INPUT | OUTPUT

Validadores/Scripts Plutus y su propósito

+

Valores por dentro

+ VALIDADORES_

Validadores en Aiken: Cómo obtengo un validador?

Todos los validadores son predicados, pero no cualquier predicado es un validador.

```
fn logica_validador() -> Bool
{
  // Lógica de validación
}
```



```
validator {
  fn logica_validador() -> Bool {
    // Lógica de validación
  }
}
```

```
× While trying to make sense of your code ...
╰─▶ Validators require at least 2 arguments and at most 3 arguments.

   ╭─[/home/roberm/scratchpad/aiken-tests/validators/scratchpad.ak:1:1]
 1 │ validator {
 2 │   fn logica_validador() → Bool {
   ·   ──────────────────────┬──────
   ·                         ╰── not enough arguments
 3 │     // Logica de validacion
 4 │     True
   ╰────

 help: Please add the 2 missing arguments.
       If you don't need one of the required arguments use an underscore (e.g. `_datum`).
```

Validadores en Aiken: Parámetros obligatorios de validador*

```
validator {
  fn logica_spendig_validator(datum, redeemer, ctx: ScriptContext) -> Bool {
    // Lógica de validación
  }
}
```

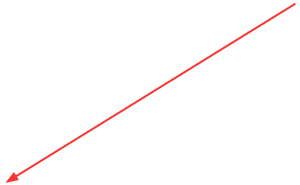
```
validator {
  fn logica_otros_validadores(redeemer, ctx: ScriptContext) -> Bool {
    // Lógica de validación
  }
}
```

*PlutusV1 y PlutusV2 - (CIP-69)

+ PROPÓSITO DEL SCRIPT_

Script Purpose: Dónde está el propósito del script?

```
ScriptContext { transaction: Transaction, purpose: ScriptPurpose }
```



Lo vamos a ver más adelante

Propósito del script/validador

Único para cada validador de la transacción.

Script Purpose: Qué puede hacer el script? Cuál es el propósito?

```
ScriptPurpose {
   Spend(OutputReference)
   Mint(PolicyId)
   WithdrawFrom(StakeCredential)
   Publish(Certificate)
}
```

```
ScriptPurpose {
    Spend(OutputReference)
    Mint(PolicyId)
    WithdrawFrom(StakeCredential)
    Publish(Certificate)
}
```

Validador de gasto (Spending validator)

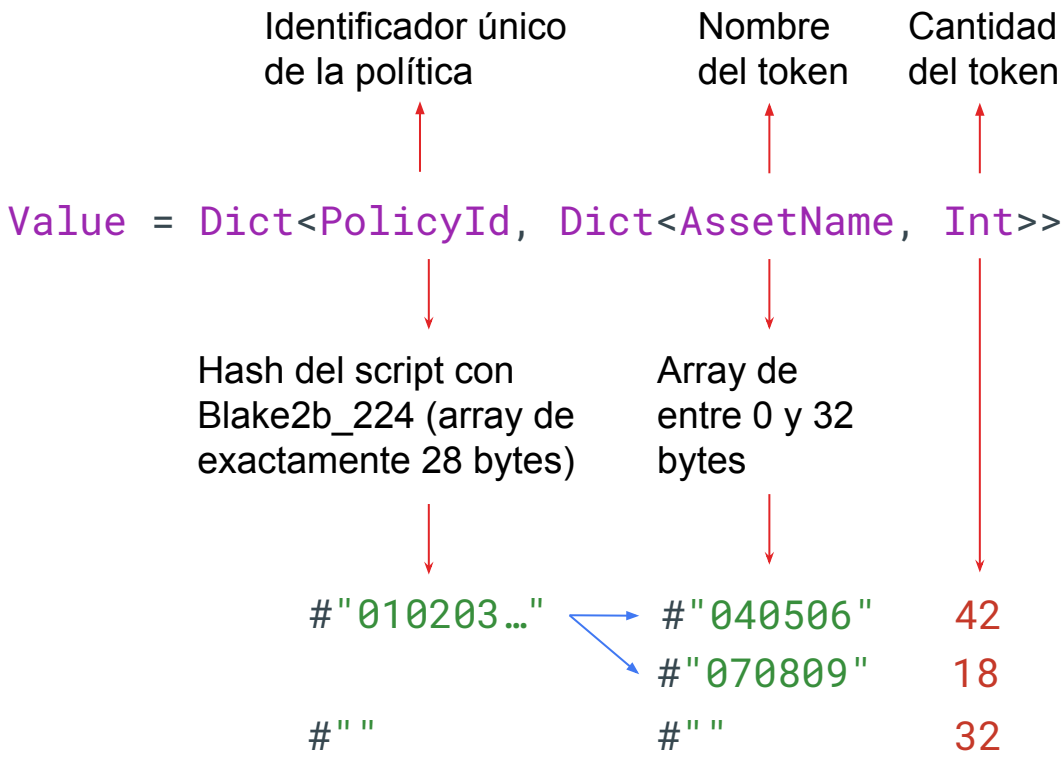
- Scripts que validan si la transacción puede **consumir** un UTxO. No validan si puede **crear** el UTxO.
- Parametrizado por el identificador único del UTxO (ID de la transacción + índice del output).
- Para que un validador custodie un UTxO, hay que crearlo en la dirección del validador.
- La dirección del validador depende del hash del script. Por lo tanto, los scripts son inmutables.

```
ScriptPurpose {
    Spend(OutputReference)
    Mint(PolicyId)
    WithdrawFrom(StakeCredential)
    Publish(Certificate)
}
```

