# BNB_Week1_Replies

## ABI considered schemas (api) ?

ABI is application binary interface, a description on how to interact with the contract, similar to spec of an API

*Fox Reymann | 03/06/2023*

## All governance tokens are utility tokens but not all utility token are governance token. is the following statement correct?

I mean it's really a matter of semantics and definitions. Generally yes you could say this though.

*Fox Reymann | 03/06/2023*

## all this evm sizes so impact on the requirements that the nodes need to have, I mean computer that run that software need to satisfy specific characteristics...

well yes. EVM is small so hardware requirements are low and more decentralised

*Fox Reymann | 03/06/2023*

## any good faucets for testnet BNB which give more than 0.1?

I think you can get 1 from here: [https://faucet.quicknode.com/binance-smart-chain/bnb-testnet](https://faucet.quicknode.com/binance-smart-chain/bnb-testnet)
but you have to tweet

*Moderator | 03/06/2023*

## Are the blocks verified every x amount of time or every x number of transactions?

BSC goal is 5 seconds block time, so time it is

*Fox Reymann | 03/06/2023*

## Are there any golden rules for gas optimisation balancing the cost to deploy versus the cost to transact? i.e. cost for you versus cost for the user.

We will go through this in the lesson but generally most projects are going to optimise for the users if their contract is a public facing product like a swap protocol.

*Fox Reymann | 03/06/2023*

## Are there any tutorials for getting started with Contract Auditor? Like to become security auditor.

https://www.damnvulnerabledefi.xyz/ or code4rena

*Fox Reymann | 03/06/2023*

## Are there currently, any real world applications that makes use of public/private key decryption used in communication?

WhatsApp for example :)

*Fox Reymann | 03/06/2023*

## Are we able to pick our own team? I already know a couple of people on the bootcamp.

please talk to Yasen from Encode on Discord

*Fox Reymann | 03/06/2023*

## Are we going to audit smart contracts?

we are going to cover auditing, I don't think there is a homework to audit one. if you want to audit one please add this to Live Pool on Sli.do.

*Fox Reymann | 03/06/2023*

## Are we going to cover a full Dapp development, that is, the way in which we can interact with the BNB chain on frontend side?

Mostly solidity but some frontend

*Fox Reymann | 03/06/2023*

Yes, we will cover ethers.js to interact with BNB from your dApp. But we don't teach frontend web frameworks, like React or Vue

*Fox Reymann | 03/06/2023*

## Are we going to integrate with protocols?

Yes, PancakeSwap for sure.

*Fox Reymann | 03/06/2023*

## Are we going to make any project in this bootcamp ?

Homeworks, many of these are small projects. After bootcamp there is a hackathon for the big project.

*Fox Reymann | 03/06/2023*

## Are we going to work with diamond smart contract>

We will cover it in the Upgradability lesson, but now homework I think.

*Fox Reymann | 03/06/2023*

## Are we working on strictly testnets or mainnets

for homeworks only on bnb testnet but we are going to do mainnet fork locally

*Fox Reymann | 03/06/2023*

## Are we working with IPFS too?

We are going to cover IPFS on Decentralised Storage lecture.

*Moderator | 03/06/2023*

## BNB greenfield?

gm

*Fox Reymann | 03/06/2023*

## but if we import from github we are not depending on a specific version of the contract. this can led to breaking potentially our contract?

When you deploy your contract it imports the current version into your byte code so if the repo updates your code wont. The deployed code is immutable

*Fox Reymann | 03/06/2023*

## can it be clarified how an event emit is consumed by website? is it like a webhook or a websocket?

You can listen with something like ethers js or web3 js or wgami for react.js

*Fox Reymann | 03/07/2023*

## Can recieve function handle bytes data in it?

Doesn't take arguments but could access bytes in function body

*Fox Reymann | 03/07/2023*

## can two different tokens have the same symbol? how it's managed in the DEX?

yes that can and you do need to be careful of that because some scams make us of this. Generally you should check the actual token address not just the symbol.

