London Hopper Colloquium 2020
London, UK – 28 October

Formal Methods & The Blockchain

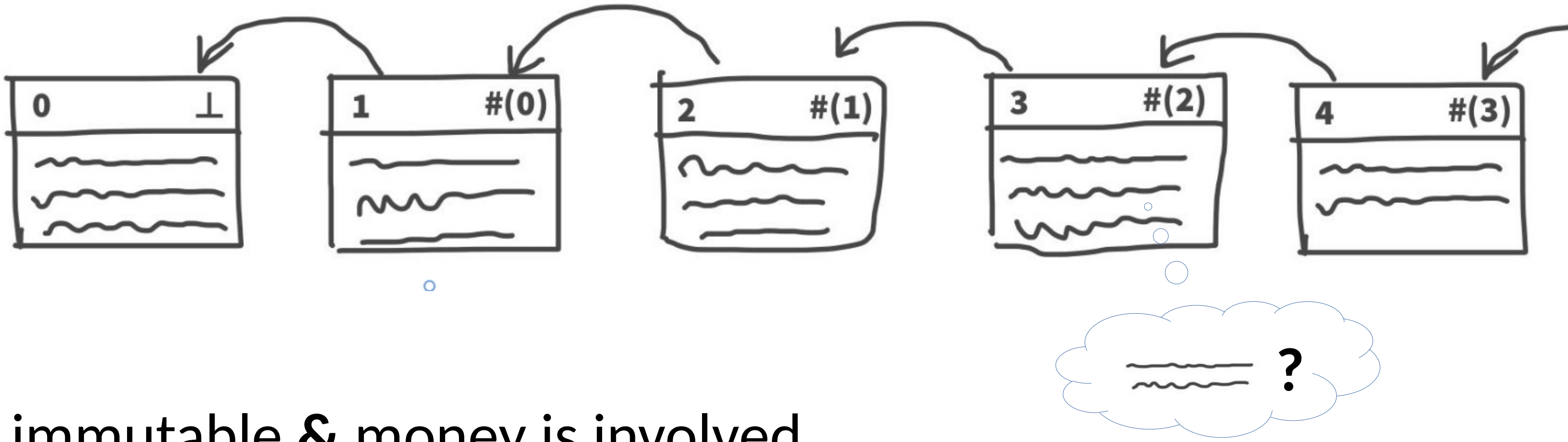
Maria A Schett

3rd year PhD student
University College London

{ mail@} maria-a-schett.net

Problem and Motivation

- **a blockchain:**



transactions or
“smart contracts”

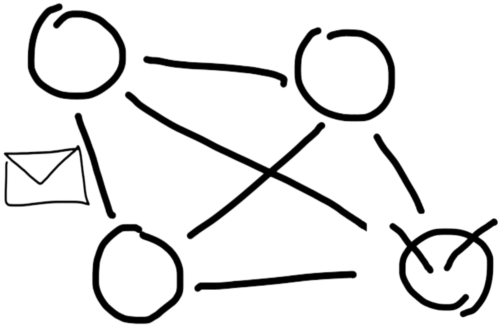
- immutable **&** money is involved
- **expensive** to run

Problem and Motivation (2)

formal reasoning

goal: cost reduction with guarantees

(i) distributed Protocols



goal: min(✉)

(ii) compiler optimizations

executing

costs $$

goal: min(**$$**)

Related Work

(i) distributed Protocols

[1] D. Mazières. “The **Stellar consensus protocol**: a federated model for internet-level consensus”, 2015

[2] G. Danezis & D. Hrycyszyn, “**Blockmania**: from Block DAGs to Consensus”, 2018, arXiv

(ii) compiler optimizations

[3] H. Massalin, “**Superoptimizer**: A Look at the Smallest Program”, ASPLOS, 1987

[4] A. Jangda & G. Yorsh, “**Unbounded Superoptimization**”, Proc. Onward! 2017

[5] “**Ethereum**: A Secure Decentralised Generalised”, Transaction LedgerTechnical Report Byzantium Version e94ebda

Approach and Uniqueness

(i) distributed Protocols

- pen & paper proof of **correctness** □

goal: min(✉)

(ii) compiler optimizations

- case study on Ethereum bytecode
- **SMT/OMT** solver
- rule extraction

goal: min(**$$**)

Results and Contributions

(i) distributed Protocols

1. show correctness of **Stellar** consensus $\mathcal{P}$ with infinite ✉

2. show refinement to $\mathcal{P}$ with finite ✉ [6]

(ii) compiler optimizations

ebso Ethereum bytecode superoptimizer [7]

syrup synthesize optimized Ethereum bytecode [8]

ppltr generate optimization rules [9]

Future Work

(i) distributed $\mathcal{P}$rotocols

show **Blockmania** approach

of interpreting $\mathcal{P}$

on block**graph**

reduces the sent ✉

(work in progress)

(ii) compiler optimizations

- optimize optimization
- optimize other bytecode
- integrate in compiler

References

Thank you!
{mail @} maria-a-schett.net

[6] Á. García-Pérez & M. A. Schett, “**Deconstructing Stellar Consensus**”, OPODIS 2019

[7] J. Nagele & M. A. Schett. “**Blockchain Superoptimizer**”, preproc LOPSTR 2019

[8] E. Albert, P. Gordillo, A. Rubio, M. A. Schett . “**Synthesis of Super-Optimized Smart Contracts using Max-SMT**”, CAV, 2020

[9] M. A. Schett & J. Nagele. “**Populating the Peephole Optimizer of a Smart Contract Compiler**”, FMBC, 2020