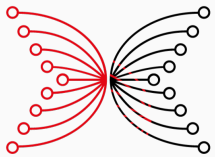
1st-year PhD Report

Orestis Melkonian

July 16, 2020

THE UNIVERSITY *of* EDINBURGH



INPUT | OUTPUT

Introduction

Motivation

- Smart contract vulnerabilities lead to dramatic monetary losses (cf. DAO attack)
- Hence the need to make sure contract behaviour is provably correct/safe
- Chains are immutable → need to provide guarantees statically
- Formal verification to the rescue!
- Relatively few mechanised results thus far

Research Questions

- A mechanisation of the soundness of the BitML compiler
  - Encoded in constructive type theory
  - Mechanised in the Agda proof assistant
  - EXTRA: Hope to distil general principles for the mechanisation of compilation correctness proofs across application domains
- A theoretical basis for conducting meta-theory of UTxO-based blockchain models
  - Relative expressiveness of the (E)UTxO accounting model
  - Allow reasoning about smart contracts and verifying their properties

Methodology

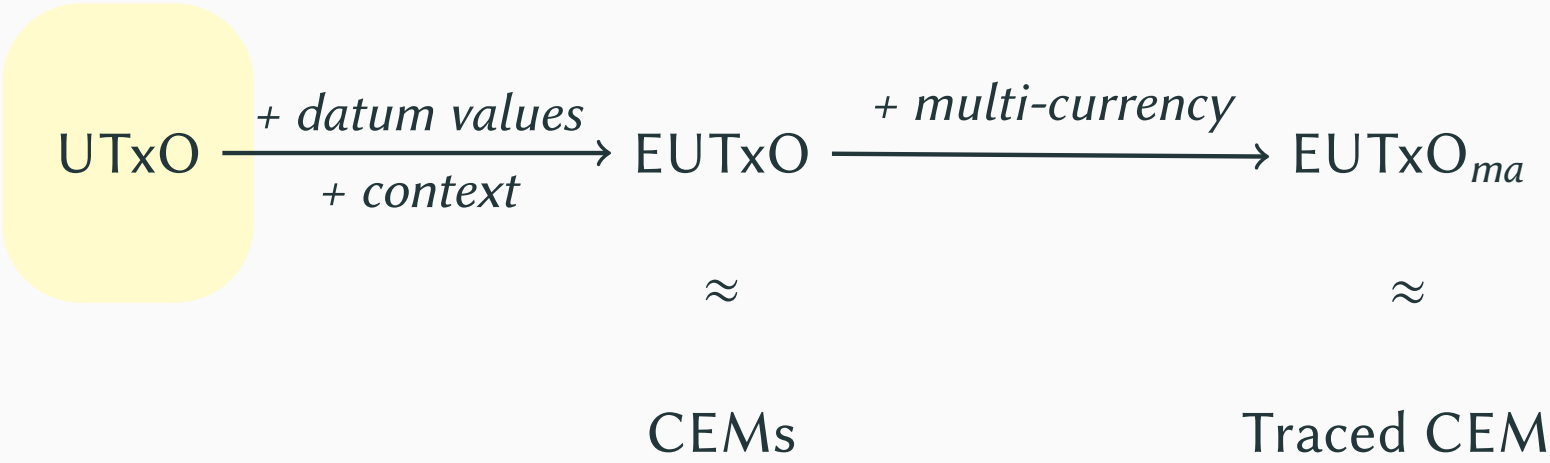
MSc in Utrecht

MSc Thesis

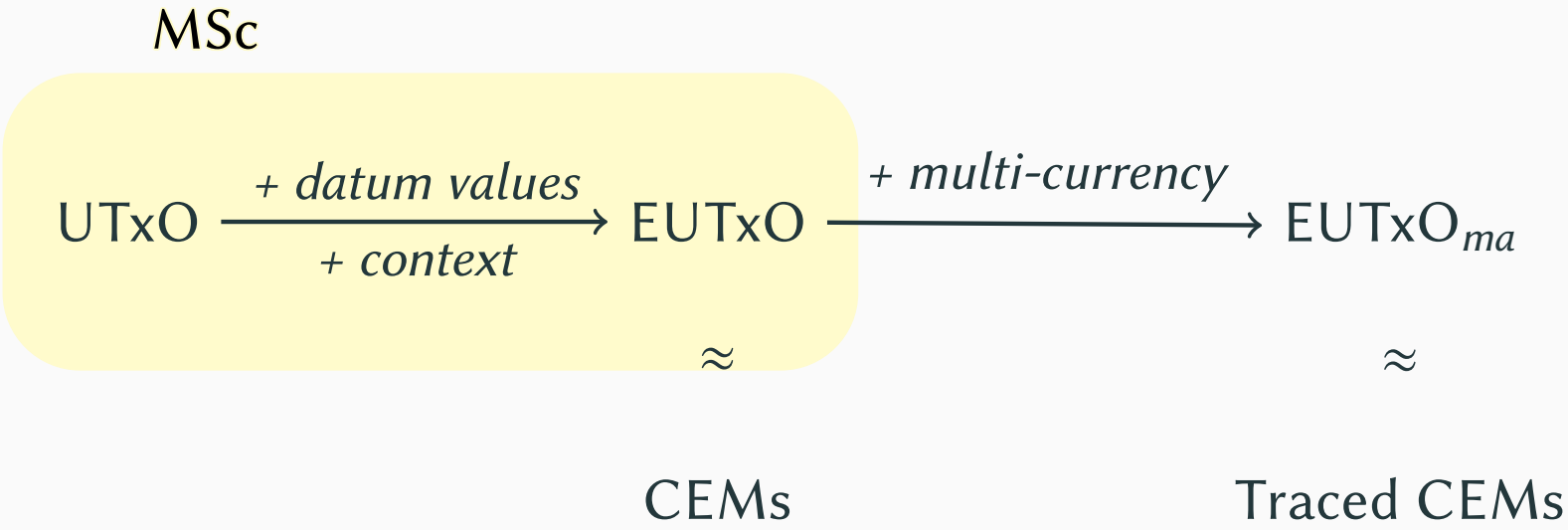
- Under the supervision of
  - Wouter Swierstra (Utrecht University)
  - Manuel Chakravarty (IOHK)
- Two objects of study:
  1. The *Bitcoin Modelling Language (BitML)* and its compilation to Bitcoin transactions
  2. The ***Extended*** *UTxO Model*, as designed for the Cardano blockchain

UTXO [2018-2019]

MSc



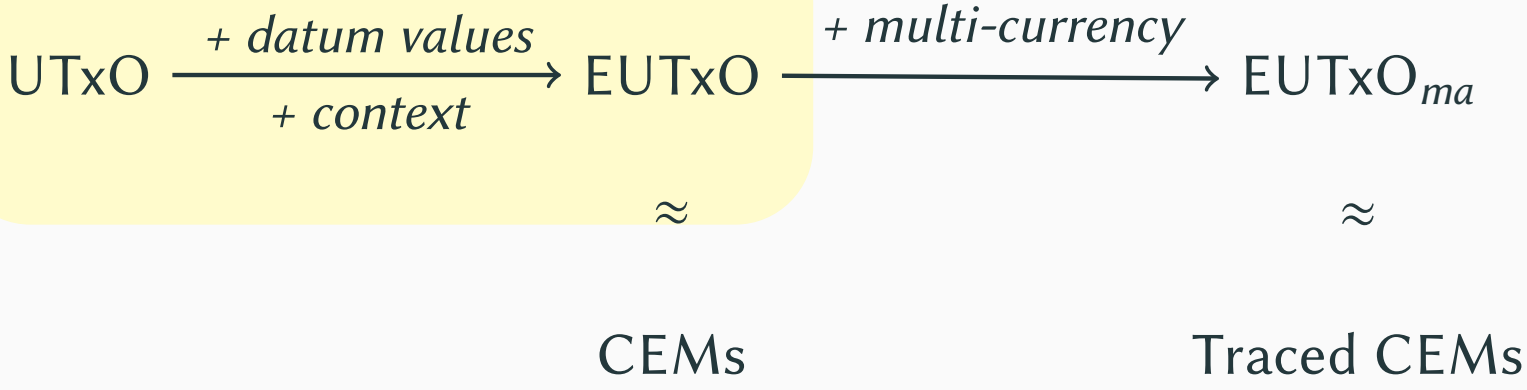
UTXO [2018-2019]



