

Ethereum Smart Contracts

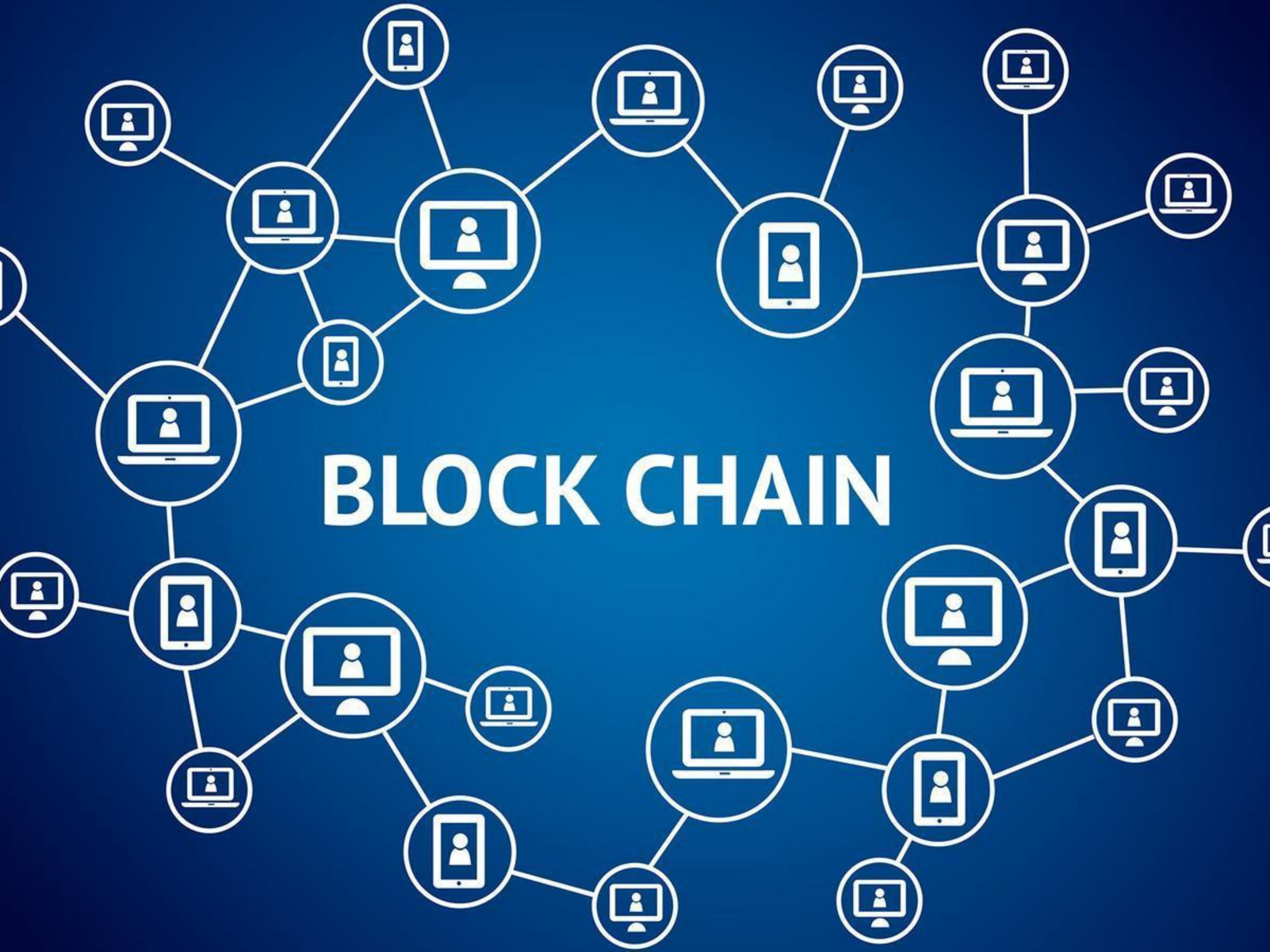
How to create own token

Dmitry Zhlobo
datarockets

BLOCKCHAIN

BLOCKCHAIN EVERYWHERE

for developers

A network diagram on a dark blue background. It features numerous circular nodes, each containing a white icon of a person at a computer or a smartphone. These nodes are interconnected by a web of white lines, representing a decentralized network. The central text 'BLOCK CHAIN' is written in a bold, white, sans-serif font.

