SOLIDITY

(SMART CONTRACT)

QUICK COURSE

NICK ZSABO

SMART CONTRACT

Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.

VITALIK BUTERIN

ETHEREUM

BITCOIN'S SCRIPT

Bitcoin uses a scripting system for transactions. Forth-like, Script is simple, stack-based, and processed from left to right. It is purposefully not Turing-complete, with no loops.

REFERENCES:

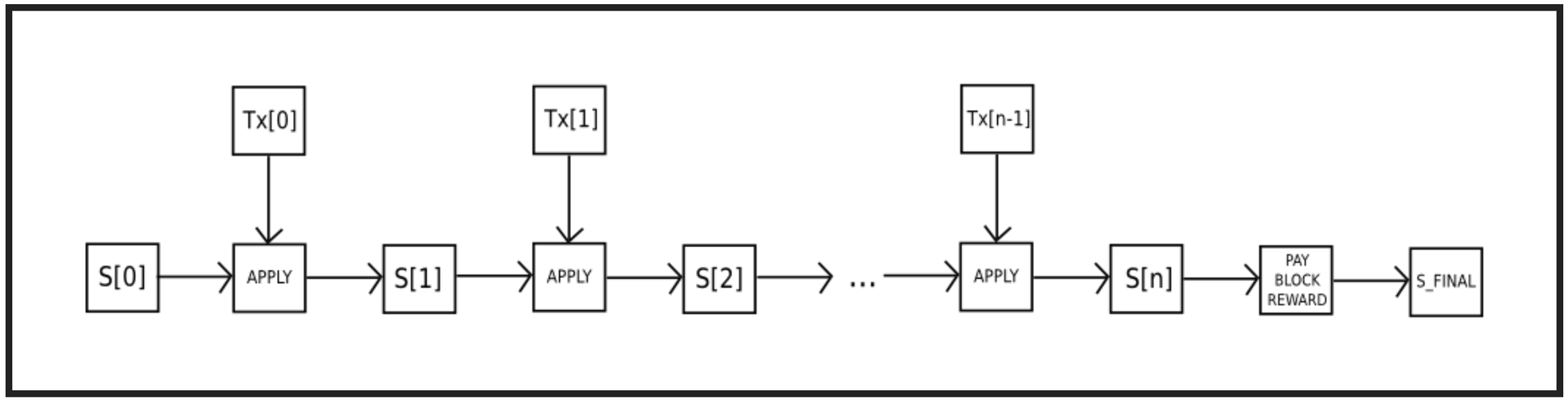
- BitcoinWiki / Script
- Example Script

```
contract Multiplication {

    int _multiplier;

    function Multiplication(int multiplier) {
        _multiplier = multiplier;
    }

    function multiply(int a) returns (int r) {
        r = a * _multiplier;
        return r;
    }
}
```

