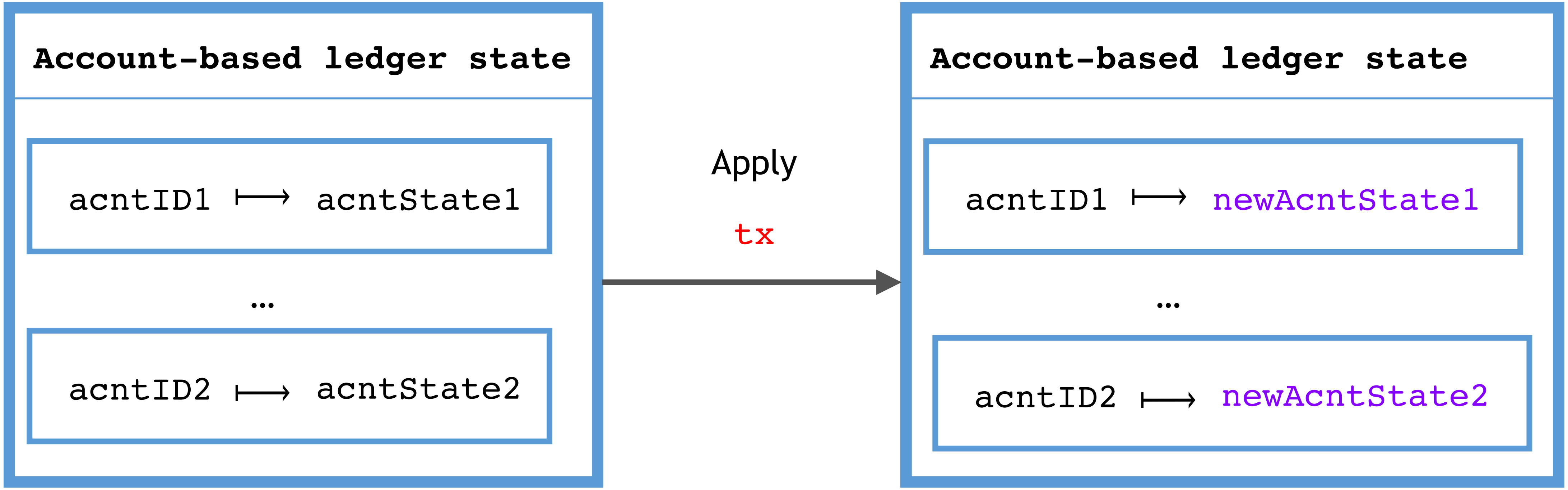
INPUT | OUTPUT

Structured Contracts on Cardano

Statefulness in the EUTxO model

Polina Vinogradova, **Orestis Melkonian**, Philip Wadler, Manuel Chakravarty, Jacco Krijnen,
Michael Peyton Jones, James Chapman, Tudor Ferariu

Account-based Ledgers



Account-based ledger state

acntID1 ⟼ acntState1

…

acntID2 ⟼ acntState2

Apply

tx

Account-based ledger state

acntID1 ⟼ newAcntState1

…

acntID2 ⟼ newAcntState2

EUTxO Ledger

```
UTxO set

txin1 ↦ (myScriptAddr1, value1, datum1)

 …

txin2 ↦ (myScriptAddr2, value2, datum2)
```

