

Anonymous

2 hours ago

can you please share the link for today's homework?

Moderator

2 hours ago

<https://discord.com/channels/705799923014041651/1029362428514938990>

Anonymous

2 hours ago

is there anyway to save these Q&As sessions?

Moderator

2 hours ago

yes we archive them and will put them on discord

Anonymous

2 hours ago

is there any extensions for solidity that works as github copilot?

Moderator

2 hours ago

copilot did work surprisingly well with solidity

Anonymous

2 hours ago

in practice, would we avoid implementing #18 and #19 of the assignment, in favor of using Web3 events to find out what payments a user has made?

Moderator

2 hours ago

Depends on the use case. For example if the data is needed by the contract, then it needs to be accessible onchain - using merkle tree proofs would be better than just storing in structs. If the data doesn't, then using events is a good call.

Anonymous

3 hours ago

As the value of tokens sent to 0x...dead increases, wouldn't it become increasingly lucrative to bruteforce the key for it?

Moderator

3 hours ago

Yes, however cos of the amount of zero's the hamming weight is very low i.e. would require an enormous amount of computation. The formula is $1/(256^n)$ where n is the number of zeroes in the address

Anonymous

3 hours ago

How is it possible that this address was created without a private key?

Fox Reymann

3 hours ago

you can use random numbers to create an address. just stick to the format and fill in with random values. no private key needed.

Anonymous

3 hours ago

how does burning work? and why is it done?

Anonymous

3 hours ago

Regarding the Polynetwork hack... Why are there so many recent micro-transactions to both of these accounts?

Moderator

2 hours ago

Good question. Maybe we can get @zachxbt from Twitter on the case?

Anonymous

3 hours ago

if you need 32 eth to stake, why does the beacon chain have decimals?

Anonymous

3 hours ago

What does EaD stand for?

Anonymous

3 hours ago

under the input data of the transaction to dai, it was expressed in wad, but I can't seem to reconcile that number to the eth value. What's the conversion rate?

Moderator

3 hours ago

A wad is a decimal number with 18 digits of precision that was introduced by the DS-Math library

F

Frank Beatrice III

3 hours ago

Why does it say "Poly Network Exploiter" ? Etherscan historical records or did they self name?

Moderator

3 hours ago

This is labelled by Etherscan. People usually send a form informing Etherscan of the exploit/hack.

Anonymous

3 hours ago

Can you emit one of the custom errors. For instance, if you want to issue a warning instead of reverting the transaction?

Moderator

3 hours ago

You have to use the revert keyword with custom errors.

Anonymous

3 hours ago

could you explain the interface type in the try/catch example?

Fox Reymann

3 hours ago

Only external functions support exception handling. These exceptions can be caught via try and catch statements. So interface is there so we have external function.

Anonymous

3 hours ago

does the comment above the `error` keyword produce a string error message somewhere, interpolating the variables?

Fox Reymann

3 hours ago

not sure what you mean, comments are ignored except of license

Anonymous

3 hours ago

So assert is just for testing your code

Fox Reymann

3 hours ago

yes

Anonymous

3 hours ago

address immutable owner = msg.sender was declared outside of constructor. How is msg.sender determined in this context?

Fox Reymann

3 hours ago

deployers address

Anonymous

3 hours ago

Can you create more than 1 contract per file?

Fox Reymann

3 hours ago

why would you have a requirement like that?

Anonymous

3 hours ago

what if one needs more than 24kb? have one contract call another?

Moderator

3 hours ago

Potentially. You could use SSTORE2 to store data if its static data. You can use CCIP (EIP-3668) to store/compute the data offchain.

Anonymous

3 hours ago

When would be the best case to use enums?

Fox Reymann

3 hours ago

current state of the contract (like a state machine), code readability etc.

Anonymous

3 hours ago

whats the 24kb limit? is that the max size of Solidity contract?

Moderator

3 hours ago

Yes, as specified in EIP-170. The exact size is 24,576 KB

Anonymous

3 hours ago

is `virtual` used in the parent or child? in your example it seems like it's used in Child1, but the explanation says it allows child contracts to override.

Fox Reymann

3 hours ago

A function that allows an inheriting contract to override its behavior will be marked at virtual. The function that overrides that base function should be marked as override. yes, Example is not clear.

Anonymous

3 hours ago

Is there the concept of superclass and interface like java ? In this case we could "extend" another contract and "implement" some interface functionality

Moderator

3 hours ago

The super keyword does allow you to access the parent contract if the method is inherited

Anonymous

3 hours ago

When you inherit, does it count against the 24kb limit?

Fox Reymann

3 hours ago

yes

C

Cas

3 hours ago

works _; also in overwritten functions , so to parent code is inserted at theat _ point?

Fox Reymann

3 hours ago

yes

Anonymous

3 hours ago

Does trying to override a non-virtual function produce a compile time error?

Fox Reymann

3 hours ago

yes

Anonymous

3 hours ago

if inheriting from multiple contracts with different constructors, how does that work?

Anonymous

3 hours ago

Can you give a real world example on a parent / child contract vs all in 1?

Fox Reymann

3 hours ago

Token \$Encode inherits from OpenZeppeling standard ERC20

Anonymous

3 hours ago

does the self destruct only work if the self destruct function was written into the contract in the first place?

Fox Reymann

3 hours ago

yes

Anonymous

3 hours ago

DataStruct[] public records; What's the use of [] in this struct? Also, records seems like it's a list? (edited)

Fox Reymann

3 hours ago

[] indicates an array.

Anonymous

3 hours ago

does using the DataStruct({ }) setup the variable as memory storage? what are other forms of storage?

Anonymous

3 hours ago

Yesterday you mentioned that once you deploy a contract, its always there on the chain. How do we prevent someone from using an older contract? Security risk?

Fox Reymann

3 hours ago

if you plan ahead you can include selfdestruct method in your contract. of if you've used CREATE2/3 methods to create the contract you can overwrite it

Anonymous

3 hours ago

Where can i find the documents from last time?

Fox Reymann

3 hours ago

Encode Discord -> Ethdenver Bootcamp -> Course Materials

C

Cas

1 day ago

Archived

once deployed it stays forever in the blockchain 😊 each deploy create a new contract at new address. So callers need to change address to use new one?

Fox Reymann

1 day ago (only visible to you)

you can deploy to the same address. this is a big topic. google 'upgradable contracts' and also CREATE2 method

C

Cas

1 day ago

Archived

Possible to enlarge fontsize of Remix editor code ? (edited)

Fox Reymann

1 day ago (only visible to you)

you can change zoom level in Zoom. Please zoom in