

BNB_Week2_Replies

is there any reason to chose a language different from solidity apart the fact of knowing it already?

solidity is the most popular and has the best tooling so not really but personal choice I suppose.

Moderator | 03/13/2023

Is there something like watching some events and react accordingly to that events ? Like subscription to events ?

Front end example: <https://wagmi.sh/react/hooks/useContractEvent>

Analytics example: <https://docs.tenderly.co/web3-actions/tutorials-and-quickstarts/how-to-handle-on-chain-events>

Moderator | 03/13/2023

Is this block explorer open source?

I don't think so, it is a fork of etherscan.

Moderator | 03/13/2023

Isn't it better to have a specific version?

for production deployment, yes.

Moderator | 03/13/2023

looking at slides of lesson 2 it was talked about modifiers and events. Are we going to cover these topics today?

We are covering it now actually.

Moderator | 03/13/2023

msg.value is the wei sent to the function or the wei that was spendened on the transaction?

wei sent excluding gas fees.

Moderator | 03/13/2023

No breakpoint to debug the Solidity code?

You would need to use the debugger to step through the program.

Moderator | 03/13/2023

**ok so memory=save function temporary vars instances?
storage=save class variable? rom=save constants and ...?**

yes more or less.

Moderator | 03/13/2023

**ok so the time that remain we have to join the group room and
work on the homework?**

yes

Moderator | 03/13/2023

**one question, when invoking a view method, the transaction was
reporting an execution cost of 2492. why that happen? should be
read method without gas cost?**

There is still an amount of gas associated with a view function, it is just that you do not get charged for it.

Moderator | 03/13/2023

**opensea got streaming api using websocket, do they use event to
open streaming?**

Most likely they are listening to onchain events and transaction to build up there own databases and then offer that data through an API.

Moderator | 03/13/2023

Please how is attendance taken?

Encode takes care of this. They check if you're there on the live lesson.

Moderator | 03/13/2023

Should the totalSupply function inherited from OpenZeppelin return the friendly number, or the 10^18 number? I.e. 1000000 or 1000000000000000000000000000000?

the 10^{18} number, the front end can handle the decimals

Moderator | 03/13/2023

so are the "memory" and "storage" tags implicit depending on where the variable is declared?

yes and also the type but compiler will tell you.

Moderator | 03/13/2023

So basically if nft are stored on aws s3 even if the url is saved as metadata in the blockchain the asset on s3 can be potentially changed or even deleted

Yes. That was one of the initial criticisms of NTFs. However you can overcome this with something like ipfs.

Moderator | 03/13/2023

So can we say proof of work is a protocol too?

yes more or less.

Moderator | 03/13/2023

So does EVM-compatible actually mean that a blockchain can run the same smart contracts as Ethereum out of the box without any extra configuration?

Generally it means you can use solidity but you would still need to configure your tooling/environment etc. Each chain is slightly different.

Moderator | 03/13/2023

so for example if there have been deployed 500k contracts of 25kb size, it means that a node needs at least 10qb of memory

archive node yes but there are also light nodes etc

Moderator | 03/13/2023

So if BEP-20 is equivalent of ERC-20 for the BNB tokens, what is the equivalent of BEP-2 for describing the Ethereum native token (\$ETH)?

They don't have one on ETH as far as I'm aware. It's quite different on ETH. this standard setup for BNB presents significant limitations for utilizing BEP-2 tokens. Specifically, BEP-2 tokens don't support smart contracts, which most cryptocurrencies and decentralized applications (dApps) depend on to function. As such, you can only use BEP-2 tokens for paying transaction fees on Binance exchanges. However, you can unlock the utility of BEP-2 tokens by converting them to BEP-20 tokens for use in the DeFi space.

Moderator | 03/13/2023

So if i invoke a Smart contract function that does invoke other contracts functions multiple Times or even transfer eth/token multiple Times it just count s as a single transaction? That also explain Why the balance in ethereum is not base on utxo but on EVM states?

Yes you can write a smart contract that executes your logic and calls multiple contracts. Then you just call your smart contract with one transaction.

Moderator | 03/13/2023

So if im working with alchemy fork it may use my real eth or other coin ?

no it simulates real eth but doesn't make any changes on the real chain,

Moderator | 03/13/2023

so if its a local copy of mainnet does it have the size?

It doesn't download all the data as it can simulate without verifying... IE it's only needs the data it is interacting with. It very light weight.

Moderator | 03/13/2023

So in order for me to create a signer i need my credentials and I can only be signer for the accounts I have right?

yes it's creating an object out the private key and account details.

Moderator | 03/13/2023

so is `uint256[] memory a;` same as `uint256[] a;` in the context of the function?

no you have to be explicit because the array is a reference data type.

Moderator | 03/13/2023

So it's possible to mint a token within a bigger contract?

yes that's possible.