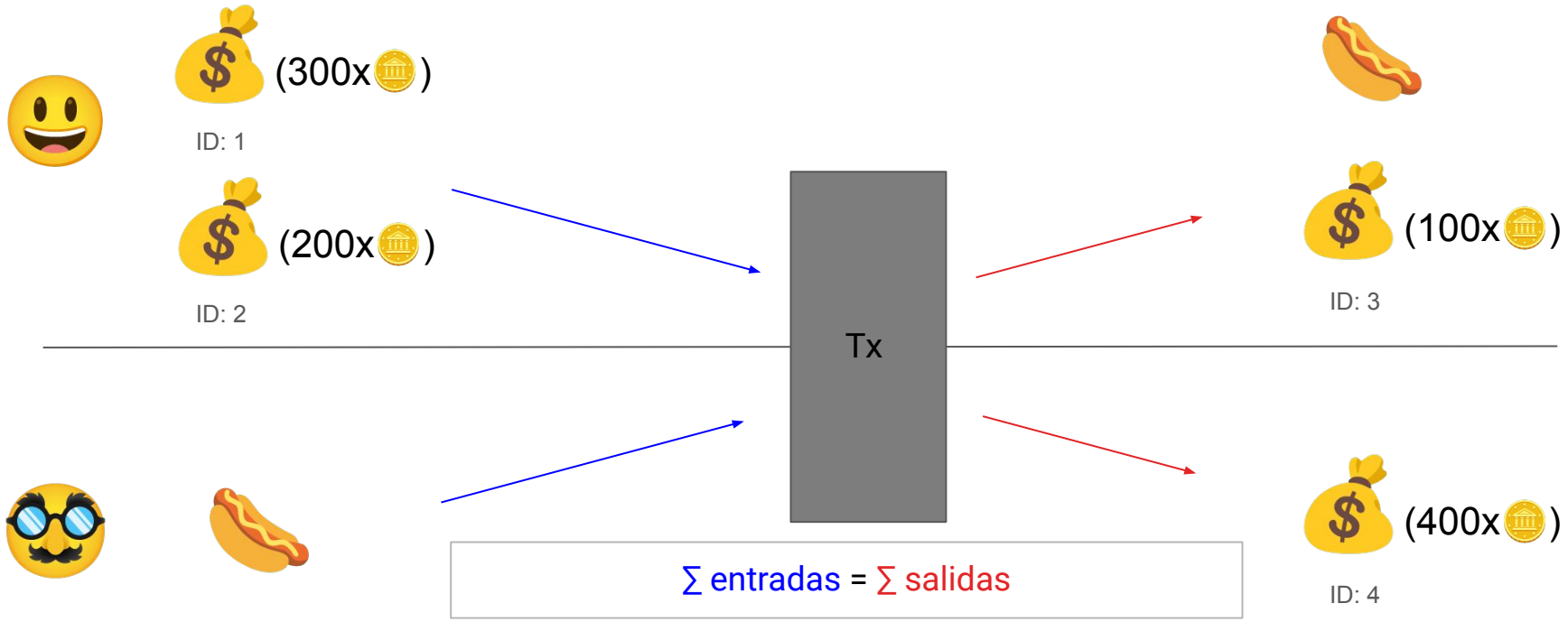
Política monetaria (Minting Policy)

- Scripts que validan si los tokens que la transacción quiere acuñar o quemar cumplen con una política previamente establecida.
- Parametrizado por el identificador único de la política (hash del script).
- Cada token tiene su propia política, la cual es única e inmutable.
- Una política monetaria sólo custodia el acuñado o quemado de sus propios tokens.

