Automated Support for Writing High-Assurance Smart Contracts

Carnegie Mellon University

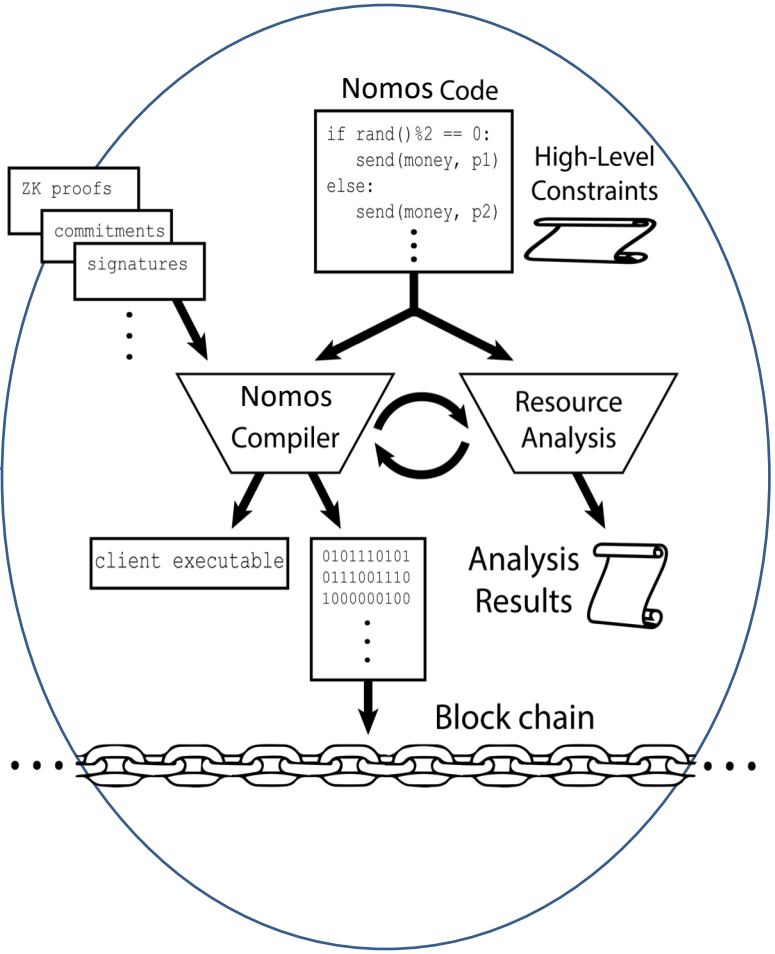
ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Smart Contract Challenges:

- Difficult prog. model
  - Distributed execution
  - Need for complex crypto
- Resource usage costs
- Incentives

Solution:

- New contract prog. language: NOMOS
- Session types enforce protocols
- Linear type system protects assets



Scientific Impact:

- Designs for blockchain-based:
  - Extractable witness encryption [PKC'22]
  - One-round, async. MPC [TCC'21]
- Tranparency dictionaries [NDSS'22]
- Central moment analysis [PLDI'21]
- New frameworks for universal composability [PLDI'19]

...

Broader Impact:

- Influenced design of Facebook's Move language
- Contributions to CS Academy, online HS CS curriculum
- Outreach program to educate HS teachers

Jan Hoffmann (CMU), Andrew Miller (UIUC), Bryan Parno (CMU)

Project #s: 1801369 (CMU) & 1801321 (UIUC)