coinbase

Smart contracts: Approach with caution

Jake Craige
Crypto Payments Engineering

Ethereum Devcon4, 2018

Who should care?

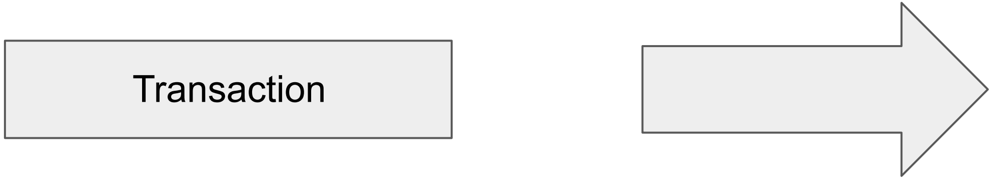
Who should care?

- Exchanges
- Wallets
- Explorers

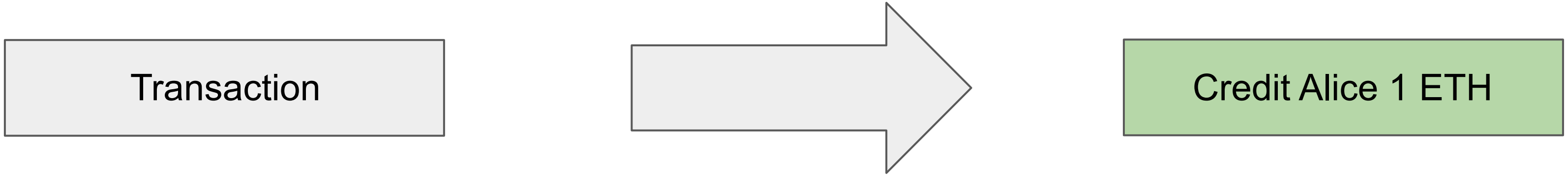
Who should care?

- Exchanges
- Wallets
- Explorers
- Anyone building on Ethereum

Why?



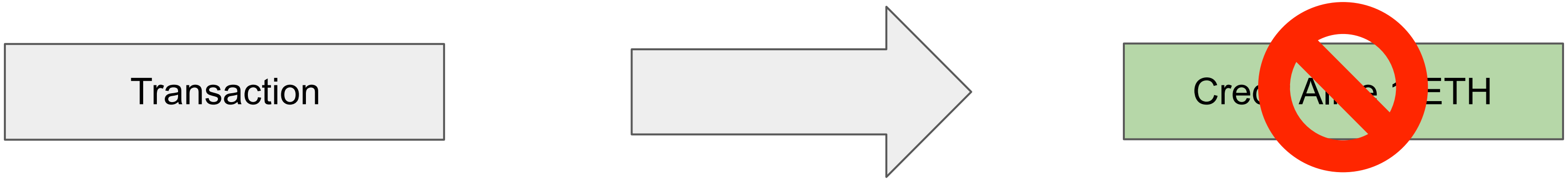
Why?



Transaction

Credit Alice 1 ETH

Why?



Transaction

Credit Alice 1 ETH

Why?

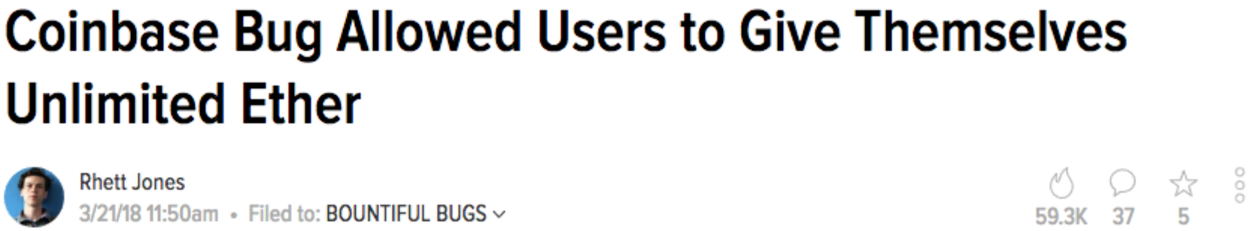
Invalid Data

Why?

Invalid Data

Lost Funds

Why?



Coinbase Bug Allowed Users to Give Themselves Unlimited Ether

Rhett Jones

3/21/18 11:50am • Filed to: BOUNTIFUL BUGS

59.3K 37 5

Why?

Ethereum account balance manipulation

ETH contract handling errors

So, what can go wrong?

How does ether move?

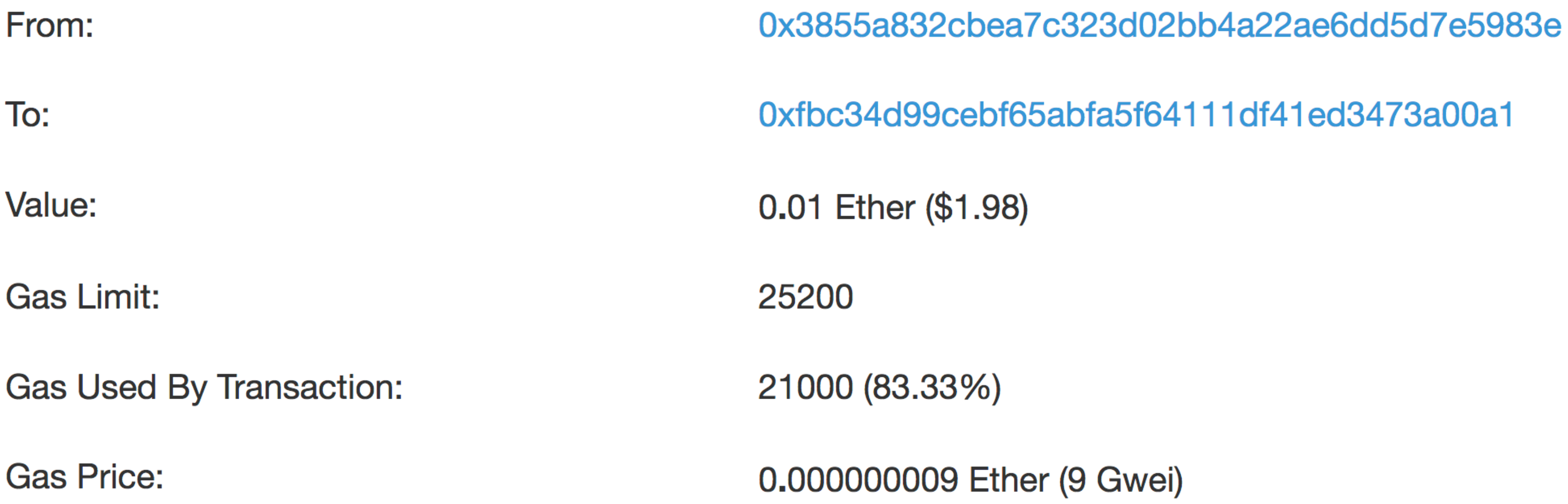
How does ether move?

- Account Transfers

How does ether move?

