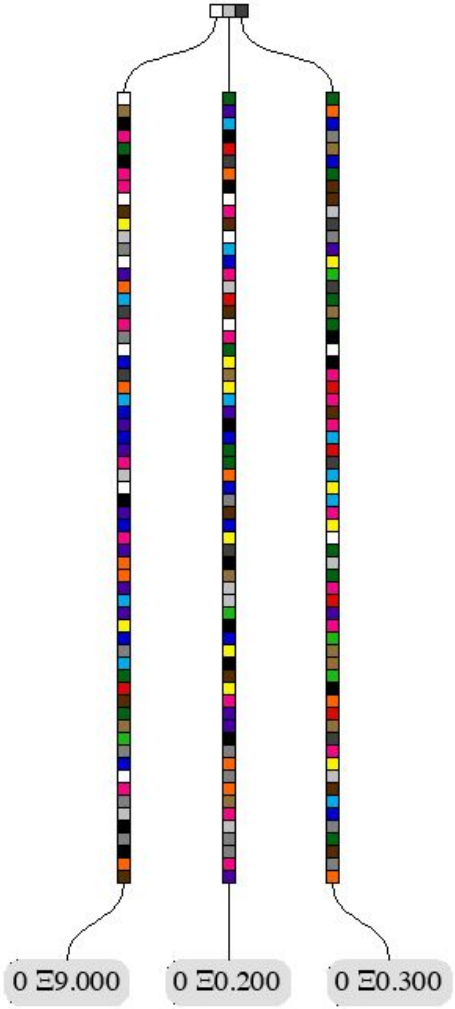
STARKs for Stateless Ethereum, the beginning

Alexey Akhunov

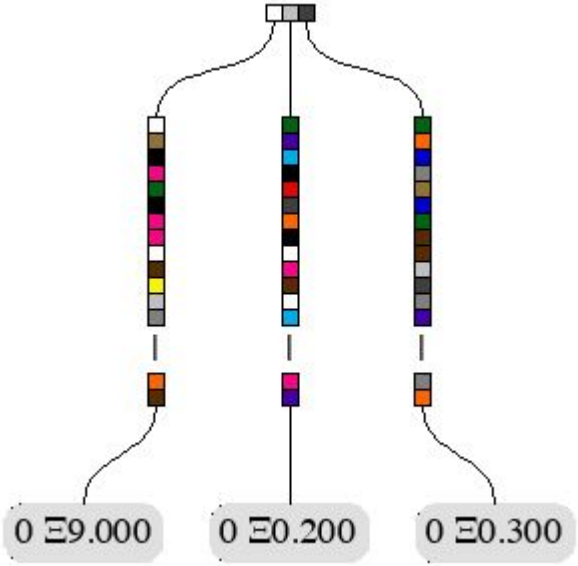
1



Genesis (initial state)

