Replies-Expert_Solidity_Feb_2023-3

Why do they store the data on to the layer1?

The idea is to have the security of L1 but scalability of L2. Essentially because L2 has less security/stake behind them. So putting them on L1 provides security.

Moderator | 02/20/2023

How can we prevent the L2 operator from censoring out transactions and skipping them (not including in any blocks)?

Currently a lot of L2 are centralised so unfortunately we must trust them. That's the trade off of most L2 scalability. But most L2s are building decentralised sequencers

Moderator | 02/20/2023

why don't layer2s just create independent blockchains? why do they have to then reconcile with the layer1? what is the advantage of this?

The idea is to have the security of L1 but scalability of L2. Essentially because L2 has less security/stake behind them. So putting them on L1 provides security.

Moderator | 02/20/2023

How can we prevent the L2 operator from censoring out transactions and skipping them (not including in any blocks)?

The sequencer is centralised not the whole L2 that is.

Moderator | 02/20/2023

How can a trade be reversed? Bond might not be sufficient enough to pay for a loss I guess

It could happen in the case of a re-org on the L2 for example.

Moderator | 02/20/2023

How do I announce to L1 that I am L2 network - is there certain handshake protocol, etc.?

There is no protocol as such. Each L2 will have their own custom contract on the L1 which handles the interface between L2 and L1

Moderator | 02/20/2023

Is it then more expensive to use zk rollups?

Yes there is more data to be processed. Making proofs but one approach is to batch more transactions into each proof which make it cheaper.

Moderator | 02/20/2023

If something goes wrong with L2, can we get all the transaction information from L1?

Yes you can reproduce the L2 state from L1 data.

Moderator | 02/20/2023

Which receipt is "valid", L2 transaction or L1? After being paid on L2, can I be sure ill receive the money? Or there can be a problem when writing on L1?

Generally when a transaction is accepted on L2 it is considerer to have reached finality but yes correct there is a small risk that it could be rejected when being posted to L1.

Moderator | 02/20/2023

the L2 sort of "clones" the entire current state of L1(regularly) to process tx before sending the data(after tx) back to L1? is that a sort of simple way?

No the L2 state is separate and it does not clone L1.

Moderator | 02/20/2023

In the event of a fraudulent transaction in optimistic rollup, isn't it difficult to roll back all the transactions after this fraudulent transaction posted?

Yes this is a very complex and difficult to do in practise.

Moderator | 02/20/2023

Is ethereum mainnet looking to implement the compression techniques implemented on L2?

Yes for sure. The roadmap has a lot of these changes: https://twitter.com/VitalikButerin/status/1588669782471368704?lang=en

Moderator | 02/20/2023

Are there any 'sidechains' on ethereum that aren't rollups?

Generally no if you mean specific app chains although we might see something like that soon in L3s . We already see some specialisation such as optimism focusing on gaming.

Moderator | 02/20/2023

If L2 could take so long, it doesn't quite seem like an optimisation?

It's a trade off. Gas is very low so optimised but yes true finality could be said to be slower.

Moderator | 02/20/2023

Do you think that some other language will replace Solidity for EVM?

Potentially but it would be difficult because solidity is so widespread and known within blockchain ecosystem. The tooling and libraries are very well developed. But of course it is possible.

Moderator | 02/20/2023

seen radix?

yes cool project.

Moderator | 02/20/2023

How would L2 rollups and L1 sharding coexist on Ethereum in the future? Building L2 networks for each shard?

Not 100% sure but this might be a good read: https://notes.ethereum.org/@vbuterin/proto_danksharding_faq#What-is-Danksharding

Specifically the way L2 will make use of data blobs.

Moderator | 02/20/2023

Can contracts deployed on L2 to communicate with contracts on the L1, such as checking the balance of an ERC20 for a wallet address on the mainnet?

I think you need to write a bridge contract so technically possible but not easy.

Moderator | 02/20/2023

The bundle of Txs from L2 , do they appear as 1 or multiple Txs on L1?

Yes so all L2 Tx's are bundle into a single L1 transaction.

Moderator | 02/20/2023

If this type bug persists in smart contract, isn't it scary to do DefiFinance?