*Fox Reymann | 03/07/2023*

## Can we also import bytecode and analyze its functions?

There are decompilers yes

*Fox Reymann | 03/07/2023*

## Can we call function setScore() from within constructor() ?

yes sure.

*Fox Reymann | 03/07/2023*

## can we do this in foundry?

yes but it has to pass the hardhat test still

*Fox Reymann | 03/07/2023*

## Can we get the contract on hardhat by only knowing the address and chain (given that the contract is already deploy)?

Yes I think so but you might need an ABI or to do a low level call to interact with it.

*Fox Reymann | 03/07/2023*

## can we interchangeably use the terms cryptocurrency & token?

yes

*Fox Reymann | 03/07/2023*

## can we say that we could use in general Remix as the IDE and openzeppelin just for his lib of predefined contracts?

Yes openZeppelin can be used with any IDE

*Fox Reymann | 03/07/2023*

## Can we share the homework exercises .pdf on GitHub too? Or just answers

just answers please, pdf's are copyrighted.

*Fox Reymann | 03/07/2023*

## can we track how many ERC-20 an address hold on any particular block height? What is the method used?

yes it is possible but there is no easy way to do it. The data exists but you would need to listen to transaction and index and process all the transaction occurring on the chain. You might be better off using the graph etc.

*Fox Reymann | 03/07/2023*

## Can you store bunch of data while minting nft. Like I want to create a nft for crop details, so can we mint nft over complete data of crop? (crop name, owner

Yea sure you could do that.

*Moderator | 03/07/2023*

## Code must be functional or just passing the test is ok?

Just passing tests is fine.

*Fox Reymann | 03/07/2023*

## could you please elaborate on what really protocol is? What does it stands for. I can't really understand what it does? For what use

protocol, in computer science, a set of rules or procedures for transmitting data between electronic devices, such as computers. In order for computers to exchange information, there must be a preexisting agreement as to how the information will be structured and how each side will send and receive it.

*Fox Reymann | 03/07/2023*

## Could you please give me a little bit more examples on realworld usage of function keywords like external internal public private?

lets say you have a helper method that is used by other methods but for securiy reasons you prefer not to make it publicly accessible, then make it private.

*Fox Reymann | 03/07/2023*

## developing with the erc1155 allows to be also compatible with erc20 and erc721 services? I mean is erc1155 somehow an extension based on the erc20-erc721 ones?

Yes I believe it is compatible. 1155 is a way to combine 20/721 functionality into one contract so you do not need lots of token contracts for your project.

*Moderator | 03/07/2023*

## Did they call it Evolution and not Improvement because BIP is for bitcoin?

Good question. Not sure but that sounds feasible.

*Fox Reymann | 03/07/2023*

## difference between ERC20 and BEP20 tokens? is it just the blockchain where they are deployed?

Correct. We are sometimes going to call BEP20 tokens on BSC ERC20 as this is same thing.

*Fox Reymann | 03/07/2023*

## Do pure functions safe on gas or why are they used seperatly?

pure keyword is just to ensure your method is not modyfing blockchain state - storage, it is to help with development / security, not to save gas. but of course if you don't modify storage you use less gas

*Fox Reymann | 03/07/2023*

## Do u interact with the decentralized storages from like nextjs app right? is there any possibility to interact from solidity ?

Normally a hash is saved in your smart contract that points to the correct data hash on IPFS. You might be able to get data onchain from IPFS through chainlink.

*Fox Reymann | 03/07/2023*

## Do we always need to flatten the contract file to verify contract ? when importing some open zeppelin libs ?

Tools like hardhat or foundry can do this for you automatically.

*Fox Reymann | 03/07/2023*

## do we automatically produce a token when we deploy a contract?

No, one thing our contract could do is deploy a token but it can do many other things instead.

*Fox Reymann | 03/07/2023*

## do we need to be on the same network as our contract address?

yes

*Fox Reymann | 03/07/2023*

## Do you use validators and miners interchangeably? I though the current standard for consensus is POS (Proof of stake) where there is no miner competition.