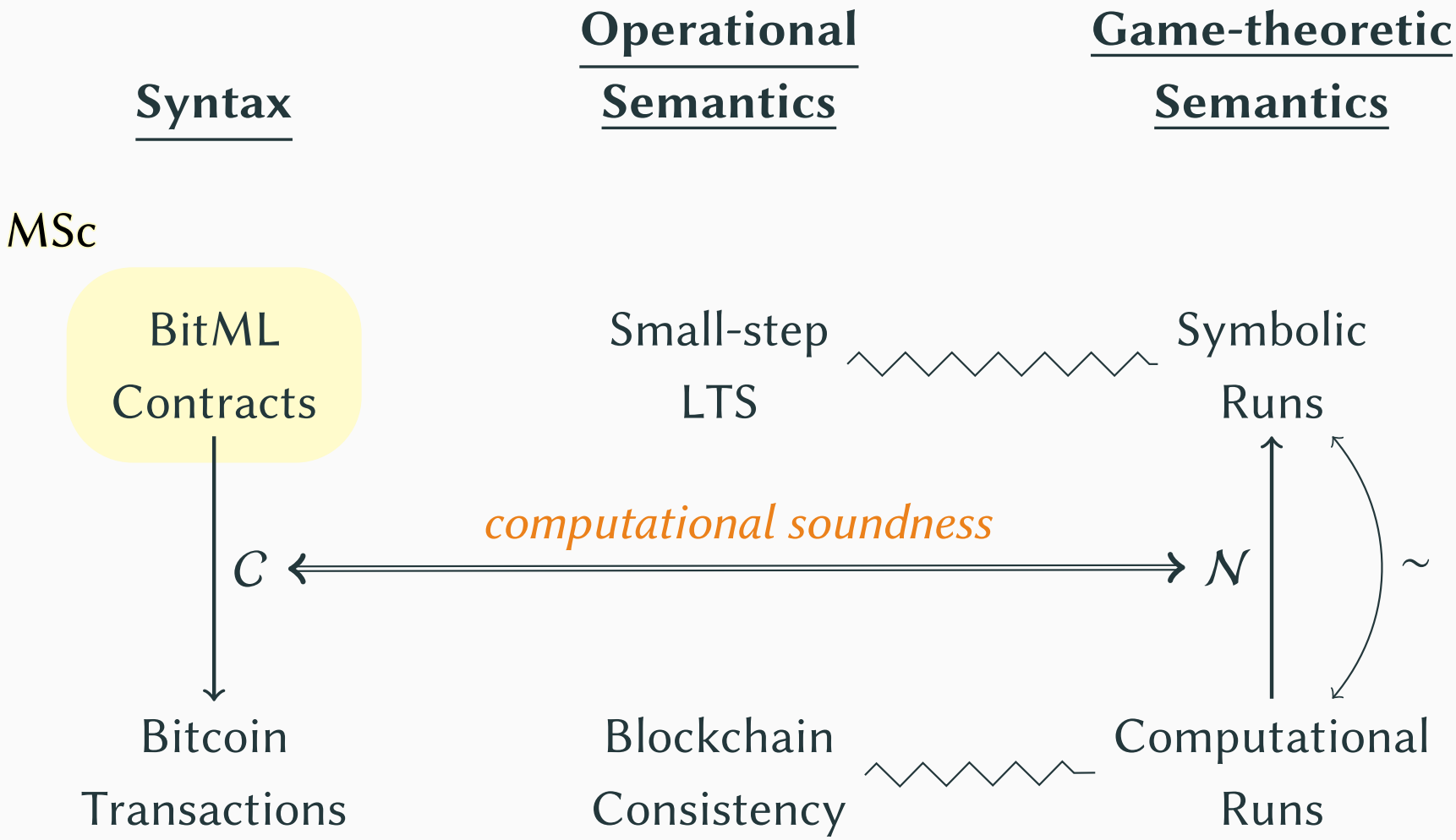
UTXO [2018-2019]