`txin = (txId, ix)`

- Pointer to a specific output of transaction `tx`

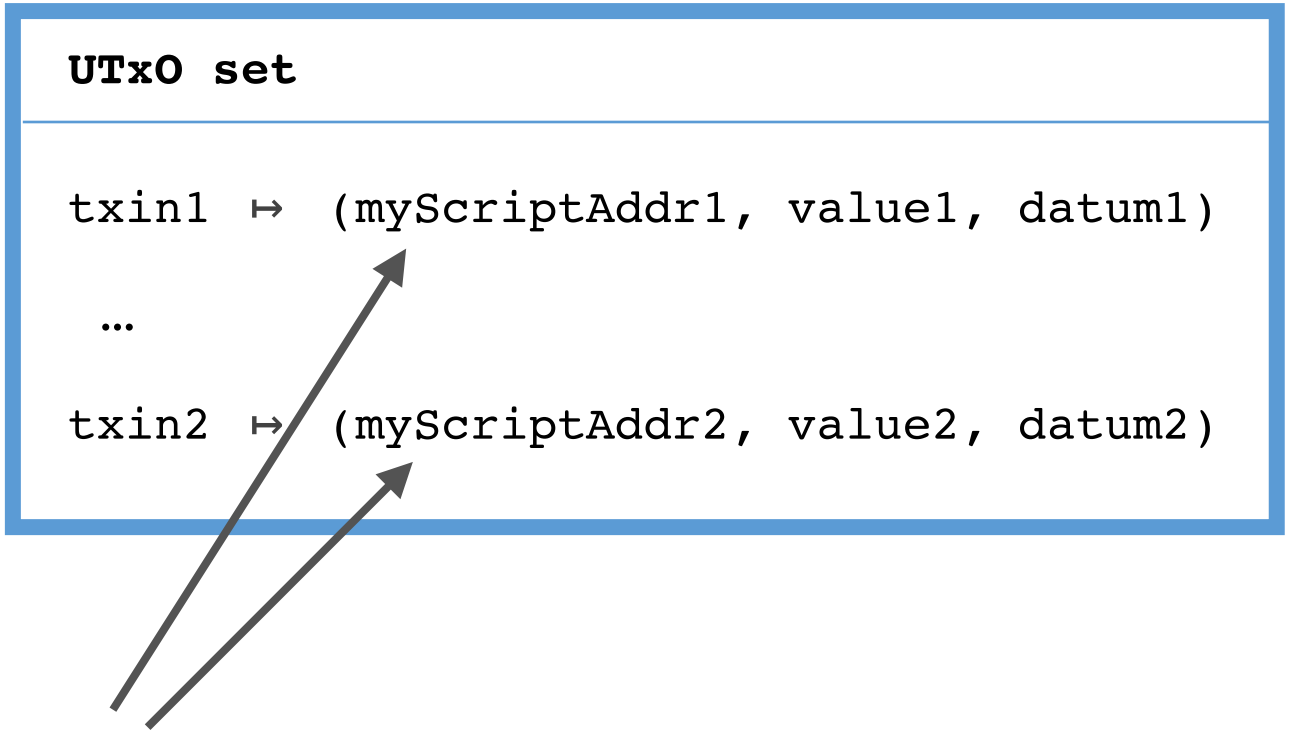
`txID`

- Encoding of the transaction `tx` whose output `txin` points to

`ix`

- Index of corresponding output of `tx` in its list of outputs

EUTxO Ledger



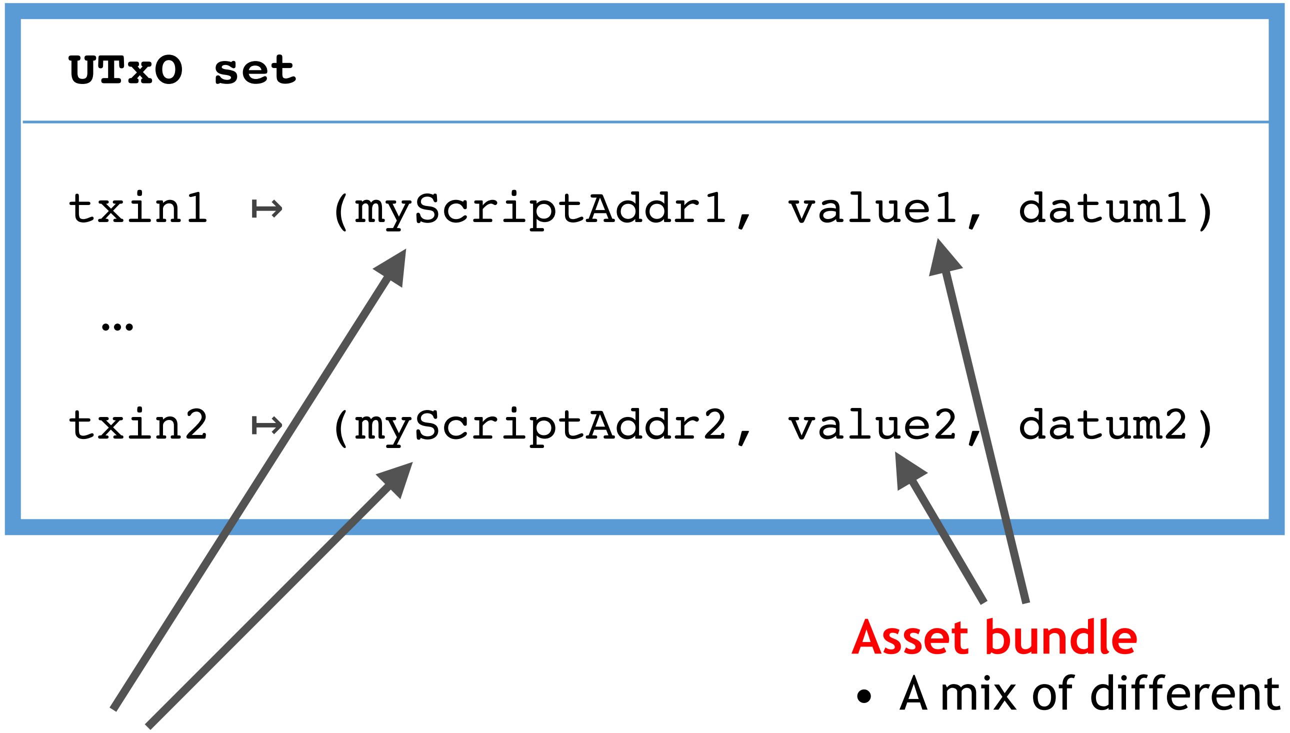
UTxO set

```
txin1 ↦ (myScriptAddr1, value1, datum1)

 …

txin2 ↦ (myScriptAddr2, value2, datum2)
```