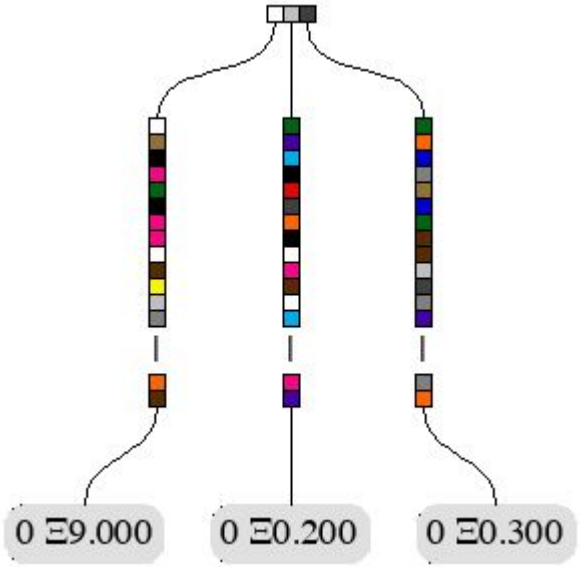
Visual adjustment

2

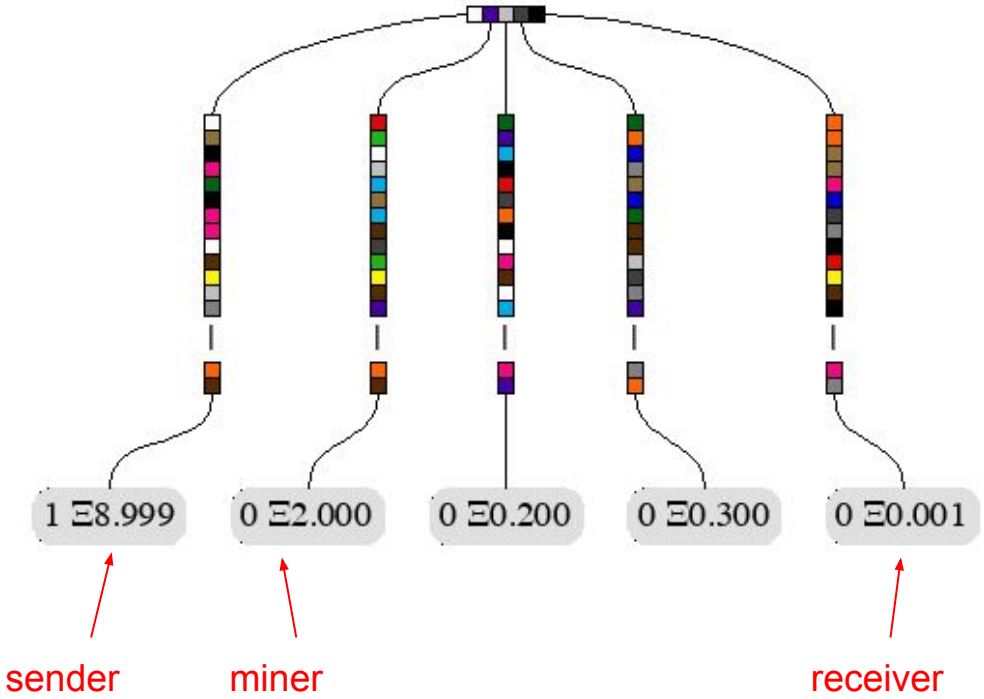


Send 0.001 to a fresh account + mining reward

2

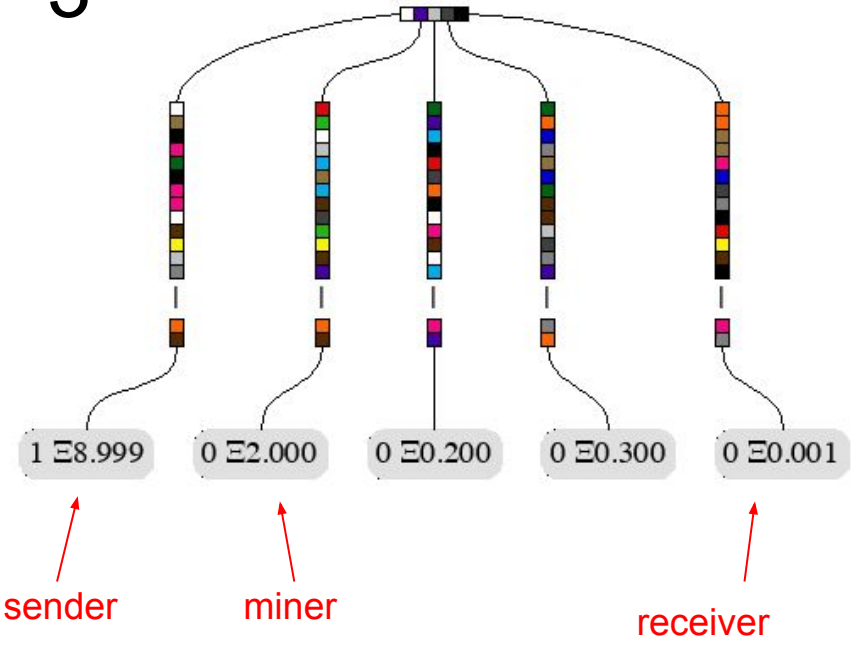


3

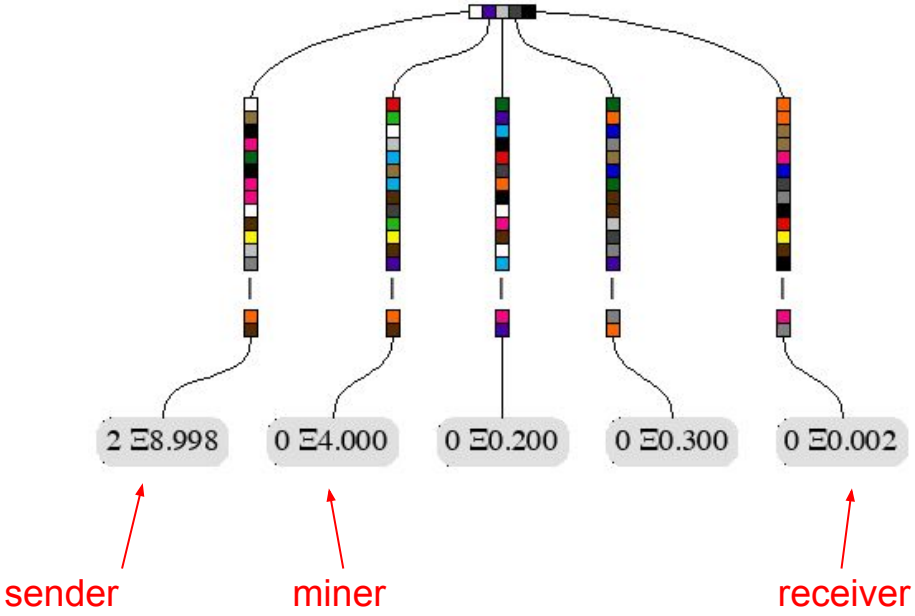


Send another 0.001

3



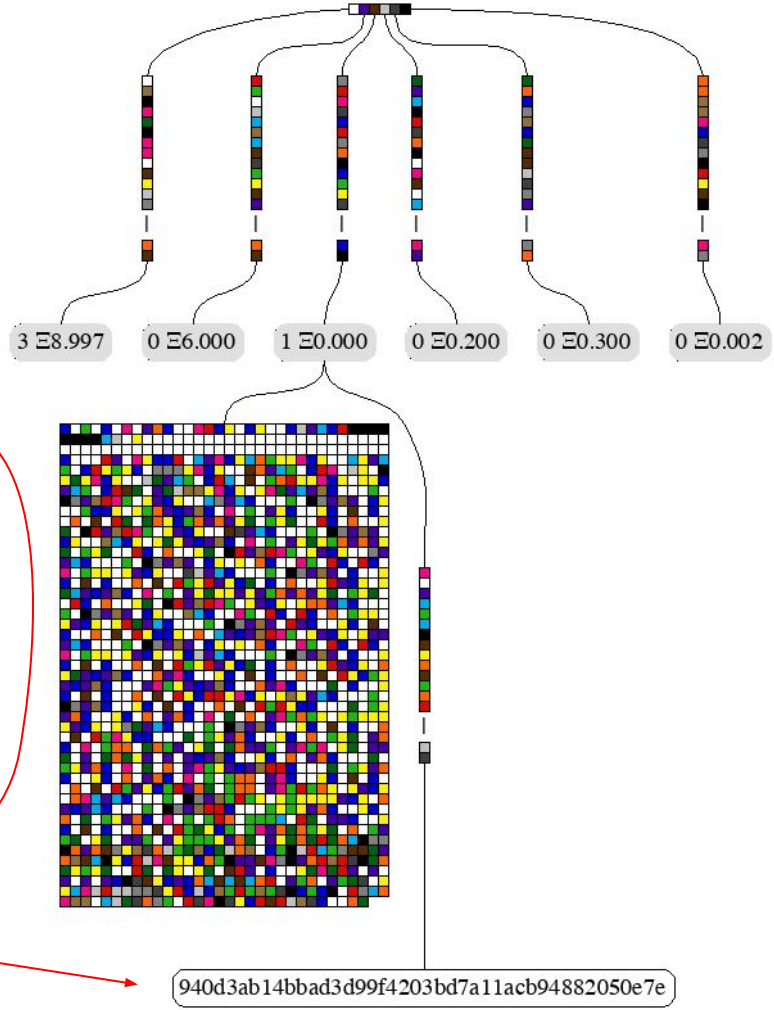
4



Deploy token contract

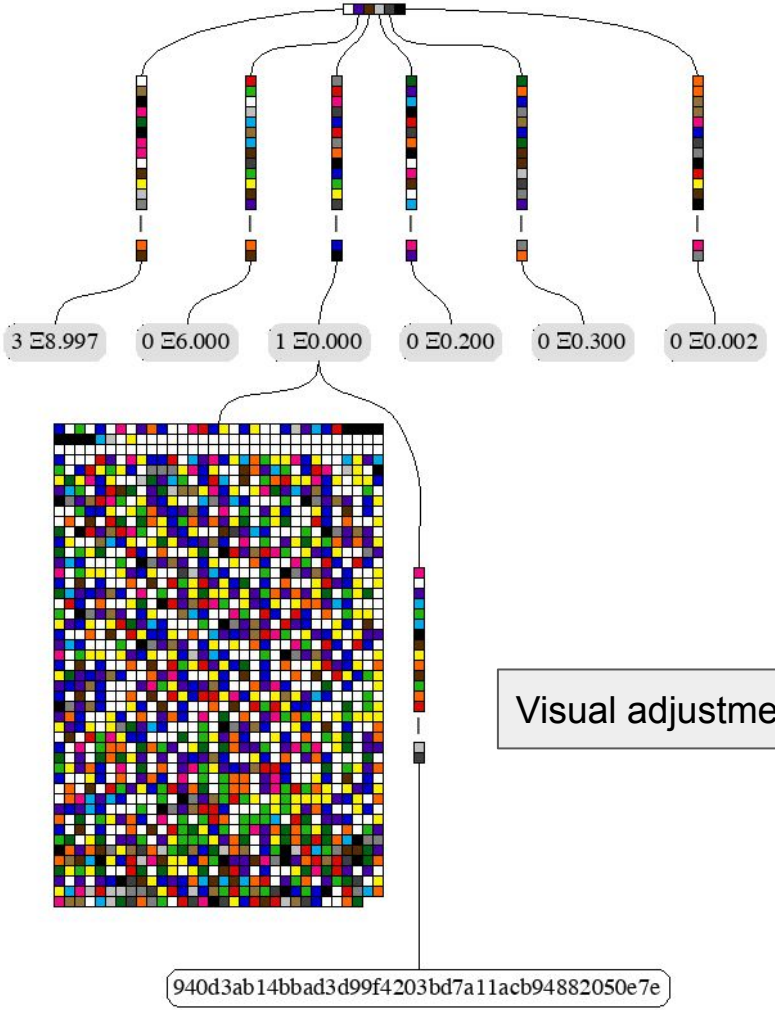
```
contract Token {
    uint256 public totalSupply;
    mapping(address => uint256) public balanceOf;
    address public minter;

    constructor(address _minter) public {
        minter = _minter;
    }

    /* Send tokens */
    function transfer(address _to, uint256 _value) public returns (bool) {
        uint256 fromBalance = balanceOf[msg.sender];
        uint256 toBalance = balanceOf[_to];
        require(fromBalance >= _value);                // Check if the sender has enough
        require(toBalance + _value >= toBalance);      // Check for overflows
        balanceOf[msg.sender] = fromBalance - _value;  // Subtract from the sender
        balanceOf[_to] = toBalance + _value;
        return true;
    }

    /* Allows the owner to mint more tokens */
    function mint(address _to, uint256 _value) public returns (bool) {
        require(msg.sender == minter);             // Only the minter is allowed to mint
        uint256 toBalance = balanceOf[_to];
        require(toBalance + _value >= toBalance);  // Check for overflows
        balanceOf[_to] = toBalance + _value;
        totalSupply += _value;
        return true;
    }
}
```