TyDe @ ICFP: *Formal investigation of the Extended UTxO model*

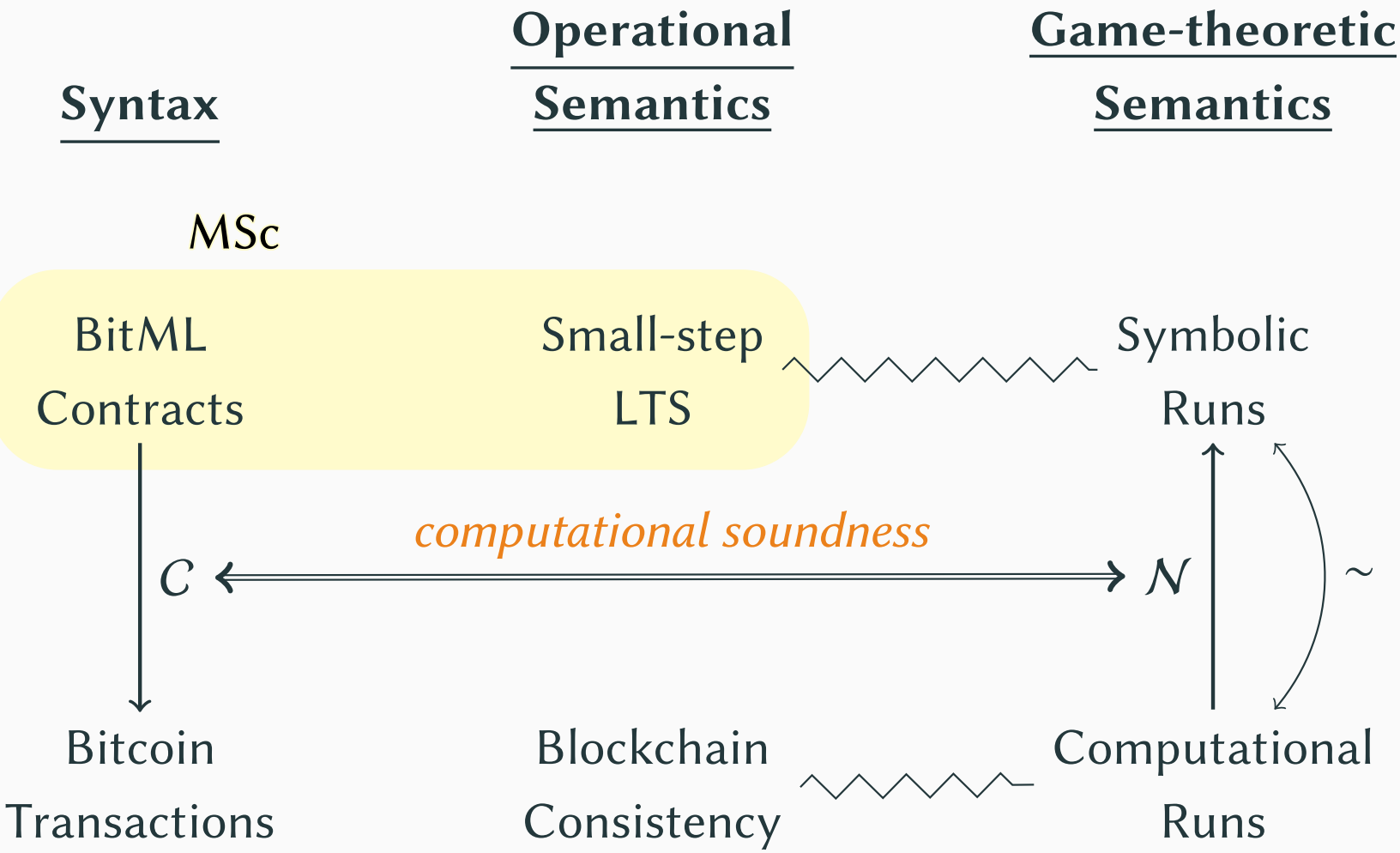
MSc



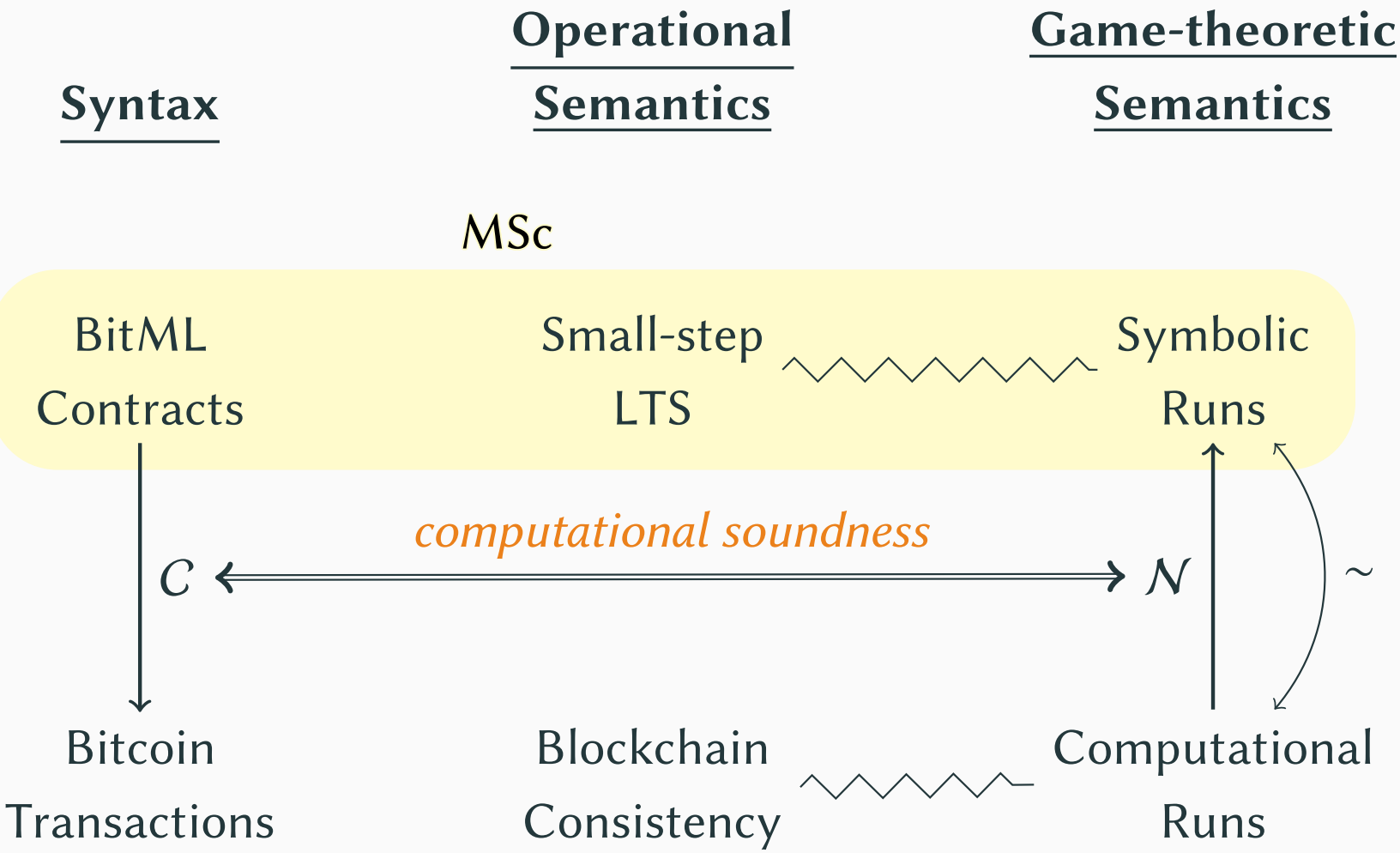
BitML [2018-2019]



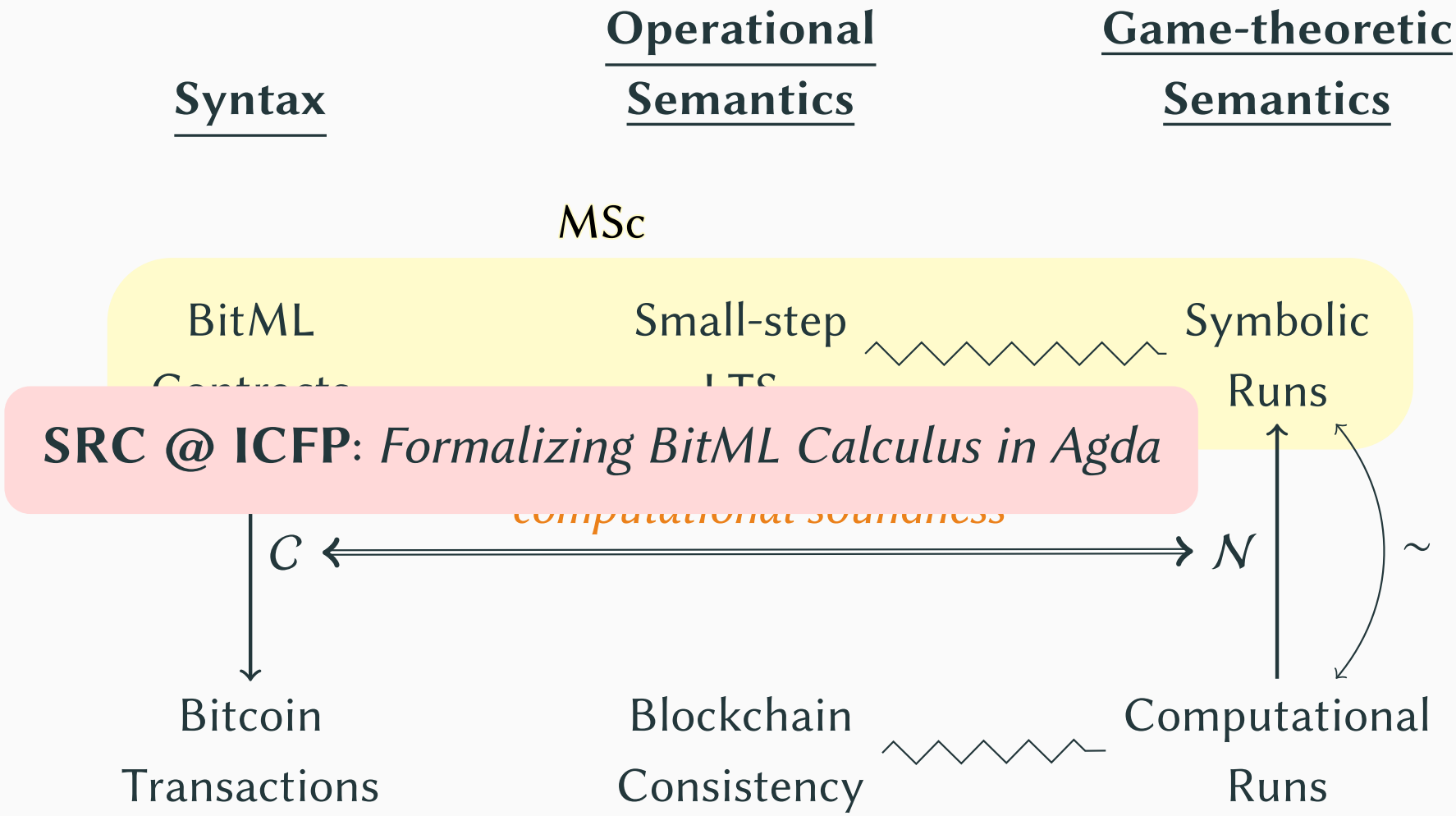
BitML [2018-2019]



BitML [2018-2019]