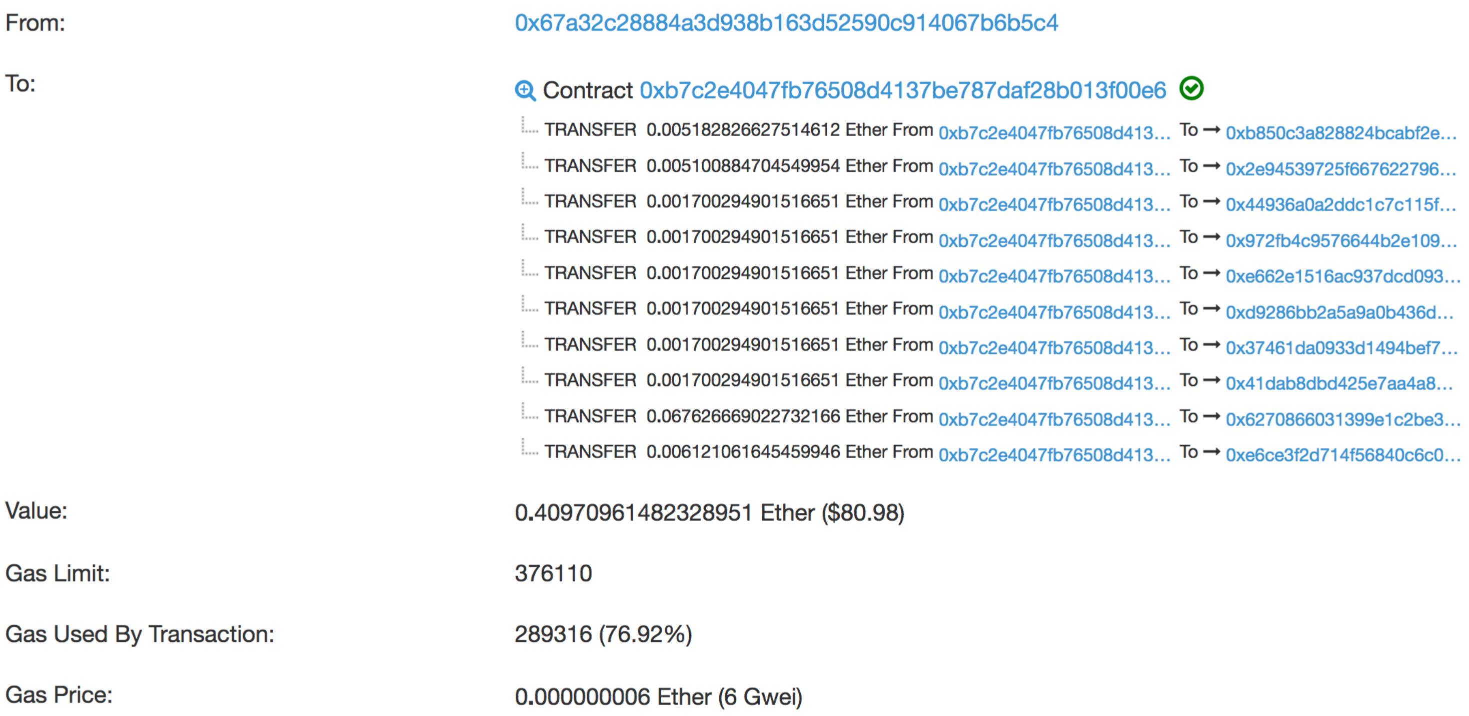
- Account Transfers
- Contract Transfers

Account Transfer



From:	0x3855a832cbea7c323d02bb4a22ae6dd5d7e5983e
To:	0xfbc34d99cebf65abfa5f64111df41ed3473a00a1
Value:	0.01 Ether ($1.98)
Gas Limit:	25200
Gas Used By Transaction:	21000 (83.33%)
Gas Price:	0.000000009 Ether (9 Gwei)

Contract Transfer



From:	0x67a32c28884a3d938b163d52590c914067b6b5c4
To:	Contract 0xb7c2e4047fb76508d4137be787daf28b013f00e6 ✓ TRANSFER 0.005182826627514612 Ether From 0xb7c2e4047fb76508d413... To → 0xb850c3a828824bcabf2e... TRANSFER 0.005100884704549954 Ether From 0xb7c2e4047fb76508d413... To → 0x2e94539725f667622796... TRANSFER 0.001700294901516651 Ether From 0xb7c2e4047fb76508d413... To → 0x44936a0a2ddc1c7c115f... TRANSFER 0.001700294901516651 Ether From 0xb7c2e4047fb76508d413... To → 0x972fb4c9576644b2e109... TRANSFER 0.001700294901516651 Ether From 0xb7c2e4047fb76508d413... To → 0xe662e1516ac937dcd093... TRANSFER 0.001700294901516651 Ether From 0xb7c2e4047fb76508d413... To → 0xd9286bb2a5a9a0b436d... TRANSFER 0.001700294901516651 Ether From 0xb7c2e4047fb76508d413... To → 0x37461da0933d1494bef7... TRANSFER 0.001700294901516651 Ether From 0xb7c2e4047fb76508d413... To → 0x41dab8dbd425e7aa4a8... TRANSFER 0.067626669022732166 Ether From 0xb7c2e4047fb76508d413... To → 0x6270866031399e1c2be3... TRANSFER 0.006121061645459946 Ether From 0xb7c2e4047fb76508d413... To → 0xe6ce3f2d714f56840c6c0...
Value:	0.40970961482328951 Ether ($80.98)
Gas Limit:	376110
Gas Used By Transaction:	289316 (76.92%)
Gas Price:	0.000000006 Ether (6 Gwei)

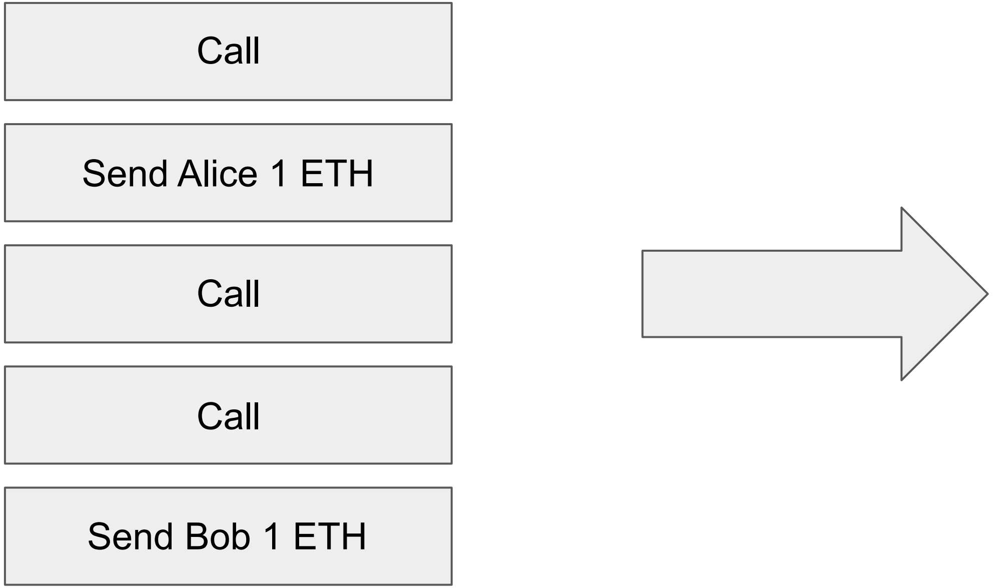
Transaction Trace

```
[
  {
    "action": {
      "callType": "call",
      "from": "0x2dc772d3d7ae59f80e6bf1f69234cdc477cd2517",
      "gas": "0x2b39",
      "input": "0xd018db3e00000000000000000000000028eefc16be1156146d0c4d15f890faa01306af49",
      "to": "0xf171d6dee1176af9ff3358cebc55b0b1a9ad1de1",
      "value": "0x38d7ea4c68000"
    },
    "blockHash": "0x03a812fd4867abf603d91594e0cb4a17b60b190793376555c19b01a0ae6136d9",
    "blockNumber": 3034561,
    "result": {
      "gasUsed": "0x22b5",
      "output": "0x0000000000000000000000000000000000000000000000000000000000000001"
    },
    "subtraces": 2,
    "traceAddress": [],
    "transactionHash": "0xd5bd8fd17998c2393ab565e58f4afdf7696d82e9c85b377cce73de2d435ddd14",
    "transactionPosition": 28,
    "type": "call"
  },
  {
    "action": {
      "callType": "delegatecall",
      "from": "0xf171d6dee1176af9ff3358cebc55b0b1a9ad1de1",
      "gas": "0x2726",
      "input": "0x",
      "to": "0x28eefc16be1156146d0c4d15f890faa01306af49",
      "value": "0x38d7ea4c68000"
    },
    "blockHash": "0x03a812fd4867abf603d91594e0cb4a17b60b190793376555c19b01a0ae6136d9",
    "blockNumber": 3034561,
    "result": {
      "gasUsed": "0x0",
      "output": "0x"
    },
    "subtraces": 0,
    "traceAddress": [
      0
    ],
    "transactionHash": "0xd5bd8fd17998c2393ab565e58f4afdf7696d82e9c85b377cce73de2d435ddd14",
    "transactionPosition": 28,
    "type": "call"
  },
  {
    "action": {
      "callType": "call",
      "from": "0xf171d6dee1176af9ff3358cebc55b0b1a9ad1de1",
      "gas": "0x8fc",
      "input": "0x",
      "to": "0x2dc772d3d7ae59f80e6bf1f69234cdc477cd2517",
      "value": "0x38d7ea4c68000"
    },
    "blockHash": "0x03a812fd4867abf603d91594e0cb4a17b60b190793376555c19b01a0ae6136d9",
    "blockNumber": 3034561,
    "result": {
      "gasUsed": "0x0",
      "output": "0x"
    },
    "subtraces": 0,
    "traceAddress": [
      1
    ],
    "transactionHash": "0xd5bd8fd17998c2393ab565e58f4afdf7696d82e9c85b377cce73de2d435ddd14",
    "transactionPosition": 28,
    "type": "call"
  }
]
```

