Smart Contracts on the Move

Enrique Fynn
Università della Svizzera Italiana
Switzerland

Alysson Bessani
Universidade de Lisboa
Portugal

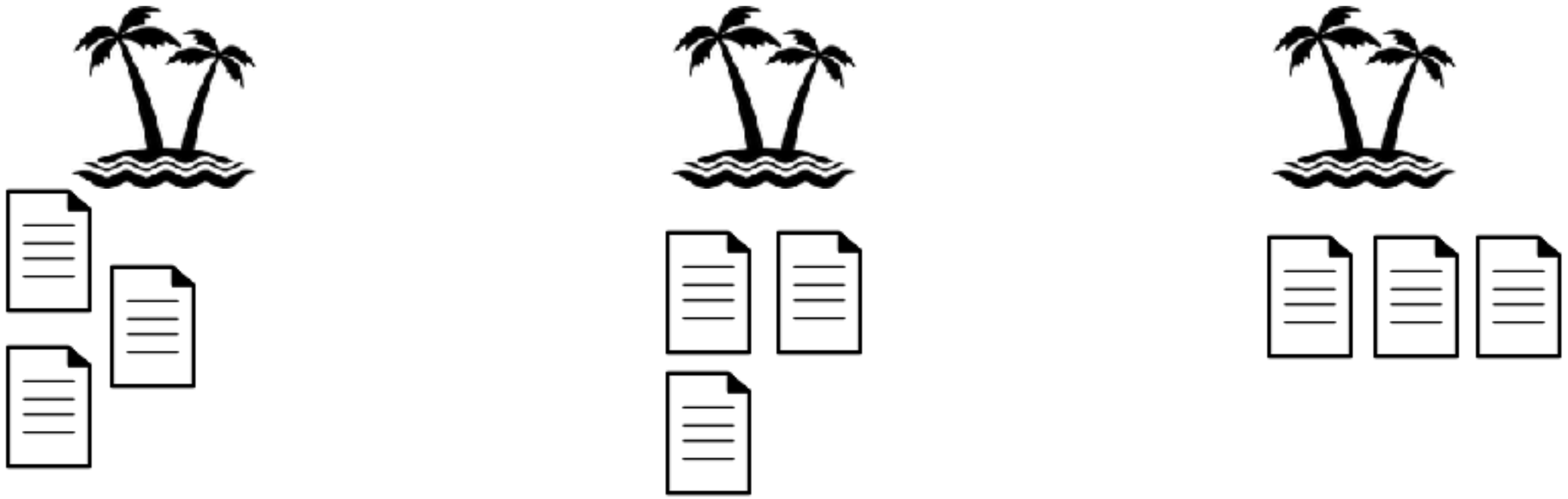
Fernando Pedone
Università della Svizzera Italiana
Switzerland