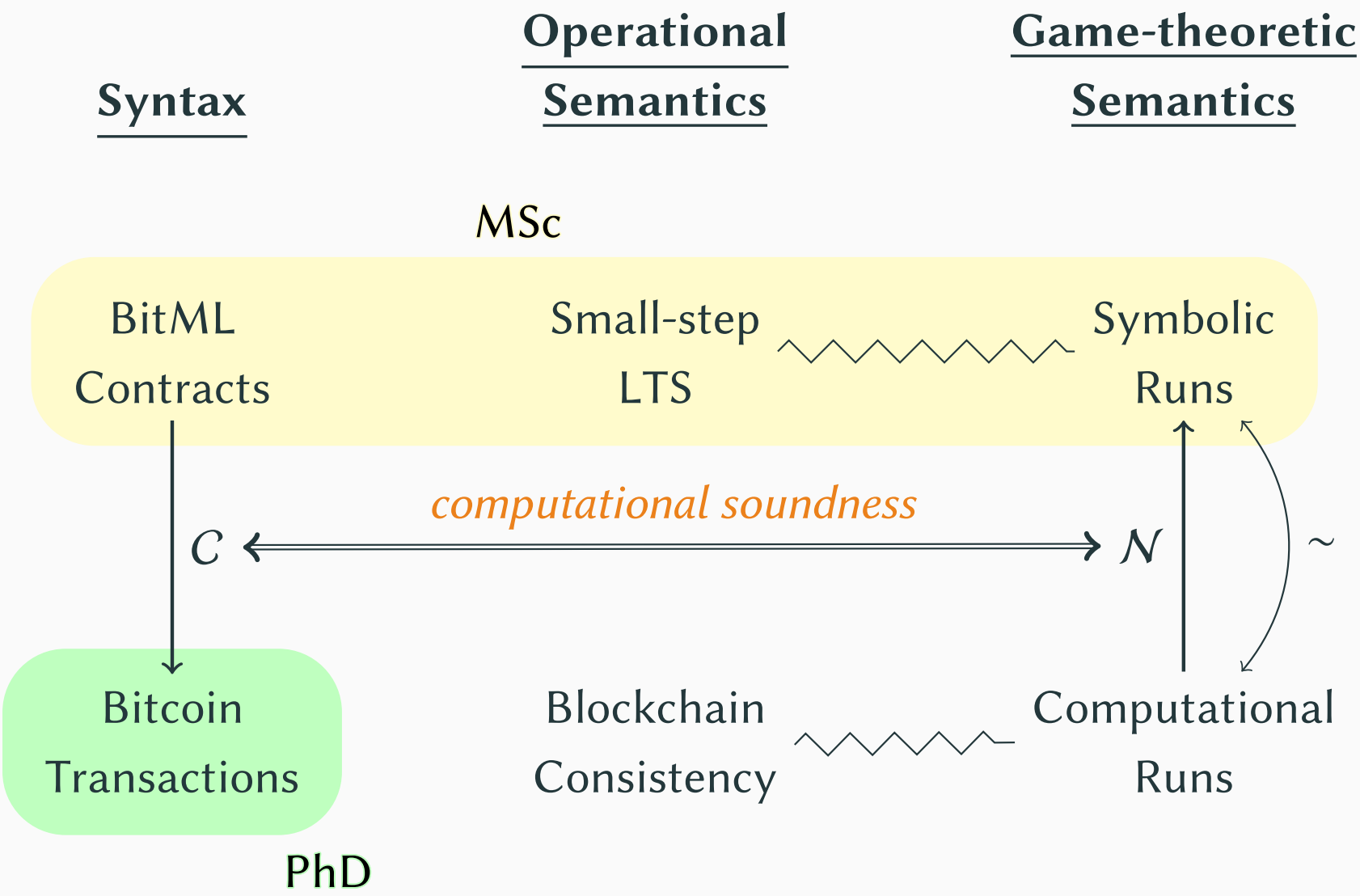


BitML [2018-2019]

