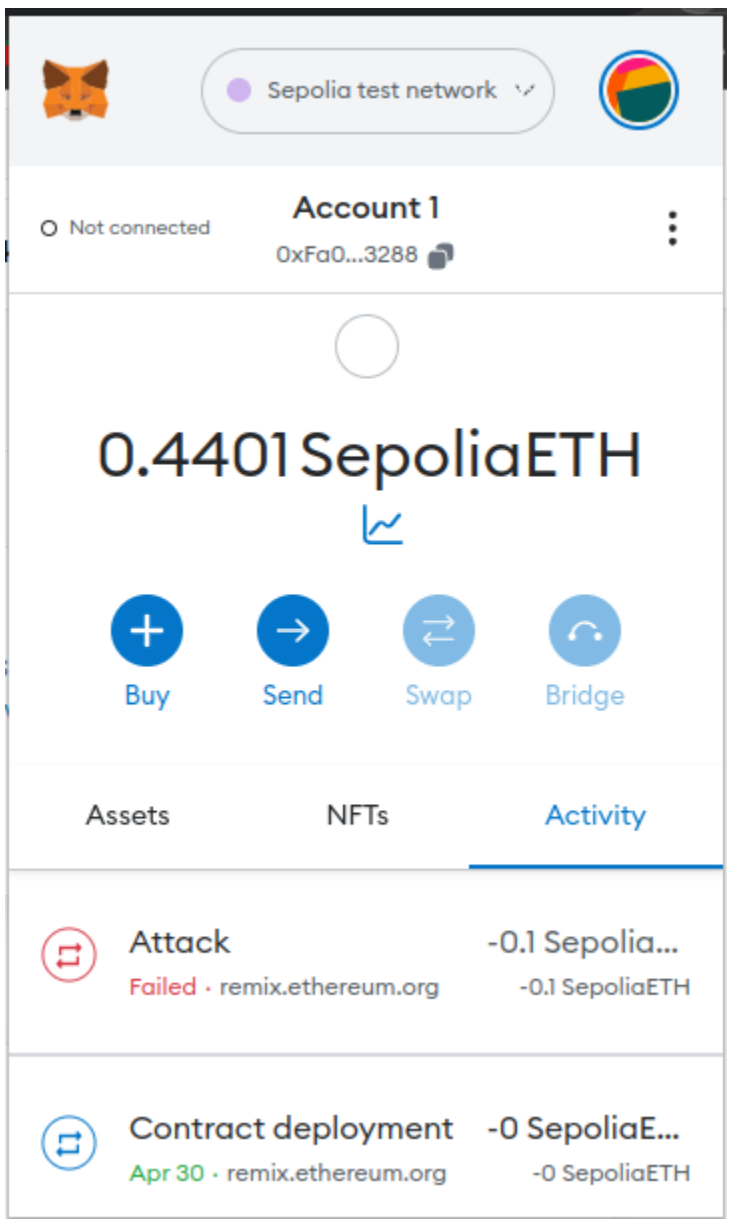
BFSC Ethernaut CTF Assignment

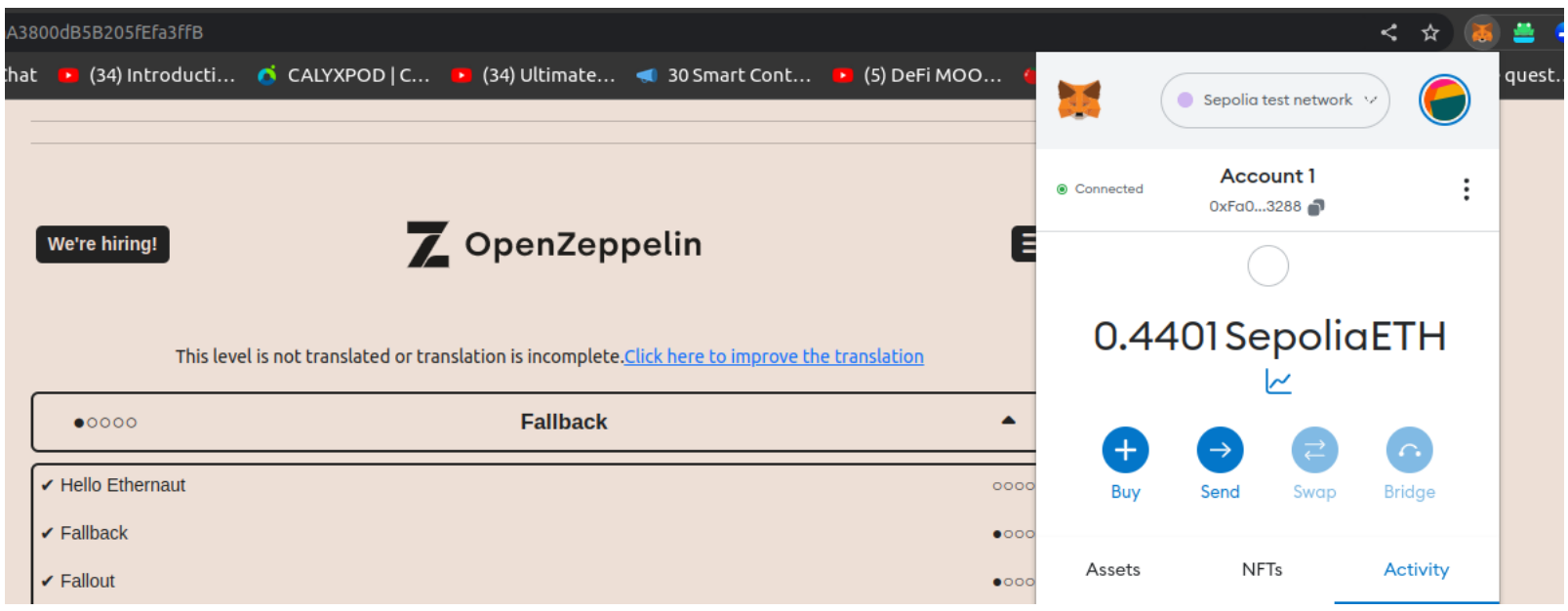
Manmeet Singh Brar
20UCS112

Wallet Address - 0xFa00D29d378EDC57AA1006946F0fc6230a5E3288(Metamask)

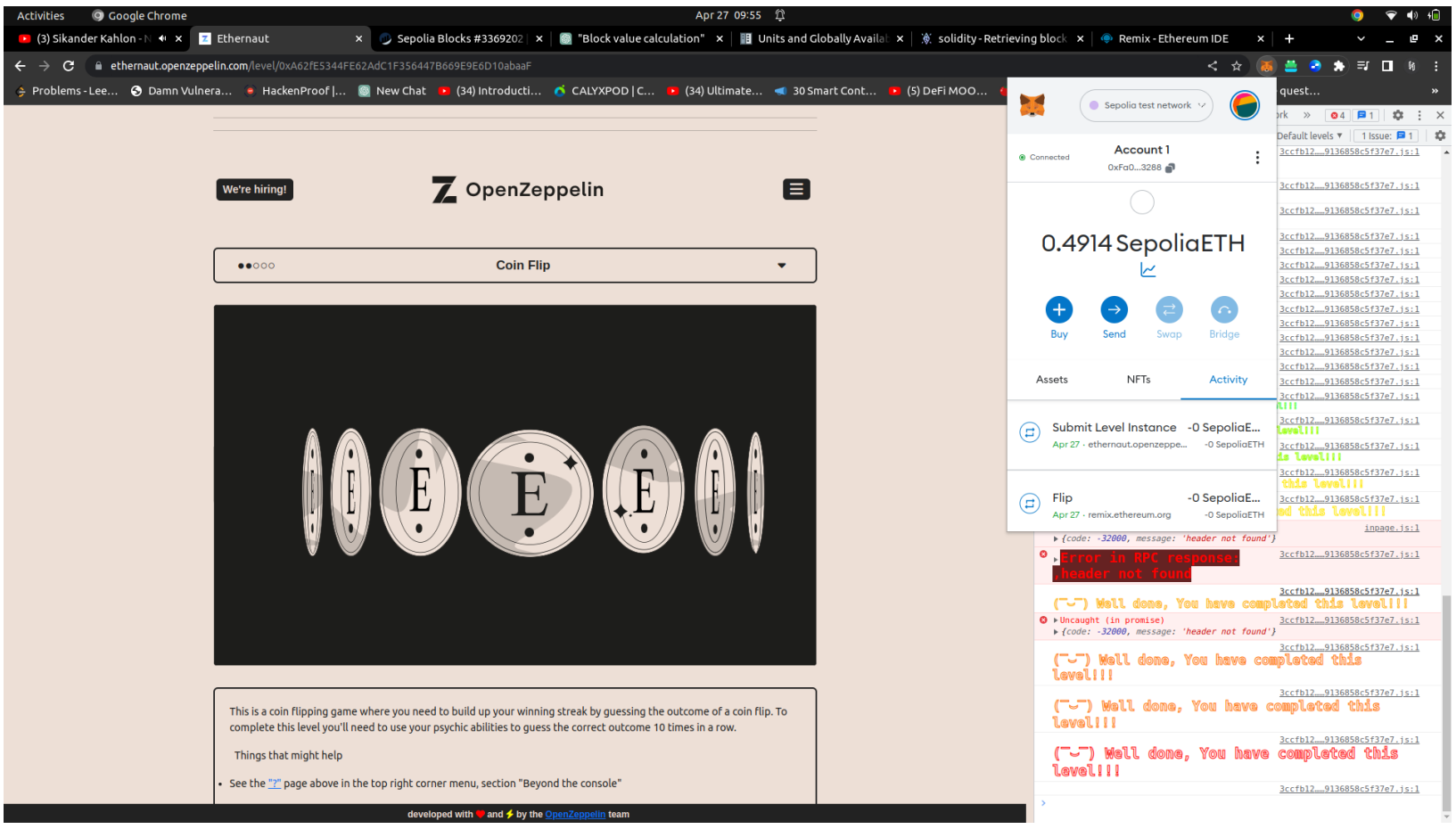
https://sepolia.etherscan.io/address/0xfa00d29d378edc57aa1006946f0fc6230a5e3288



First Three CTFs (Hello Ethernaut, Fallback, Fallout) were done in class itself.