Transaction Trace

```
"action": {
  "callType": "call",
  "from": "0x2dc772d3d7ae59f80e6bf1f69234cdc477cd2517",
  "gas": "0x2b39",
  "input": “0xd018db3e0000000000000000…”,
  "to": "0xf171d6dee1176af9ff3358cebc55b0b1a9ad1de1",
  "value": "0x38d7ea4c68000"
},
"blockHash": “0x03a812fd4867abf603d91594e0cb4…”,
"blockNumber": 3034561,
"result": {
  "gasUsed": "0x22b5",
  "output": “0x0000000000000000000000000000000000000…”
},
```

Example #1



Call

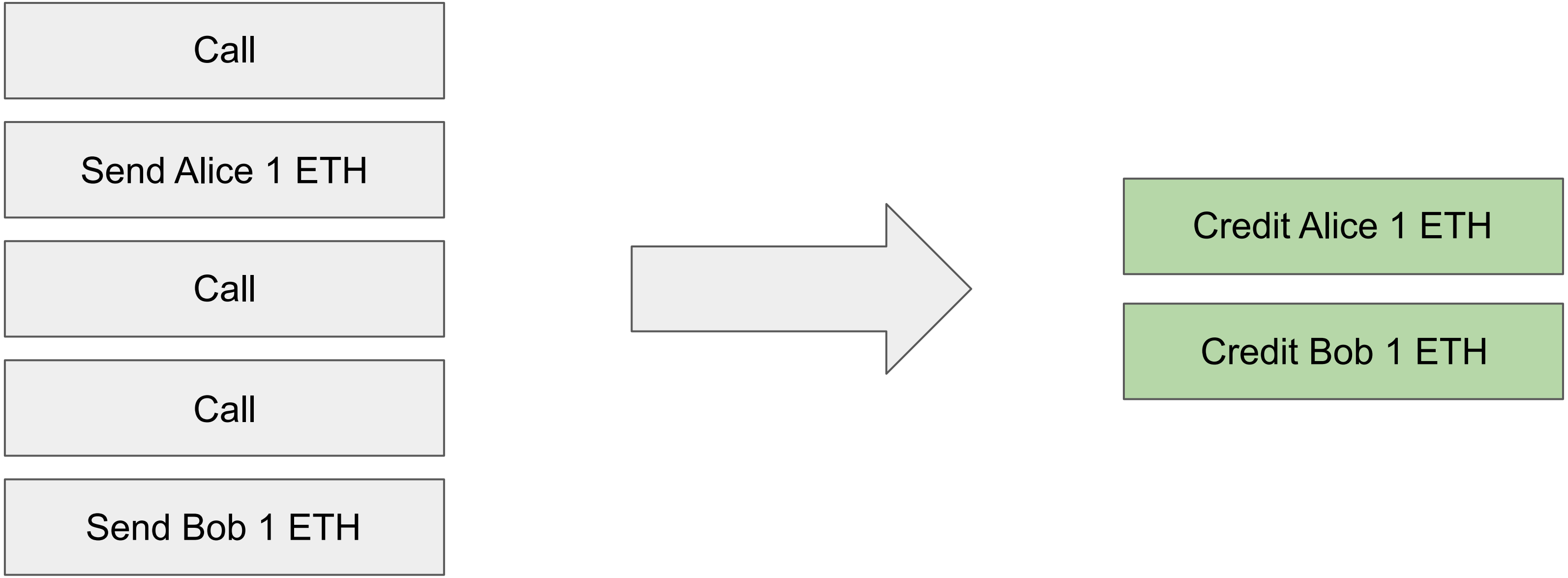
Send Alice 1 ETH

Call

Call

Send Bob 1 ETH

Example #1



Call

Send Alice 1 ETH

Call

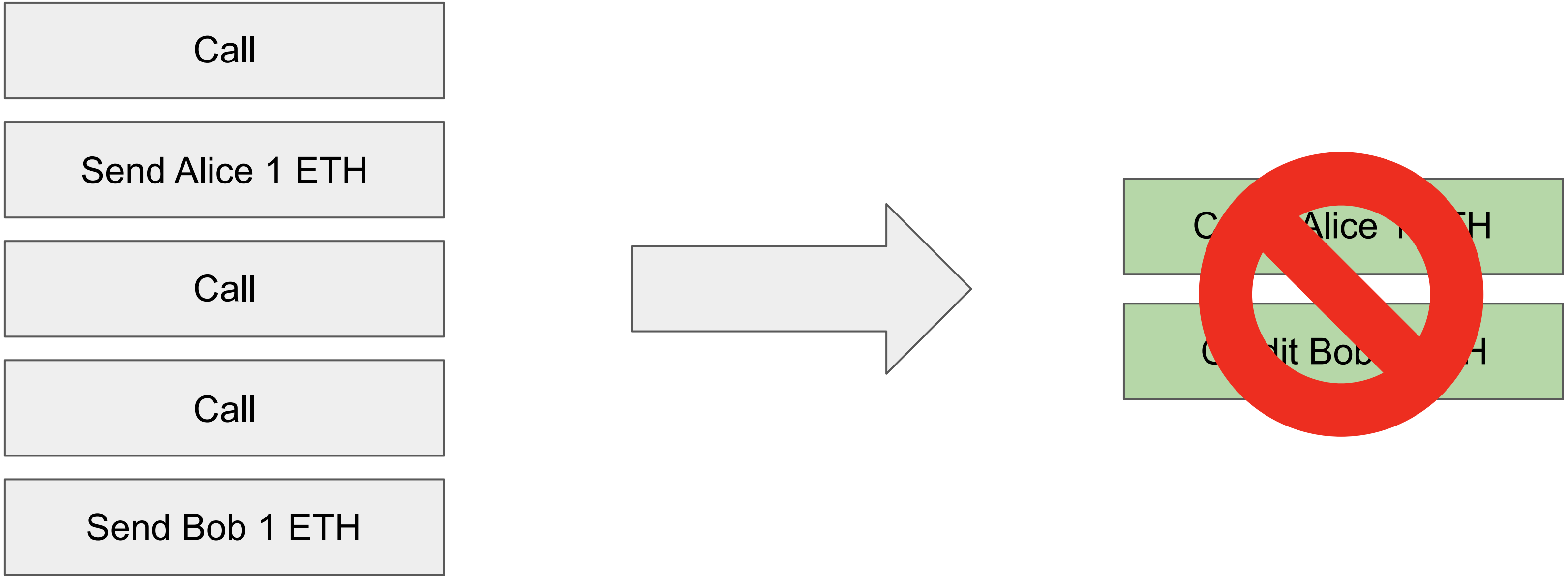
Call

