DID 合约

- DID格式：`did:etd:<etd address>`
- DID Document格式

  ```
  {
    '@context': [
        "https://www.w3.org/ns/did/v1",
        "https://w3cid.org/security/suites/secp256k1recovery-2020/v2"
    ]
    id: "did:etd:0x7c...",
    alsoKnownAs: "ETD Wallet",
    created: "2023-04-28T14:30:00.000Z",
    verificationMethod: [
      {
        id: 'did:etd:0x7c...#controller'
        type: 'EcdsaSecp256k1RecoveryMethod2020',
        controller: 'did:etd:0x7c...'
      }
    ]
    authenticationMethod: [
      'did:etd:0x7c...'
    ]
  }
  ```

- 合约结构
  - 事件触发
    - `AttributeChanged`
    - `OwnerChanged`
  - 可调用方法
    - `createWeId()`：创建并注册DID
      - 接受参数
        - `address identity`：本地生成以太坊地址/现有钱包地址,
        - `bytes memory alsoknownas`：自定义用途，例如“ETD Wallet”
        - `bytes memory created`：创建时间戳
        - `int updated`：过期时间，0表示永久DID
    - `changeOwner ()`：更换DID Controller
      - `address identity`：DID
      - `address newOwner`：DID new owner
    - `setAttribute()`：更新DID属性
      - `address identity`：DID
      - `bytes32 name`：属性名
      - `bytes memory value`：值
      - `int updated`：更新时间
  - 注意，这里三个方法都只能DID 本身的Controller（即Wallet DID）才可以调用
- 合约代码

`EtdDIDRegistry.sol`

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.6;

contract EtdDIDRegistry{

    bytes32 constant private KEY_CREATED = "created";
    bytes32 constant private KEY_ALSO_KNOWN_AS = "alsoKnownAs";

    mapping(address => address) public owners;  // owner = owners[did]
    mapping(address => uint) public changed;

    modifier onlyOwner(address identity, address actor) {
    require (actor == identityOwner(identity), "bad_actor");
    _;
  }

    event AttributeChanged(
        address indexed identity,
        bytes32 name,
        bytes value,
        uint previousBlock,
        int updated
    );

    event OwnerChanged(
        address indexed identity,
        address owner,
        uint previousBlock
    );

    function createWeId(
        address identity,
        bytes memory alsoknownas,
        bytes memory created,
        int updated
    )
        public
        onlyOwner(identity, msg.sender)
    {
        emit AttributeChanged(identity, KEY_CREATED, created, changed[identity],
updated);
        emit AttributeChanged(identity, KEY_ALSO_KNOWN_AS, alsoknownas,
changed[identity], updated);
        changed[identity] = block.number;
    }

    function changeOwner(address identity, address newOwner) public
onlyOwner(identity, msg.sender) {
        owners[identity] = newOwner;
        emit OwnerChanged(identity, newOwner, changed[identity]);
        changed[identity] = block.number;
    }
    function setAttribute(address identity, bytes32 name, bytes memory value, int updated ) public onlyOwner(identity, msg.sender) {
        emit AttributeChanged(identity, name, value, changed[identity], updated);
        changed[identity] = block.number;
    }

    function identityOwner(address identity) public view returns(address) {
        address owner = owners[identity];
        if (owner != address(0x00)) {
            return owner;
        }
    return identity;
    }

}
```

- 合约部署在测试网Georli：`0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A`

合约测试

1.创建

- 测试代码：`test.js`

```
(async () => {
    try {
        const contractName = 'EtdDIDRegistry'
        const artifactsPath = `browser/contracts/artifacts/${contractName}.json`
        const contractAddress = "0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A";

        const metadata = JSON.parse(await remix.call('fileManager', 'getFile', artifactsPath))

        await window.ethereum.enable()
        const accounts = await web3.eth.getAccounts()
        const defaultAccount = accounts[0]

        let contract = new web3.eth.Contract(metadata.abi)
        // const contract = new ethers.Contract(contractAddress, metadata.abi);

        contract.options.address = contractAddress
        const result = await contract.methods.createWeId(
            accounts[0],
            web3.utils.asciiToHex("ETD Wallet"),
            web3.utils.asciiToHex("2023-04-28T14:30:00.000Z"),
            0
        ).send({ from: defaultAccount })