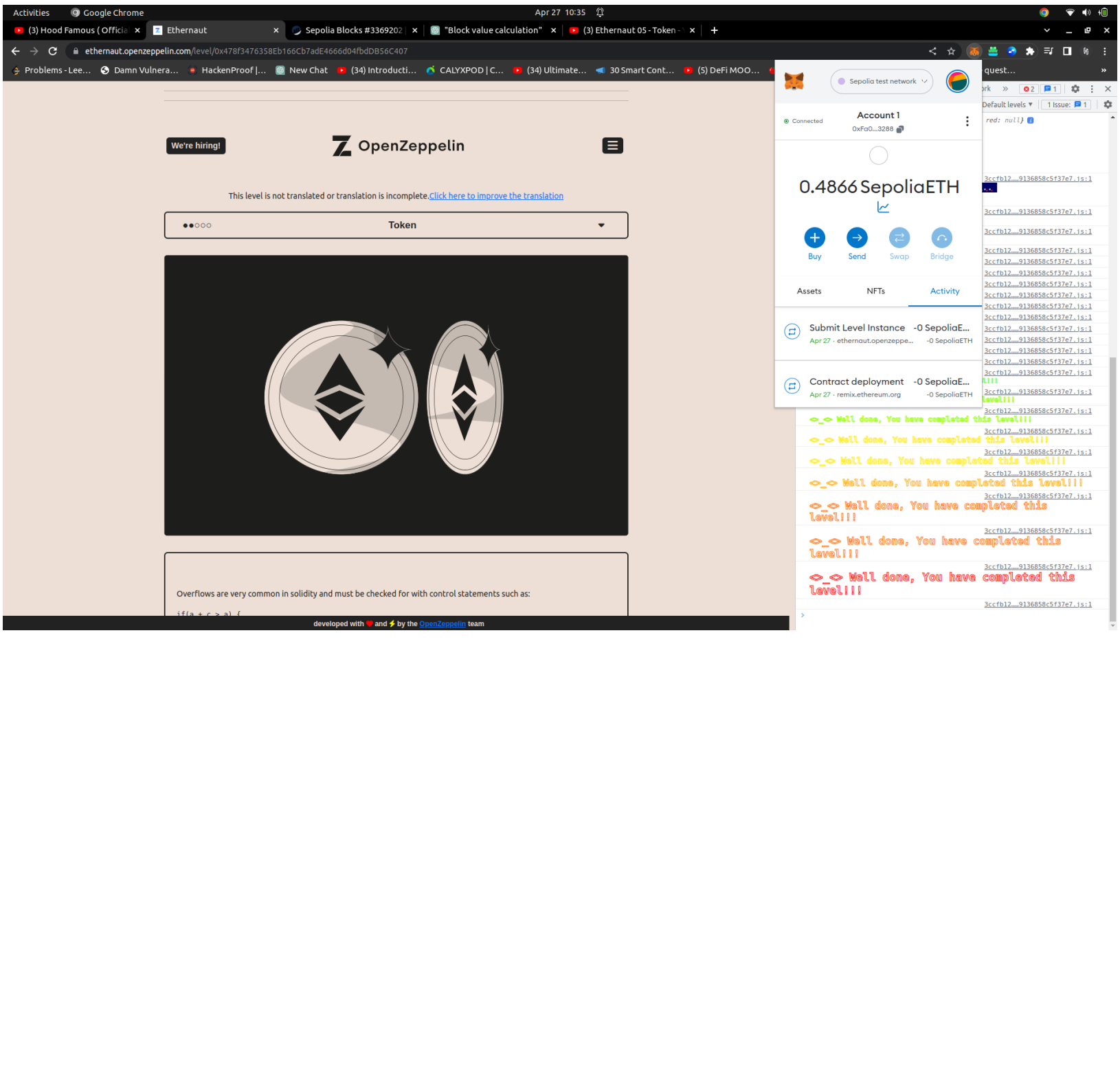


Coin Flip

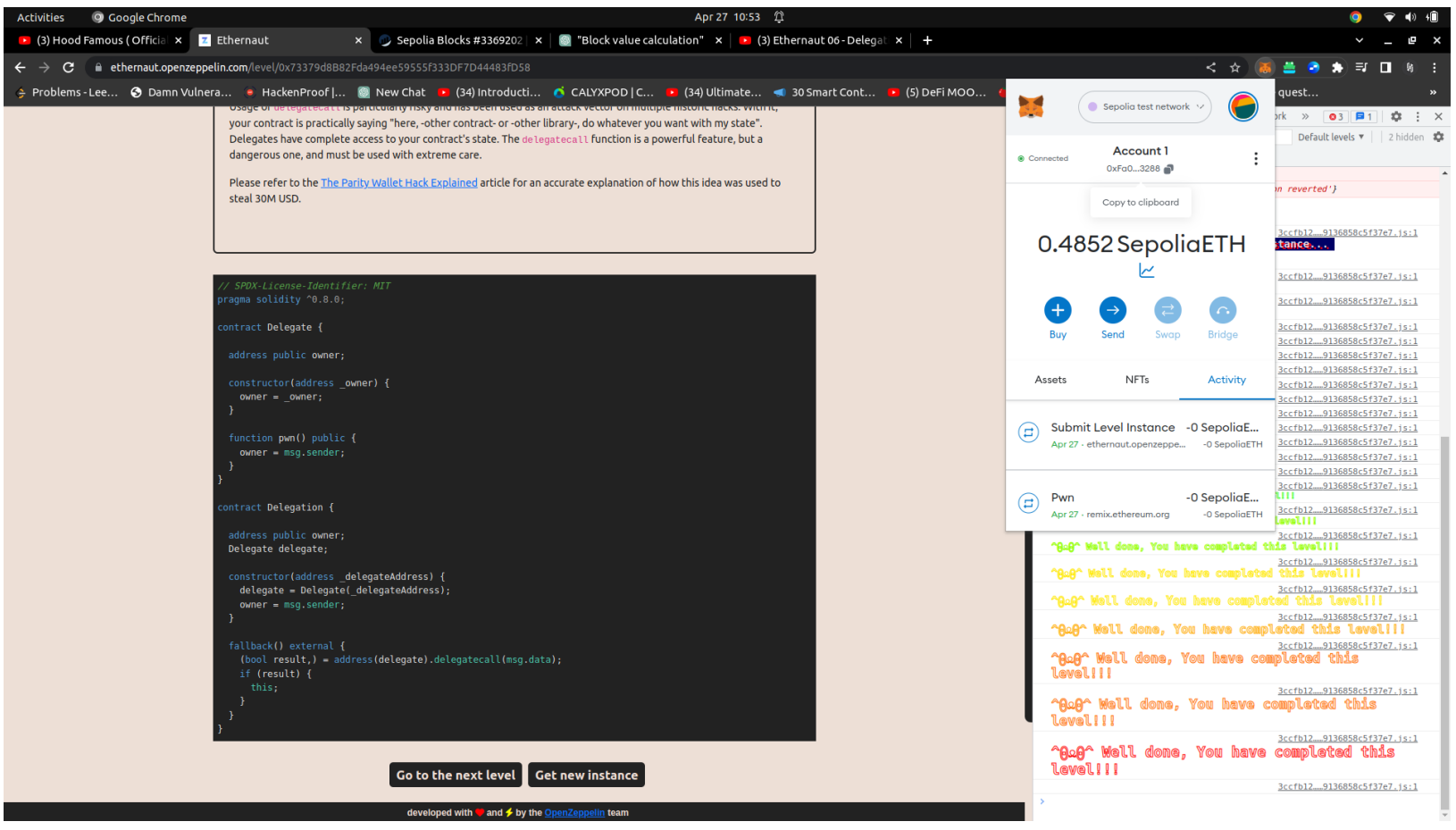


Telephone

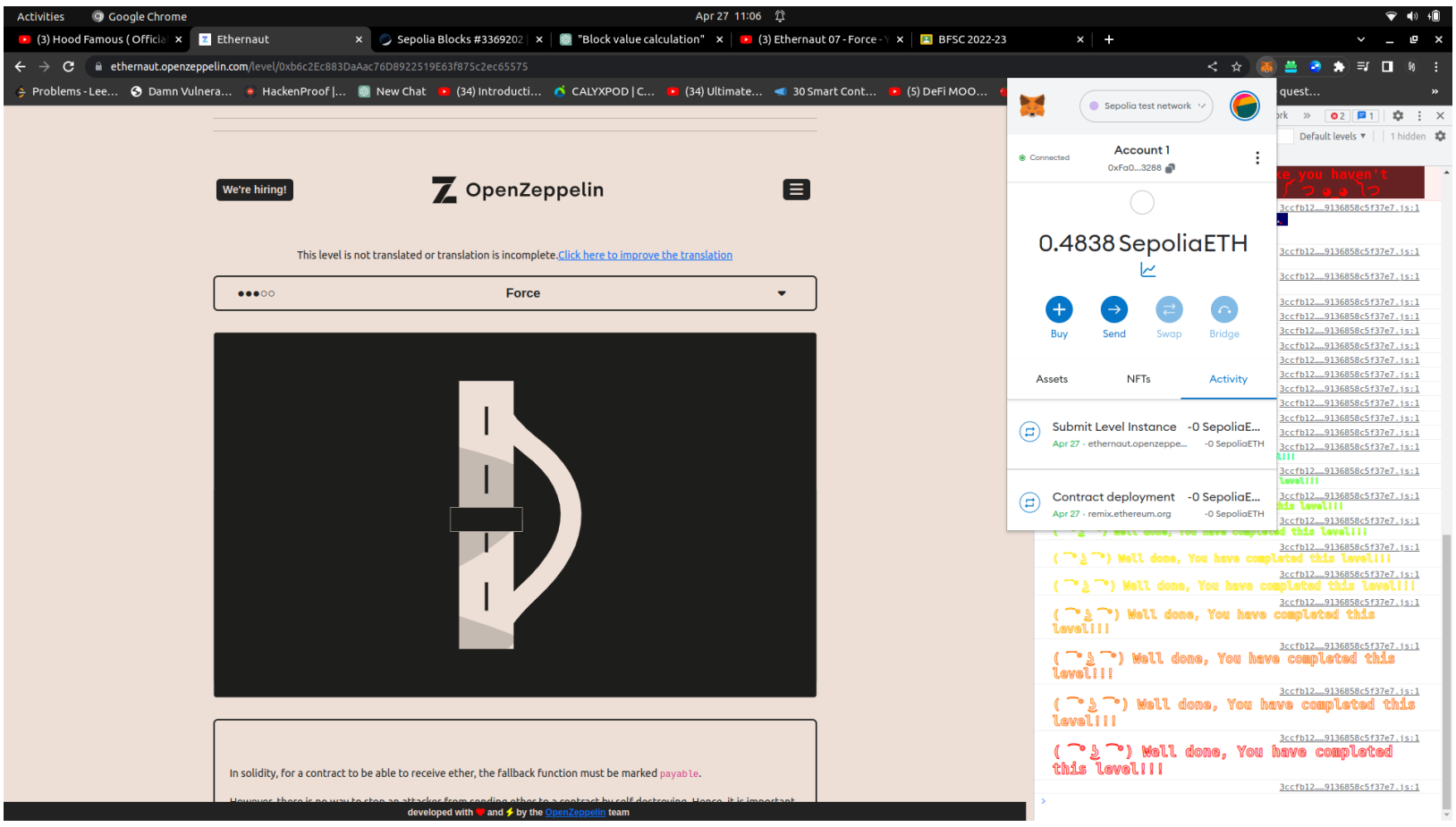
Token


Activities
Google Chrome
Apr 27 10:35
(3) Hood Famous (Officia
Ethernaut
Sepolia Blocks #3369202
"Block value calculation"
(3) Ethernaut 05 - Token -
ethernaut.openzeppelin.com/level/0x478f3476358Eb166Cb7adE4666d04fbdDB56C407
We're hiring!
OpenZeppelin
This level is not translated or translation is incomplete.Click here to improve the translation
Token
Overflows are very common in solidity and must be checked for with control statements such as:
developed with ❤ and ⚡ by the OpenZeppelin team
Sepolia test network
Account 1
0xFa0...3288
Connected
0.4866 SepoliaETH
Buy
Send
Swap
Bridge
Assets
NFTs
Activity
Submit Level Instance
-0 SepoliaE...
Apr 27 · ethernaut.openzeppe...
-0 SepoliaETH
Contract deployment
-0 SepoliaE...
Apr 27 · remix.ethereum.org
-0 SepoliaETH
<>_<> Well done, You have completed this level!!!

