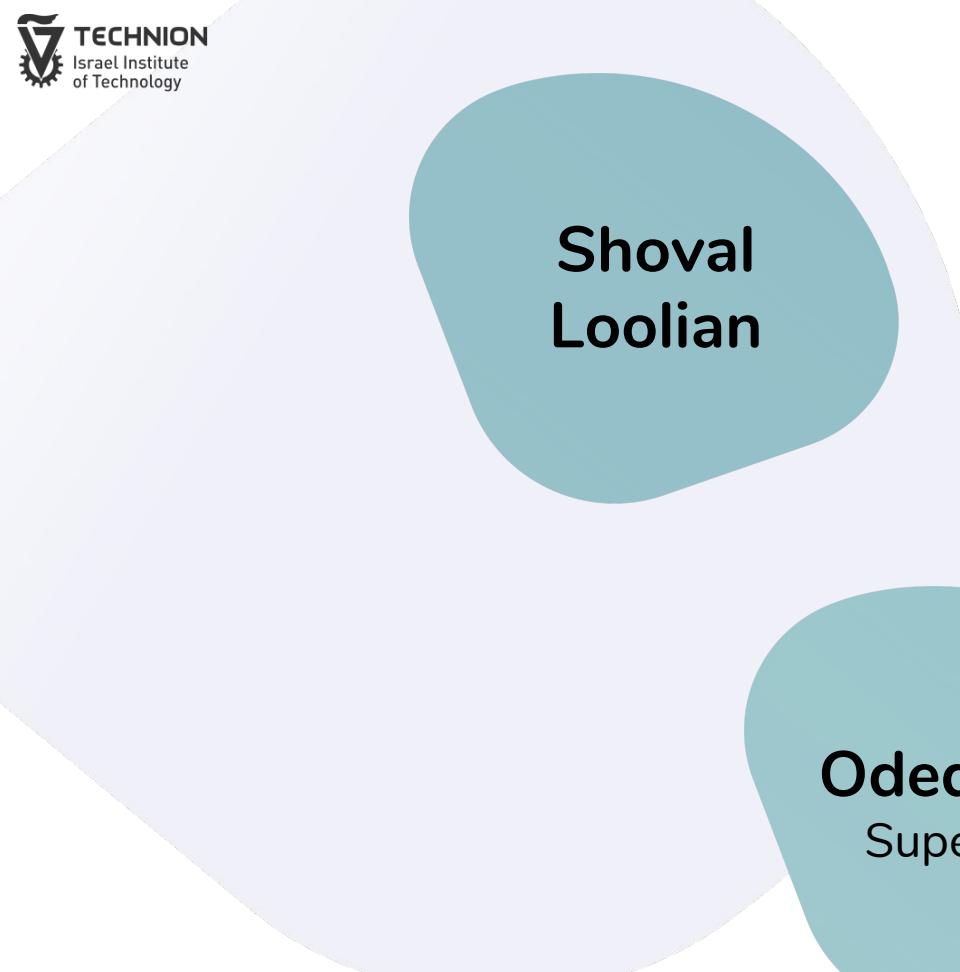


Smart Contracts for Cryptocurrencies





**Shoval
Loolian**



**David
Strouk**



Oded Naor
Supervisor

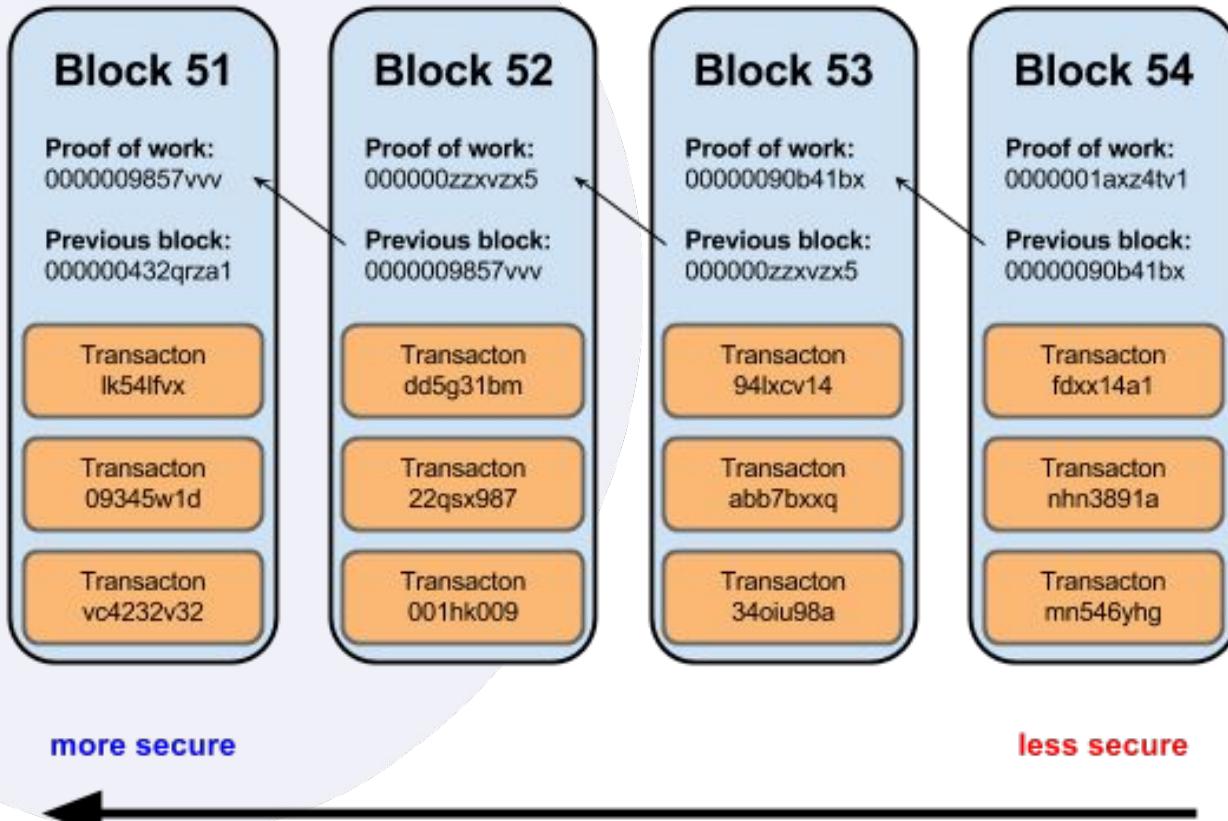


Background

Blockchain

- Growing general public ledger of cryptographically-signed transactions.
- Pseudo-anonymity: All transactions are public, but are not tied to anyone's real identity.
- Secured by collective compute power of miners.