5



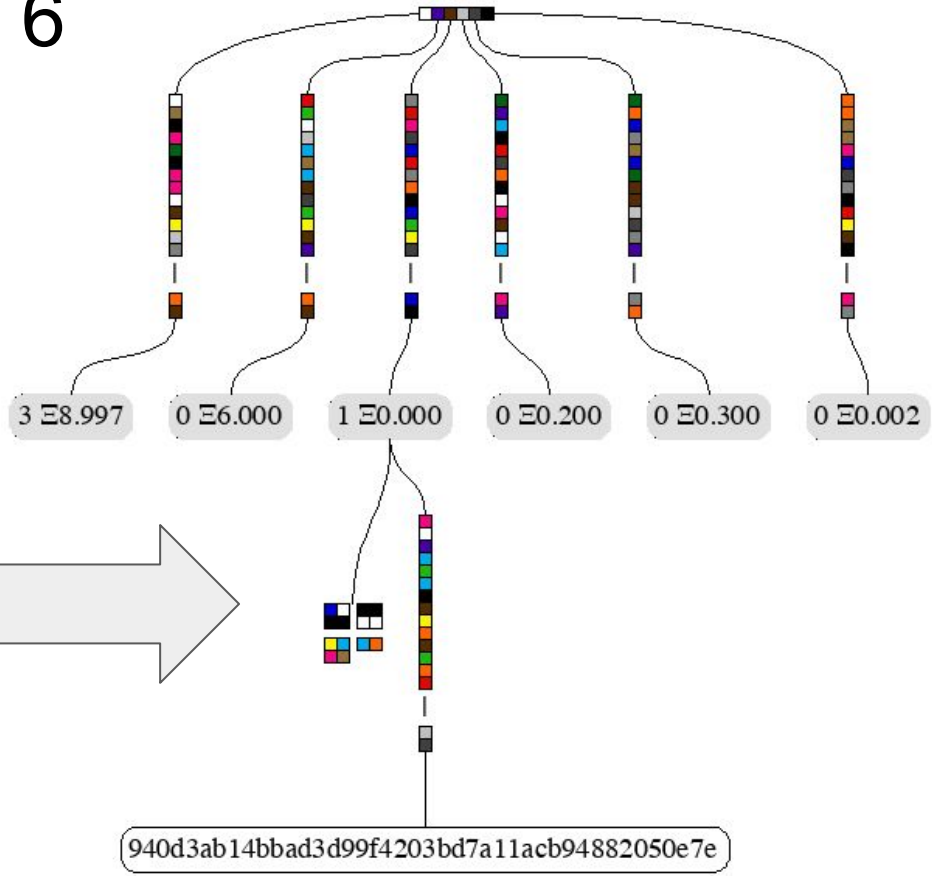
Address of the minter

5

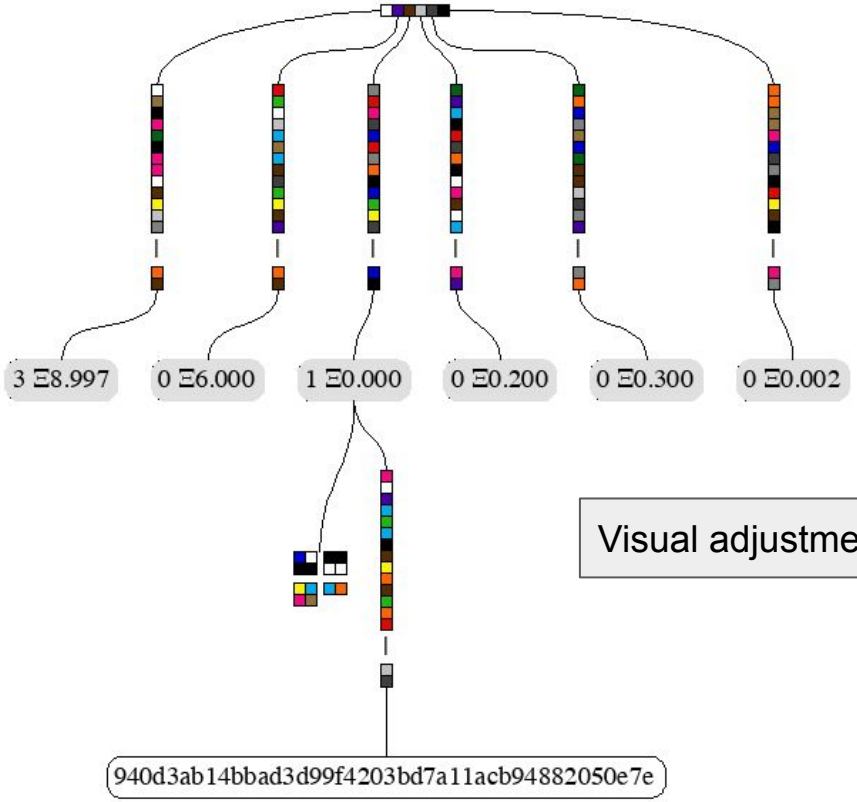


Visual adjustment

6

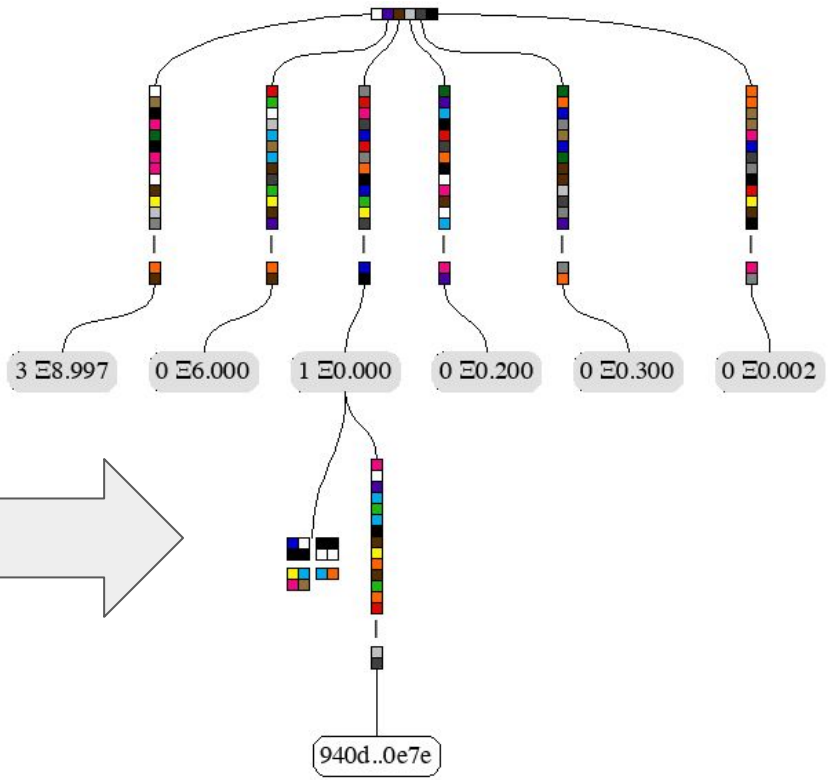


6



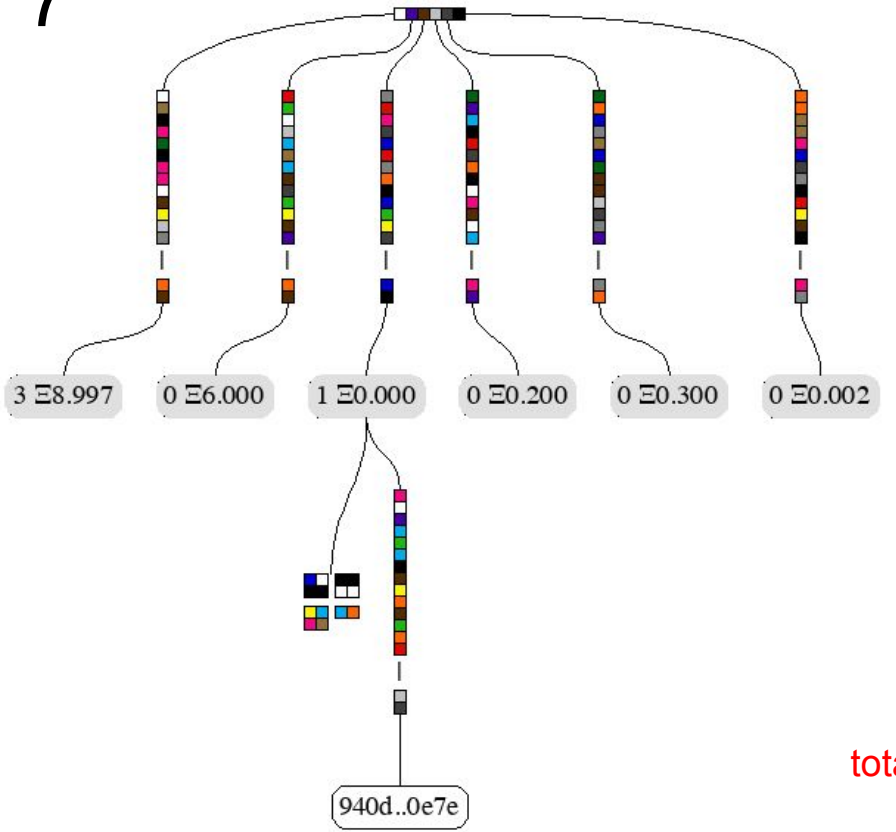
Visual adjustment

7

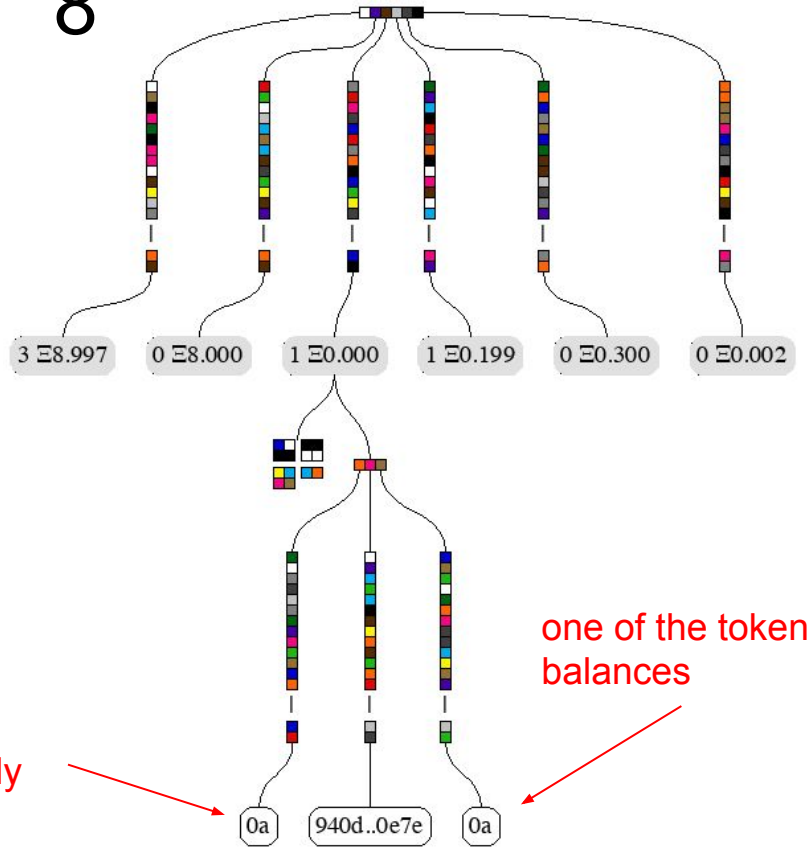


Mint 10 tokens

7



8

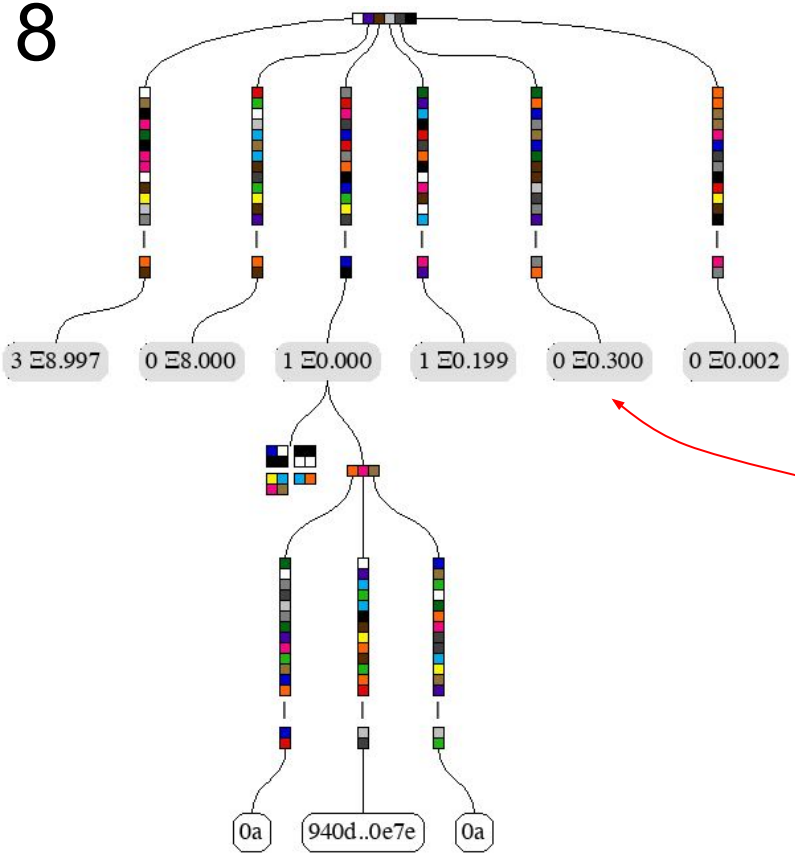


totalSupply

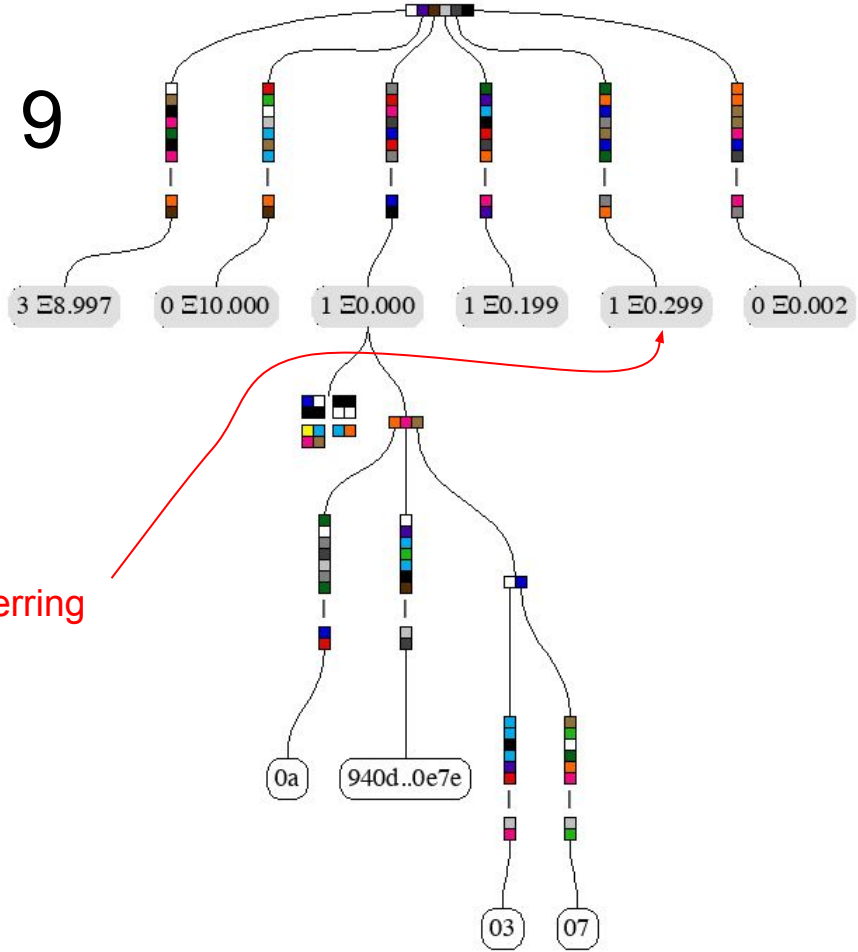
one of the token balances

Transfer 3 tokens

8



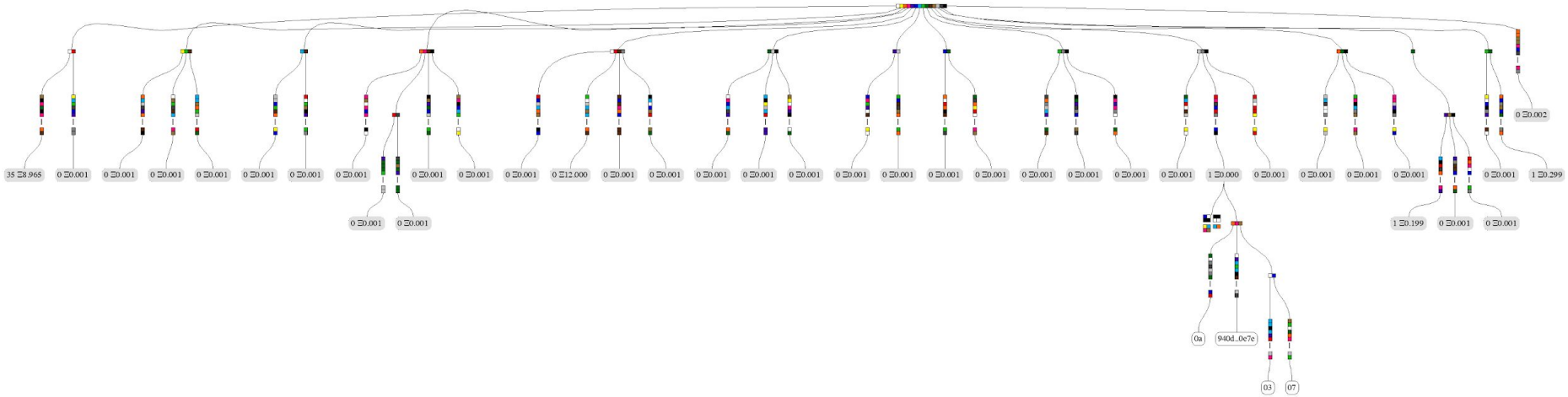
9

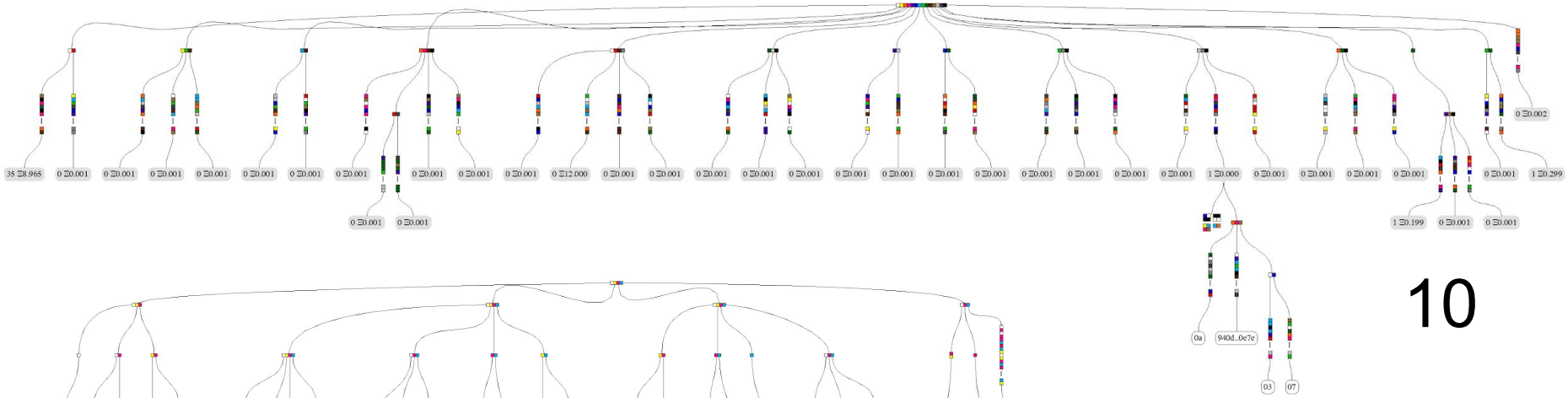


transferring owner

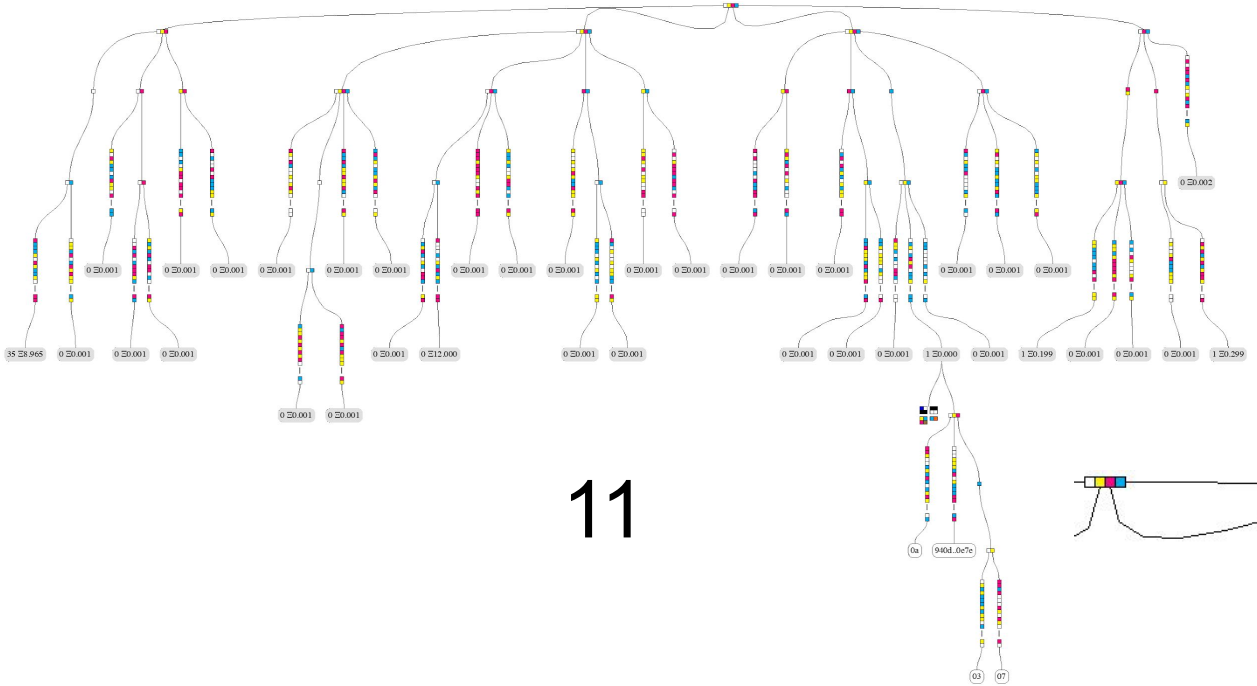