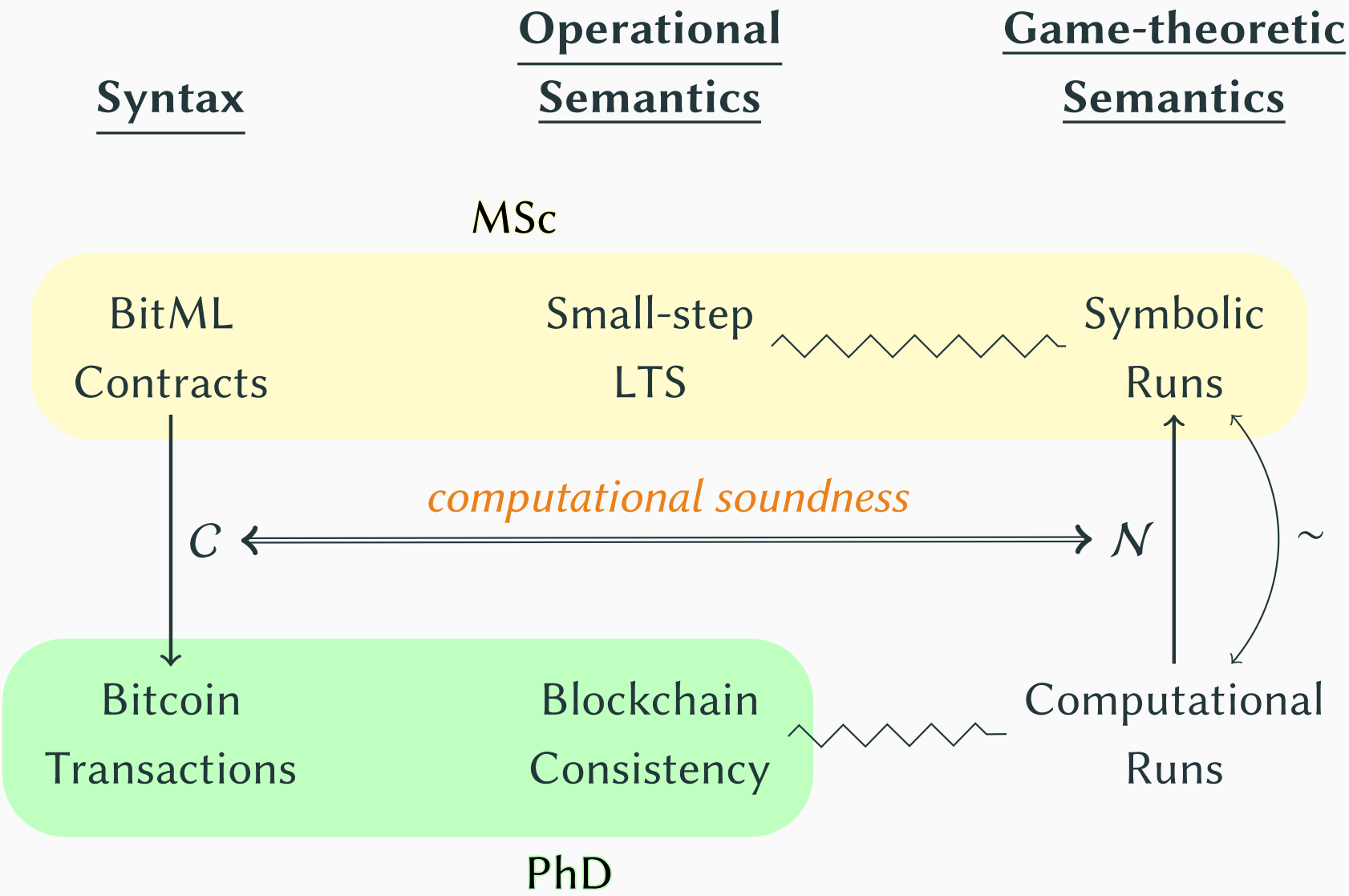


PhD in Edinburgh

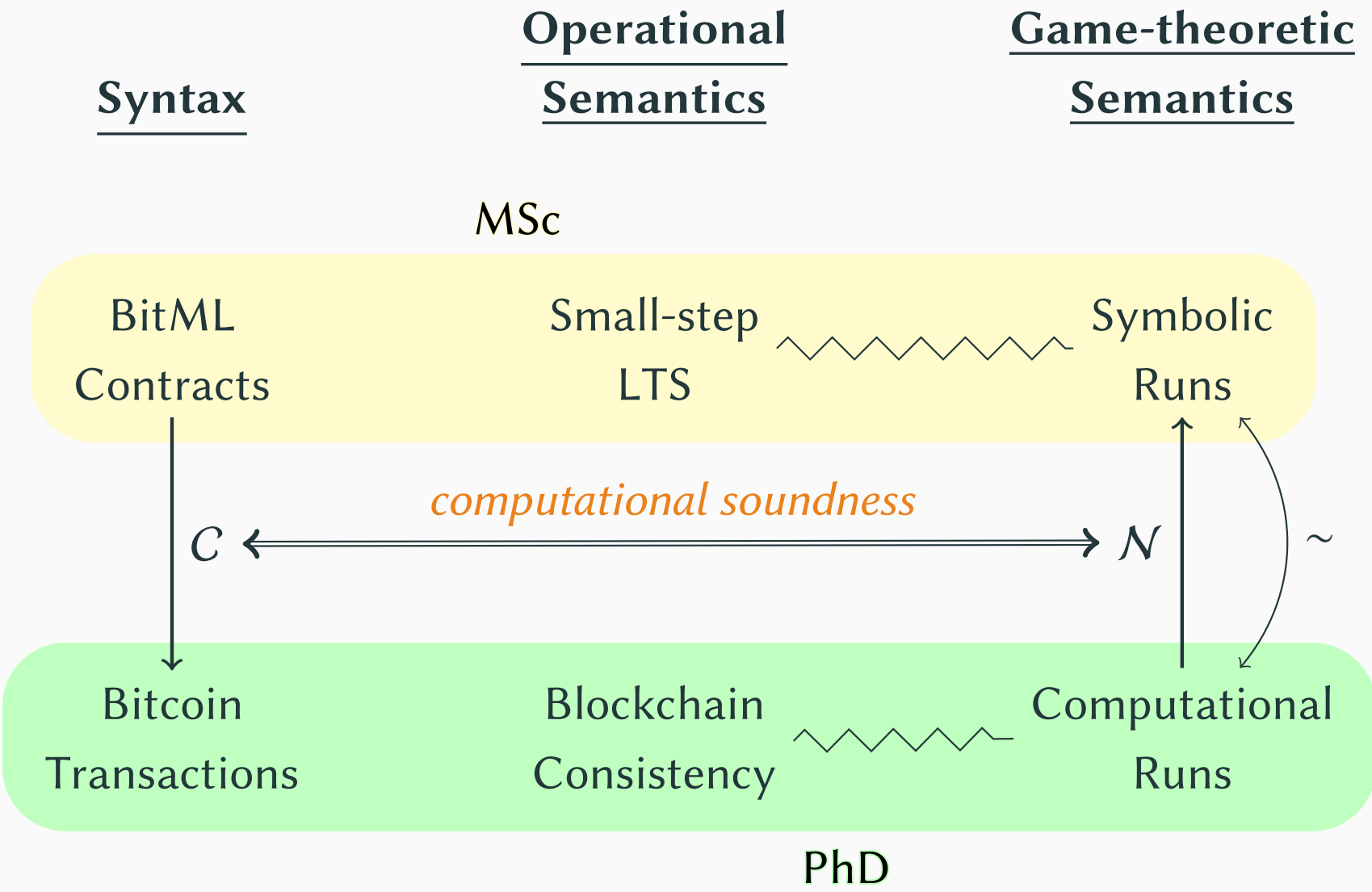
BitML [Sep-Dec 2019]



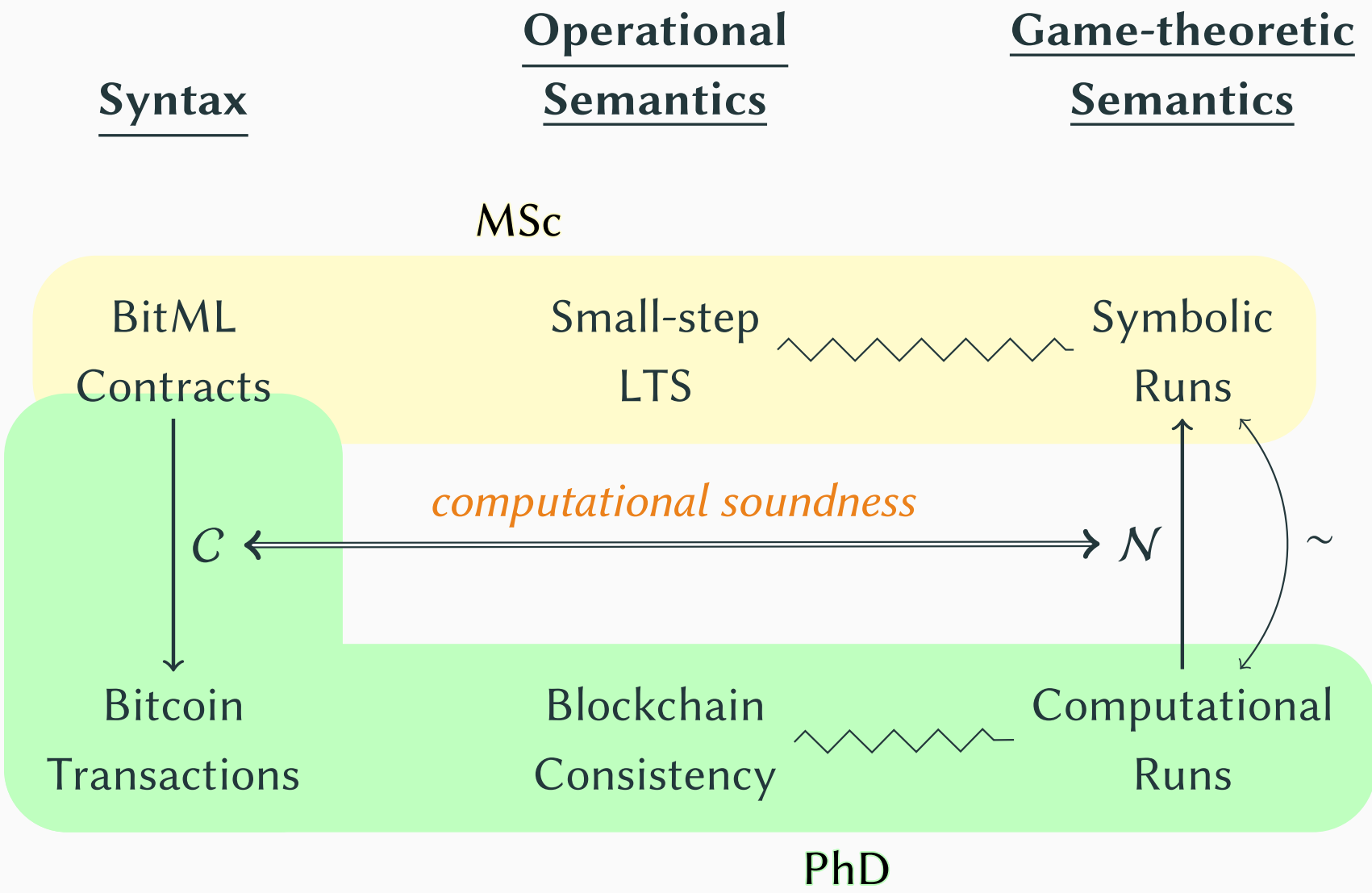
BitML [Sep-Dec 2019]