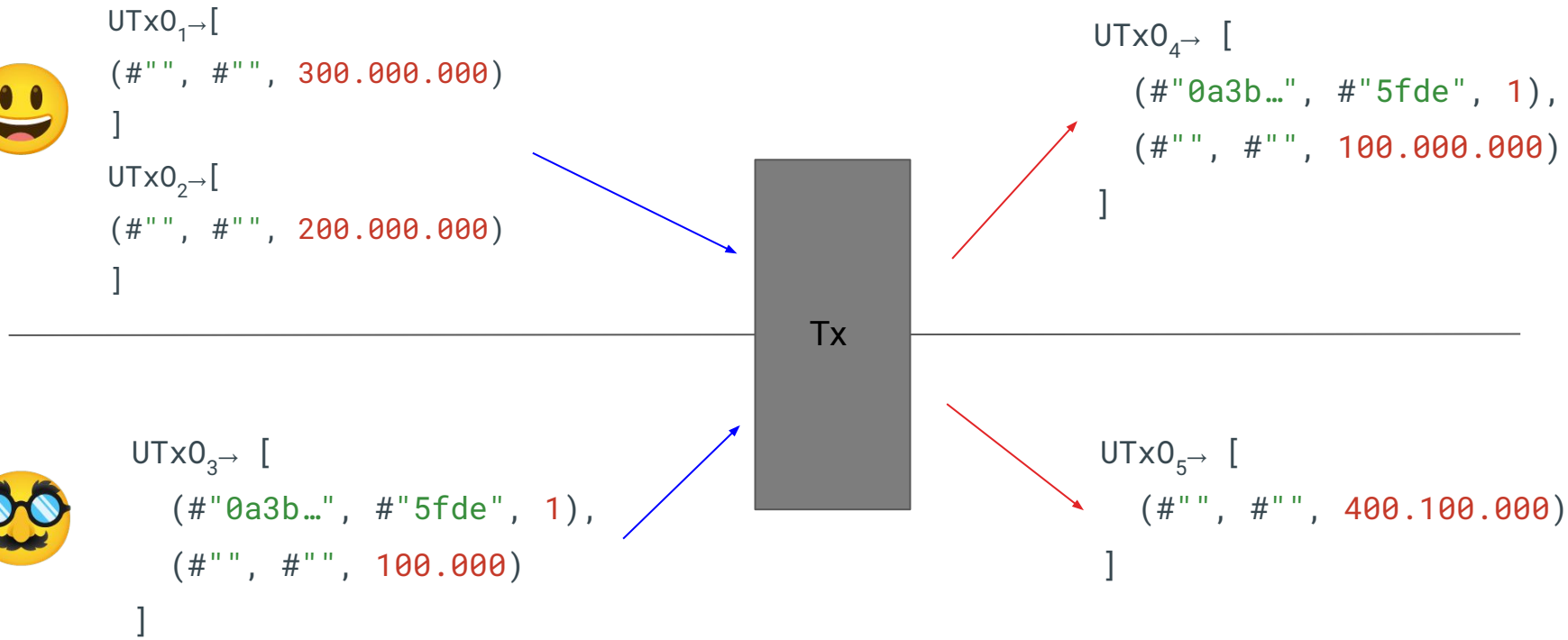
Valor: Qué son los valores?