Send 0.001 to 32 different addresses

10

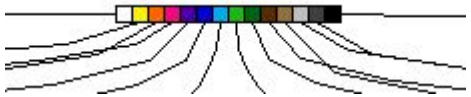


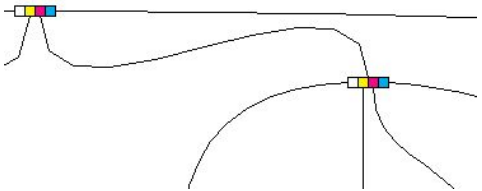


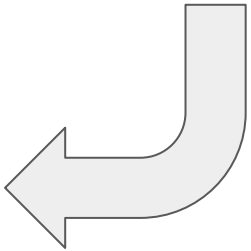
10

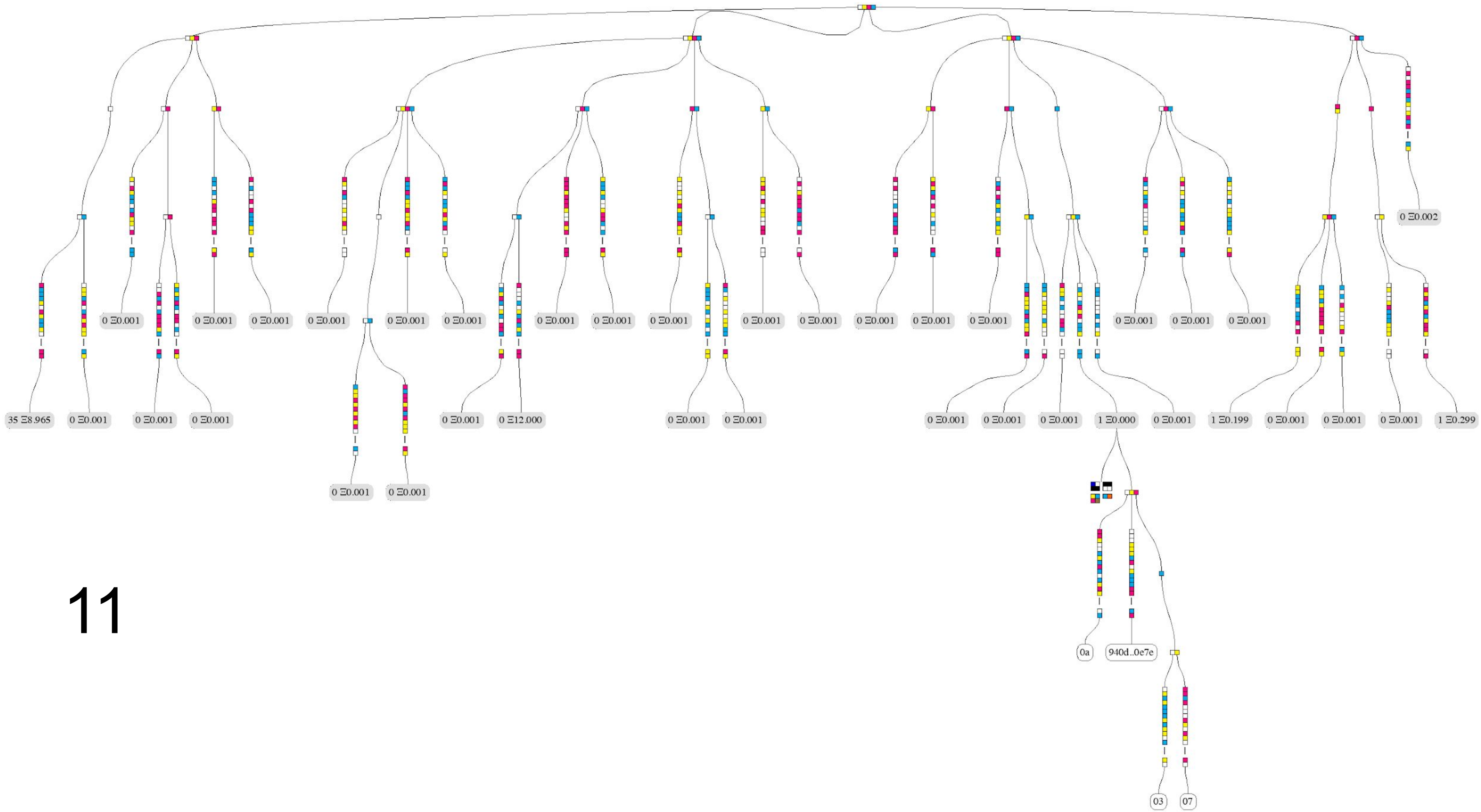


11



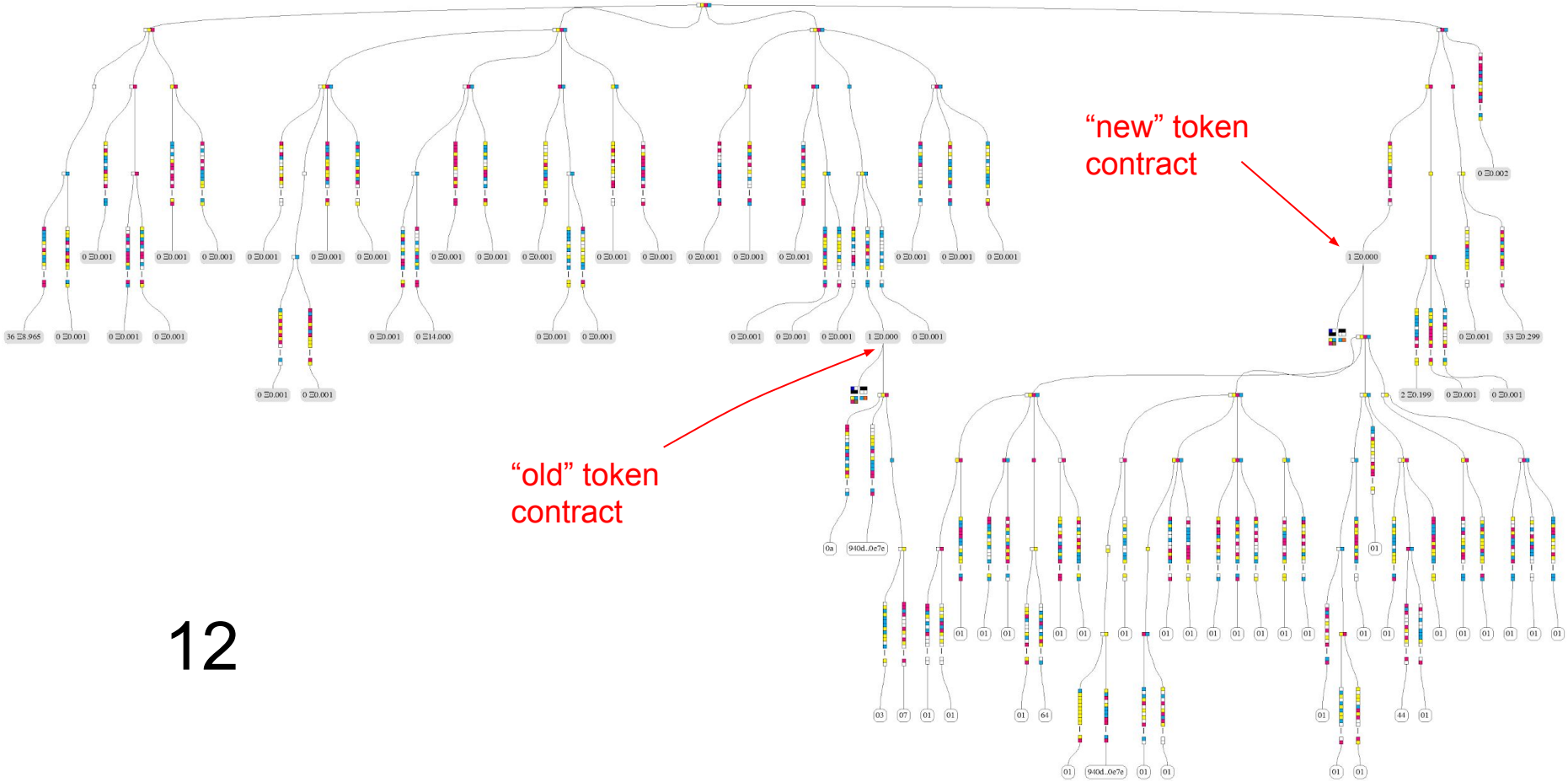




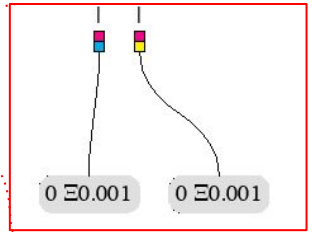

0 Ξ0.002
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
35 Ξ8.965
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ12.000
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
1 Ξ0.000
0 Ξ0.001
1 Ξ0.199
0 Ξ0.001
0 Ξ0.001
0 Ξ0.001
1 Ξ0.299
0 Ξ0.001
0 Ξ0.001
0a
940d..0e7e
03
07

