BNB_Replies_week_4_and_5

Do we have to download any packages for store layout? I tried this sol2uml storage ./src/filename.sol --contract filename but it isn't working

https://www.npmjs.com/package/sol2uml/v/1.1.6

Moderator | 04/11/2023

Does the order of unallocated slots make any difference in gas optimization? Should it be thought to be built with unallocated slots last?

Ideally you would pack the variables to avoid unallocated areas of memory which will we be trying in the practical.

Moderator | 04/11/2023

dynamic array would change the slots of other variables (declared after it) if we add element to this array, i guess

No because the dynamic array is just a 32bit pointer and the actual array data is in a separate storage slot.

Moderator | 04/11/2023

how to protect users from sandwich attacks?

Use flashbots or other private relays. L2s also have centralised sequencers so the mempool is not public. Also there are things like cowswap

Moderator | 04/11/2023

is there a tool to draw UML graphs from solidity code?

Yes I forget which one is used last time but here is an article with a few examples: https://medium.com/coinmonks/convert-solidity-code-to-uml-flow-diagrams-3a5cd412177

Moderator | 04/11/2023

Is there a way to keep the source for the Oracle hidden to avoid OEV? is it OEV if someone influences BNBUSD price for the pancakeswap prediction function?

I think it is more the case that the Oracle themselves have an advantage by the fact that they know data first, and could therefore exploit that in some way

Moderator | 04/11/2023

What VSCode Extension do u use to intellisense and autocomplete solidity ? (also inherit from open zeppelin etc...)

There is a few but I use this one: https://marketplace.visualstudio.com/items?itemName=JuanBlanco.solidity

Moderator | 04/11/2023

whats the difference between APY and APR?

APY refers to the amount of interest earned on your savings and APR is how much interest you owe.

Moderator | 04/11/2023

How do the bots do a simulation do they like fork mainnet?

Generally they need to simulate the block locally using forked data. One method it to use state overrides in geth.

Moderator | 04/06/2023

In the reentrancy example, if we first set the user balance to zero before sending, what happens if the send fails for some reason? Will the entire transaction fail and automatically roll back the account balance to original, or does that need to be coded in an error catch?

transactions are atomic so either all the transaction is executed or none. So yes it rollsback any state changes if you revert.

Moderator | 04/06/2023

is there any chance of overlap in memory if there are multiple large dynamic array in smart contract?

Compiler will prevent over/under flow. You can used unchecked to avoidride which can lead to over/under flow. You also need to be careful if you are writing inline assembly.

Moderator | 04/06/2023

Please more content for MEV - Sandwiching and bots

What MEV topics are you most interested in? PBS, Flashbots, Sandwiching/front fronting, bots, effects on consensus/decentralisations risks?

Moderator | 04/06/2023

putting a max slippage can help avoid to be front runt?

The best way to avoid front running is to use flashbots relay,

Moderator | 04/06/2023

how are these zk proofs actually programmed? is it the mathematical model that we put in in any particular language? like in solidity in our smart contract?

Depends on the system but there are domain specific languages for writing the curcuits such as noir language.

Moderator | 04/05/2023

so did tornado cash implement a ZK proof in their smart contract?

Yes they use a zk system and proofs to prove deposit and withdrawals are legit without revealing identity.

Moderator | 04/05/2023

what's the difference between Symmetric cryptography and asymmetric cryptography?

asymmetric refers to the fact that you have different keys from encryption and description

Moderator | 04/05/2023

in proxy pattern all data is in the proxy contract ?

yes

Moderator | 04/04/2023

in that case would you call contract A the "parent contract" ?

No, this isn't to do with inheritance. It would be called the proxy.

Moderator | 04/04/2023

is this done with composition ?

Yes it is in the idea of composition.

Moderator | 04/04/2023

Is the share of the fees proportional to how much you've added to the liquidity pool?

yes exactly

Moderator | 04/03/2023

no explorer checks for forks then?

The fork is local so can't accesses by a public explorer.

Moderator | 04/03/2023