Are there more resources on Consensus Mechanisms? Especially on checkpoints. It makes little sense to me that not all nodes need to hold the chain's history.

good start: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Fox Reymann | 02/06/2023

Are you going to talk about account abstraction in this course?

Later in this lesson yes. For something specific please add to sli.do poll.

Moderator | 02/06/2023

Account Abstraction in talked in detailts in Zero Knowledge Course.

Fox Reymann | 02/06/2023

Can you run a node and validate without staking any Ether?

No sure of your question but to clarify. Validators run a node, validate transactions and submit blocks. To submit a new block you need to stake 32ETH.

You can also run nodes that do not submit blocks but keep track of the chain and checks existing blocks are valid.These nodes don't need to stake.

Moderator | 02/06/2023

Could you clarify why require is preferred to revert even though you can’t use Errors with the require statement?

it is a different use case

Moderator | 02/10/2023

Could you please share the Avalanche Snow resources you mentioned?

Snow Whitepaper: https://arxiv.org/pdf/1906.08936.pdf

Fox Reymann | 02/06/2023

custom type must have underlying primitive type? or can be custom struct, etc.?

correct, must have underlying primitive type

Fox Reymann | 02/09/2023

Do events affect the size of the code?

Events affect size of deployed bytecode.

Fox Reymann | 02/09/2023

Do pre-compiles work in hardhat / foundry?

yes

Fox Reymann | 02/09/2023

does the contract have a size limit? and would imports increase the size?

yes, there is a limit. yes, imports increase size of a contract.

Fox Reymann | 02/09/2023

Doesn't overusing "require" make the function more gas costly?

Yes. Just don't overuse.

Fox Reymann | 02/09/2023

How is randomness in committee selection guaranteed?

https://eth2book.info/altair/part2/building_blocks/randomness

Fox Reymann | 02/06/2023

How mechanism of linking external libraries different in remix and eg hardhat? Are they same process for deployed libraries like OZ, as for your own libraries?

Compiler is generating final bytecode, I don't think there is a difference between remix and hardhat in this case. This is just an IDE in this case.

Fox Reymann | 02/09/2023

How mechanism of linking external libraries different in remix and eg hardhat? Given that the libraries are from a different source., github for example

what do you say it differs?

Fox Reymann | 02/09/2023

the linking only occurs when you are using functions in a deployed library, it would be done as part of the deployment

Moderator | 02/10/2023

how to know if one should use interface or abstract?

Abstract contracts can contain function implementation whereas interfaces cannot. So use abstract only if you need to implement functions.

Moderator | 02/09/2023

I've read that the `success` return val of low level `call()` can return false positives for contracts with no fallback function defined?

I'm not sure. Would you like to test it and share your finding on discord?

Fox Reymann | 02/09/2023

If the abstract can contain implemention, can we not just implement the function directly? What's the main reason to use the abstract instead of direct impl

This is about software design. Abstract indicated it is not a final contract but one abstract contract can be inherited by multiple different contracts.

Fox Reymann | 02/09/2023

In your opinion should a no-op transactions revert?

I'll investigate this

Moderator | 02/10/2023

Is it possible to have bugs in the precompiled contracts, so all the clients execute those would be impacted, thus induce the risks?

yes

Fox Reymann | 02/09/2023

Is it safe to use block.randao_reveal as a VRF in solidity?

i believe so, i'll check and comment in the security lesson

Moderator | 02/10/2023

Is memory default attribute for parameters in the function?

If you don't specify storage type of a function argument then function arguments are always in memory and you are passing an argument to a function by value.

Moderator | 02/09/2023

is there any difference in the EVM between require/revert/assert? e.g. REVERT vs INVALID opcodes etc. (guess there's the return string in requires as well)

this is mostly about what is the logic behind your operation - do you revert on error, require a condition or assert something has gone correctly. As Laurence says there are some differences in EVM.

Fox Reymann | 02/09/2023

it's not possible to comment on other questions here,you can only ask questions I guess?

You can only ask. Moderators from Extropy.io answer the questions.

Fox Reymann | 02/09/2023

Links in the notes slightly contradict the terminology of the notes - does require produce exactly the same results as revert?

require(condition) under the hood uses revert, so essentially they are the same and it's just a matter of style and usability.

Fox Reymann | 02/09/2023

Overuse events will cause more gas cost right? How to balance that?

you need to consider who is paying, and the cost difference of the event

Moderator | 02/10/2023

So for contract deployed to production, `pragma solidity 0.8.13;` is better than `pragma solidity ^0.8.0;` , right?

For security reasons it better to have a fixed pragma. In case of bugs / differences in Solidity version it is better to specify exact version that the contracts have been compiled with.

Fox Reymann | 02/09/2023

So positions can change?

yes

Moderator | 02/09/2023

The "Casper FFG + LMD GHOS" can not be implemented in the POW system?

No Gasper is the mechanism for POS and requires POS to work.

Moderator | 02/06/2023

The type of currencies to be chosen for transaction fee is permission less? Or a list of of currencies would be allowed?

In Ethereum you must use ETH. Depends on the implementation for other chains but most use their own 'native' token.

Moderator | 02/06/2023

What does block.prevrandao do?

https://eips.ethereum.org/EIPS/eip-4399

Fox Reymann | 02/09/2023

What if function selectors clash? 4 bytes is not enough to prevent malicious collision! What happen with the hack?

we are going to explain Poly Network hack if we have time. other way please check resources on rekt.news

Fox Reymann | 02/09/2023

What is a Client?

Client is a software that runs on an Ethereum node

Fox Reymann | 02/06/2023

What is sybil resistance mechanism?

A **Sybil resistance mechanism**, on the other hand, is the process by which the decentralized system deters again **Sybil attacks**.

Moderator | 02/06/2023

Essentially a mechanism to make it expensive/difficult to create account that is eligible to produce a block. Otherwise you could just create millions of accounts and get selected for a block in POW. POS a bit different but same idea.

Moderator | 02/06/2023

What is the aim of homework? To optimise for gas or storage?

If you feel like optimising you can but that's not part of the homework.

Moderator | 02/09/2023

What's the gas pricing for using precompiled contracts?

it is a normal CALL operation

Fox Reymann | 02/09/2023

What's the way of finding out what opcodes do solidity functions use?

This is a good resource: https://ethervm.io/

Moderator | 02/09/2023

write a contract, compile into bytecode, analyse the bytecode

Fox Reymann | 02/09/2023

When library fns are inlined into your contract - (if internal is the visibility), does that that mean we pay the gas to redeploy OZ code each time we use them?

yes

Fox Reymann | 02/09/2023

where does the 'randomness' required for committee selection etc. come from or how is it calculated?

https://www.youtube.com/watch?v=rUOBPu4W28c

Fox Reymann | 02/06/2023

Which would be more gas efficient between the high level solidity call and the low-level call?

we will explore this in the optimisation lesson

Moderator | 02/10/2023

Will cover the smart contract upgradeability in this course?

Yes we will cover this.

Moderator | 02/06/2023

would a library basically consist of pure functions then?

no

Fox Reymann | 02/09/2023

Would you recommend using via-ir?

yes it can help with stack errors

Moderator | 02/10/2023