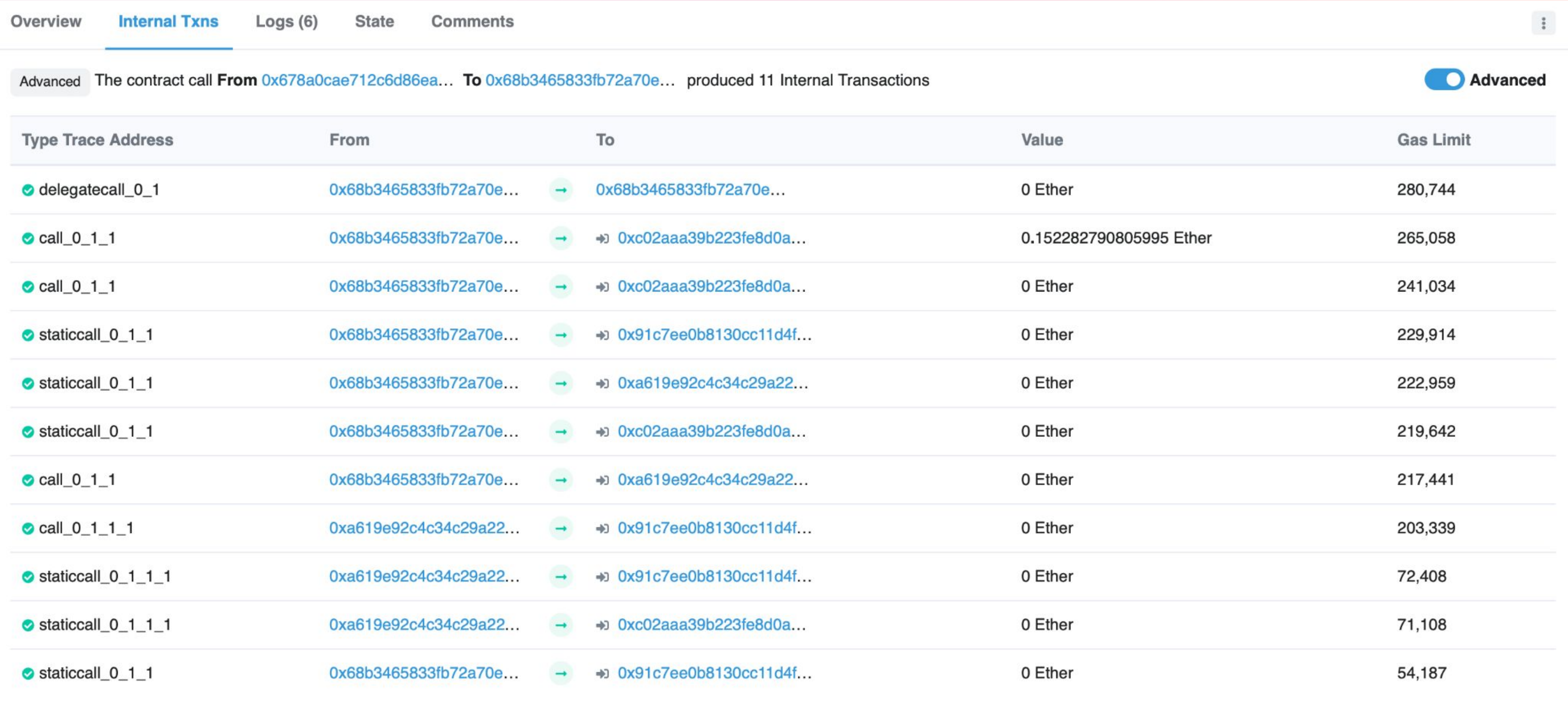
EVM Tracing in go-ethereum

From zero to hero

Sina Mahmoodi

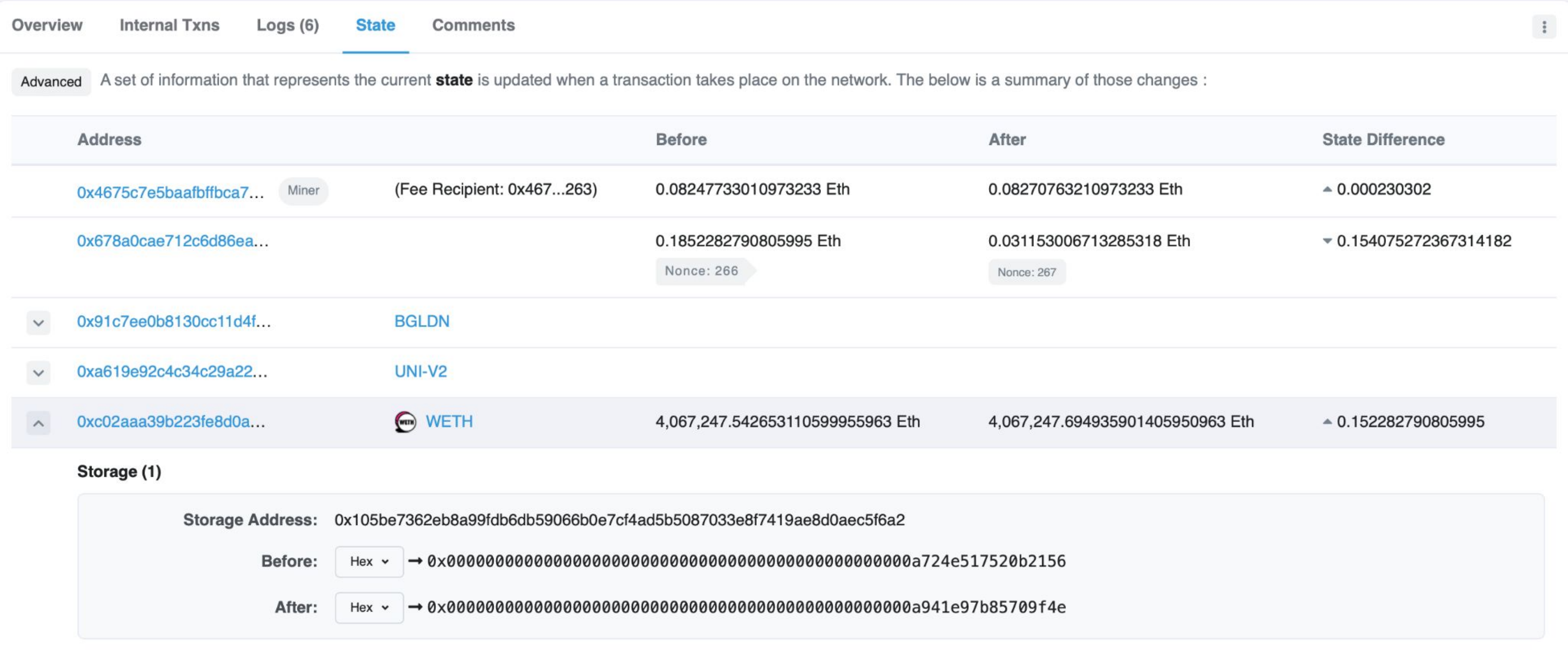
Ethereum Foundation

A few words...



Advanced The contract call **From** 0x678a0cae712c6d86ea… **To** 0x68b3465833fb72a70e… produced 11 Internal Transactions

Type Trace Address	From		To	Value	Gas Limit
✓ delegatecall_0_1	0x68b3465833fb72a70e…	→	0x68b3465833fb72a70e…	0 Ether	280,744
✓ call_0_1_1	0x68b3465833fb72a70e…	→	0xc02aaa39b223fe8d0a…	0.152282790805995 Ether	265,058
✓ call_0_1_1	0x68b3465833fb72a70e…	→	0xc02aaa39b223fe8d0a…	0 Ether	241,034
✓ staticcall_0_1_1	0x68b3465833fb72a70e…	→	0x91c7ee0b8130cc11d4f…	0 Ether	229,914
✓ staticcall_0_1_1	0x68b3465833fb72a70e…	→	0xa619e92c4c34c29a22…	0 Ether	222,959
✓ staticcall_0_1_1	0x68b3465833fb72a70e…	→	0xc02aaa39b223fe8d0a…	0 Ether	219,642
✓ call_0_1_1	0x68b3465833fb72a70e…	→	0xa619e92c4c34c29a22…	0 Ether	217,441
✓ call_0_1_1_1	0xa619e92c4c34c29a22…	→	0x91c7ee0b8130cc11d4f…	0 Ether	203,339
✓ staticcall_0_1_1_1	0xa619e92c4c34c29a22…	→	0x91c7ee0b8130cc11d4f…	0 Ether	72,408
✓ staticcall_0_1_1_1	0xa619e92c4c34c29a22…	→	0xc02aaa39b223fe8d0a…	0 Ether	71,108
✓ staticcall_0_1_1	0x68b3465833fb72a70e…	→	0x91c7ee0b8130cc11d4f…	0 Ether	54,187



