TECHNION
Israel Institute of Technology

ANDREW AND ERNA VITERBI
FACULTY OF ELECTRICAL ENGINEERING

Smart Contracts for Cryptocurrencies

February, 26 2019

TECHNION
Israel Institute
of Technology

ANDREW AND ERNA VITERBI
FACULTY OF
ELECTRICAL
ENGINEERING

Shoval Loolian

David Strouk

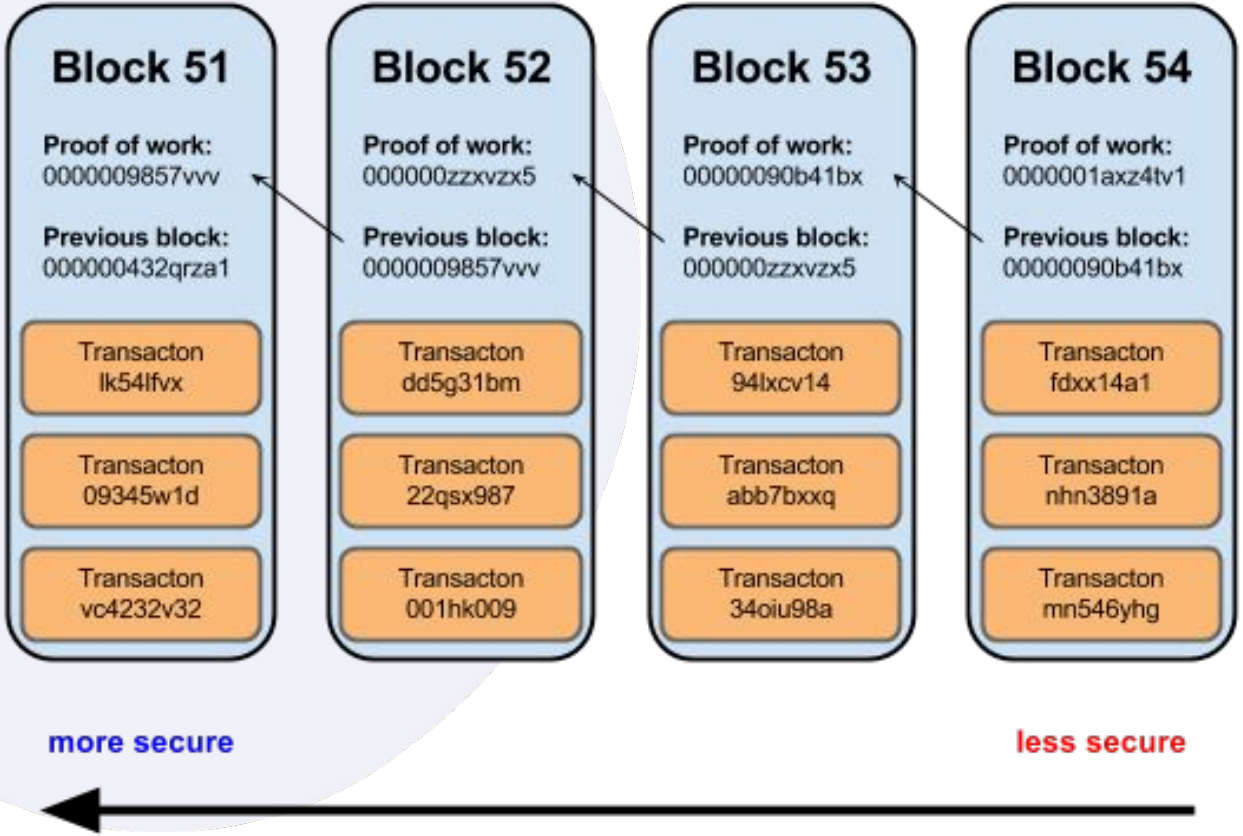
Oded Naor
Supervisor


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

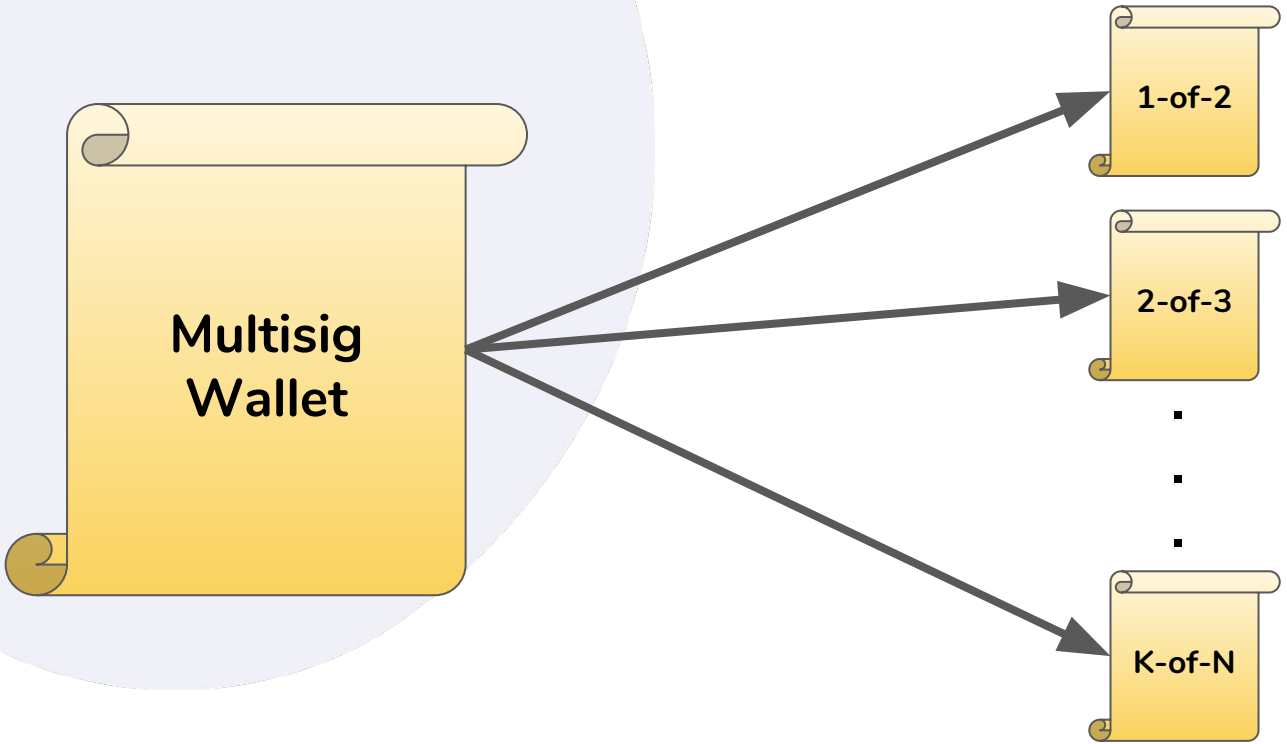
- Shared account between two or more people
- Allow transfer only when reached enough confirmations


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

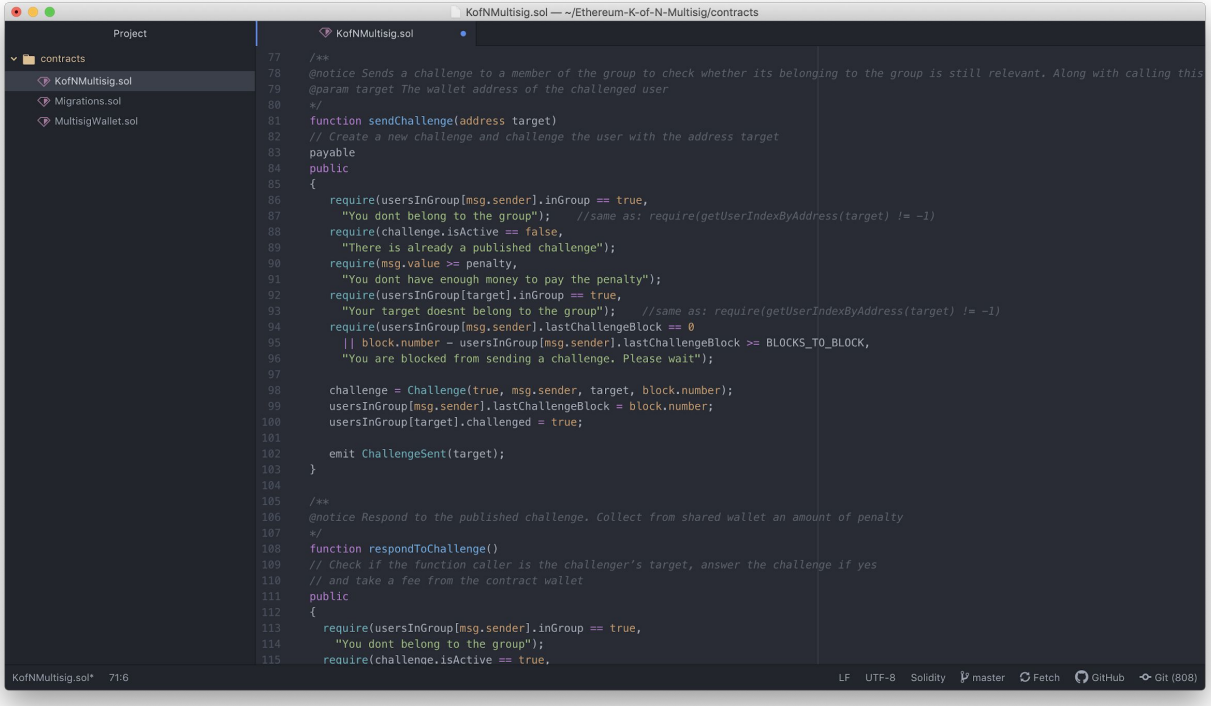
- **sendChallenge**(address target) payable
- **respondToChallenge**()
- **tryToRemoveChallengedUser**()

