Slido Q and A from Week 3

I understand less and less each lesson and it is getting close to zero. I think I am missing too many pre-requisites.

```
 If there are questions or topics that are difficult, let us know on Discord and we will try to give more materials and resources to help you out.
```

Is there any online content I could read though to get back on track or something that would allow me to just get a little from the coming lessons?


```
 If there are questions or topics that are difficult, let us know on Discord and we will try to give more materials and resources to help you out.
```


Are there L3s out there in production yet?

```
 I believe Madara (on Starknet) is production ready.  https://www.madara.zone/
```

By randomness do you mean using the powers of tau?

```
 Yes, that is one process to use for the randomness, but we will explore this in the upcoming lessons.
```

Can proofs be made homomorphic? So we can P1 + P2 and verify the result with the same computations as just for P1?

Not in a simple way, but we will explore in the upcoming lessons.

Can you repeat? What is an argument for VeriftTx function in solidity? where should i get that from proof?

You need the generate the proof which then you will receive the verifyTx argument and you can use that to verify the transaction.

Does zokrates have R1CS constraints similar to circom?

Yes, it's close to R1CS but still encapsulates witness generation. https://zokrates.github.io/toolbox/ir.html

For layer 2: is executor a smart contract or a node that run on the L1?

For Layer 2, as we explored for example with Starknet, you have the Sequencer which bundles all the transactions together and generates the proof which is sent to an L1 smart contract that verifies for integrity. Nodes are synchronizing and process the transactions of the network.

Have Optimism made it easier for people to build on the OP stack than, for example, Arbitrum or other L2s?

I believe a lot of L2's have made significant progress overall in terms of people building on their stack. I personally don't have much experience with the OP stack.

how can we know the pk and vk in remix?

```
Remix only shows the verification key.
```

Is token bridge done by normal bridge solution, not special way, between L2 (e.g. Optimism <-> Arbitrum)?

```
Yes. Check orbiter finance
```

Is zkPorter just an offchain DA layer that can be used in combination with zkSync DA on L1?

```
"Yes,  you have the option of off-chain DA. https://era.zksync.io/docs/reference/concepts/zkSync.html#the-state-of-zksync"
```

is zksync era an hyperchain too? i thought hyperchains were L3s?

```
zksync era is a generalized L2.
```

It's not related to lesson, but job board channel in discord seems to have closed. Does Encode club no longer share such information?

```
Thanks for pointing it out. We will share it with Encode Team. :)
```

With regards to this point about L3s not scaling as a clone of L2, settling on L2, wouldn't it be the case that a batch of transactions being reduced to 1 state diff transaction on L2 rather than e.g. 745 transactions directly on L2 that this one state diff transactions would represent a significant cost saving in terms of gas?

```
Layer 3's would play an important role in the ecosystem and scalability. Currently afaik Layer 2 would be more for the financial aspect, while Layer 3 would play a major roles such as gaming,
```

where you could define your own specialized settings for your layer. In terms of scalability, we are yet to see how this plays out.

So is the priority-queue something on the bridge smart contract on the L1 and is accessed via an RPC call to the L1?

Yes that would be correct. But the specific implementation can vary depending on the L2.

We saw that there are several solutions for DA other than Ethereum (e.g. Celestia), are there any alternative solutions also for the Settlement part?

Storage proofs is an interesting are to explore

What do you mean about data availability in the blockchain space? I mean this is hard to store data on the blockchain as this is extremely costly on chain no?

Yes, storing data on-chain is extremely expensive, hence the data availability problem. https://ethereum.org/en/developers/docs/data-availability/

What does it mean for an L2 (or L3) to have the same security of the L1? What are the features/mechanisms that are required to be considered secure?

It inherits the properties from the L1 in that sense. Similarly for L3, they would inherit the properties from the L2 and L1.

Features/mechanism to consider could be data availability, consensus mechanism, etc

What does it mean to say optimism has access to L1 state root?

Refers to the ability to interact with and reference the state of the Ethereum.

What does validating bridge mean? How is it different from a regular token bridge between two chains?

It focuses on moving transaction from a network to another off-chain system. https://www.infura.io/blog/post/validating-bridges-scaling-blockchains

What is the exact difference between app spesific layers and generalized l2's? Can we consider these app spesific chains like permissioned chains?

Appchains are layers that have their own designed settings to operate. Take for example a game, they can defined their own settings for a particular game for example. Generalized L2's these are scaling solution for L1 and L2's can operate for many different apps.