Valor: Transacción con valores imaginarios

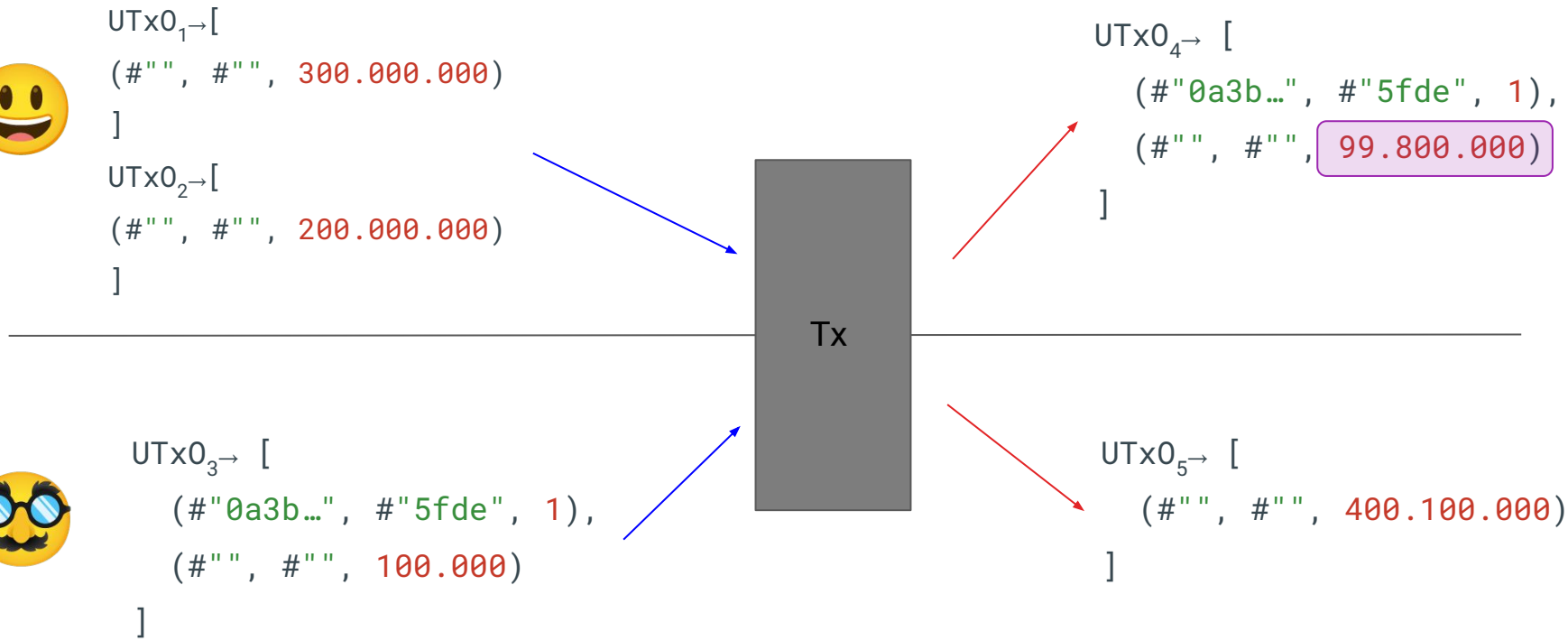


Valor: Transacción con Valores reales sin tarifa (fee)