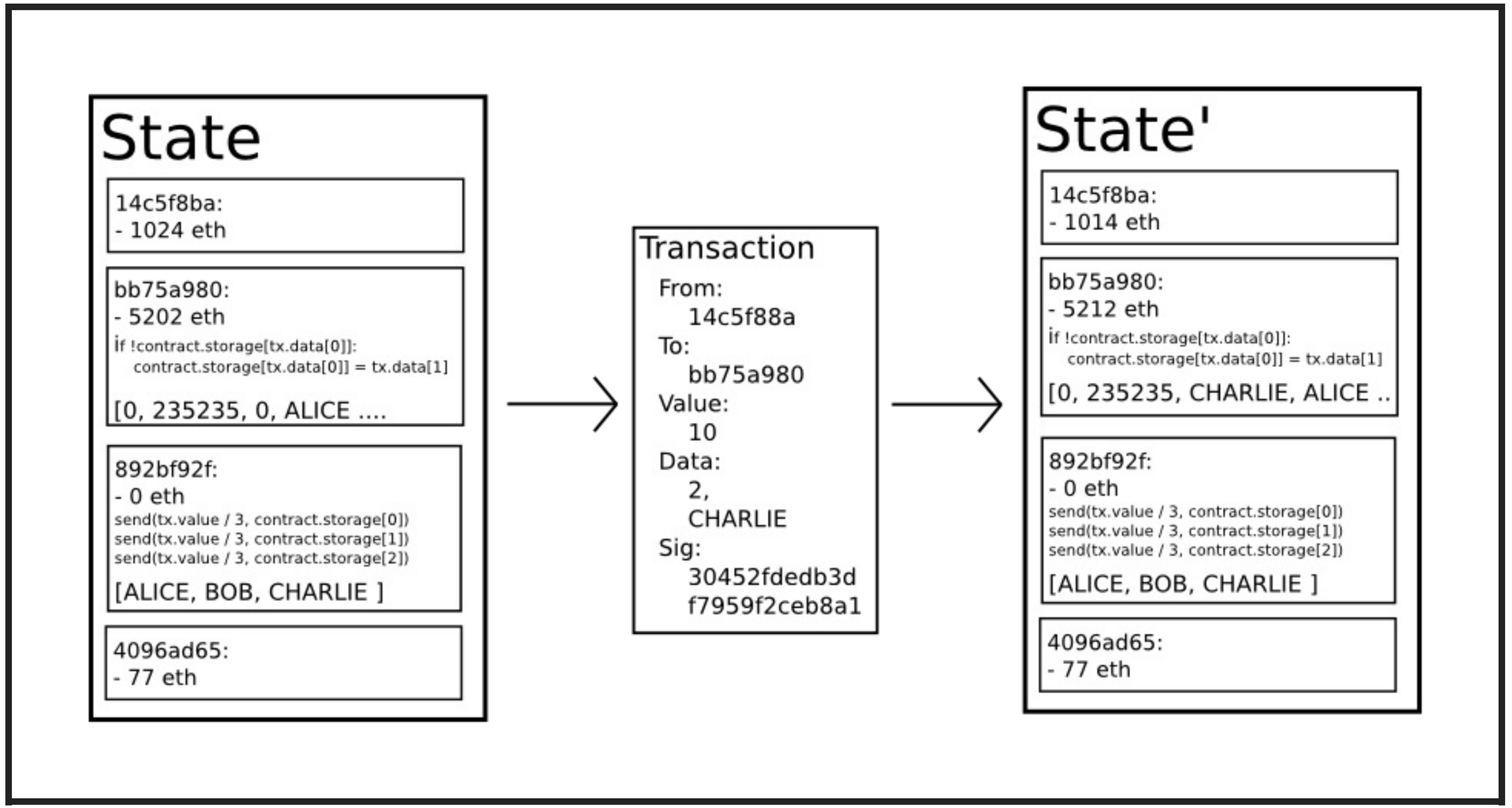
```
contract Multiplication {

    int _multiplier;
    event Multiplied(int indexed a,
        address indexed sender, int result );

    function Multiplication(int multiplier) {
        _multiplier = multiplier;
    }

    function multiply(int a) returns (int r) {
       r = a * _multiplier;
       Multiplied(a, msg.sender, r);
       return r;
    }
```

```
contract Bank {

    // We want an owner that is allowed to selfdestruct.
    address owner;

    mapping (address => uint) balances;

    // Constructor
    function Bank(){
        owner = msg.sender;
    }

    // This will take the value of the transaction and add to the senders account.
    function deposit() {
        balances[msg.sender] += msg.value;
    }

    // Attempt to withdraw the given 'amount' of Ether from the account.
    function withdraw(uint amount) {
        // Skip if someone tries to withdraw 0 or if they don't have enough Ether to make the withdrawal.
        if (balances[msg.sender] < amount || amount == 0)
            return;
        balances[msg.sender] -= amount;
        msg.sender.send(amount);
    }

    function remove() {
        if (msg.sender == owner){
            selfdestruct(owner);
        }
```

ETHEREUM BLOCKCHAIN



ETHEREUM BLOCKCHAIN (CONT.)



Q & A