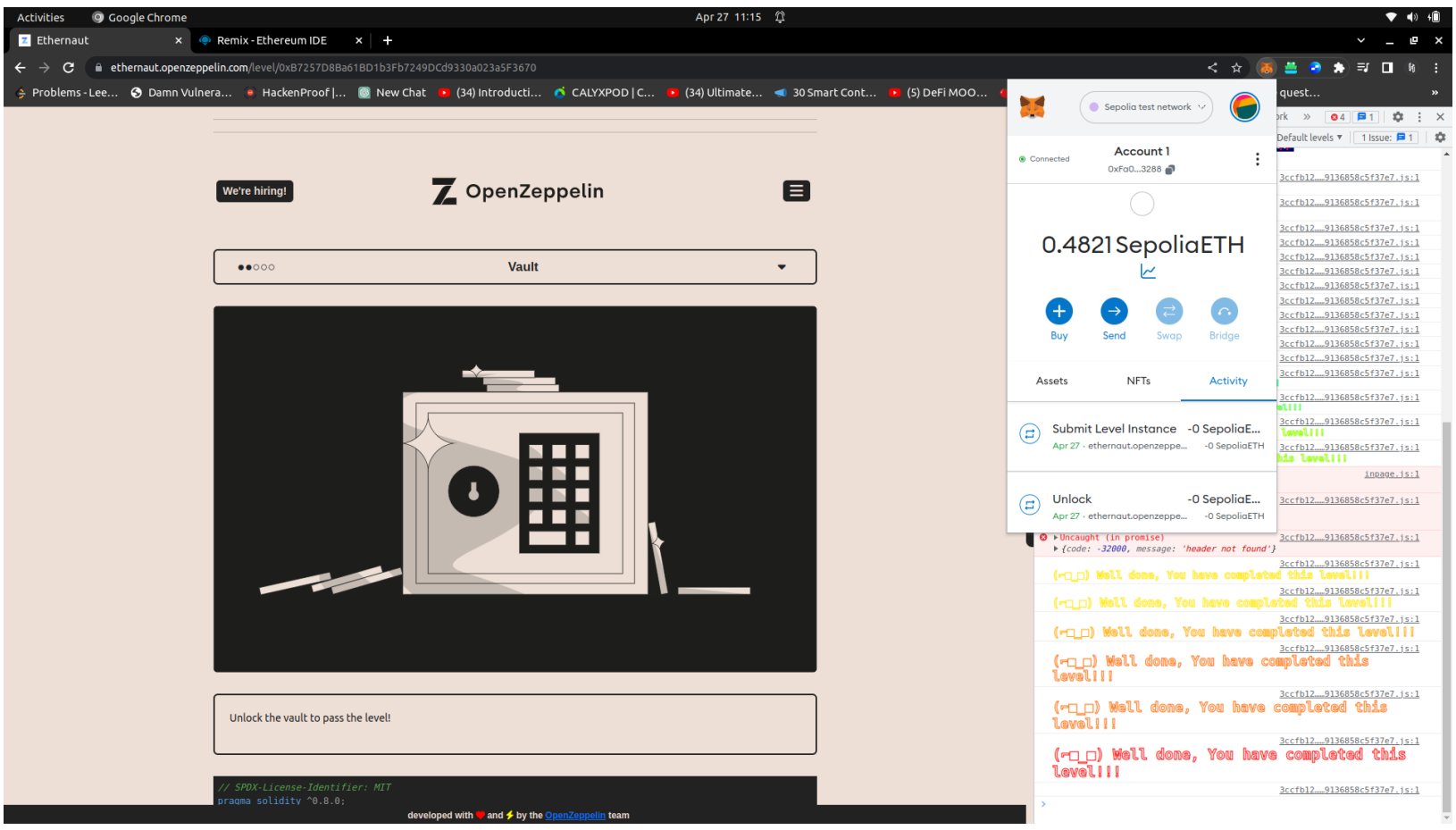
Delegation


Activities
Google Chrome
Apr 27 10:53
(3) Hood Famous (Officia
Ethernaut
Sepolia Blocks #3369202
"Block value calculation"
(3) Ethernaut 06 - Delegat
ethernaut.openzeppelin.com/level/0x73379d8B82Fda494ee59555f333DF7D44483fD58
your contract is practically saying "here, -other contract- or -other library-, do whatever you want with my state". Delegates have complete access to your contract's state. The delegatecall function is a powerful feature, but a dangerous one, and must be used with extreme care.
Please refer to the The Parity Wallet Hack Explained article for an accurate explanation of how this idea was used to steal 30M USD.
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract Delegate {
address public owner;
constructor(address _owner) {
owner = _owner;
}
function pwn() public {
owner = msg.sender;
}
}
contract Delegation {
address public owner;
Delegate delegate;
constructor(address _delegateAddress) {
delegate = Delegate(_delegateAddress);
owner = msg.sender;
}
fallback() external {
(bool result,) = address(delegate).delegatecall(msg.data);
if (result) {
this;
}
}
}
Go to the next level
Get new instance
developed with ❤ and ⚡ by the OpenZeppelin team
Sepolia test network
Account 1
0xFa0...3288
Connected
Copy to clipboard
0.4852 SepoliaETH
Buy
Send
Swap
Bridge
Assets
NFTs
Activity
Submit Level Instance
-0 SepoliaE...
Apr 27 · ethernaut.openzeppe...
-0 SepoliaETH
Pwn
-0 SepoliaE...
Apr 27 · remix.ethereum.org
-0 SepoliaETH
^_^ Well done, You have completed this level!!!

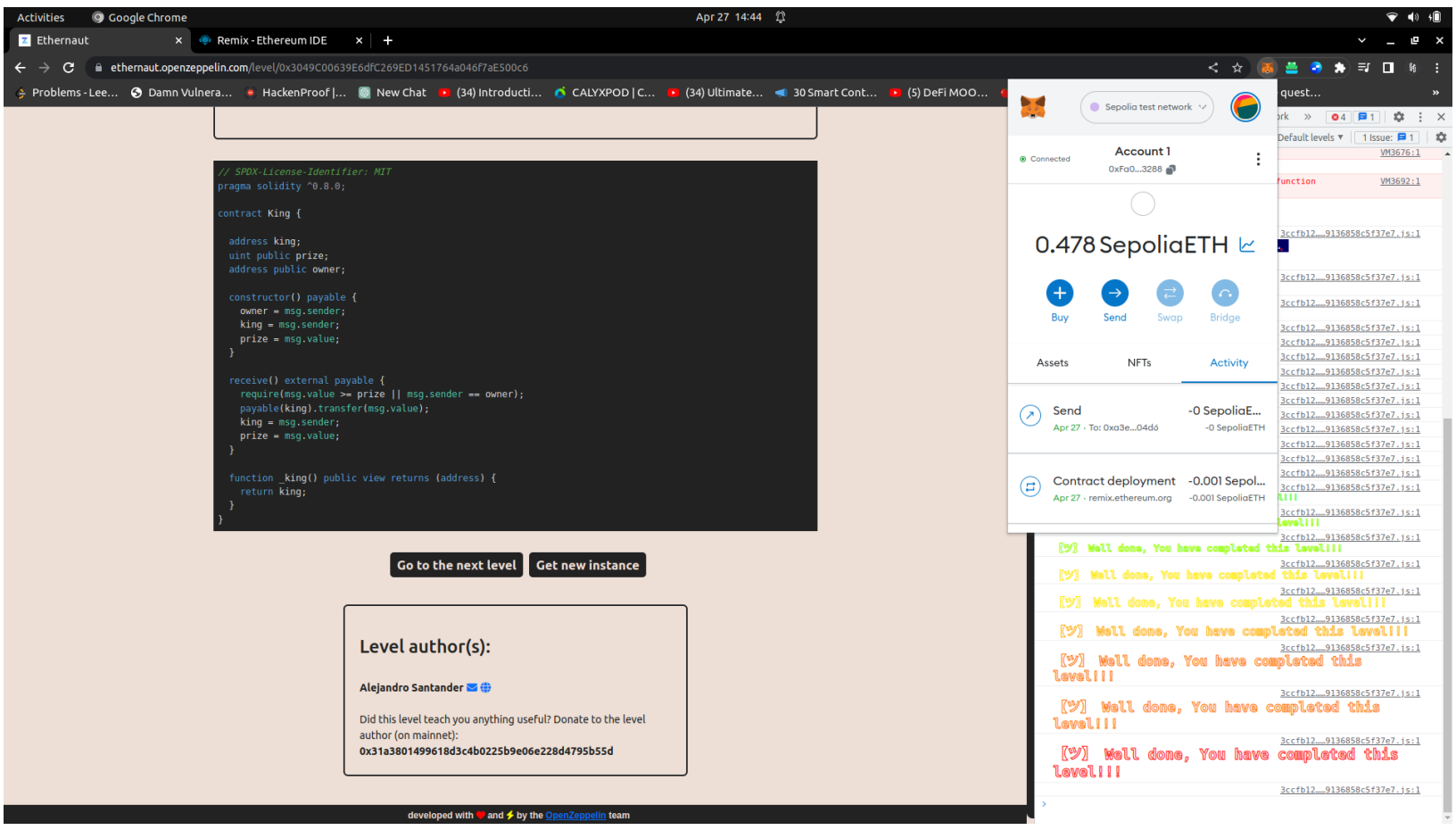
Force


Activities
Google Chrome
Apr 27 11:06
(3) Hood Famous (Officia
Ethernaut
Sepolia Blocks #3369202
"Block value calculation"
(3) Ethernaut 07 - Force -
BFSC 2022-23
ethernaut.openzeppelin.com/level/0xb6c2Ec883DaAac76D8922519E63f875c2ec65575
Problems - Lee...
Damn Vulnera...
HackenProof |...
New Chat
(34) Introducti...
CALYXPOD | C...
(34) Ultimate...
30 Smart Cont...
(5) DeFi MOO...
We're hiring!
OpenZeppelin
Force
This level is not translated or translation is incomplete.Click here to improve the translation
In solidity, for a contract to be able to receive ether, the fallback function must be marked payable.
developed with ❤ and ⚡ by the OpenZeppelin team
Sepolia test network
Account 1
0xFa0...3288
0.4838 SepoliaETH
Buy
Send
Swap
Bridge
Assets
NFTs
Activity
Submit Level Instance -0 SepoliaE...
Apr 27 · ethernaut.openzeppe... -0 SepoliaETH
Contract deployment -0 SepoliaE...
Apr 27 · remix.ethereum.org -0 SepoliaETH
Default levels
1 hidden
3ccfb12.....9136858c5f37e7.js:1
(͡° ͜ʖ ͡°) Well done, You have completed this level!!!