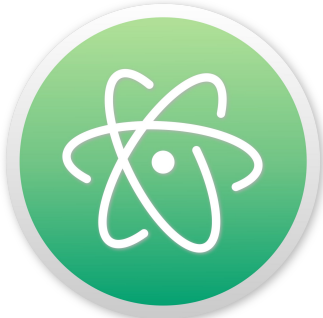
Misuse Prevention

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

Work Environment

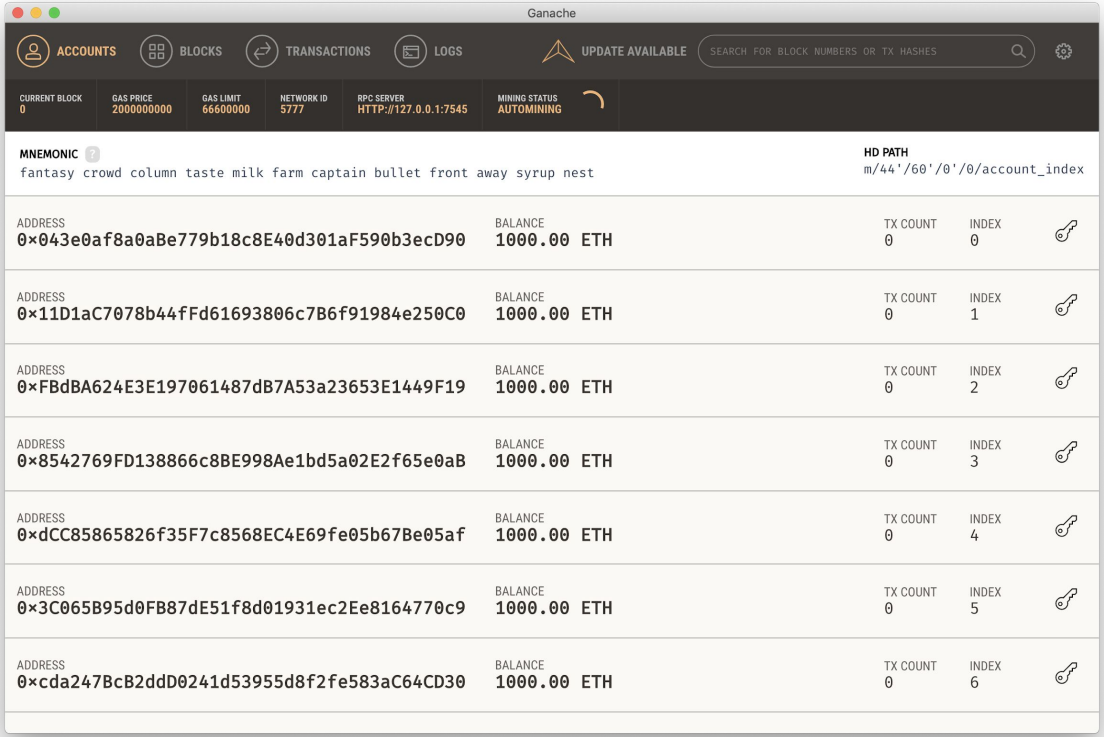
1





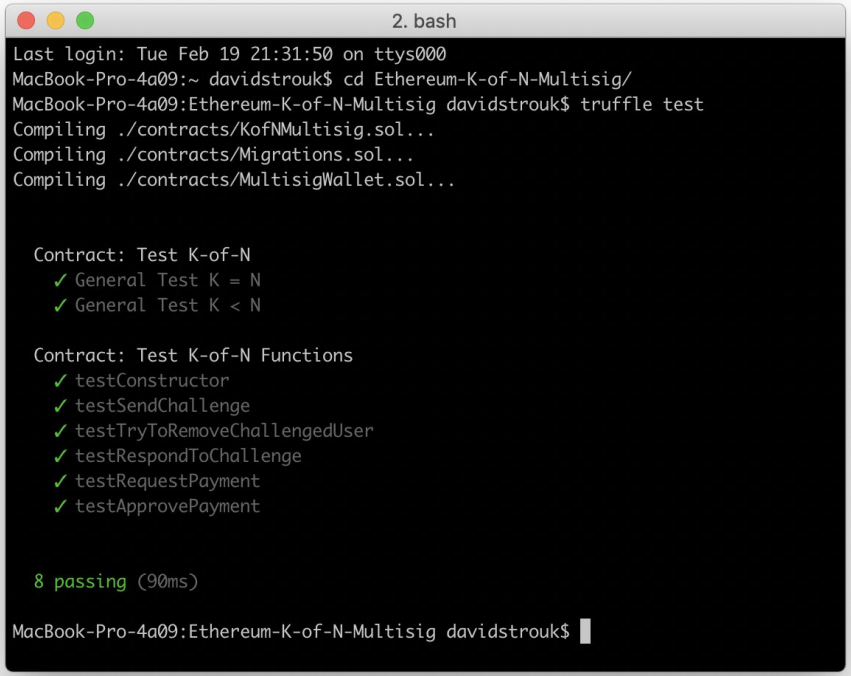
Work Environment

2



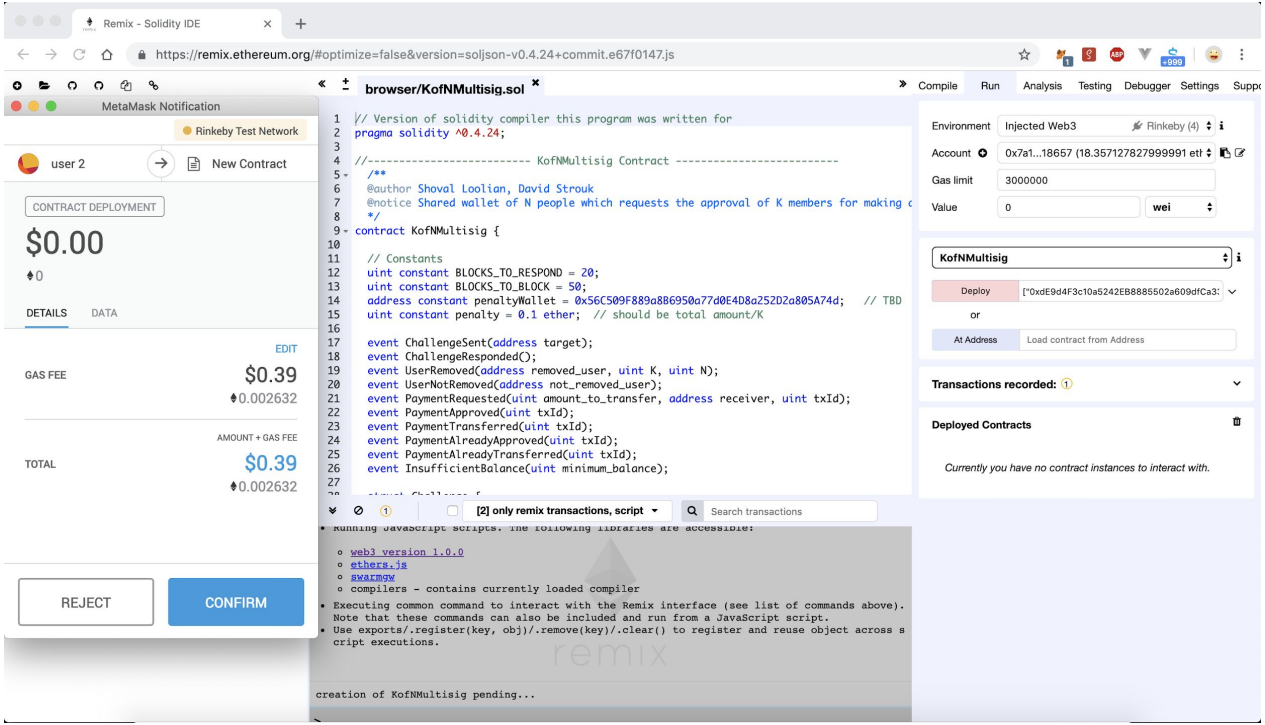
Work Environment

3



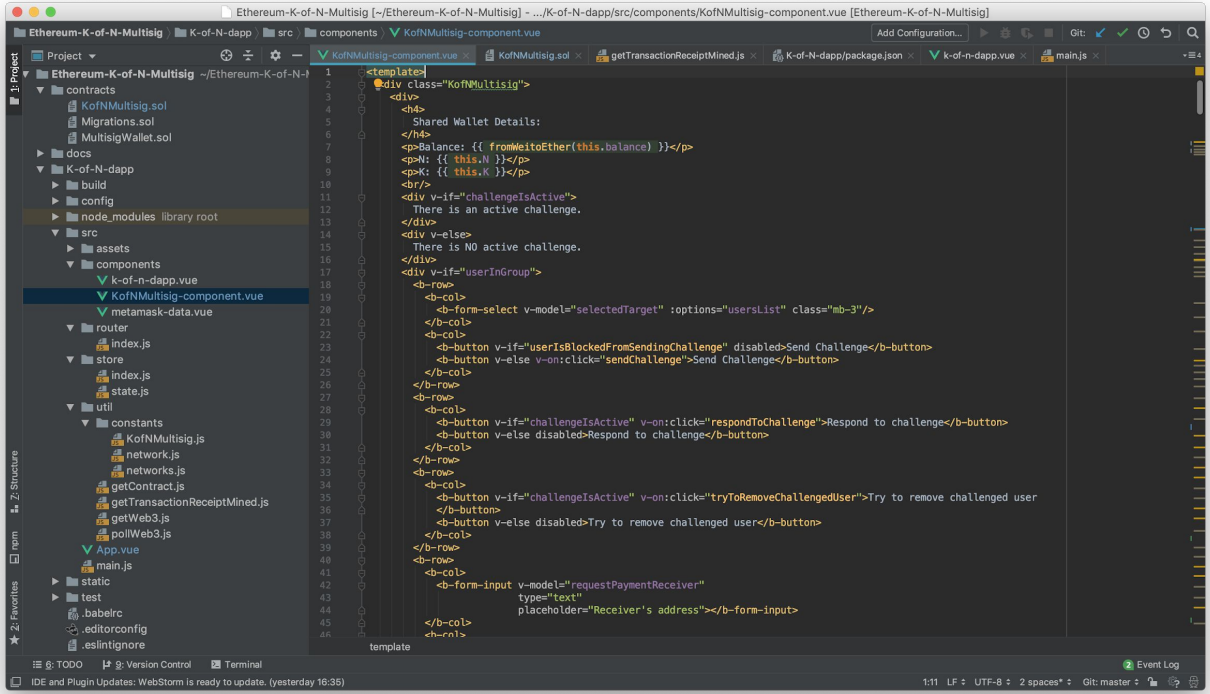
Work Environment

4

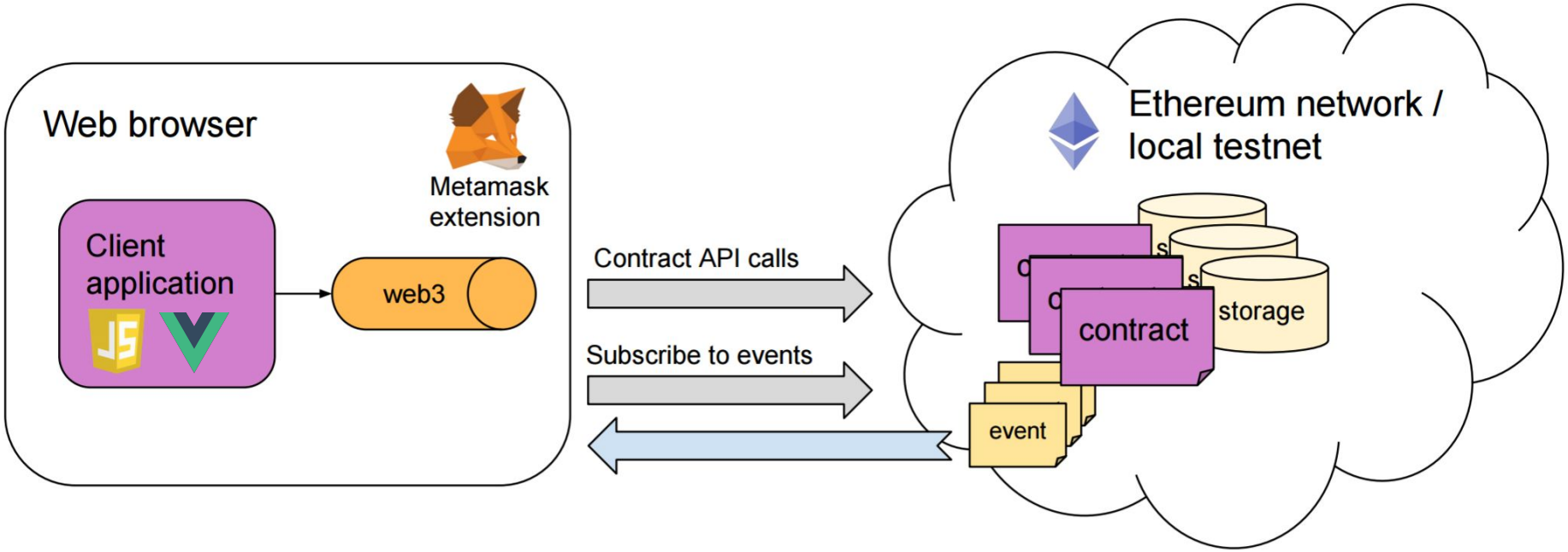


Work Environment

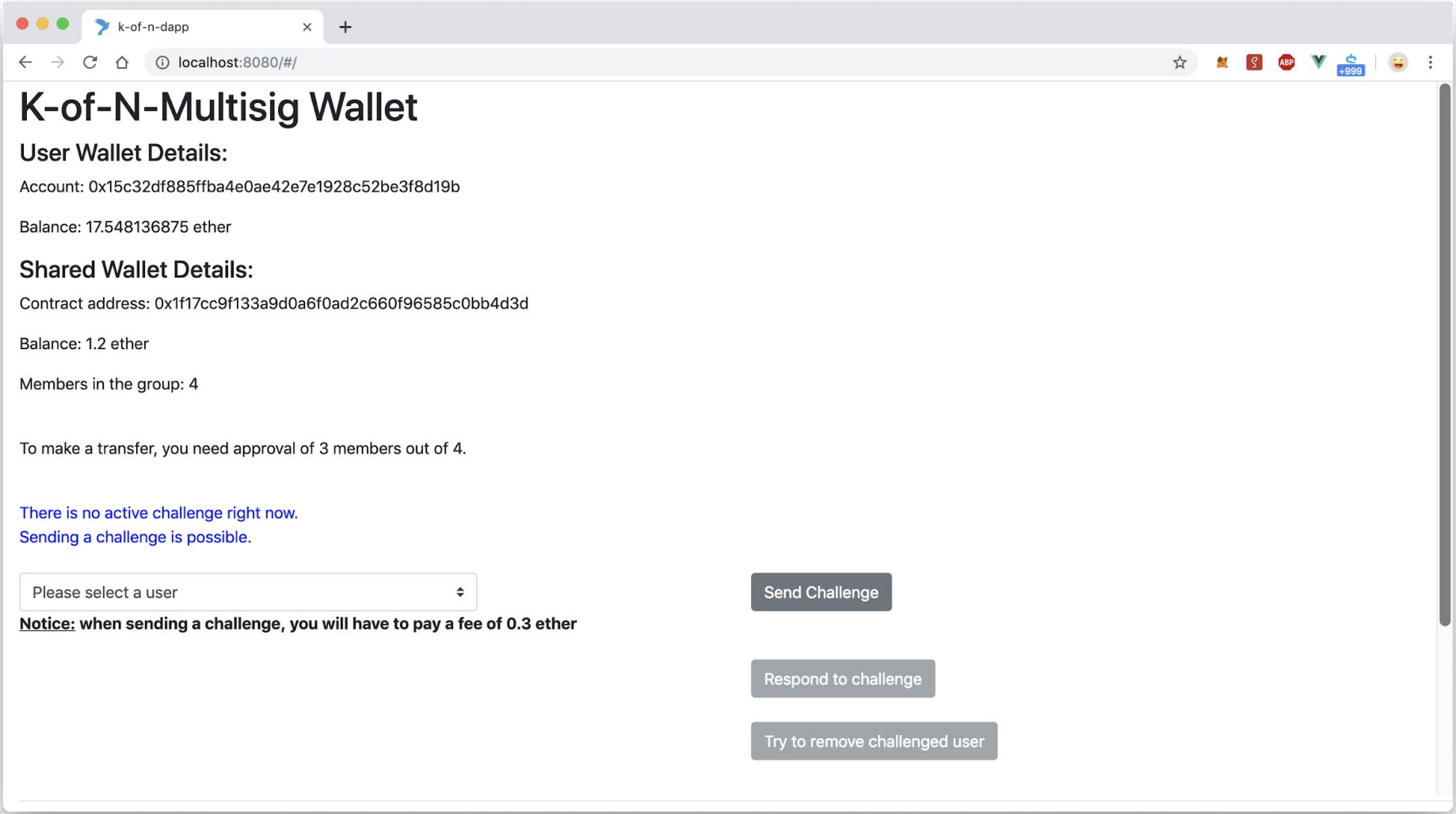
5

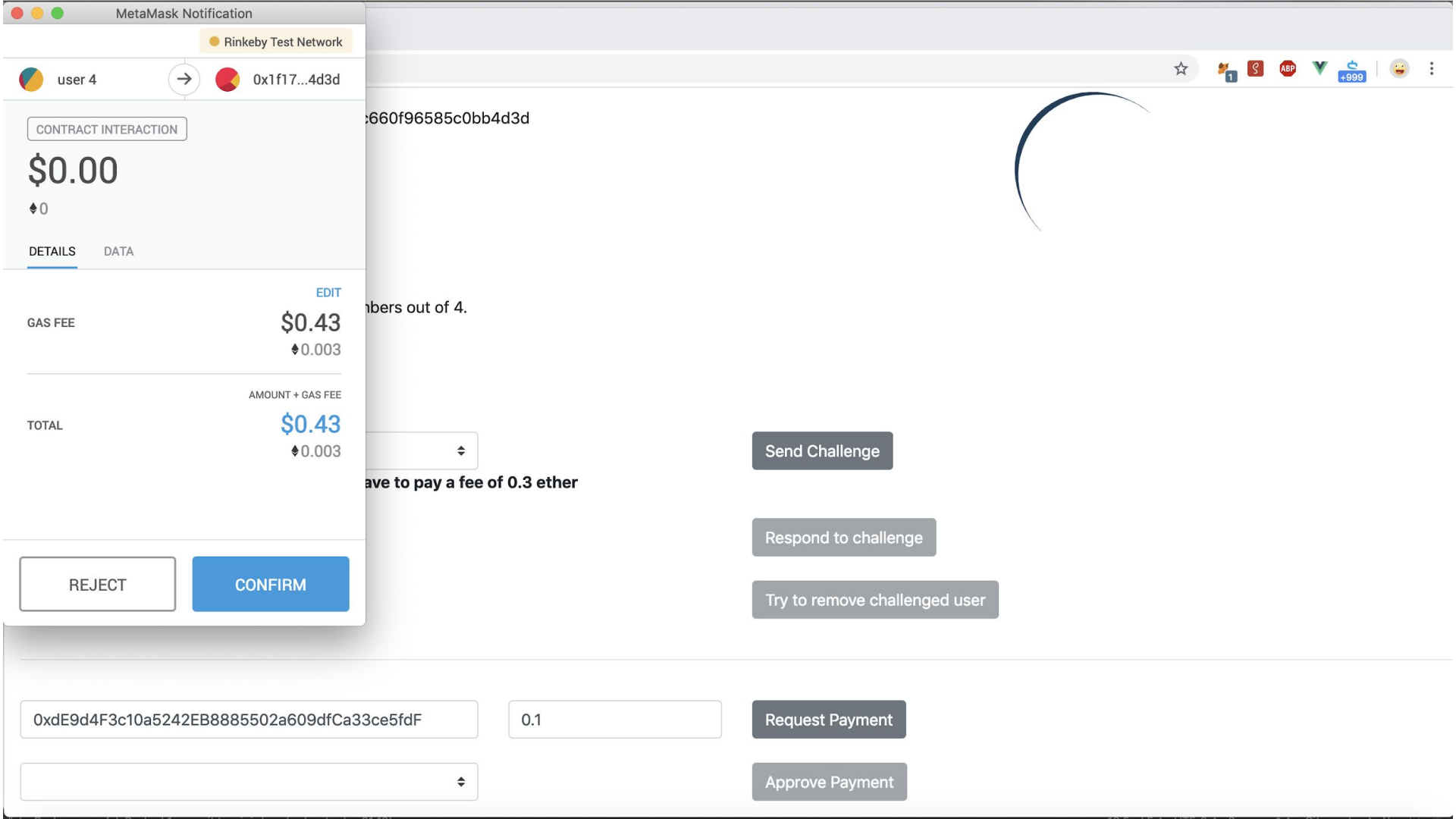


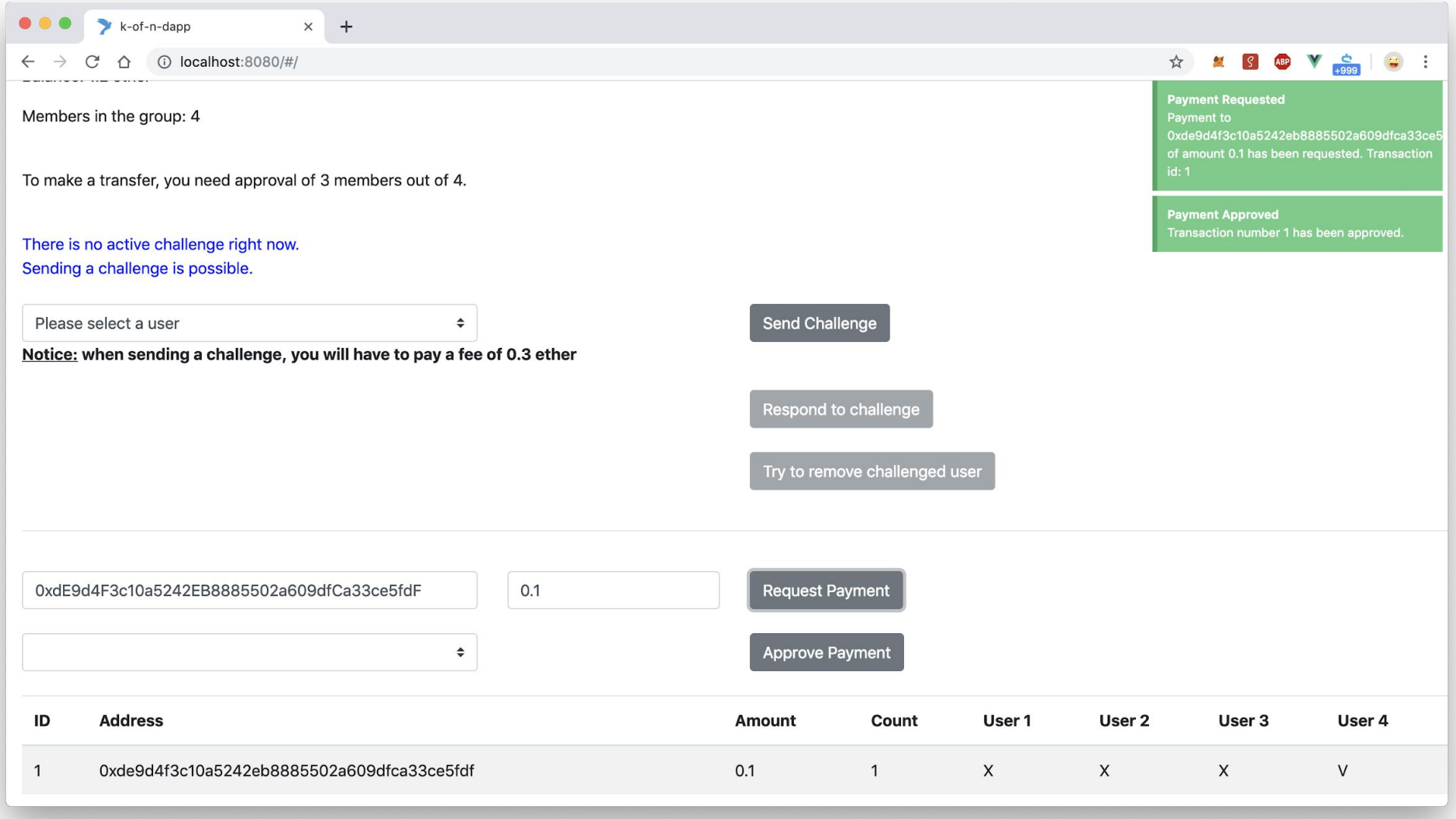
Front and Back Ends

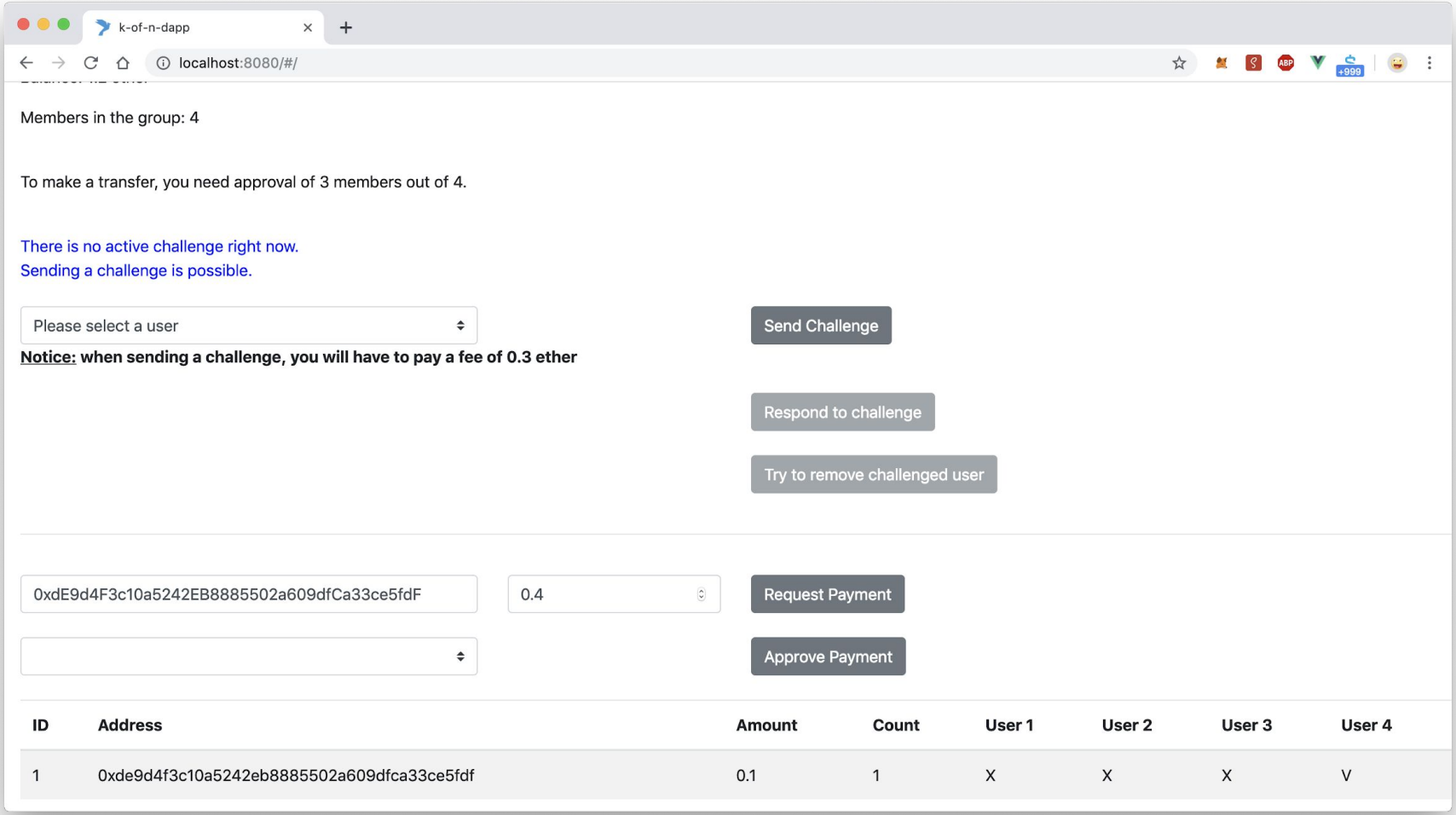


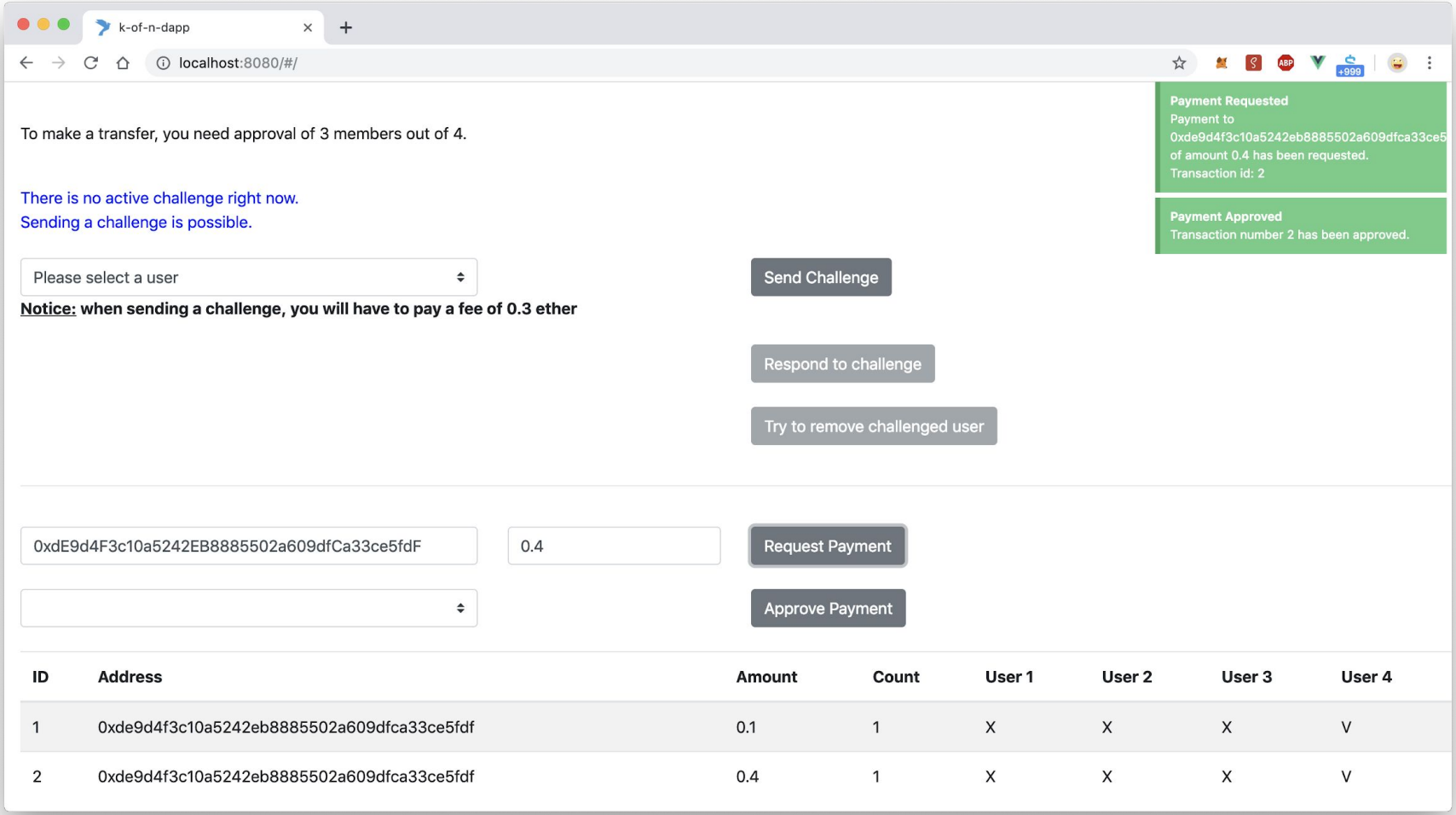
Live Demo

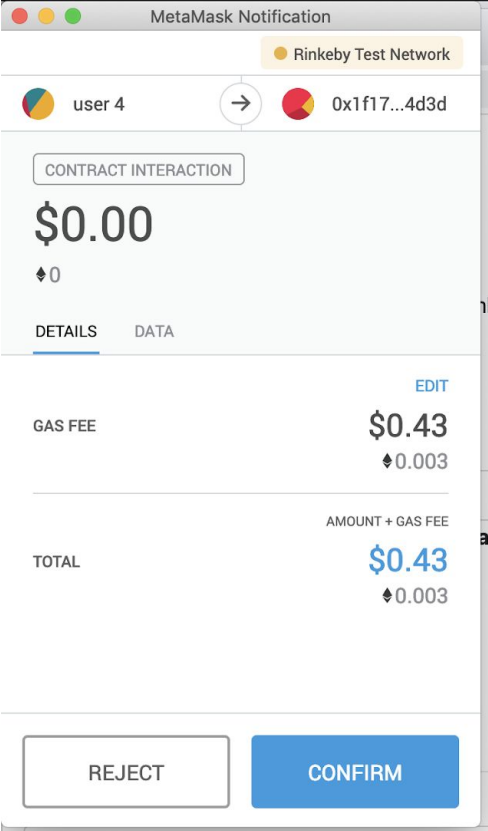

k-of-n-dapp
localhost:8080/#/
K-of-N-Multisig Wallet
User Wallet Details:
Account: 0x15c32df885ffba4e0ae42e7e1928c52be3f8d19b
Balance: 17.548136875 ether
Shared Wallet Details:
Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d
Balance: 1.2 ether
Members in the group: 4
To make a transfer, 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
Notice: when sending a challenge, you will have to pay a fee of 0.3 ether
Send Challenge
Respond to challenge
Try to remove challenged user