Overview | Internal Txns | Logs (6) | State | Comments

Advanced A set of information that represents the current **state** is updated when a transaction takes place on the network. The below is a summary of those changes :

Address		Before	After	State Difference
0x4675c7e5baafbffbca7... Miner	(Fee Recipient: 0x467...263)	0.08247733010973233 Eth	0.08270763210973233 Eth	▲ 0.000230302
0x678a0cae712c6d86ea...		0.1852282790805995 Eth Nonce: 266	0.031153006713285318 Eth Nonce: 267	▼ 0.154075272367314182
0x91c7ee0b8130cc11d4f...	BGLDN			
0xa619e92c4c34c29a22...	UNI-V2			
0xc02aaa39b223fe8d0a...	WETH	4,067,247.542653110599955963 Eth	4,067,247.694935901405950963 Eth	▲ 0.152282790805995

Storage (1)

Storage Address: 0x105be7362eb8a99fdb6db59066b0e7cf4ad5b5087033e8f7419ae8d0aec5f6a2

Before: Hex → 0x000000000000000000000000000000000000000000000000a724e517520b2156

After: Hex → 0x000000000000000000000000000000000000000000000000a941e97b85709f4e

Section 1

Basics of tracing

eth_call

```
eth.call({
    from: '0x00',
    to: ’WETH_TOKEN_ADDRESS’,
    data: 'encode(“balanceOf(address)”, “0x00”)’
})
```

debug_traceCall

```
debug.traceCall({
  from: '0x00',
  to: 'WETH_TOKEN_ADDRESS',
  data: 'encode("balanceOf(address)", "0x00")'
}, 'latest')
```

Tracing historical transactions

- debug_traceTransaction
- debug_traceBlockByNumber/Hash
- debug_traceChain
    - Subscription API via Websocket

Section 2

Built-in tracers

Opcode tracer

Field	Type	Desc
pc	uint64	Program counter
op	byte	Opcode name
gas	uint64	Remaining gas
gasCost	uint64	Cost of opcode
memory	[]byte	Memory
memSize	int	Memory size
stack	[]uint256	Stack
returnData	[]byte	Last call’s return data
storage	map[hash]hash	Accessed storage
depth	int	Call depth
refund	uint64	Refund counter
error	string	Error message

Opcode tracer notes

- Memory, stack, return data, and storage can be disabled/enabled
- Watch out for memory
    - Tracing #14742200 fails with 64Gb memory 💥
- If you control node, consider **debug_standardTraceBlockToFile**

Call tracer

```
debug.traceCall(
    {...},
    'latest',
    { tracer: 'callTracer'}
)

debug.traceTransaction(
    TX_HASH,
    { tracer: 'callTracer'}
)
```

Prestate tracer

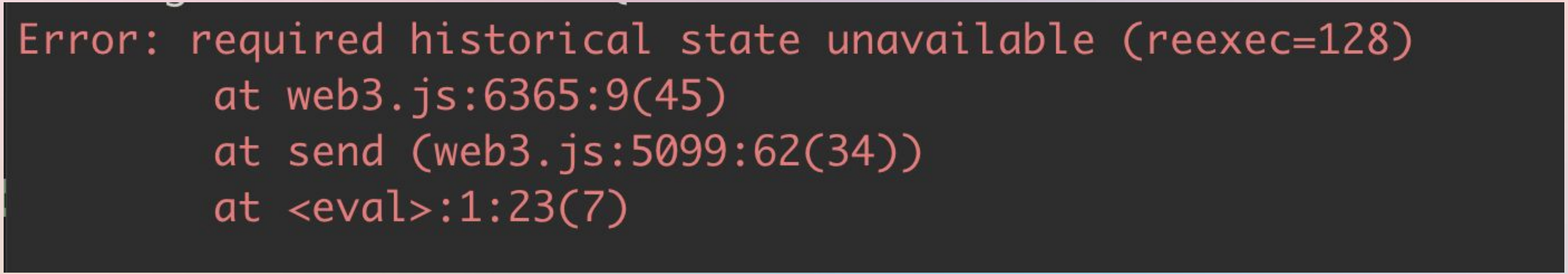
Two modes:

- Prestate: outputs accounts which are needed to execute a tx
- Diff: outputs the modifications to state during a tx (as in etherscan)

State pruning

Ever seen this error?

