ETH Denver Answers

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

deployers address

Can you have methods inside struct?

No. Just holds data

_a.max(_b) is passing both a and b variables as arguments to the function max?

Correct. This is to determine which of the two variables is bigger.

https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/utils/math/Math.sol

"input data are method arguments" -> Every method argument in a contract will be displayed in the "Input Data" section of the etherscan page?? (bit/ly links)

correct

It was added as hexcode (from text) within a metamask transaction from one EOA to another.

A single hash can already verify that data wasn't changed. What does Merkle Tree add to that?

Merkle Trees are used to hash a collection of hashes, so you only need to store and verify the Top Hash thereby saving space and computation. If one leaf or a node is changed, the Top Hash would change as a result.

adding layers to Ethereum increases operational risks? (ex. L3, L4)

yes, each L2 has some risks

all those methods like ¨to. .be .equal, etc¨ come with HardHat?

These are global Mocha functions: https://mochajs.org/#getting-started

Also any thoughts on scroll?

it is is very early stages

Any thoughts on zkSync? Seem like a promising EVM compatible zk rollup, as most solidity smart contracts can be migrated to it.

zkSync looks promising, StarkNet is also working on EVM compatibility

are ABIs in web3 similar to APIs in web2 ?

The ABI is how the compiler builds the application. API is used for external functions/programs to access your code

Are all Polygon solutions sidechains with their own security or some of them are roll-ups using Ethereum security?

some are using rollups

Generally no as it's very expensive. often alternative solutions are like IPFS are used to store large files like images.

are there any design patterns commonly used in contracts? like facade, builder, etc...

There are approximately around 5 patterns. Like the factory or iterable map pattern. Please go here for more info:

https://dev.to/jamiescript/design-patterns-in-solidity-1i28

are there any repos anywhere that have examples of this layer 2 infrastructure we can read?

read StarkNet or ZKSync whitepapers to ZK L2s

are there examples of contract upgrades where the data is migrated? the ones in defi that I see dont do

that, such as uni v3, etc

EIP-1967 has the data(state) stored in the proxy contract i.e. the first contract. The logic (functions) is in the implementation contract. The data will always stay in the proxy.

are variables shown in orange boxes in Remix once deployed?

The orange box in remix usually (with the default theme) means your writing to the network

Arrays - there used to be a problem of it being too big and costing too much gas to iterate. I think it was solved with increasing max gas, can you elaborate?

You can use mapping to a struct with the data. This will be much more efficient than a big array which you may have to iterate through

as a developer, it makes a difference developing to L1 than to L2 (except for gas costs for the users and execution times for users?)

depends what L2. is it EVM compatible or not is the biggest question with ETH L2s

As default if i declare a variable without any visibility definition is intended as private ?

public for functions, internal for variables

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

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

best practice for .sol files - 1 smart contract per file?

yes

Binance holding 20,000,000 tokens is too centralized. Would it work if no matter the amount of Token an account holds it get one vote per account?

then Binance could create a script to split tokens to 10000 accounts and votes 10000 times

can arbitrage be done between a dex and a cex?

yes if you have a program to work with both

can cybersecurity play any role in securing smart contracts in the future or is that only on the blockchain infrastructure side?

Cybersecurity in the traditional sense does definitely play a role. For example the hack with Axie Infinity was done with social engineering. The dev team can always be targeted with malware.

Can Laurence explain MPC? hear it mentioned with Fireblocks but would be good to get an explainer

Multi-Party Computation allows multiple parties to make calculations using their combined data without revealing their individual inputs.

can multiple modifier co-exist in a single function?

yes

Yes, but it will cost a lot of gas to run

can one access ganache via remix?

Yes, you can access Ganache via Remix.

can the modifier add an else statement or it should be 2 modifiers run on the function?

modifier can have an else statement

Yes you can. You should use if else conditionals if the logic is tightly coupled.

Can use Ethers with Foundry?

no

Can we consider the EVm similar to other VM (like java) where the compiled code is executed and this evm run with its separate process with its own context ?

Yes

can we pair a mapping with some kind of an array/list to keep track of all the addresses we insert in the mapping?

Yes you can. This is used in ERC721Enumerable for example

Can we repeat what is OFAC compliant blocks?