Blockchain



Blocks are “more secure” as you go further back in the chain

Ethereum

- Decentralized platform that runs smart contracts
- Blockchain allows building any kind of application
- Ethereum wallet is characterized by :



Private Key - required to control your funds



Public Key - possible destination for payment (address)



Smart Contracts

The Problem

- Shared account between two or more people
- Allow transfer only when reached enough confirmations

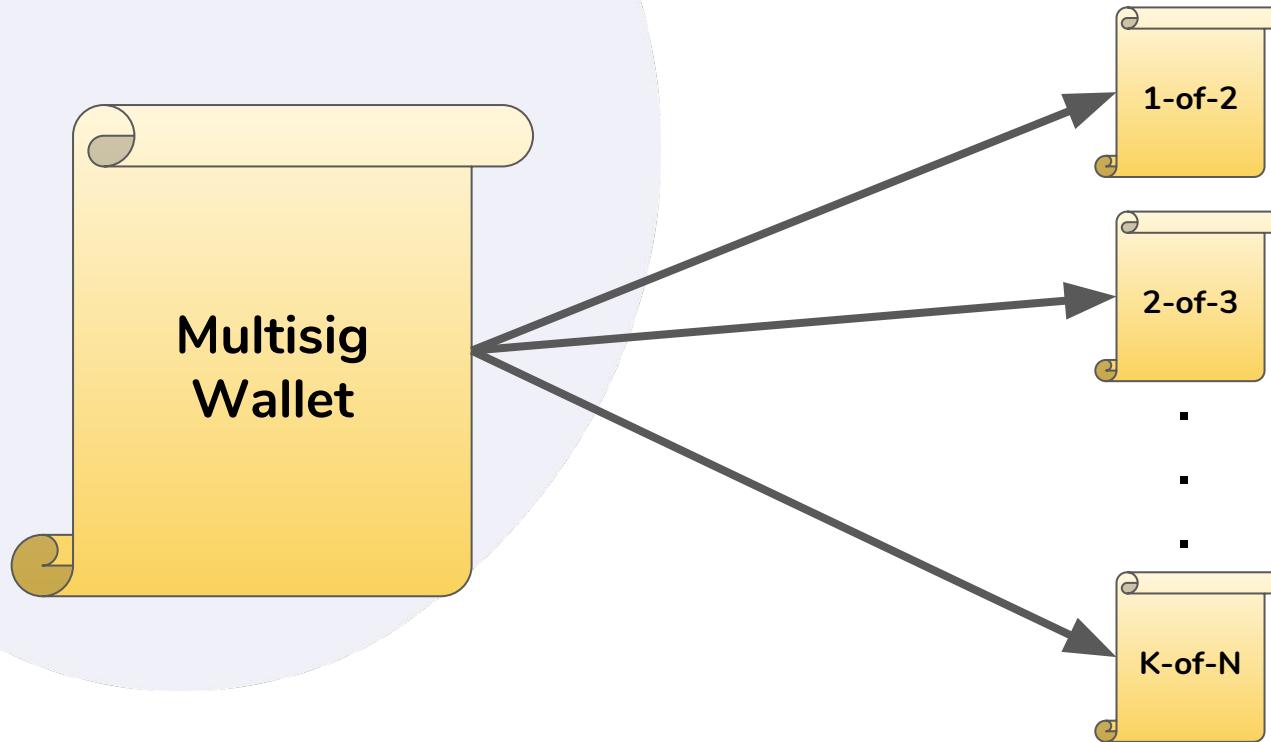


K-of-N Multisig

Description

- Define members list and required number of confirmations
- When requesting a transfer, wait for enough users to approve
- Remove inactive user

Implementation



Implementation

```
struct User {
    address wallet;
    bool inGroup;
    bool challenged;
    uint lastChallengeBlock;
}
```



Implementation

```
struct Transaction {
    address receiver;
    uint amountToTransfer;
    uint count;
    mapping (address => bool) usersApproves;
bool transferred;
}
```



Implementation

```
contract KofNMultisig {
    ...
    uint N;
    uint K;

    address[] usersWallets;
    mapping (address => User) usersInGroup;
    mapping (uint => Transaction) ledger;
    uint numberOfTransactions;
    Challenge challenge;
    ...
}
```

Implementation

- **constructor**(address[] wallets, uint k)
- () **payable** - fallback function

Implementation

- **requestPayment**(uint amount, address receiver)
- **approvePayment**(uint txId)

The Problem

- What if someone can't access his personal key?
- Funds will be inaccessible because there are not enough confirmations.
- We want to allow removal of inactive users.

The Solution

- Publish a challenge to the suspicious user.
- The user have a predefined period of time to respond the challenge.
- If he didn't send any response, then he will be removed from the group.

Implementation

```
struct Challenge {  
    bool isActive;  
    address sender;  
    address target;  
    uint startBlock;  
}
```



Implementation

```
struct User {  
    address wallet;  
    bool inGroup;  
    bool challenged;  
    uint lastChallengeBlock;  
}
```

```
contract KofNMultisig {  
    ...  
    uint N;  
    uint K;  
    ...  
    Challenge challenge;  
    ...  
}
```

Implementation

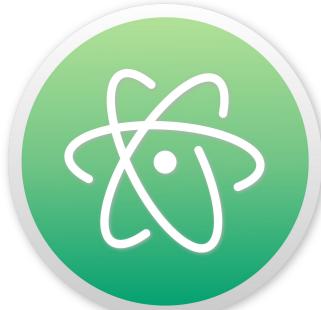
- **sendChallenge**(address target) payable
- **respondToChallenge()**
- **tryToRemoveChallengedUser()**

Misuse Prevention

- Flooding of challenges
- Member intentionally gone
- Subgroup attempts to cheat the rest of the group

Work Environment

1



```
Project KofNMultisig.sol — ~/Ethereum-K-of-N-Multisig/contracts

contracts
  KofNMultisig.sol
  Migrations.sol
  MultisigWallet.sol

KofNMultisig.sol
77  /**
78   *notice Sends a challenge to a member of the group to check whether its belonging to the group is still relevant. Along with calling this
79   *param target The wallet address of the challenged user
80   */
81 function sendChallenge(address target)
82 // Create a new challenge and challenge the user with the address target
83 payable
84 public
85 {
86     require(usersInGroup[msg.sender].inGroup == true,
87         "You dont belong to the group"); //same as: require(getUserIndexByAddress(target) != -1)
88     require(challenge.isActive == false,
89         "There is already a published challenge");
90     require(msg.value >= penalty,
91         "You dont have enough money to pay the penalty");
92     require(usersInGroup[target].inGroup == true,
93         "Your target doesnt belong to the group"); //same as: require(getUserIndexByAddress(target) != -1)
94     require(usersInGroup[msg.sender].lastChallengeBlock == 0
95     || block.number - usersInGroup[msg.sender].lastChallengeBlock >= BLOCKS_TO_BLOCK,
96         "You are blocked from sending a challenge. Please wait");
97
98     challenge = Challenge(true, msg.sender, target, block.number);
99     usersInGroup[msg.sender].lastChallengeBlock = block.number;
100    usersInGroup[target].challenged = true;
101
102    emit ChallengeSent(target);
103 }
104
105 /**
106  *notice Respond to the published challenge. Collect from shared wallet an amount of penalty
107 */
108 function respondToChallenge()
109 // Check if the function caller is the challenger's target, answer the challenge if yes
110 // and take a fee from the contract wallet
111 public
112 {
113     require(usersInGroup[msg.sender].inGroup == true,
114         "You dont belong to the group");
115     require(challenge.isActive == true,
```

