Temporal Specification and Verification of Smart Contracts

Yuandong Cyrus Liu

Grinnell College • MAP

February 1, 2024

What is smart contract?

[a]

- Trust of the third party like banks.
- Lawyers, ambiguous.

- Trust of protocols.
- Correctness of the code.
- Bugs.

[a] https://www.linkedin.com/pulse/smart-contracts-vs-traditional-utkarsh-dhawan/

Research problems

How to specfiy temporal behaviors with formal logic?

- Understand temporal logic and formal specification.
- Extend the specification language.

How to verify the temporal properties automatically?

- Write temporal formulae for smart contract properties (modeling security concerns).
- Extend exsiting verification tools to verify temporal properties of smart contracts.

Outcomes

Intersection of theory and practical.

Deliverables

- Literature reviews and experiments.
- Develop temporal specification language for smart contracts.
- Model smart contract temporal behaviors.

Final Demonstration

- Public presentation in CS research symposium and international conferences (PLDI, POPL, ICFP).
- Software Artifact that can parse and prove temporal properties of smart contracts (built on top open source tools).

Requirements

what should I have?

- Math skills: formal logic and proofs (CSC 208, CSC 218).
- Programming: data structure (CSC 207), JAVA.
- Passion: open to challenges and curious about why it works or not.

I'm still not sure...

- Take some tasks here, 2 exercises from each chapter of the first 3 chapters.
  (https://softwarefoundations.cis.upenn.edu/lf-current/toc.html),
- Bring your solutions, let's discuss! (liuyuan@grinnell.edu)

Q & A