        console.log(result)
    } catch (e) {
        console.log(e.message)
    }
  })()
```

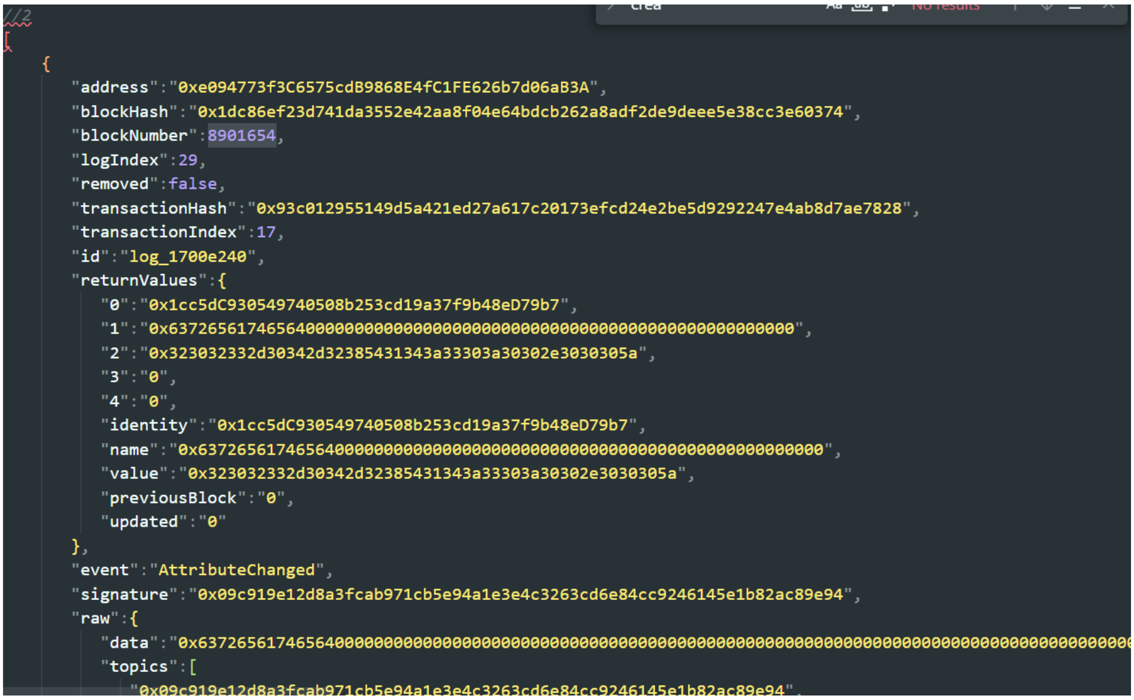
- 结果
  拼接图 (1)

2.查询Event

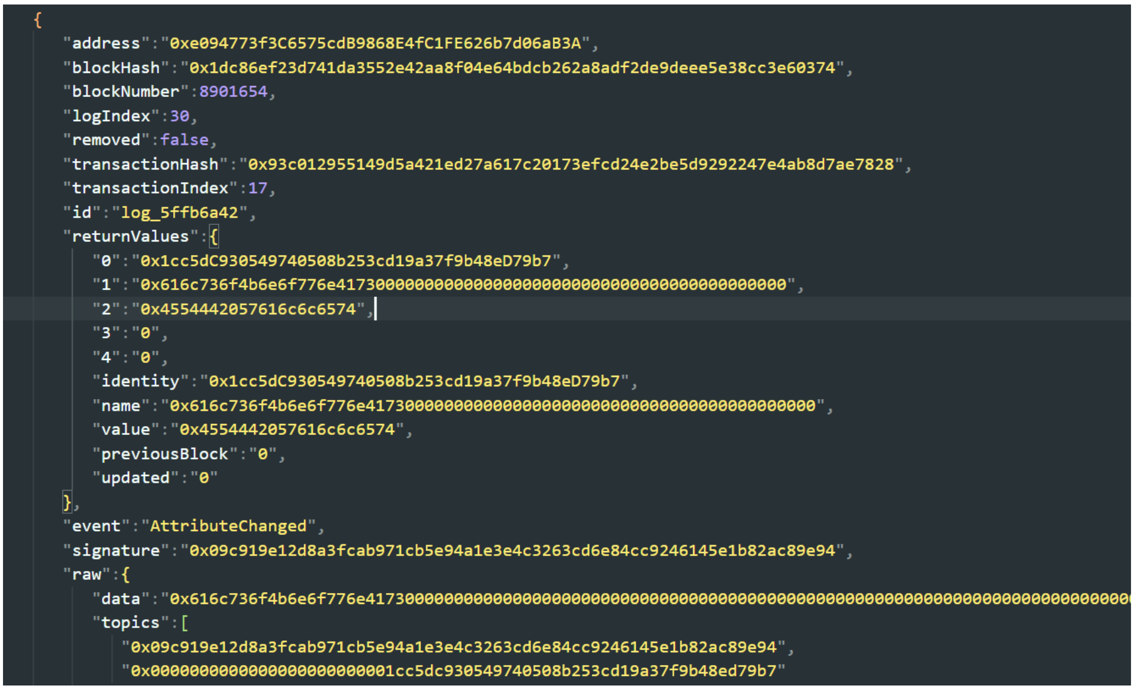
- 测试代码 js

