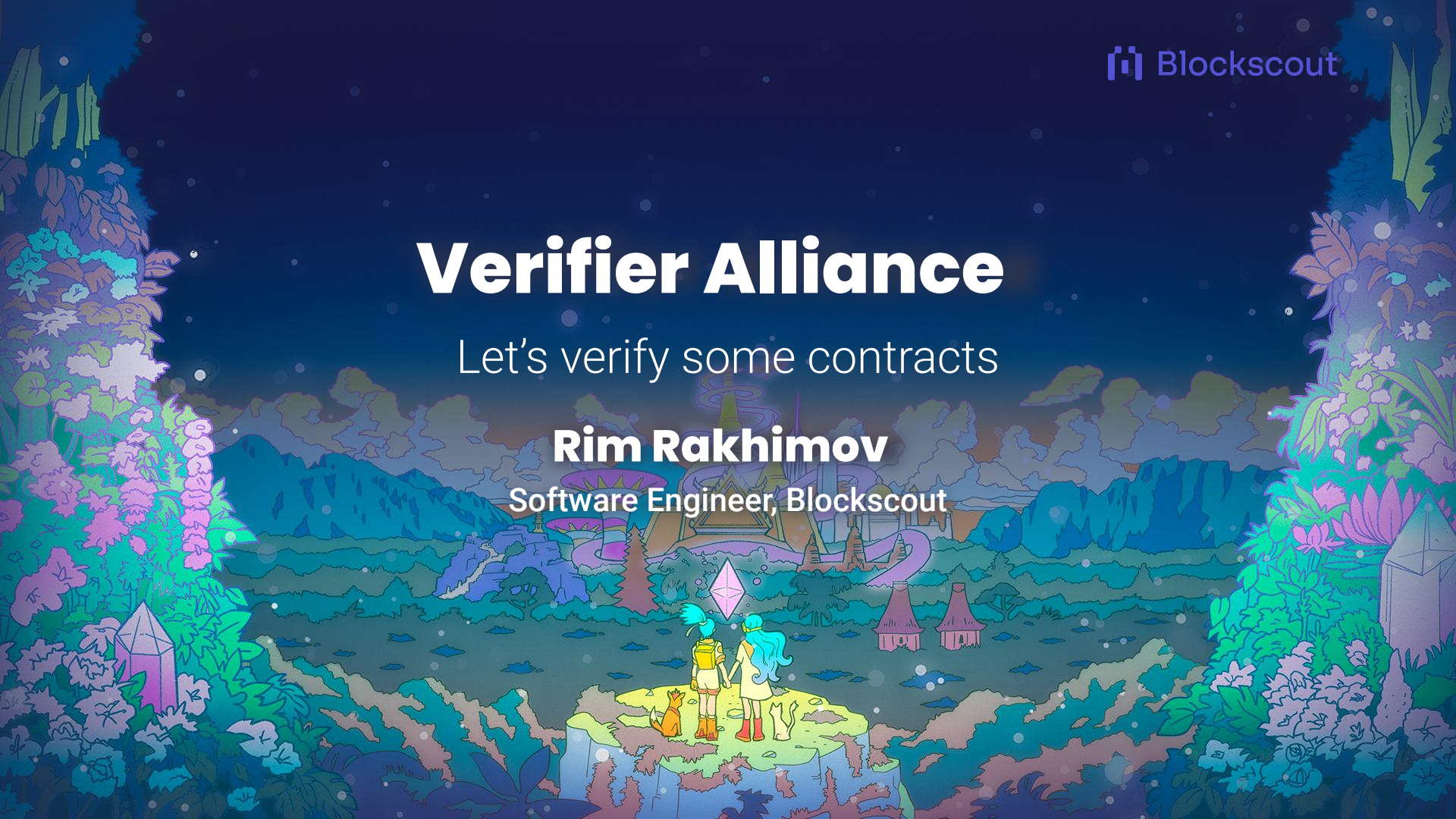


Verifier Alliance

Let's verify some contracts

Rim Rakhimov

Software Engineer, Blockscout



Transactions 1
Account history
Token transfers 0
Tokens 0
Internal txns 1
Coin balance history
Contract