Send Bob 1 ETH

Credit Alice 1 ETH

Credit Bob 1 ETH

Example #1



Call

Send Alice 1 ETH

Call

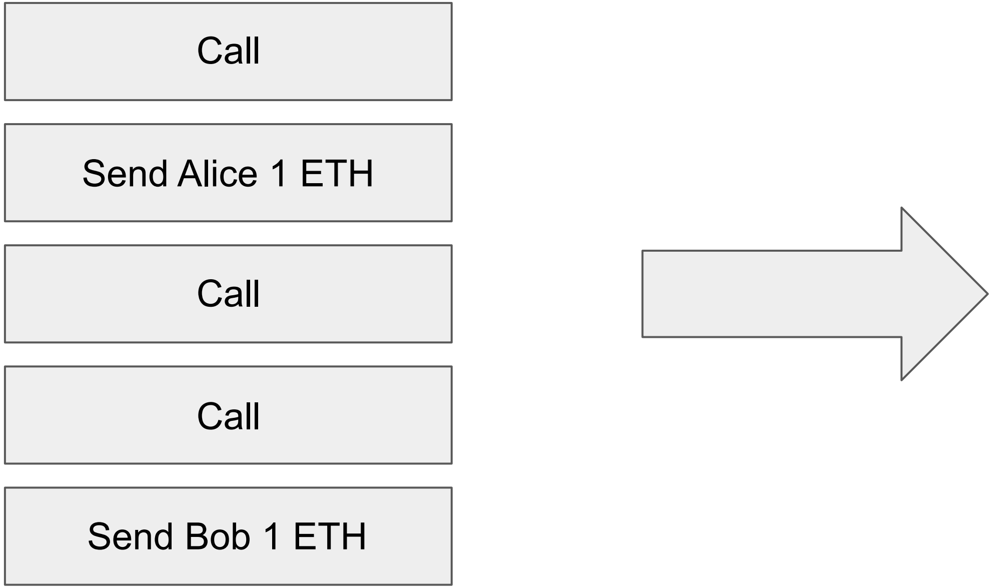
Call

Send Bob 1 ETH

C Alice 1 TH

C dit Bob H

Example #1



Call

Send Alice 1 ETH

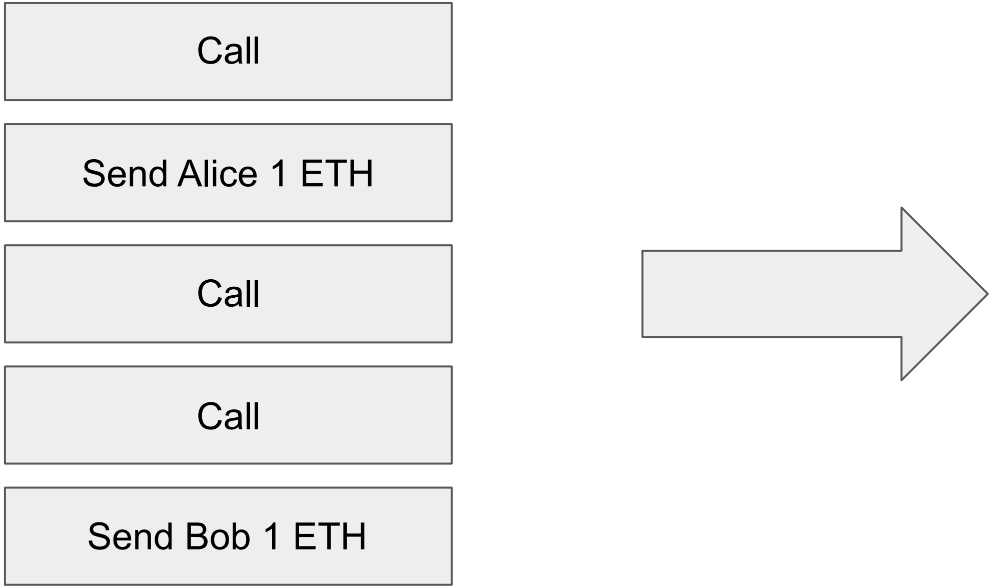
Call

Call

Send Bob 1 ETH

Example #1

Transaction status: **Failure**



Call

Send Alice 1 ETH

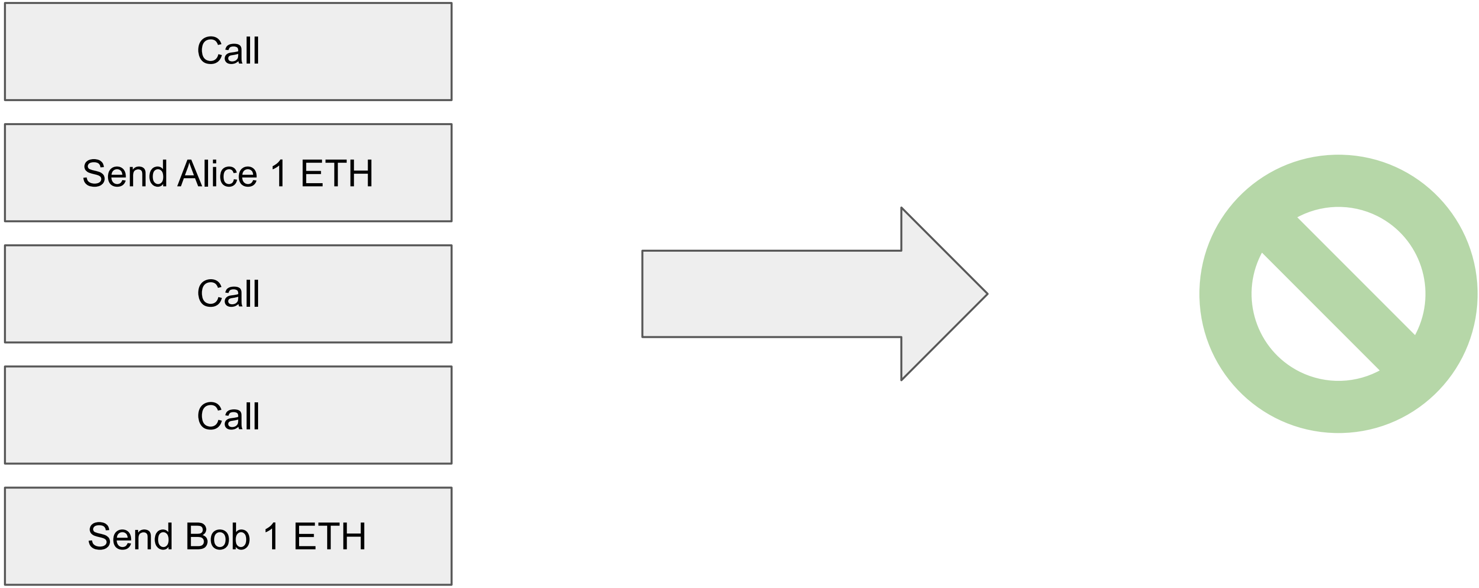
Call

Call

Send Bob 1 ETH

Example #1

Transaction status: **Failure**



Call

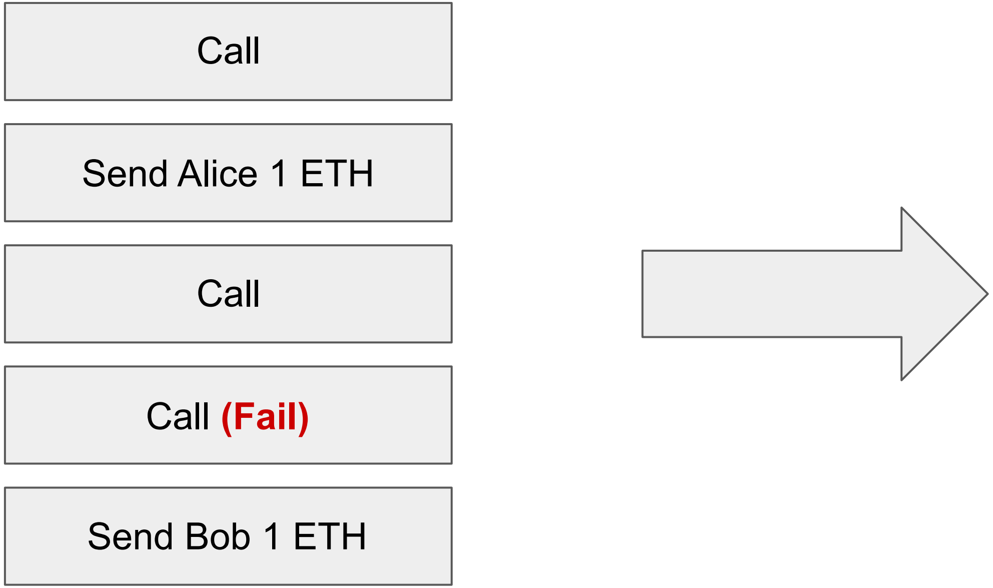
Send Alice 1 ETH

Call

Call

Send Bob 1 ETH

Example #2



Call

Send Alice 1 ETH