Correct we should use Validator term although sometimes people say miner to mean validator.

*Fox Reymann | 03/07/2023*

## does abi should be %100 the same with the same paramater names, upper case lower case sensitive?

Not sure about case sensitivity but it should be the same yes. You don't need to copy the whole ABI just the methods you want to interact with.

*Fox Reymann | 03/07/2023*

## does Foundry have gas optimisation such tool ?

yes

*Fox Reymann | 03/07/2023*

## does Foundry have gas optimisation too?

yes forge test --gas-report

*Fox Reymann | 03/07/2023*

## Does foundry use ganache or anvil?

You can you use either but anvil is the default.

*Fox Reymann | 03/07/2023*

## Does hardhat require vs code?

No you can use any IDE but it has good support for VSCode

*Fox Reymann | 03/07/2023*

## Does it apply to MaxOS too or command are only for windows?

Commands are for Mac/linux. I think you can run on windows but most people will use on mac/linux

*Fox Reymann | 03/07/2023*

## does it matter if we use just only uint instead of uint256? By size what does it mean to variables having size?

uint is uint256. uint256 takes 256 bits of memory / storage, uint8 takes 8 bits of memory / storage.

*Moderator | 03/07/2023*

## does it mean that every nonce value will be used only once for a particular account?

yes and also the nonce must increment by 1 for each translation. so a tx with nonce 2 must come directly after nonce 1

*Fox Reymann | 03/07/2023*

## does signer mean contract owner? or wallet owner?

A Signer in ethers is an abstraction of an Ethereum Account, which can be used to sign messages and transactions and send signed transactions to the Ethereum Network to execute state changing operations. Could be the contract owner but doesnt have to be

*Fox Reymann | 03/07/2023*

## Does something like payment subscriptions exists in solidity ? Something like u automatically pay for netflix ? Without needing to approve that transaction ?

difficult as smart contracts have this "dumb" property as in they only run when called. Things like push protocol exists on eth etc

*Fox Reymann | 03/07/2023*

## Does the approve function enable the transferFrom?

Essentially yes. the transfer requires the approval

*Fox Reymann | 03/07/2023*

## Does the constructor always need to be before the functions and after the modifiers? How important is the order of components in the code?

constructor can be placed anywhere. good practise it to have it at the top. order of methods might matter for gas optimalization.

*Fox Reymann | 03/07/2023*

## does the keyword `memory` has to do anything with accessing the memory pool (mempool)

no it's different. mempool is the transactions waiting to validated/mined.

*Fox Reymann | 03/07/2023*

## Does the new Filecoin Virtual Machine have similar goals to BNB Greenfield?

Filecoin aims to provide a decentralized storage infrastructure that can be used for a wide range of applications, while BNB Greenfield specifically targets the needs of decentralized AI projects.

*Fox Reymann | 03/07/2023*

## does the pure visibility on a function always have to return a value?

not sure, but what would be a use case for a pure function that doesn't modify the state and doesn't return anything?

*Fox Reymann | 03/07/2023*

## does token owner mean the deployer of the contract?

as in getOwner? yes

*Fox Reymann | 03/07/2023*

## Doing assembly with yul+ Is also part optimization , Will we cover this on the course?

We cover yul + assembly in the expert solidity course but not in this one

*Fox Reymann | 03/07/2023*

## Don't you think algorand and polygon fees are cheaper than Bnb chain? Most of the startups are deploying with polygon and

## algorand....

please check chain ranks on DefiLlama. BNB is more popular than both polygon and algorand

*Fox Reymann | 03/07/2023*

## Each line code consumes gaz, how is it possible to do complex contracts, particularly relying on unoptimized libraries... Is it important to keep code simple ?

Yes each opcode consumes gas and contracts are very limited in what they can do. Yes important. Avoiding loops etc is important.

*Fox Reymann | 03/07/2023*

## enum can be seen as a switch structure in other languages?

Not the same but similar. Use case is slightly different.