Script

- Stateless user-defined code with a boolean output
- Executed when a transaction spends the UTxO entry

EUTxO Ledger

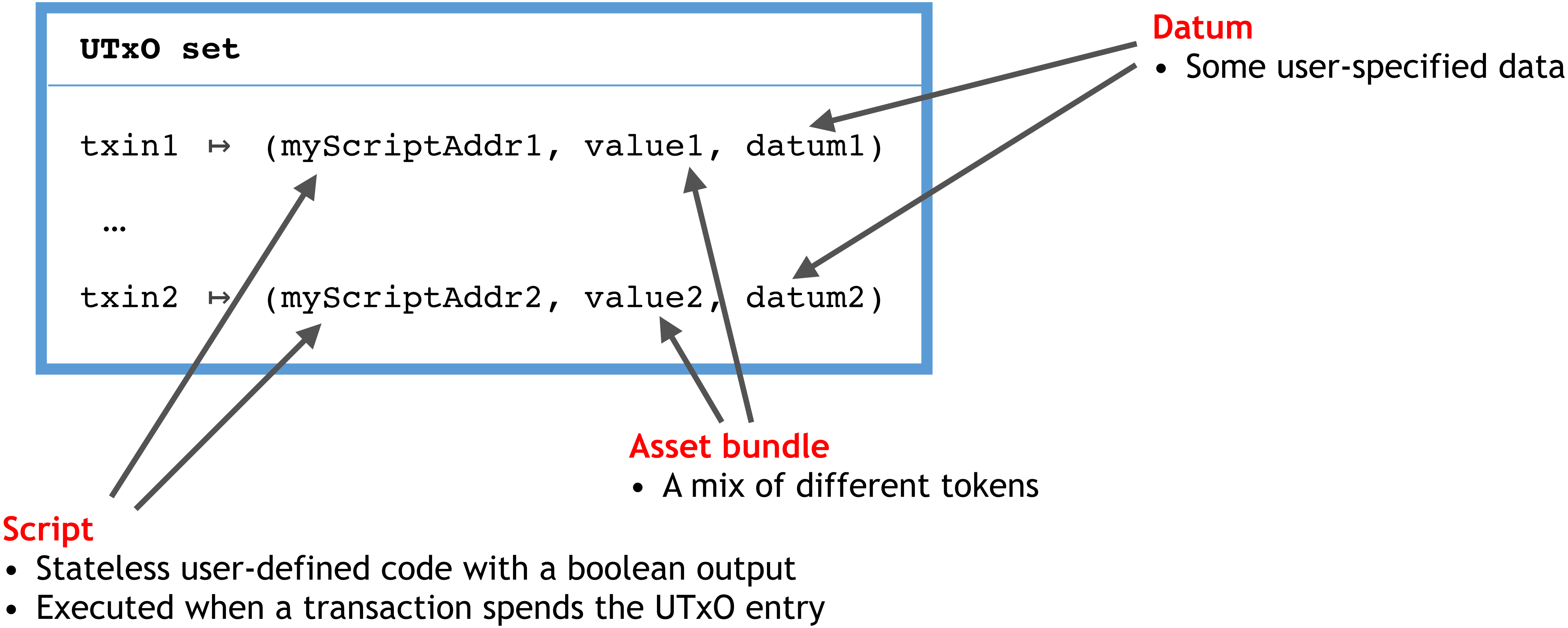


```
UTxO set

txin1 ↦ (myScriptAddr1, value1, datum1)

 …

txin2 ↦ (myScriptAddr2, value2, datum2)
```

Asset bundle
- A mix of different tokens

Script
- Stateless user-defined code with a boolean output
- Executed when a transaction spends the UTxO entry

EUTxO Ledger



UTxO set

```
txin1 ↦ (myScriptAddr1, value1, datum1)

 …

txin2 ↦ (myScriptAddr2, value2, datum2)
```