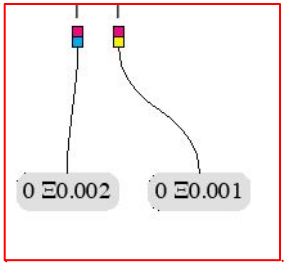
11

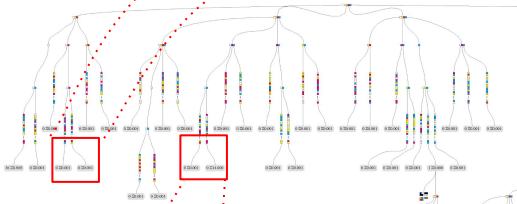
Deploy new token, mint and transfer 1 token to 32 different addresses

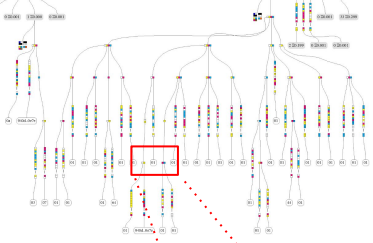


12



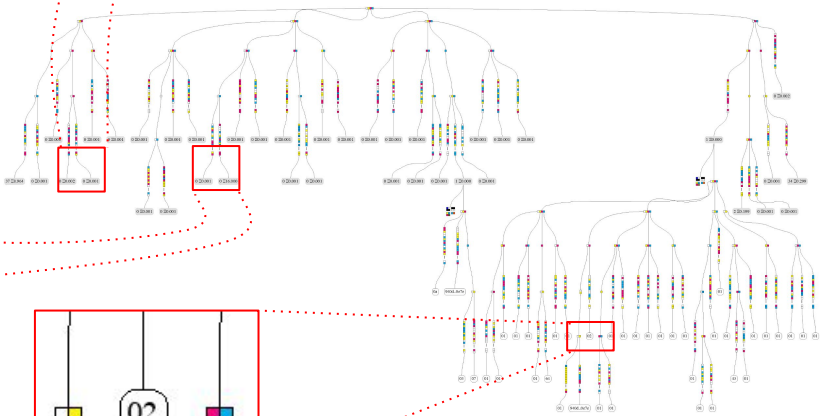


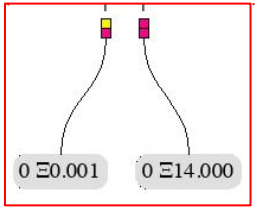


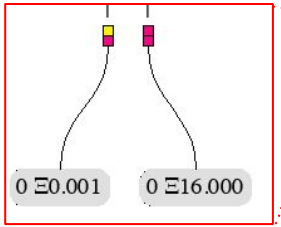


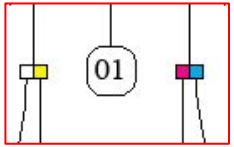
Send 0.001 and 1 token

13

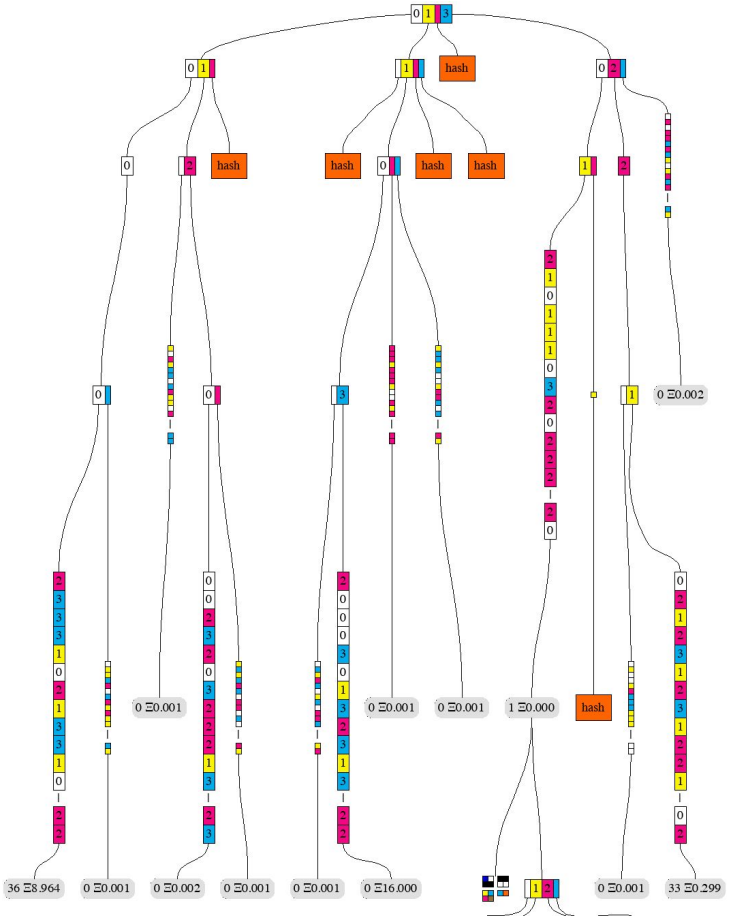


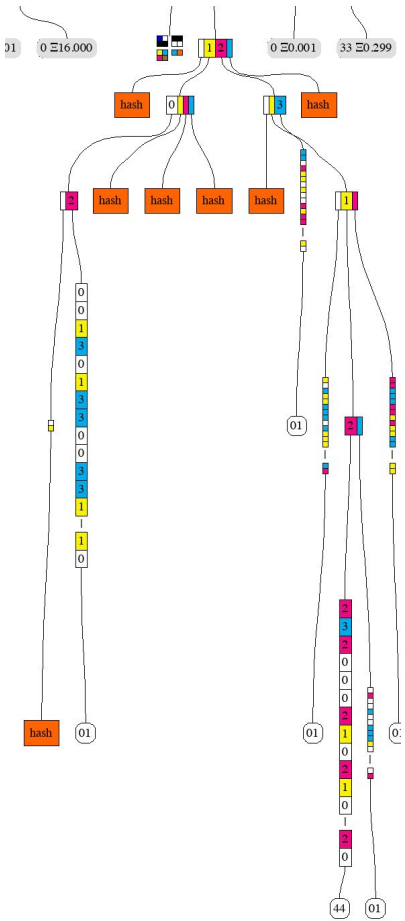




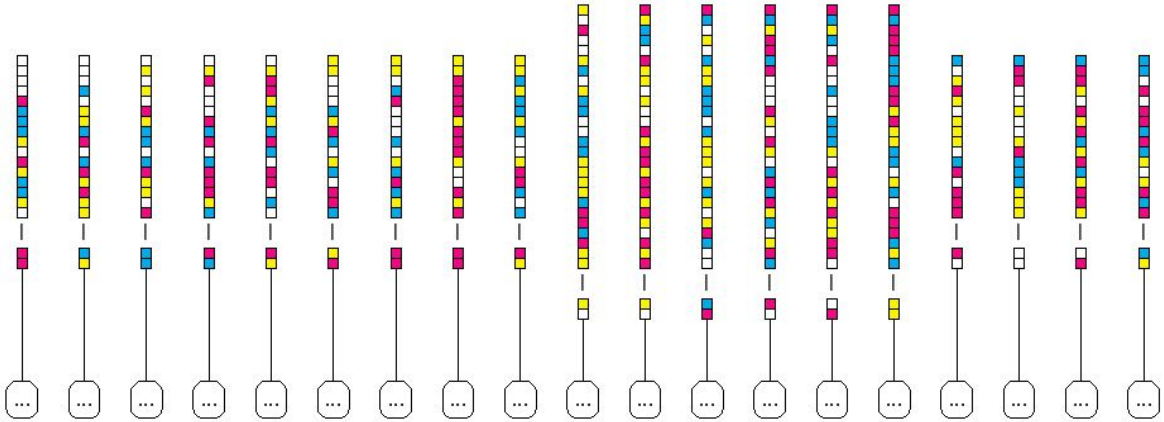


Block proof
for 12->13





Composition of a block proof



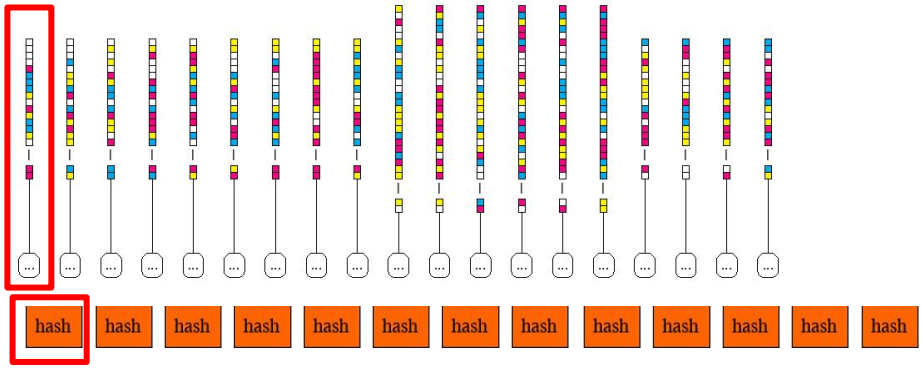
HASHES

CONTRACT CODES

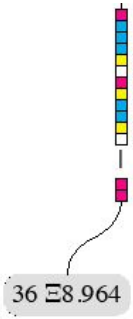
```
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
```

```
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

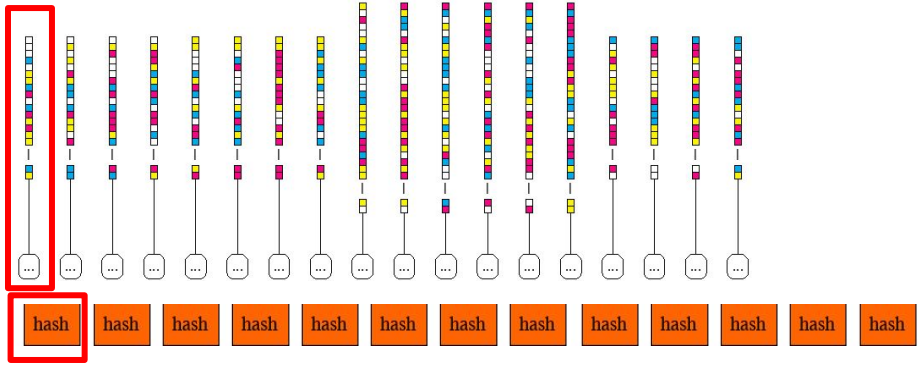


STACK

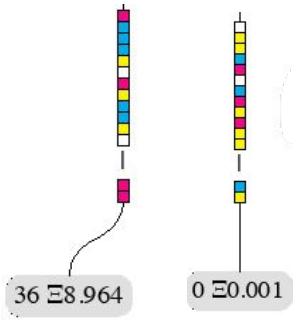


LEAF 124	HASH
LEAF 124	HASH
BRANCH 0,3	HASH
LEAF 125	BRANCH 0,1,2,3
LEAF 124	HASH
LEAF 124	LEAF 126
BRANCH 0,2	LEAF 125
BRANCH 0,2	LEAF 124
HASH	LEAF 124
BRANCH 0,1,2	BRANCH 2,3
HASH	LEAF 125
LEAF 124	BRANCH 0,1,2
LEAF 124	BRANCH 0,1,3
BRANCH 0,3	HASH
LEAF 125	BRANCH 0,1,2,3
LEAF 125	CODE
BRANCH 0,2,3	ACCLEAF 125
HASH	HASH
HASH	EXTENSION <1>
BRANCH 0,1,2,3	BRANCH 1,2
HASH	LEAF 124
HASH	LEAF 124
HASH	BRANCH 0,1
EXTENSION <01>	EXTENSION <2>
LEAF 125	LEAF 126
BRANCH 0,2	BRANCH 0,2,3
	BRANCH 0,1,2,3

Verification of block proof



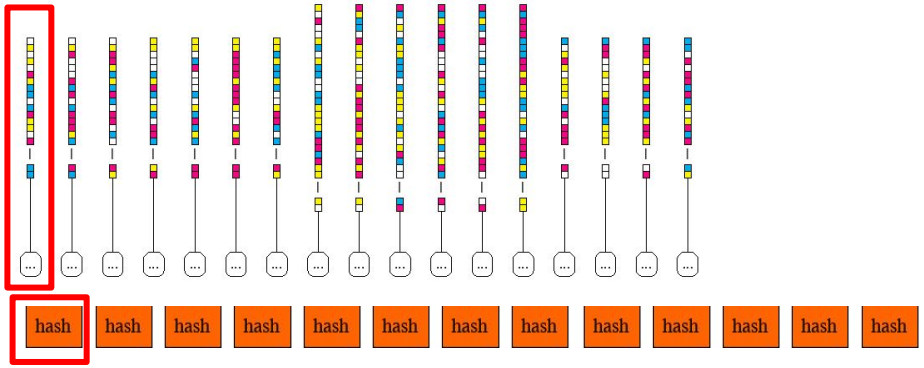
STACK

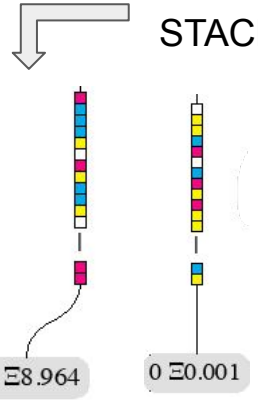



