DASFAA 2025

NTU VIDA

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

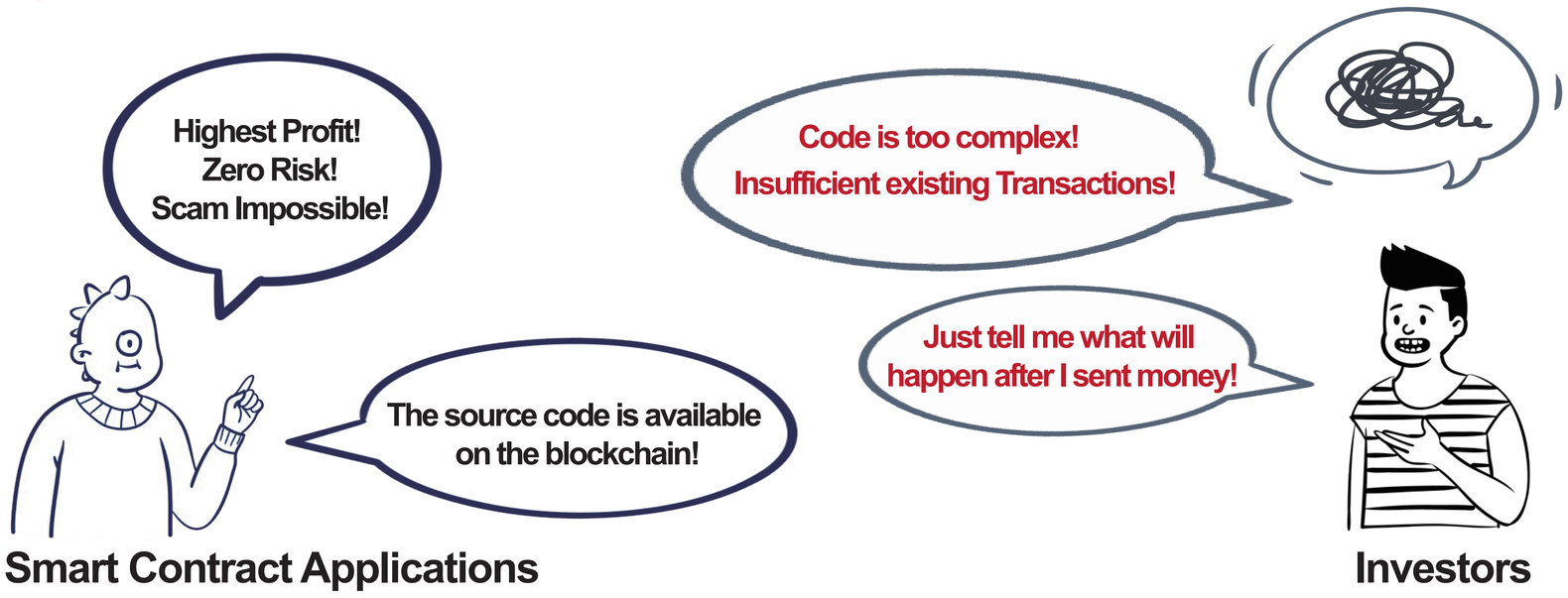
SINGAPORE MANAGEMENT UNIVERSITY

GOPLUS

PrettiSmart: Visual Interpretation of Smart Contracts via Simulation

Xiaolin Wen xiaolin004@e.ntu.edu.sg
Tai D. Nguyen dtnguyen.2019@smu.edu.sg
Lun Zhang allen@gopluslabs.io
Jun Sun junsun@smu.edu.sg
Yong Wang yong-wang@ntu.edu.sg