Smart Contracts

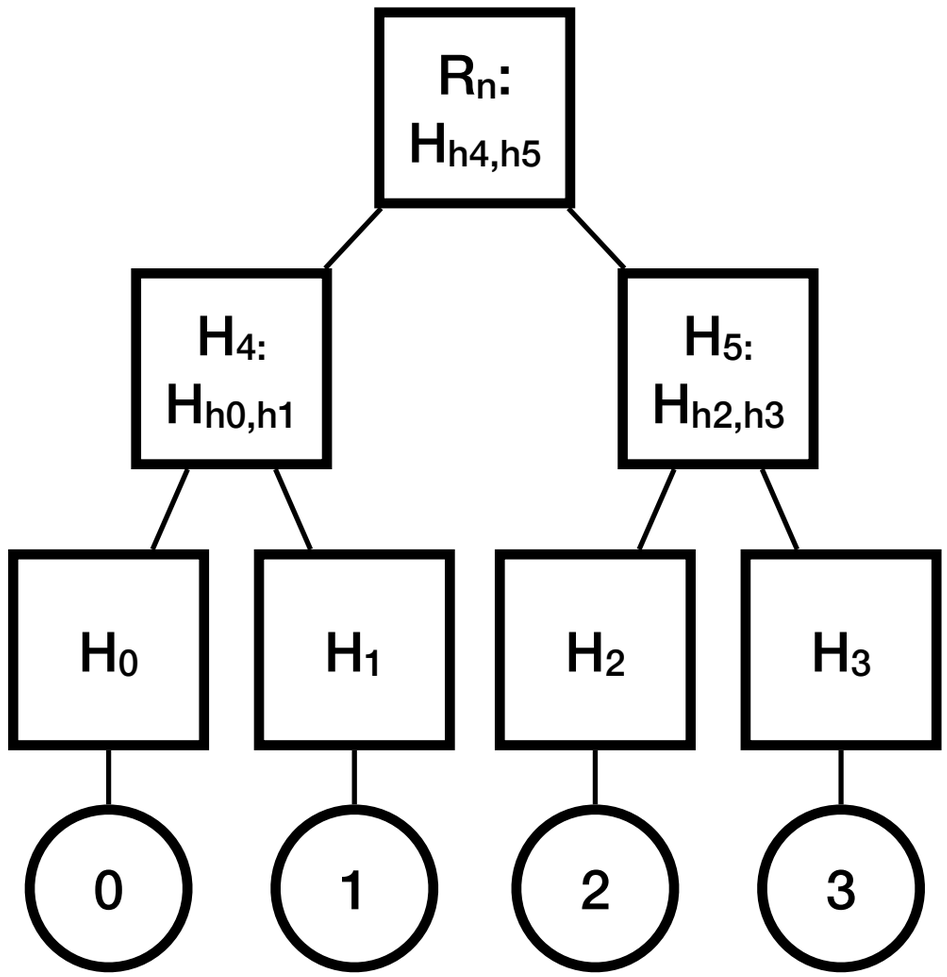
Blockchain isolation

On the Move

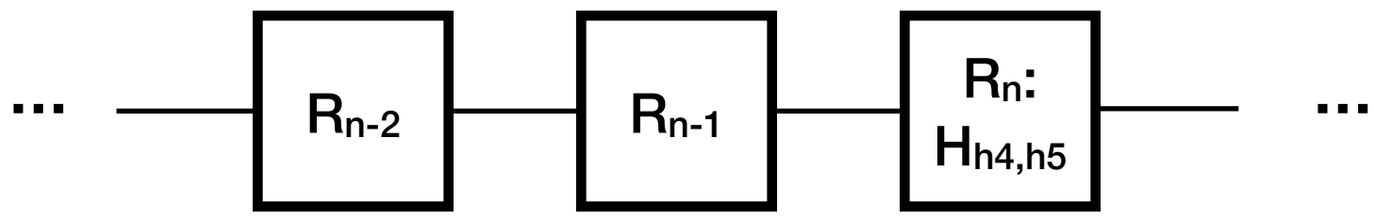
On the Move



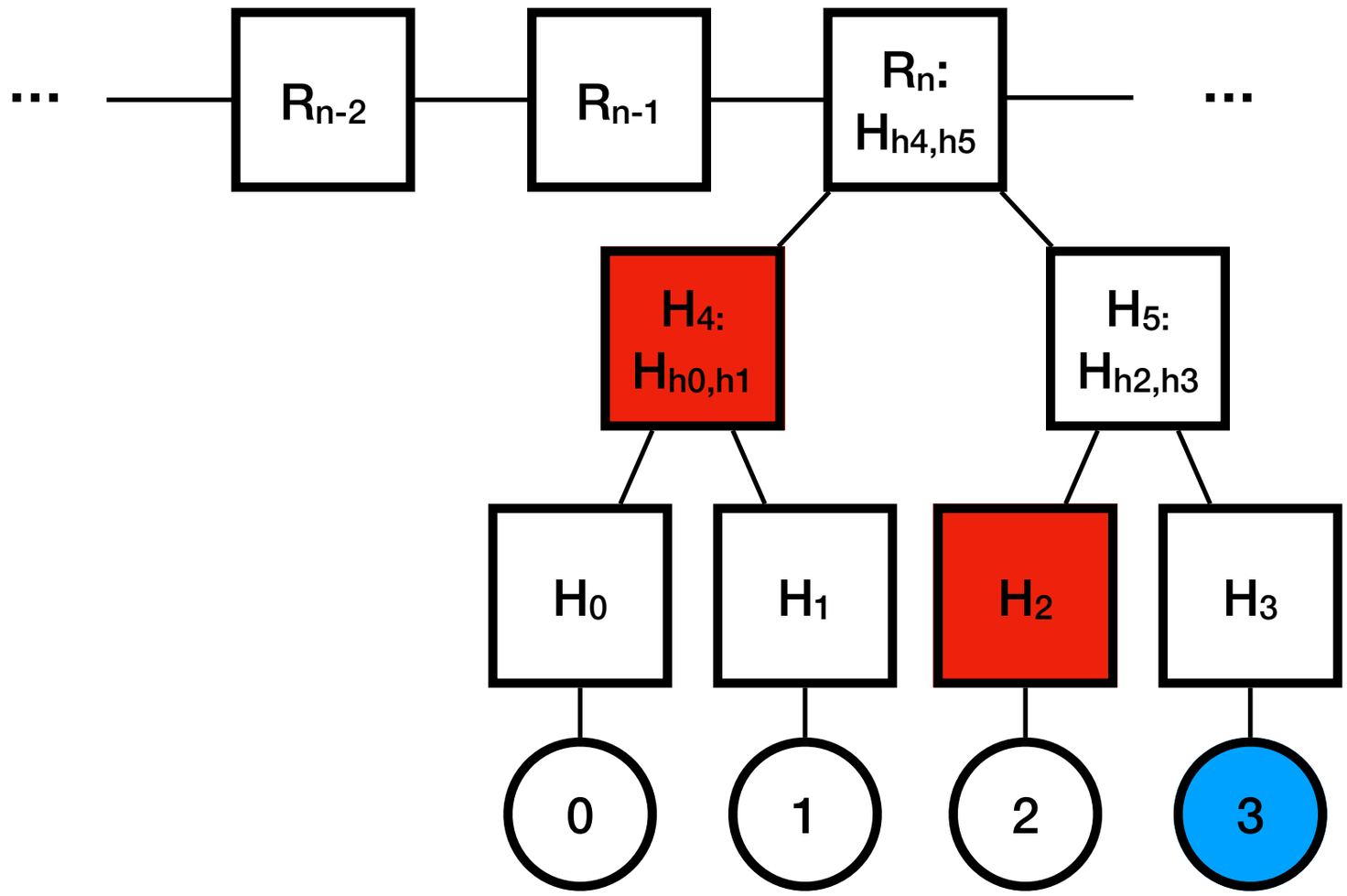
Merkle-trees



Blockchain



Blockchain



The Move protocol

- Core idea: Provide developers with a framework to move data between blockchains/shards.