Contract creation code
Verify & publish

```
0x6080604052348015600e575f80fd5b5060a580601a5f395ff3fe080604052348015600e575f80fd5b50600436106030575f3560e01c80632e64cec11460345780636057361d146048575b5f80fd5b5f5460405190815260200160405180910390f35b605760533660046059565b5f55565b005b5f602082840312156068575f80fd5b503591905056fea264697066735822122097b584831b638126257b6ecbb9c73fb7c810d8f9f4d63cfd861350982942e664736f6c634300081a0033
```

Deployed ByteCode

```
0x6080604052348015600e575f80fd5b50600436106030575f3560e01c80632e64cec11460345780636057361d146048575b5f80fd5b5f5460405190815260200160405180910390f35b605760533660046059565b5f55565b005b5f602082840312156068575f80fd5b503591905056fea264697066735822122097b584831b638126257b6ecbb9c73fb7c810d8f9f4d63cfd861350982942e664736f6c634300081a0033
```

Transactions 1
Account history
Token transfers 0
Tokens 0
Internal txns 1
Coin balance history
Contract ✓

Code
Read contract
Write contract

Contract Source Code Verified (Exact Match)

Contract name	Storage	Compiler version	v0.8.26+commit.8a97fa7a
EVM Version	Cancun	Optimization enabled	true
Optimization runs	1984	Verified at	Nov 07 2024 01:04:48 AM
Contract file path	contracts/1.Storage.sol		

Contract source code (Solidity)

```

1 // SPDX-License-Identifier: GPL-3.0
2
3 pragma solidity >=0.8.2 <0.9.0;
4
5 /**
6  * @title Storage
7  * @dev Store & retrieve value in a variable
8  * @custom:dev-run-script ./scripts/deploy_with_ethers.ts
9  */
10 contract Storage {
11
12     uint256 number;
13
14     /**
15      * @dev Store value in variable
16      * @param num value to store

```

What is contract verification

Let's verify a contract (1)



Contract creation code

On-chain creation code

Verify & publish

0x6080604052348015600e575f80fd5b5060b980601a5f395f3fe080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b6044481602ae05f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e01b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033

Deployed ByteCode

On-chain runtime code

0x6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e01b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033

Let's verify a contract (1)



Contract creation code

On-chain creation code

Verify & publish

0xe080604052348015600e575f80fd5b50600b980601a5f395ff3fe080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602ae05f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e07b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033

Deployed ByteCode

On-chain runtime code

0xe080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602ae05f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e07b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033

```
contract TrickyStorage_1 {
    uint256 value;

    function store(uint256 new_value) external {
        value = new_value + 42;
    }
}
```


Let's verify a contract (1)

Contract creation code

On-chain creation code

Verify & publish

0xe080604052348015600e575f80fd5b5060b980601a5f395ff3fe080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e07b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033

Deployed ByteCode

On-chain runtime code

0xe080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e07b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033

```
contract TrickyStorage_1 {
    uint256 value;

    function store(uint256 new_value) external {
        value = new_value + 42;
    }
}
```

solc-v0.8.26

Let's verify a contract (1)

Contract creation code	On-chain creation code	Verify & publish
<pre>0xe080604052348015600e575f80fd5b50600b980601a5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e07b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033</pre>		
Deployed ByteCode	On-chain runtime code	
<pre>0xe080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e07b5f52601160045260245fdd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033</pre>		

```
contract TrickyStorage_1 {
    uint256 value;

    function store(uint256 new_value) external {
        value = new_value + 42;
    }
}
```

solc-v0.8.26

```
{
  "optimizer": {
    "enabled": true,
    "runs": 1
  }
}
```


Let's verify a contract (2)

```
contract TrickyStorage_1 {  
    uint256 value;  
  
    function store(uint256 new_value) external {  
        value = new_value + 42;  
    }  
}
```

```
{  
  "optimizer": {  
    "enabled": true,  
    "runs": 1  
  }  
}
```