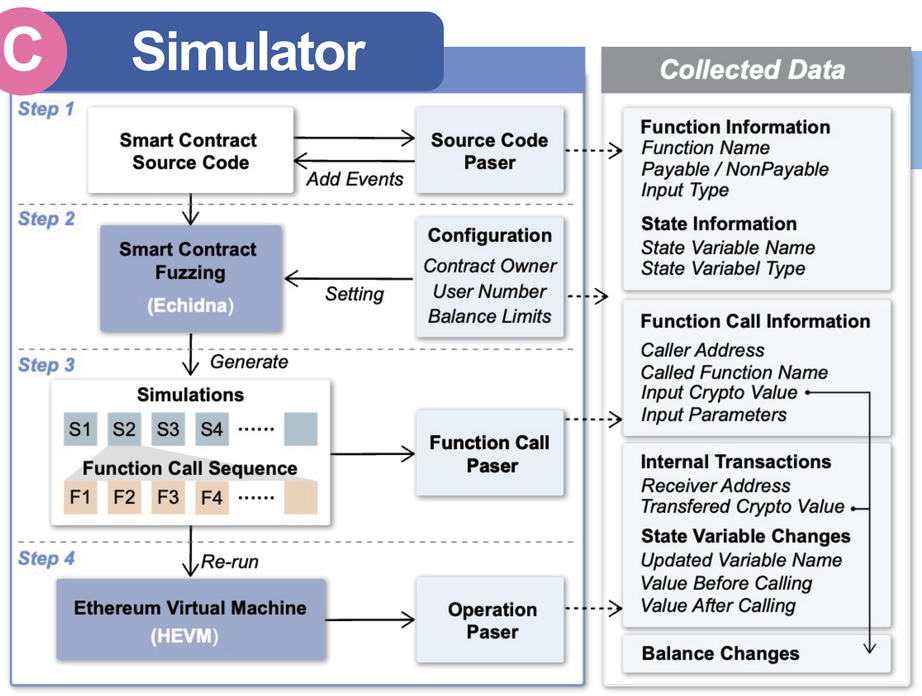
A Motivation — Why do we need to visually interpret smart contracts?



B Contribution

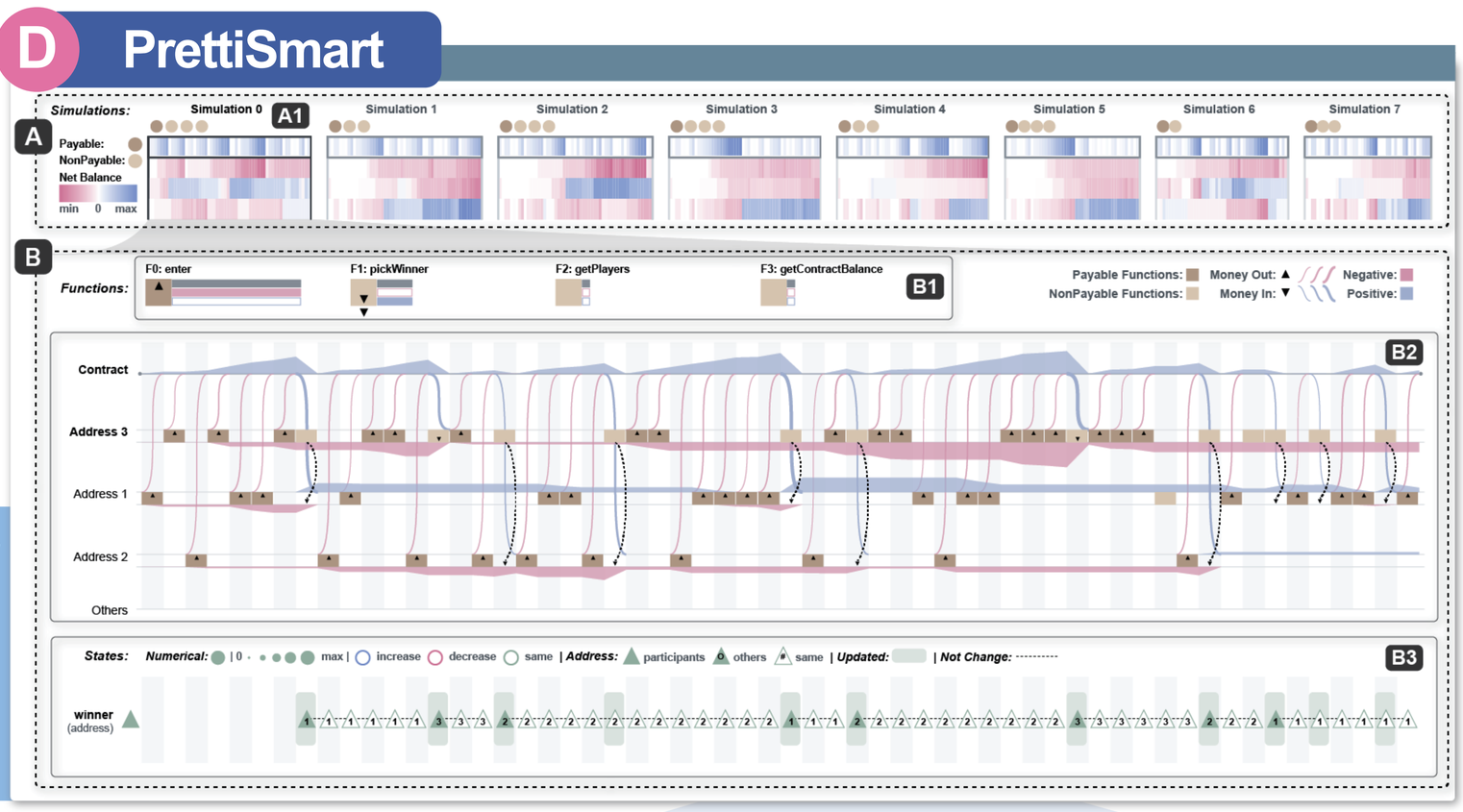
1. **Design Requirements** for visually interpreting smart contracts, through collaboration with six domain experts.
2. **Smart Contract Simulator** capable of simulating real-world scenarios in which multiple smart contract users invoke various functions.
3. **PrettiSmart**, a novel interactive visual analytic system that enables intuitive visual interpretation of smart contracts.
4. **Case Studies** and in-depth **User Interviews** with 12 cryptocurrency investors to demonstrate the effectiveness and usability of PrettiSmart.