Stands for 'Office of Foreign Assets Control' which is the Department of Treasury in the US. https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1501

Here are the addresses that are required to be blocked: https://github.com/flashbots/rpc-endpoint/blob/main/server/ofacblacklist.go

Can you do sorts and lookups in these arrays or do you have to performs these functions manually?

you can, consider gas costs. but there are no build in helpers, you need to code your sort

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

you can emit Events if you don't want to revert

You have to use the revert keyword with custom errors.

can you explain the artifacts folder of json files derived from the solidity files?

JSON is Application Binary Interface, so an interface that tells other libraries how to interact with your contract

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

Token $Encode inherits from OpenZeppeling standard ERC20

can you provide context of the various parties in MPC?

Depends on application. Nucypher is an example, with decentralised encryption/decryption where you only need to have x/n nodes decrypting a message.

conceptually understand why reducing context switching is good for progress. But why would testing be in JS for code written in solidity?

Pros & Cons. But the idea was JS is more flexible language with more libraries and tooling. Also if you are a JS might be easier. But I prefer foundry.

constructor is the 1st function which is called?

It's a specialised function which is only run once at the beggining. And will never be called again.

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

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.

Could you please advise how to test for events using Foundry?

Check this:

https://book.getfoundry.sh/cheatcodes/expect-emit

Could you please explain a bit about ethereum's security model ? I heard many people say other L1 has a inferior security model but not suer why.

When compared to newer blockchains it's the size of the network and the computing power required to change the block. As ethereum is quite big - this is very expensive to do.

Could you point us to a Solidity written example of an arbitrage flash loan?

https://github.com/stalinMacias/profitable_flashloans/blob/master/contracts/Flashloan.sol

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

[] indicates an array.

deleting from a mapping? how does it work?

Changing the value to zero.

did they ever find out the hacker?

https://twitter.com/laurashin/status/1496087239037698048

Difference b/w cairo playground and starknet playground pl?

cairo playground is for cairo - programs, starknet playground is for contracts on starknet

Do auditors assume any legal liability for mistakes or misrepresentations? If so, to whom are they legally accountable... project owners, investors, users?

usually not

do comments affect gas when deploying contract?

no

Do comments count against 24kb limit?

no, only bytecode does, comments are removed by the compiler

do comments in contracts consume gas?

No it doesn't

Do events cost gas?

yes, not much

Do you have an opinion on ERC-725?

This seems quite useful however it is currently stagnant.

https://eips.ethereum.org/EIPS/eip-725

Do you have to use "memory" keyword on any variable defined within a function?

There is nothing within the compiler to force you to use memory keyword on variables so it's up to you.

Do you think AMM will withstand time? majority of LPs on Uni v3 loses money

do you know any better alternatives? there are some improvement ideas, like surge pricing etc.

DEX are definitely superior than CEX's - especially in light of recent events.

Also some work is being done on Directional liquidity pooling to make LP more profitable.

does arweave use IPFS?

No it's a different technology

Does Cairo support modifiers like Solidity does?

no modifiers, you have to code your access control in function body

does COWswap do cow mapping before it goes into AMM?

yes

Does it means that 2 nodes uploading the same file will have the same hash?

yes

does it use the same amount of storage as running a node when we make a fork of mainnet?

what storage? your contract are going to use the same amount of Ethereum's storage

Does OpenSea support ERC1155, and if so, does it show all the NFT's held in each contract?

Not yet but coming: https://docs.opensea.io/docs/opensea-erc1155-tutorial

does revert string affect gas cost in starknet contract

yes

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

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

does the function 'setScore' choose a random uint256?

is uses newScore function parameter as new score value

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

yes

Does the sequencer or prover ever need to read data from L1 before finalizing a transaction on Starknet? e.g. checking that someone's token balance is enough

no, it reads your balanace on L2

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

yes

Ethers is using javascript... for those of us who are not familiar w/ JS, is there an alternative?

You could use Brownie which is a python based framework for Smart Contracts.

https://github.com/eth-brownie/brownie

how are prices determined?

the price will be whatever the exchange supports

how can no one pays for the storage in IPFS? there is a cost someone is paying?

There are indirect costs due to service maintenance and upkeep

how can they apply math to encrypted numbers? unless the encryption preserves the relative relationship amongst the numbers?

It does.

How can we map a struct?

mapping(address ⇒ NameOfStruct) public mappingOfStructs;

how can we map to only one of the variable in struct lets say struct People {string name; age uint8} and i only wanna map to age

why would you do that? I do believe you should do that

The mapping will return the full struct. If you want to just change the age, you can.

how can we test our gas used in contract?

gas reporting plugins are available. you are going to use one in homework

How can you prevent an audit company from not reporting an exploit in order to maybe hack it at a later stage if the contract balance worth it?