Let's verify a contract (2)

```
contract TrickyStorage_1 {  
    uint256 value;  
  
    function store(uint256 new_value) external {  
        value = new_value + 42;  
    }  
}
```

Combine into
Standard Json Input

```
{  
  "optimizer": {  
    "enabled": true,  
    "runs": 1  
  }  
}
```

```
{  
  "language": "Solidity",  
  "sources": {  
    "contracts/TrickyStorage-1.sol": {  
      "content": "contract TrickyStorage_1 ..."  
    }  
  },  
  "settings": {  
    "optimizer": {  
      "enabled": true,  
      "runs": 1  
    }  
  }  
}
```


Let's verify a contract (2)

```
contract TrickyStorage_1 {  
    uint256 value;  
  
    function store(uint256 new_value) external {  
        value = new_value + 42;  
    }  
}
```

Combine into
Standard Json Input

```
{  
  "optimizer": {  
    "enabled": true,  
    "runs": 1  
  }  
}
```

```
{  
  "language": "Solidity",  
  "sources": {  
    "contracts/TrickyStorage-1.sol": {  
      "content": "contract TrickyStorage_1 ..."  
    }  
  },  
  "settings": {  
    "optimizer": {  
      "enabled": true,  
      "runs": 1  
    }  
  }  
}
```

solc-v0.8.26
--standard-json



Let's verify a contract (2)

```
contract TrickyStorage_1 {
  uint256 value;

  function store(uint256 new_value) external {
    value = new_value + 42;
  }
}
```

```
{
  "optimizer": {
    "enabled": true,
    "runs": 1
  }
}
```

Combine into
Standard Json Input

```
{
  "language": "Solidity",
  "sources": {
    "contracts/TrickyStorage-1.sol": {
      "content": "contract TrickyStorage_1 ..."
    }
  },
  "settings": {
    "optimizer": {
      "enabled": true,
      "runs": 1
    }
  },
  "evm": {
  }
}
```

solc-v0.8.26
--standard-json



Standard Json
Output

```
{
  "contracts": {
    "contracts/TrickyStorage-1.sol": {
      "TrickyStorage_1": {
        "evm": {
          "bytecode": { /*compiled creation code*/
            "object": "60806040..."
          },
          "deployedBytecode": { /*compiled runtime code*/
            "object": "60806040..."
          }
        },
        ...
      }
    }
  },
  ...
}
```


Let's verify a contract (3)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b5060b980601a5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c8
0636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058
575f80fd5b5035919050565b80820180821115607d57634e487b7160e01b5f52601160045260245ffd5b9291505056fea26469706673582
212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033
```



match?

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b5060b980601a5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c8
0636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058
575f80fd5b5035919050565b80820180821115607d57634e487b7160e01b5f52601160045260245ffd5b9291505056fea26469706673582
212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033
```

Let's verify a contract (3)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b5060b980601a5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e01b5f52601160045260245ffd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033
```

Verified

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b5060b980601a5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b603960353660046049565b603b565b005b604481602a605f565b5f5550565b5f602082840312156058575f80fd5b5035919050565b80820180821115607d57634e487b7160e01b5f52601160045260245ffd5b9291505056fea26469706673582212201ed0d03edb7667e64bcabfcbad977c32d6299a98747650fe0a9ed6a8f181ae1664736f6c634300081a0033
```


A little more complex contract (1)



Contract creation code

Verify & publish

0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163ad0899b60e01b815260048101829052602a602482015273513ddf9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ff45b5050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033

Deployed ByteCode

0x6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163ad0899b60e01b815260048101829052602a602482015273513ddf9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ff45b5050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033

...

```
library SafeMath {
    function sum(uint256 a, uint256 b) external pure returns (uint256) {
        return a + b;
    }
}

contract TrickyStorage_2 {
    uint256 value;

    function store(uint256 new_value) external {
        value = SafeMath.sum(new_value, 42);
    }
}
```