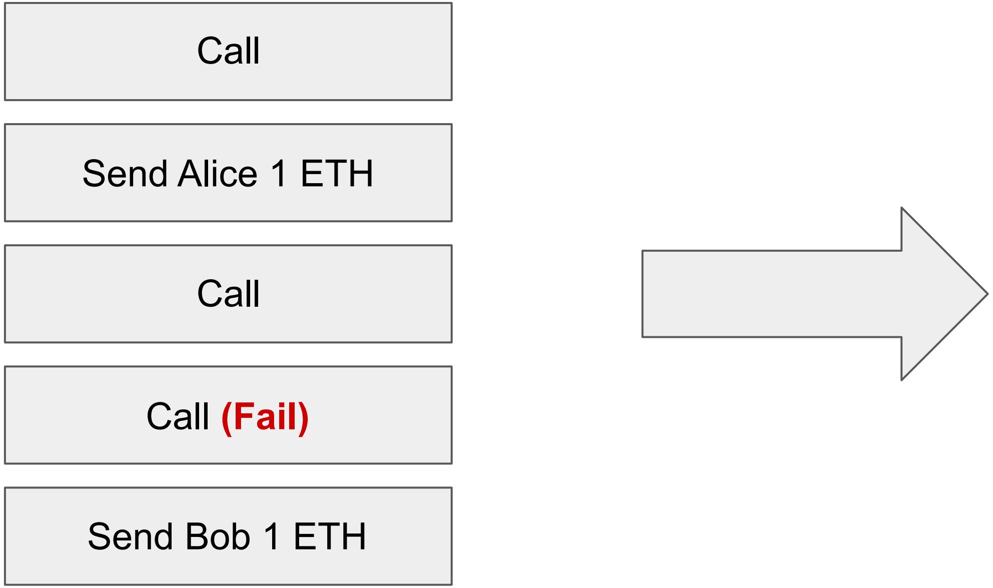
Call

Call **(Fail)**

Send Bob 1 ETH

Example #2

Transaction status: **Success**



Call

Send Alice 1 ETH

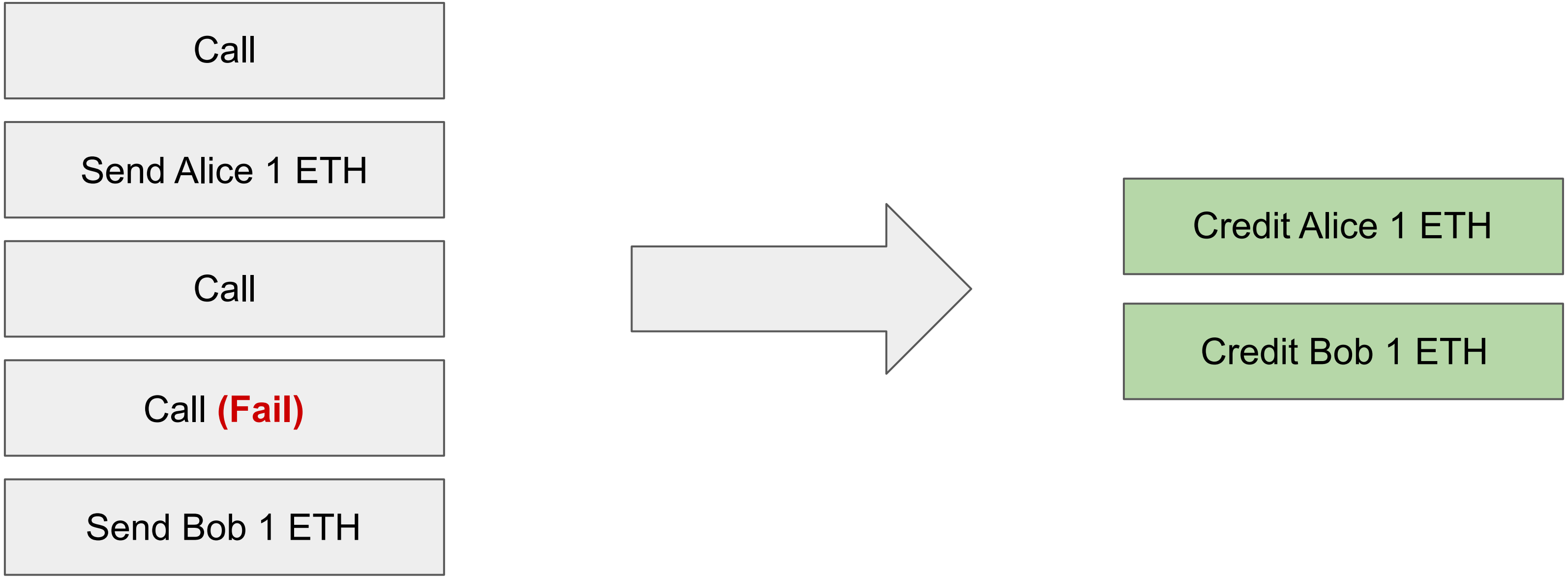
Call

Call **(Fail)**

Send Bob 1 ETH

Example #2

Transaction status: **Success**



Call

Send Alice 1 ETH

Call

Call **(Fail)**

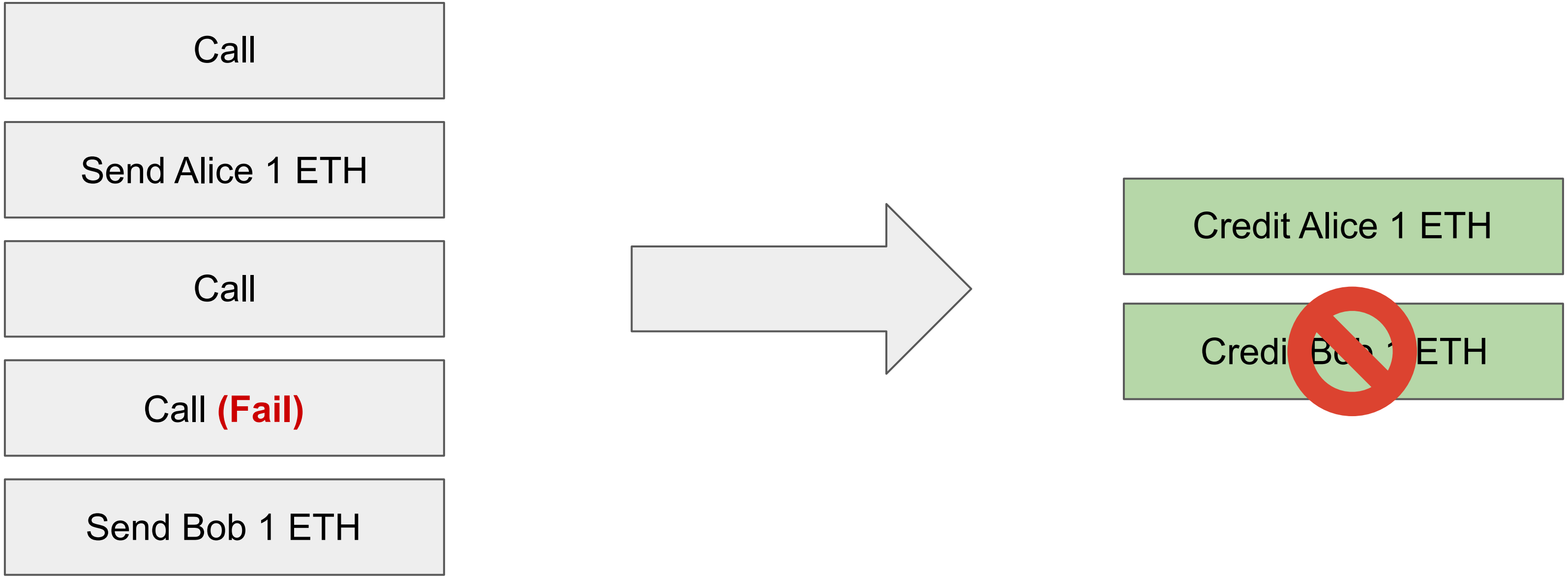
Send Bob 1 ETH

Credit Alice 1 ETH

Credit Bob 1 ETH

Example #2

Transaction status: **Success**



Call

Send Alice 1 ETH

Call

Call **(Fail)**

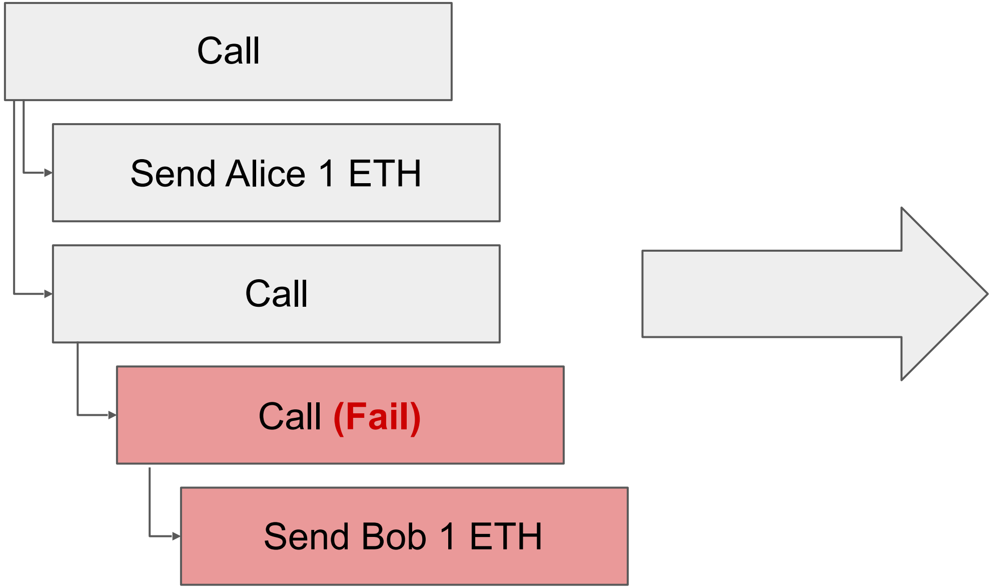
Send Bob 1 ETH

Credit Alice 1 ETH

Credit Bob 1 ETH

Example #2

Transaction status: **Success**