Datum

- Some user-specified data

Asset bundle

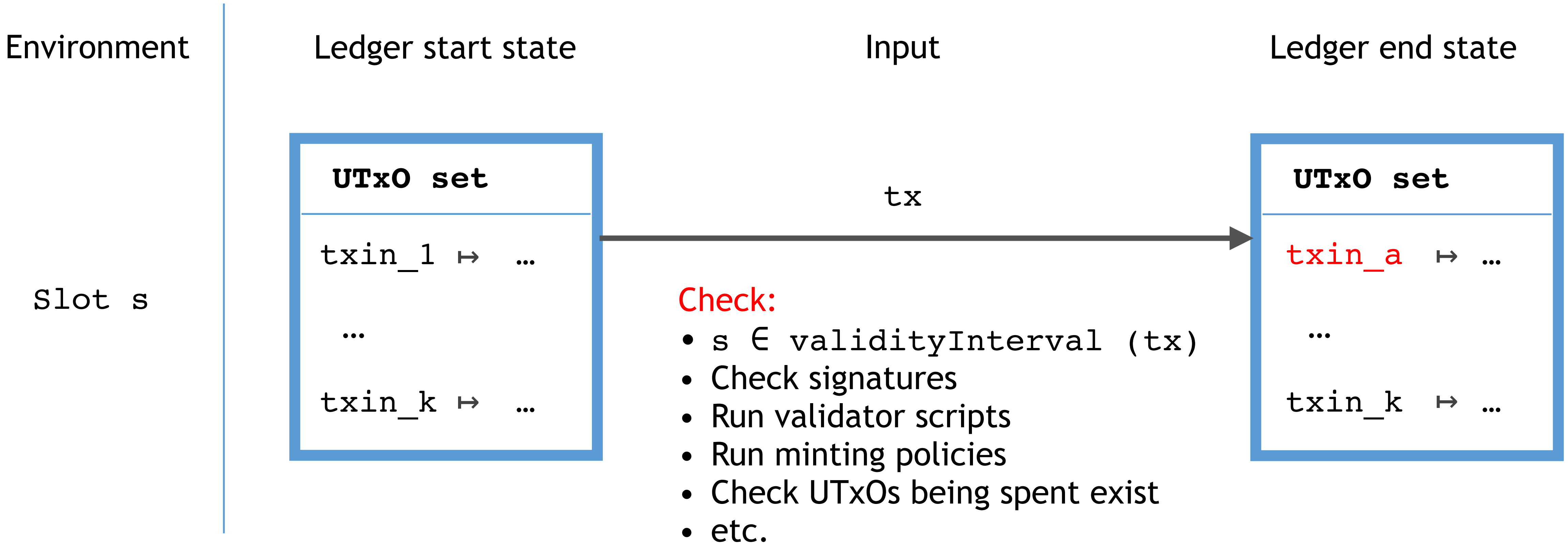
- A mix of different tokens

Script

- Stateless user-defined code with a boolean output
- Executed when a transaction spends the UTxO entry

EUTxO Ledger Update Specification

Using small-step operational semantics



Environment

Slot s

Ledger start state

UTxO set

txin_1 ↦ …

…

txin_k ↦ …

Input

tx

Check:

- s ∈ validityInterval (tx)
- Check signatures
- Run validator scripts
- Run minting policies
- Check UTxOs being spent exist
- etc.

Ledger end state

UTxO set

txin_a ↦ …

…

txin_k ↦ …

EUTxO

Challenges :

- Non-conventional programming **paradigm**
- Programming in **stateless** predicates

Advantages :

- **Predictable**
  - gas cost
  - outcome of contract execution
  - ledger changes made by valid transaction
- Amenable to **formal verification**

Examples :

- Cardano
- Ergo

Account-based

Challenges :

- **Can have unpredictable**
  - gas cost
  - outcome of contract execution
  - ledger changes made by valid transaction
- Formal verification is harder

Advantages :

- **Familiar** programming paradigm
- Straightforward use of **account states**

Examples :

- Ethereum
- Tezos

Motivation : Simulating Accounts

- **State** :
    - unique account ID, owner, assets
- **API** :
    - withdraw, deposit, open, close, transfer

EUTxO implementation :

- How do we **specify** this?
- What does it mean to **implement this program** using stateless predicates on transaction data?
- How can we be sure distinct implementations **meet the same specification**?

Motivation : Simulating Accounts

- **State** :
  - unique account ID, owner, assets

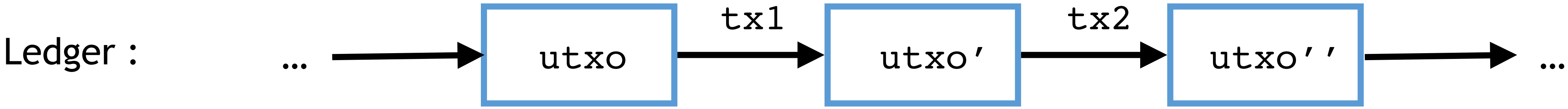
- **API** :
  - withdraw, deposit, open, close, transfer

EUTxO implementation :

- How do we **specify** this?
- What does it mean to **implement this program** using stateless predicates on transaction data?
- How can we be sure distinct implementations **meet the same specification**?