- Introduce programmability in the moving operations

- Tradeoff is transparency. Developers should think about “scalable” smart contracts

The Move protocol

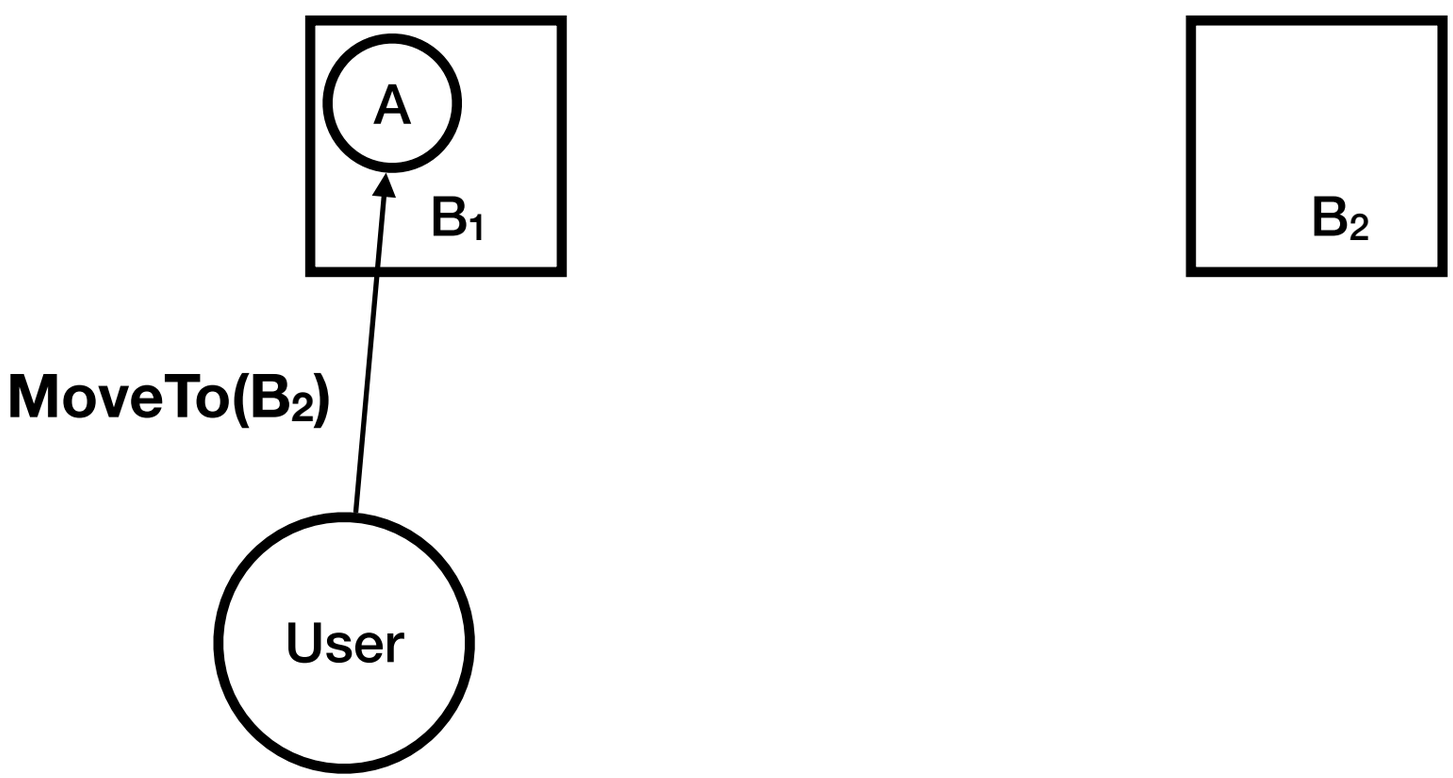
- User locks the smart contract in source blockchain
- User recreates contract in target blockchain (prove it!)
- When a contract is locked and recreated a portion of the contract’s code runs

How a contract is moved

```
contract A {
uint v;
function moveTo(b) public;
function moveFinish() public;
}
```