MetaMask Notification
Rinkeby Test Network
user 4
0x1f17...4d3d
CONTRACT INTERACTION
$0.00
0
DETAILS
DATA
EDIT
GAS FEE
$0.43
0.003
AMOUNT + GAS FEE
TOTAL
$0.43
0.003
REJECT
CONFIRM
c660f96585c0bb4d3d
nbers out of 4.
ave to pay a fee of 0.3 ether
Send Challenge
Respond to challenge
Try to remove challenged user
0xdE9d4F3c10a5242EB8885502a609dfCa33ce5fdF
0.1
Request Payment
Approve Payment


k-of-n-dapp
localhost:8080/#/
Payment Requested
Payment to 0xde9d4f3c10a5242eb8885502a609dfca33ce5 of amount 0.1 has been requested. Transaction id: 1
Payment Approved
Transaction number 1 has been approved.
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


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


k-of-n-dapp
localhost:8080/#/
Payment Requested
Payment to
0xde9d4f3c10a5242eb8885502a609dfca33ce5
of amount 0.4 has been requested.
Transaction id: 2
Payment Approved
Transaction number 2 has been approved.
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



nbers out of 4.

Send Challenge

ave to pay a fee of 0.3 ether

Respond to challenge

Try to remove challenged user

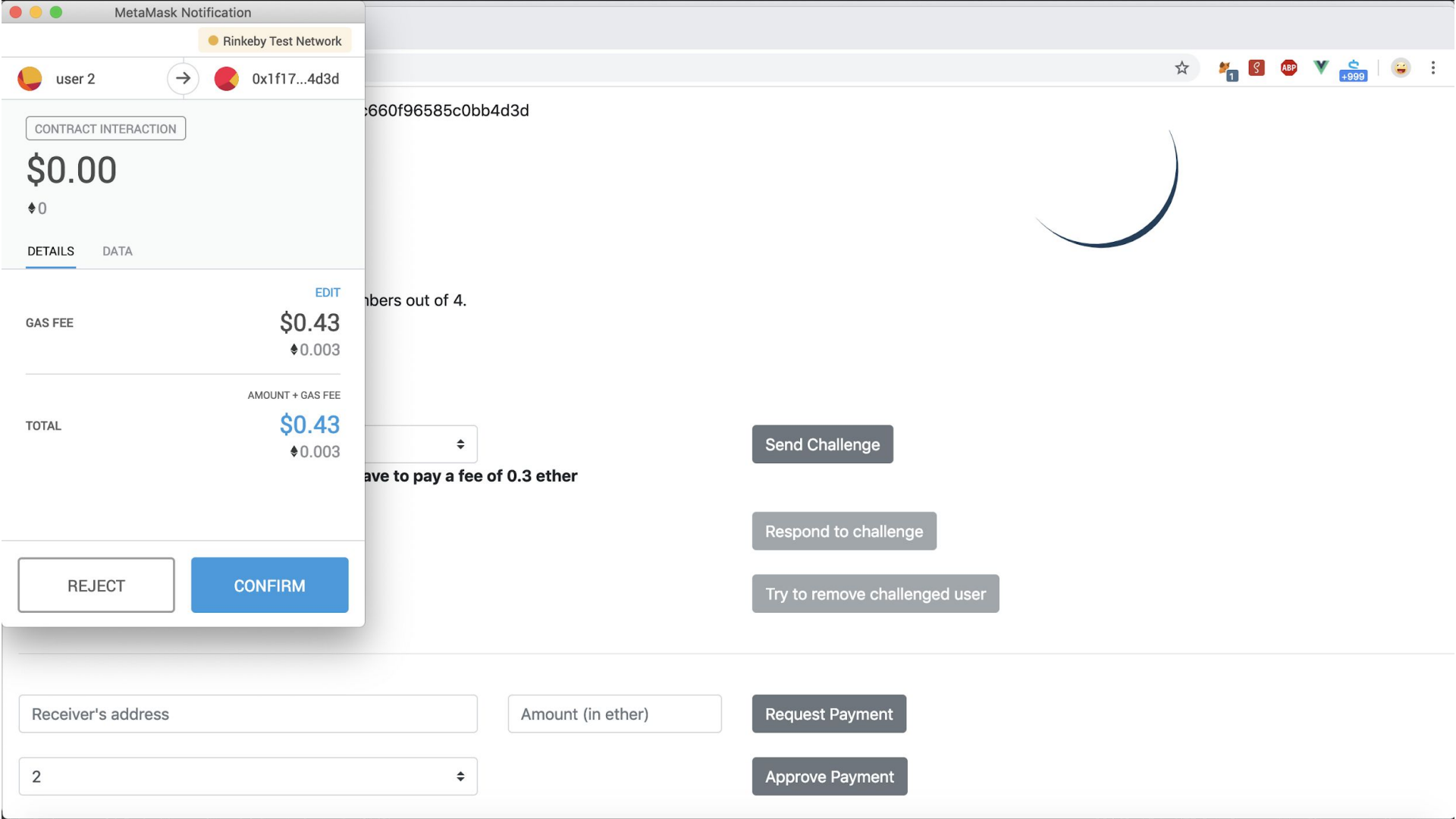
0xdE9d4F3c10a5242EB8885502a609dfCa33ce5fdF