Work Environment

Ganache

ACCOUNTS BLOCKS TRANSACTIONS LOGS UPDATE AVAILABLE SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK 0 GAS PRICE 2000000000 GAS LIMIT 66600000 NETWORK ID 5777 RPC SERVER HTTP://127.0.0.1:7545 MINING STATUS AUTOMINING

| MNEMONIC | HD PATH | | |
|---|------------------------------|------------|---------|
| fantasy crowd column taste milk farm captain bullet front away syrup nest | m/44'/60'/0'/0/account_index | | |
| ADDRESS 0x043e0af8a0aBe779b18c8E40d301aF590b3ecD90 | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 0 |
| ADDRESS 0x11D1aC7078b44fFd61693806c7B6f91984e250C0 | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 1 |
| ADDRESS 0xFBdBA624E3E197061487dB7A53a23653E1449F19 | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 2 |
| ADDRESS 0x8542769FD138866c8BE998Ae1bd5a02E2f65e0aB | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 3 |
| ADDRESS 0xdCC85865826f35F7c8568EC4E69fe05b67Be05af | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 4 |
| ADDRESS 0x3C065B95d0FB87dE51f8d01931ec2Ee8164770c9 | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 5 |
| ADDRESS 0xcda247BcB2ddD0241d53955d8f2fe583aC64CD30 | BALANCE 1000.00 ETH | TX COUNT 0 | INDEX 6 |

2



3

Work Environment

```
2. bash
Last login: Tue Feb 19 21:31:50 on ttys000
MacBook-Pro-4a09:~ davidstrouk$ cd Ethereum-K-of-N-Multisig/
MacBook-Pro-4a09:Ethereum-K-of-N-Multisig davidstrouk$ truffle test
Compiling ./contracts/KofNMultisig.sol...
Compiling ./contracts/Migrations.sol...
Compiling ./contracts/MultisigWallet.sol...

Contract: Test K-of-N
✓ General Test K = N
✓ General Test K < N

Contract: Test K-of-N Functions
✓ testConstructor
✓ testSendChallenge
✓ testTryToRemoveChallengedUser
✓ testRespondToChallenge
✓ testRequestPayment
✓ testApprovePayment

8 passing (90ms)

MacBook-Pro-4a09:Ethereum-K-of-N-Multisig davidstrouk$
```



4

Work Environment

Remix - Solidity IDE

MetaMask Notification

Rinkeby Test Network

user 2

New Contract

CONTRACT DEPLOYMENT

\$0.00

+\$0

DETAILS DATA

GAS FEE \$0.39

+\$0.002632

AMOUNT + GAS FEE \$0.39

+\$0.002632

REJECT CONFIRM

creation of KofNMultisig pending...

```
// Version of solidity compiler this program was written for
pragma solidity ^0.4.24;

//----- KofNMultisig Contract -----
/** 
 * @author Shoval Loolian, David Strouk
 * @notice Shared wallet of N people which requests the approval of K members for making a payment
 */
contract KofNMultisig {
    // Constants
    uint constant BLOCKS_TO_RESPOND = 20;
    uint constant BLOCKS_TO_BLOCK = 50;
    address constant penaltyWallet = 0x56C509F889a886950a77d0E4D8a252D2a805A74d; // TBD
    uint constant penalty = 0.1 ether; // should be total amount/K

    event ChallengeSent(address target);
    event ChallengeResponded();
    event UserRemoved(address removedUser, uint K, uint N);
    event UserNotRemoved(address not_removedUser);
    event PaymentRequested(uint amount_to_transfer, address receiver, uint txId);
    event PaymentApproved(uint txId);
    event PaymentTransferred(uint txId);
    event PaymentAlreadyApproved(uint txId);
    event PaymentAlreadyTransferred(uint txId);
    event InsufficientBalance(uint minimum_balance);
}

//----- Events -----
```

[2] only remix transactions, script

Search transactions

Running JavaScript Scripts. The following libraries are accessible:

- web3 version 1.0.0
- ethers.js
- swarmy
- compilers - contains currently loaded compiler

Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script.

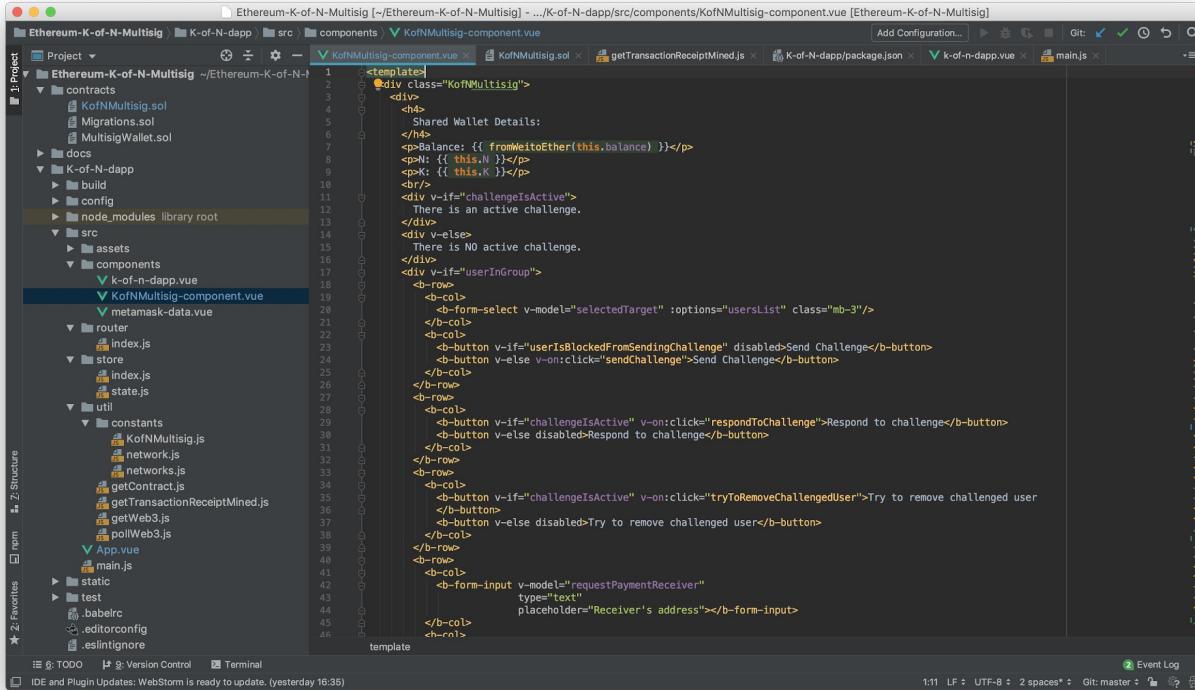
Use exports/.register(key, obj)/.remove(key)/.clear() to register and reuse object across a script executions.

