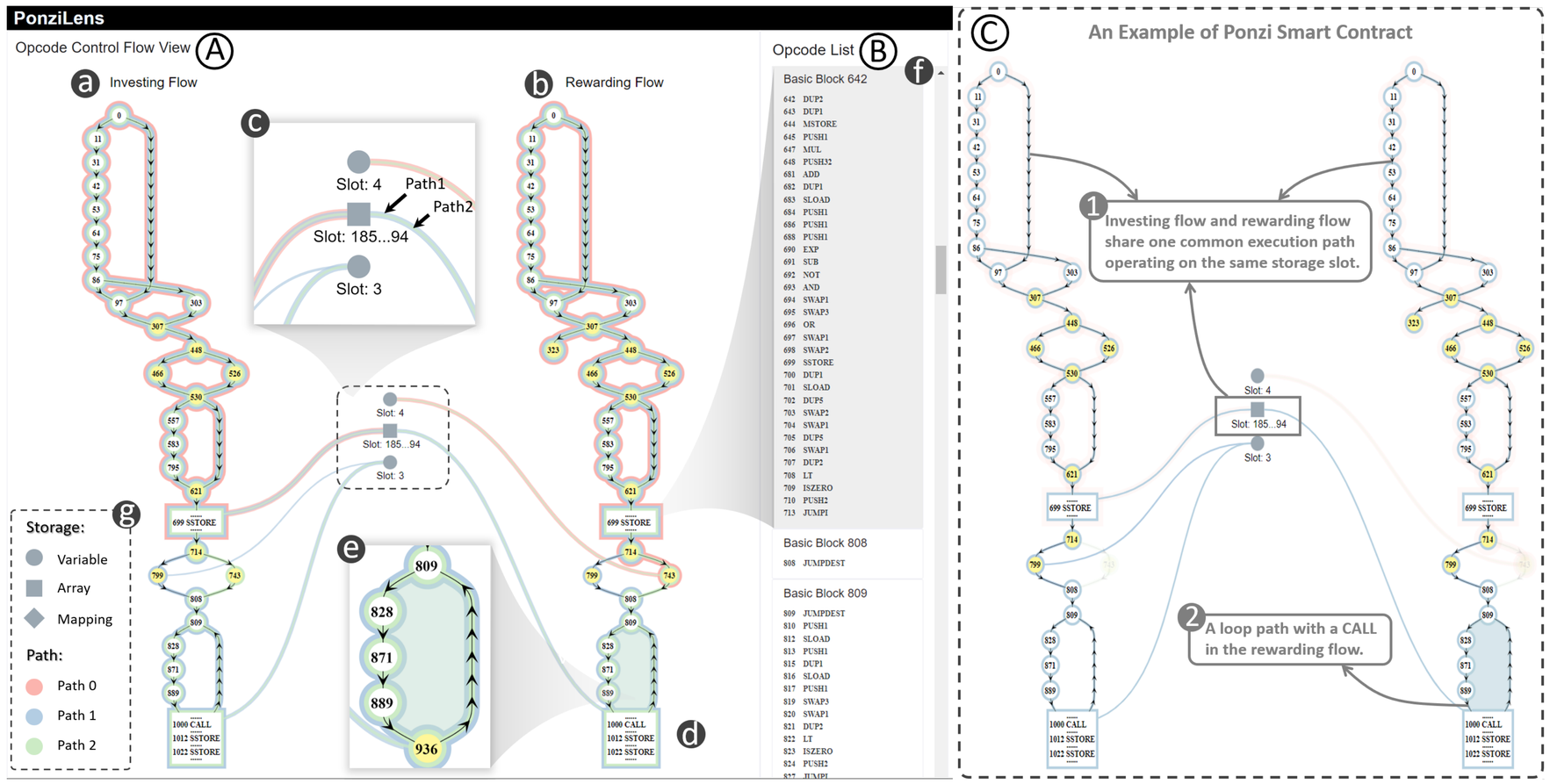
Motivation

- Due to the decentralization and anonymity of Ethereum, Ponzi schemes have been easily deployed and caused significant losses to investors.
- However, there are still no explainable and effective methods to help investors easily identify Ponzi schemes and validate whether a smart contract is actually a Ponzi scheme.
- We propose ***PonziLens***, a novel visualization approach to help investors achieve early identification of Ponzi Schemes by investigating the operation codes of smart contracts.