Yes you need to be very security focused. But also over time best practise and libraries have been developed which has helped.

Moderator | 02/20/2023

what is the point of having an 'emergency' withdraw? Seems like an obvious point to attack

To prevent funds getting stuck in the contract or to remove funds in the case of an exploit.

Moderator | 02/20/2023

Why isn't tornado cash forked onchain? Or is it and we don't know?

You can fork the code but not the mixset so a fork would not be as secure although think they exists.

Moderator | 02/20/2023

any projects you are aware of that translates hardhat test scripts to solidity?

Not aware of one but you can use hardhat within Foundry which will go through later in the lesson.

Moderator | 02/21/2023

this is something certora prover tries to do? (invariant testing)

Yes similar. Invariant testing is part of Formal Verification.

Moderator | 02/21/2023

what would you recommend to use for CI/CD integration other than github for SAST?

Maybe something like https://docs.tenderly.co/simulations-and-forks/simulation-api/integration-guides/ci-cd-pipeline-for-smart-contracts

Moderator | 02/21/2023

Is the rpc call eth_getProof supported by foundry ?

https://book.getfoundry.sh/reference/cast/cast-proof?highlight=get%20proof#cast-proof

Moderator | 02/21/2023

Foundry fuzzing is similar to Brownie parameterized testing?

We don't use Brownie much but it sounds similar.

Moderator | 02/21/2023

What are advantages of fuzz testing over static analysis? (If I got that phrase right - kind of formal verificatoin of edge cases)

Static analysis is more focused on catching known vulnerabilities/pattern matching. Fuzz testing is specifically targeting unknown vulnerabilities by subjecting functions to random values. Fuzz testing with invariant testing gets more towards formal verification. Where Foundry is great is being very accessible and having a good level advance testing tools.

Although there are tools that focus more on formal verification they are usually require specialist knowledge.

Moderator | 02/21/2023

How many weeks total does this course run? Are there plans to make up for the 2 days missed at the beginning?

If we don't get through all the materials we can add two lesson on. course is 5 weeks ending mid March

Moderator | 02/21/2023

INFO: Seaport uses both hardhat & foundry tests in the same repository. https://github.dev/ProjectOpenSea/seaport

thanks

Moderator | 02/21/2023

when i was using slither, it complains addresses on constructor doesn't have a require statement for non-zero address check, is it coming from this hack?

More a general check. Important because it is easy to leave a value blank/zero address and this can cause all sorts of problems.

Moderator | 02/21/2023

is the poly network hack an example of a function selector manipulation?

yes

Moderator | 02/21/2023

And the reason this hash collision was possible is because only a few bytes were needed for the function selector?

yes exactly.

Moderator | 02/21/2023

I guess Poly attacker did not doxx themselves after being offered a job?

As far as I know he stayed anon and didn't accept the job offer haha.

Moderator | 02/21/2023

What if a single contract has two functions whose selectors collide?

The Solidity compiler is smart enough to detect function clashing during compilation so that can't happen.

Moderator | 02/21/2023

Is the only option for a protocol hack like this moving forward is to have upgradeable contracts or deploy new contracts and reroute traffic and funds to them?

The main thing is to make sure if you have a function that can call other contracts make sure it cannot call restricted contracts or functions.

Quoting from rekt:

One of the biggest design lessons that people need to take away from this is: if you have cross-chain relay contracts like this, MAKE SURE THAT THEY CAN'T BE USED TO CALL SPECIAL CONTRACTS. The EthCrossDomainManager shouldn't have owned the EthCrossDomainData contract.

Separate concerns. If your contract absolutely needs to have special privileges like this, make sure that users can't use cross-chain messages to call those special contracts."

Moderator | 02/21/2023

Can you explain again wht the function signature (params) couldn't be changed?

Just the way the function was written. The func params where hard coded.

Moderator | 02/21/2023

What's the benefit of cloning a tx?

If you realise that a tx in a mempool is going to be profitable, you can clone it, put it into the mempool with higher gas fee and get the profit.