*Fox Reymann | 03/07/2023*

## gm Laurence, can you pls send us the links of every VS Code extension you use while writing Solidity Smart contracts?

https://marketplace.visualstudio.com/items?itemName=tintinweb.solidity-metrics

*Fox Reymann | 03/07/2023*

## Have I to take care of memory size / overflow when developing a contract to not exceed the EVM limits?

The memory space is very large. Prob will run out of gas before memory when calling functions. You should have tests to cover this.

*Fox Reymann | 03/07/2023*

## How can i see a previous imported contract before they changed it?

I guess if the library is on github you could look at the commits. Tools like Foundry use git import to import code and you can specify versions. if it's deployed generally can't be changed unless it's upgradable then you would see the change in the transactions.

*Fox Reymann | 03/07/2023*

## How deep u can go to reorganize blocks ?

In theory you can reorganise as many blocks as you wish, but in practise it is used when longer chain has been created and never goes more than few block backwards.

*Fox Reymann | 03/07/2023*

## How do I deploy and verify at the same time?

You can verify your contract via Remix by using a plugin called ETHERSCAN-CONTRACT VERIFICATION.

*Fox Reymann | 03/07/2023*

you can do this with smart contract dev tools like Foundry, Hardhat, Truffle. Just like a script that deploys and verifies at the same time.

*Fox Reymann | 03/07/2023*

## How do the smart contracts from different blockchains communicate

Good question and a hard problem in crypto. Sometimes through oracles or bridge type systems. Essentially you need a contract on each chain and some system to securely pass messages between.

*Moderator | 03/08/2023*

## How do you define the owner of the contract on test ? Just using the name "owner" ?

The owner would be the address that has deployed the contract.

*Moderator | 03/08/2023*

## How does gasless mint for NFT works?

essentially a 3rd party pays the gas for you.

*Moderator | 03/08/2023*

## How exactly do you read values of private-scoped state in a contract?

The contract itself can read it or you need to workout the storage slot and then decode the raw bytes in that slot.

*Moderator | 03/08/2023*

https://solidity-by-example.org/hacks/accessing-private-data/

*Moderator | 03/08/2023*

## how expensive are virtual functions and virtual tables?

We don't have the concept of virtual function or virtual tables in solidity.

*Moderator | 03/08/2023*

## how is the msg.sender handled in the foundry tests?

You can specify addresses that is calling the contract/deploying within your test. The address you specify will be the msg.sender.

*Moderator | 03/08/2023*

## how many transactions normally will a block have

median would be 100-200, it is limited by block's gas limit

*Moderator | 03/08/2023*

## How the storage protocols like Greenfield are important to Decentralised AI projects?

It will be pretty important I guess because AI requires lots of data and data is very expensive onchain.

*Moderator | 03/08/2023*

## How u implement the interface ? Using is keyword like inheriting the parent contract

yes eg contract x is y {//code here}

*Moderator | 03/08/2023*

## I am still confused, I am in the encode discord but I don’t see any bootcamp resources that y’all post

if you don't see BNB bootcamp on discord please talk to Encode to give you access

*Moderator | 03/08/2023*

## I don't find any source code repo of etherscan explorer. Can you provide it?

It's not actually open source but you can look at something like this: [https://tryethernal.com/](https://tryethernal.com/)

*Moderator | 03/08/2023*

## I don't think bytes data can be handled in receive function. for e.g bytes public data, if I use bytes in receive function will give error.

not sure but this works:

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.17;

contract sdr{
```

```
bytes32 a = bytes32(uint256(123));
```

```
receive() external payable {
a = a;
}
}
```

*Moderator | 03/08/2023*

maybe misunderstood the question.

*Moderator | 03/08/2023*

## I don’t really understand why “public view” is necessary

to mark it as public instead or private, internal. To specify function as 'view' so read only instead of a function that modifies blockchain stats so requires a transaction,

*Moderator | 03/08/2023*

## I'm curious how images are changed, "revealed" after an NFT drops if the URI is minted in the metadata

URI stays the same but I would guess they change what is stored at URI

*Moderator | 03/08/2023*

## if a constant is called an outside contract will the value of the constant be deployed along with the contract?

yes

*Moderator | 03/08/2023*

## If a transaction failed, would it cost gas too?

Yes it would still use the gas up to the point it reverts.

*Moderator | 03/08/2023*

## If anyone knows where is the place to find the PDF please

Discord → BNB Bootcamp → Course Materials

*Moderator | 03/08/2023*

## If for some reasons when an event is emitted the listener is offline what happens.

So the event would exist in the block data but the listener would need to go back and process the blocks it missed unless it is an indexed event and then it could search for events.

*Moderator | 03/08/2023*

## If I create a NFT for crop, so I must store it's crop name, yield date, expected yeild , owner and crop photo? So what should I use?

You can use something like IPFS because it's not chain specific.

*Moderator | 03/08/2023*

## If im creating BEP20 token contract, will msg.value contain BNB value or value of my token ?

msg.value is value of native token value.

*Moderator | 03/08/2023*

## If miners can add their own transactions to a block in their node isn't it going to be flagged as invalid by the other nodes in the network when it's published?

No as long as it is a valid transaction that is ok.

*Moderator | 03/08/2023*

## If one change Account in Remix after deplyement, one cannot setScore?

depends if access to setScore is restricted or not. if you have onlyOwner modifier than yes, if you change account to not an owner account you won't be able to setScore

*Moderator | 03/08/2023*

## If the ERC1155 is more efficient and saves more gas fees, why are people still sticking to ERC721? Is it most likely due to comfort/familiarity?

I suppose ECR721 is more tested and is the industry standard.

*Moderator | 03/08/2023*

## if there is an overflow should we use assert?

overlfow is handled by the compiler but we will cover this later.

*Moderator | 03/08/2023*

## If we import the ERC20 contract from OpenZeppelin, do we write anything special to make it BEP20, or does just deploying it to BNB chain accomplish this?

You willl need to follow the BEP20 spec

*Moderator | 03/08/2023*

## If we use the open zeppelin contract, do we need to do anything special to make it BEP20, or just deploying to BNB testnet does this?

see previous answer

*Moderator | 03/08/2023*

## if wrong token is send to the contract, what is a process to return it? who particularly can do such return?

You would need to handle this in your code either by rejecting/reverting the transaction or returning the amount etc. Or have some function to return the token.

*Moderator | 03/08/2023*

## in contract we wrote interface { } to put BEP20 methods. is it necessary?

We will go through interfaces in the lesson. You need an interface or the ABI to interact with another contract or you do low level call.

*Moderator | 03/08/2023*

## In maps we can only have values of the type declared right ?

just the key that is restricted. so you can have address ⇒ struct but not struct ⇒ address

*Moderator | 03/08/2023*

You can't have mixed types values. Is that what you meant?

*Moderator | 03/08/2023*

## in some Fail testing I've seen .to.be.reverted , can you explain how this works?

yes, it just means that we expect the function to revert. So if the function reverts the test passes.

*Moderator | 03/08/2023*

## In the code "DataStruct memory newRecord; " , what does memory mean here?

see above question

*Moderator | 03/08/2023*

## In which sense BNB Chain is disjoined from Binance? Is it running independently on financial/development somehow "government" side?

it is now a separate entity, BNB Chain organisation.

*Moderator | 03/08/2023*

## is `owner` also a keyword recognized by solidity? since we never saved an address into owner

you just got the answer from Laurence, we have to set the owner variable. by default after declaration is has been set to address(0) so 0×0000....

*Moderator | 03/08/2023*