Call

Send Alice 1 ETH

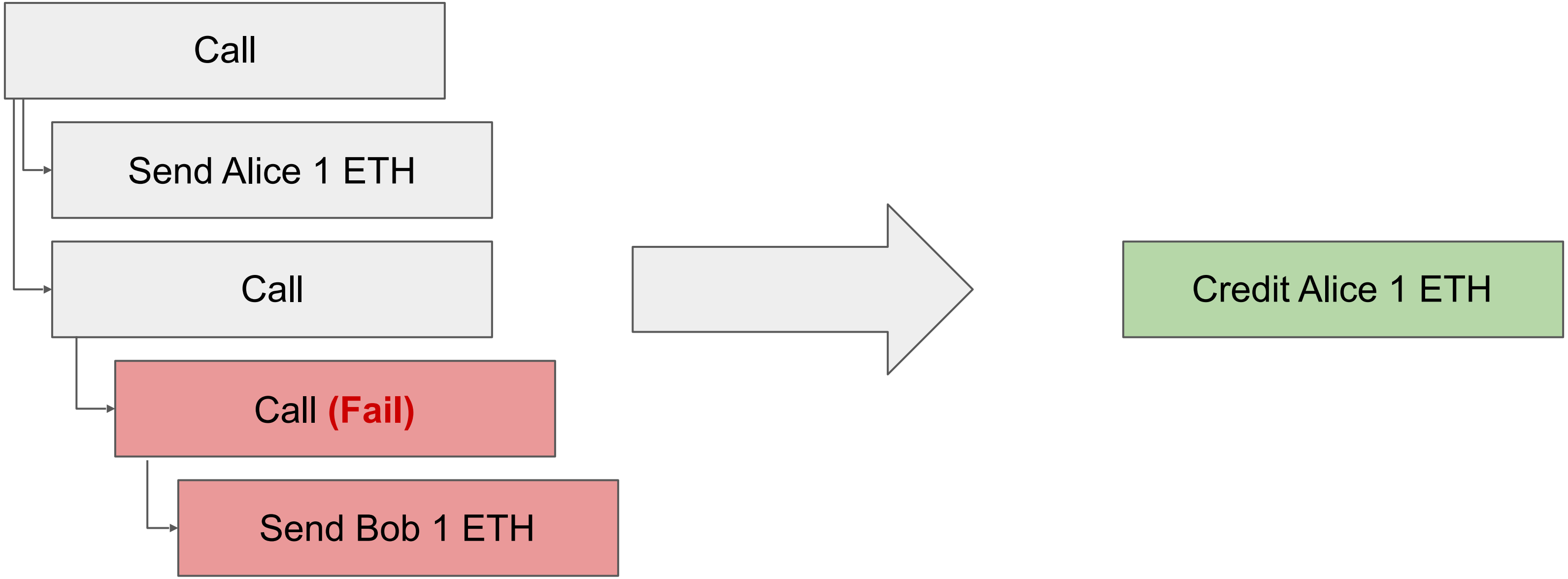
Call

Call **(Fail)**

Send Bob 1 ETH

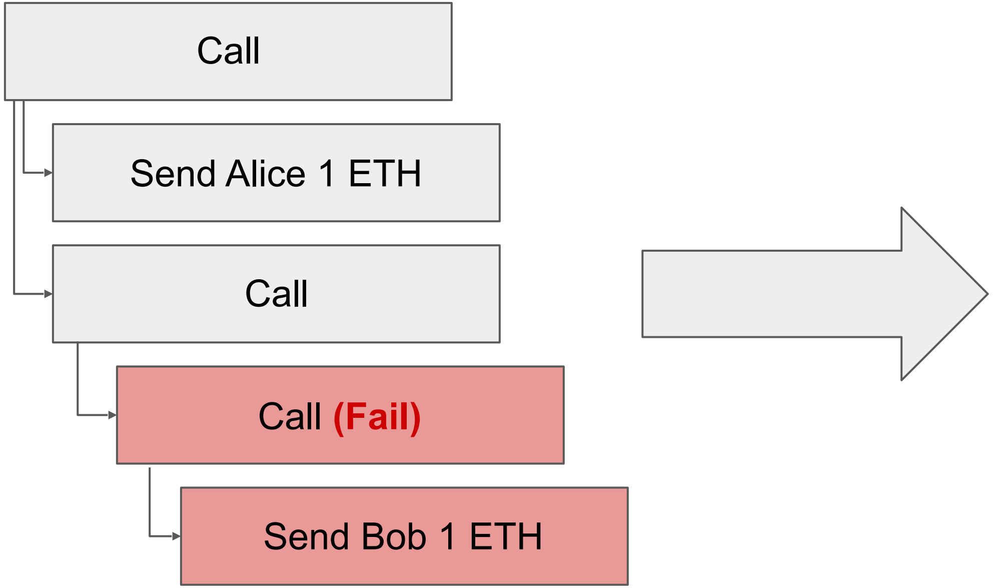
Example #2

Transaction status: **Success**



Example #3

Transaction status: **Success**



Call

Send Alice 1 ETH

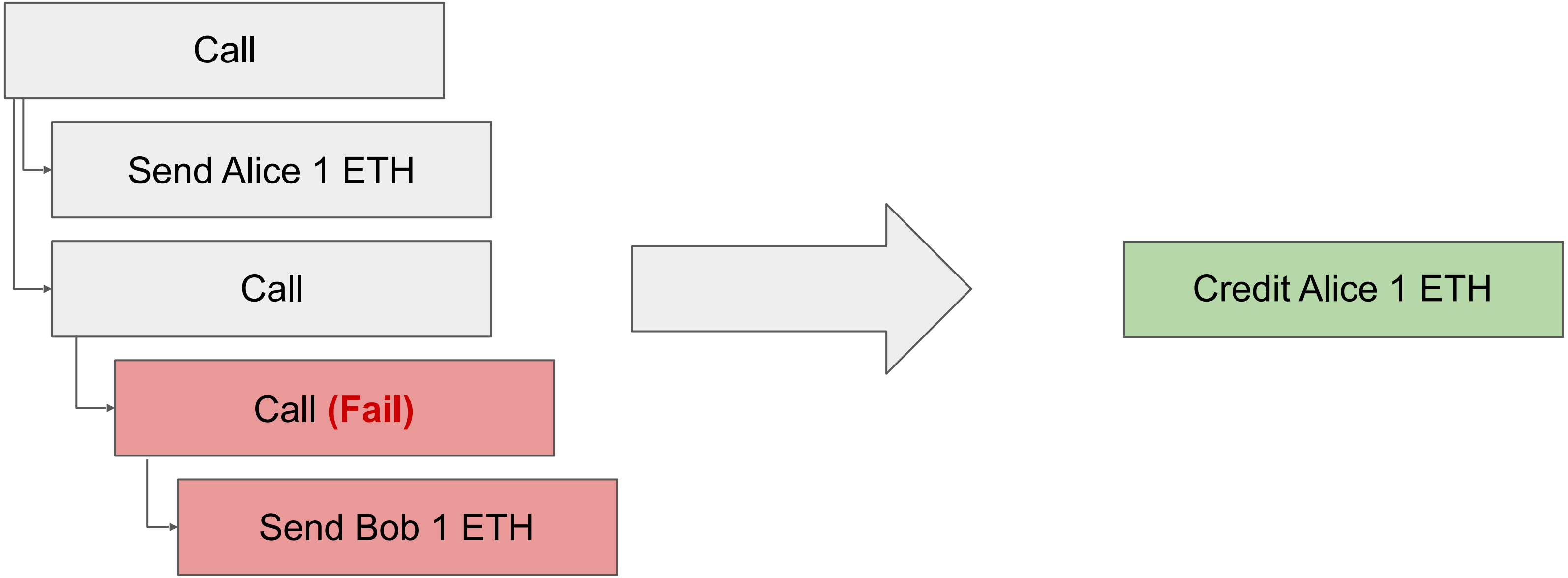
Call

Call **(Fail)**

Send Bob 1 ETH

Example #3

Transaction status: **Success**



Call

Send Alice 1 ETH

Call

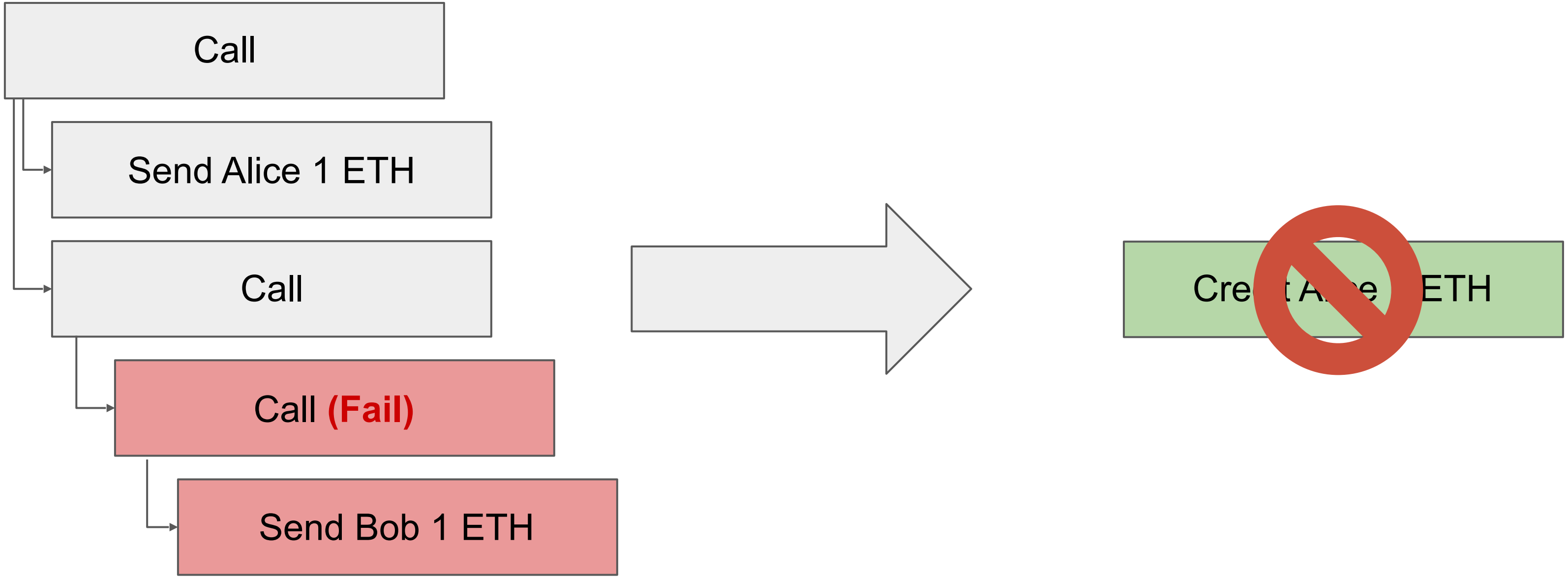
Call **(Fail)**

Send Bob 1 ETH

Credit Alice 1 ETH

Example #3

Transaction status: **Success**



Call

Send Alice 1 ETH

Call