We need a model of stateful computation here!

Enter “Structured Contracts”



Enter “Structured Contracts”

$$\begin{tikzcd}
\text{Ledger :} & \cdots \arrow[r] & \texttt{utxo} \arrow[r, "\texttt{tx1}", ""'{name=T1}] \arrow[d, "\pi"] & \texttt{utxo'} \arrow[r, "\texttt{tx2}", ""'{name=T2}] \arrow[d] & \texttt{utxo''} \arrow[r] \arrow[d, "\pi"] & \cdots \\
\text{Contract Spec :} & \cdots \arrow[r] & \texttt{state} \arrow[r, "\texttt{i1}", ""'{name=I1}] & \texttt{state'} \arrow[r, "\texttt{i2}", ""'{name=I2}] & \texttt{state''} \arrow[r] & \cdots
\arrow[from=T1, to=I1, dashed, "\pi_{Tx}"]
\arrow[from=T2, to=I2, dashed, "\pi_{Tx}"]
\end{tikzcd}$$

Enter “Structured Contracts”

$$\begin{tikzcd}
\text{Ledger :} & \dots \arrow[r] & \texttt{utxo} \arrow[rr, "\texttt{tx1}"] \arrow[d, "\pi"] & {} \arrow[d, dashed, "\pi_{Tx}"] & \texttt{utxo'} \arrow[rr, "\texttt{tx2}"] \arrow[d] & {} \arrow[d, dashed, "\pi_{Tx}"] & \texttt{utxo''} \arrow[r] \arrow[d, "\pi"] & \dots \\
\text{Contract Spec :} & \dots \arrow[r] & \texttt{state} \arrow[rr, "\texttt{i1}"] & {} & \texttt{state'} \arrow[rr, "\texttt{i2}"] & {} & \texttt{state''} \arrow[r] & \dots
\end{tikzcd}$$

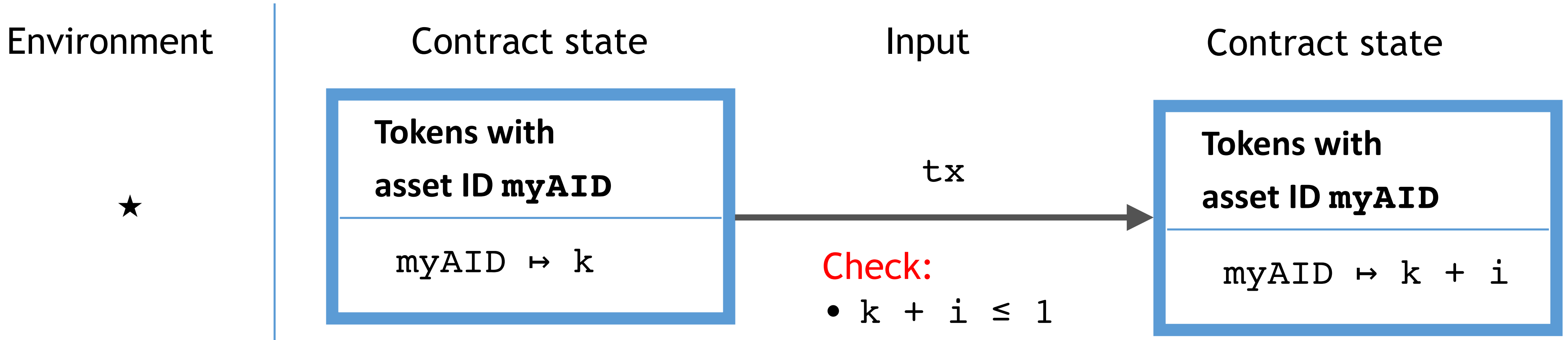
An **instance** of a structured contract requires :

- **Specification** (in small-step operational semantics)
- **Projections** π (partial function), π_{Tx}
- **Proof** of commutativity of any square

Example 1 : NFT

Defining property :

- “Quantity on the ledger cannot be increased past 1 by a transaction”
- suggests a state transition system
- can specify and implement



Environment

★

Contract state

Tokens with asset ID `myAID`

`myAID ↦ k`

Input

`tx`

Check:

- `k + i ≤ 1`

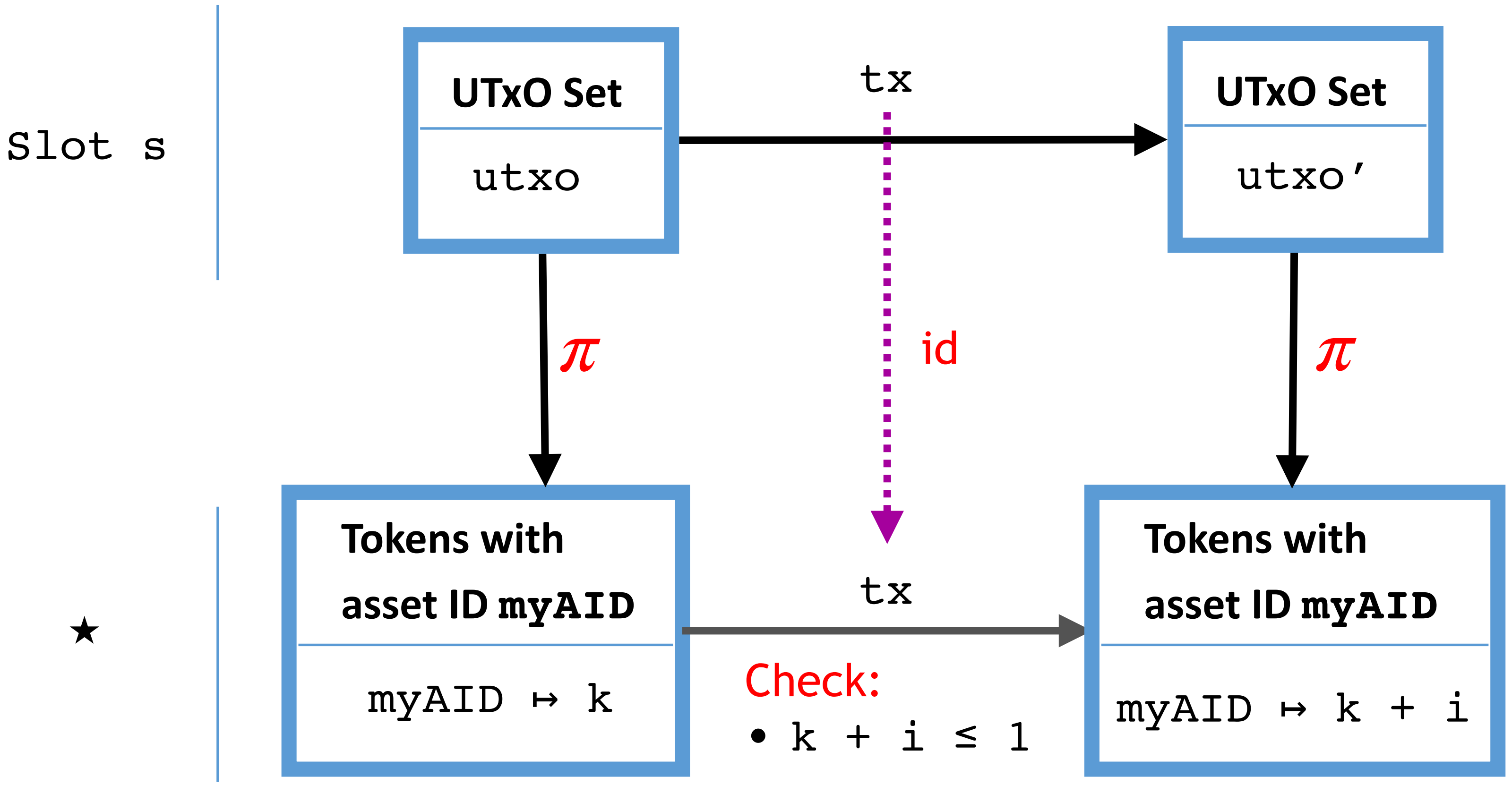
Contract state

Tokens with asset ID `myAID`

`myAID ↦ k + i`

`i` := # tokens with `myAID` in `mint (tx)`

NFT Implementation



Slot s

UTxO Set

utxo

tx

UTxO Set

utxo’

π

id

π

★

Tokens with

asset ID **myAID**

myAID ↦ k

tx

Check:

- k + i ≤ 1

Tokens with

asset ID **myAID**

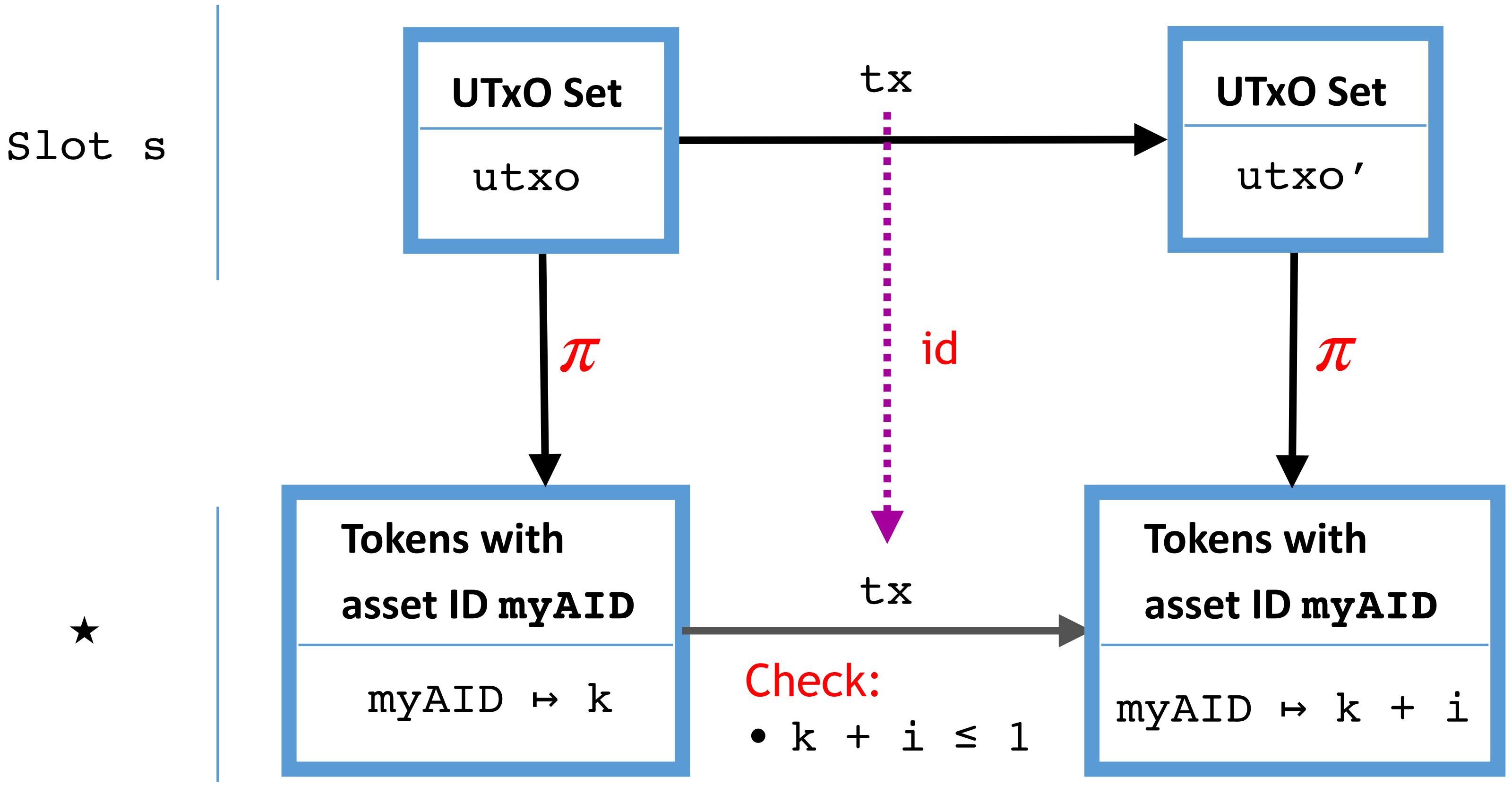
myAID ↦ k + i

i := # tokens with myAID in mint (tx)

Need to :

- Define π
- Prove square commutes

NFT Implementation



Slot s

★

UTxO Set

utxo

tx

UTxO Set

utxo’

π

id

π

Tokens with asset ID **myAID**

myAID ↦ k

tx

Check:

- k + i ≤ 1

Tokens with asset ID **myAID**

myAID ↦ k + i

π (utxo) :=

myAID ↦ k if (k ≤ 1) & …

★ otherwise

where

k := # tokens with myAID in utxo

i := # tokens with myAID in mint (tx)

NFT Implementation

Proving correctness

`myAID` includes to a **minting policy**, which checks :

- A **specific UTxO entry** is being spent by `tx`
- The **quantity** of assets with `myAID` being **minted** is 1

$$\pi\ (\texttt{utxo}) := \begin{cases} \texttt{myAID} \mapsto \texttt{k} & \text{if } (\texttt{k} \leq \texttt{1})\ \texttt{\&}\ \ldots \\ \star & \text{otherwise} \end{cases}$$

where
`k` := # tokens with `myAID` in `utxo`

To prove commutativity :

- assume **replay protection**
- **exclude** the case where π (`utxo`) = $\star$
  - starting UTxO has at **most 1 token** with `myAID`

NFT Defining Property

- From definition of π, we have :