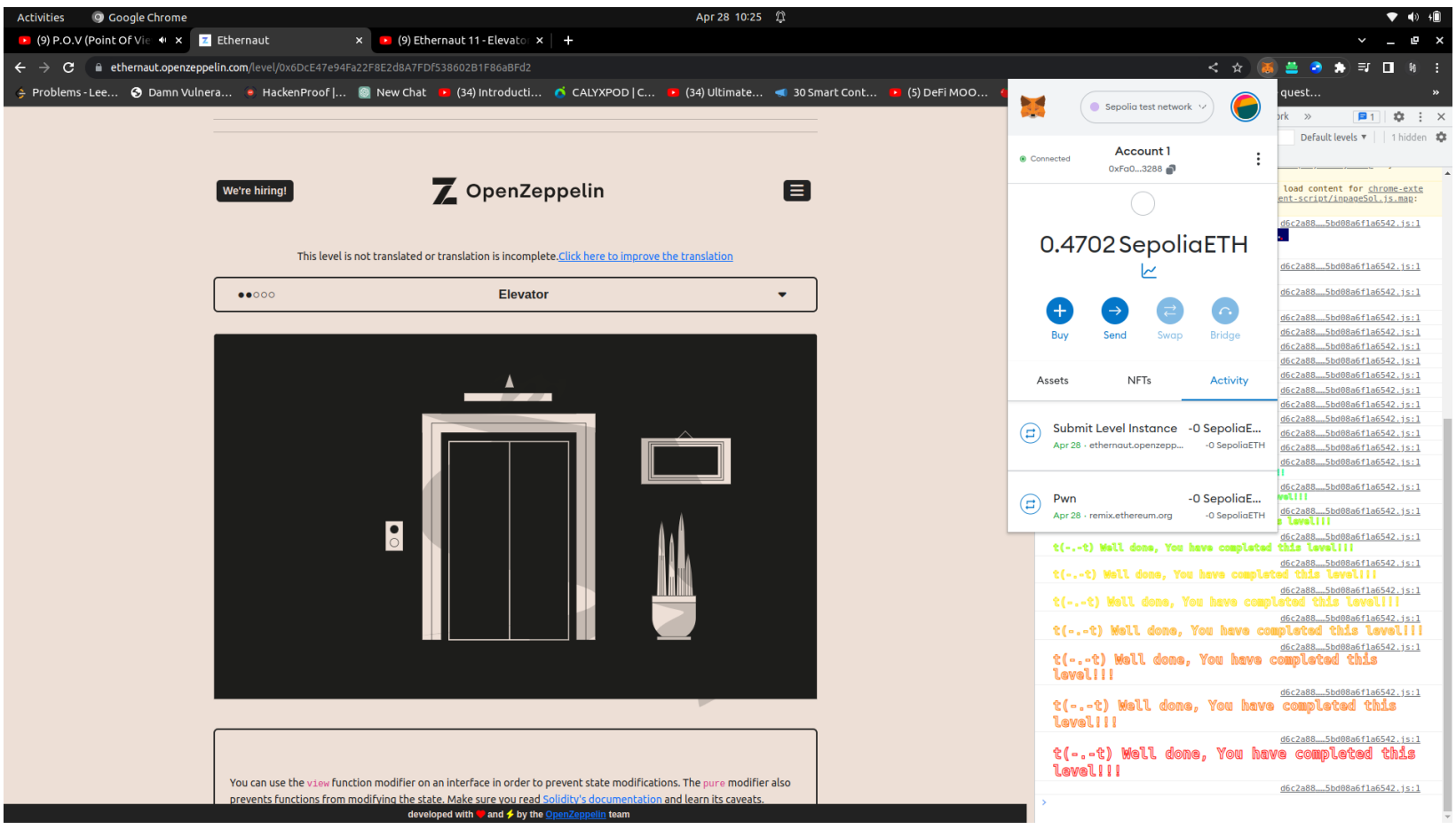
Vault


Activities
Google Chrome
Apr 27 11:15
Ethernaut
Remix - Ethereum IDE
ethernaut.openzeppelin.com/level/0xB7257D8Ba61BD1b3Fb7249DCd9330a023a5F3670
We're hiring!
OpenZeppelin
Vault
Unlock the vault to pass the level!
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
developed with ❤ and ⚡ by the OpenZeppelin team
Sepolia test network
Account 1
0xFa0...3288
Connected
0.4821 SepoliaETH
Buy
Send
Swap
Bridge
Assets
NFTs
Activity
Submit Level Instance
-0 SepoliaE...
Apr 27 · ethernaut.openzeppe...
-0 SepoliaETH
Unlock
-0 SepoliaE...
Apr 27 · ethernaut.openzeppe...
-0 SepoliaETH
Uncaught (in promise)
{code: -32000, message: 'header not found'}
(⌐□_□) Well done, You have completed this level!!!

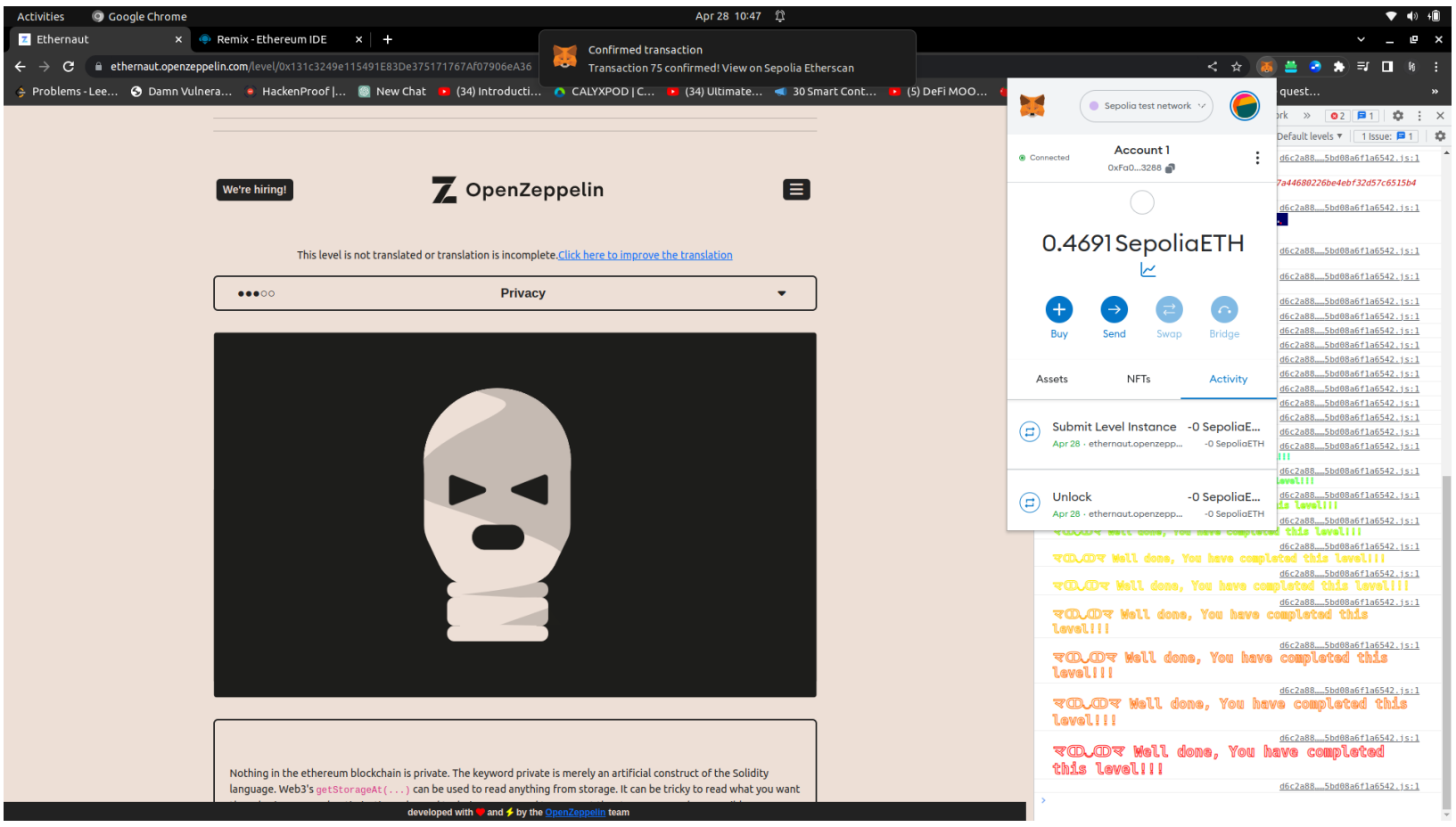
King


Activities
Google Chrome
Apr 27 14:44
Ethernaut
Remix - Ethereum IDE
ethernaut.openzeppelin.com/level/0x3049C00639E6dfC269ED1451764a046f7aE500c6
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract King {
address king;
uint public prize;
address public owner;
constructor() payable {
owner = msg.sender;
king = msg.sender;
prize = msg.value;
}
receive() external payable {
require(msg.value >= prize || msg.sender == owner);
payable(king).transfer(msg.value);
king = msg.sender;
prize = msg.value;
}
function _king() public view returns (address) {
return king;
}
}
Go to the next level
Get new instance
Level author(s):
Alejandro Santander
Did this level teach you anything useful? Donate to the level author (on mainnet):
0x31a3801499618d3c4b0225b9e06e228d4795b55d
developed with ❤ and ⚡ by the OpenZeppelin team
Sepolia test network
Account 1
0xFa0...3288
Connected
0.478 SepoliaETH
Buy
Send
Swap
Bridge
Assets
NFTs
Activity
Send
-0 SepoliaE...
Apr 27 · To: 0xa3e...04d6
-0 SepoliaETH
Contract deployment
-0.001 Sepol...
Apr 27 · remix.ethereum.org
-0.001 SepoliaETH
[ツ] Well done, You have completed this level!!!