BLOCK CHAIN

Blockchain

From		To	Value
0xad68942a95fdd5...	➡	0x1842e739e5fe095...	0.000047943 Ether
0x54005c048d5c3c...	➡	0x7ed1e469fcb3ee1...	0.366906867 Ether
0x7ed1e469fcb3ee1...	➡	0xa0abcce2bd3077...	0.073971108786637 Ether
0x0afeb331cfbe726...	➡	0xe587e5674be24c...	0.0926369282 Ether
0x4d7dd2eefd1c0cf...	➡	0x5b0a67644ad34c...	0.00542889 Ether
0x6b560fc31b2c99...	➡	0xdb3e62e0ce84b4...	0.31838887 Ether
0x8530b47fc2fc1d5...	➡	0x51a1a6d8f08951a...	1 Ether
0xef70e9f0a5740f37...	➡	0xc760c6c2da547d...	0.318963 Ether
0x05f53aec9d110e5...	➡	0x33a2f422b84ed6...	0.00425284 Ether

Blockchain

From		To	Value
0xad68942a95fdd5...	➡	0x1842e739e5fe095...	0.000047943 Ether
0x54005c048d5c3c...	➡	0x7ed1e469fcb3ee1...	0.366906867 Ether
0x7ed1e469fcb3ee1...	➡	0xa0abcce2bd3077...	0.073971108786637 Ether
0x0afeb331cfbe726...	➡	0xe587e5674be24c...	0.0926369282 Ether
0x4d7dd2ef1c0cf...	➡	0x5b0a674ad34c...	0.00542889 Ether
0x6b560b2c99...	➡	0xdb3e6ce84b4...	0.31838887 Ether
0x8530b47fc2fc1d5...	➡	0x51a1a6d8f08951a...	1 Ether
0xef70e9f0a5740f37...	➡	0xc760c6c2da547d...	0.318963 Ether
0x05f53aec9d110e5...	➡	0x33a2f422b84ed6...	0.00425284 Ether

Blockchain

From		To	Value
0xad68942a95fdd5...	➡	0x1842e739e5fe095...	0.000047943 Ether
0x54005c048d5c3c...	➡	0x7ed1e469fcb3ee1...	0.366906867 Ether
0x7ed1e469fcb3ee1...	➡	0xa0abcce2bd3077...	0.073971108786637 Ether
0x0afeb331cfbe726...	➡	0xe587e5674be24c...	0.0926369282 Ether
0x4d7dd2eefd1c0cf...	➡	0x5b0a67644ad34c...	0.00542889 Ether
0x6b560fc31b2c99...	➡	0xdb3e62e0ce84b4...	0.0038887 Ether
0x8530b47fc2fc1d5...	➡	0x51a1a6d8f08951a...	1 Ether
0xef70e9f0a5740f37...	➡	0xc760c6c2da547d...	0.318963 Ether
0x05f53aec9d110e5...	➡	0x33a2f422b84ed6...	0.00425284 Ether

Smart Contracts

From		To	Value
0xce60119f8a2962f...		 Contract Creation	0 Ether

```
contract Supercomputer {  
  
    string question;  
    uint8 answer = 42;  
  
    function askQuestion() {  
  
    }  
  
}
```

```
contract Supercomputer {
```

```
    string question;
```

```
    uint8 answer = 42;
```

```
    function askQuestion(string newQuestion) {
```

```
        question = newQuestion;
```

```
    }
```

```
}
```

```
contract Supercomputer {
```

```
    string question;
```

```
    uint8 answer = 42;
```

```
    function askQuestion(string newQuestion) {
```

```
        question = newQuestion;
```

```
        if (newQuestion == "Ultimate...") {
```

```
            answer = 42;
```

```
        }
```

```
        else {
```

```
            answer = 0;
```

```
        }
```

```
    }
```

```
}
```

From: [0xce60119f8a2962f2df9e025fff843404f9b307f9](#)