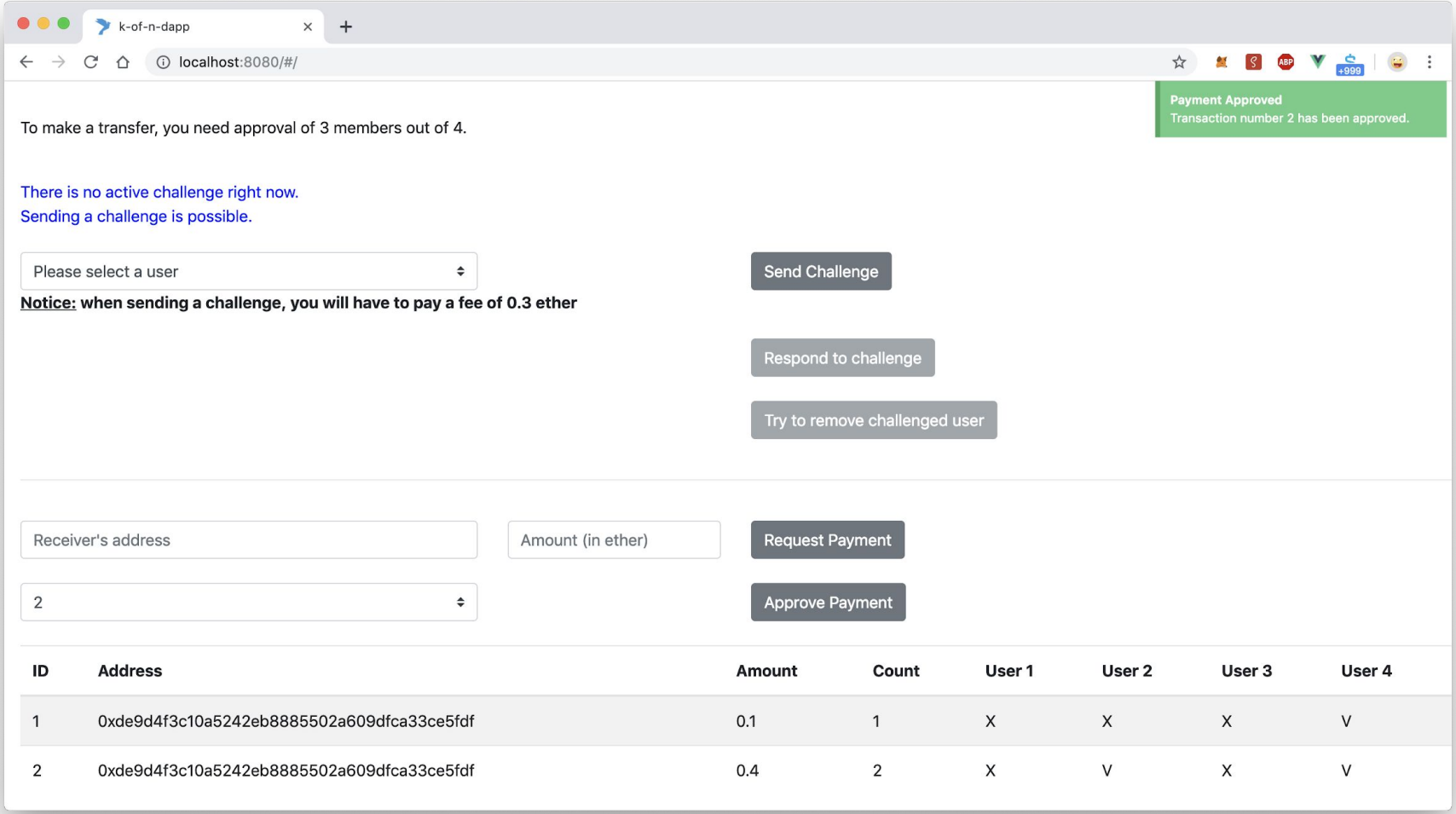
0.4

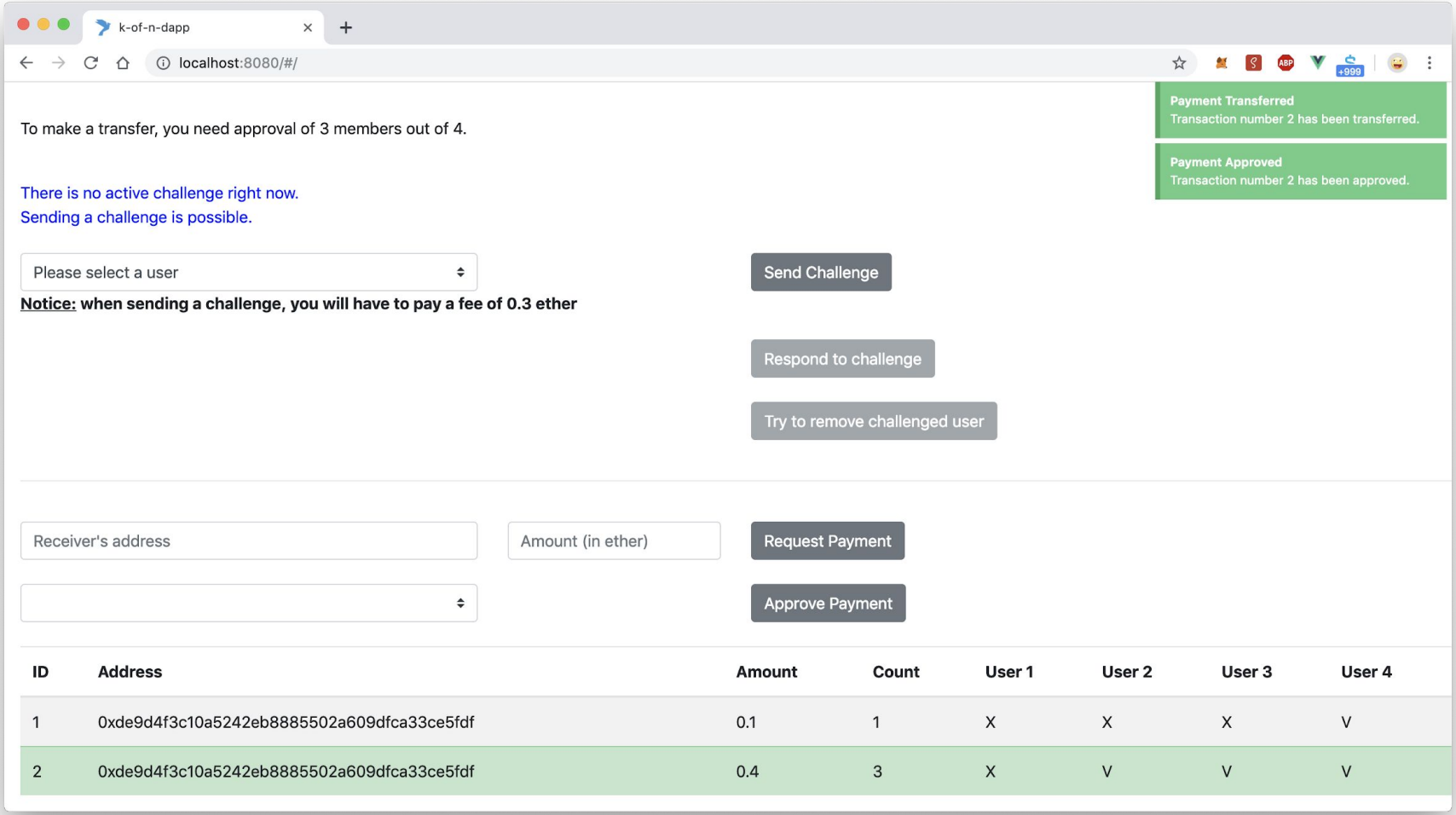
Request Payment

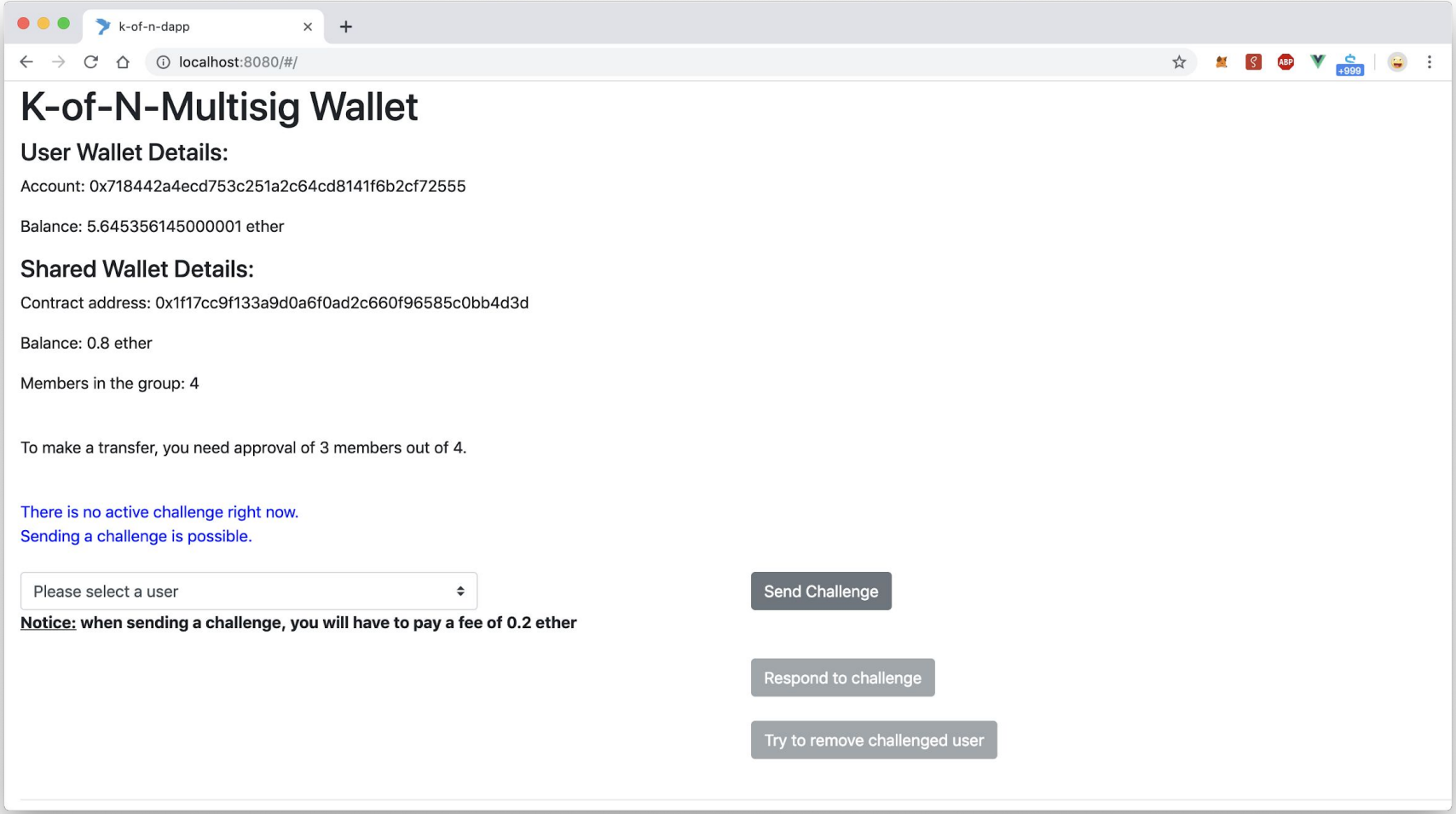
Approve Payment

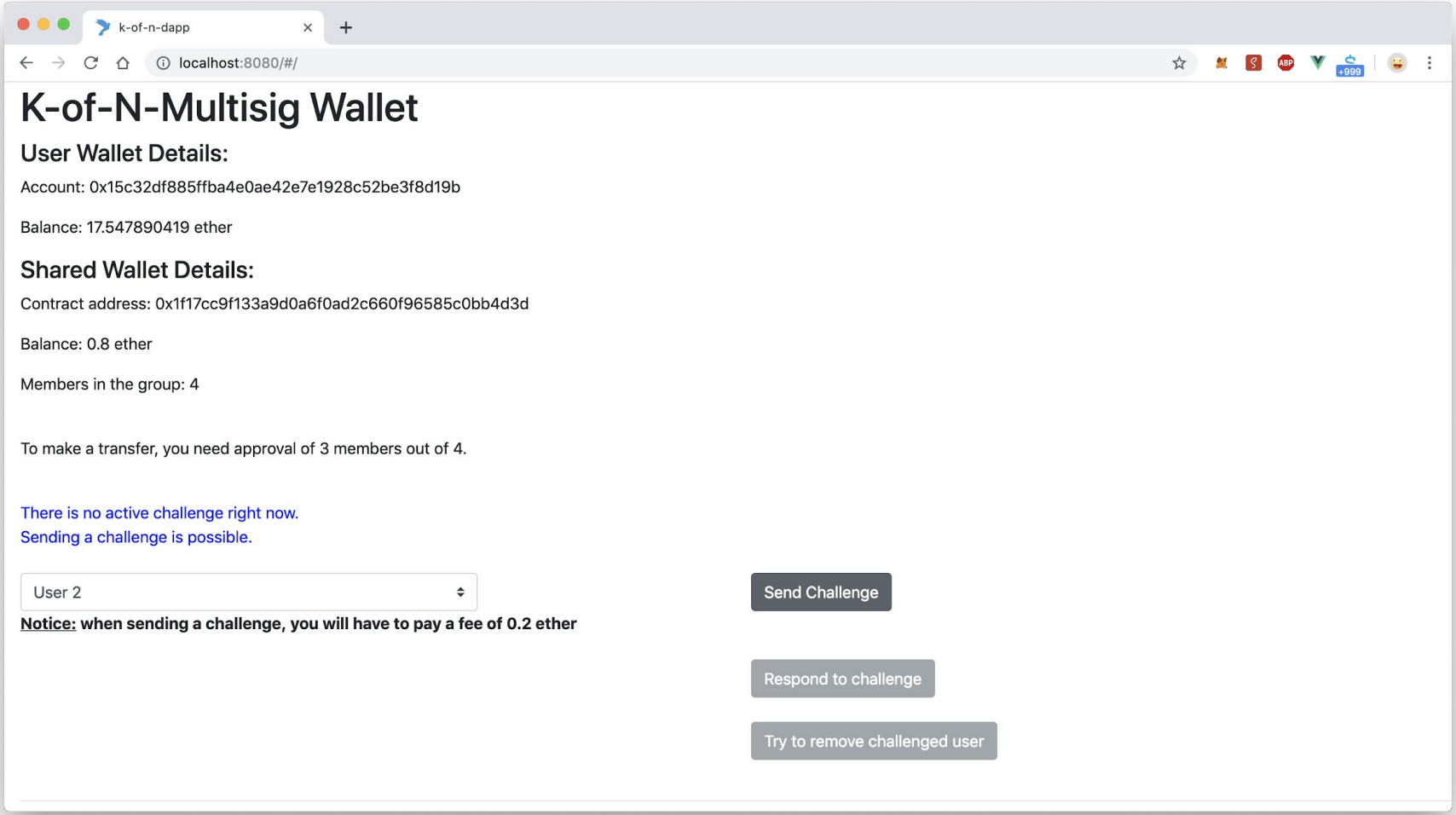
ID	Address	Amount	Count	User 1	User 2	User 3	User 4

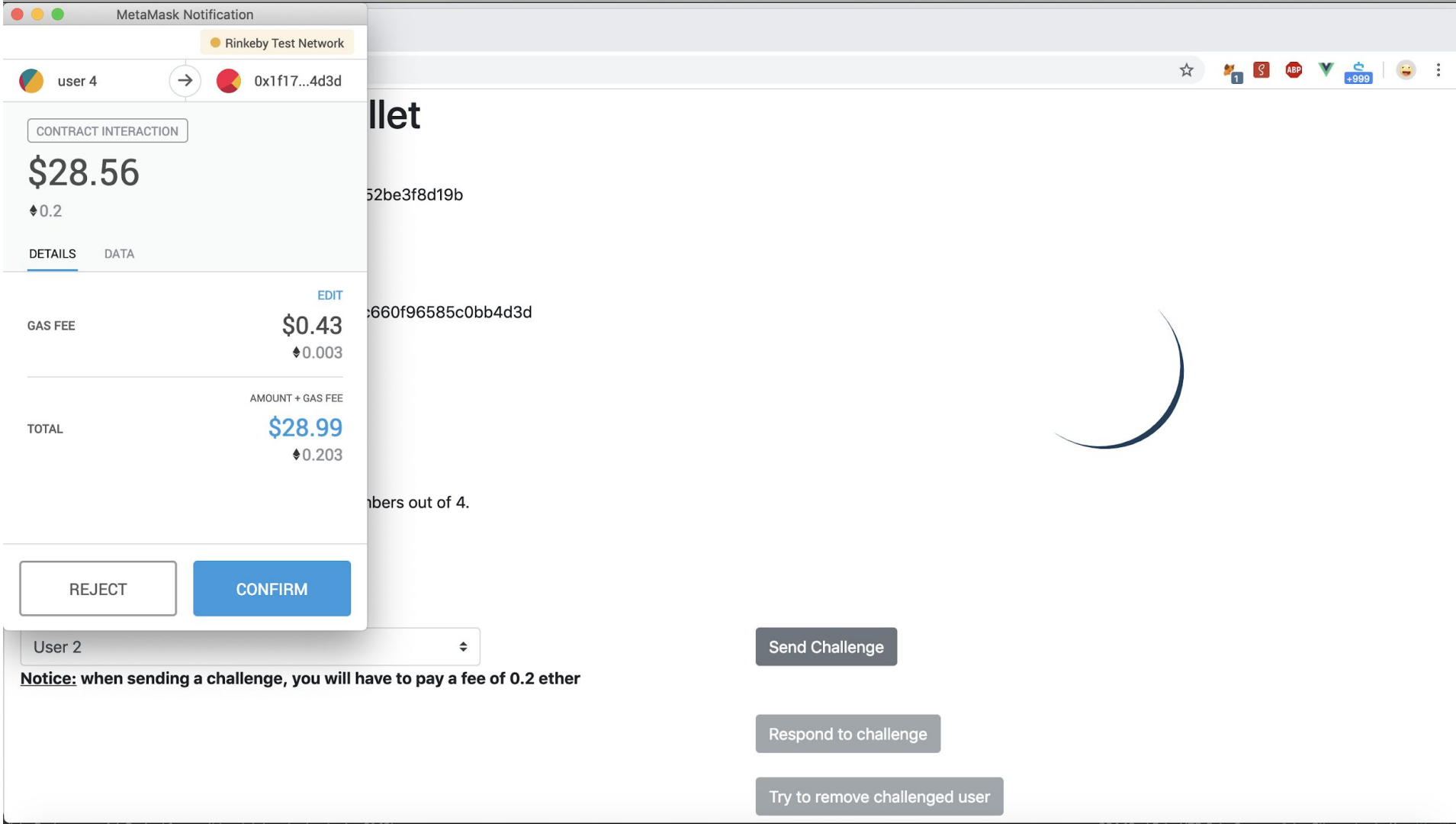

MetaMask Notification
Rinkeby Test Network
user 2
0x1f17...4d3d
CONTRACT INTERACTION
$0.00
0
DETAILS
DATA
EDIT
GAS FEE
$0.43
0.003
AMOUNT + GAS FEE
TOTAL
$0.43
0.003
REJECT
CONFIRM
660f96585c0bb4d3d
bers out of 4.
ave to pay a fee of 0.3 ether
Send Challenge
Respond to challenge
Try to remove challenged user
Receiver's address
Amount (in ether)
Request Payment
2
Approve Payment