remix



5

Work Environment

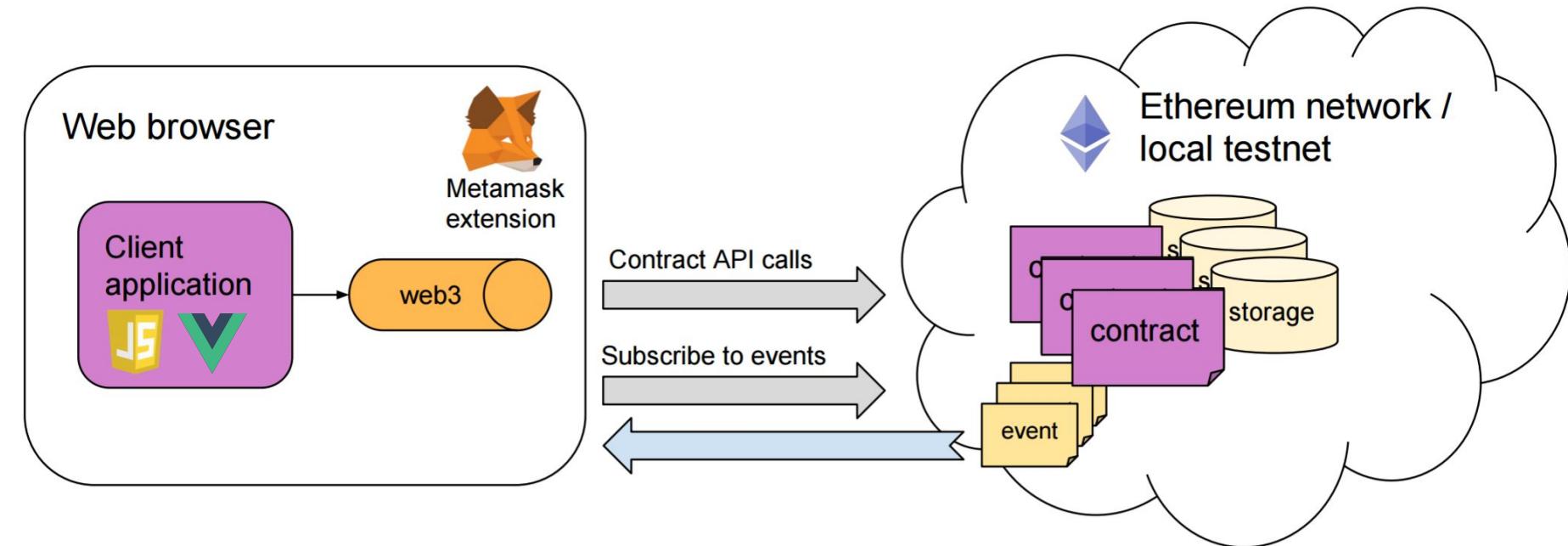


The screenshot shows a code editor in an IDE (WebStorm) displaying a Vue.js component template. The component is named `KofNMultisig-component.vue`. The template contains HTML and CSS-like directives. It includes sections for wallet details, challenge status, user group, and various buttons for interacting with the challenge state. The code editor has a dark theme with syntax highlighting for HTML, CSS, and JavaScript.

```
<template>
  <div class="KofNMultisig">
    <div>
      <h4> Shared Wallet Details:</h4>
      <p>Balance: {{ fromWeiToEther(this.balance) }}</p>
      <p>{{ this.N }}</p>
      <p>{{ this.K }}</p>
    </div>
    <div v-if="challengeIsActive">
      There is an active challenge.
    </div>
    <div v-else>
      There is NO active challenge.
    </div>
    <div v-if="userInGroup">
      <b-row>
        <b-col>
          <b-form-select v-model="selectedTarget" :options="usersList" class="mb-3"/>
        </b-col>
        <b-col>
          <b-button v-if="userIsBlockedFromSendingChallenge" disabled>Send Challenge</b-button>
          <b-button v-else v-on:click="sendChallenge">Send Challenge</b-button>
        </b-col>
      </b-row>
      <b-row>
        <b-col>
          <b-button v-if="challengeIsActive" v-on:click="respondToChallenge">Respond to challenge</b-button>
          <b-button v-else disabled>Respond to challenge</b-button>
        </b-col>
      </b-row>
      <b-row>
        <b-col>
          <b-button v-if="challengeIsActive" v-on:click="tryToRemoveChallengedUser">Try to remove challenged user</b-button>
          <b-button v-else disabled>Try to remove challenged user</b-button>
        </b-col>
      </b-row>
      <b-row>
        <b-col>
          <b-form-input v-model="requestPaymentReceiver" type="text" placeholder="Receiver's address"/>
        </b-col>
      </b-row>
    </div>
  </div>
</template>
```



Front and Back Ends



Live Demo



● ○ ● k-of-n-dapp × +

localhost:8080/#/ +999

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x15c32df885ffba4e0ae42e7e1928c52be3f8d19b

Balance: 17.548136875 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1.2 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

[There is no active challenge right now.](#)

[Sending a challenge is possible.](#)