You can't. As Laurence has suggested use multiple companies.

how come 4 bytes = 8 characters?

In hexadecimal 2 characters is 1 byte

How competitive is the flashloan-based arbitrage bots space nowadays on Mainnet?

Pretty competitive unless you go super long tail. A lot of the arbitrage bots are actually using the mempool to predict future prices and make arbs in the same blocks as they appear. For most of the big dex's most of your profit will be paid in order to get your transaction a head of others.

- paid as transaction fees.

how do we check the real time gas price and how do we determine the right/optimal gas limit to use?

you can ask blockchain nodes for actual price. how do you determine? depends on your needs

You'd have to calculate manually. There are plugins for Hardhat and Foundry to give you the price

How do we find the address of a node to connect to, or do we need to run our own?

usually you connect to RPC provider, like infura, alchemy. you have to find one if you want to connect direclty.

how do you return a memory result since it gets dropped

Short answer is you can't.

how do you specify between cold/warm storage for variables/functions ?

Cold: storage slot hasn’t been accessed during this transaction - so first time you use it in the tx

Warm: storage slot has been accessed during this transaction - 2nd, 3rd write to this storage

how does a curve correspond to a hash/key?

The ECDSA (Elliptic Curve Digital Signature Algorithm) is used to create a private and public key. It's not connected to the hash (Patricia Trie) directly. ECDSA is used over other algorithms because it's smaller in size and are quicker to verify.

how does hard fork restore the funds? it reverted to an older state before the leak? Were there also additional

change in rules of how Ethereum works?

Chain didn't go back in time but they just changed the rules to revert the hackers actions and safe guard funds.

How does Starknet works without a native token? it uses eth for paying for the transactions?

yes

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

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

How is the deployed contract's address derived?

check CREATE method documentation

how is the input data added to the transaction? Is it just simply an emit?

input data are method arguments

How many is too many for the array, is there something that calculates gas cost before you go too far?

you can test in your dev environment using gas reporter tools. how many is too many? you have to be able to fit in a block and pay the tx fee

how to measure performance?

gas reporting plugin for your dev tool

How would we deploy a contract using e.g. a Trezor hardware wallet?

you would need a library to connect your deployment script to trezor wallet. there are available.

I guess the EVM "slot" is totally different from a PoS "slot"?

Yes here we are talking about slots of the stack machine of the EVM.

I know it sounds damn but do spaces matter? For instance, can you have two spaces between modifier and onlyOwner and would the code still work fine?

spaces don't matter

Compiler removes it at compile time.

I read a 2016 post stating that uint8 costs more gas than uint256 ...does this still hold true?

Depends. Yes if it's on it's own but there are ways you can pack uint8s into slots next to each other which will make it cheaper. But will will get onto this later when we do gas optimisation.

I see gas measured in 'gas' in remix, shouldn't it be in gwei?

`tx fee = gas * gas price` gas is in units, gas price is in gwei/unit

so no

I suck at testing, whats your favorite tool to run test, foundry, hh, remix etc.. Are there any further resources we should explore to learn how to test better?

Google Test Driven Development Practice exercises. And then just practice.

Hardhat uses Mocha and Chai which are JavaScript - which may make sense if you are familiar with JS. However, Foundry tests with Solidity which reduces context switching. Tests in Foundry are faster too.

I've read that revert is cheaper in Gas than require. Does it have any different security implications?

What is cheaper is the usage of custom error codes as opposed to strings (in require statements). Custom error codes was introduced into Solidity V 0.8.4. Using strings in the EVM is very expensive, but by using custom codes you save a lot on storage and gas costs. Right now, you can only use the revert keyword with custom error codes, but this will change in later solidity versions.

if layer 1 scalability was built better, wouldn't there be no need for layer 2s?

yes, but due to the scalability trilema L2s are going to stay

If we enter a second value under the same key in a mapping will that replace the previous one? Can we create an array of values for a single key?

It will get overwritten. You can do a mapping to another mapping potentially.

If we only use Foundry, should we care about Ethers?

yes, for dApp frontend and web2 backend

In general, do you recommend using these tools instead of writing our own unit tests?

surely no, use test driven development. use these tools when you're done with coding.