```
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
```

```
HASH
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

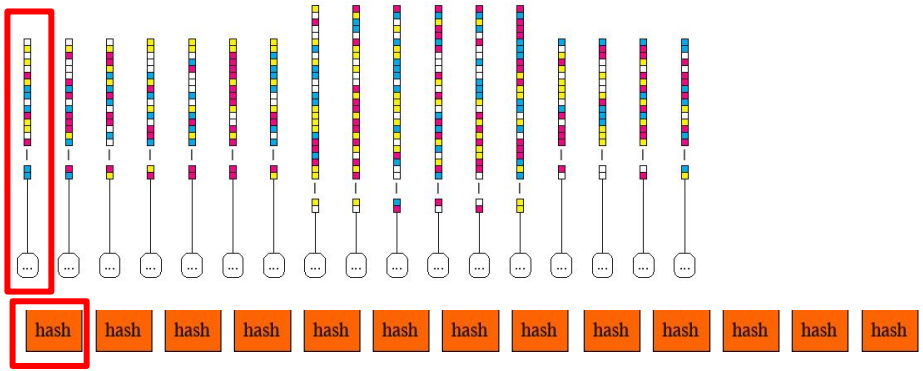


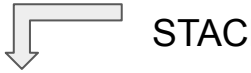


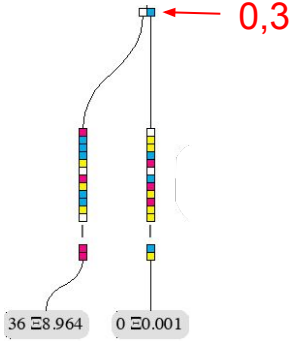

```
BRANCH 0,3
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
```

```
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof



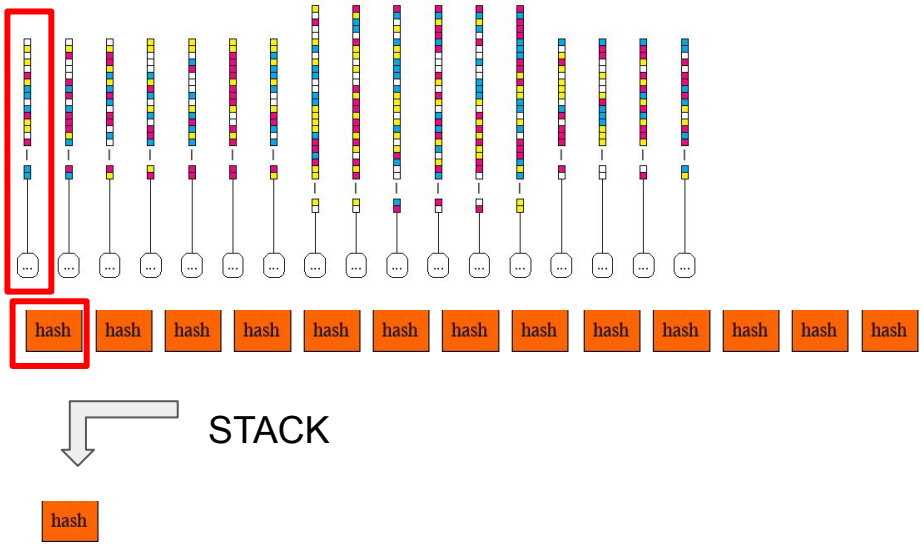





```
BRANCH 0,3
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
```

```
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

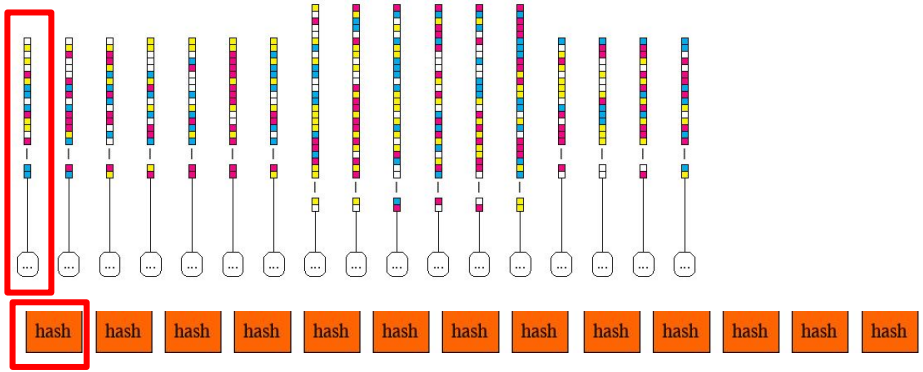
Verification of block proof

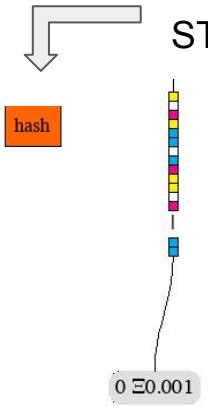


```
BRANCH 0,3
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
```

```
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

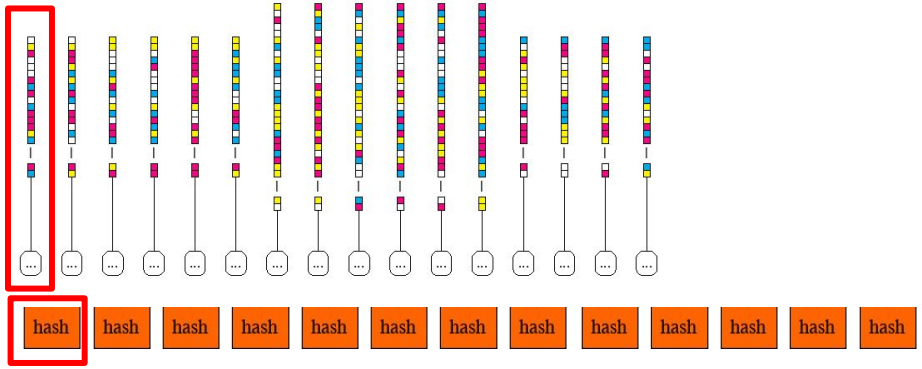


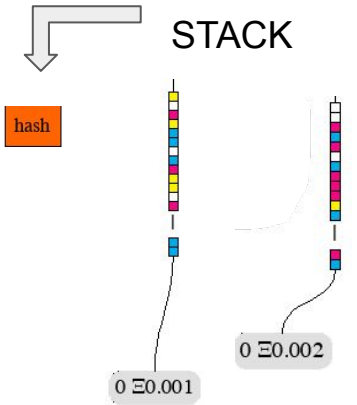



```
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
```

```
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

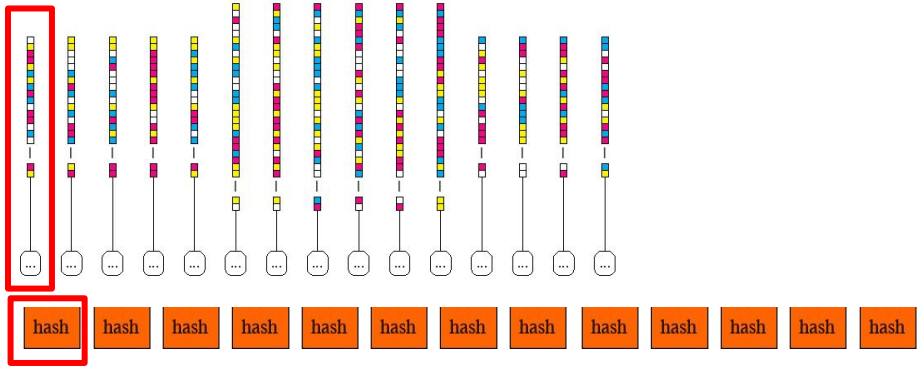


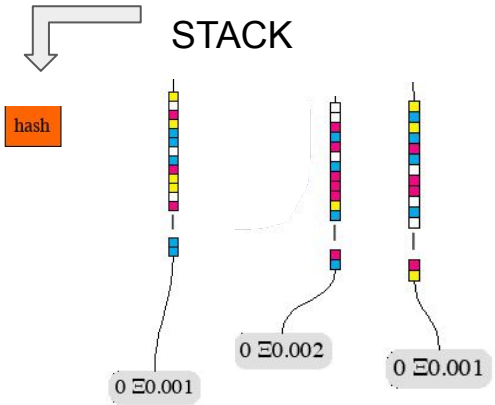



```
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
```

```
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

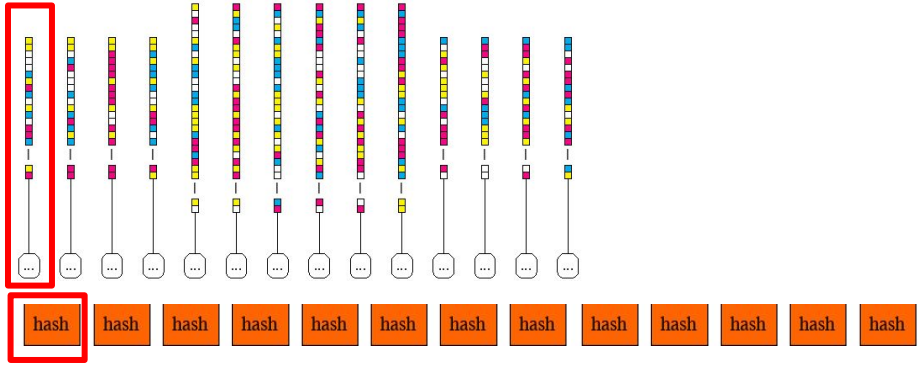


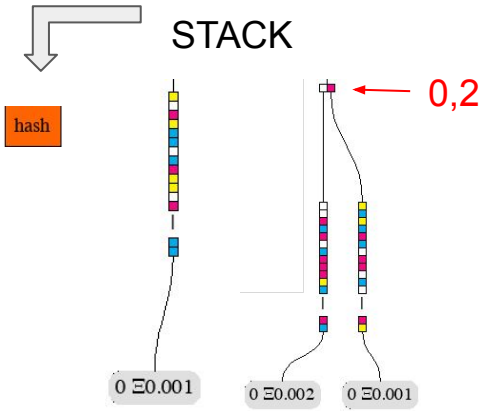



