The Extended UTXO Model

Manuel M.T. Chakravarty, James Chapman, Kenneth MacKenzie,
Orestis Melkonian, Michael Peyton Jones, Philip Wadler

(presented by **Alexander Nemish**)

February 14, 2020

Introduction

Motivation

- A lot of blockchain applications recently
- Sophisticated transactional schemes via smart contracts
- Reasoning about their execution is:
    1. *necessary*, significant funds are involved
    2. *difficult*, due to concurrency
- Hence the need for tools that verify no such bugs exist
    - This has to be done statically!
    - Formal methods to the rescue!

Background

Bitcoin

- Based on *unspent transaction outputs* (UTxO)
- Smart contracts in the simple language SCRIPT

Ethereum

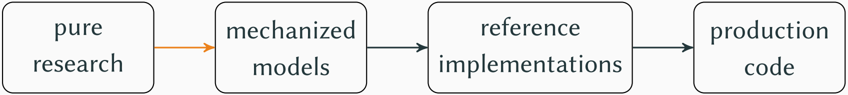
- Based on the notion of accounts
- Smart contracts in (almost) Turing-complete Solidity/EVM

Cardano (IOHK)

- UTxO-based, with several extensions
- Due to the extensions, smart contracts become more expressive

Methodology

- Keep things on an abstract level
  - Setup long-term foundations
- Fully mechanized approach, utilizing Agda's rich type system
- Fits well with IOHK's research-oriented approach



Contributions

- Detailed description of the Extended UTXO model (EUTXO)
- Formalization in Agda
- Formal proof of bisimulation with a specific form of state machines

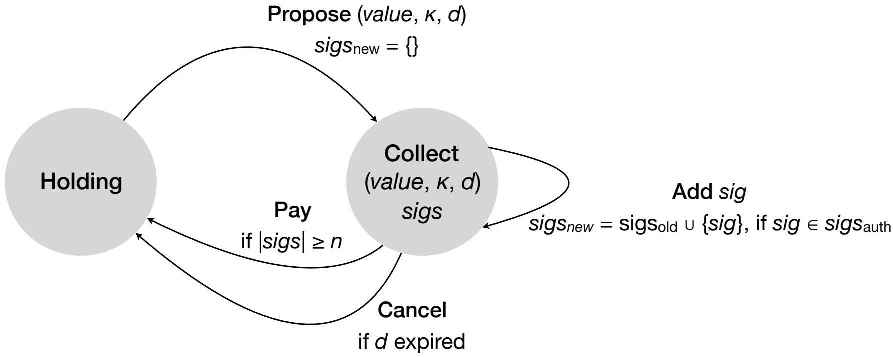
EUTXO, Informally...

Contract Continuity

- New data value on outputs
- More information available to validators
- Restrict discussion to state machines here
  - However, much more computational patterns are possible
  - e.g. the entirety of Marlowe, a DSL for financial contracts, has been implemented as a state machine on top of EUTXO.

Example: Multi-signature Contract

- **n-out-of-m** signature scheme
- Plain UTXO requires off-chain communication
- Can be expressed as a simple state machine:



Example: Implementation in EUTXO

- State machine is associated to a *validator* function
- *Data values* in outputs correspond to states
  - $\in \{\text{Holding}, \text{Collecting}\}$
- Validator takes one of four possible transitions
  - $\in \{\text{Propose}, \text{Add}, \text{Cancel}, \text{Pay}\}$
  - Choice provided by the *redeemer* of the spending input

EUTXO, Formally...

Enhanced Scripting

1. *Data values* additionally carried by outputs
    - passed as extra argument of type Data during validation
    - allows a contract to carry data without changing its code
2. More information about the transaction available to the validator
    - passed as extra argument of type TxInfo during validation
    - allows inspection of the transaction's outputs, thus supporting contract continuity
3. Transactions have (restricted) access to time
    - addition transaction field: *validity interval*
    - specifies a time interval, in which the transaction must be processed

Ledger Primitives

Quantity	an amount of currency
Tick	a tick
Address	an “address” in the blockchain
Data	a type of structured data
DataHash	the hash of a value of type Data
TxId	the identifier of a transaction
txId : Tx → TxId	get a transaction’s identifier
Script	the (opaque) type of scripts
scriptAddr : Script → Address	the address of a script
dataHash : Data → DataHash	the hash of a data value
$[\![\_]\!]$: Script → Args → $\mathbb{B}$	applying a script to its arguments

Defined Types

$$
\begin{aligned}
\textbf{Output} &= (\mathit{value} : \text{Quantity}, \mathit{addr} : \text{Address}, \mathit{dataHash} : \text{DataHash}) \\
\textbf{OutputRef} &= (\mathit{id} : \text{TxId}, \mathit{index} : \mathbb{N}) \\
\textbf{Input} &= (\mathit{outputRef} : \text{OutputRef}, \mathit{validator} : \text{Script}, \\
&\quad\ \mathit{data} : \text{Data}, \mathit{redeemer} : \text{Data}) \\
\textbf{Tx} &= (\mathit{inputs} : \text{Set}[\text{Input}], \mathit{outputs} : \text{List}[\text{Output}], \\
&\quad\ \mathit{validityInterval} : \text{Interval}[\text{Tick}]) \\
\textbf{Ledger} &= \text{List}[\text{Tx}]
\end{aligned}
$$