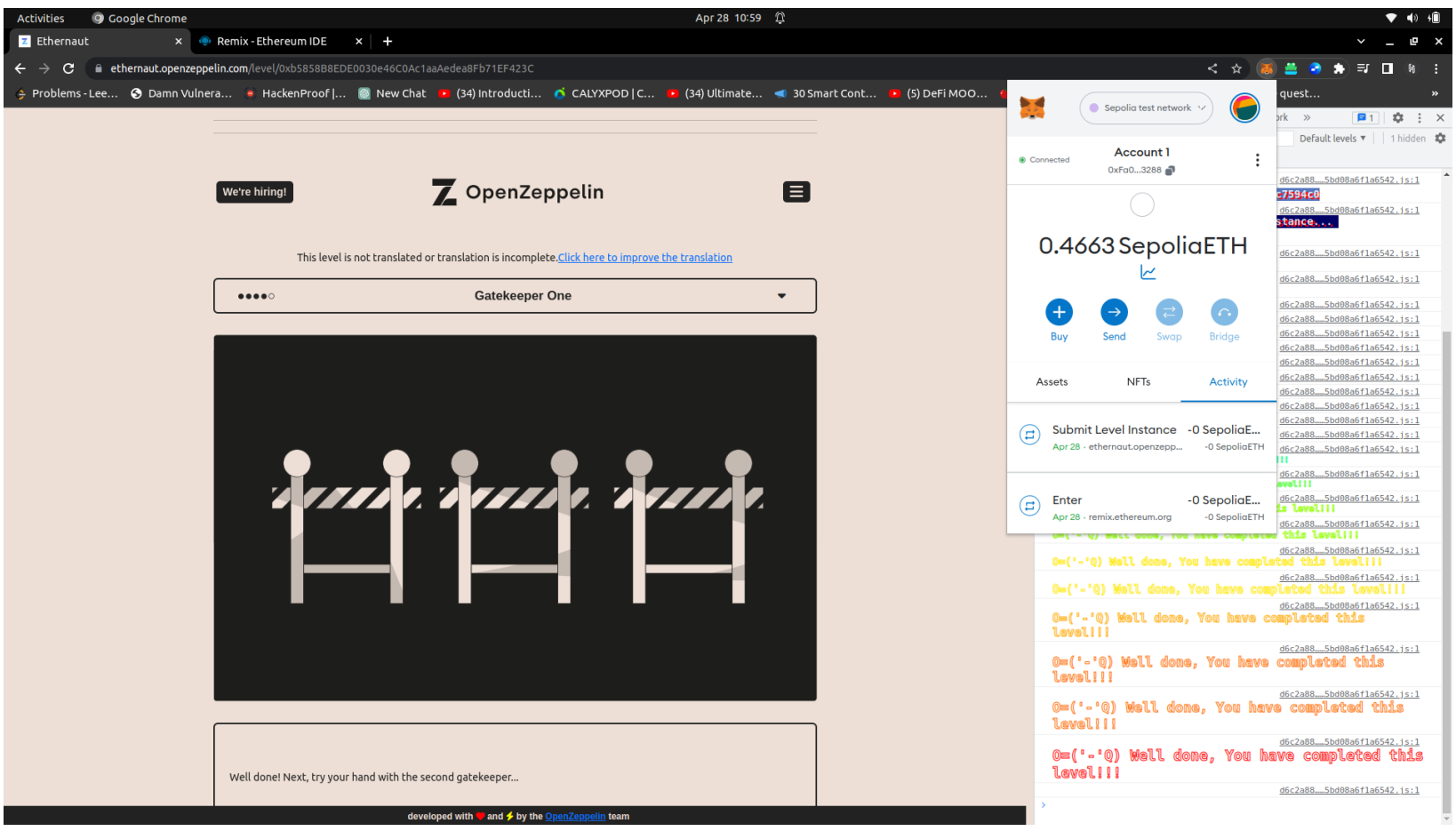
Elevator



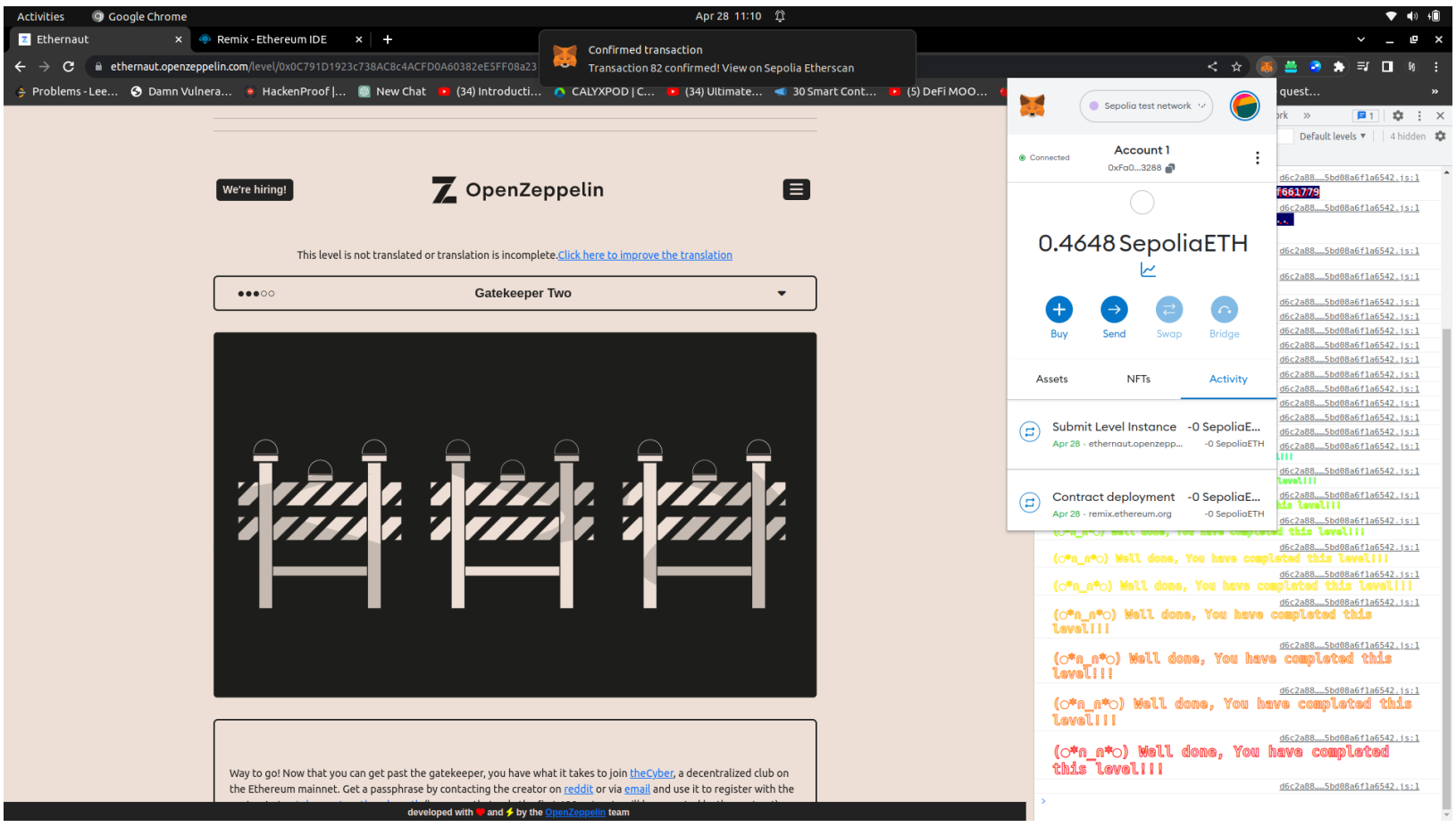
Privacy



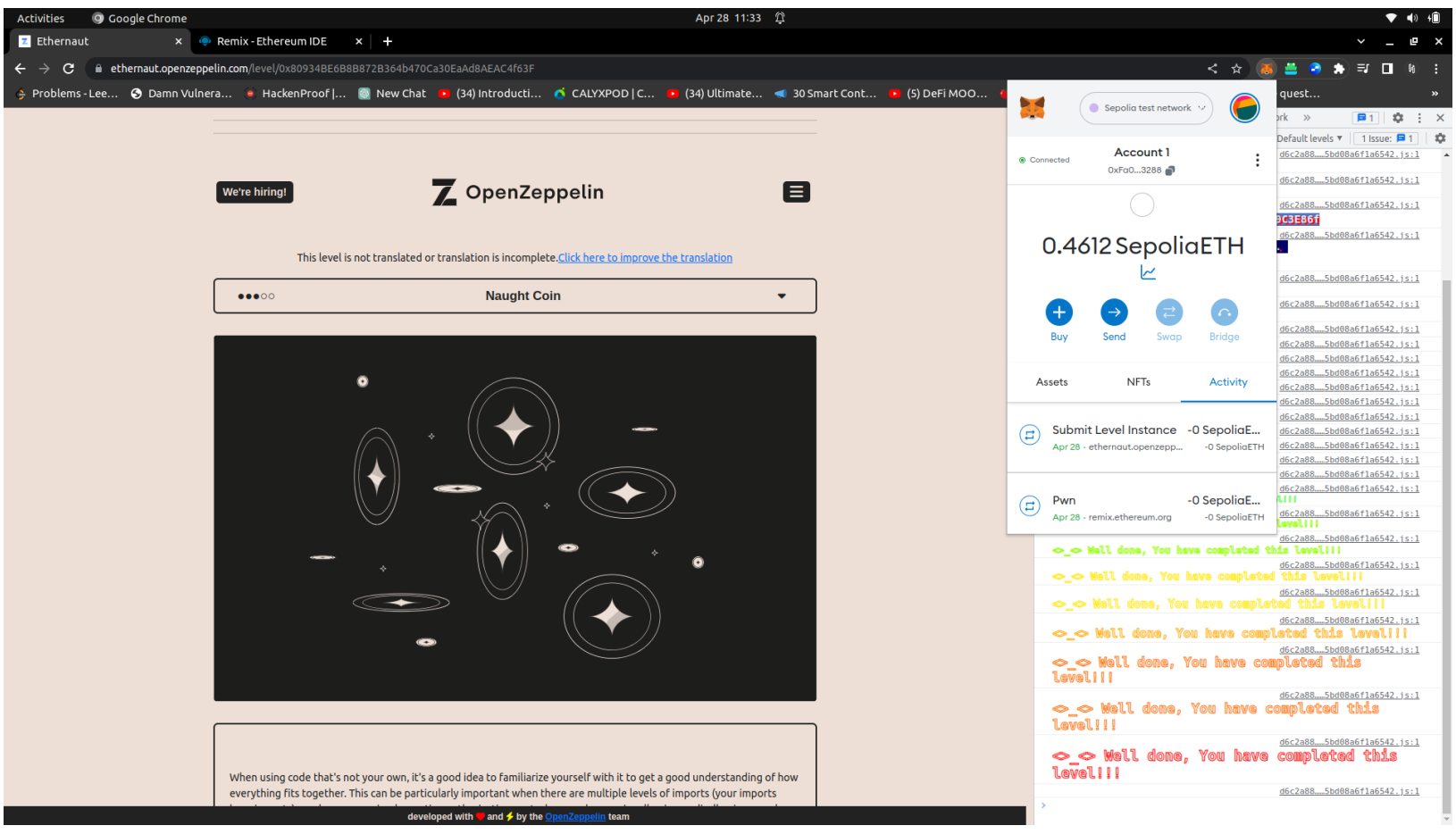
Gatekeeper One