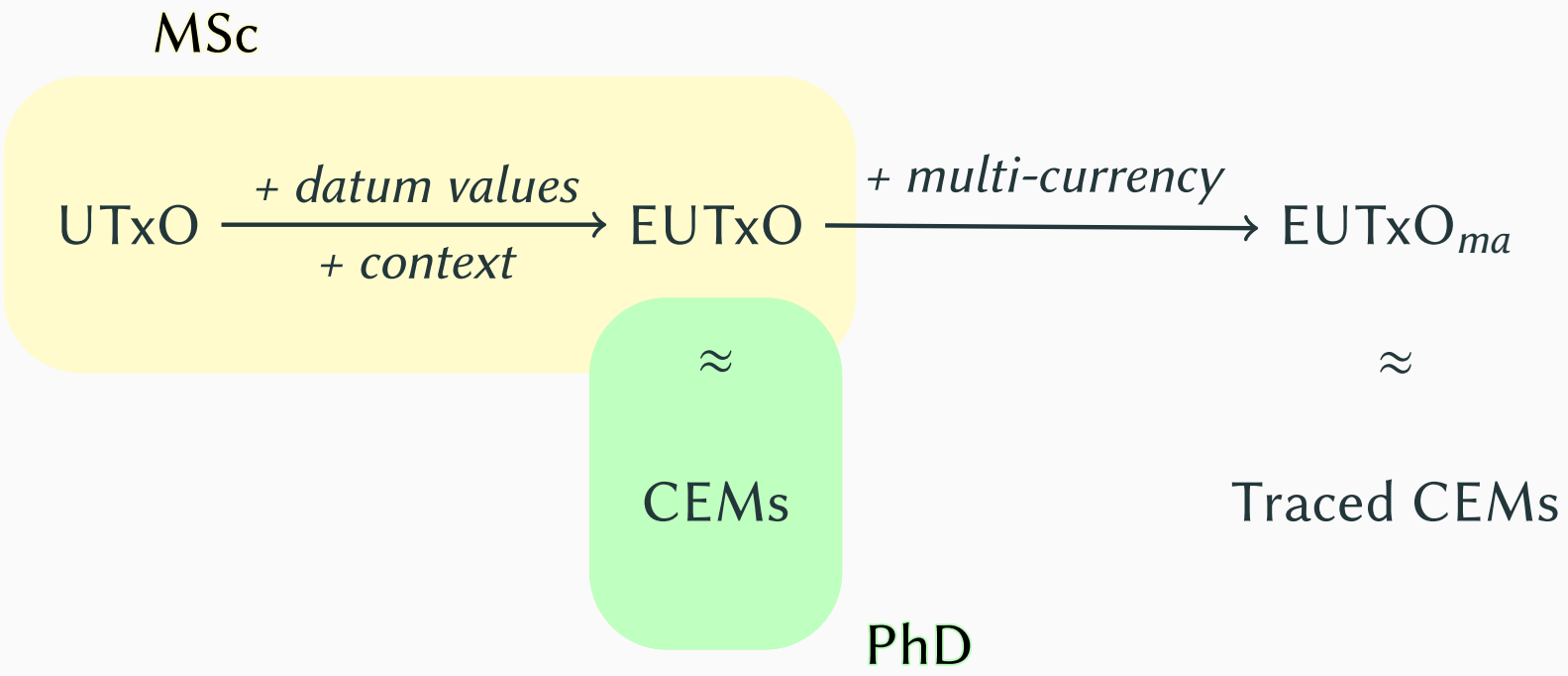
BitML [Sep-Dec 2019]



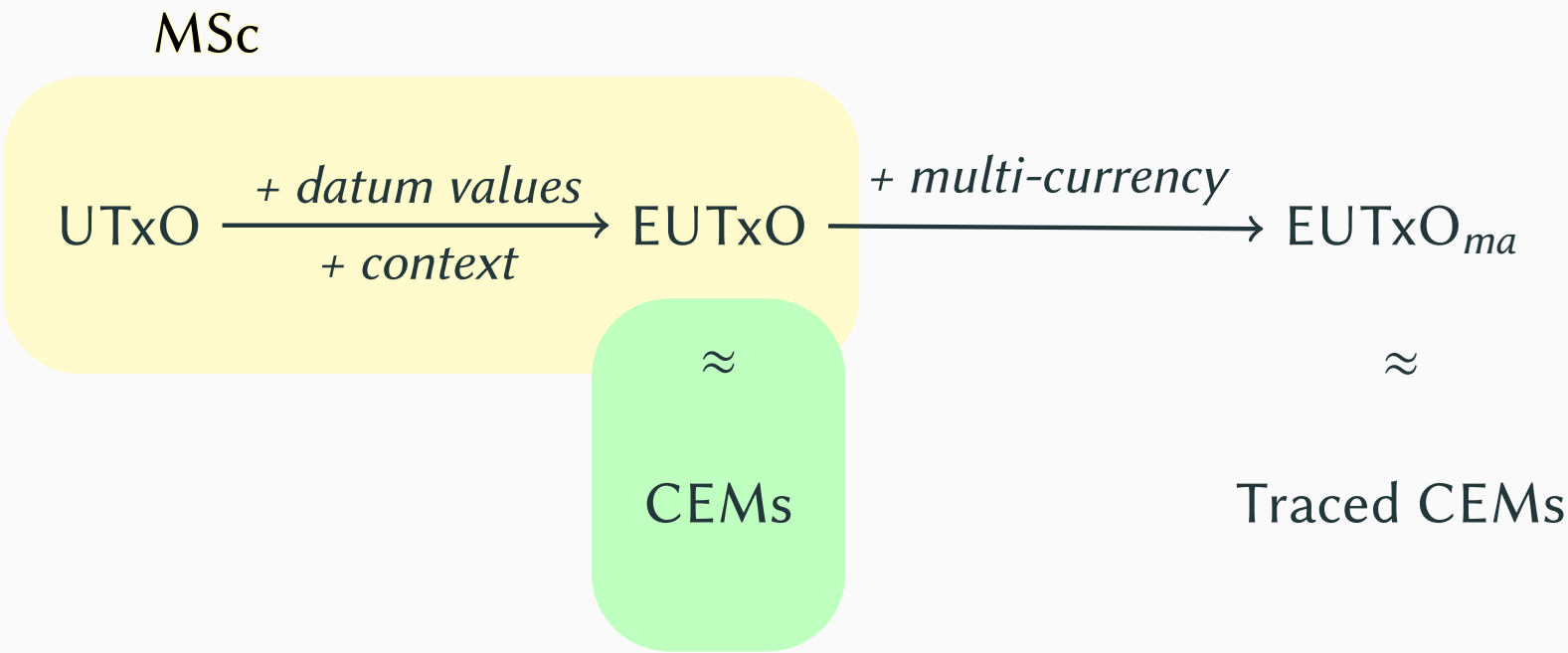
BitML [Sep-Dec 2019]



UTXO [Jan-Jun 2020]

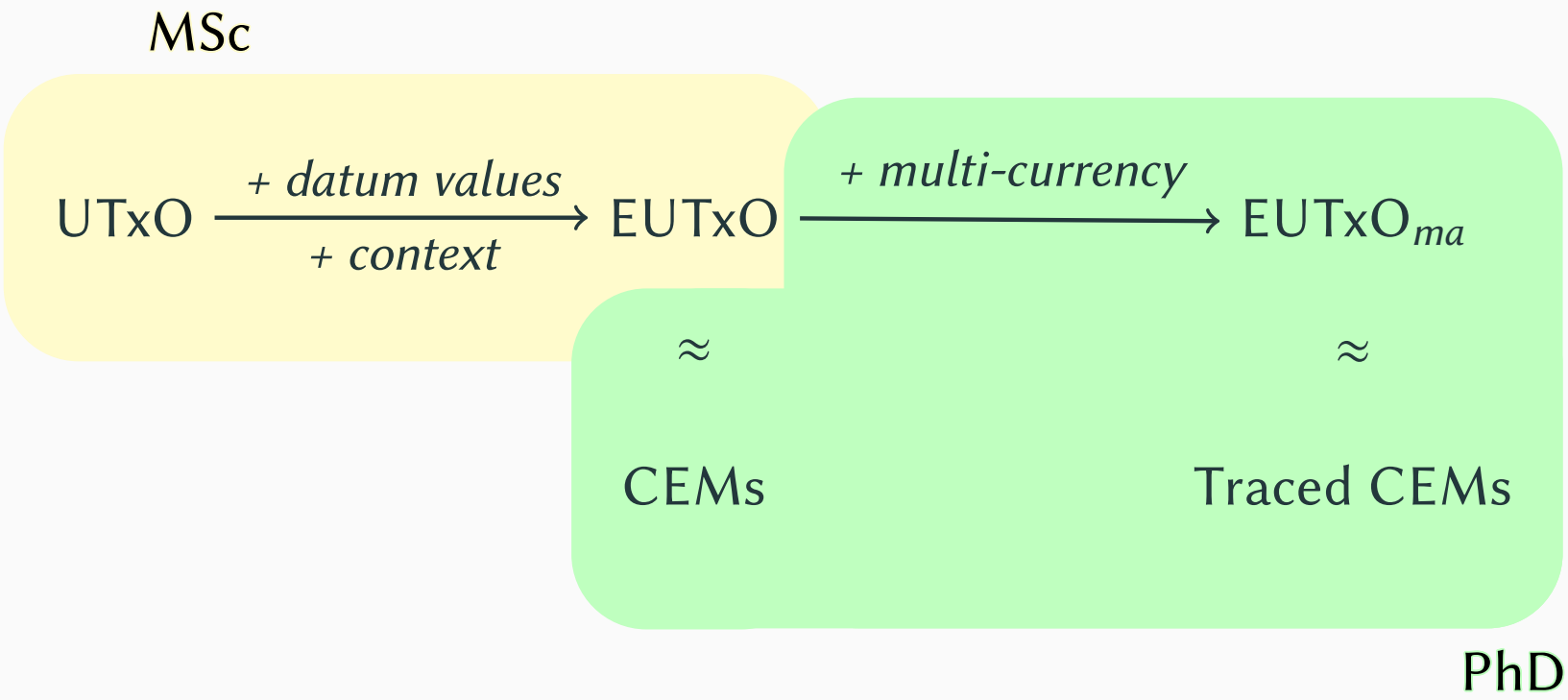


UTXO [Jan-Jun 2020]