In ZK, how long is each batch? seconds?

in order of minutes

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.

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.

Is address(0) the zero address you're referring to?

yes

Is anyone using the Haskell EVM client: https://github.com/jamshidh/ethereum-client-haskell/blob/master/src/Blockchain/VM.hs

I didn't hear about it, ask on Zoom chat if anyone knows who is using it

Is Ethers only accessible via Hardhat?

no, it is general purpose web3 library

is forking mainnet all on the command line or do we need to create a hardhat/foundry repo to start the node?

cli is sufficient, it is your local node that uses mainnet as a data source

Is IPFS censorship resistant? If I hosted a song there, could it be taken down for copyright infringement?

It is, as long there are enough nodes to host the files

Is it better to use online remix, download the client or use remix on vs code? What do you suggest?

depends on your needs and preferences.

It's up to you. Online remix may have problems with memory when you are trying to test transactions with a big data set

is it good practice to use multiple tools? It seems like each of these have different pros & cons, but might not play nice together all the time.

it depends of individual circumstances, but always, the more checks the better. you don't want to find your project on rekt.news

Is it need to compile the contract every time we make a change to it?

yes

Correct. This is why I put on the auto-compile feature on remix to speed up development

Is it possibile to have more than 1 constructor even with some parameters, using the override property of the OOP ?

No you can't

Is it possibile to use the concept of "this" like in the OOP referring the object itself?

Yes. "this" would refer to the contract itself (address)

is it possible to have 2 constructors in the same contract? if so, how is it determined which runs first?

No. Only one constructor is allowed, The compiler will complain

is it still possible to make profitable flash loans?

It might be possible but it's hard because of gas limitation. If you have the liquidity then you can save a lot of gas not having to make calls to flash-loans provider and all the logic code that goes with that. Having said that flashbots is moving away from gas auction systems so maybe it might be easier again.

is it still prevalent in POS?

Yes lots of MEV in POS

Is my intuition correct that gas optimization is useless for view/pure functions?

If it's used by a node to view data it has no cost, however if it's used in a transaction it will cost gas, so gas optimisations would still be valid.

Is proofing similar to regular txn validation?

in regular tx nodes only validate user's signature and then execute the tx, proof is like a mini quick to validate version of a tx that has happened on L2

Is remix only local? if I want to move around diff PCs, is there a way where I can sync my contracts/work across the devices so that I can work on diff PCs?

You can connect it to your github/gist

you can export / import your workspace to a file

Is the EVM run in the execution client?

Yes, the EVM is run on the nodes as a virtualised stack.

is the explanation valid for ETH1 or for ETH2? - it's because we are talking about miners, MEV, etc. If it's only ETH1, maybe it's good to say it?

Also note that they changed the definition from miner extractable value to maximum extractable value.

Is the setup a once every transaction or once every network launch?

once every SNARK based proof system launch

is the shared public ledger effectively the chain of hashes? how are these information stored and distributed in each nodes in the network?

each full node has all the data

If you mean for the Ethereum network - this is stored on contract storage which is replicated on nodes over the network. We also have off-chain data like events, that give enough information (i.e. block number) to query on chain data to reconstruct data if required.

is there a cost to host a website in ipfs?

Yes, although not much (check pinata.cloud). As the data will need to be pinned. IPNS might be the a better solution as website content tends to get updated.

Is there a difference between importing OpenZeppelin contract vs inheriting OpenZeppelin contract?

you have to import to inherit

Is there a feasible way to use Merkle Trees to verify a set of data without knowing the order of the data (the leaves of the tree)?

You would need to know some data like index to verify - https://solidity-by-example.org/app/merkle-tree/

Is there a guide for how to link a github account to hardhat?

This would be as simple as making a remote repo on your github account and pushing your local repo (with your files) to that remote folder

Is there a list/db/webiste that summarizes the aim and give some sort of feeback/rating to the most important/valuable projects/tokens? So many around

https://defillama.com/ maybe?

is there a plan to expand the method ID derivation beyond 4 bytes? like something much harder than what the Poly exploiter took advantage of?

The exploit happened because of bad design. delegate call was used, not the collision of the hash function necessarily.

is there a technical explanation for the lack of floating point arithmetic support?

