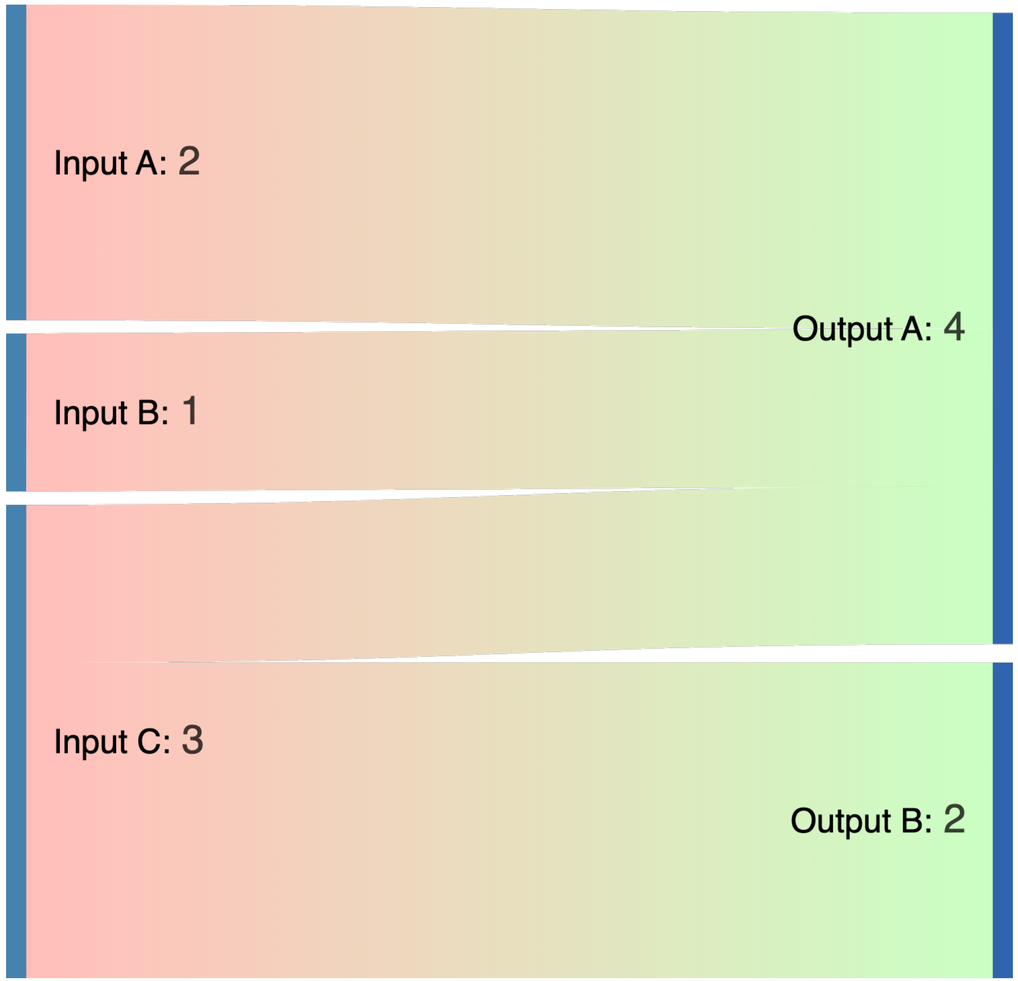
Ordinal Inscriptions:

The Good, the Bad, and the Ugly

@arikaleph

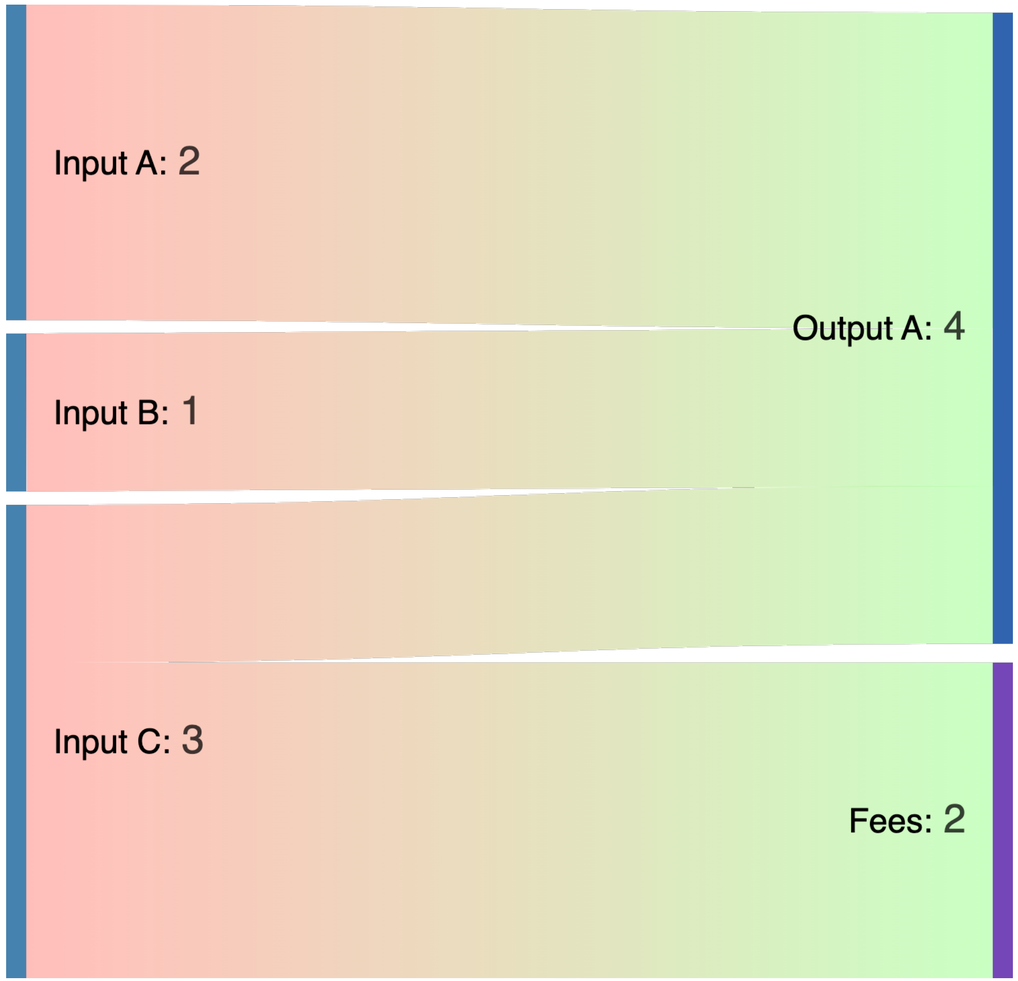
Ordinal Flow

Inputs	Outputs
2	4
1	2
3	



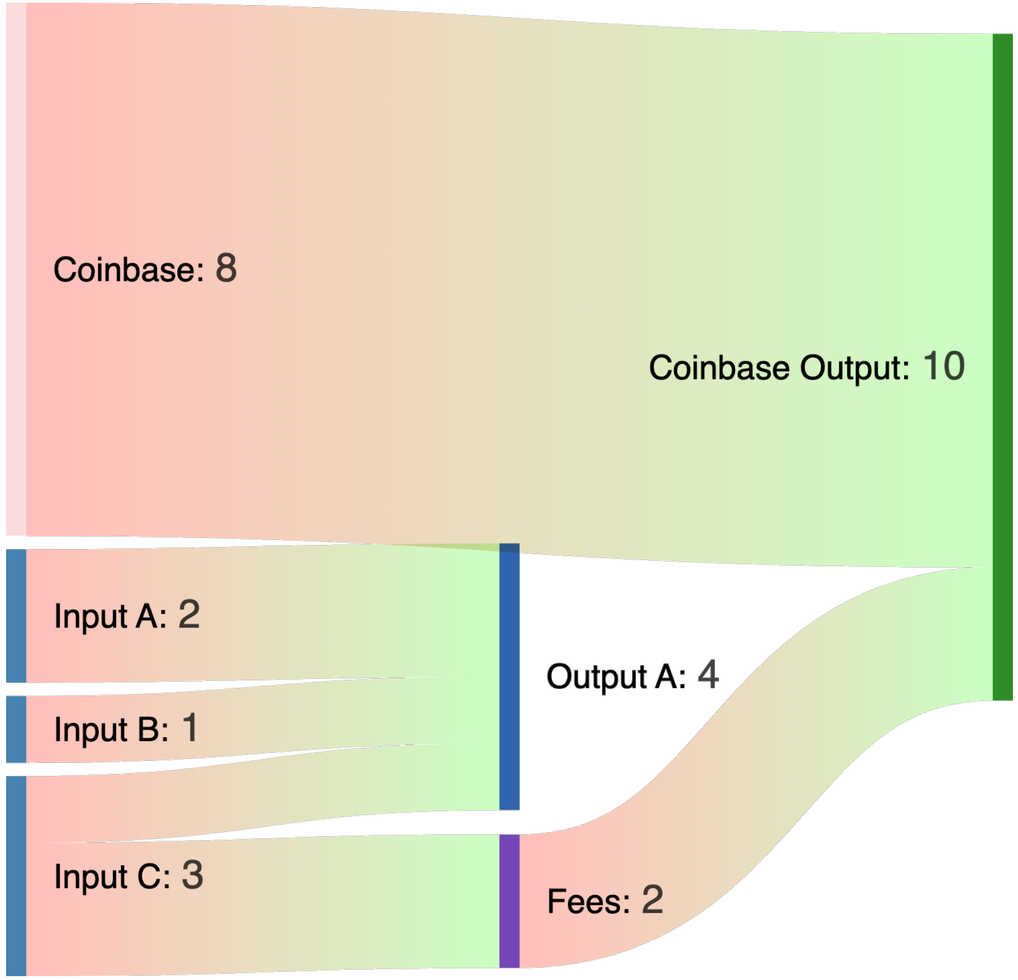
Ordinal Flow

Inputs	Outputs
2	4
1	
3	



Ordinal Flow

Inputs	Outputs
2	4
1	
3	



Ordinal Inscriptions

- Attached to one satoshi
- Any content type
- Content length constraints:
  - Block size (hard)
  - Transaction relay limit (soft)

What's Broken

- Script evaluation
- OP-Code parsing
- MIME Type Recognition
- Defacing

Inscription Scripts

```
OP_FALSE
OP_IF
    OP_PUSH "ord"
    OP_1
    OP_PUSH "text/plain;charset=utf-8"
    OP_0
    OP_PUSH "Hello, world!"
OP_ENDIF
```

Inscription Scripts

```
OP_FALSE
OP_IF
    OP_PUSH "ord"
    OP_1
    OP_PUSH "text/plain"
    OP_0
    OP_PUSH "Hello, world!"
OP_ENDIF
```

```
00
63
    036f7264
    51
    0a746578742f706c61696e
    00