Feature of Ponzi Scheme

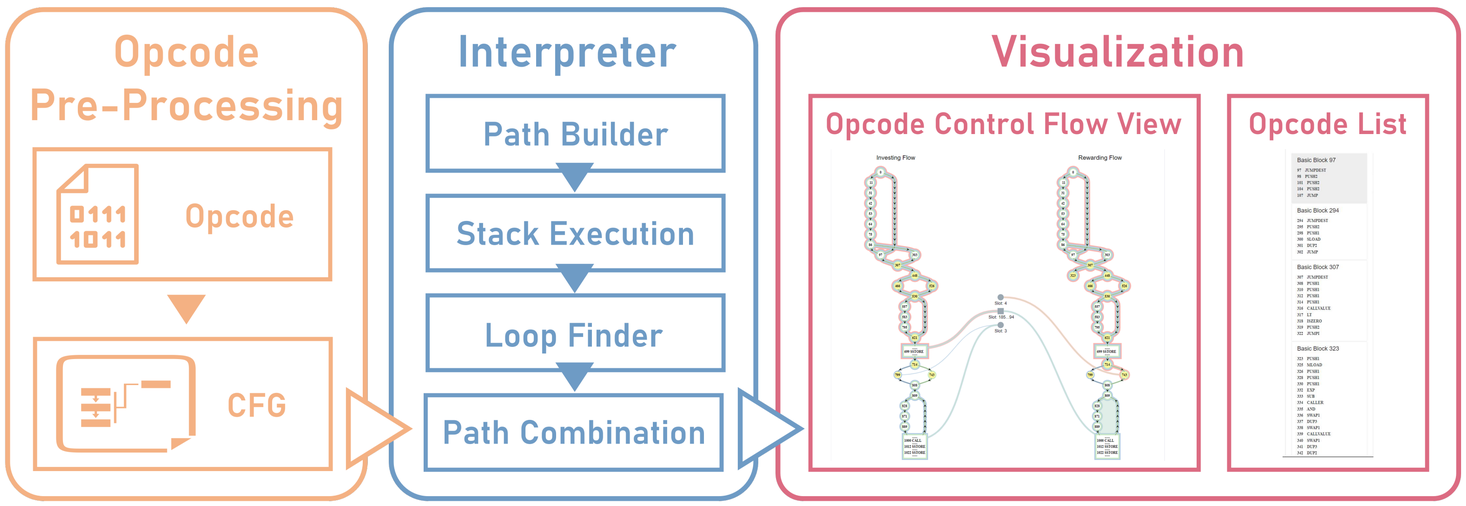
1. Investing flow and rewarding flow share one common execution path operating on the same storage slot.
2. A loop during rewarding for cases where ether is returned to more than one past investor.

PonziLens: A visualization tool to achieve early detection of Ponzi Schemes on Ethereum



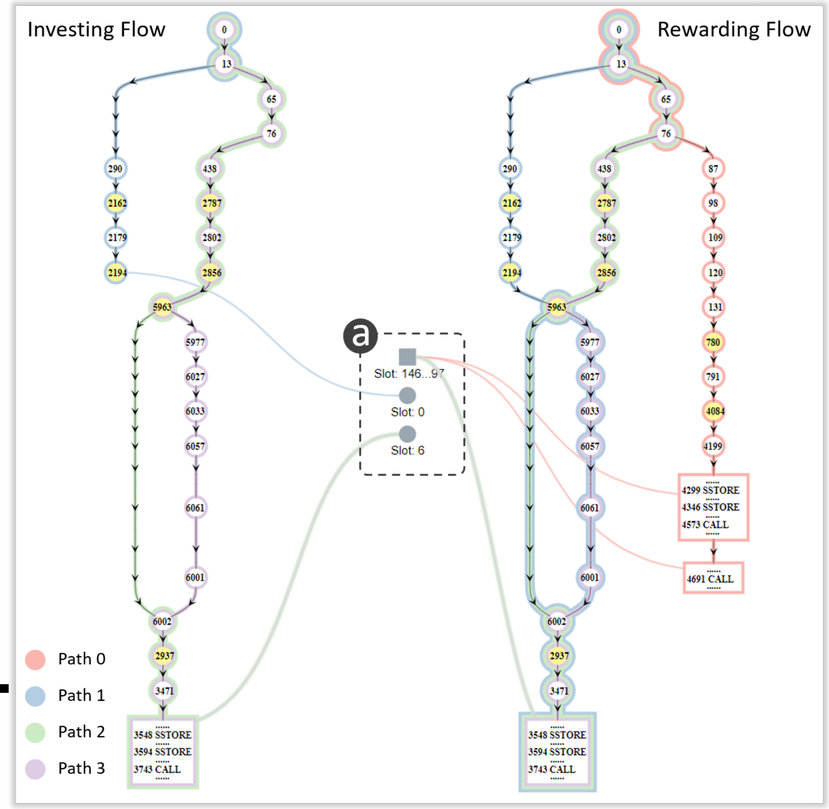
The user interface of PonziLens consists of (A) Opcode Control Flow View and (B) Opcode List. (A) The Opcode Control Flow View shows (a) investing flow, (b) rewarding flow, and (c) storage interactions — all of which are critical for identifying a Ponzi smart contract. (B) The Opcode List shows all the original operation codes of a smart contract, where the operation code of a basic block can be highlighted (f). (d) shows that a basic code block in control flow can be unfolded to check the critical instructions within it. (e) shows an execution loop within a CALL instruction. (g) is the legend illustrating the storage type and the aggregated paths. (C) shows the Opcode Control Flow View with the aggregated path in blue Path1 highlighted.

Pipeline of PonziLens



The architecture of PonziLens consists of three modules: opcode pre-processing, interpreter, and visualization.

An Example of Non-Ponzi Smart Contract



The opcode control fow of EthPledge, a smart contract for charity. PonziLens shows the investing fow and the rewarding fow, as well as their interactions with storage slots (a). The execution paths involved in the investing and rewarding fows use diferent storage slots, indicating that investments cannot be transferred to prior investors, so this smart contract is NOT a Ponzi scheme.