Tracing needs the state prior to the given historical tx



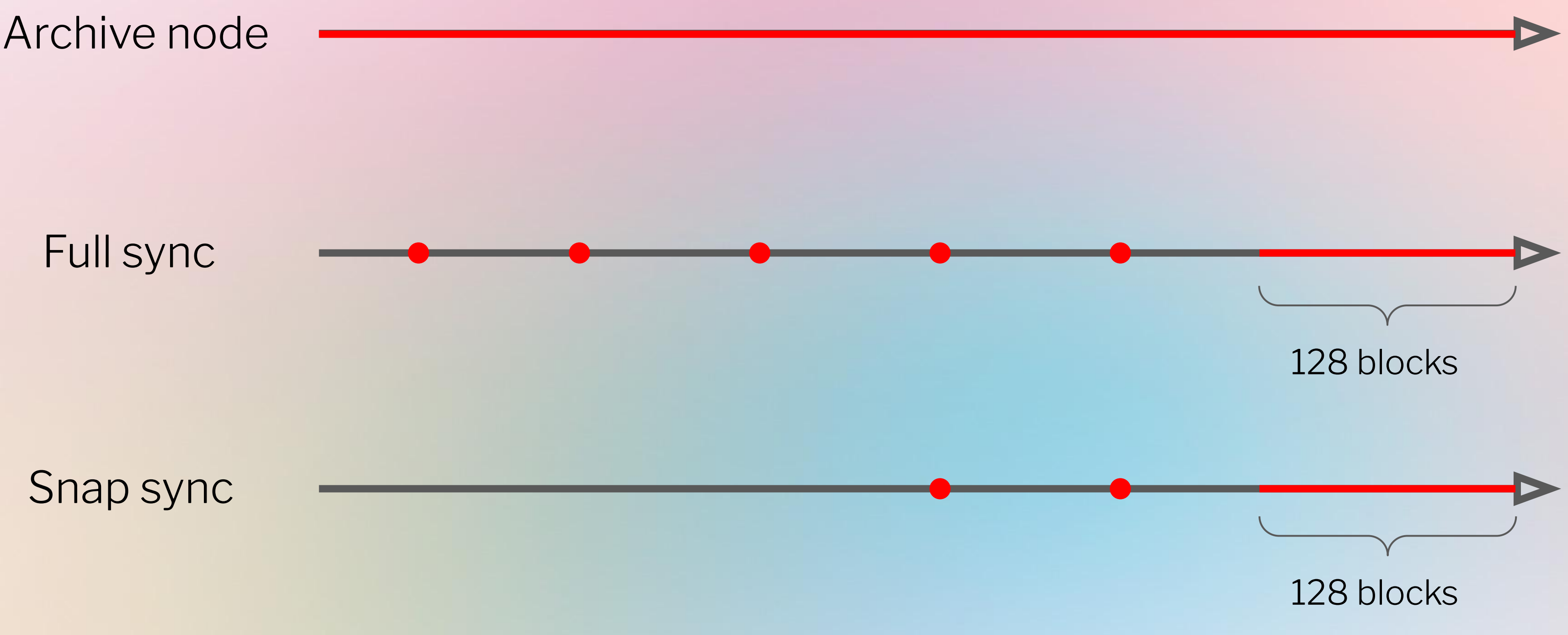
```
Error: required historical state unavailable (reexec=128)
        at web3.js:6365:9(45)
        at send (web3.js:5099:62(34))
        at <eval>:1:23(7)
```

How is the state prepared?

- Fetch state of parent block from database
- Execute txes in block until just before target tx

But what if state of previous block is NOT in db?

State persistence



Reexec

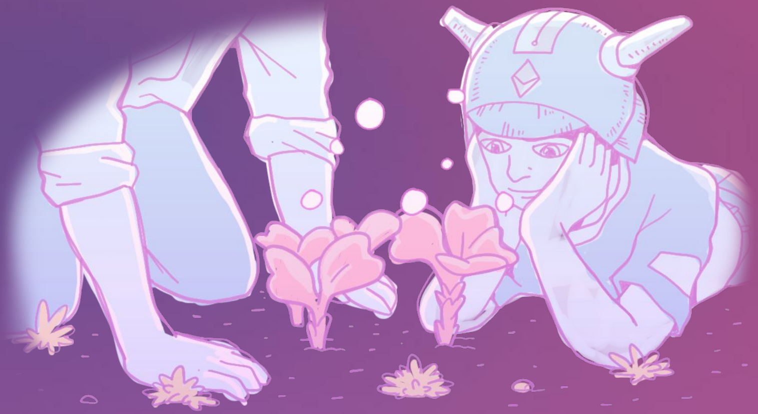
How state is prepared, take 2:

- Fetch state of parent block from database
- If not available:
  - Go back up to `reexec` blocks for first available state
  - Execute blocks sequentially to build up state
- Execute txes in block until just before target

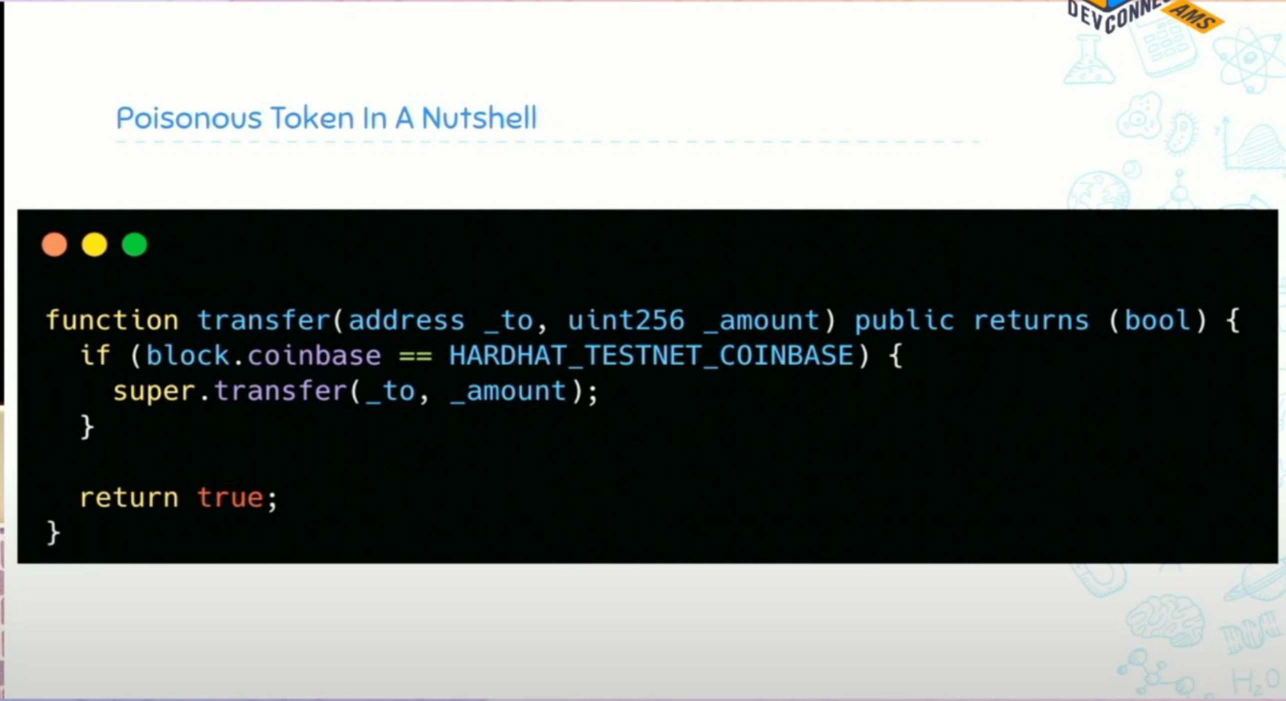
Tricks

- See available states via `debug_getAccessibleStates`
- Set `reexec` param higher accordingly
- If interested in a range of blocks consider turning on `--gcmode=archive`

Custom tracer



Detecting a poisonous token



Poisonous Token In A Nutshell

```
function transfer(address _to, uint256 _amount) public returns (bool) {
  if (block.coinbase == HARDHAT_TESTNET_COINBASE) {
    super.transfer(_to, _amount);
  }

  return true;
}
```

Solidity method invocations

- Collect list of method signatures (the first 4 bytes of the signature hash)
- Client-side map them to known method names

Roadmap

- debug_traceMulticall
- trace_* namespace

Thank you!

Sina Mahmoodi

go-ethereum

sina.mahmoodi@ethereum.org

@sina_mahmoodi