```
(async () => {
    try {
        const Web3 = require('web3');
        const web3 = new Web3(new Web3.providers.HttpProvider('https://goerli.infura.io/v3/2c19e69b16e7440ea07fc3aeb8478d85'))
        const contractName = 'EtdDIDRegistry'
        const artifactsPath = `browser/contracts/artifacts/${contractName}.json`
        const contractAddress = "0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A";

        const metadata = JSON.parse(await remix.call('fileManager', 'getFile', artifactsPath))
        await window.ethereum.enable()

        let contract = new web3.eth.Contract(metadata.abi)
        // const contract = new ethers.Contract(contractAddress, metadata.abi);

        contract.options.address = contractAddress

        const eventName = 'AttributeChanged';
        const startBlock = 8901654; // 起始区块号

        contract.getPastEvents(eventName, {
            fromBlock: startBlock,
            toBlock: 'latest'
        }, (error, events) => {
            if (error) console.error(error);
            console.log(events);
        });
    } catch (e) {
        console.log(e.message)
    }
  })()
```

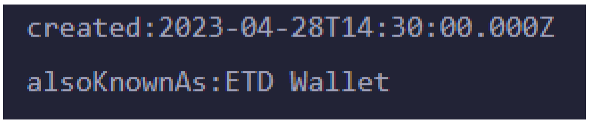
- 结果



```
//2
[
    {
        "address":"0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A",
        "blockHash":"0x1dc86ef23d741da3552e42aa8f04e64bdcb262a8adf2de9deee5e38cc3e60374",
        "blockNumber":8901654,
        "logIndex":29,
        "removed":false,
        "transactionHash":"0x93c012955149d5a421ed27a617c20173efcd24e2be5d9292247e4ab8d7ae7828",
        "transactionIndex":17,
        "id":"log_1700e240",
        "returnValues":{
            "0":"0x1cc5dC930549740508b253cd19a37f9b48eD79b7",
            "1":"0x6372656174656400000000000000000000000000000000000000000000000000",
            "2":"0x323032332d30342d32385431343a33303a30302e3030305a",
            "3":"0",
            "4":"0",
            "identity":"0x1cc5dC930549740508b253cd19a37f9b48eD79b7",
            "name":"0x6372656174656400000000000000000000000000000000000000000000000000",
            "value":"0x323032332d30342d32385431343a33303a30302e3030305a",
            "previousBlock":"0",
            "updated":"0"
        },
        "event":"AttributeChanged",
        "signature":"0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",
        "raw":{
            "data":"0x637265617465640000000000000000000000000000000000000000000000000000000000000000000000000000000
            "topics":[
                "0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",
```



```
    {
        "address":"0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A",
        "blockHash":"0x1dc86ef23d741da3552e42aa8f04e64bdcb262a8adf2de9deee5e38cc3e60374",
        "blockNumber":8901654,
        "logIndex":30,
        "removed":false,
        "transactionHash":"0x93c012955149d5a421ed27a617c20173efcd24e2be5d9292247e4ab8d7ae7828",
        "transactionIndex":17,
        "id":"log_5ffb6a42",
        "returnValues":{
            "0":"0x1cc5dC930549740508b253cd19a37f9b48eD79b7",
            "1":"0x616c736f4b6e6f776e4173000000000000000000000000000000000000000000",
            "2":"0x4554442057616c6c6574",
            "3":"0",
            "4":"0",
            "identity":"0x1cc5dC930549740508b253cd19a37f9b48eD79b7",
            "name":"0x616c736f4b6e6f776e4173000000000000000000000000000000000000000000",
            "value":"0x4554442057616c6c6574",
            "previousBlock":"0",
            "updated":"0"
        },
        "event":"AttributeChanged",
        "signature":"0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",
        "raw":{
            "data":"0x616c736f4b6e6f776e41730000000000000000000000000000000000000000000000000000000000000000000000000
            "topics":[
                "0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",
                "0x0000000000000000000000001cc5dc930549740508b253cd19a37f9b48ed79b7"
```

- 解析结果 - DID Document
    - 

      ```
      created:2023-04-28T14:30:00.000Z
      alsoKnownAs:ETD Wallet
      ```

- did <-> did doc (RPC)

  faucet：

    account：0x1cc5dC930549740508b253cd19a37f9b48eD79b7

- ENS合约
- metamask登陆流程

  签名验证的流程
- 收费

-

合约部署到ETD

合约地址：`0xcB839E80E07CaF3cCe434198eeD262f1283db4Cb`

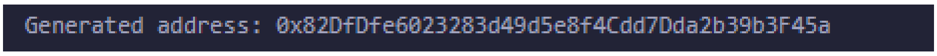
v2: `0xDca6E0B44C662c4Ed093732cC8F5b0c0075FC25E`

调用测试

- 创建DID：`test.js`