Moderator | 03/13/2023

so local variables are not visible in the contract? private key would be visible in a function for instance?

local vars are limited to the scopr of the function. private limited to scope of the contract but it is not private as in the data is onchain and you can read it in otherways. Bit misleading that we use the keyword private. It's more of a gas optimisation that actually making it private.

Moderator | 03/13/2023

So not all contracts are in clear in the blockchain unless the developers verify them

yes

Moderator | 03/14/2023

So the contract monitoring its something like prometheus or open telemetry in web2 ?

yes or zeppelin defended etc.

Moderator | 03/14/2023

so those contracts are meant for being imported in a own contract or are also deployed on the ethereum mainnet and we can interact with them directly there?

Compiler will import the fuctions into your byte code at deploy time.

Moderator | 03/14/2023

so we can say BEP20 Token is a warpped version of an ERC20 token?

it is not even wrapped, it is the same, difference is only in naming and chain on which it is deployed.

Moderator | 03/14/2023

Solidity runs in cascade?

you always run a single method

Moderator | 03/14/2023

Sounds better to use Foundry as much as possible 😊

test run quicker for sure.

Moderator | 03/14/2023

the limit of the env size implies that if I'm developing a fat contract it has to be split among different contracts?

contract size limit is 24.576 kb. not sure what you mean by fat?

Moderator | 03/14/2023

the more text in the second argument in a require is more gas spend? for example requiere(msg.sender == owner, " you are not the owner");

yes and custom errors also use less gas but you have to trade off gas for readability.

Moderator | 03/14/2023

The nonce value is 0 for every network of every wallet account, right? i.e. account generates a tx on Ethereum -> nonce = 1 but Polygon, Fantom, Avalanche nonces will still be 0 for that account.

yea each network has it's own nonce.

Moderator | 03/14/2023

Then is Etherscan open source?

Actually no

Moderator | 03/14/2023

there can be multiple receive functions in a single contract?

No can only be one as far as I know.

Moderator | 03/15/2023

transactions on the ethereum blockchain are stored out of the EVM?

Complex but we will get to this later. Not stored in the evm

Moderator | 03/15/2023

What about structs[id] = Struct(_val1, _val2);

Yes array of struct is valid

Moderator | 03/15/2023

What about the treasure map for the homework? 😊

Soon

Moderator | 03/15/2023

What consensus mechanism using BNB chain ?

Proof of Staked Authority

Moderator | 03/15/2023

What do u think of polybase.xyz ?

Not overly familiar with this project.

Moderator | 03/15/2023

what do you think about the hardhat deploy plugin?

I'm not super familiar with the specific plugin. I mostly use foundry but any way you can automate and script your deployment is good IMO.

Moderator | 03/15/2023

what does it mean when an input parameter address in a function is set as payable

You cannot send native token to a function unless it is marked payable.

Moderator | 03/15/2023

what does msg stand for? is there classes in Solidity?

'msg' is a global variable, global state accessible to your method. 'msg' holds different data related to your transaction, like sender, value, etc.

Moderator | 03/16/2023

What if your private key is exposed? What if you loose your seed phrase your wallet? How can you access it? Is EIP 4337 is the answer to this?

exposed - malicious person can steal your funds. if you loos your seed phrase you lose access to your funds. yes, EIP4337 so account abstraction can solve the issue.

Moderator | 03/16/2023

What is 100% gaz mean? What is the referential?

100% of the block limit

Moderator | 03/16/2023

what is bytes and what does it do?

It's just a datatype. bytes is used to store binary data

Moderator | 03/16/2023

what is Enum and what does it do?

An enum type is a special data type that enables for a variable to be a set of predefined constants. The variable must be equal to one of the values that have been predefined for it. so limits function outputs and also makes code much more readable.

Moderator | 03/16/2023

what is the difference between constant and then declaring a variable as immutable?

For constant variables, the value has to be fixed at compile-time, while for immutable , it can still be assigned at construction time.

Moderator | 03/16/2023

what is the difference between etherscan and BSCscan? Is it just tools for different blockchains?

very little difference, BSCScan is a fork of Etherscan

Moderator | 03/16/2023

what is the difference between require and if statements?

if is a standard conditional, a way to change flow of execution of your program. require is going to exit the program (revert) if the requirement is not meet

Moderator | 03/16/2023

what is the license for

License field is not required by the compiler. What is it for? To make sure that legal status of your code is clear.

Moderator | 03/16/2023

what is the main difference between transfer and transferFrom?

transfer-from allows you to transfer someone else's balance. eh an exchange Transaction

Moderator | 03/16/2023

What is the memory keyword that was used when creating a new struct? Is it going to be discussed in later lessons?

We will look more into this later but memory data is not saved to contract state (chain) and is just used in the node for the execution then it is deleted. Uses less gas.

Moderator | 03/16/2023

what is the use case of enum when writing contract?

It's a way to restrict the possible outputs of a function.

Moderator | 03/16/2023