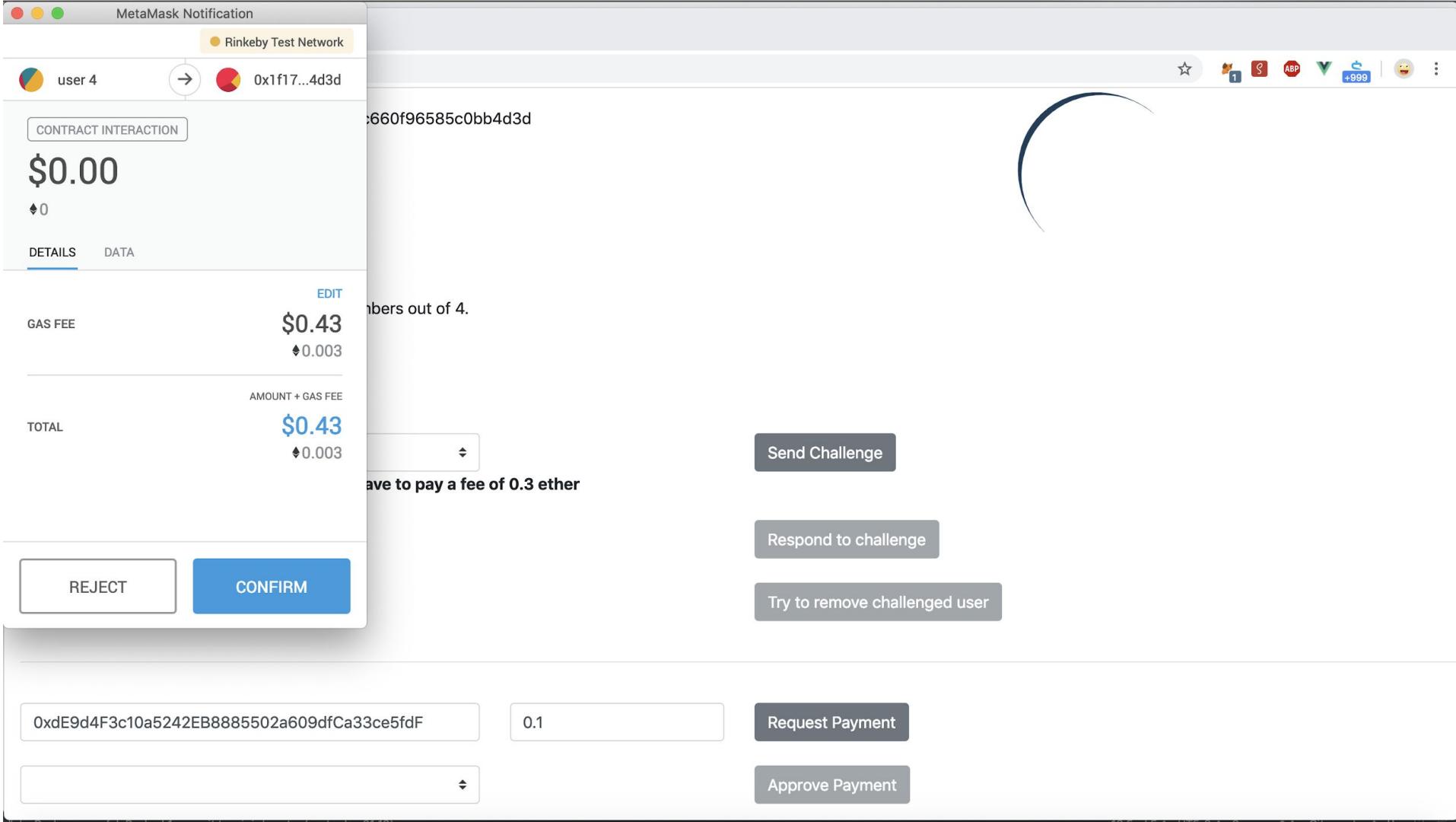
Please select a user

[Send Challenge](#)

[Notice: when sending a challenge, you will have to pay a fee of 0.3 ether](#)

[Respond to challenge](#)

[Try to remove challenged user](#)



k-of-n-dapp

localhost:8080/#/

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

0xdE9d4F3c10a5242EB8885502a609dfCa33ce5fdF

0.1

Request Payment

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |

Payment Requested
Payment to
0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf of amount 0.1 has been requested. Transaction id: 1

Payment Approved
Transaction number 1 has been approved.

k-of-n-dapp

localhost:8080/#/

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

0xdE9d4F3c10a5242EB8885502a609dfCa33ce5fdF

0.4

Request Payment

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

0xde9d4F3c10a5242EB8885502a609dfCa33ce5fdf

0.4

Request Payment

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |
| 2 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.4 | 1 | X | X | X | V |

MetaMask Notification

Rinkeby Test Network

user 4 → 0x1f17...4d3d

CONTRACT INTERACTION

\$0.00

♦ 0

members out of 4.