```
{

"blockHash":"0xa4b94f9d0edae3b387181c677a2b6ee9233d129c1e5cb49f7169a060849fb
ff3",
   "blockNumber":5414735,
   "contractAddress":null,
   "cumulativeGasUsed":54347,
   "effectiveGasPrice":1000000000,
   "from":"0x1cc5dc930549740508b253cd19a37f9b48ed79b7",
   "gasUsed":54347,

"logsBloom":"0x000000000000000000000000000000100800000000000000000000000000
0000000100000000100000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000002000000000040000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00400000000000000000000000000002001000000000000000000000000000000000000",
   "status":true,
   "to":"0xe094773f3c6575cdb9868e4fc1fe626b7d06ab3a",

"transactionHash":"0x63690c9c0a5ee60abe88abe77b05126e99f301fbab3491bfb677245
f61336057",
   "transactionIndex":0,
   "type":"0x0",
   "events":{
      "AttributeChanged":[
         {
            "address":"0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A",
            "blockNumber":5414735,

 "transactionHash":"0x63690c9c0a5ee60abe88abe77b05126e99f301fbab3491bfb67724
5f61336057",
            "transactionIndex":0,

 "blockHash":"0xa4b94f9d0edae3b387181c677a2b6ee9233d129c1e5cb49f7169a060849f
bff3",
            "logIndex":0,
            "removed":false,
            "id":"log_1ef5abaf",
            "returnValues":{
               "0":"0x82DfDfe6023283d49d5e8f4Cdd7Dda2b39b3F45a",

"1":"0x6372656174656400000000000000000000000000000000000000000000000000",
               "2":"0x323032332d30352d32315431343a33303a30302e3030305a",
               "3":"0",
               "4":"0",
               "identity":"0x82DfDfe6023283d49d5e8f4Cdd7Dda2b39b3F45a",

"name":"0x6372656174656400000000000000000000000000000000000000000000000000",
               "value":"0x323032332d30352d32315431343a33303a30302e3030305a",
               "previousBlock":"0",
               "updated":"0"
            },
            "event":"AttributeChanged",

 "signature":"0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac8
9e94",
            "raw":{

"data":"0x637265617465640000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000008000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000183230323332d30352d32315431343a33303a30302e3030305a00
00000000000000",
               "topics":[

 "0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",

 "0x00000000000000000000000082dfdfe6023283d49d5e8f4cdd7dda2b39b3f45a"
               ]
            }
         },
         {
            "address":"0xe094773f3C6575cdB9868E4fC1FE626b7d06aB3A",
            "blockNumber":5414735,

 "transactionHash":"0x63690c9c0a5ee60abe88abe77b05126e99f301fbab3491bfb67724
5f61336057",
            "transactionIndex":0,

 "blockHash":"0xa4b94f9d0edae3b387181c677a2b6ee9233d129c1e5cb49f7169a060849f
bff3",
            "logIndex":1,
            "removed":false,
            "id":"log_c9299e70",
            "returnValues":{
               "0":"0x82DfDfe6023283d49d5e8f4Cdd7Dda2b39b3F45a",

"1":"0x616c736f4b6e6f776e4173000000000000000000000000000000000000000000",
               "2":"0x4554442057616c6c6574",
                "3":"0",
                "4":"0",
                "identity":"0x82DfDfe6023283d49d5e8f4Cdd7Dda2b39b3F45a",

"name":"0x616c736f4b6e6f776e417300000000000000000000000000000000000000000000",
                "value":"0x4554442057616c6c6574",
                "previousBlock":"0",
                "updated":"0"
            },
            "event":"AttributeChanged",

 "signature":"0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac8
9e94",
            "raw":{

"data":"0x616c736f4b6e6f776e4173000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000080000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000a4554442057616c6c6574000000000000000000000000000000
00000000000000",
                "topics":[

 "0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",

 "0x00000000000000000000000082dfdfe6023283d49d5e8f4cdd7dda2b39b3f45a"
                ]
            }
        }
    ]
  }
}
```

传入的地址:



```
Generated address: 0x82DfDfe6023283d49d5e8f4Cdd7Dda2b39b3F45a
```

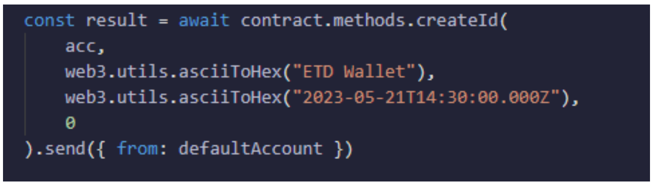
生成的did: `did:etd:<identity>`

```
             "identity":"0x82DfDfe6023283d49d5e8f4Cdd7Dda2b39b3F45a",
```

- 查询
  - 结果

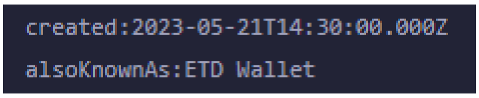
```
[
   {
      "address":"0xDca6E0B44C662c4Ed093732cC8F5b0c0075FC25E",
      "blockNumber":5414849,

 "transactionHash":"0xc42f49222c5a979a74819321994c2a3b702e981ae172454b2a
fdccd6d88e6b4a",
      "transactionIndex":0,

 "blockHash":"0xe06468d32b3a3de2eaab22b5af4785d2f94d43e4b5ce3056ded4de65
36108da8",
      "logIndex":0,
      "removed":false,
      "id":"log_8b63adc1",
      "returnValues":{
         "0":"0xDEa155F91B5d364746df7957ef4582fE70b280e8",

"1":"0x6372656174656400000000000000000000000000000000000000000000000000"
,
         "2":"0x323032332d30352d32315431343a33303a30302e3030305a",
         "3":"0",
         "4":"0",
         "identity":"0xDEa155F91B5d364746df7957ef4582fE70b280e8",

"name":"0x63726561746564000000000000000000000000000000000000000000000000
00",
         "value":"0x323032332d30352d32315431343a33303a30302e3030305a",
         "previousBlock":"0",
         "updated":"0"
      },
      "event":"AttributeChanged",

 "signature":"0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b8
2ac89e94",
      "raw":{

"data":"0x63726561746564000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000080000000
000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000018323032332d30352d32315431343a33
303a30302e3030305a0000000000000000",
         "topics":[

 "0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",

 "0x000000000000000000000000dea155f91b5d364746df7957ef4582fe70b280e8"
         ]
      }
   },
   {
      "address":"0xDca6E0B44C662c4Ed093732cC8F5b0c0075FC25E",
      "blockNumber":5414849,

 "transactionHash":"0xc42f49222c5a979a74819321994c2a3b702e981ae172454b2a
fdccd6d88e6b4a",
      "transactionIndex":0,

 "blockHash":"0xe06468d32b3a3de2eaab22b5af4785d2f94d43e4b5ce3056ded4de65
36108da8",
      "logIndex":1,
      "removed":false,
      "id":"log_2cc9243f",
      "returnValues":{
         "0":"0xDEa155F91B5d364746df7957ef4582fE70b280e8",
"1":"0x616c736f4b6e6f776e41730000000000000000000000000000000000000000000"
,
         "2":"0x4554442057616c6c6574",
         "3":"0",
         "4":"0",
         "identity":"0xDEa155F91B5d364746df7957ef4582fE70b280e8",

"name":"0x616c736f4b6e6f776e417300000000000000000000000000000000000000000
00",
         "value":"0x4554442057616c6c6574",
         "previousBlock":"0",
         "updated":"0"
      },
      "event":"AttributeChanged",

 "signature":"0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b8
2ac89e94",
      "raw":{

"data":"0x616c736f4b6e6f776e41730000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000080000000
000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000a4554442057616c6c65740000000000
0000000000000000000000000000000000",
         "topics":[

 "0x09c919e12d8a3fcab971cb5e94a1e3e4c3263cd6e84cc9246145e1b82ac89e94",

 "0x000000000000000000000000dea155f91b5d364746df7957ef4582fe70b280e8"
         ]
      }
   }
]
```

输入：



```
const result = await contract.methods.createId(
    acc,
    web3.utils.asciiToHex("ETD Wallet"),
    web3.utils.asciiToHex("2023-05-21T14:30:00.000Z"),
    0
).send({ from: defaultAccount })
```

解码输出：



```
created:2023-05-21T14:30:00.000Z
alsoKnownAs:ETD Wallet
```

github: https://github.com/uport-project/ethr-did