Gatekeeper Two

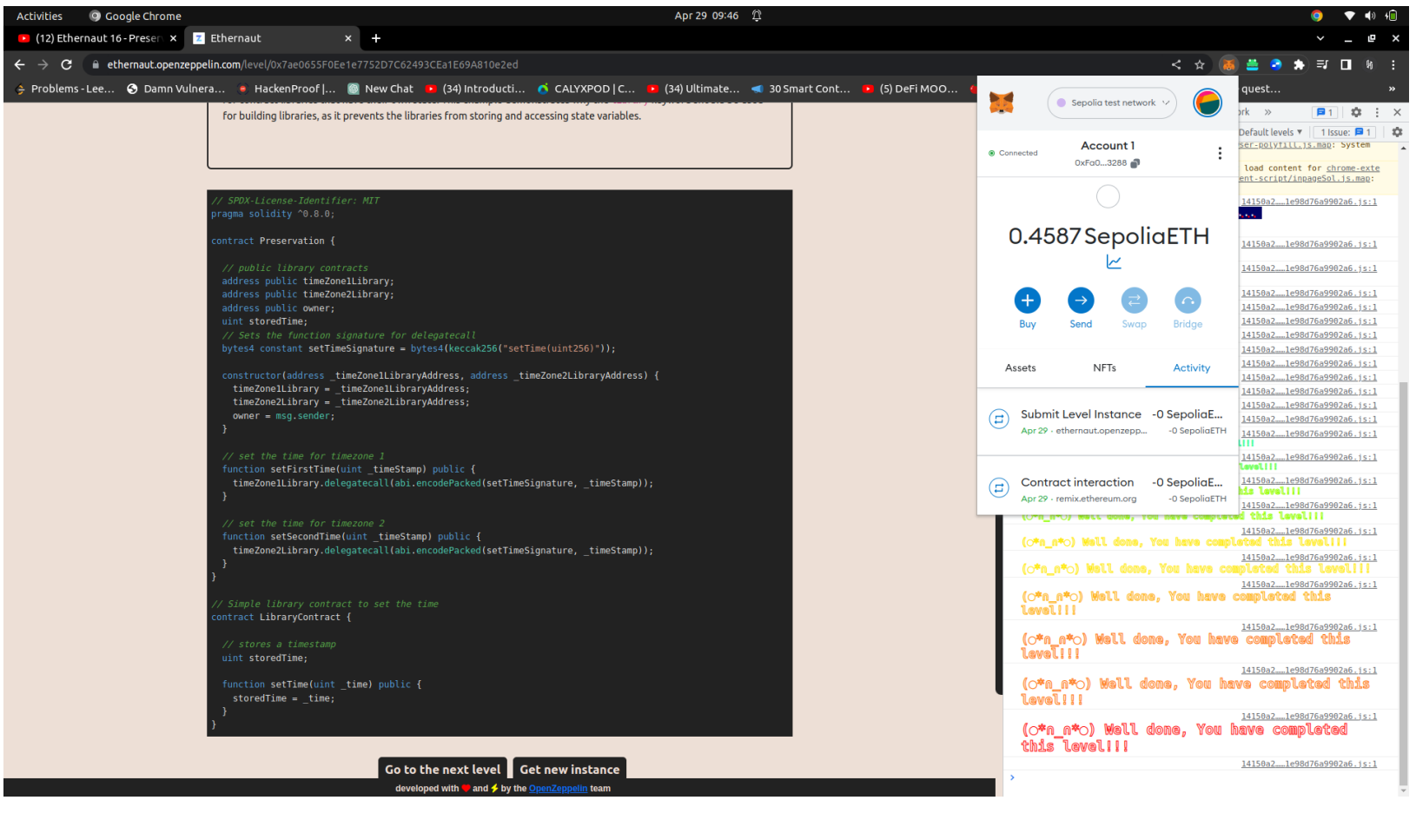


Naught Coin

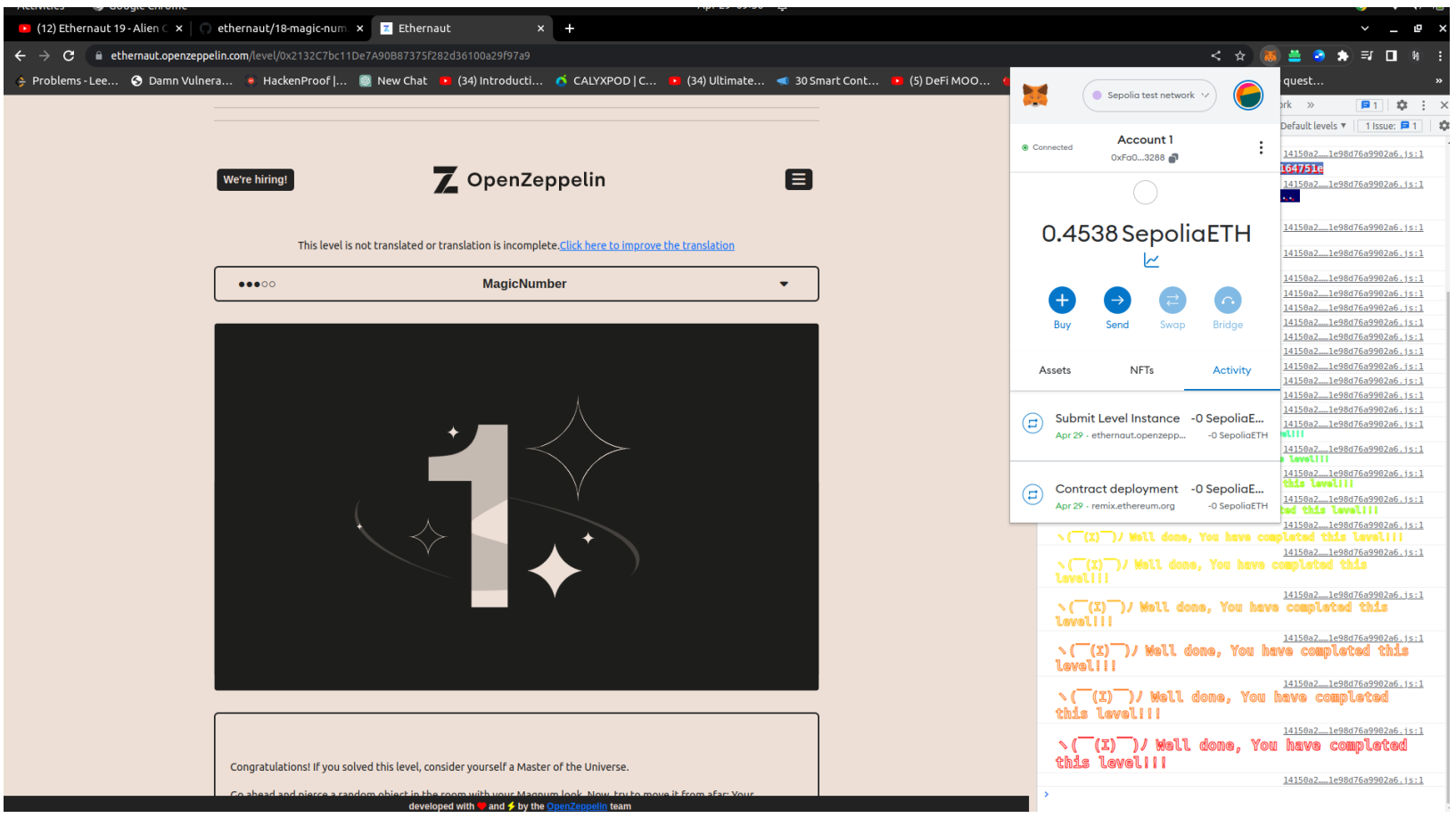


Preservation

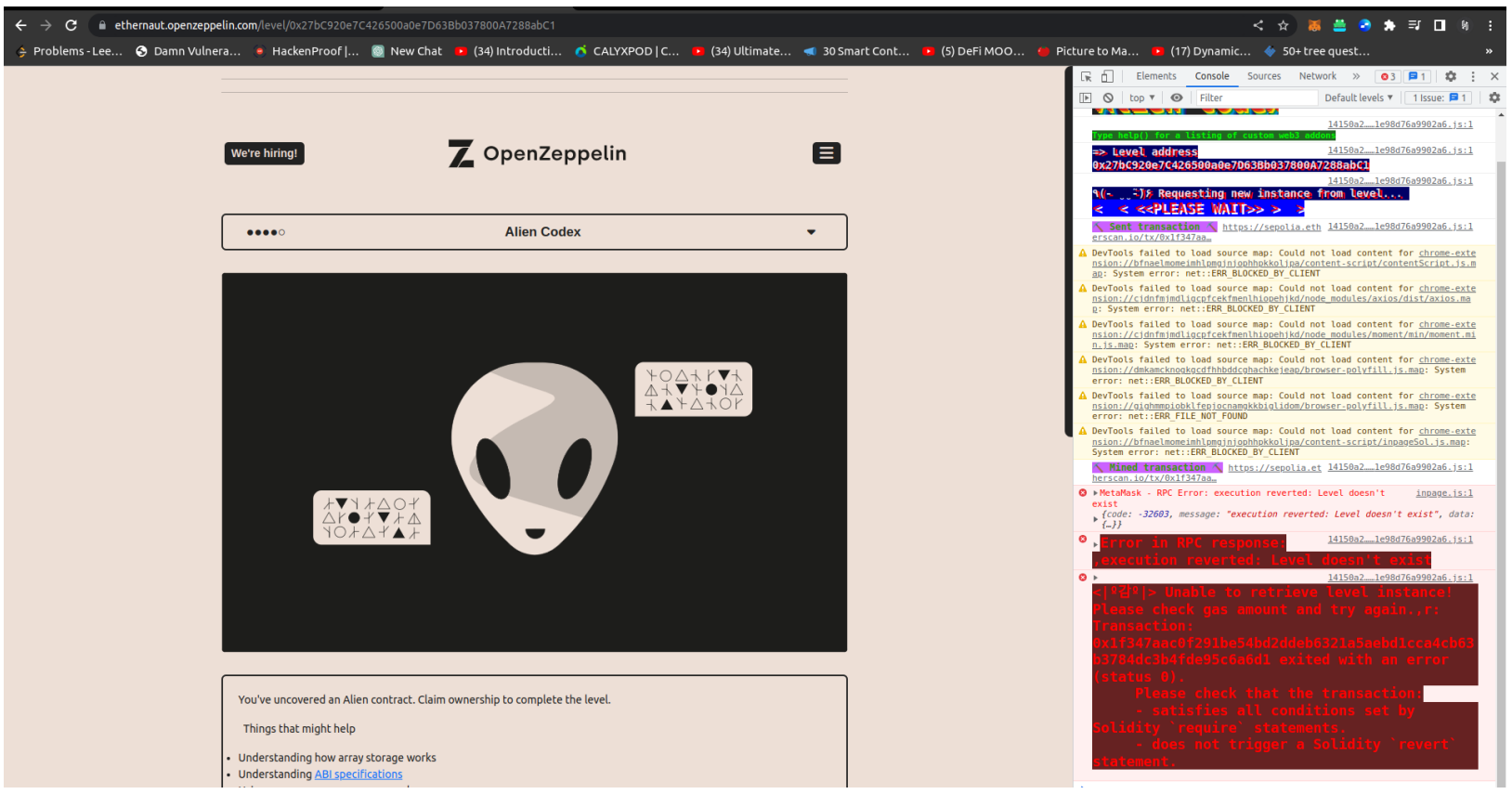