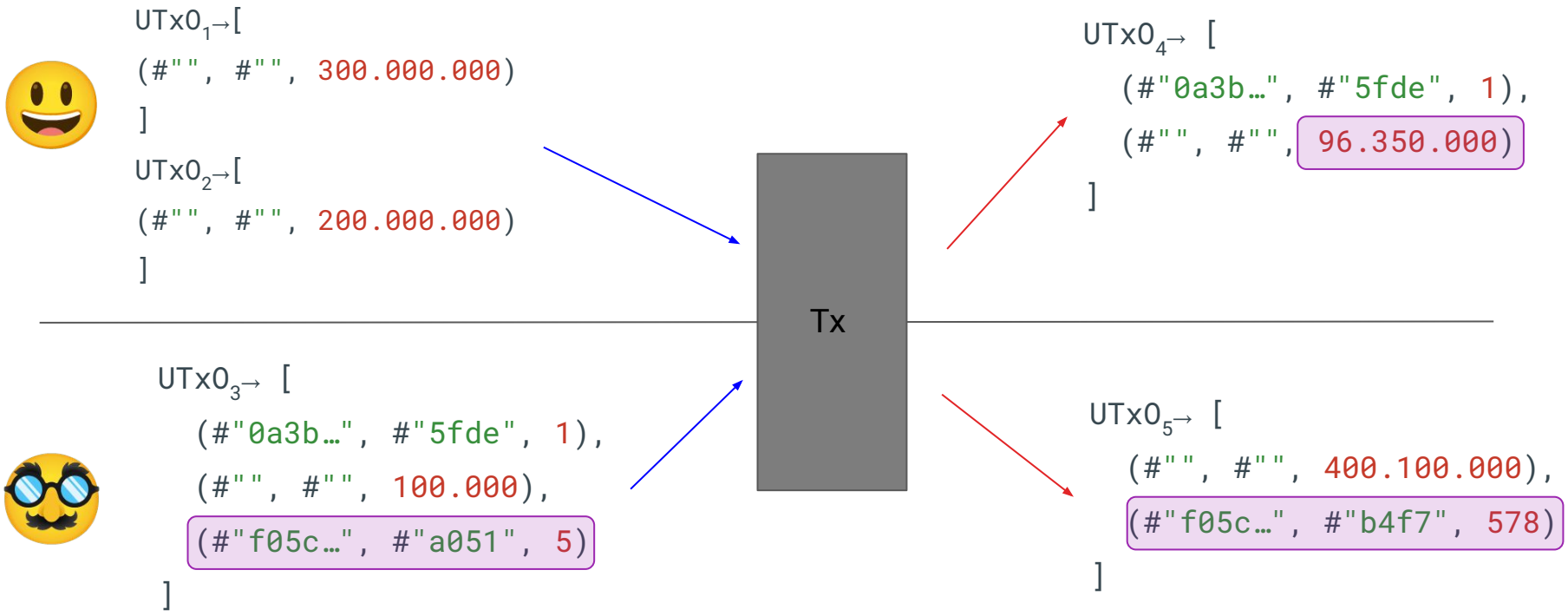
∑ entradas = ∑ salidas

Valor: Transacción con Valores reales con tarifa (fee)



∑ entradas = ∑ salidas + Tarifa (fee)

Valor: Transacción con Valores reales con tarifa (fee)



∑ entradas = ∑ salidas + Tarifa (fee) - T. Acuñados + T. Quemados

```
ScriptPurpose {
    Spend(OutputReference)
    Mint(PolicyId)
    WithdrawFrom(StakeCredential)
    Publish(Certificate)
}
```

Validador de retiro (Withdraw Validator)

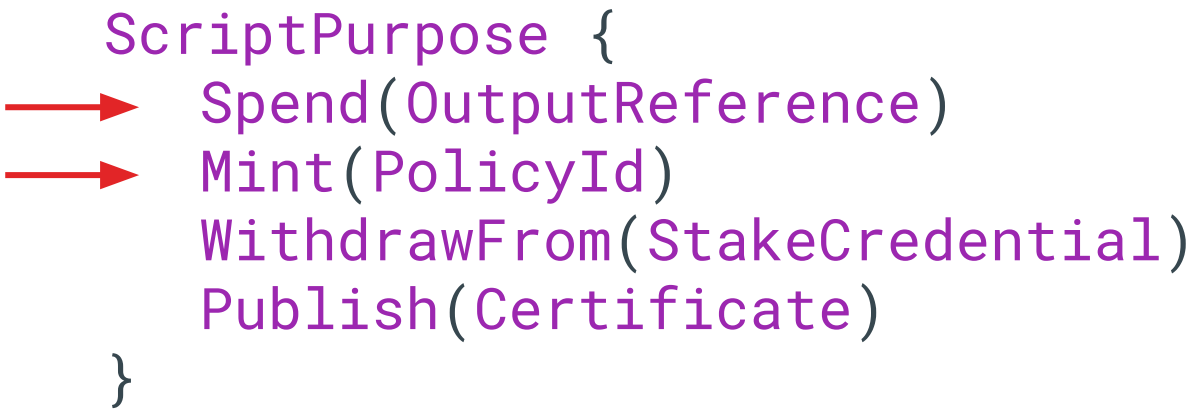
- Scripts que validan retiros de recompensas acumulados por hacer staking.
- Parametrizado por la cuenta de recompensa.
- No se puede retirar parte de las recompensas, tiene que ser todo. Pero podemos tomar decisiones sobre cómo distribuir ese todo.

```
ScriptPurpose {
    Spend(OutputReference)
    Mint(PolicyId)
    WithdrawFrom(StakeCredential)
    Publish(Certificate)
}
```

Validador de certificado (Certificate Validator)

- Scripts que validan cambios en certificados:
  - Registrar una credencial
  - Dar de baja una credencial
  - Delegar una credencial a una stake pool
  - Registrar una stake pool
  - Dar de baja una stake pool
  - Acciones de gobernanza
  - Mover bienes en tesorería
- Parametrizado por el certificado que se está utilizando

Script Purpose: Los propósitos más usados




Fin
Preguntas?
INPUT | OUTPUT