DETAILS DATA

GAS FEE \$0.43 ♦ 0.003

AMOUNT + GAS FEE \$0.43 ♦ 0.003

TOTAL \$0.43 ♦ 0.003

EDIT

Send Challenge

Save to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

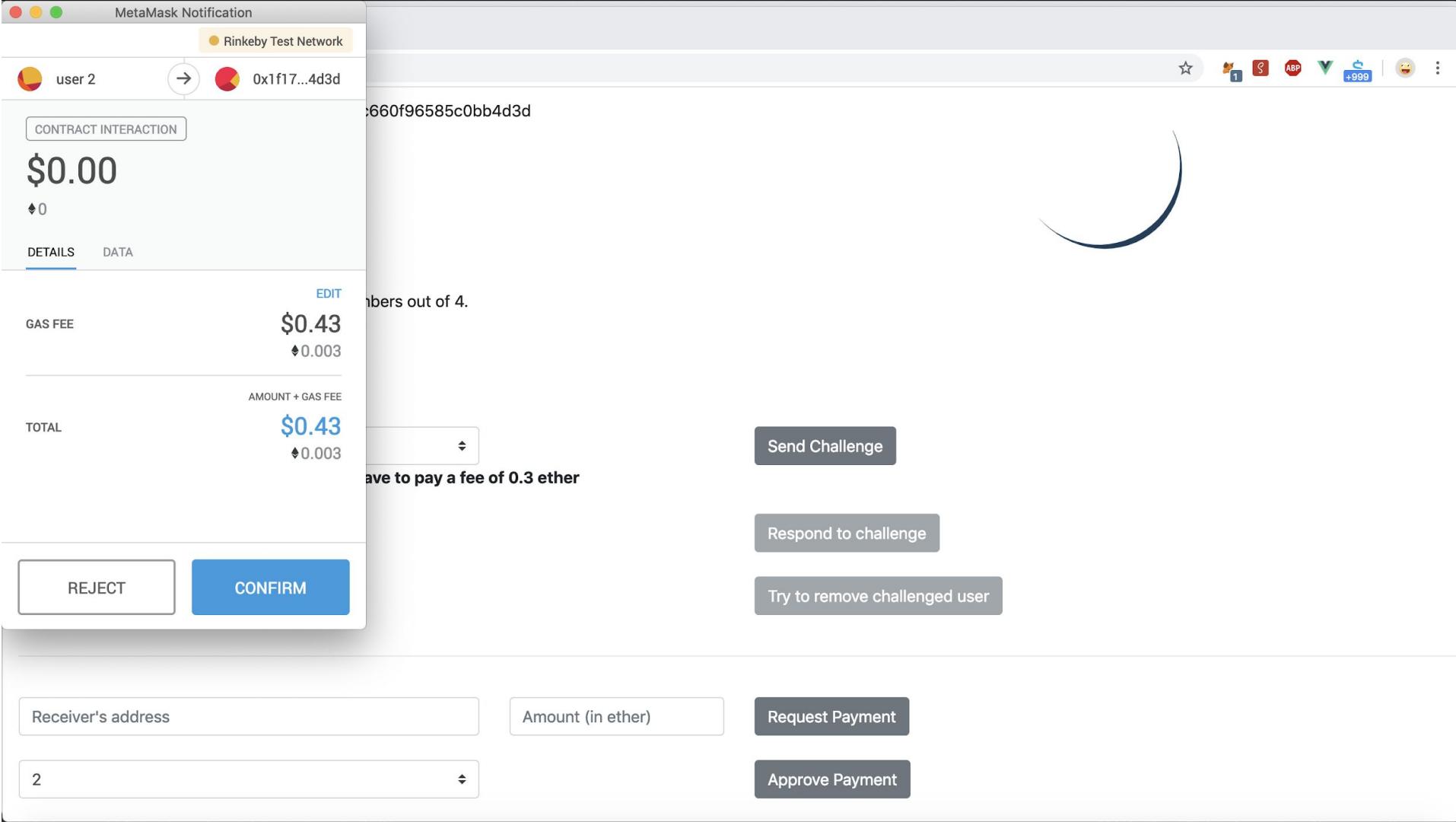
REJECT CONFIRM

0xdE9d4F3c10a5242EB8885502a609dfCa33ce5fdF

0.4 Request Payment

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|---------|--------|-------|--------|--------|--------|--------|
| | | | | | | | |



k-of-n-dapp

localhost:8080/#/

To make a transfer, you need approval of 3 members out of 4.

Payment Approved
Transaction number 2 has been approved.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

Receiver's address

Amount (in ether)

Request Payment

2

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |
| 2 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.4 | 2 | X | V | X | V |

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

Receiver's address

Amount (in ether)

Request Payment

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |
| 2 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.4 | 3 | X | V | V | V |

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x718442a4ecd753c251a2c64cd8141f6b2cf72555

Balance: 5.645356145000001 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 0.8 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x15c32df885ffba4e0ae42e7e1928c52be3f8d19b

Balance: 17.547890419 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 0.8 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

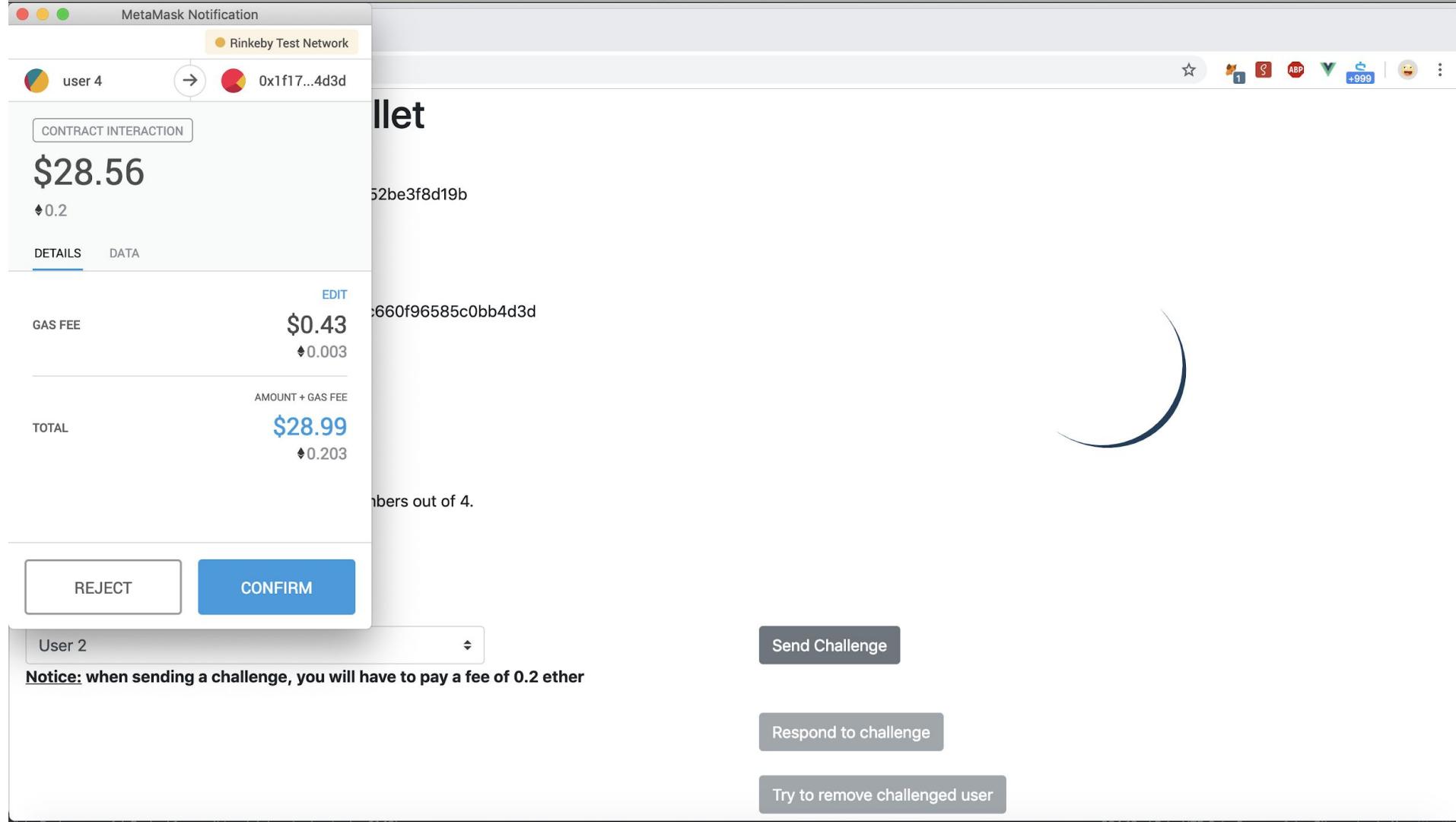
User 2

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user



k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x15c32df885ffba4e0ae42e7e1928c52be3f8d19b

Balance: 17.34777772 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 0.8 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is an active challenge right now.

Please wait until it has been answered or time has passed for sending a new one.