Let's verify a contract (2)

```
library SafeMath {  
    function sum(uint256 a, uint256 b) external pure returns  
(uint256) {  
        return a + b;  
    }  
}  
  
contract TrickyStorage_2 {  
    uint256 value;  
  
    function store(uint256 new_value) external {  
        value = SafeMath.sum(new_value, 42);  
    }  
}
```

Combine into
Standard Json Input

```
{  
  "language": "Solidity",  
  "sources": {  
    "contracts/TrickyStorage-2.sol": {  
      "content": "library SafeMath ..."  
    }  
  },  
  "settings": {  
    "optimizer": {  
      "enabled": true,  
      "runs": 1  
    }  
  }  
}
```

solc-v0.8.26
--standard-json



Standard Json
Output

```
{  
  "contracts": {  
    "contracts/TrickyStorage-2.sol": {  
      "TrickyStorage_2": {  
        "evm": {  
          "bytecode": { /*compiled creation code*/  
            "object": "60806040..."  
          },  
          "deployedBytecode": { /*compiled runtime code*/  
            "object": "60806040..."  
          }  
        },  
        ...  
      }  
    }  
  }  
}
```


A little more complex contract (3)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273__$9e30dc62696a7b2364588369d98712b6df__$9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```



match?

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

A little more complex contract (3)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273__$9e30dc62696a7b2364588369d98712b6df__$9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```



match?

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```


A little more complex contract (4)



Standard Json
Output

```
{
  "contracts": {
    "contracts/TrickyStorage-2.sol": {
      "TrickyStorage_2": {
        "evm": {
          "bytecode": { /*compiled creation code*/
            "linkReferences": {
              "contracts/TrickyStorage-2.sol": {
                "SafeMath": [
                  {
                    "length": 20,
                    "start": 116
                  }
                ]
              }
            },
            "object": "60802018..."
          }
        }
      }
    }
  }
}
```

A little more complex contract (4)



Standard Json
Output

```
{
  "contracts": {
    "contracts/TrickyStorage-2.sol": {
      "TrickyStorage_2": {
        "evm": {
          "bytecode": { /*compiled creation code*/
            "linkReferences": {
              "contracts/TrickyStorage-2.sol": {
                "SafeMath": [
                  {
                    "length": 20,
                    "start": 116
                  }
                ]
              }
            },
            "object": "60802018..."
          }
        }
      }
    }
  }
}
```


A little more complex contract (5)



Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273__$9e30dc62696a7b2364588369d98712b6df$__9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

A little more complex contract (5)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273__$9e30dc62696a7b2364588369d98712b6df$__9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b535919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

116 bytes

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```


A little more complex contract (5)



Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273__$9e30dc62696a7b2364588369d98712b6df$__9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b535919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

116 bytes

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

A little more complex contract (5)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b535919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

116 bytes

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```


A little more complex contract (5)

Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```



match?

A little more complex contract (5)



Compiled Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```

Verified

On-chain Creation Code

```
0x6080604052348015600e575f80fd5b506101188061001c5f395ff3fe6080604052348015600e575f80fd5b50600436106026575f3560e01c80636057361d14602a575b5f80fd5b6039603536600460b6565b603b565b005b60405163cad0899b60e01b815260048101829052602a602482015273513ddfe9cdfcc551a4088bf956477ce7d5f2887e9063cad0899b90604401602060405180830381865af4158015608f573d5f803e3d5ffd5b505050506040513d601f19601f8201168201806040525081019060b1919060cc565b5f5550565b5f6020828403121560c5575f80fd5b5035919050565b5f6020828403121560db575f80fd5b505191905056fea264697066735822122036cbbd47009d2c233e50a23cc7be08b002c152e65efdd1c9d17a1ccd70d26cab64736f6c634300081a0033
```


Code Transformations

Actions that may be applied to the compiled code which do not affect its EVM opcodes

- Libraries
- Cbor Auxdata
- Constructor Arguments
- Immutables
- Call Protection



Code Transformations

Actions that may be applied to the compiled code which do not affect its EVM opcodes



Panel: Source Code Verification

- Nov 13th — 5:30 PM
- Stage 2
- Blockscout, Sourcify and Routerscan