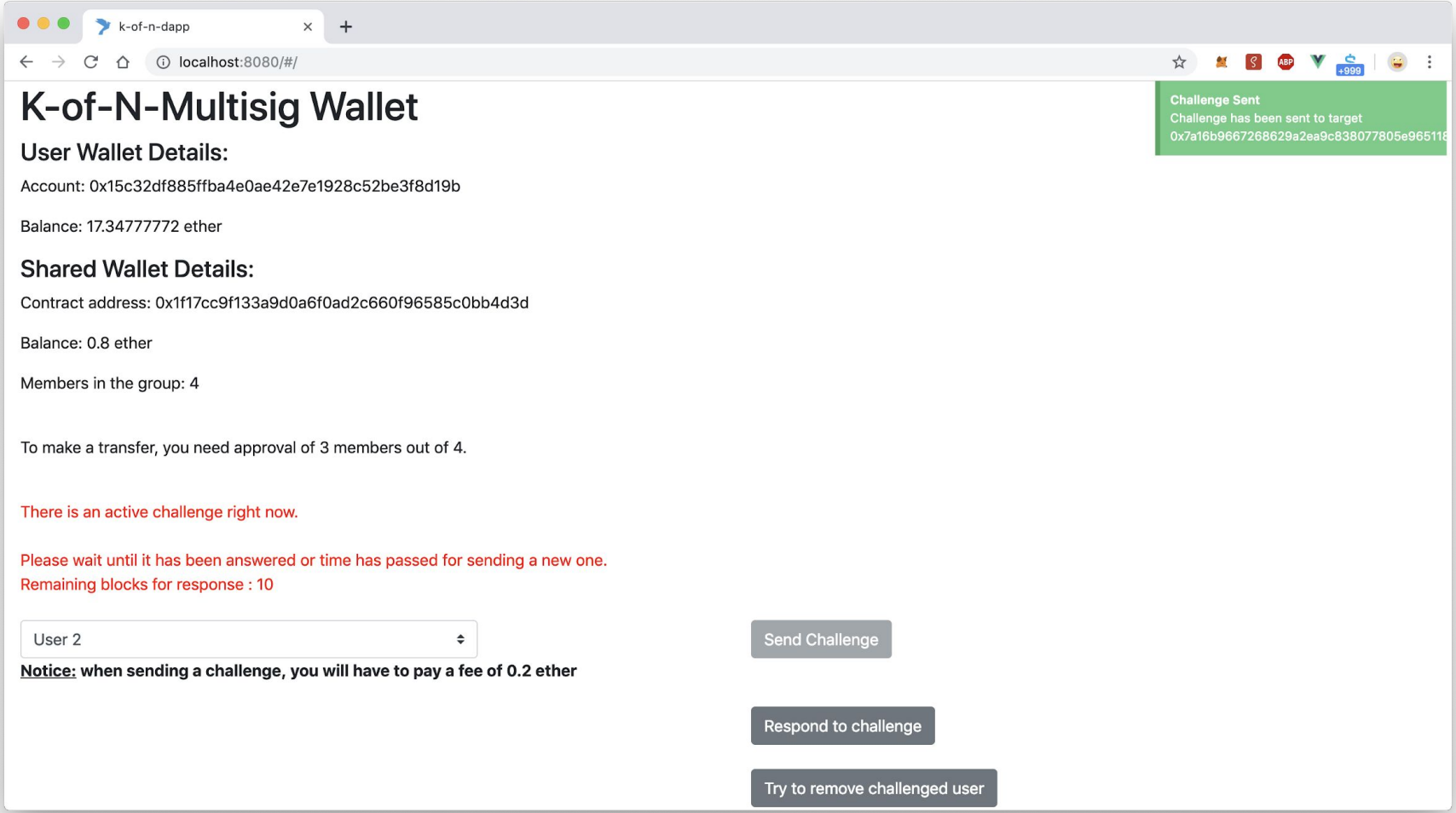

k-of-n-dapp
localhost:8080/#/
Payment Approved
Transaction number 2 has been approved.
To make a transfer, you need approval of 3 members out of 4.
There is no active challenge right now.
Sending a challenge is possible.
Please select a user
Send Challenge
Notice: when sending a challenge, you will have to pay a fee of 0.3 ether
Respond to challenge
Try to remove challenged user
Receiver's address
Amount (in ether)
Request Payment
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

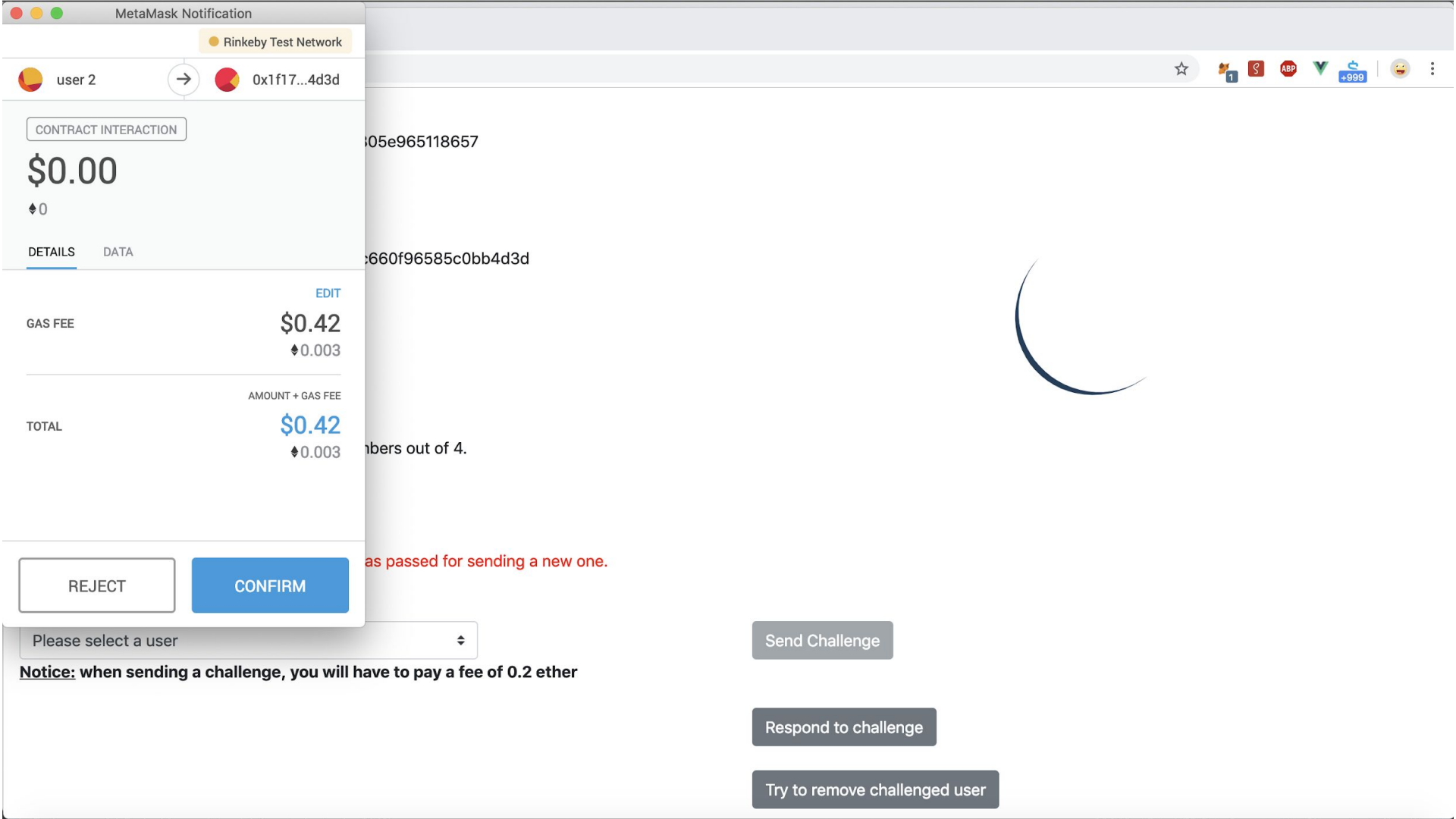

k-of-n-dapp
localhost:8080/#/
Payment Transferred
Transaction number 2 has been transferred.
Payment Approved
Transaction number 2 has been approved.
To make a transfer, you need approval of 3 members out of 4.
There is no active challenge right now.
Sending a challenge is possible.
Please select a user
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

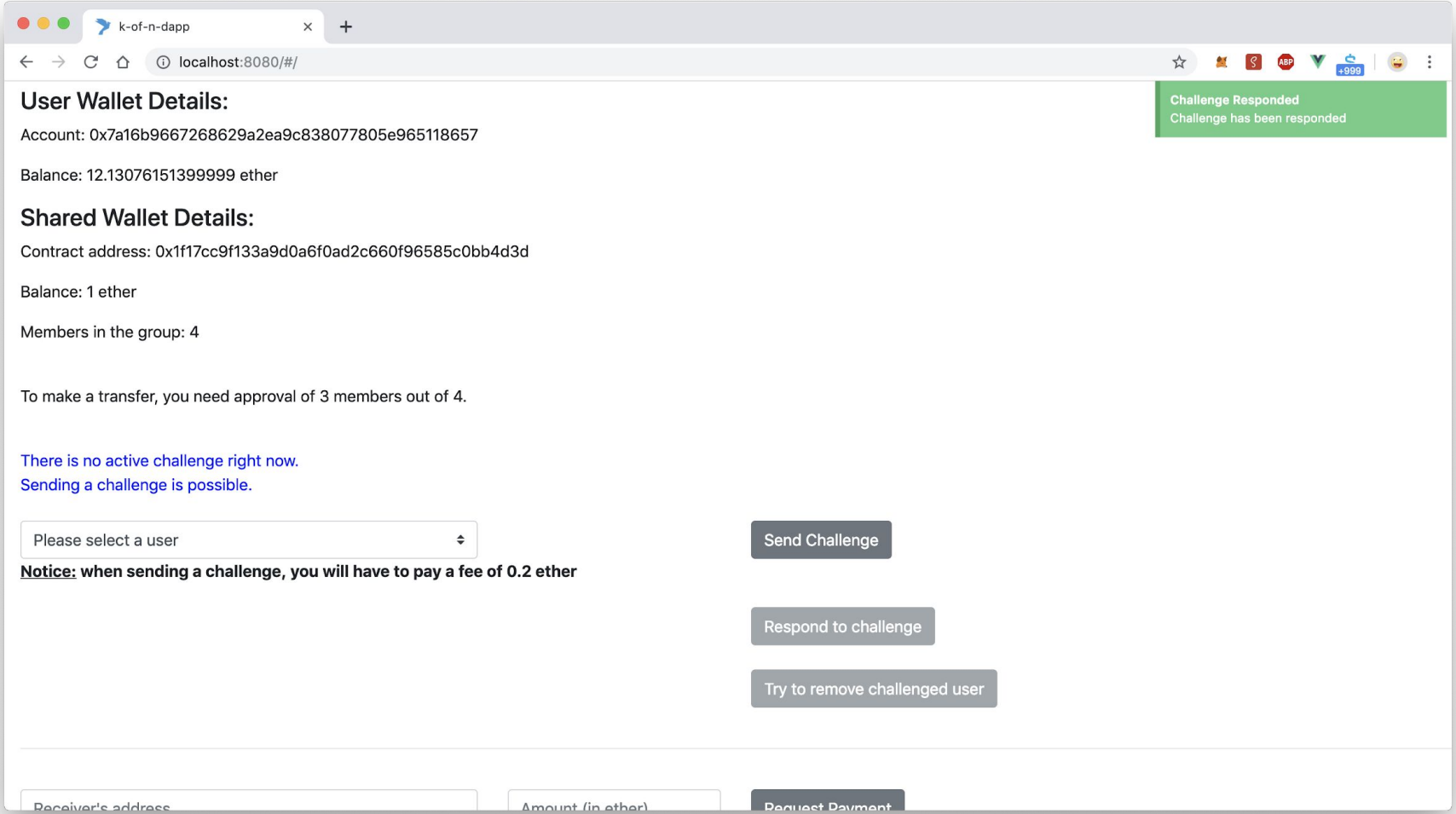

k-of-n-dapp
localhost:8080/#/
K-of-N-Multisig Wallet
User Wallet Details:
Account: 0x718442a4ecd753c251a2c64cd8141f6b2cf72555
Balance: 5.645356145000001 ether
Shared Wallet Details:
Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d
Balance: 0.8 ether
Members in the group: 4
To make a transfer, 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
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Send Challenge
Respond to challenge
Try to remove challenged user

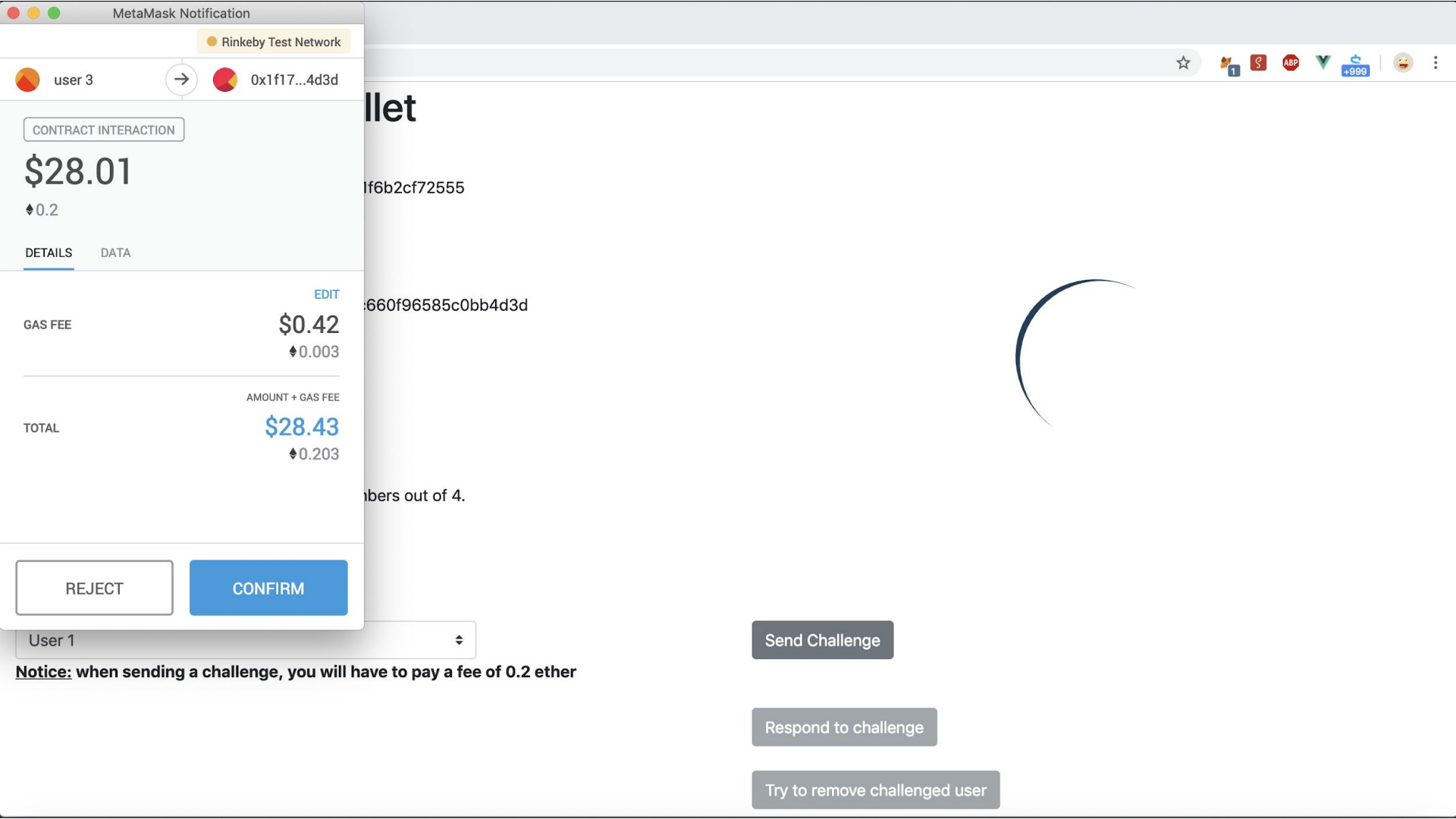

k-of-n-dapp
localhost:8080/#/
K-of-N-Multisig Wallet
User Wallet Details:
Account: 0x15c32df885ffba4e0ae42e7e1928c52be3f8d19b
Balance: 17.547890419 ether
Shared Wallet Details:
Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d
Balance: 0.8 ether
Members in the group: 4
To make a transfer, you need approval of 3 members out of 4.
There is no active challenge right now.
Sending a challenge is possible.
User 2
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Send Challenge
Respond to challenge
Try to remove challenged user