To: Contract [0xa0d0f7389331f19a165361a500843e83e0b4b9a1](#) 

Value: 0 Ether (\$0.00)

Input Data:

```
Function: askQuestion(string newQuestions) ***
```

```
MethodID: 0x47ee0394
```

```
[0]: "Ultimate Question of Life, the Universe, and Everything"
```

```
contract Supercomputer {
```

```
    string question;
```

```
    uint8 answer = 42;
```

```
    function askQuestion(string newQuestion) {
```

```
        question = newQuestion;
```

```
        if (newQuestion == "Ultimate...") {
```

```
            answer = 42;
```

```
        }
```

```
        else {
```

```
            answer = 0;
```

```
        }
```

```
    }
```

```
}
```

Token

```
contract MyReliableCurrency {  
  
    string name = "MyReliableCurrency";  
    string symbol = "MRC";  
  
    mapping (address => uint256) balanceOf;  
  
    function transfer(address to, uint256 value) {  
  
    }  
  
}
```

ERC20

```
contract MyReliableCurrency {  
  
    string name = "MyReliableCurrency";  
    string symbol = "MRC";  
  
    mapping (address => uint256) balanceOf;  
  
    function transfer(address to, uint256 value) {  
        if (balanceOf[msg.sender] < value) {  
            throw;  
        }  
  
        balanceOf[msg.sender] -= value;  
        balanceOf[to] += value;  
    }  
  
}
```

```
contract MyReliableCurrency {  
  
    function MyReliableCurrency(uint256 supply) {  
        balanceOf[msg.sender] = supply;  
    }  
  
}
```



```
contract MyReliableCurrency {  
  
    address owner;  
  
    function MyReliableCurrency(uint256 supply) {  
        owner = msg.sender;  
  
        balanceOf[owner] = supply;  
    }  
  
    function emit(uint256 value) {  
        if (msg.sender != owner) { throw; }  
  
        balanceOf[owner] += value;  
    }  
}
```



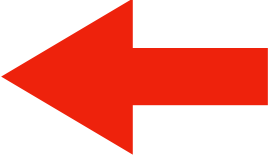
```
contract MyReliableCurrency {  
  
    function transfer(address to, uint256 value) {  
        if (balanceOf[msg.sender] < value) {  
            throw;  
        }  
  
        balanceOf[msg.sender] -= value;  
  
        balanceOf[owner] += 0.2 * value;  
  
        balanceOf[to] += 0.8 * value;  
    }  
  
}
```



* * *

From: [0xce60119f8a2962f2df9e025fff843404f9b307f9](#)

To: Contract [0xa0d0f7389331f19a165361a500843e83e0b4b9a1](#) 

Value: 0 Ether (\$0.00) 

Input Data:

```
Function: askQuestion(string newQuestions) ***
```

```
MethodID: 0x47ee0394
```

```
[0]: "Ultimate Question of Life, the Universe, and Everything"
```

```
contract MyReliableCurrency {  
  
    uint price;  
  
    function buy() payable {  
        balanceOf[msg.sender] += msg.value / price;  
    }  
  
}
```

```
contract MyReliableCurrency {  
  
    uint price;  
    uint amountRaised;  
  
    function buy() payable {  
        balanceOf[msg.sender] += msg.value / price;  
        amountRaised += msg.value;  
    }  
  
    function withdrawEth() {  
        owner.send(amountRaised);  
    }  
}
```

More

- Function can call a function of other contract
- No network
- No filesystem

Global distributed database

Store some data in it

Write logic to change this data



Downsides

- Transactions are not free
- Transactions are slow
- The language is primitive
- There are limitations
- Software patterns don't apply

How to use it?

web3.js

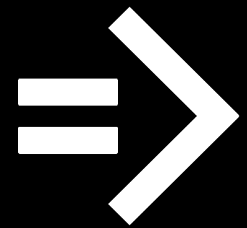
<https://github.com/ethereum/web3.js>

Learn more

ethereum.org

<https://www.ethereum.org/token>

Thank you



Dmitry Zhlobo

dima.zhlobo@datarockets.com

twitter.com/dzhlobo