Remaining blocks for response : 10

User 2

Send Challenge

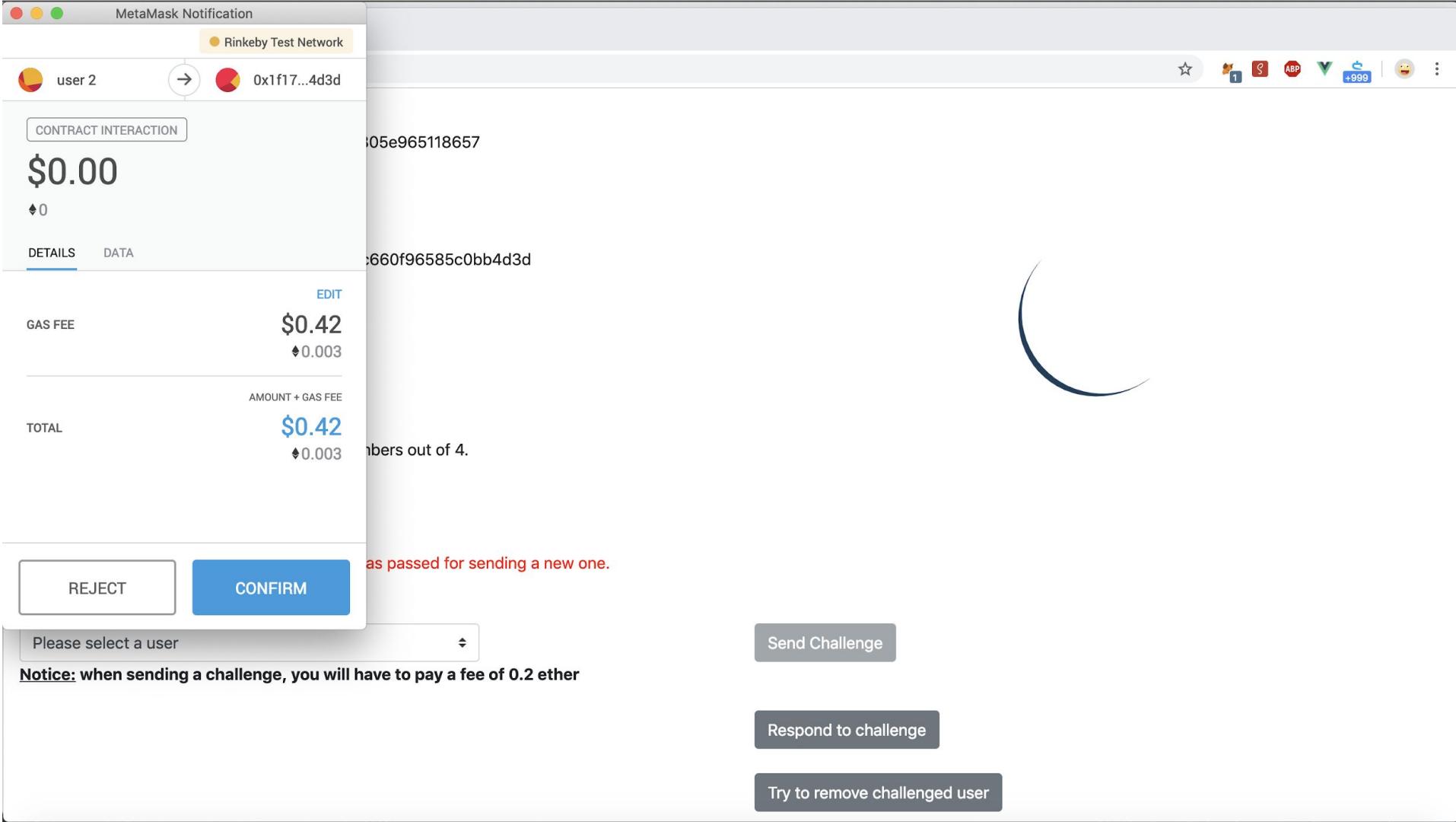
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user

Challenge Sent
Challenge has been sent to target
0x7a16b9667268629a2ea9c838077805e965118

+999



 k-of-n-dapp

localhost:8080/#/

User Wallet Details:

Account: 0x7a16b9667268629a2ea9c838077805e965118657

Balance: 12.13076151399999 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user

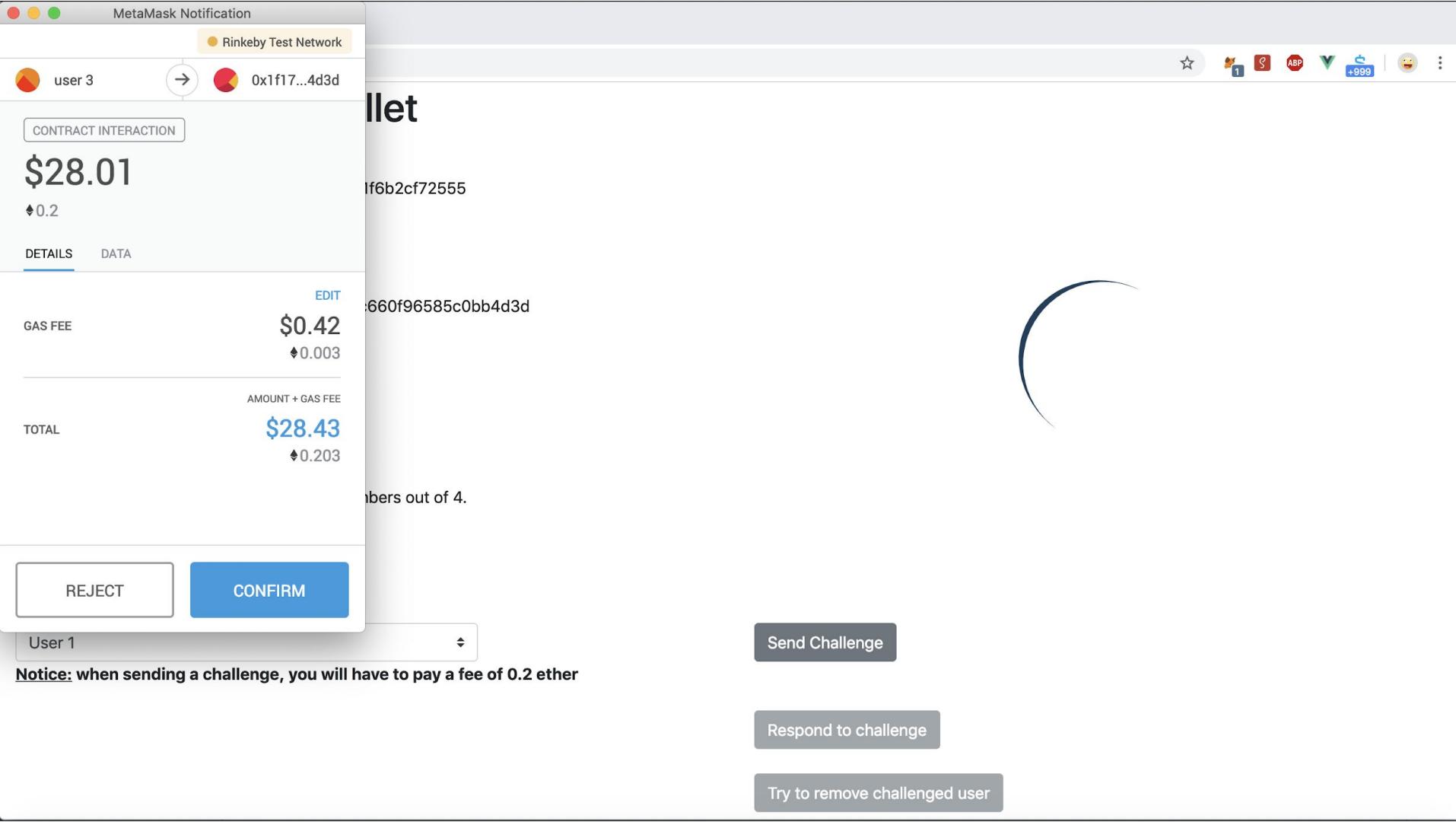
Receiver's address

Amount (in ether)

Request Payment

Challenge Responded
Challenge has been responded

ABP +999



k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x718442a4ecd753c251a2c64cd8141f6b2cf72555

Balance: 5.445288446 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 0.8 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is an active challenge right now.