C Simulator



The simulator framework (A) consists of four steps: source code parsing, fuzzing configuration, function call parsing, and operation parsing. (B) shows the collected data for the visualizations.

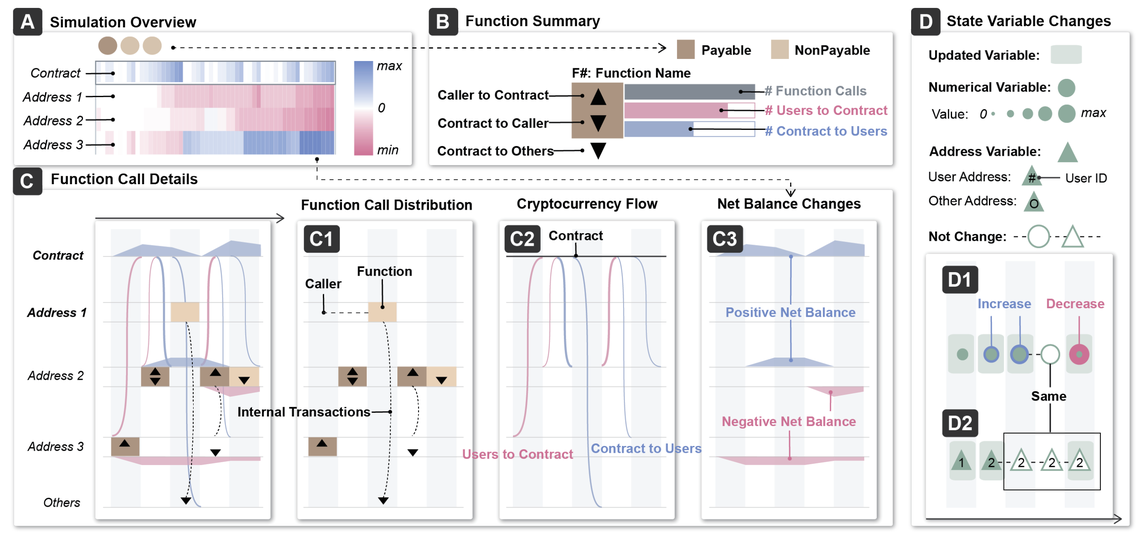
D PrettiSmart



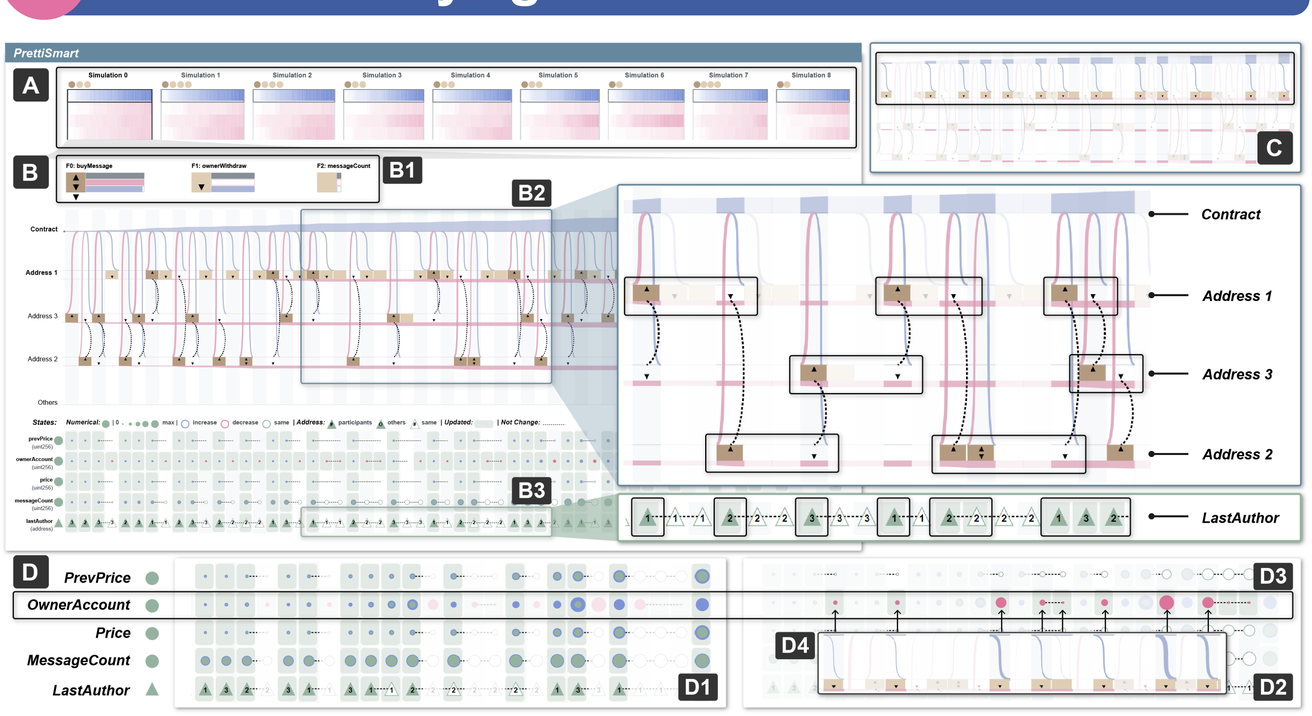
The interface of PrettiSmart consists of a Simulation Overview Module (A) to provide a visual summary for each simulation (A1) generated by our simulator and a Simulation Detail Module (B) to show the details of each simulation, including the Function Summary (B1), the Function Call Details involving cryptocurrency flows and balance changes (B2), and State Variable Changes (B3).

This smart contract could be a Ponzi scheme fraud! All simulated users have a negative net balance (losing money), the chain-like internal transactions resemble a hand-over Ponzi scheme, and the owner can steal funds through a function.

E Visual Design



F Case: Identifying a Fraudulent Smart Contract



Welcome to Discuss !!!

Paper Link

Project Page

VIDA Lab