Aave V1 & V2 come in which pattern?

I believe Aave uses the delegatecall proxy pattern.

Moderator | 02/14/2023

Any design pattern to have a truly upgradeable contract but guarantee functionality for users? Can we use registry for this?

By definition no but you can get close by restricting the upgradability to the absolute minimum required.

Moderator | 02/14/2023

Aren't there ricks with function selector clashes from contracts with simple function names?

yes but Transparent Proxies reduce the risk,

Moderator | 02/14/2023

Aren't, you supposed to call initialize on deploying?

If you using a plugin it will call it for you if you are not then yes you will need to call it manually.

Moderator | 02/14/2023

Can access to the admin account be restricted by a multi-sig or dao to decrease trust? Is this common?

Yes this is possible and there are some good docs here:
https://docs.openzeppelin.com/defender/guide-upgrades

Moderator | 02/14/2023

Can we embed Yul in Soldiity?

Yes you can use assembly { } to embed assembly into solidity or you can write pure yul contracts.

Moderator | 02/15/2023

Could you briefly repeat difference between the notation and the assembly code? whats the 00: 6080... a little confused

00: 6080 PUSH1 0×80 / 00: would be the program counter. 6080 is the two bytes the EVM uses. 60 would be the opcode the evm understands , 80 is the value. Then push1 is the opcode name that easy to read and 0×80 the value. So two different ways of representing the same thing

Moderator | 02/15/2023

Does anyone have an example of post-merge randomness that's secure? Thanks.

VRF for sure. We are researching using randao as source of randomness

Fox Reymann | 02/13/2023

Does operator pop from top of stack, or does it look in so that the top remain unchanged and then the return value goes on top of the inputs?

No it doesn't technically pop the items from top of stack but effect is similar in that it cleans up the items as it operates on them.

Moderator | 02/15/2023

Good resource to understand complex storage better https://programtheblockchain.com/posts/2018/03/09/understanding-ethereum-smart-contract-storage/

Nice :)

Moderator | 02/15/2023

Hey. Would individual strings be limited to 32bytes?

no, they would be stored in multiple slots, like arrays

Fox Reymann | 02/13/2023

How can we differentiate between the PUSH opcode that pushes a memory location and the one that pushes a value to the stack?

You have to read the stack and understand the number of arguments and order of arguments of an opcode and work it out.

Moderator | 02/15/2023

How can we envision deploying a contract, setting a state variable & getting a state variable in the stack terminology?

we are going through contract deployment opcodes in later lesson, step by step. this video https://www.youtube.com/watch?v=yxgU80jdwL0&t=899s shows storing a state variable going through stack and opcodes

Fox Reymann | 02/13/2023

How do we calculate the 0x27 and 0xb6?

The compiler will calculate for you.

Moderator | 02/15/2023

how is CREATE2 used for upgrades then? Won't the bytecode be necessary different as you're upgrading? Do you then have to 'bruteforce' using the salt?

Yes this is true but it's still useful for deterministic addresses. For example you can deploy on multiple networks & the address will be the same.

Moderator | 02/14/2023

How is msg.sender 'stored' under delegatecall? Is it part of calldata?

It's part of the global variables and store in the global scope
https://docs.soliditylang.org/en/v0.8.18/units-and-global-variables.html

Moderator | 02/14/2023

I had the 'Stack too deep' error. I had a struct with 14/15 variables. I removed 2-3 from the struct and the error disappeared. Any info on this would be great!

Contract can only work on 16 slots in stack. Your 14-15 variables + other opcodes needed to process to program must have run over 16. You've removed some variables and then it

could execute.

Fox Reymann | 02/13/2023

I saw yesterday in audit competition restriction to use assembly code. Why would the project to keep their code completely done in solidity?

Hard to say without seeing it might be that when writing assembly you have more scope to optimise gas but it's harder to keep the code secure. Maybe they want to focus on security not gas optimisation?

Moderator | 02/16/2023

If a delegate call loads the implementation contract onto the main contract? what the effect of that on gas?

Calling the implementation will cost more gas but the execution of the actual function will be the same.

Moderator | 02/14/2023

If operator comes last, how does pc know which byte is the operator (if it doesn't know how many / what size) operands?

The opcode takes a fix amount of arguments and will take from top of the stack.

Moderator | 02/15/2023

In account storage, is key 1 start from 0 and increases by 1. So key 1 is 1, key 2 is 2 and so on?

The key would be the address of the account. If I understood your question correctly.

Moderator | 02/15/2023

In the above example(adding nums), does result need to be stored in memory if it is just being loaded from memory in the next line and returned to the function?

Potentially not, it's mostly there for illustration purposes in the examples.