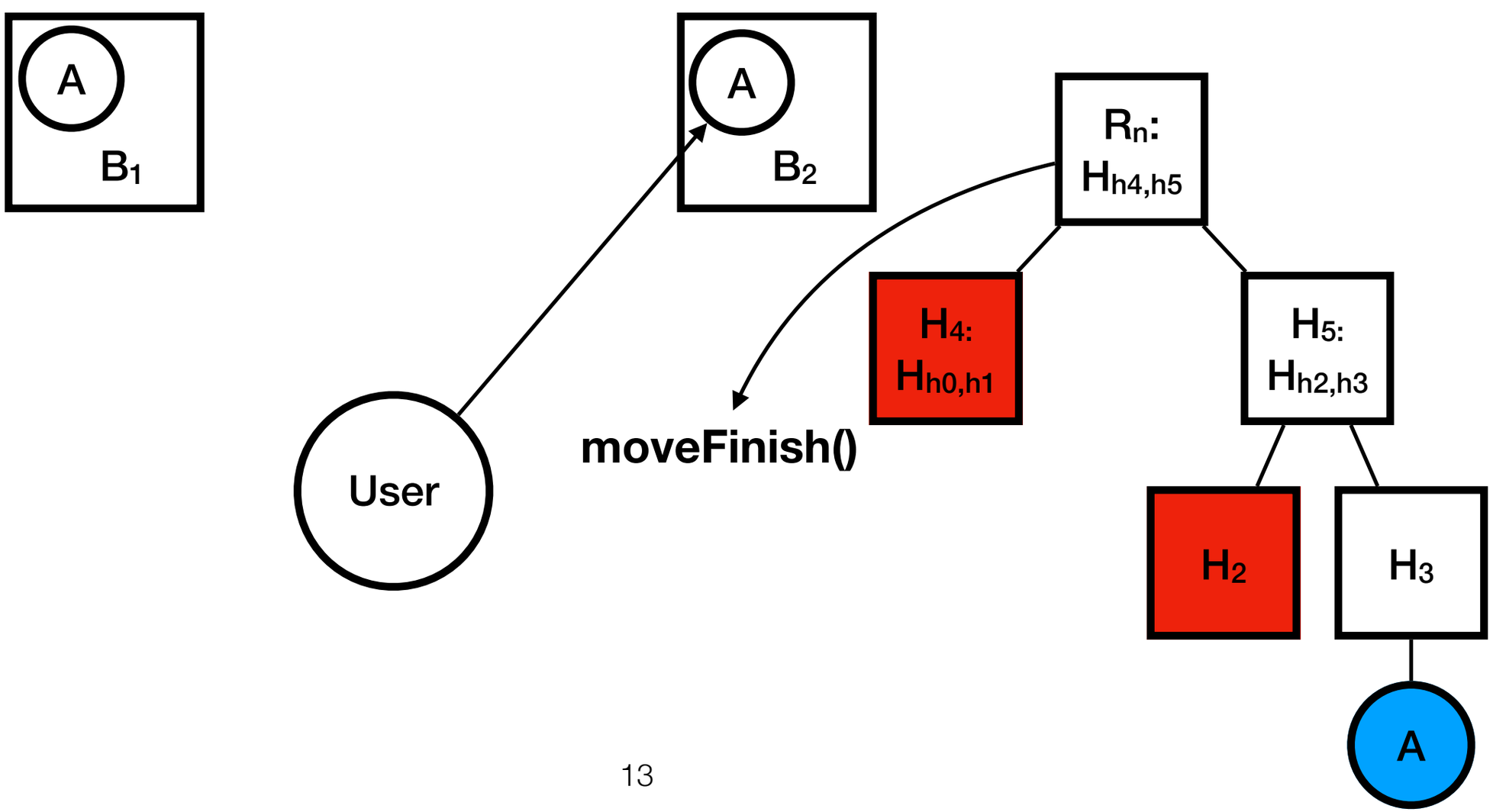
How a contract is moved

```
contract A {
uint v;
function moveTo(b) public;
function moveFinish() public;
}
```



How a contract is moved

```
contract A {
uint v;
function moveTo(b) public;
function moveFinish() public;
}
```



Expressivity

```
address owner;
uint movedAt;
  function moveTo(uint _blockchainId) public {
    require(owner == msg.sender);
    require(now - movedAt >= 3 days);
  }
  function moveFinish() public {
    movedAt = now;
  }
```

- One can program complex logic in between move operations
- In this case a contract is bound to a blockchain for at least 3 days after being moved again

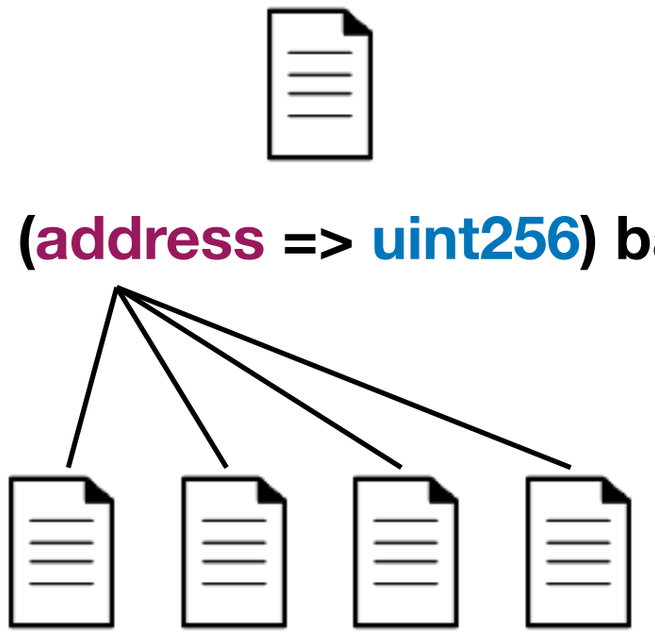
Usecase: ERC-20

- Widely used Ethereum interface
- Allow different implementations of tokens to interact

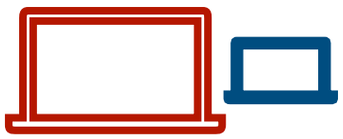
ERC-20 token

```
mapping (address => uint256) balances;
```