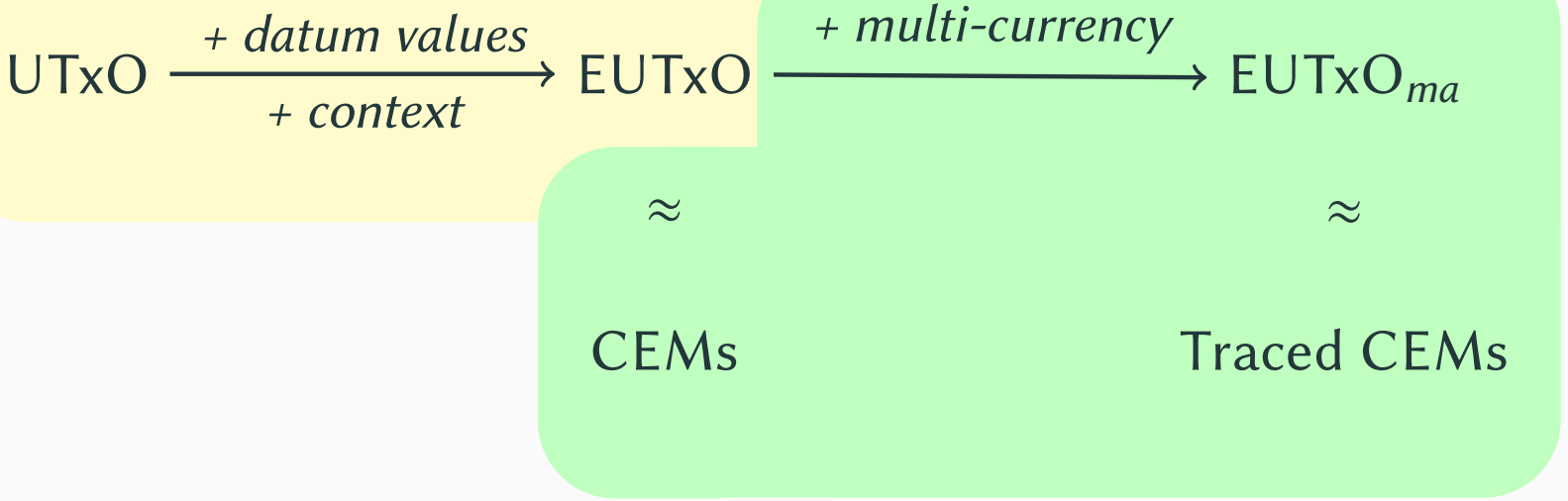
WTSC @ FC: *The Extended UTXO Model*

UTXO [Jan-Jun 2020]



UTXO [Jan-Jun 2020]