Fox Reymann | 02/22/2023

Is there any incentive for flashbots not to MEV? Would it even be possible to have a fraud-proof incentive to run flashbots?

possible, it is their system, but Flashbots is a research and development organization working on mitigating the negative externalities of current Maximal Extractable Value

Fox Reymann | 02/22/2023

Doesn't front-running mean the front-runner pays more gas fees so that their transaction is executed first?

to front run you have to pay more gas, but your goal is to extract more profit then the gas cost

Fox Reymann | 02/22/2023

if i send tx through flashbots, and it gets frontrun - what ahppens? flashbots say it's not them, I say it wasn't me...

such operations would destroy their reputation.

Fox Reymann | 02/22/2023

what's a profitable block?

block that gathers tx's with highest reward (tx fees) is the most profitable block

Fox Reymann | 02/22/2023

Why is MEV accepted as inevitable? It seems like a false narrative perpetuated only to serve the biggest actors

there is always going to be a war, like between hackers and cybersecurity professionals

Fox Reymann | 02/22/2023

That's a hard problem though, isn't it? - "something in the protocol so they 'have to' accept highest bid - how to prove they received it?"

that is how the software works, it is open sourced. cheating would destropy Flashbots reputation.

Fox Reymann | 02/22/2023

what does flashbot do? are they are solution to combat MEV?

they do lots of things. Will is explains at the moment. More details on their website.

Fox Reymann | 02/22/2023

Is MEV opposed to decentralisation? Zero sum like a trilemma? or are there solutions which are MEV-proof without tending to centralisation? commit-reveal? ZK?

ZK blockchains / L2s can solve MEV

Fox Reymann | 02/22/2023

Is there a reason OFAC-censorship-resistance is improving?

the more decentralised Ethereum will become the more censorship resistant it is going to be

Fox Reymann | 02/22/2023

best decompiler in ur opinion?

I would go with https://ethervm.io/decompile

Fox Reymann | 02/22/2023

Do these MEV mitigation attempts then hamper the ability to cancel your own transaction by making a second one with a higher gas fee?

no

Fox Reymann | 02/22/2023

You could pay more gas to the sequencer to put your tx first?

but you don't have access to the mempool so how would you frontrun?

Fox Reymann | 02/22/2023

Can we retry and add new submissions for the same level?

yes

Fox Reymann | 02/22/2023

Can you explain withdrawl time period in arbitrium, how it works ?

arbitrum optimistic approach to validity requires time period to allow submitting fraud proofs. hence we need withdrawal time period, to make sure block is valid before one withdraws

Fox Reymann | 02/22/2023

Also how sequencer take care of loads and how it is communicating with ethereum. There is geth which is complied as lib right?

Arbitrum is using geth, probably compiled as a library, would need to check

Fox Reymann | 02/22/2023

Smaller variable is not necessarily cheaper... require additional operations. Does this mean using a larger data variable is more cost efficient?

Depends if you pack the variables into a struct for example that might offset gas of extra operations. So it's always good to test gas and not assume one will be cheaper than the other.

Moderator | 02/23/2023

structs vs mappings? which is more gas efficient?

Depends how many variables you want to store. If you have 10 mappings it's going to be cheaper to store than data in 1 struct. If you have 2 mappings might not be worth using a struct

Moderator | 02/23/2023

what's the way to reuse memory without using assembly? using block scopes?

The compiler doesn't free memory so you can't reuse memory without assembly.

Moderator | 02/23/2023

why are is using unchecked cheaper in for loops that checked?

Overflow check costs gas.

Moderator | 02/23/2023

why is using ++i cheaper than i++ in a for loop?

Good question. Long story short, i++ returns the non-incremented value, and ++i returns the incremented value, so for example, doing

https://ethereum.stackexchange.com/questions/133161/why-does-i-cost-less-gas-than-i

Moderator | 02/23/2023

If you already have a contract in place, would you redeploy with newer solidity version?

Would depend if the optimisation were worth the time and effort to do so.

Moderator | 02/23/2023

is there a benefit to passing structs as function arguments rather than individual variables?

It may be cheaper to use a struct if the compiler can pack those values into less memory slots.

Moderator | 02/23/2023