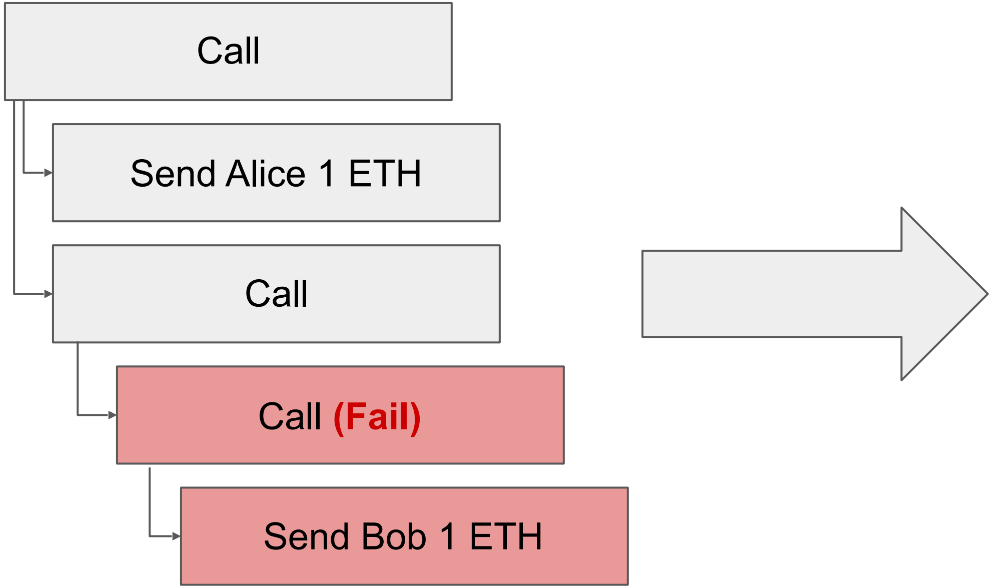
Call **(Fail)**

Send Bob 1 ETH

Cre t A e ETH

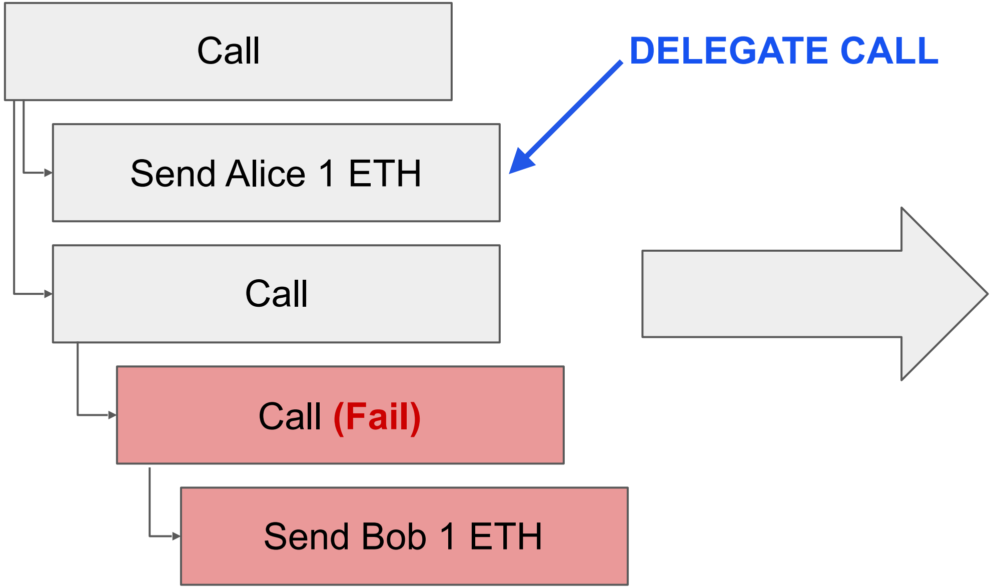
Example #3

Transaction status: **Success**



Example #3

Transaction status: **Success**



Call

Send Alice 1 ETH

Call

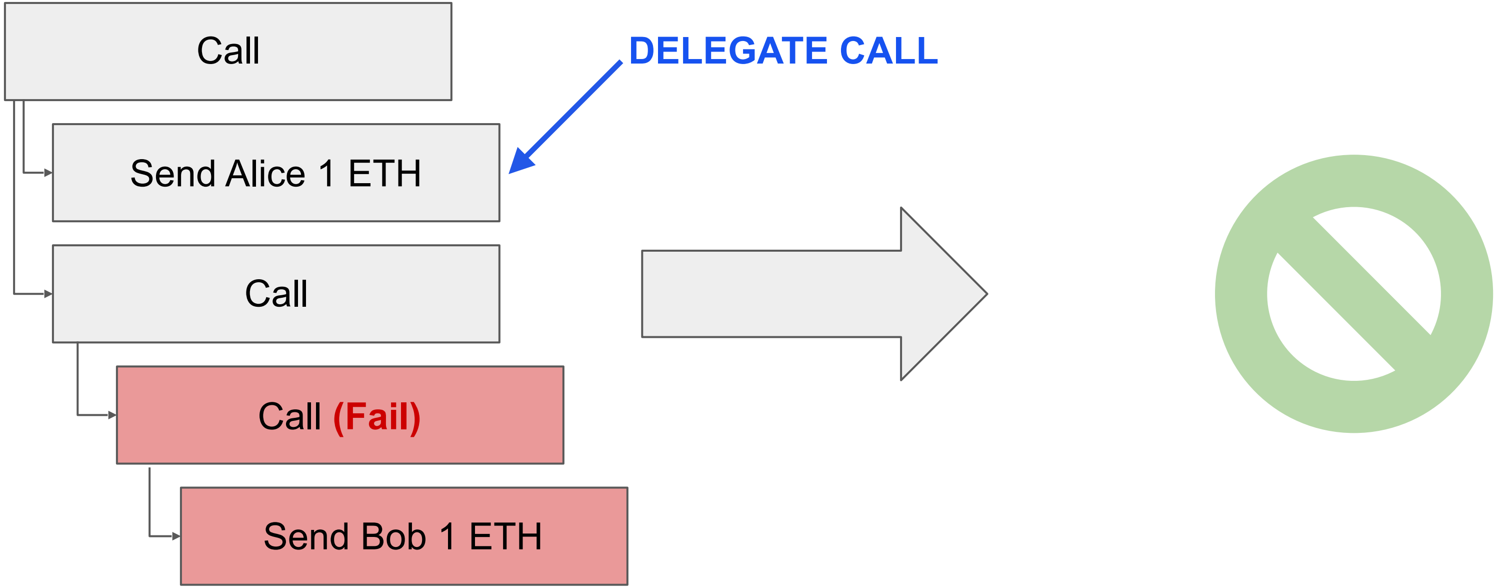
Call **(Fail)**

Send Bob 1 ETH

DELEGATE CALL

Example #3

Transaction status: **Success**



Minimizing Risk

Detection & Response

Detection & Response

- Don’t assume you know everything

Detection & Response

- Don’t assume you know everything
- Cross-check your data with other sources

Detection & Response

- Don’t assume you know everything
- Cross-check your data with other sources
- If something is off, **fail securely**

Four Takeaways

Takeaway #1

Always check the transaction receipt status

Takeaway #2

Takeaway #2

Parse the trace as a tree

Takeaway #2

Parse the trace as a tree

Takeaway #2

Parse the trace as a tree

Fail errored subtrees

Takeaway #3

Takeaway #3

Reject delegate and callcode calls

Takeaway #3

~~Reject delegate and callcode calls~~

Select call, create, selfdestruct and rewards calls

Takeaway #4

Takeaway #4

Don’t trust, until verified

Takeaway #4

Don’t trust, until verified

Stay safe out there.

Jake Craige // @jakecraige