```
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
```

```
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

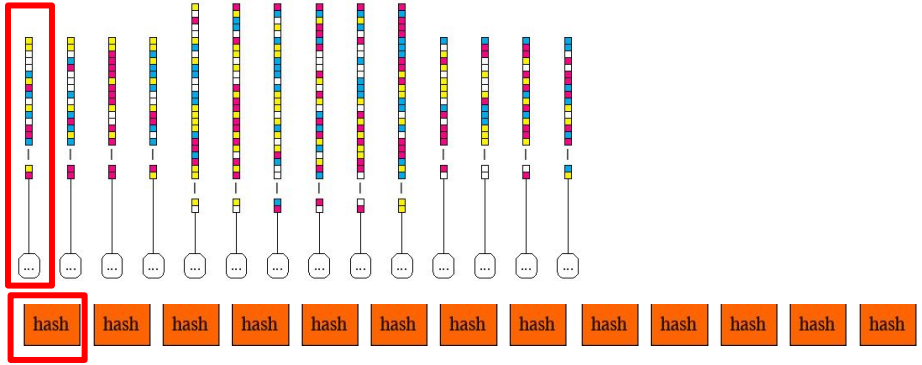


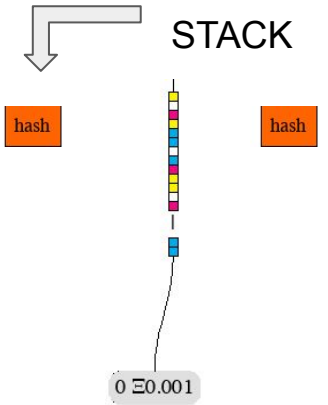



```
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
```

```
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

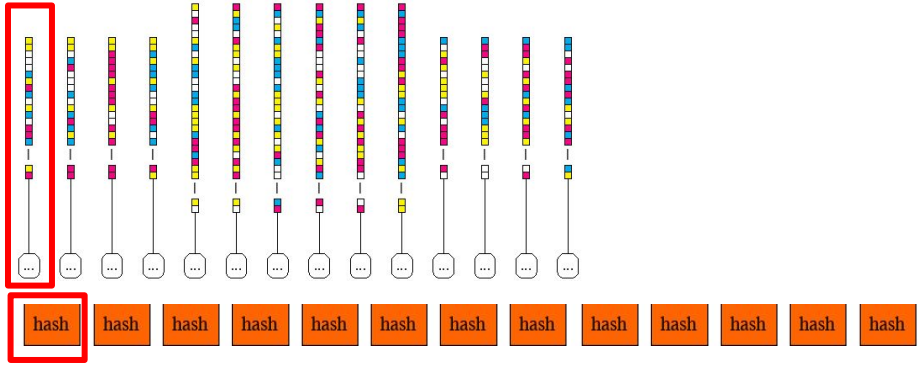


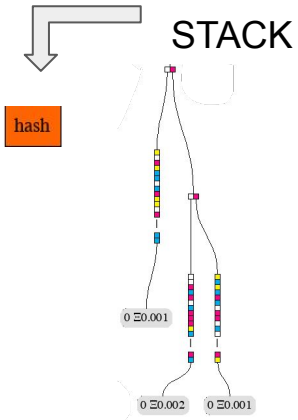



```
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
```

```
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

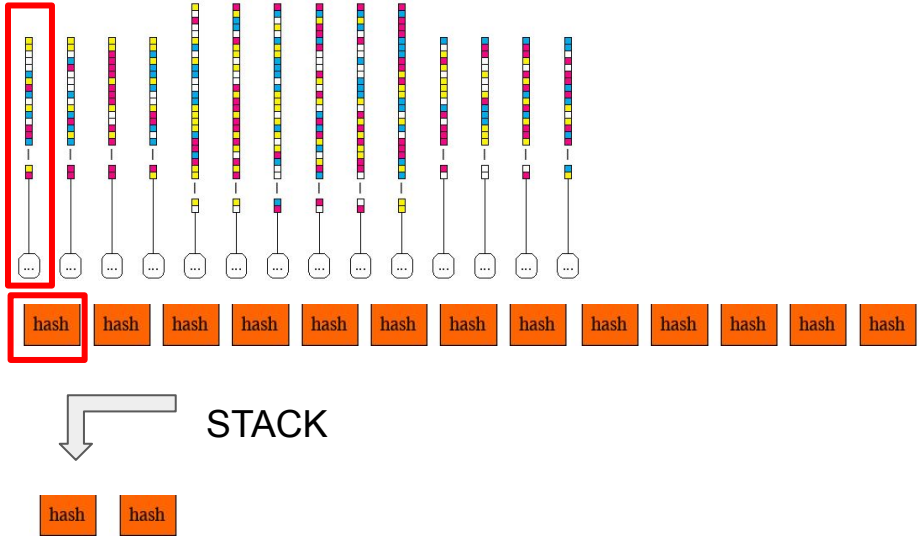





```
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
```

```
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

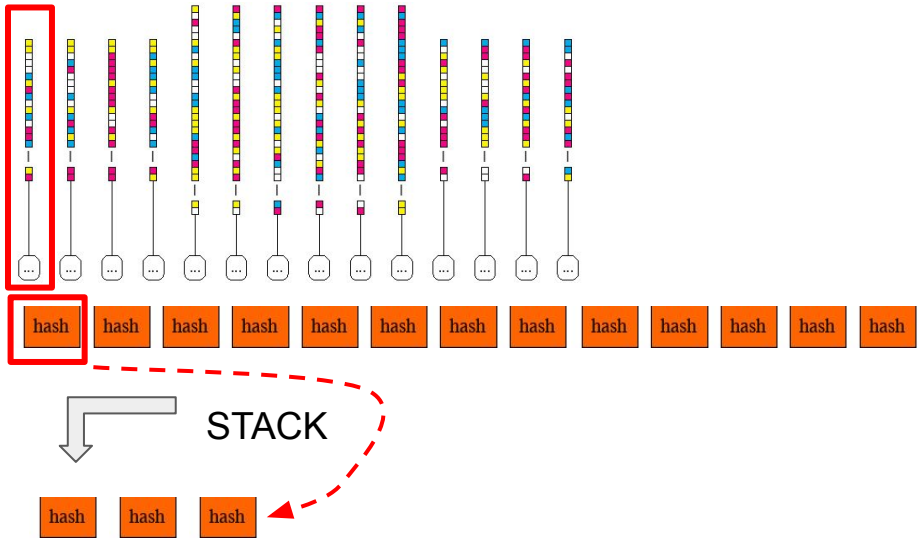
Verification of block proof



```
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
```

```
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

Verification of block proof

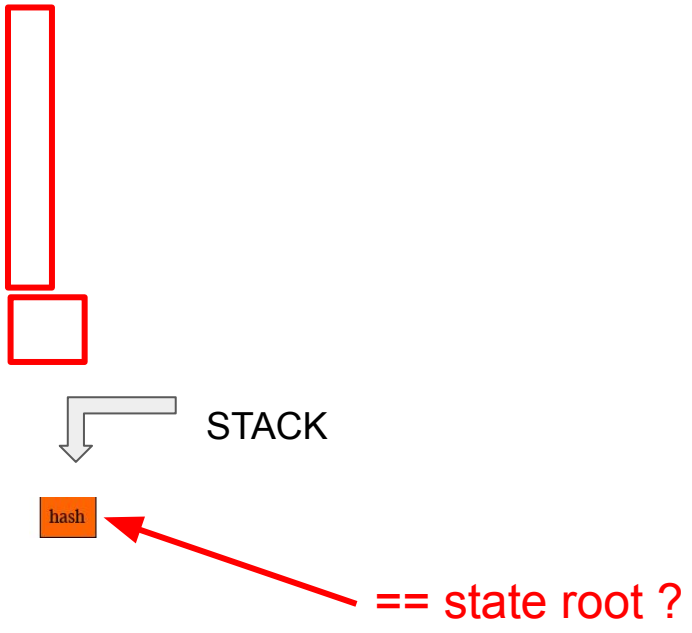


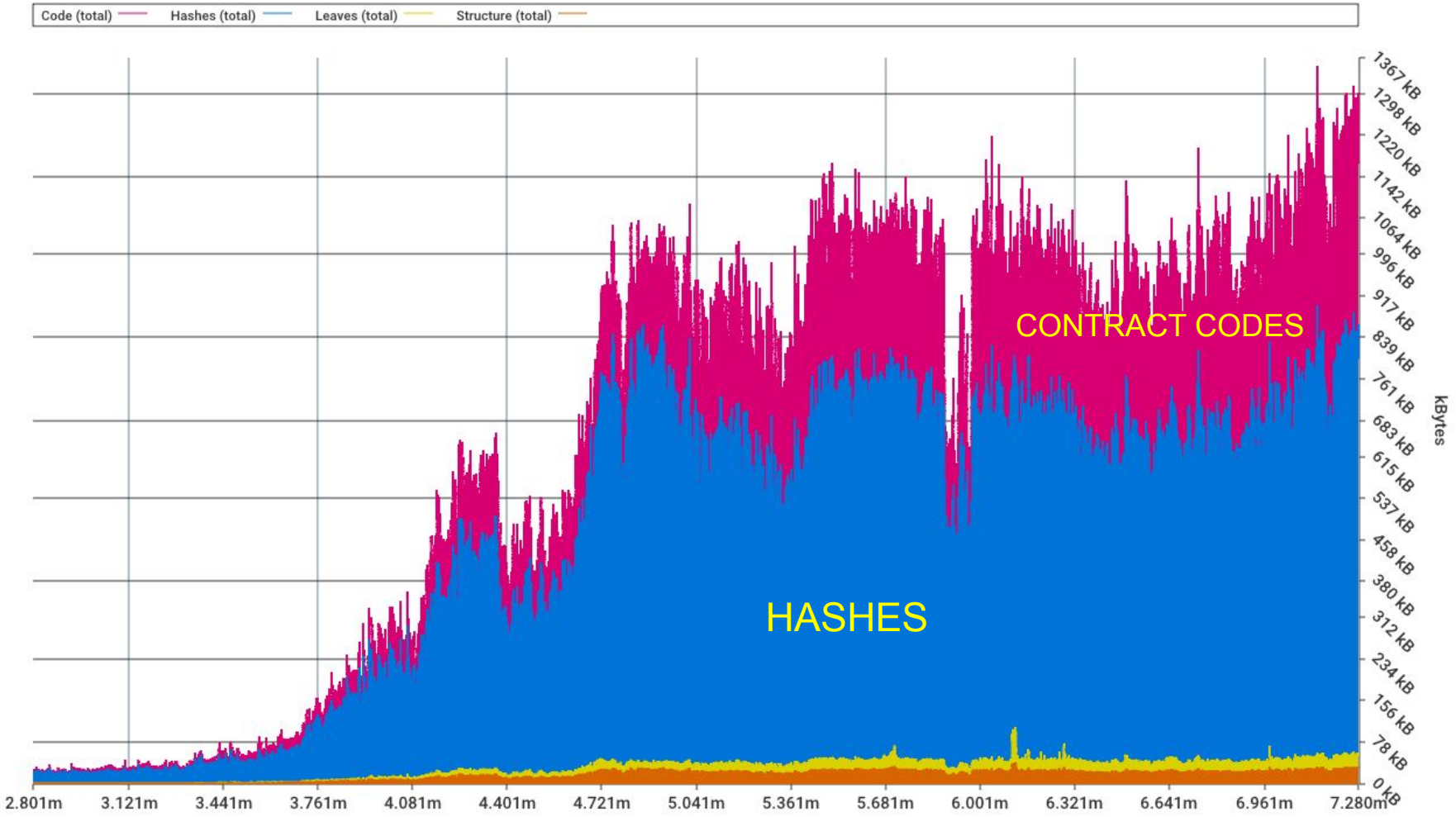
…. and so on ...

```
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
```