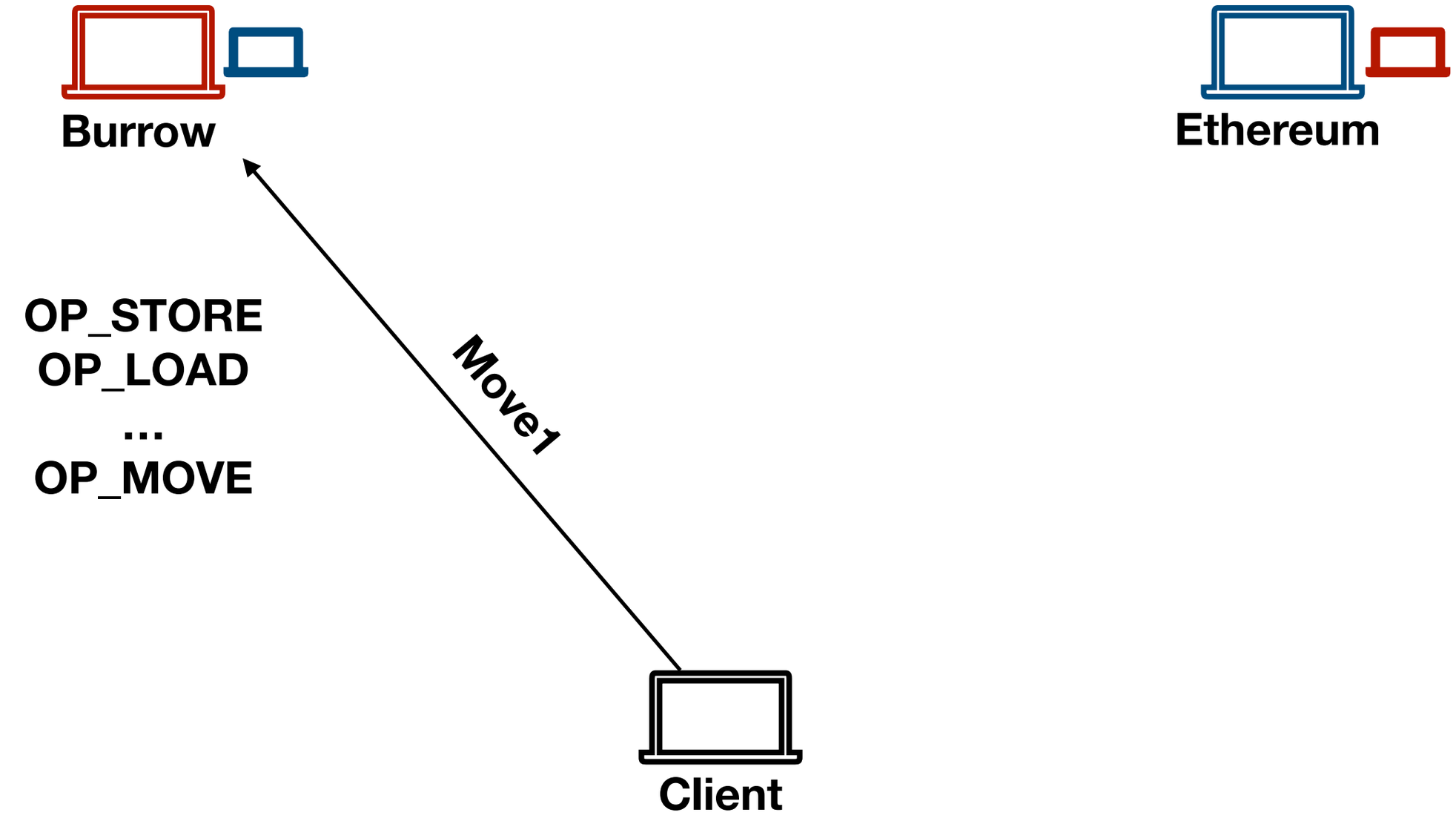
ERC-20 token



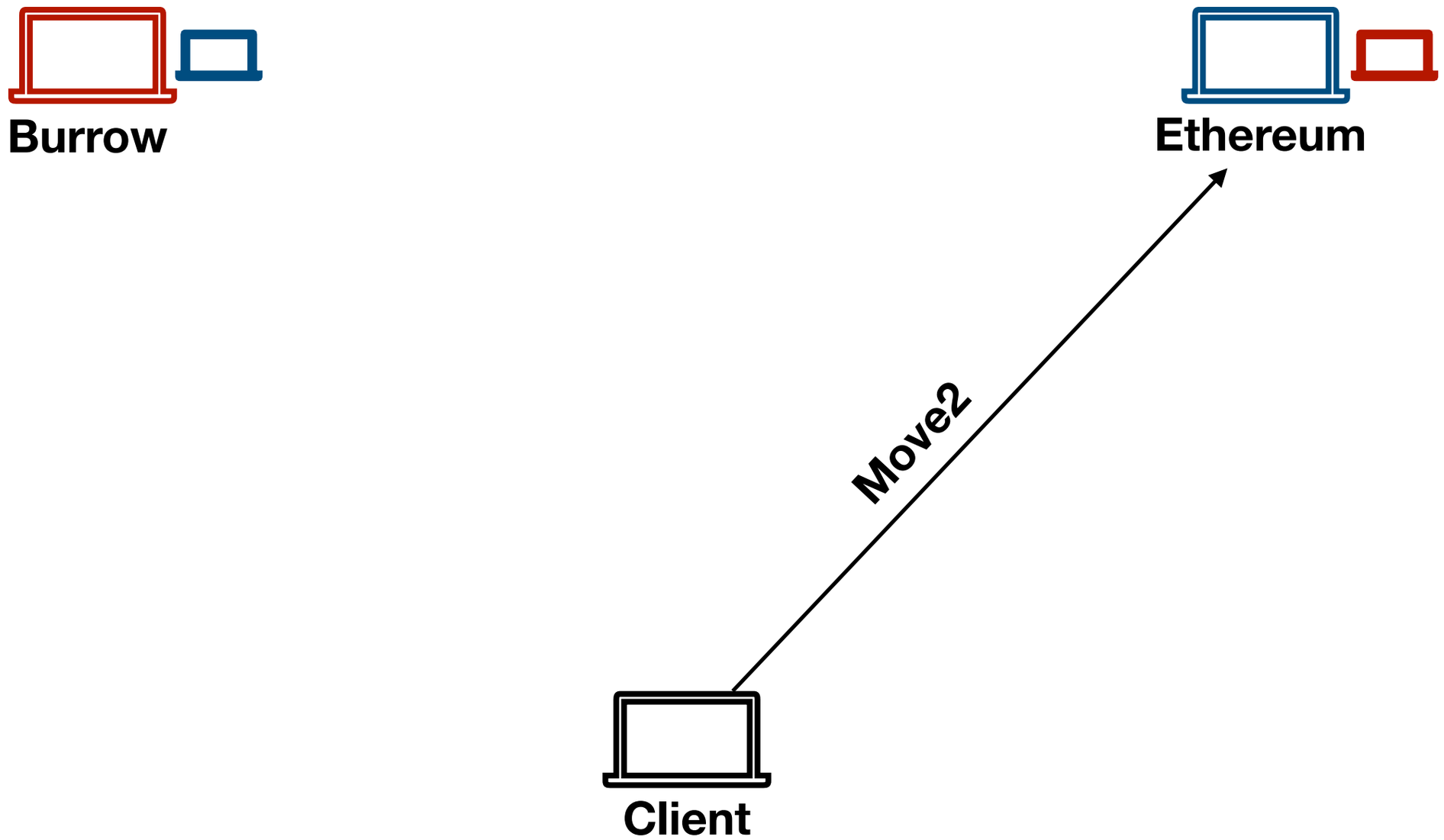
Burrow - Ethereum bridge



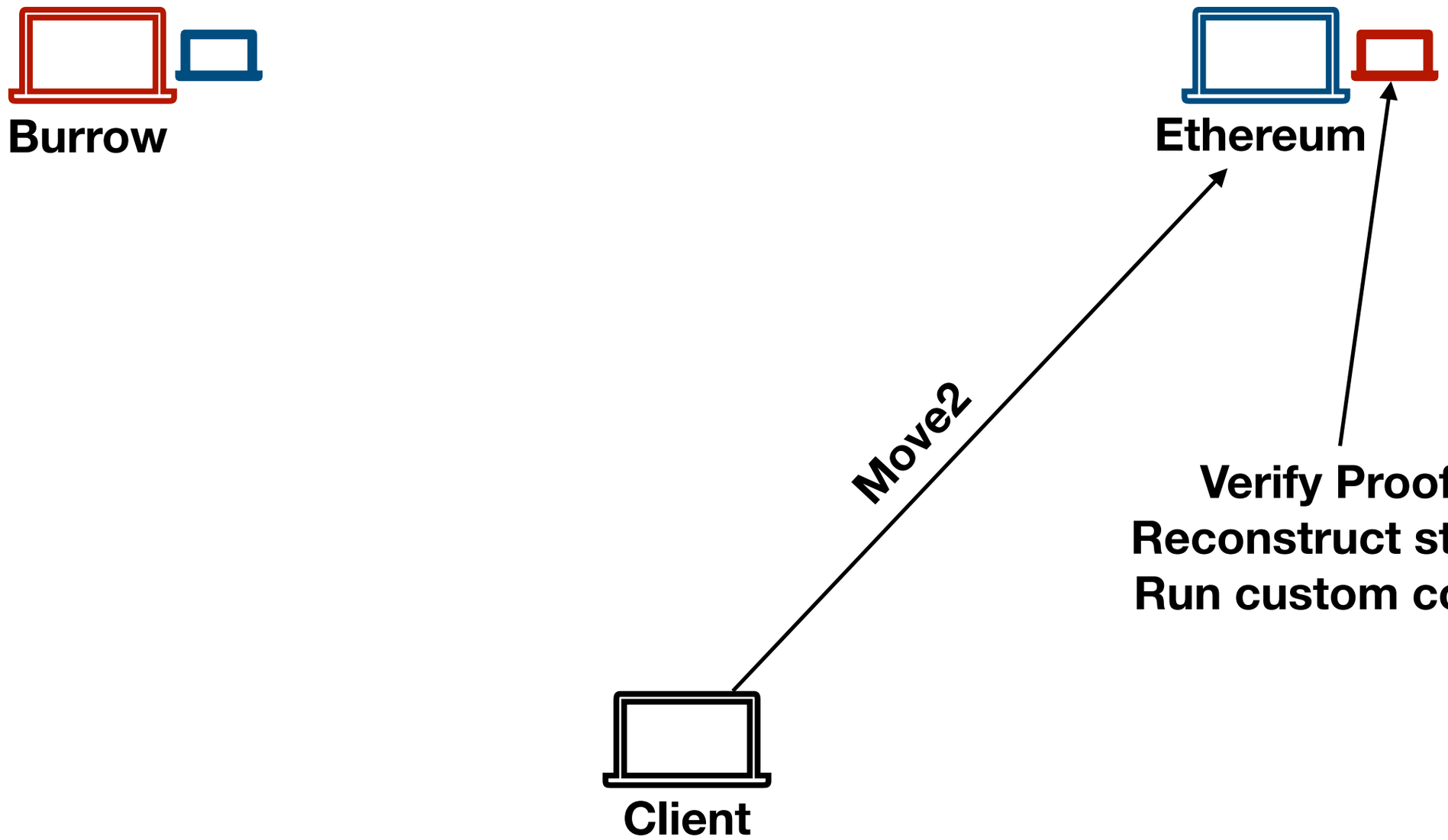
Burrow - Ethereum bridge



Burrow - Ethereum bridge



Burrow - Ethereum bridge



Usecase: CryptoKitties

- Ethereum game that congested the network at its peak
- Breeding cats and selling them for fun and profit

CryptoKitties state

- All cats are in the same contract

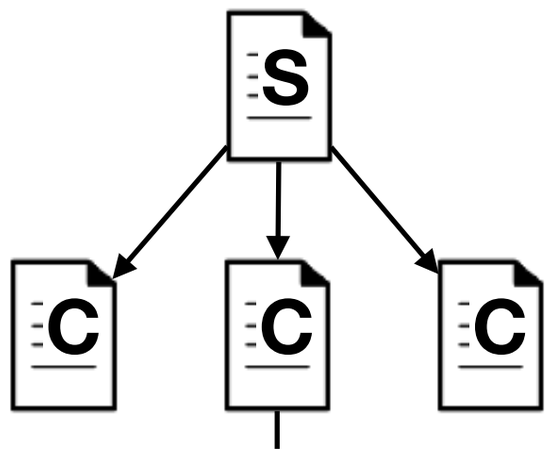
Kitties[ ]
mapping (uint256 => address) kittyIndexToOwner
mapping (uint256 => address) sireAllowedToAddress
...

CryptoKitties state

- All cats are in the same contract

Kitties[ ]
mapping (uint256 => address) kittyIndexToOwner
mapping (uint256 => address) sireAllowedToAddress
...