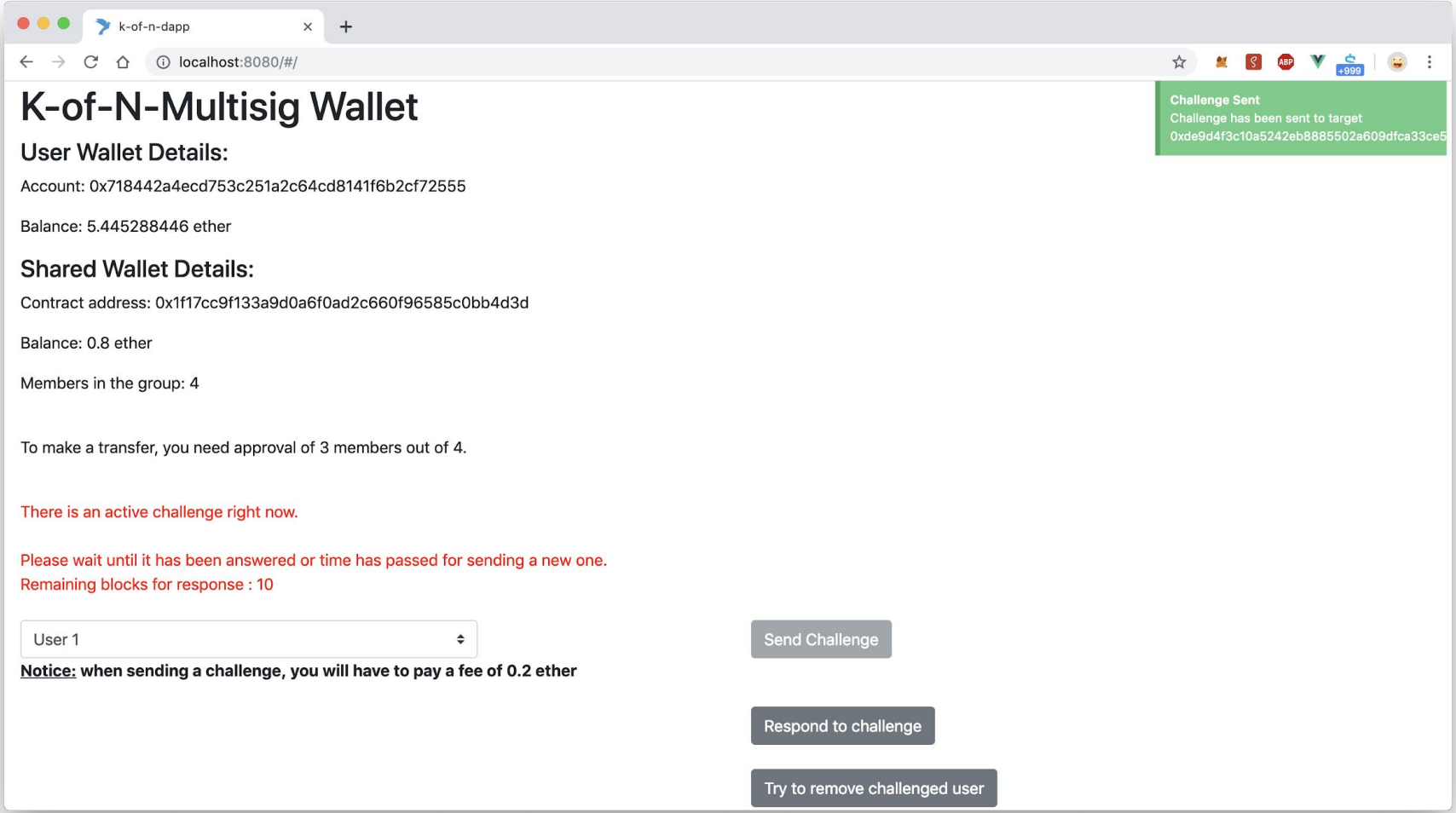

MetaMask Notification
Rinkeby Test Network
user 4
0x1f17...4d3d
CONTRACT INTERACTION
$28.56
0.2
DETAILS
DATA
EDIT
GAS FEE
$0.43
0.003
AMOUNT + GAS FEE
TOTAL
$28.99
0.203
REJECT
CONFIRM
llet
52be3f8d19b
:660f96585c0bb4d3d
bers out of 4.
User 2
Send Challenge
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Respond to challenge
Try to remove challenged user

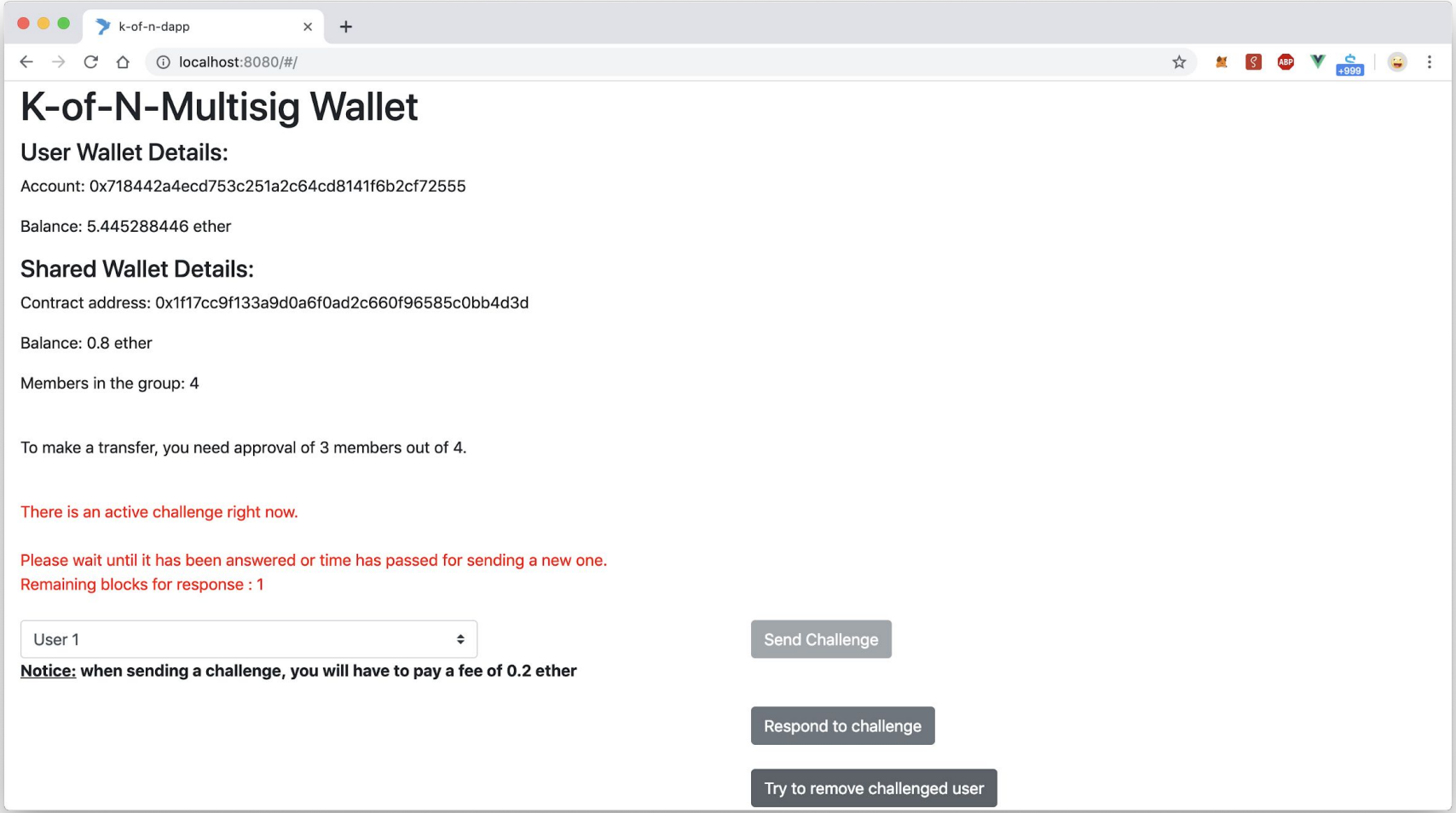

k-of-n-dapp
localhost:8080/#/
K-of-N-Multisig Wallet
Challenge Sent
Challenge has been sent to target
0x7a16b9667268629a2ea9c838077805e965118
User Wallet Details:
Account: 0x15c32df885ffba4e0ae42e7e1928c52be3f8d19b
Balance: 17.34777772 ether
Shared Wallet Details:
Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d
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
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Send Challenge
Respond to challenge
Try to remove challenged user

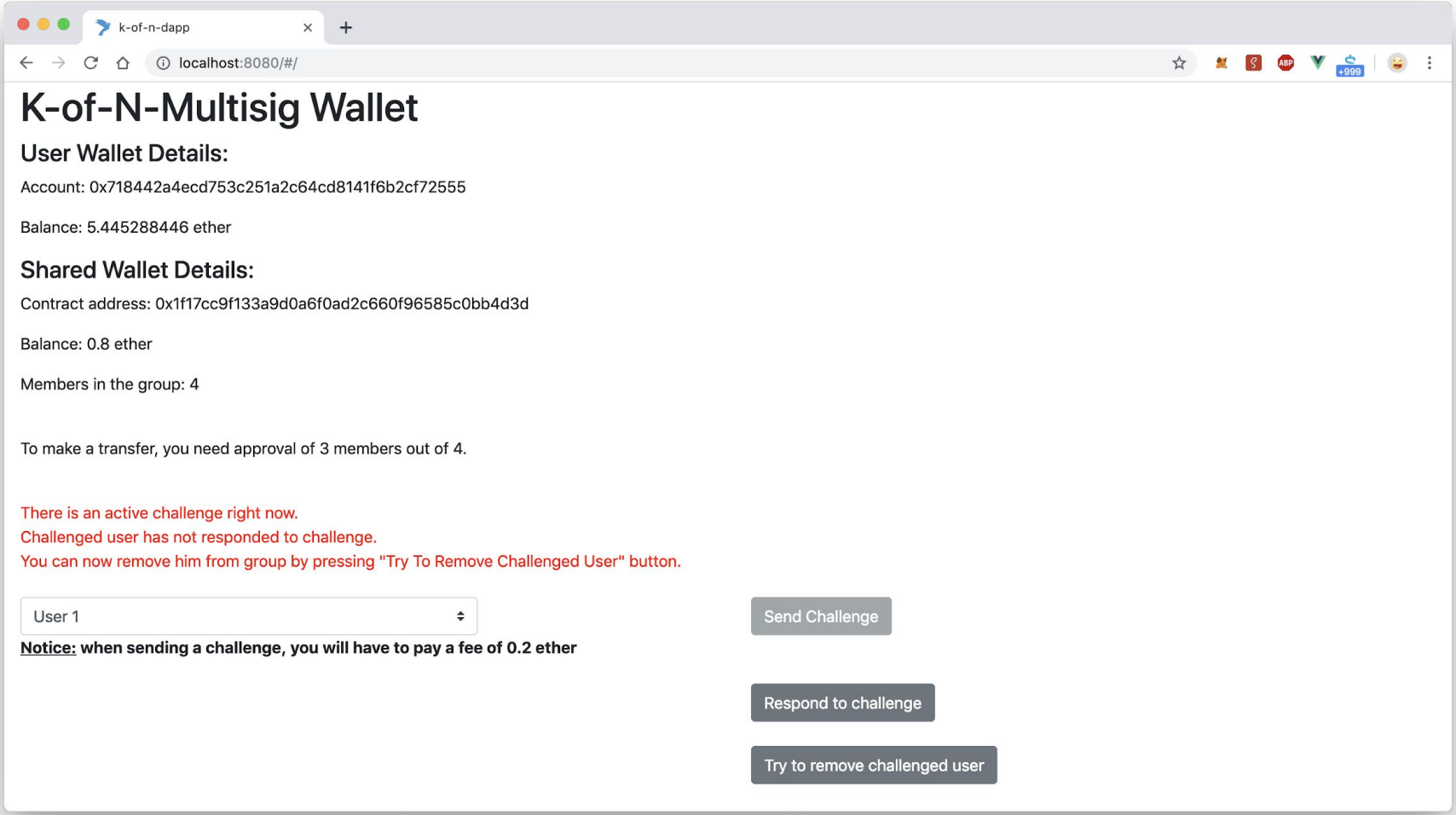

MetaMask Notification
Rinkeby Test Network
user 2
0x1f17...4d3d
CONTRACT INTERACTION
$0.00
0
DETAILS
DATA
EDIT
GAS FEE
$0.42
0.003
AMOUNT + GAS FEE
TOTAL
$0.42
0.003
REJECT
CONFIRM
05e965118657
660f96585c0bb4d3d
bers out of 4.
as passed for sending a new one.
Please select a user
Send Challenge
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Respond to challenge
Try to remove challenged user

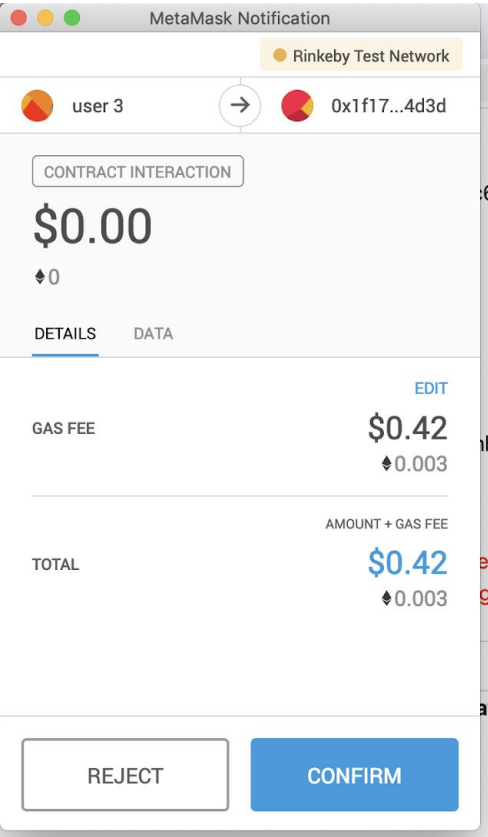

k-of-n-dapp
localhost:8080/#/
+999
User Wallet Details:
Account: 0x7a16b9667268629a2ea9c838077805e965118657
Balance: 12.13076151399999 ether
Challenge Responded
Challenge has been responded
Shared Wallet Details:
Contract address: 0x1f17cc9f133a9d0a6f0ad2c660f96585c0bb4d3d
Balance: 1 ether
Members in 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


MetaMask Notification
Rinkeby Test Network
user 3
0x1f17...4d3d
CONTRACT INTERACTION
$28.01
0.2
DETAILS
DATA
EDIT
GAS FEE
$0.42
0.003
AMOUNT + GAS FEE
TOTAL
$28.43
0.203
REJECT
CONFIRM
llet
1f6b2cf72555
660f96585c0bb4d3d
bers out of 4.
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/#/
+999
K-of-N-Multisig Wallet
Challenge Sent
Challenge has been sent to target
0xde9d4f3c10a5242eb8885502a609dfca33ce5
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
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Send Challenge
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.
Please wait until it has been answered or time has passed for sending a new one.
Remaining blocks for response : 1
User 1
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Send Challenge
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
Notice: when sending a challenge, you will have to pay a fee of 0.2 ether
Send Challenge
Respond to challenge
Try to remove challenged user



660f96585c0bb4d3d

bers out of 4.

e.

g "Try To Remove Challenged User" button.