Please wait until it has been answered or time has passed for sending a new one.

Remaining blocks for response : 10

User 1

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user

Challenge Sent
Challenge has been sent to target
0xde9d4f3c10a5242eb8885502a609dfca33ce5

+999

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x718442a4ecd753c251a2c64cd8141f6b2cf72555

Balance: 5.445288446 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 0.8 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is an active challenge right now.

Please wait until it has been answered or time has passed for sending a new one.

Remaining blocks for response : 1

User 1

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x718442a4ecd753c251a2c64cd8141f6b2cf72555

Balance: 5.445288446 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 0.8 ether

Members in the group: 4

To make a transfer, you need approval of 3 members out of 4.

There is an active challenge right now.
Challenged user has not responded to challenge.
You can now remove him from group by pressing "Try To Remove Challenged User" button.

User 1

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.2 ether

Respond to challenge

Try to remove challenged user

MetaMask Notification

Rinkeby Test Network

user 3 → 0x1f17...4d3d

CONTRACT INTERACTION

\$0.00

♦ 0

DETAILS DATA

GAS FEE \$0.42 ♦ 0.003

AMOUNT + GAS FEE

TOTAL \$0.42 ♦ 0.003

EDIT

Members out of 4.

Try To Remove Challenged User

Send Challenge

Save to pay a fee of 0.2 ether

REJECT CONFIRM

Try to remove challenged user

Respond to challenge

Receiver's address

Amount (in ether)

Request Payment

ETH sol Go Eth Git Inb Fac Sh Sm Tw Cry Rin remux Rin Fac Rin +999

localhost:8080/#/

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1 ether

Members in the group: 3

To make a transfer, you need approval of 3 members out of 3.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3333333333333333 ether

Respond to challenge

Try to remove challenged user

Receiver's address

Amount (in ether)

Request Payment

Approve Payment

User Removed
User
0xde9d4f3c10a5242eb8885502a609dfca33ce5
has been removed from group. N = 3, K = 3

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf

Balance: 4.892501201136729 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1 ether

Members in the group: 3

You don't belong to the group



user 3



0x1f17...4d3d



CONTRACT INTERACTION

\$0.00

♦0

DETAILS DATA

GAS FEE

\$0.42

♦0.003

AMOUNT + GAS FEE

\$0.42

♦0.003

TOTAL

members out of 3.

EDIT

Send Challenge

Respond to challenge

Try to remove challenged user

REJECT

CONFIRM

0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf

2

Request Payment

Approve Payment

ID Address

Amount

Count

User 1

User 2

User 3

User 4

k-of-n-dapp

localhost:8080/#/

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Notice: when sending a challenge, you will have to pay a fee of 0.3333333333333333 ether

0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf 0.2

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |
| 2 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.4 | 3 | X | V | V | V |
| 3 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 2 | 1 | X | X | V | X |
| 4 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.2 | 1 | X | V | X | X |

Payment Approved
Transaction number 4 has been approved.

Payment Requested
Payment to
0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf
of amount 0.2 has been requested.
Transaction id: 4

k-of-n-dapp

localhost:8080/#/

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3333333333333333 ether

Respond to challenge

Try to remove challenged user

Receiver's address

Amount (in ether)

Request Payment

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |
| 2 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.4 | 3 | X | V | V | V |
| 3 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 2 | 1 | X | X | V | X |
| 4 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.2 | 2 | X | V | X | V |

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x718442a4ecd753c251a2c64cd8141f6b2cf72555

Balance: 5.445134418 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1 ether

Members in the group: 3

To make a transfer, you need approval of 3 members out of 3.

There is no active challenge right now.
Sending a challenge is possible.

User 2

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3333333333333333 ether

Respond to challenge

Try to remove challenged user

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x7a16b9667268629a2ea9c838077805e965118657

Balance: 11.797210527666657 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1 ether

Members in the group: 3

To make a transfer, you need approval of 3 members out of 3.

There is an active challenge right now.

Please wait until it has been answered or time has passed for sending a new one.

Remaining blocks for response : 10

User 3

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.3333333333333333 ether

Respond to challenge

Try to remove challenged user

k-of-n-dapp

localhost:8080/#/

K-of-N-Multisig Wallet

User Wallet Details:

Account: 0x7a16b9667268629a2ea9c838077805e965118657

Balance: 11.797166987666657 ether

Shared Wallet Details:

Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d

Balance: 1.3333433333333332 ether

Members in the group: 2

To make a transfer, you need approval of 2 members out of 2.

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.6666716666666666 ether

Respond to challenge

Try to remove challenged user

User Removed
User
0x718442a4ecd753c251a2c64cd8141f6b2cf725
has been removed from group. N = 2, K = 2

k-of-n-dapp

localhost:8080/#/

There is no active challenge right now.
Sending a challenge is possible.

Please select a user

Send Challenge

Notice: when sending a challenge, you will have to pay a fee of 0.6666716666666666 ether

Respond to challenge

Try to remove challenged user

Receiver's address

Amount (in ether)

Request Payment

1

Approve Payment

| ID | Address | Amount | Count | User 1 | User 2 | User 3 | User 4 |
|----|--|--------|-------|--------|--------|--------|--------|
| 1 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.1 | 1 | X | X | X | V |
| 2 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.4 | 3 | X | V | V | V |
| 3 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 2 | 1 | X | X | V | X |
| 4 | 0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf | 0.2 | 2 | X | V | X | V |

Conclusion

1. Get familiar with concepts of blockchain, Bitcoin, Ethereum, smart contracts, ...
2. Install a work environment for building and running smart contracts on Ethereum blockchain.
3. Learn how to write in Solidity
4. Designing and programming the code of our smart contract.
5. Search and solve misuses and issues in our code.
6. Run our contract on a Test Network.
7. Build a web dApp for user interface

Questions