    0d48656c6c6f2c20576f726c6421
68
```

Inscription Scripts

```
OP_TRUE
OP_FALSE
OP_IF
    OP_PUSH "ord"
    OP_1
    OP_PUSH "text/plain"
    OP_0
    OP_PUSH "Hello, world!"
OP_ENDIF
```

```
51
00
63
    036f7264
    51
    0a746578742f706c61696e
    00
    0d48656c6c6f2c20576f726c6421
68
```

Inscription Scripts

```
OP_TRUE
OP_FALSE
OP_IF
    OP_PUSH "ord"
    OP_PUSH 0x01
    OP_PUSH "text/plain"
    OP_0
    OP_PUSH "Hello, world!"
OP_ENDIF
```

```
51
00
63
    036f7264
    0101
    0a746578742f706c61696e
    00
    0d48656c6c6f2c20576f726c6421
68
```

Inscription Scripts

```
<pubkey> OP_CHECKSIG
OP_FALSE
OP_IF
    OP_PUSH "ord"
    OP_PUSH 0x01
    OP_PUSH "text/plain"
    OP_0
    OP_PUSH "Hello, world!"
OP_ENDIF
```

```
20<pubkey>ac
00
63
    036f7264
    0101
    0a746578742f706c61696e
    00
    0d48656c6c6f2c20576f726c6421
68
```

Demo