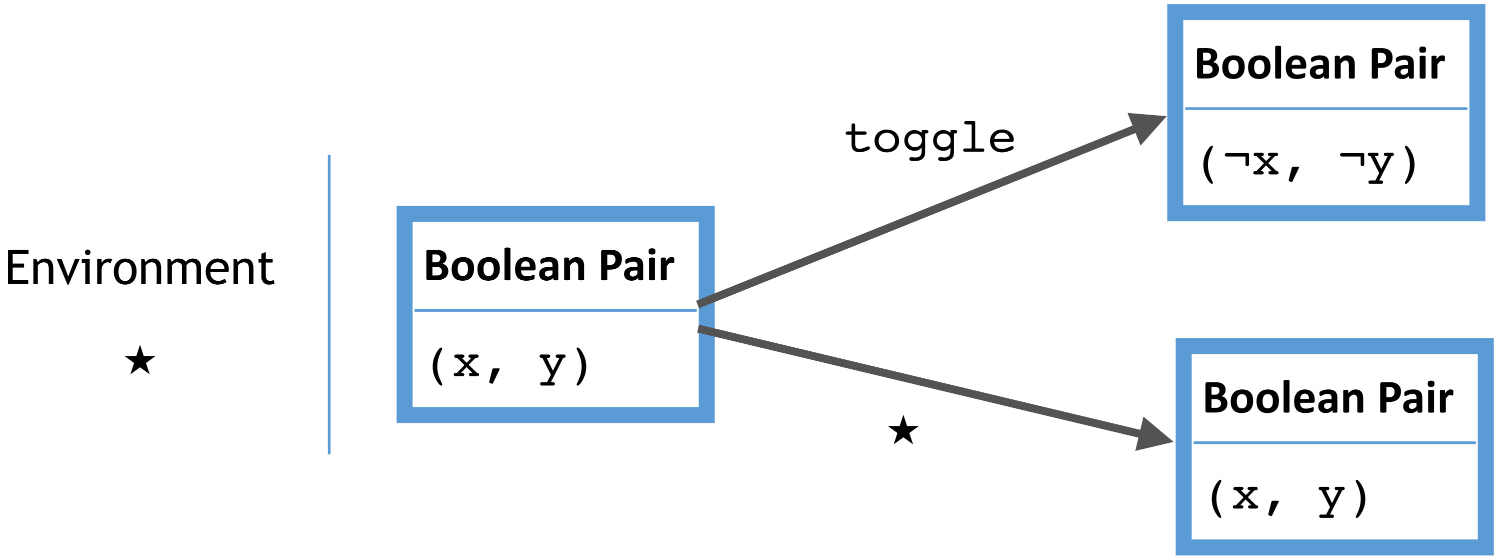
For any `utxo`,

$$\pi\,(\mathtt{utxo}) \neq \star \quad \Rightarrow \quad \pi\,(\mathtt{utxo}) \leq (\mathtt{myAID} \mapsto 1)$$

- **Commutativity of square** implies that

$$\pi\,(\mathtt{utxo}) \neq \star \quad \Rightarrow \quad \pi\,(\mathtt{utxo'}) \leq (\mathtt{myAID} \mapsto 1)$$

Example 2 : TOGGLE



TOGGLE Implementations

Naive

UTxO set
txin ↦ (toggleVal, NFTpointer, (x, y))

Distributed

UTxO set
txin_x ↦ (toggleVal, NFTpointerX, x)
txin_y ↦ (toggleVal, NFTpointerY, y)

TOGGLE Implementations

Naive

```
UTxO set

txin ↦ (toggleVal, NFTpointer, (x, y))
```

Distributed

```
UTxO set

txin_x ↦ (toggleVal, NFTpointerX, x)
txin_y ↦ (toggleVal, NFTpointerY, y)
```

Not pictured here : `NFTpointer`, `NFTpointerX`, and `NFTpointerY` policy code, `toggleVal` code, and commutativity proof obigation

TOGGLE Implementations

Naive

```
UTxO set
txin ↦ (toggleVal, NFTpointer, (x, y))
```

Distributed

```
UTxO set
txin_x ↦ (toggleVal, NFTpointerX, x)
txin_y ↦ (toggleVal, NFTpointerY, y)
```

- Both implement the **same spec**
- Developers can **compare** implementations across memory use, parallelizability, etc.

Structured contracts (SCs)

As a model of stateful computation on the EUTxO ledger

- **Generalization** of constraint-emitting machines (CEMs), in which :
    - projections π, π_{Tx} are **fixed**
    - implementations are **fixed** and **automatically generated**

- SCs define a class of **all stateful contracts**
    - that can be implemented via **user-defined scripts**
    - where correct **ledger** evolution ⇒ correct on-chain **contract state** evolution

- Enable **comparison** of implementations if a given spec

Structured contracts

Limitations

- **No automation** for implementation of simulation proof
  - difficult b/c user decides on the implementation
  - Future work

- Hard to guarantee **existence of valid transaction** corresponding to given state update
  - Even more difficult **in practice** : user has no control over UTxO state, slot, fees, etc. that their transaction will actually be applied to
  - Also future work!

Structured contracts

Mechanized in Agda

https://omelkonian.github.io/structured-contracts/