It is because the data has to be deterministic - i.e. the data has to be reproduced exactly as is on very node. If there is a floating point number there will be unpredictable results which will cause difference in state across the network.

is there a tool to measure or calculate the gas of each transaction?

yes, gas reporting plugins

is there an engineering design advantage for not allowing floating numbers?

EVM can't allow floating numbers as it is executed by different nodes with different CPU architectures handling floating point in different ways. And we need the same results on all nodes. So we can't do floating point operations.

is there an Ethereum version similar to bitcoin Lightning Network?

https://ethereum.org/en/developers/docs/scaling/sidechains/

is there any advantage of writing your own code instead of importing a contract?

Writing your own code is normally more gas efficient however there is a higher chance of shooting yourself in the foot as Solidity has many foot guns.

Although using OpenZeppelin contracts may not be as as gas efficient, they have been audited and will be secure if implemented correctly.

is there any difference if we run the "it" functions inside the first "describe" function versus creating a new "describe" called deployment?

no, this is just for code readability, behaviour driven development style tests

is there any equivalent of "hardhat node" -- a local blockchain -- for these layer-2 solutions?

check for example Protostar project for StarkNet

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

copilot did work surprisingly well with solidity

is there anyway to save these Q&As sessions?

yes we archive them and will put them on discord

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

you can extend a class and implement some interface. not sure what superclass is.

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

Isnt the mapping similar to index except it allows retrieval one at a time rather than a full dump?

Correct and is used as a way to store and read data efficiently

Let's say you build decentralized Facebook and want to store an array with the friends from a person. Is storage friends[] the way to go, or The Graph, or...?

It's too expensive to store on the EVM storage. Look into Layer2's or off-chain data storage.

maybe a bit tangential, but how can the testnet accurately test contracts, without using tons of gas/resources?

It does use test gas/test eth but test eth is free and can be obtained from a faucet so it's doesn't matter so much. generally the faucets limit the amount of eth you can get to prevent abuse though.

multichains like cosmos IBC or DOT with its equilvalent, have been safe within its eco? its only when bridging outside the eco, the bridges have been victims?

correct

Noob perspective: seems we need to write more code to do the testing than the actual coding. Is that normal?

Correct. Also the context switching can be less if you're using Foundry as the tests are in Solidity and not JS.

Noob question, how is unit testing via Ethers diff than calling functions under Remix "Deploy and Run Transactions"?

unit tests are program that test units of your code. deploy and run is manual testing.

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?

No, you are able to reuse the deploying account (EOA) to create new contracts.

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

Pinata is an IPFS service? https://www.pinata.cloud/

IPFS pinning service

please elaborate on 100% test coverage. how one should measure that?

100% means all lines covered with a unit test. there are plugins to measure that

Poly Midon sounds really impressive if true. Why less fanfare than Starknet? People dont believe?

it doesn't work yet

Possible to enlarge fontsize of Remix editor code ?

you can change zoom level in Zoom. Please zoom in

proxy contracts need to be implemented at the creation of your implementation contracts? or can any smart contract be upgraded with a proxy later on?

You could deploy a new proxy to point to an existing contract but you can't change an existing immutable contract into a proxy.

Question for optimizations - modifier is copied every time it is used, so modifier to a function that does the same could save resources?

You could use require statements or even inline function. You would need to see the gas costs when you test. Read here for more info: https://ethereum.stackexchange.com/questions/29867/using-require-or-modifier

Re. pub key > address: how can we verify the signature of a transaction if we don't even have the public key, but only the address?

If you have values (r, v,s) you can recover the public key with ecrecover function. Look here for more info: https://coders-errand.com/ecrecover-signature-verification-ethereum/

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

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

Searchers are bots or programs? how do they work?

We'll see an example shortly

Programs/bots are independent operators that look for arbitrage opportunities

https://ethereum.org/en/developers/docs/mev/#mev-extraction

should the modifier be entered before each affected function?

yes

Yes, its added before the curly brackets

Since the address changes when the data is modified, does the original address still have the unchanged version?

Yes

Yes, as long as it's still pinned on the IPFS nodes

Slightly off topic: Is there a way to easily transfer ownership? or create a function to do so?

Yes there is, transferOwnership function with onlyOwner modifier (custom function, a lot of contracts use this). There is also a library by Open Zeppelin which you can use. https://docs.openzeppelin.com/contracts/2.x/api/ownership

So assert is just for testing your code

yes

So Cosmos and DOT have solved the trilemma?

Not an expert on those but I believe cosmos and dot both have a validator limit . so they are less decentralised but more scalable and equally secure.