Validity of EUTXO Transactions (I)

1. **The current tick is within the validity interval**

$$\text{currentTick} \in t.\mathit{validityInterval}$$

2. **All outputs have non-negative values**

$$\forall o \in t.\mathit{outputs},\ \ o.\mathit{value} \geq 0$$

3. **All inputs refer to unspent outputs**

$$t.\mathit{inputs} \subseteq \text{unspentOutputs}(l)$$

4. **Value is preserved**

$$\sum_{i \in t.\mathit{inputs}} \text{getSpentOutput}(i, l).\mathit{value} = \sum_{o \in t.\mathit{outputs}} o.\mathit{value}$$

5. **No output is double spent**

If $i_1, i_2 \in t.\mathit{inputs}$ and $i_1.\mathit{outputRef} = i_2.\mathit{outputRef}$ then $i_1 = i_2$

Validity of EUTXO Transactions (II)

6. **All inputs validate**

$$\forall i \in t.inputs,\ [\![i.validator]\!](i.data,\ i.redeemer,\ \mathrm{toTxInfo}(t, i)) = \mathrm{true}$$

7. **Validator scripts match output addresses**

$$\forall i \in t.inputs,\ \mathrm{scriptAddr}(i.validator) = \mathrm{getSpentOutput}(i, l).addr$$

8. **Data values match output hashes**

$$\forall i \in t.inputs,\ \mathrm{dataHash}(i.data) = \mathrm{getSpentOutput}(i, l).dataHash$$

Expressiveness of EUTXO

Constraint Emitting Machines (CEM)

To formally reason about the expressiveness of EUTXO, we introduce a specific form of state machines:

- Type of states S, type of inputs I
- $\mathrm{final} : S \to \mathrm{Bool}$
- $\mathrm{step} : S \to I \to \mathrm{Maybe}\ (S \times \mathrm{TxConstraints})$

These are similar to Mealy machines, but differ in some aspects:

1. No notion of initial states
2. **Strictly** final states
3. Blockchain-specific output values (TxConstraints)

Behavioural Equivalence: Notation

- A ledger l corresponds to a CEM state s:

$$l \sim s$$

- New (valid) transaction submitted to ledger l:

$$l \xrightarrow{tx} l'$$

- Valid CEM transition from source state s to target state s':

$$s \xrightarrow{i} (s', tx^{\equiv})$$

Transitions-as-transactions

Given a smart contract, expressed as a CEM $\mathcal{C}$, we can derive the validator script that disallows any invalid transitions:

$$\mathrm{validator}_{\mathcal{C}}(s, i, \mathit{txInfo}) = \begin{cases} \mathrm{true} & \mathit{if}\ s \xrightarrow{i} (s', \mathit{tx}^{\equiv}) \\ & \mathit{and}\ \mathrm{satisfies}(\mathit{txInfo}, \mathit{tx}^{\equiv}) \\ & \mathit{and}\ \mathrm{checkOutputs}(s', \mathit{txInfo}) \\ \mathrm{false} & \mathit{otherwise} \end{cases}$$

Behavioural Equivalence: Weak Bisimulation

Proposition 1 (Soundness)

Given a valid CEM transition, we can construct a new valid transaction, such that the resulting ledger corresponds to the target CEM state:

$$\frac{s \xrightarrow{i} (s', tx^{\equiv}) \quad l \sim s}{\exists tx\, l' \,.\, l \xrightarrow{tx} l' \;\wedge l' \sim s'}\ \textsc{sound}$$

Proposition 2 (Completeness)

Given a new valid transaction on the ledger, it is either irrelevant to the state machine or corresponds to a valid CEM transition:

$$\frac{l \xrightarrow{tx} l' \quad l \sim s}{l' \sim s \;\vee\; \exists i\, s'\; tx^{\equiv} \,.\, s \xrightarrow{i} (s', tx^{\equiv})}\ \textsc{complete}$$

Related Work

- Bitcoin Covenants
  - Allows restricting how output values will be used in the future
  - Major inspiration for our introduction of *data values*
- Bitcoin Modelling Language (BitML)
  - A process-calculus for Bitcoin smart contracts, whose operational semantics comprise a state machine
  - Compiles down to Bitcoin transactions, without any extensions
  - Quite complicated translation and requires off-chain communication
- Scilla
  - For Ethereum contracts, using message-passing state machines dubbed *Communicating State Transition Systems*
  - Embedded in Coq, hence amendable to formal verification
  - Allows proving temporal (hyper-)properties
- Bitcoin Contracts as Timed Automata
  - Pragmatic model checking using UPPAAL
  - Does not come with formal guarantees though

Questions?