Recovery



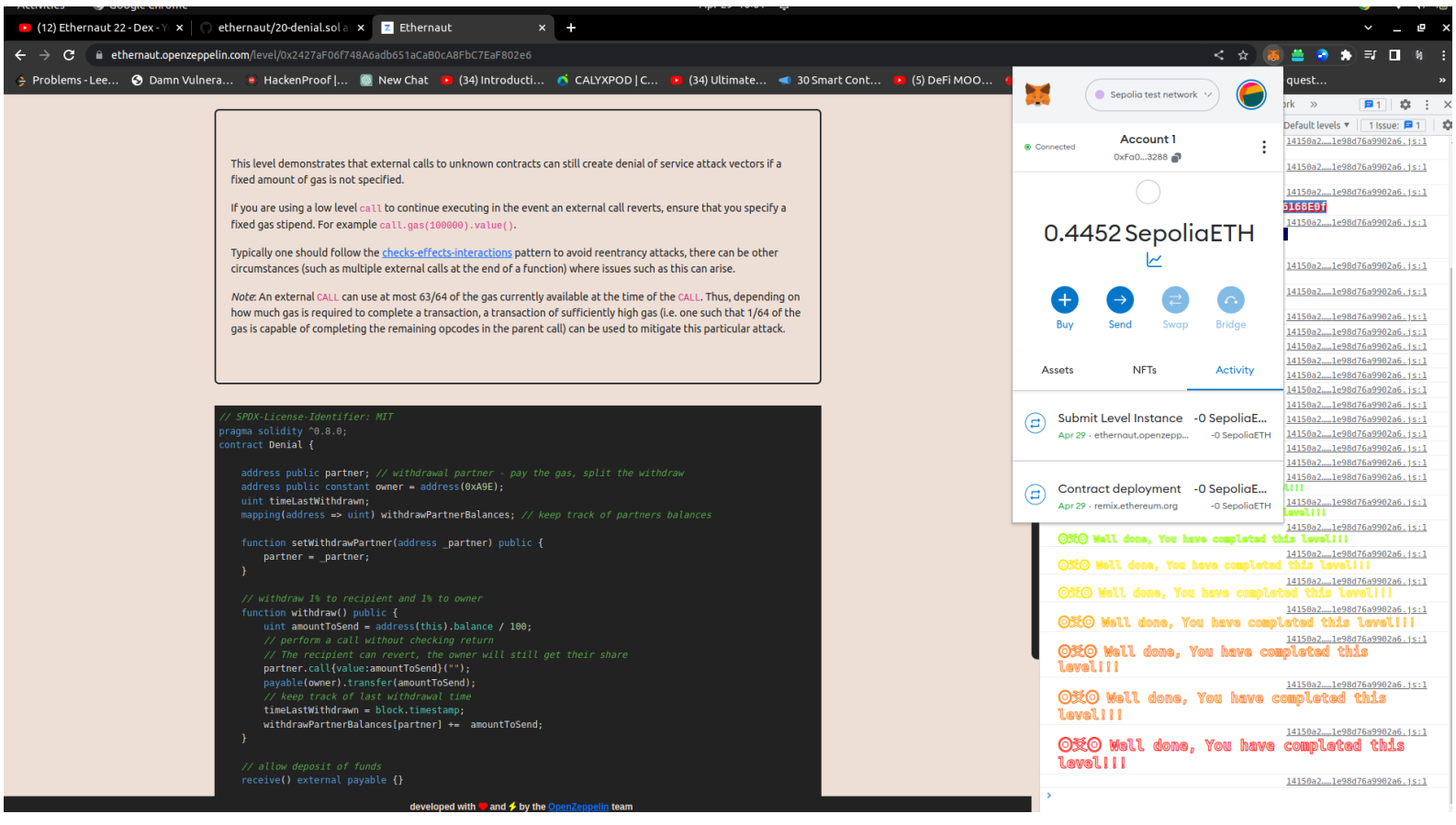
Magic Number



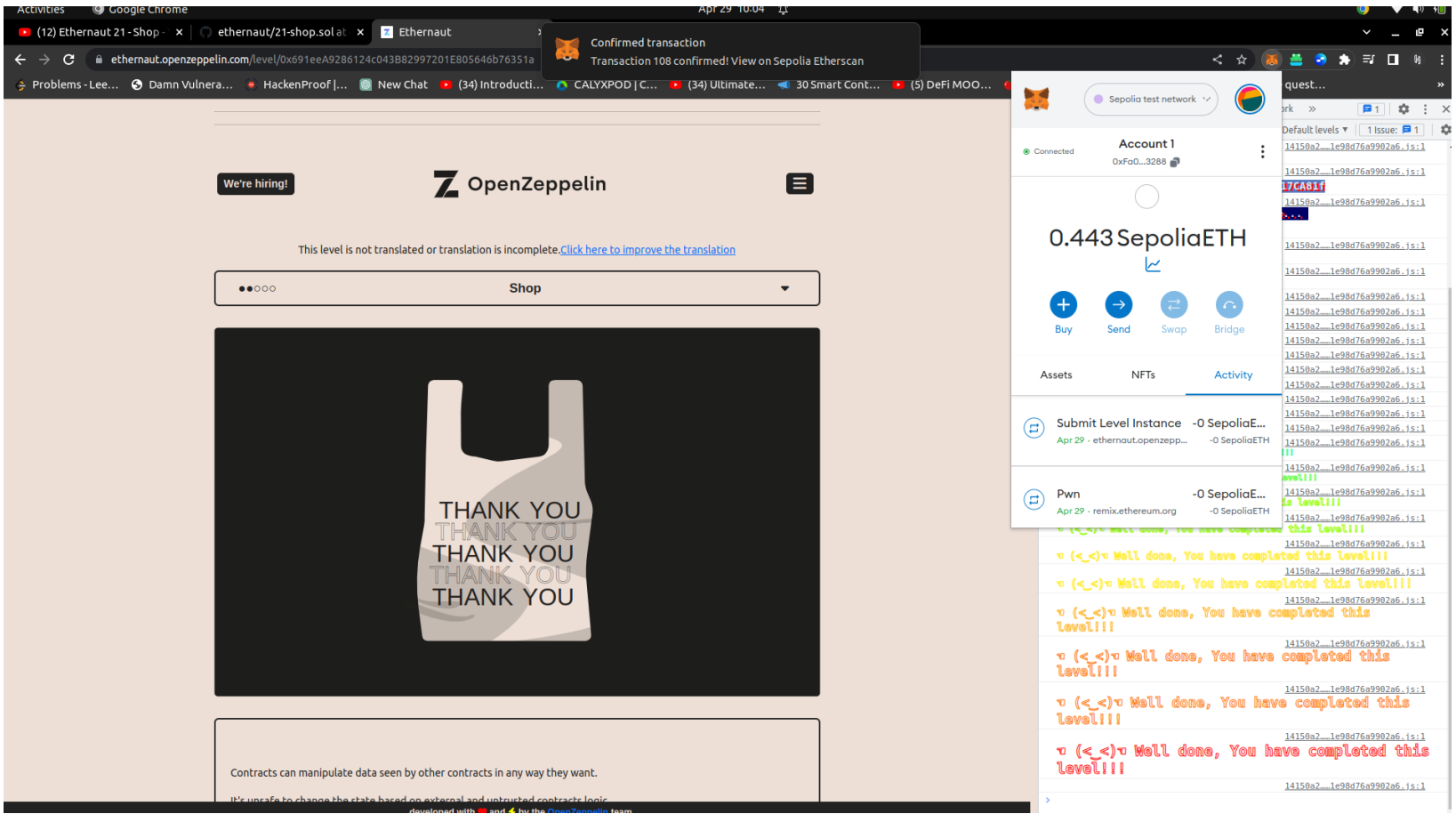
Alien Codex (Level doesnt Exist anymore)