So depending on how you hash the public key, you 'choose' which address you want to use for that same private key.. since one private key = many addresses?

one private key is equal to one public key. One mnemonic can give you many private keys what equals to many addresses. Check BIP-39

so he was brute forcing ¨offline¨ and once he got the correct hash, he sent the transaction to the blockchain?

yes

So if we make two or more transactions the log will always show the last score we set. Is there a way to see all the changes without going to each transaction?

As it stands no. However you can make an app that tracks the changes if used with an event. This is usually left up to 3rd party apps

So if we use Foundry, how to use Ether?

If you use Foundry you will not need to use Ethers as Foundry is based on Rust whereas Ethers is a JS library.

So remix cant do testing? only hardhat/foundry/truffle can do tests?

There is a "Solidity Unit Testing" plugin within remix.

So there are no data structures in solidity that allow for iteration? Or only mappings don't allow it?

Dynamic or fixed arrays.

So when an L2 has its own VM like Starknet and is not compatible with EVM, how do they plan to attract devs? wont they require a total rewrite of their dapps?

Some devs are rewriting, some are using Warp to transpile Solidity to Cairo. Developers will go there where users and liquidity goes.

so, if no exprience with javascript, foundry is the best choice?

Yes. Foundry is nice.

The storage type must be always felt or it can be a struct?

it can be a struct

tx with ether js are the same as https://etherscan.io/txsPending?

pending is just a state of the transaction

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?

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

w/ the future planned eth features, where full nodes will no longer be required or need to keep all the history, wont that remove the need for decentralization?

no, this feature is done to improve decentralisation

Waht is IR in the zkevm taxonomy chart?

Intermediate Representation - which means a lower level language like YUL or it's equivalent on other chains.

was the poly net exploit like a man in the middle attack?

kind of yes :)

wasnt plasma a state channel on Eth?

plasma chains are different that state channels

What about OpenZeppelin's tool? https://github.com/OpenZeppelin/solidity-docgen

thanks Ive added it to the lesson notes

What about optimistic rollups?

optimistic rollups are not relaying on zero knowledge proofs.

What are some good ways to measure how decentralized a network / a chain is?

number of independent miners / validators etc. depends on blockchain.

what are the differences between hardhat and truffle? is any of the two better or more used?

hardhat is much more popular choice right now

What are the possibilities of using formal specification at some point of a blockchain career? How often is being used and how important it is to learn it?

Only larger projects invest in formal verification. So if you want to work for blue chip companies then knowledge of formal verification is an advantage.

what defines when most students finish doing homework? by time or by submissions? if the latter, where should we submit?

As suggested by Derek you should push to github as part of your "portfolio". We would share answers on Zoom for you to self assess once the majority of the class has done them

what do you mean by contract bodies?

code of the contract in { }

what do you mean when doing testing you do in solidity and not in JS? isnt the smart contract written in solidity?

Yes smart contract is in solidity but you hardhard tests are written in JS.

what does push to github mean? is there a ethdenver bootcamp github that we need to push to?

Your own GitHub repo

what does the ethcrosschainData contract do?

`EthCrossChainManager` contract is used to verify the block header synchronized by the Poly Chain to confirm the cross-chain The authenticity of the information. The `EthCrossChainData` contract is used to store cross-chain data, and the public key of the relay chain validator (ie Keeper) is also stored in this contract.

what dose an ABI exactly do?

The ABI/application binary interface is an interface/representation of the inputs/outputs of a contract and is needed to make calls to a contract.

what happens if one forgot to emit and deployed the contract, is there a way to see the log?

if you didn't emit then no

What happens if we use the same name for a contract variable and a storage variable defined in a function? Is it allowed?

No, the compiler will throw up errors.

What happens to the suggested blocks that aren't selected? Are they disregarded and those clients that proposed them just accept the block that was accepted?

correct.

These are called Uncle blocks and are discarded. Ethereum uses something called the GHOST protocol (Greedy Heaviest Observed Subtree)

.

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

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

what if storage within each node grows to the point where it is no longer feasible for the general public to

enter/ afford?

we already have this issue. full ETH node is 5TB, full BSC node is 20TB. Ethereum has 'purge' in a roadmap, purge is going to minimise blockchain size.