- Cats can move

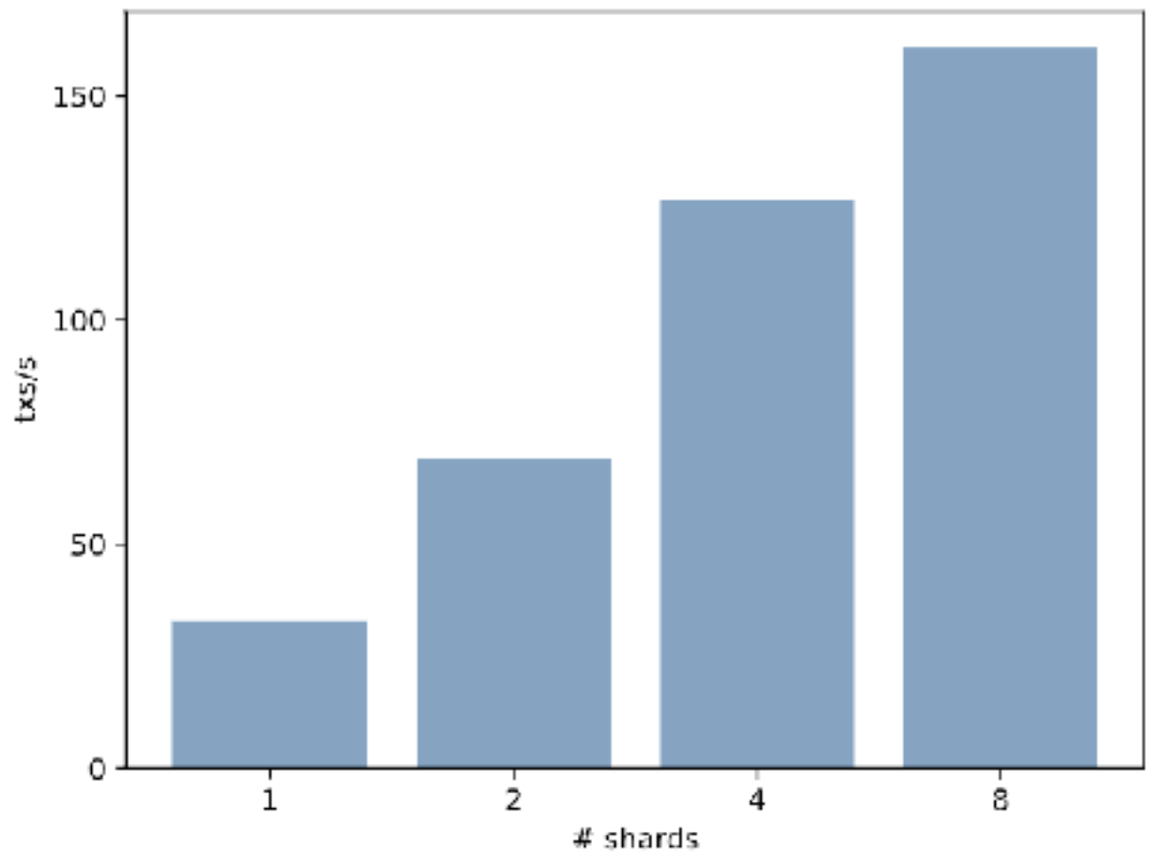


address owner
address sireAllowedToAddress
...

Experiment

- Scan transactions in the CryptoKitties smart contract
- Translate transactions
- Measure performance

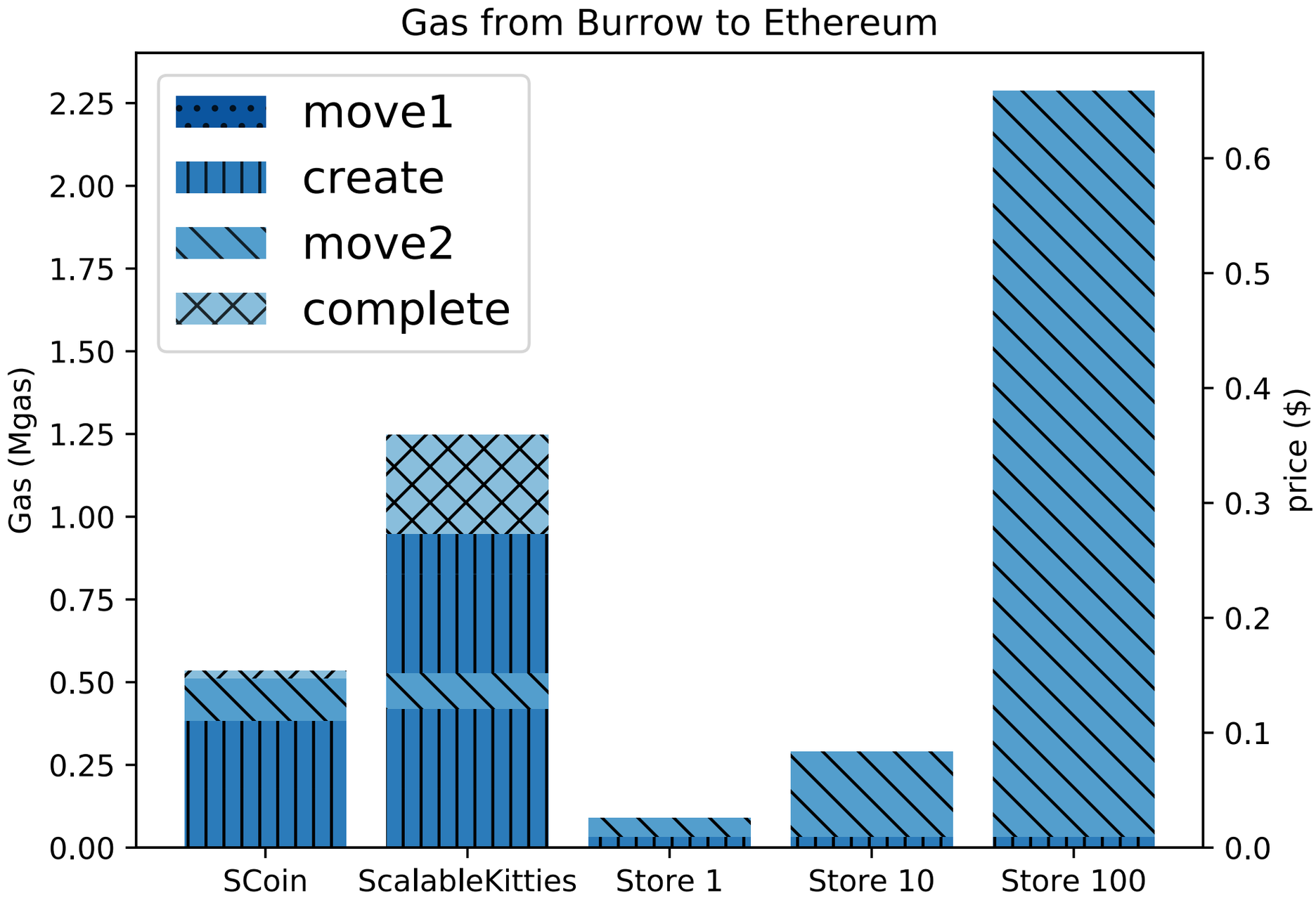
Increase in performance



EVM execution

- Gas is modelled to represent the smart contract's cost
- Users specify the amount and price of gas
- Free market between miners and users

Gas consumption



Smart Contracts on the Move

- A paradigm and protocol to execute user-centric cross-shard or IBC transactions
- Tests on two applications:
  - ERC20
  - Crypto Kitties
- How smart contracts have to be designed to inter-operate