Moderator | 02/15/2023

Is storing data in mappings cheaper than structs? Say storing 8 uint256 in struct vs 8 uint256 in mapping(uint256 => uint256)

It CAN be cheaper to use structs depending on how many mappings you have. Best thing is to try it and see. For a single mapping probably not. Here a good article: https://medium.com/@novablitz/storing-structs-is-costing-you-gas-774da988895e

Moderator | 02/14/2023

Is there a plugin for upgradeability via foundry?

Not officially. People talked about handling it by writing foundry scripts. There is also a non official plug in. Haven't personally tested it though: https://github.com/odyslam/foundry-upgrades/

Moderator | 02/14/2023

Is there a way to see on etherscan how the contract was deployed and whether it was "rewritten" via CREATE2?

Yes ...
Example:https://etherscan.io/tx/0×8733fe2859afb044abe28859e71486d24758706320fdf47eb280c5fbc9bee51f#internal

Moderator | 02/14/2023

Is there any tool like 'hardhat-gas-reporter' but for memory?

I don't know of one but gas cost should indirectly be a proxy for memory usage. That is if you use less memory you should use less gas.

Moderator | 02/15/2023

is Yul the same as assembly?

Yul is an intermediate programming language that can be used to write a form of assembly language inside smart contracts. So it give us the best of solidity and assembly. So no it's not the same but it allows us to write code very similar to assembly but with more flexibility and a bit more higher level features.

Moderator | 02/15/2023

isn't it practically impossible to bruteforce 256bit hash?

yes

Moderator | 02/14/2023

Looking at the Homework for Lesson3 exercise 3. Is there a way to use the debugger with foundry instead of remix?

Yes

Fox Reymann | 02/13/2023

on page 10, I noticed "Code" is listed as one of the areas where data can be stored. Can you provide more information on how exactly data is stored in code?

check sstore2 project on github: https://github.com/0xsequence/sstore2 .

Fox Reymann | 02/13/2023

The data contract can also be upgraded too, right?

yes but it's difficult to migrate the data.

Moderator | 02/14/2023

Then is there a bright future for diamond pattern if somebody makes it A) less complex, B) with better terminology?

Potentially, Don't write it off ,just be aware of the trade offs.

Moderator | 02/14/2023

What gets stored in calldata? What is calldata used for?

method parameters that won't change during exectution

Fox Reymann | 02/13/2023

What is RLP in transaction?

Recursive Length Prefix (RLP) https://ethereum.org/en/developers/docs/data-structures-and-encoding/rlp/

Fox Reymann | 02/13/2023

What is RLP used for?

RLP standardizes the transfer of data between nodes in a space-efficient format. The purpose of RLP is to encode arbitrarily nested arrays of binary data, and RLP is the primary encoding method used to serialize objects in Ethereum's execution layer. The only purpose of RLP is to encode structure;

Fox Reymann | 02/13/2023

What is the reason for duplicating the value using the DUP opcode?

Because we need to use the value twice.

Moderator | 02/15/2023

What sort of information is stored in the stack?

all data used during actual prorgram processing - data, memory storage etc. locations

Fox Reymann | 02/13/2023

What's a data contract vs a function contract?

A data contract is not standard terminology. There multiple types (patterns) of smart contracts. he “data” type of contract is a simple concept where data is added, updated, removed and accessed. In the process of creating data contract, we will be able to work with an Access Control List (ACL) contract which can be used to manage role-based security on all contract types, Eventing mechanism for logging and returning data and some other features of smart contracts.

Moderator | 02/14/2023

What's the difference between bytecode and a byte array? Does bytecode get turned into a byte array?

Bytecode is the code represented as bytes: https://en.wikipedia.org/wiki/Bytecode

a byte array is an array of items of type bytes. No it doesn't get turned into a bytes array.

Moderator | 02/15/2023

whats the use case of having a proxy contract instead of calling the implementation contract directly? the 2 contracts can be

widely different i presume?

Main advantage is that the main contract address users will be interacting with can remain the same while implementation can be updated.

Moderator | 02/14/2023

when should we use assembly in Solidity?

Mostly optimisation, things like checking if an address is a contract, accessing memory directly, low levels calls , calls to precompiled contracts etc. Also note that it's harder to keep your code secure when you use assembly. So default to solidity and only use assembly if you need to do something specific.

Moderator | 02/15/2023

Why "external storage" pattern not recommended?

You mean Eternal Storage? In my experience fact that no updates are possible on storage layout is why this pattern is no used.

Fox Reymann | 02/13/2023

Why is owner not stored on the left and is stored on the right?

jsut a number representation, you start numbers from right

Fox Reymann | 02/13/2023