What if the dev is also a founder..? Should you relinquish ownership to a second wallet?

multisig and timelock mechanism seem like better solutions

what is "once every SNARK based proof system launch"? more context to describe the frequency?

one blockchain launch equals one SNARK based proof system launch

what is a proposer? a builder? a validator? how are they diff?

See lesson 2 notes, the proposer is given a slot to propose a block, which validators will vote upon, the builder if different to the proposer assembles the transactions for the block

what is an airdrop?

When you distribute tokens for free based on some metric such as network usage of users etc

what is the "interface" keyword? what does it do?

In Object Oriented Programming, an Interface is a description of all functions that an object must have in order to be an "X". Again, as an example, anything that "ACTS LIKE" a light, should have a turn_on() method and a turn_off() method.

What is the correct Discord channel for this Bootcamp and how do we know which one is our team?

Please look for the ETHDENVER BOOTCAMP channel in discord. Your teams will be selected by Encode in due course.

What is the decentralized storage topic that Laurence was supposed to cover? is it like IPFS?

Yes, also Filecoin and Swarm.

What is the default value of address?

0×0000....

What is the difference between Ethereum Rollups and Bitcoin Lightning Network?

Lightning is a sidechain, doesn't use rollups

Bitcoin Lightning Network is a Sidechain. Sidechains relies on trusted parties to attest and rollups provide evidence about the state of the L1 network.The difference between a Sidechain and a Rollup is whether the bridge contract can self-enforce the validity of transactions on the L1 network or if it must rely upon a trusted set of parties to attest that it is valid.

What is the difference between gas, transaction cost, and execution cost?

tx cost = tx fee = execution cost === gas * gas price

What is the fundamental difference between Formal Verification and an Audit?

Formal Verification is a mathematics based methodology. Proves that code can't behaviour in a certain way. Audit is a process that combines multiple methodologies, can include formal verification.

What is the limit for the size of each chunk?

256 kilobytes

What is this "migration" of Sushiswap?

Easy way to move liquidity from uniswap to sushiswap

what is unit test?

Smallest piece of functional code that you can test in isolation

What makes one block more attractive vs others?

Miners/Validators are incentivised to mine/produce the transaction that pays the most

What will happen to the companies which are completely based on ad-revenue as they use our data?

Life after Google addresses this question. Summary here: https://www.blinkist.com/en/books/life-after-google-en

what's on-chain and off-chain? and how are they synchronized together?

on-chain means data computed on blockchain or data stored on blockchain. off-chain means computed not on blockchain nodes or stored not in the ledger. How to synchronise? Off-chain data can be proven by storing hash on chain. Or off-chain computation can be stored on chain using zero knowledge proof.

In addition to the above, an example of off chain data on Ethereum is Events which can only be viewed on the block explorer (etherscan.io). Smart contracts cannot access this data. It can only be used by other apps to query the blockchain.

What's the default visibility of variables?

Internal

What's the link for the gitpod?

https://gitpod.io/#https://github.com/ExtropyIO/SolidityBootcamp

What's the point of an external fn? it seems like it needlessly restricts things? any advantage to having the contract NOT being able to call its own function?

for security reasons restrict everything as much as possible.

It also a good way to save gas as public functions create a getter function too

what's the pros/cons between infura and alchemy?

individual choice for you project around things like pricing, supported chains, features

what's the purpose of hw 19 to create a shame coin? I don't understand the real life concept of this contract

Main purpose is education. Real life concept? Mark bad actors on a blockchain by sending them a $SHAME coin. Bad actors like sandwich bots, hackers etc.

Or even SBF :)

whats a failing test? and what do these tests test?

They test the functions and methods within the contract.

whats a natural field element size?

less then 252 bits, more then 251 bits usually

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

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

whats the optimizer?

https://docs.soliditylang.org/en/v0.8.17/internals/optimizer.html

whats the tradeoff when you have L3 and L4? Sort of sounds like AVAX subnets in concept but they dont have this notion of going up in higher layers

Good article about this: https://vitalik.ca/general/2022/09/17/layer_3.html

When deploying from Cairo Playground, we are not prompted to enter our address. How does it know who created the program? I expected that the Wallet prompts.

right now users can send tx's w/o wallets

When i declare a variable (like mapping) do i need to initialize it or it's as default set to an empty valid object of the type "mapping"?

Default value is zero for all types

When should you do audits, before deploying to testnet, after deploying to testnet, both, after deploying to mainnet?

before deploying to mainnet

Audits can cost a lot of money. So you should do the audit when the code has been frozen. It's also recommended to engage the audit company from the beginning so they can steer the project in the right direction.