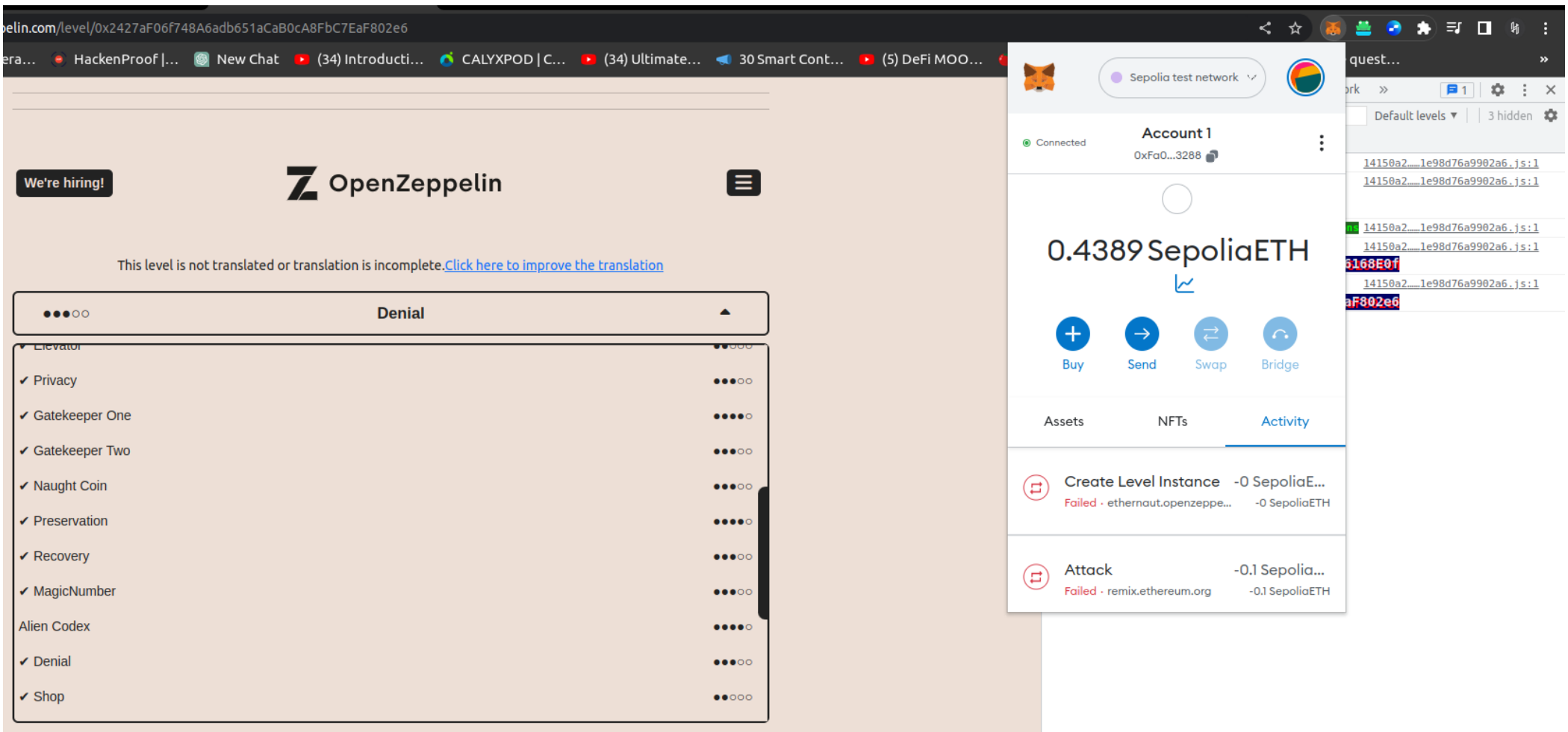
Denial



Shop

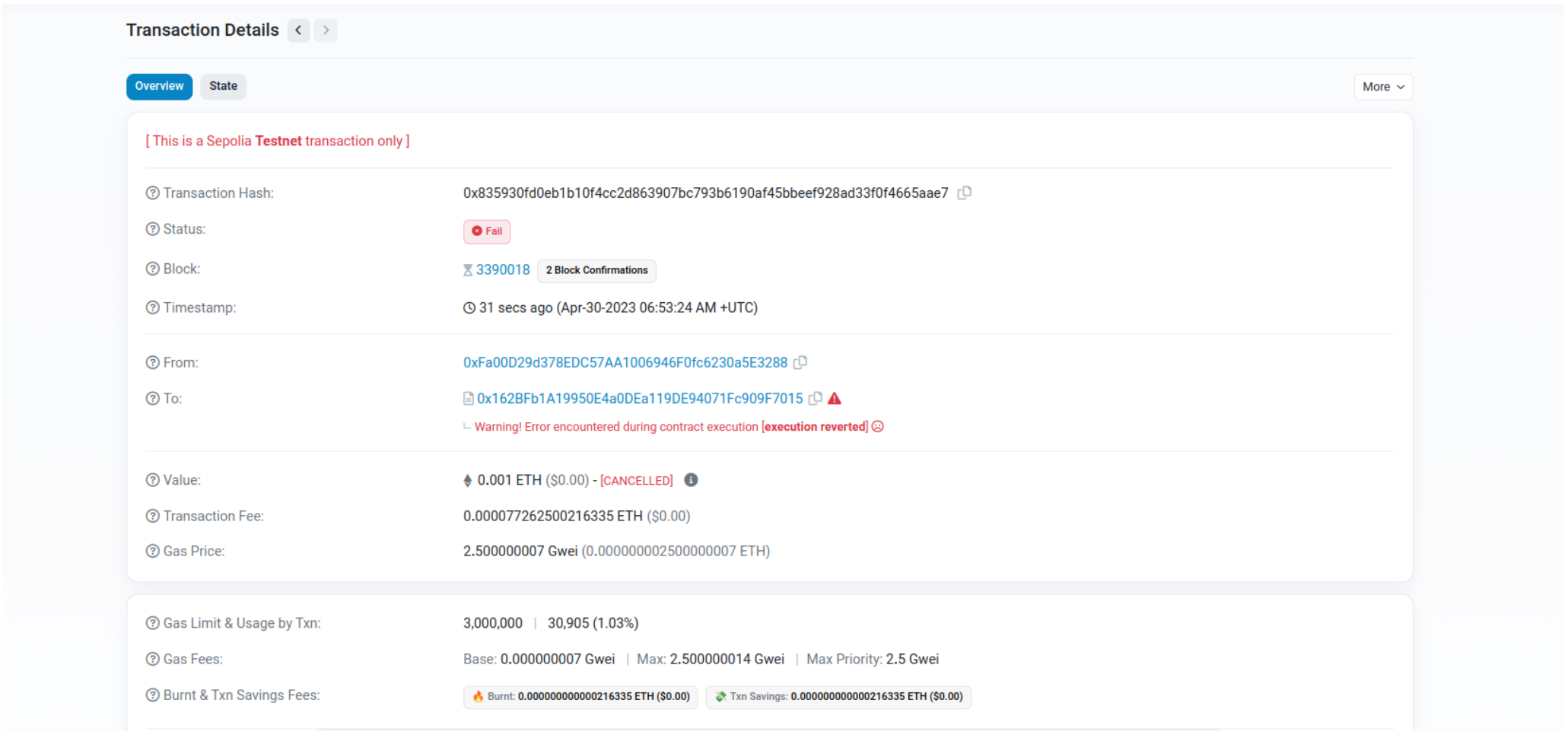


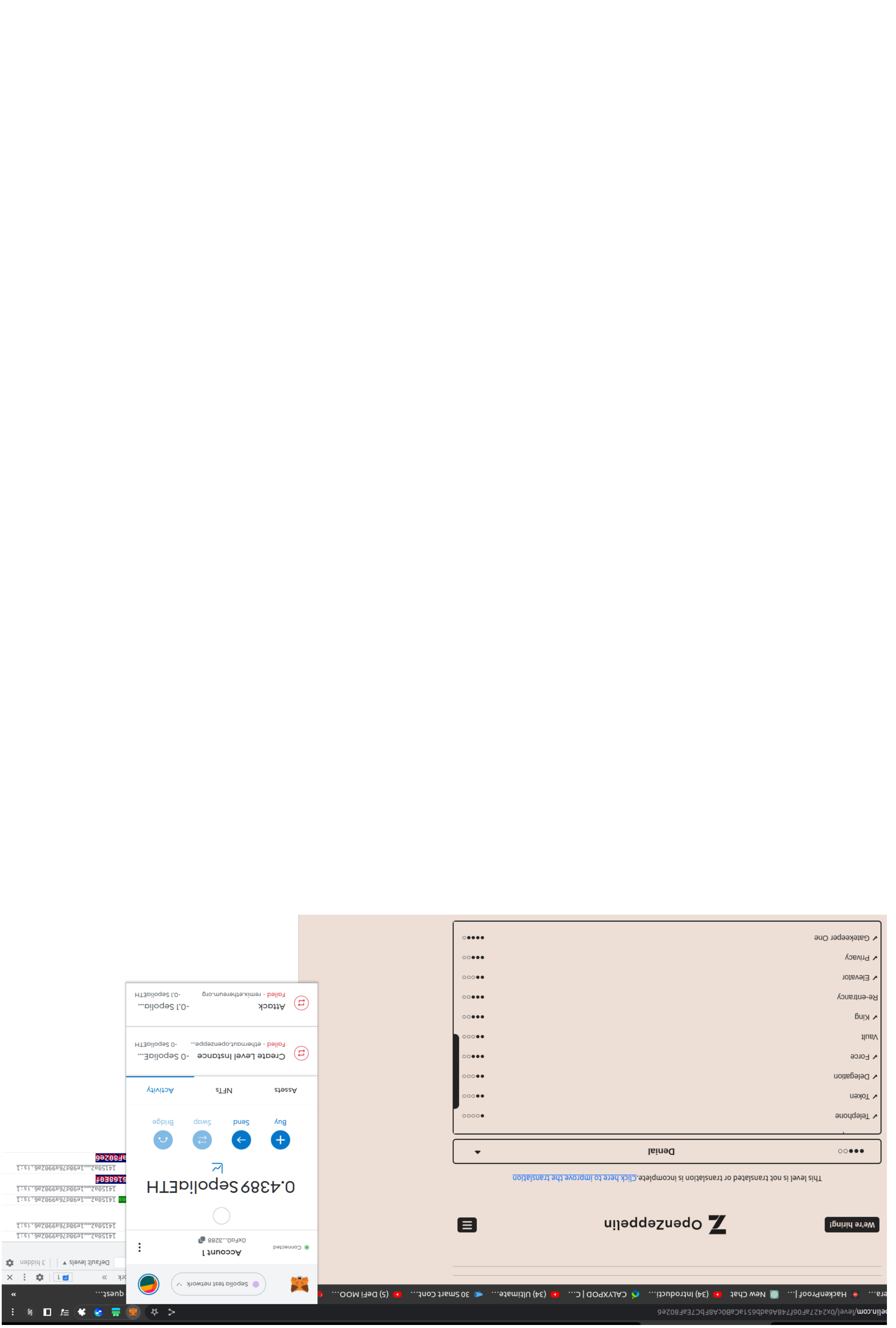
All Levels



Vault is Completed but for some reason it is not showing in navbar.

I was unable to do reentrancy my transactions kept on failing




elin.com/level/0x2427aF06F748A6adb651aCaB0cA8FbC7EaF802e6
Sepolia test network
Account 1
0xfa0...3288
Connected
0.4389 SepoliaETH
Buy
Send
Swap
Bridge
Assets
NFTs
Activity
Create Level Instance -0 SepoliaE...
Failed · ethernaut.openzeppe... -0 SepoliaETH
Attack -0.1 Sepolia...
Failed · remix.ethereum.org -0.1 SepoliaETH
Default levels
3 hidden
We're hiring!
Openzeppelin
This level is not translated or translation is incomplete. Click here to improve the translation
Denial
●●●○○
Telephone ●○○○○
Token ●●○○○
Delegation ●●○○○
Force ●●●○○
Vault ●●○○○
King ●●●○○
Re-entrancy ●●●○○
Elevator ●●○○○
Privacy ●●●○○
Gatekeeper One ●●●●○