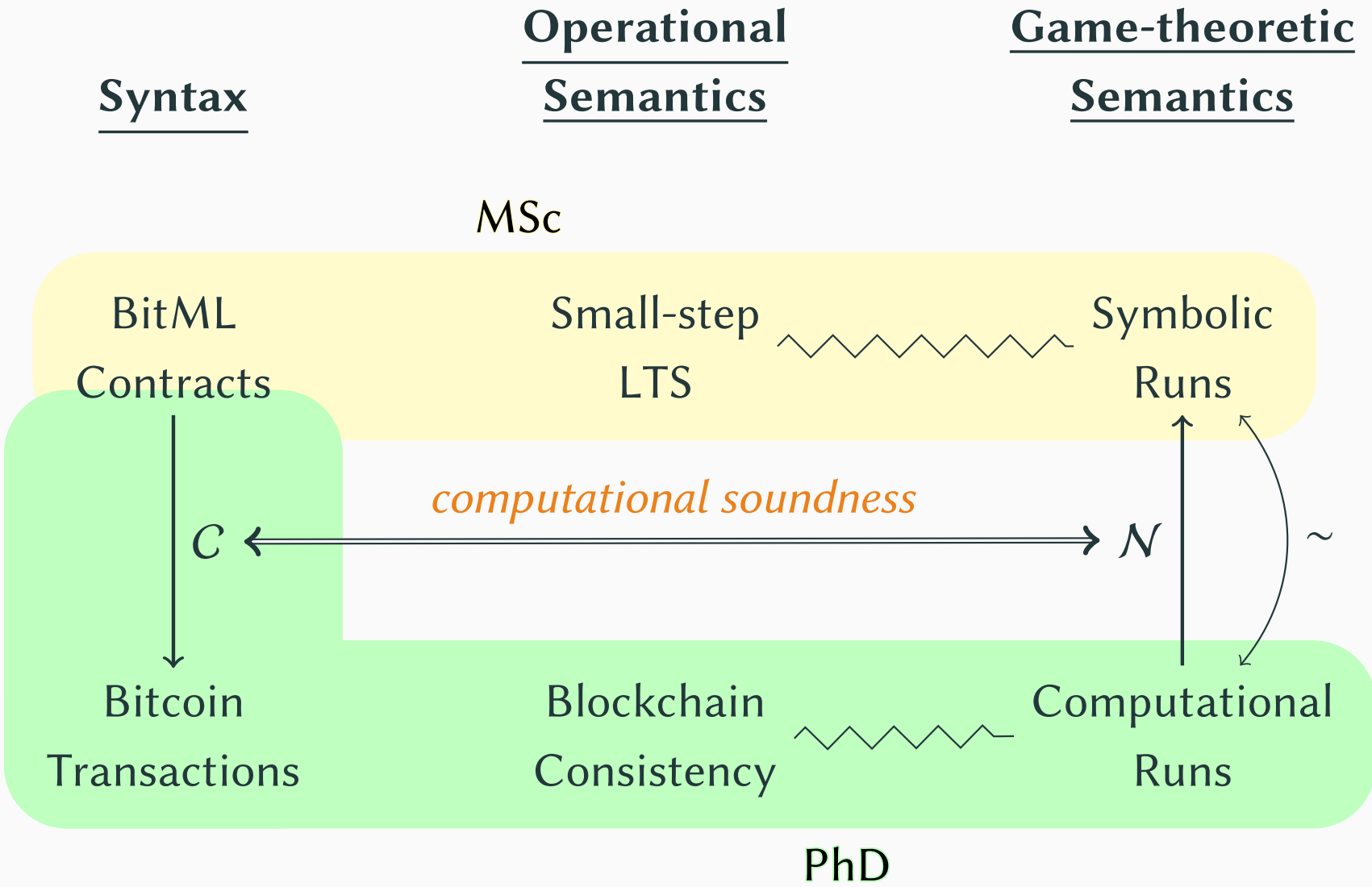
MSc



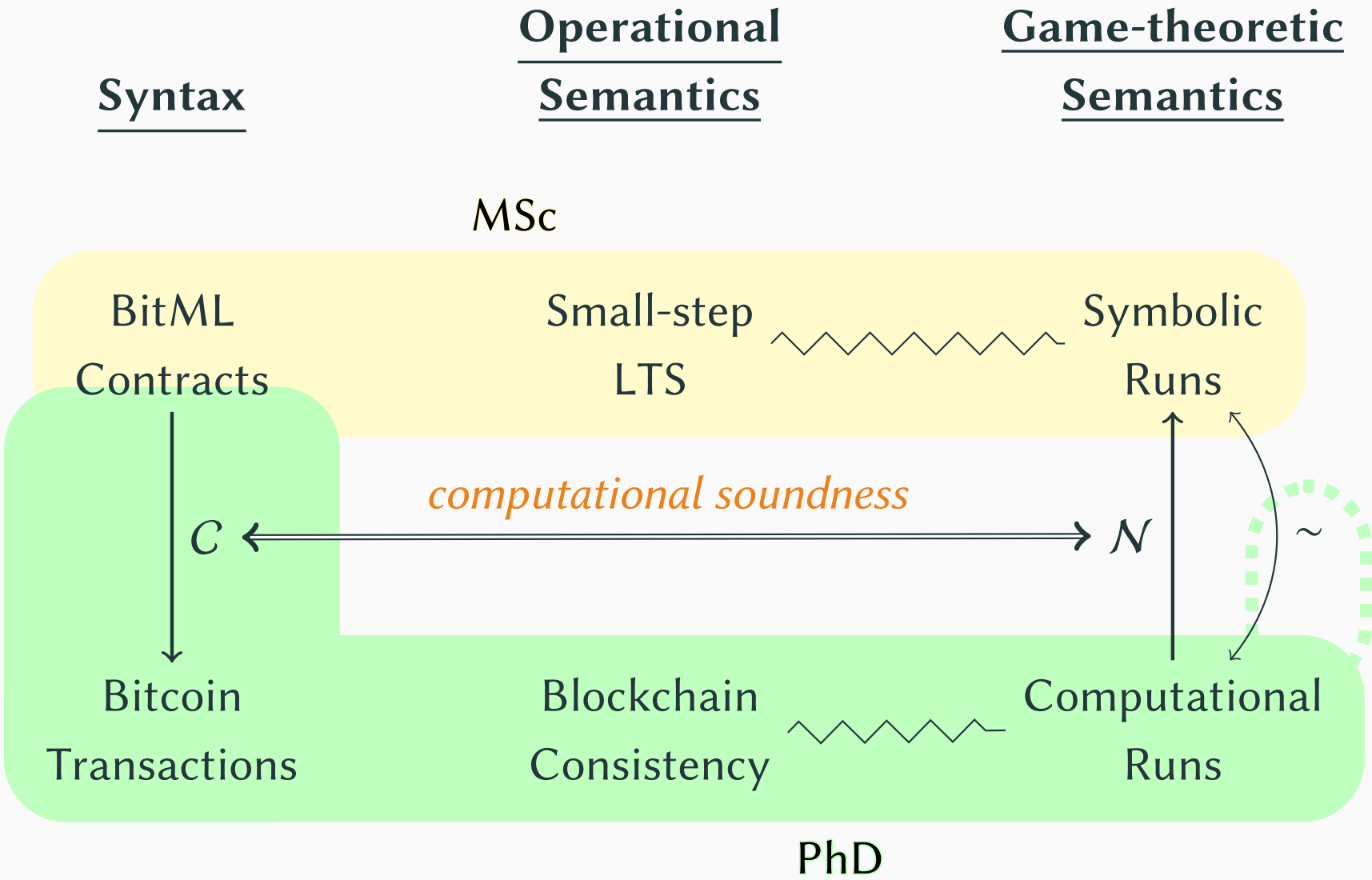
PhD

ISoLA: *Native Custom Tokens in the Extended UTXO Model*

BitML [Jul 2020]



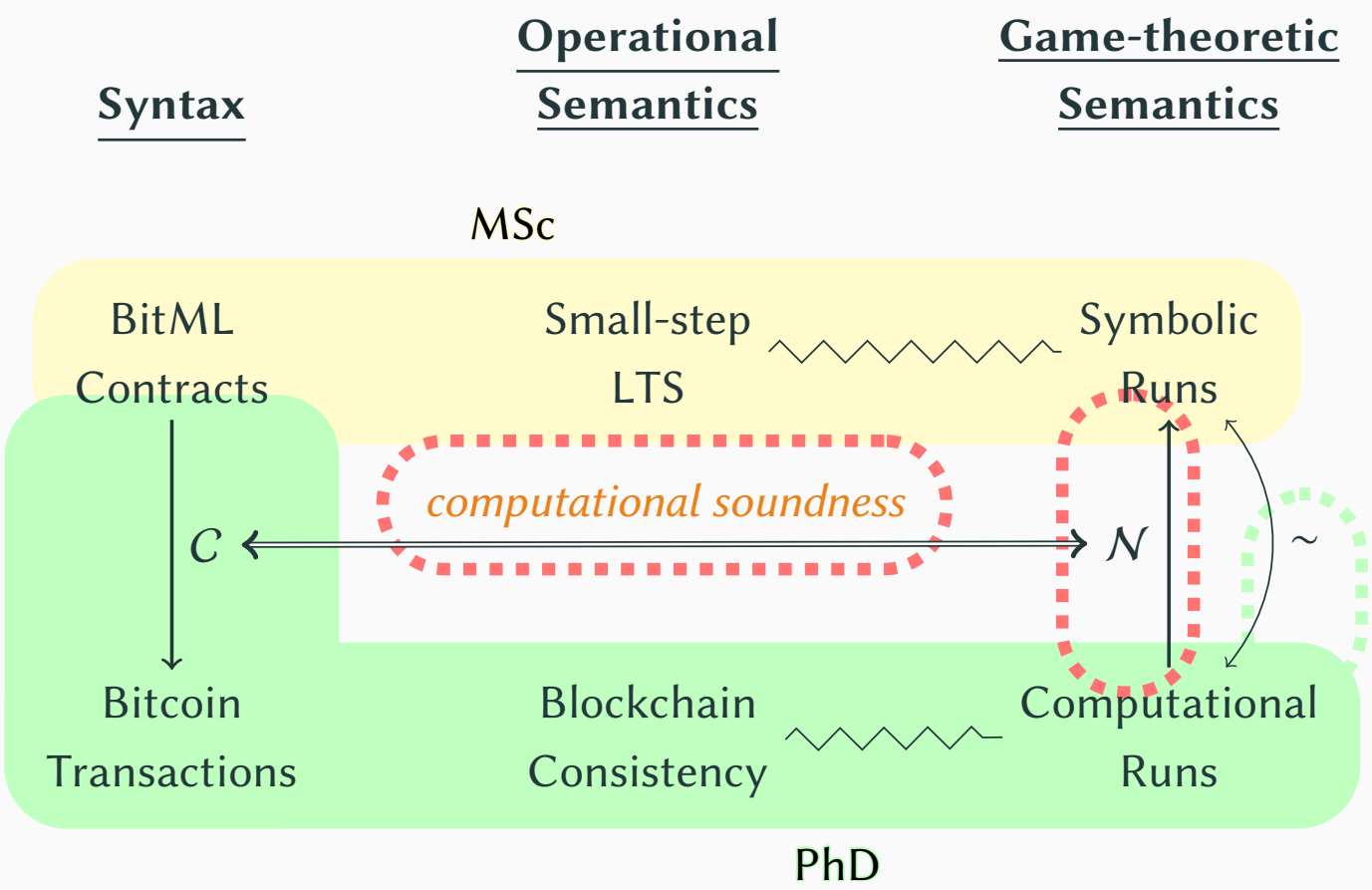
BitML [Jul 2020]



Future Directions

BitML

- Translating symbolic to computational runs
- Prove computational soundness: the compiler preserves coherence



UTxO

- Smart Contract Verification
  - Temporal/branching-time logics (LTL, CTL, CTL$*$, etc...)
- Further Meta-theory
  - Coalgebraic approach to bisimulation
  - Coinductive proof techniques

BitML → EUTxO

- BitML's semantics can be directly encoded as a CEM
- May lead to simpler soundness proof
- Allows comparison with Marlowe
  - which is implemented on top of EUTxO, in a similar fashion)

Discussion

- Coherence of topic (UTxO versus BitML)
  - where to focus on?
  - which research path seems the most promising?
  - is it worthy material for a PhD dissertation?

Discussion

- Coherence of topic (UTxO versus BitML)
  - where to focus on?
  - which research path seems the most promising?
  - is it worthy material for a PhD dissertation?
- Collaboration versus lonesomeness
  - work so far done in collab. with the Plutus team
  - in antithesis with the inherent nature of a PhD

Discussion

- Coherence of topic (UTxO versus BitML)
  - where to focus on?
  - which research path seems the most promising?
  - is it worthy material for a PhD dissertation?
- Collaboration versus lonesomeness
  - work so far done in collab. with the Plutus team
  - in antithesis with the inherent nature of a PhD
- Future directions
  - do they sound interesting and worthy to explore?
  - other comments/suggestions?