When testing with Hardhat, do you need to define the events again in Typescript, or you reference the events by name?

reference by name

when we click on getScore on the DeployedContracts on the left panel, are we interacting externally or it's internal?

externally

When would be the best case to use enums?

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

When you fork and unlock account, you have funds equal to what that address has?

yes

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

yes

when you measure gas cost : does the way you write the test function influence the result?

no

Where can i find the documents from last time?

Encode Discord → Ethdenver Bootcamp → Course Materials

where do you get "chain id" for the mainnet fork?

it is going to be 1, this is just on your localhost

where does the 'newScore' function parameter value come from?

one that invokes the method is has to pass it

Who conceptualized AAM?

https://vitalik.ca/general/2017/06/22/marketmakers.html

who pays for storage on IPFS when it proliferates/multiplies remotely?

Whoever is running the node. https://www.pinata.cloud/pricing is service with generous free limits

Why are many attacks related to bridges? like wormhole, ronin, etc? something to do with cross chain?

yes, cross chain is hard, different teams have been developing separate solutions and many of them made mistakes.

why are some languages, such as Haskell and OCaml, are claimed to be easier for formal verification?

these are purely functional programming languages, functional programming languages are easier to prove then imperative and OO approaches.

why are we so hardhat focused? wonder what % are using Foundry

hardhat is still more popular

why builders dont steal from proposers?

in what way ?

why cant zkstark provide privacy currently? only scale?

Limited resources. Privacy is coming, but scaling first.

Why do i emit the argument of the function (newScore) and not the variable score?

Because if you pass the variable this would actually emit the old state, as it takes time to store and replicate through the network

It makes more sense to emit the parameter to save time and computation

Why do popular contracts like ERC20/ERC721 don't seem to have "optimized" function names?

they must adhere to ERC20 / ERC721 standards

It helps readability for users, developers and auditors. The Solmate library uses the hash to save gas.

why do we need location for string parameters but not with uint or int

This is because strings have to be converted to bytes32 and we don't know how many slots we need rather like a dynamic array. Using memory allows the EVM to store it temporarily to be used in a function.

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

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

Why does web3.estimateGas often come back with "unable to estimate gas" error?

this is when it can't run the tx

This is usually with complex functions which can't be estimated accurately

why even use remix at all if we end up exporting our smart contract to foundry? cant we just write our smart contract in foundry?

You can, but Remix is quicker for instant feedback of compilation errors

why fork mainnet when one can user Goerli?

to test your contract against mainnet data

why is multi-chain less secure? what about it makes it so?

usually bridges. many different bridges with custom, often insecure & centralised, implementations

Why is Rust popular in web3 context?

Speed, Low level features such as control of memory, safety(memory safe etc), general design specialised for systems programming, compatibility with web assemble etc.

why use msg.sender instead of hardcoding the original owner?

Bad practice to hardcode values. Transferring ownership may be recommended for security i.e. transferring contract to multisig later on.

why would someone put up their code onto etherscan? esp like their mint function etc

the code is on the blockchain anyway, just in a bytecode, not easily readable. Why would one make it easier to read? To gain users trust.

why would you ever use an earlier compiler version?

No. Later compiler versions (solidity versions) have extra security features like safemath library (which prevent under and overflow issues) in version 0.8.0^. Also there are built in optimisations too

Will be the session recorded somewhere? There is lots of info that I would love to retrieve

youtube link is going to be posted on Discord tomorrow

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

yes

Would holding the data outside the contract and make each version will just point to where the data is work?

This is the idea about proxies, the data is in the proxy and the functions are in the implementation

would images also be stored in the abi?

images in smart contracts? abi is only an interface, no data

Would using "public" as the function in line 12 ultimately save gas since it is less functions?

Public functions cost the most gas compared to the other three visibilities

would you call “number" in contract Storage a 'global' variable ?

state variable, it is in the contract, not global

Would you recommend Open Zeppelin Defender or Tenderly?

They are both good. Tenderly does seem to have a better UX and extra features.

Wouldn't you want the events defined before the modifiers?

Doesn't matter in terms of compilation but yes in terms for code readability yes.

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?

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

Your test uses address(0) as a deployer. Wouldn't that be a bad practice due to it being the default address?

Yes that's true actually. Good spot.