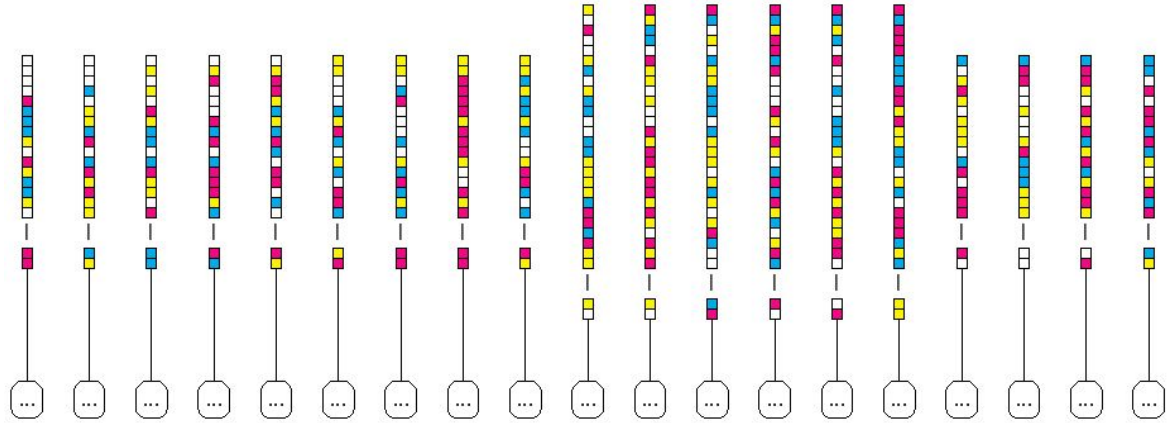
```
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

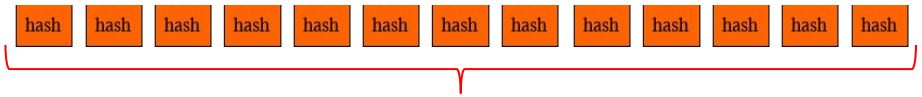
Verification of block proof




Code (total)
Hashes (total)
Leaves (total)
Structure (total)
CONTRACT CODES
HASHES
1367 kB
1298 kB
1220 kB
1142 kB
1064 kB
996 kB
917 kB
839 kB
761 kB
683 kB
615 kB
537 kB
458 kB
380 kB
312 kB
234 kB
156 kB
78 kB
0 kB
kBytes
2.801m
3.121m
3.441m
3.761m
4.081m
4.401m
4.721m
5.041m
5.361m
5.681m
6.001m
6.321m
6.641m
6.961m
7.280m

STARK for block proof verification





auxiliary (hidden) input

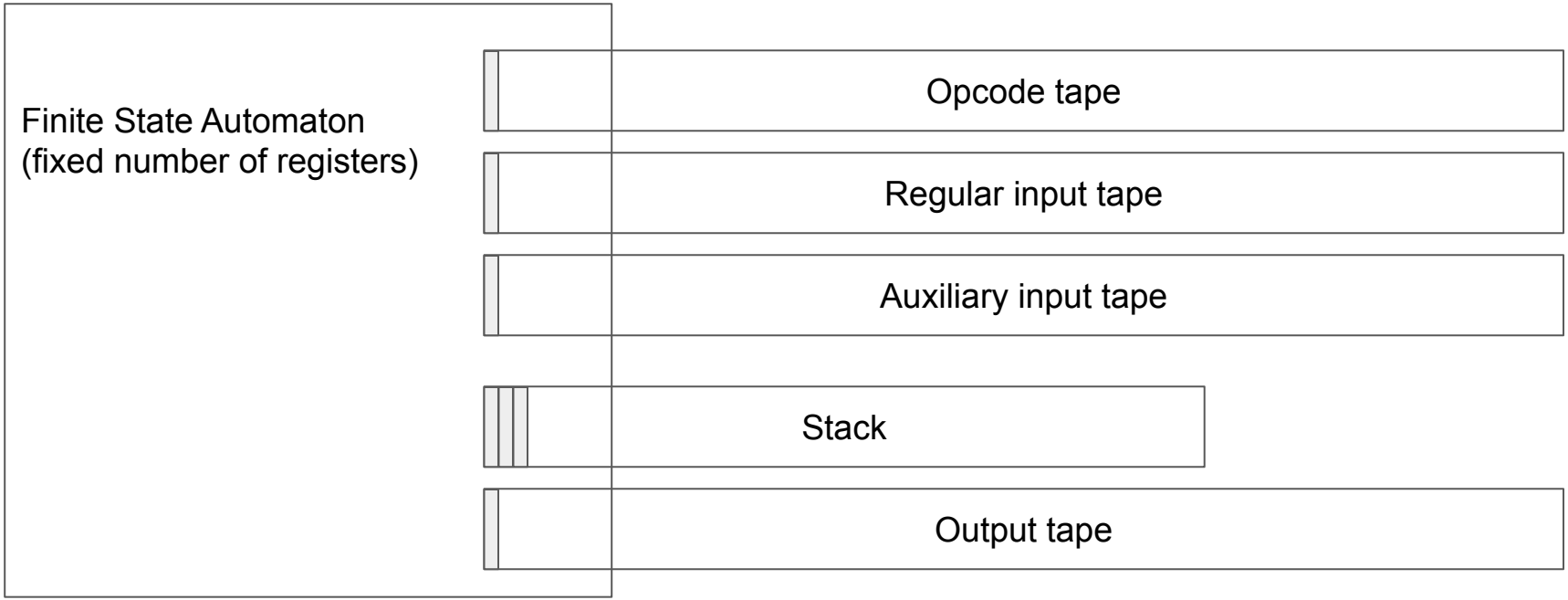
stateful?

regular (open) input

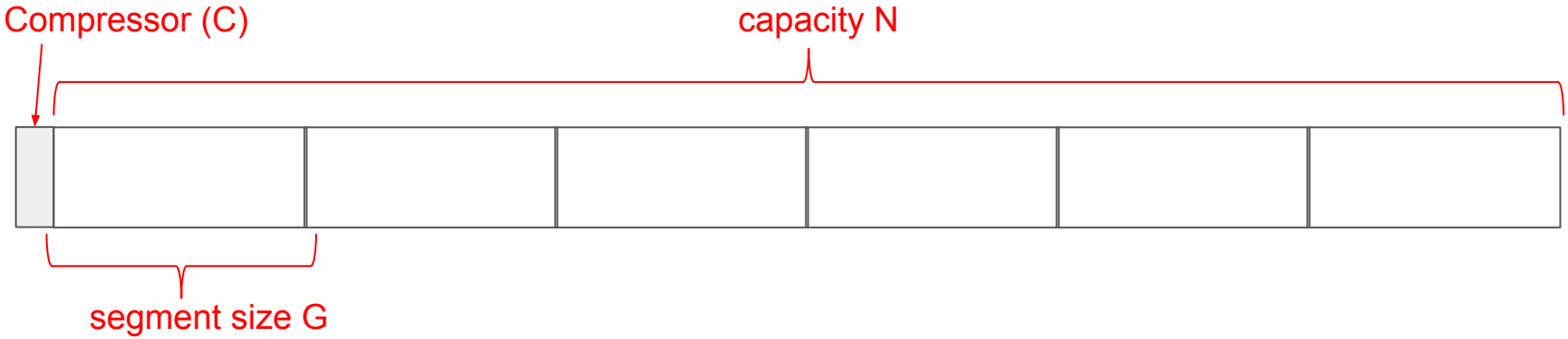
```
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 124
LEAF 124
BRANCH 0,2
BRANCH 0,2
HASH
BRANCH 0,1,2
HASH
LEAF 124
LEAF 124
BRANCH 0,3
LEAF 125
LEAF 125
BRANCH 0,2,3
HASH
HASH
BRANCH 0,1,2,3
HASH
HASH
HASH
EXTENSION <01>
LEAF 125
BRANCH 0,2
```

```
HASH
HASH
HASH
BRANCH 0,1,2,3
HASH
LEAF 126
LEAF 125
LEAF 124
LEAF 124
BRANCH 2,3
LEAF 125
BRANCH 0,1,2
BRANCH 0,1,3
HASH
BRANCH 0,1,2,3
CODE
ACCLEAF 125
HASH
EXTENSION <1>
BRANCH 1,2
LEAF 124
LEAF 124
BRANCH 0,1
EXTENSION <2>
LEAF 126
BRANCH 0,2,3
BRANCH 0,1,2,3
```

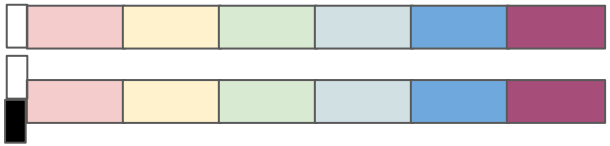
Initial ideas - “Arithmetic hardware”



Input tapes



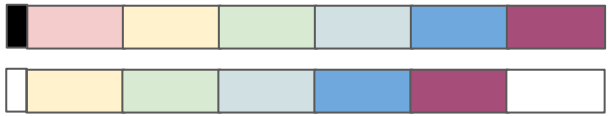
If C == 0, then $S_i` = S_i$



$(1+C)*(1+(1+S_0`+S_0)*(1+S_1`+S_1)*...*(1+S_N`+S_N))$

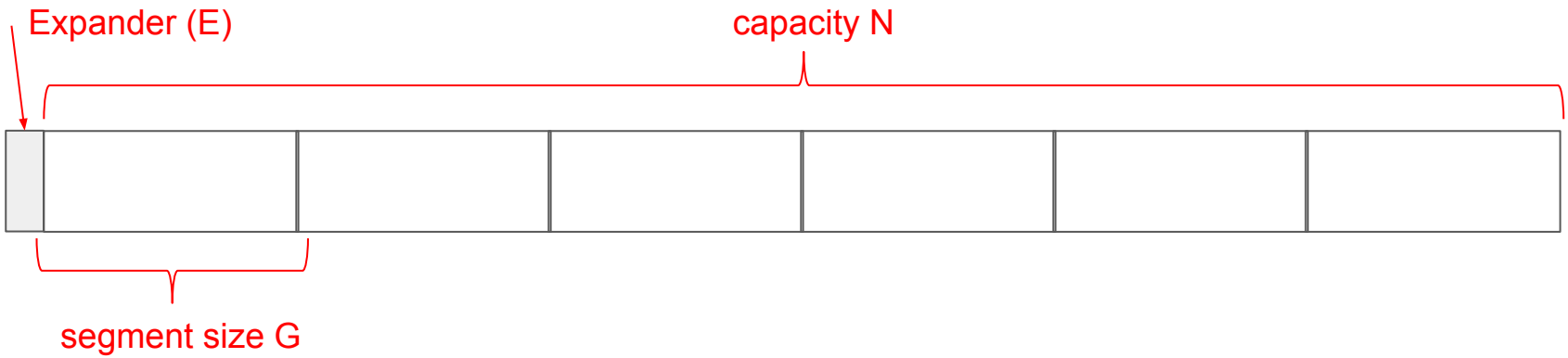
Degree N, in GF(2)

If C == 1, then $C` = 0$, and $S_i` = S_{i+G}$

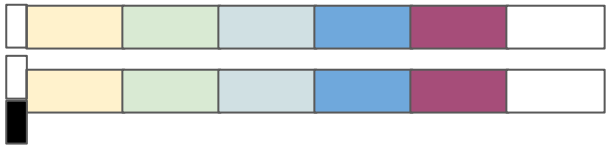


$C*(1+(1+S_0`+S_G)*(1+S_1`+S_{1+G})*...*(1+S_{N-G}`+S_N))$

Output tapes



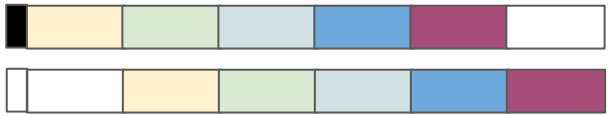
If E == 0, then $S_i` = S_i$



$(1+C)*(1+(1+S_0`+S_0)*(1+S_1`+S_1)*...*(1+S_N`+S_N))$

Degree N, in GF(2)

If E == 1, then E` = 0, and $S_i` = S_{i-G}$



$C*(1+(1+S_G`+S_0)*(1+S_{1+G}`+S_1)*...*(1+S_N`+S_{N-G}))$