## Is appropriate to have a very short intro to Account abstraction?

yes will go through this in another lesson.

*Moderator | 03/08/2023*

## Is approval function cheaper than transfer function?

Interesting question. The functions are essentially the same but operate on different mappings. So they would use similar gas. Function selectors are store in hexadecimal order so the function that is stored first should use less gas. Maybe this could be a fun project to find out.

*Moderator | 03/08/2023*

## Is approve reversible if the actual transfer does not occur?

yes you can revoke.

*Moderator | 03/08/2023*

## is BNB chain a side chain to ethereum?

no, it is not, but there are bridges between them

*Moderator | 03/08/2023*

## Is Cairo another option or still in too early stages?

Cairo is not a EVM language it is a zk language.

*Moderator | 03/08/2023*

## is deploying smart contract a transaction too?

yes

*Moderator | 03/08/2023*

## is it a good practice to set the owner in the constructor as the msg.sender?

depends on your requirements

*Moderator | 03/09/2023*

## Is it always good practice to set owner variable public?

it doesn't really matter, hacker can access private variable values too

*Moderator | 03/09/2023*

## is it better to user tx.origin or msg.sender?

in 99.9% of cases: msg.sender.

*Moderator | 03/09/2023*

## Is it common to run test and deploy scripts in ci/cd pipelines for test net and then mainnet ?

I think less so that web2 because you tend to deploy mainnet once only as it's immutable but there are some good tools you can take a look at such as: [https://docs.tenderly.co/simulations-and-forks/integration-guides/ci-cd-pipeline-for-smart-contracts](https://docs.tenderly.co/simulations-and-forks/integration-guides/ci-cd-pipeline-for-smart-contracts)

*Moderator | 03/09/2023*

## Is it like using the jibberish language and running it through an application? Forstep 4

jibberish language can be decrypted by anyone, here you're sure that only Alice can decrypt the message

*Moderator | 03/09/2023*

## Is it posible to get the logs of the slido conversations, because it is difficult to focus on the presentation and at the same time read the questions and the responses wich are really verry helpful

yes We can post these. Sorry for the delay in posting them.

*Moderator | 03/09/2023*

## Is it possible to store other formats of data like jsons or like database data except of files in IPFS ?

yea you can store JSON. Any file an be stored. You wont be able to "query" it directly on IPFS. Tableland is good for that.

*Moderator | 03/09/2023*

## Is it possible to store private data in Greenfield and use them with dApps ?

Yes it is possible.

*Moderator | 03/09/2023*

## is it possible, at the end of the lesson, to show how to unit test the transfer of NFT on Remix of Homework 6?

Not sure if we will have today but we will go through it or post the answers in discord soon

*Moderator | 03/09/2023*

## Is it pseudocode or what.

No its ethers.js

*Moderator | 03/09/2023*

## Is pull payment similar to airdrop?

Could be used for an airdrop but to be precise it is a method to pay many addresses which avoids the risk of running out gas by require people to pull their own payments

*Moderator | 03/09/2023*

## Is Remix VM (Merge) like a private test net?

Yes, it is EVM running in JavaScript in your web browser.

*Moderator | 03/09/2023*

## Is the permit part of ERC20 standard?

not right now

*Moderator | 03/09/2023*

## is the semicolon after the underscore in the modifier mandatory?

semicolons are required at the end of every instruction, so yes

*Moderator | 03/09/2023*

## is there a tool to estimate the gas cost of our contract when typing code?

Not sure about while typing but both hardhat and foundry have built in gas reports.

*Moderator | 03/09/2023*

## is there a way to peek inside the private variable?

Yes, on BSC all data is public, private variable in stored in a public storage

*Moderator | 03/09/2023*

## is there a way to programmatic get the ABI of deploy contract ?

The ABI is generated at compile time. Most Development toolchains save the ABI at compiled time in an 'ABI' folder. eg hardhat, foundry etc

*Moderator | 03/09/2023*

## Is there any guide or set of best practices to create AMMs ?

I dont think there is one specific guide you would just need to read the specs and docs of different protocols such as uniswap, curve etc.

*Moderator | 03/09/2023*

## Is there any means to check if a particular contract is upgradable?

Without reading the code it's quite difficult but you can check by reading and understanding the code. In reality many contract use some type of proxy pattern that is easy to spot.

*Moderator | 03/09/2023*