Send Challenge

ave to pay a fee of 0.2 ether

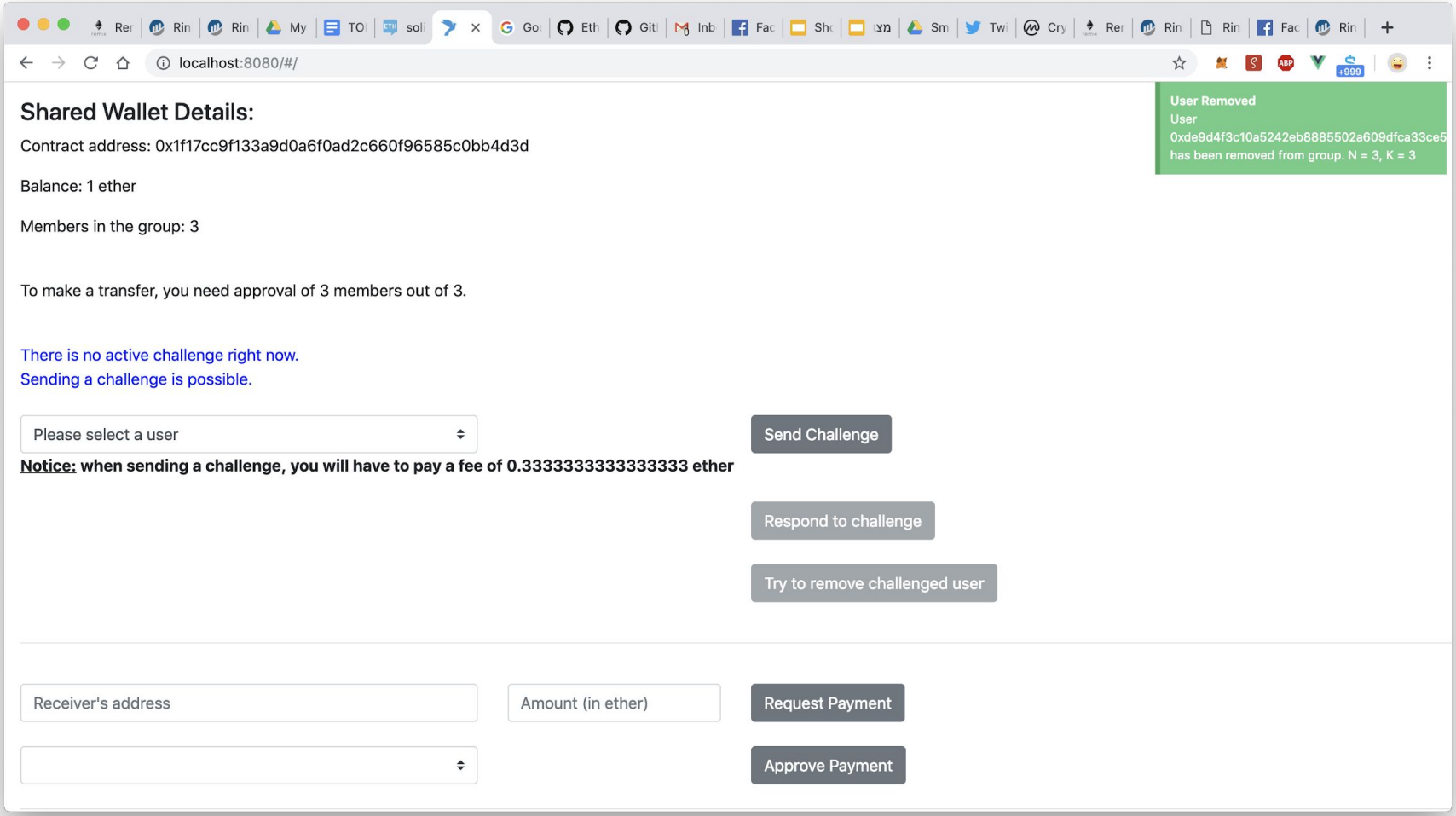
Respond to challenge

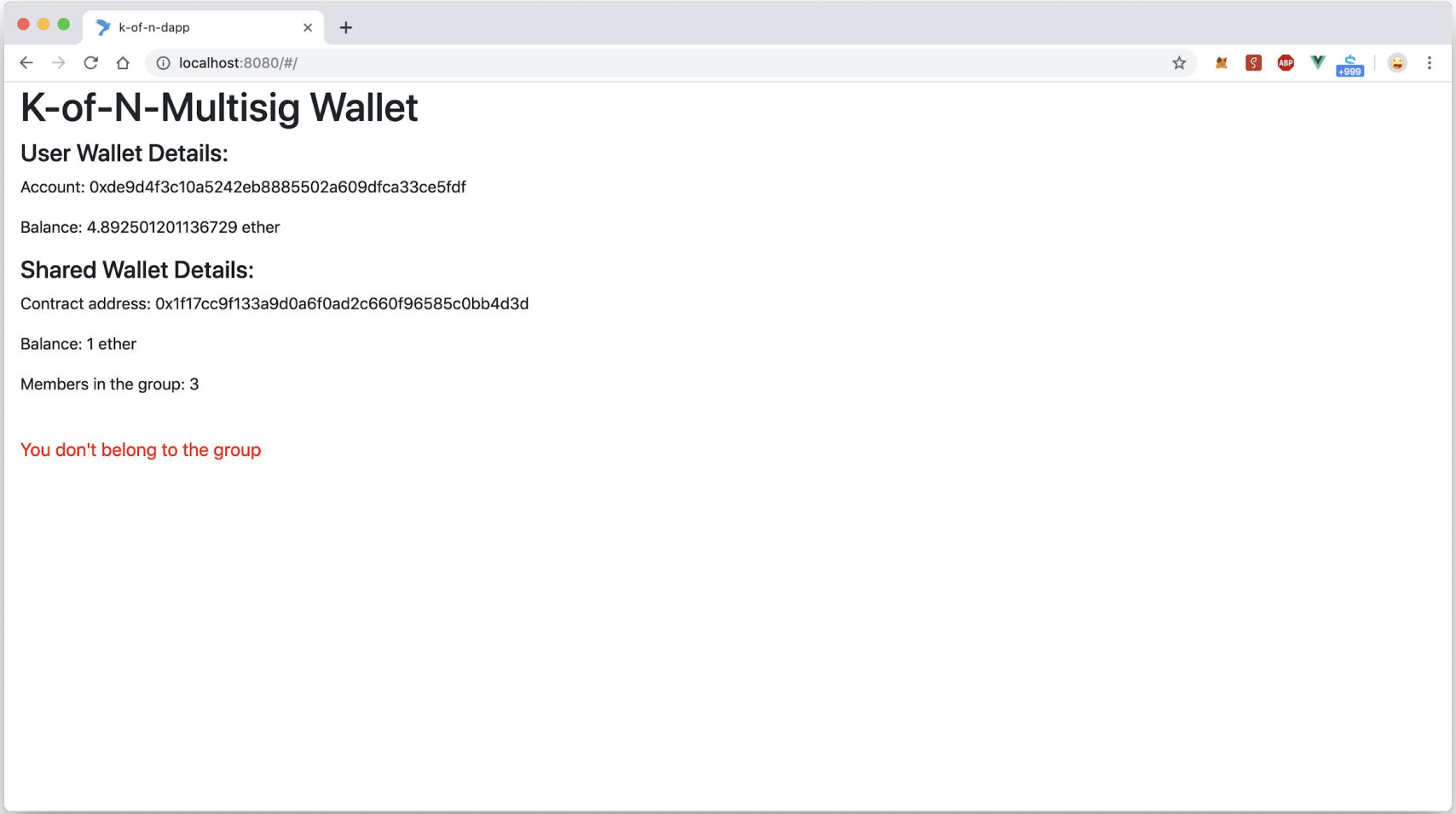
Try to remove challenged user

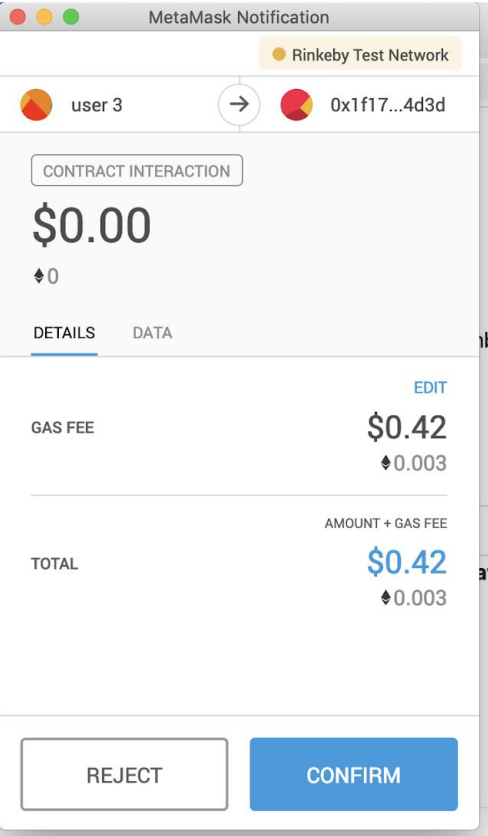
Receiver's address

Amount (in ether)

Request Payment


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/#/
+999
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



bers out of 3.

ave to pay a fee of 0.3333333333333333 ether

Send Challenge

Respond to challenge

Try to remove challenged user

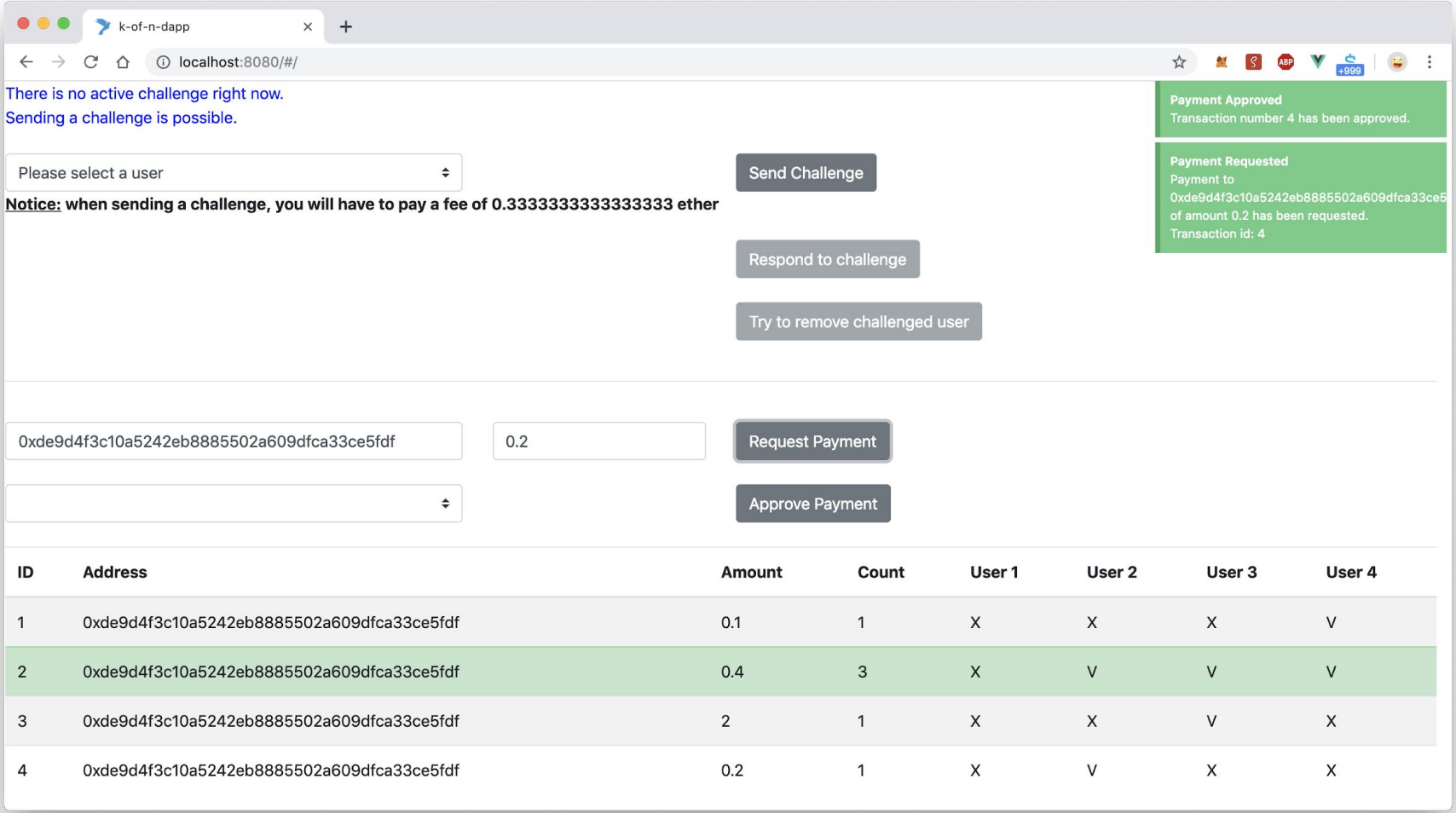
0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf

2

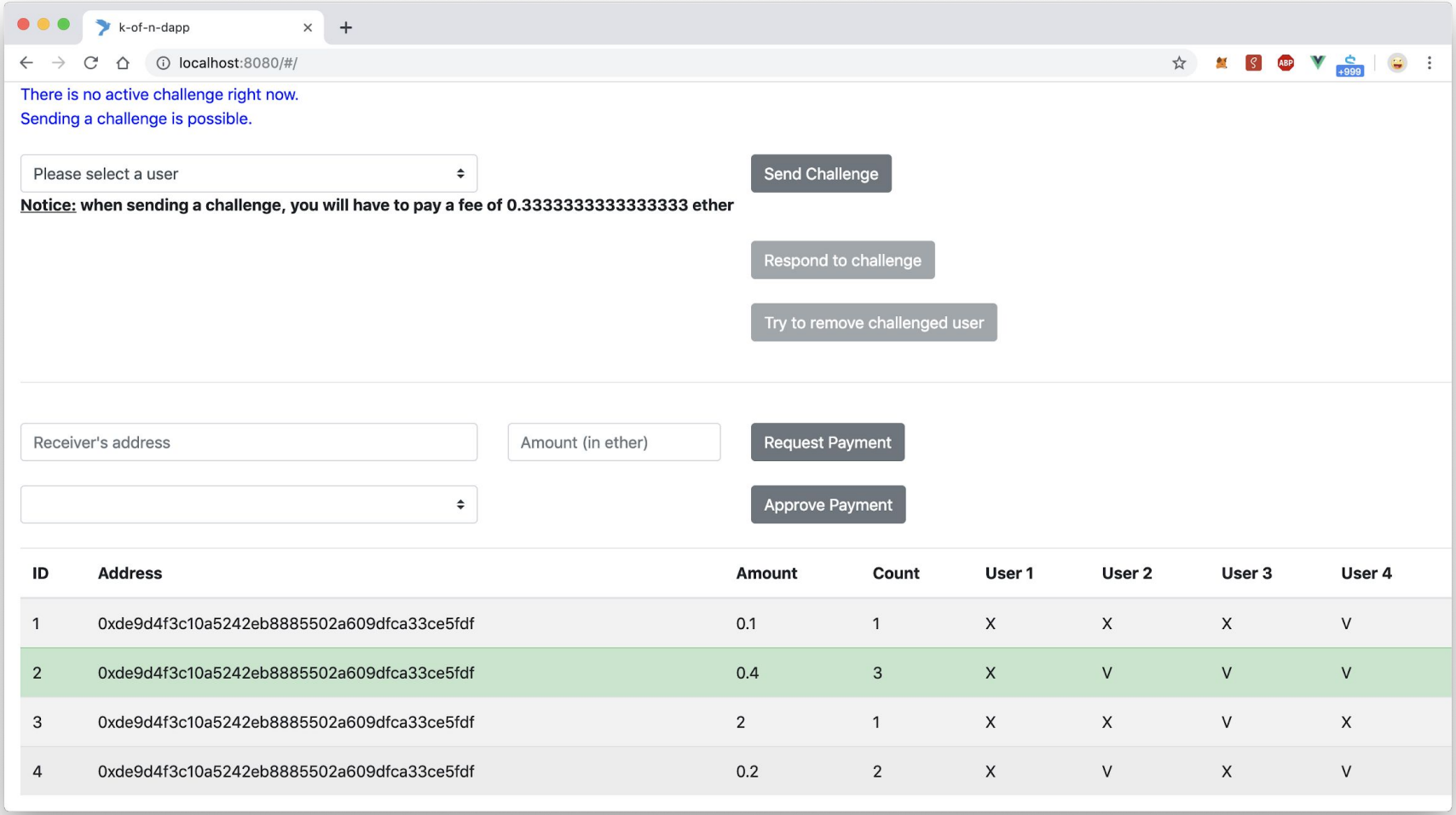
Request Payment

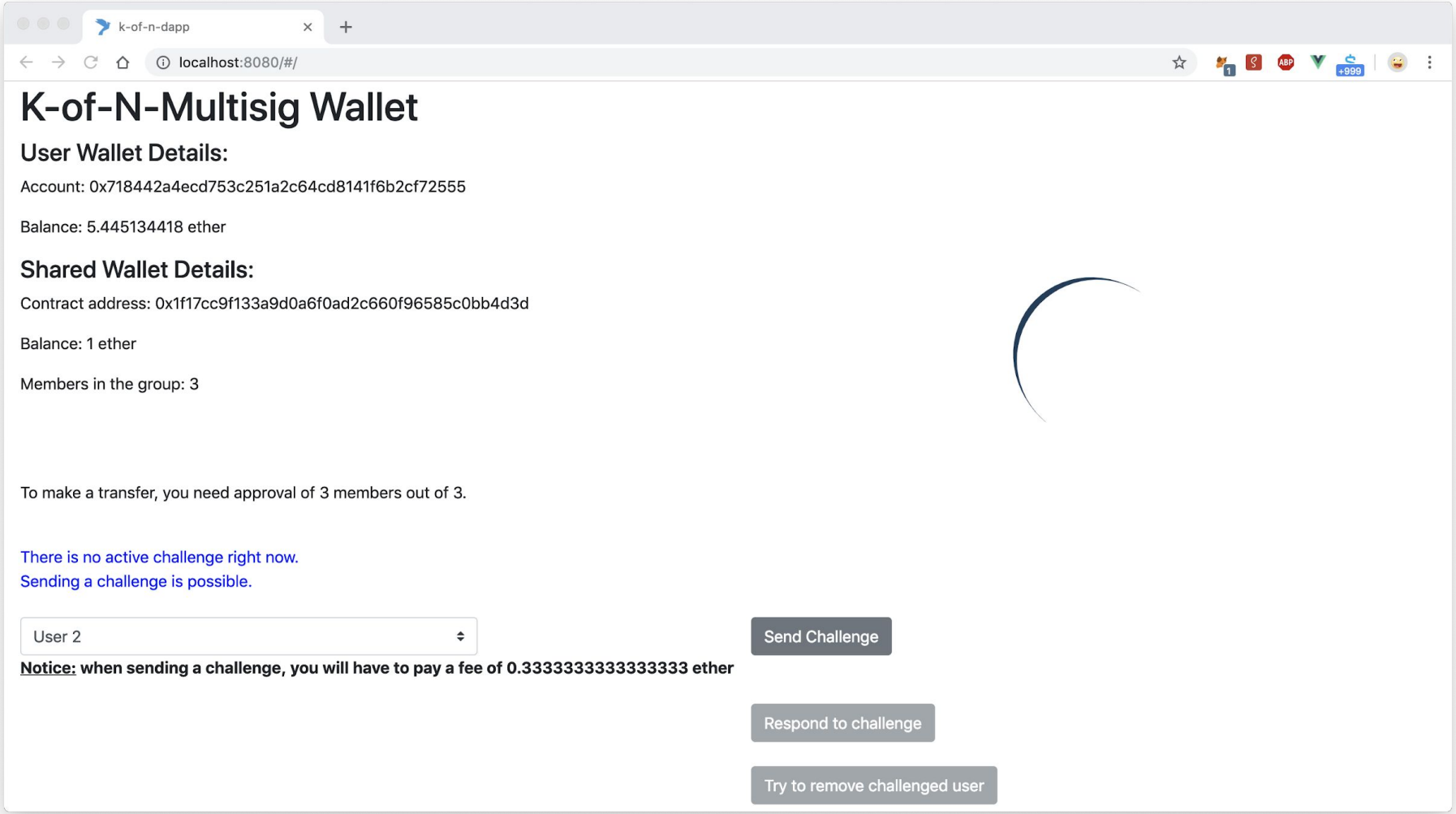
Approve Payment

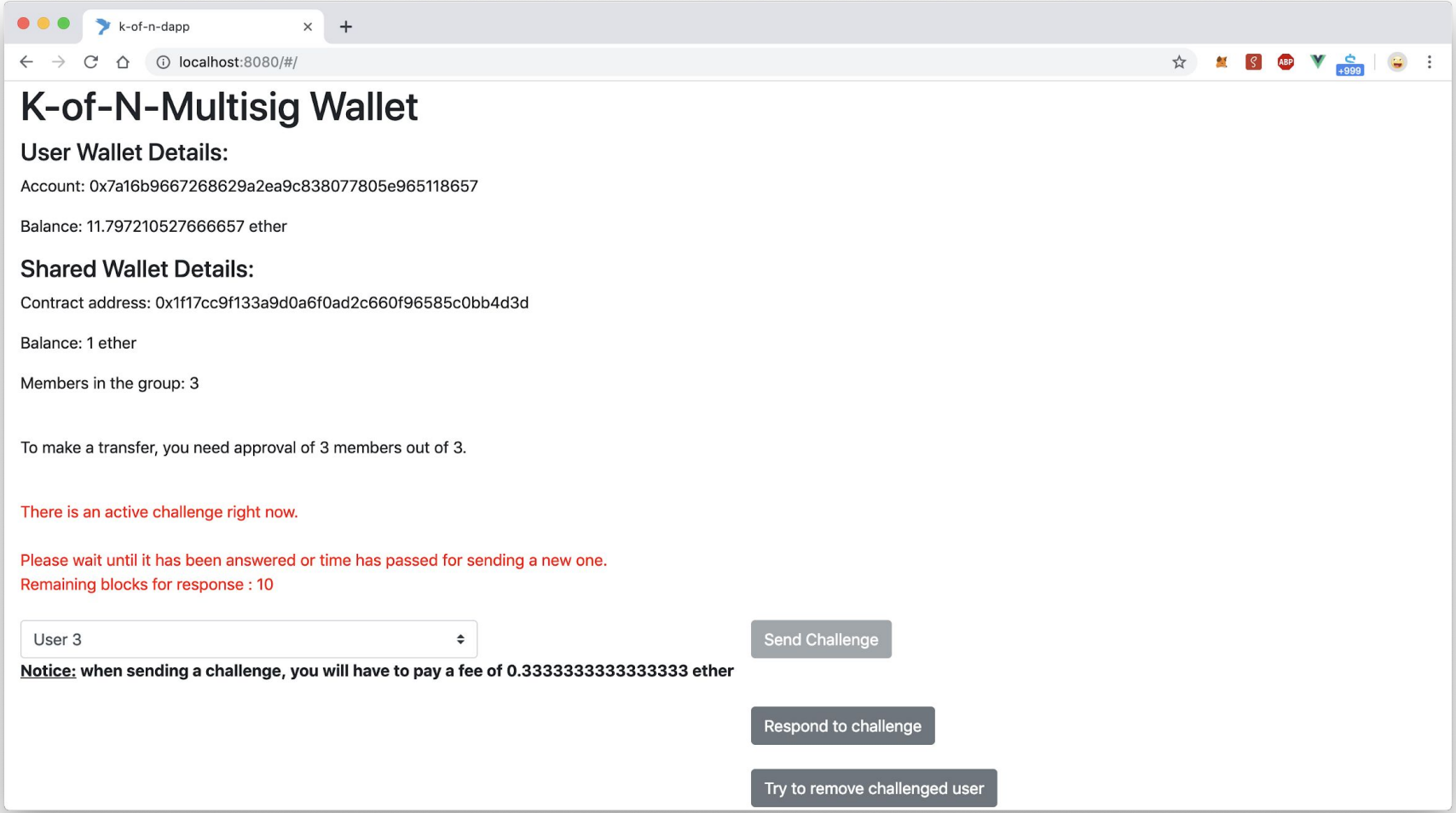
ID	Address	Amount	Count	User 1	User 2	User 3	User 4

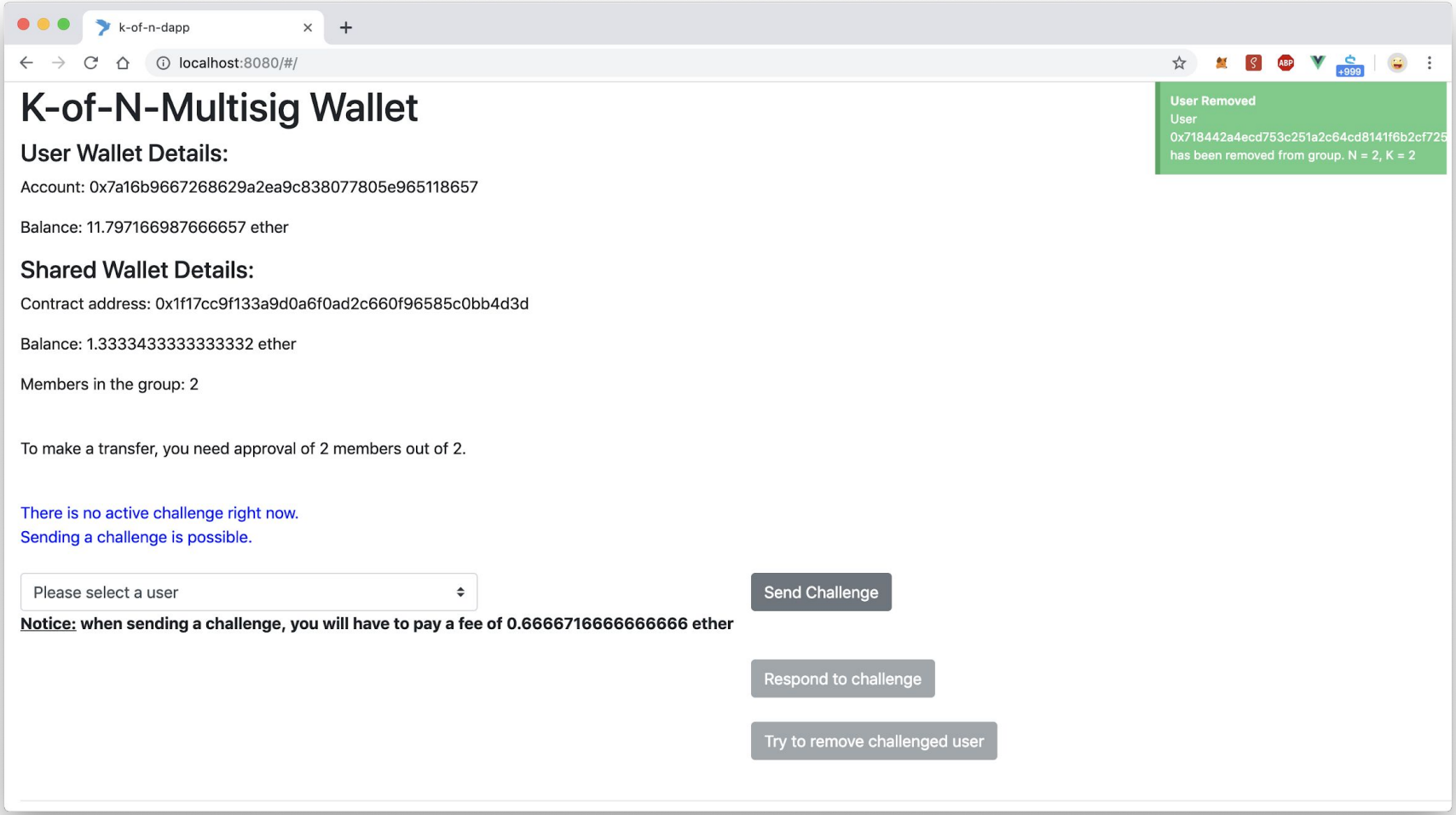


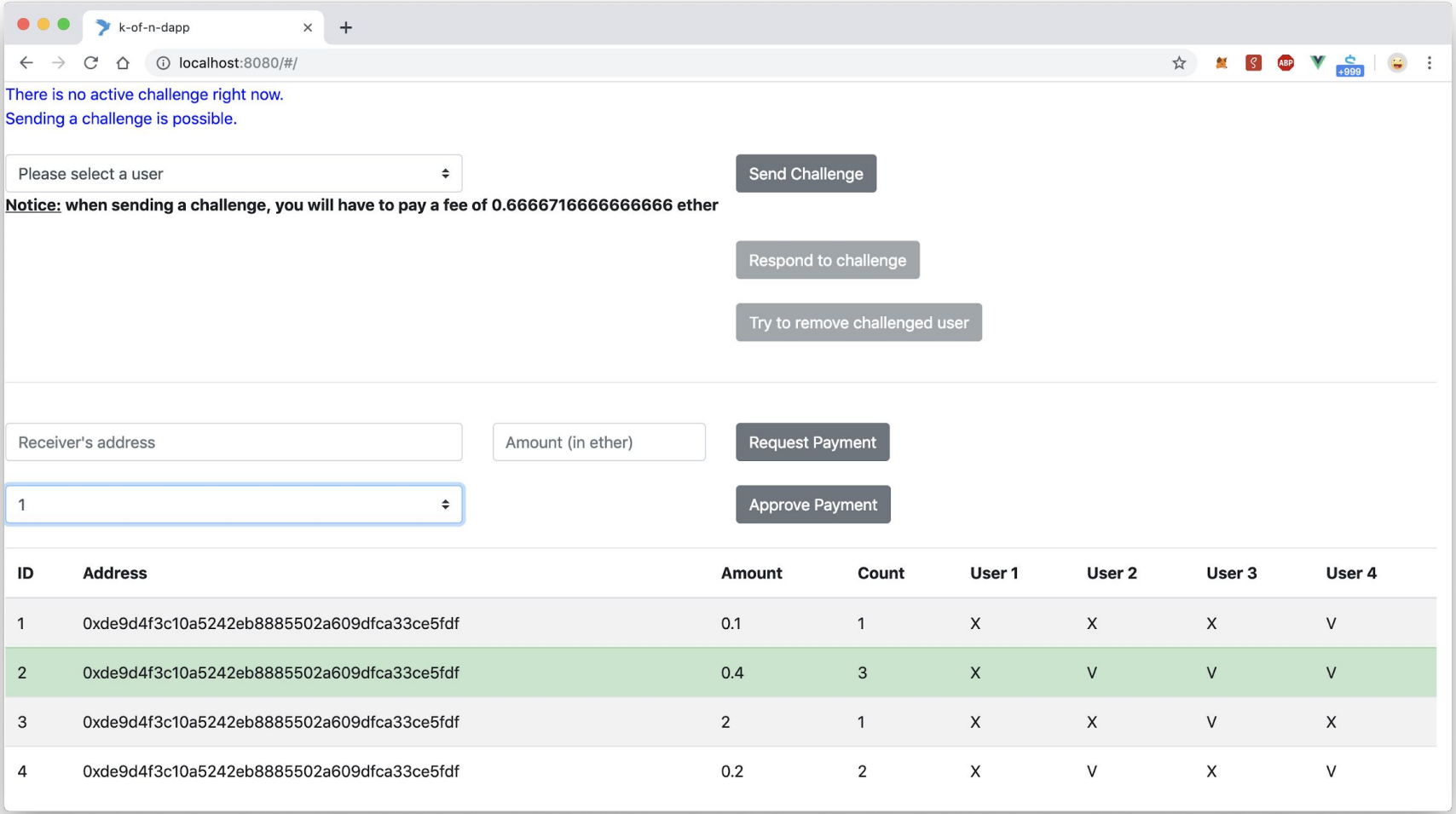
ID	Address	Amount	Count	User 1	User 2	User 3	User 4
1	0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf	0.1	1	X	X	X	V
2	0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf	0.4	3	X	V	V	V
3	0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf	2	1	X	X	V	X
4	0xde9d4f3c10a5242eb8885502a609dfca33ce5fdf	0.2	1	X	V	X	X


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/#/
+999
K-of-N-Multisig Wallet
User Removed
User
0x718442a4ecd753c251a2c64cd8141f6b2cf725
has been removed from group. N = 2, K = 2
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


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


THANK YOU