Why does the chart say that Ethereum is the data availability layer? Isn't the data on Ethereum some sort of compressed merkle tree, as it relates to layer 2?

Data Availability refers to the issue that all Layer 2 are facing. All of them are competing for

```
the same resource and where the majority of the cost comes from.
https://ethereum.org/en/developers/docs/data-availability/
```

Are "portals" like bridge relayer contracts?

```
 "Portal contracts connect to specific Aztec contracts, so there will not be 1 canonical bridge like there are in other L2s. You can also create custom bridging logic, transaction batching, etc (voting, swaps, NFTs, identity, etc)."
```

Can I do illegal things on Aztec and get away with it?

```
 May raise this later!
```

Can L2 choose to post only a subset of its transactions to L1?

```
 No, I don't think it's possible.
```

How does Aztec deal with smart contract events i.e. if user A makes TX and smart contract fires event at same time, tx could be inferred?

```
 UTXO structure allows multiple people to update the same state at the same time.
```

How is this lecture linked to zkSync?

```
 The course focuses on zkEVM which is helpful.
```

I am still struggling with UTXOs vs Ethereum do you have a short example to get it simply what is the difference between both and

what is the cons/pros? thanks!

```
 There is a great article discussing about UTXOs vs Account Model (Ethereum) and their pros/cons. https://medium.com/nervosnetwork/my-comparison-between-the-utxo-and-account-model-821eb46691b2
```

If state and nullifier trees are append-only, doesn't that lead to the size of the data for the chain growing very quickly?

```
 Correct! And we'll need good solutions to manage this.
```

If the user executes txs locally to produce a state diff, do they need a fully synced blockchain on device?

```
 Yes!
```

In Aztec, is the proof generated on the user's local device? Is that resource intensive?

```
 "Aztec executes private L2 functions and state updates on a user device. This is the way to preserve privacy, users don't send any sensitive information anywhere    Data is stored in the private, UTXO based state tree."
```

Isnt Zama more MPC than FHE?

```
 Yes, their approach to FHE is more related to MPC. In their model there are 4 entities involved: encryptor, decryptor, someone doing the FHE computation and adversary (which is similar
```

```
to an MPC). https://www.zama.ai/post/fhe-as-a-
puzzle-piece
```

"John Adler mentioned that in the worst case the user still need a user to run a full node

to reconstruct the state, so you don't get any scalability?"
I believe you refer to the Blockchain Trilemma. I would advise to read Vitalik's take on the Blockchain Trilemma.

Are arithmetic circuits anaolgy to logic gates?

```
 Somewhat, both perform operation but in
different ways.
```

Are we going to get some sort of coding homework soon to help solidify all this info we're receiving?

```
 Yes, we will have some coding examples to help
with that.
```

Do you know why TinyRAM didn't work out?

```
 I'm not familiar with that.
```

How "fat" is a typical row in these circuit tables?

```
 We will look at this in the upcoming sessions.
```

Instead of loop inside zk circuit, does circuit verify all data change (memory, storage, stack) is correct from opcode, current data, and trace data by opcode?

```
 zk circuits form a set of constraints that if
satisfied, prove a computation was carried out
```

```
correctly. It is similar to a Sudoku where you
verify if the solution is valid and not solve it.
```

So can zkevm sequencers in current systems alter the state as they like if they are in charge of execution and proof generation?

```
 No, the role of sequencers is to bundle/execute
transactions and generate proofs.
```

So is there only one circuit for the VM and for transactions we provide different instances/witnesses?

```
 We will look at them later in the course.
```

The constraint, is verified like an assert method?? I am confused if its performing the verification through the calculation or not

```
 The witness can be the trace of the operation of
the VM, so you will need to think carefully about
that. In a proof we need to make sure that all
the parts are executed correctly.
```

The zkEVM is to solve the issue about the centralization of sequencer?

```
 Centralization of sequencer is another topic
which L2s are currently trying to address it.
zkEVM is where the computation happens.
```

What does 'IR' stand for in that diagram?

```
 Intermediate Representation
```

When any one proof can be verified on-chain, what is the need for multiple proofs?

```
 We need to create multiple proofs and than
aggregate them and send it to L1.
```

Where is the sequencer and verifier in the scroll diagram ?

```
 Here is a more detailed diagram on the
architecture https://scroll.io/blog/architecture
```

Why do newer systems use a different field?

```
 Mostly because of their unique design and
optimization goals.
```

A field element is a prime field. Why is it feasible to have a felt 232, but not a felt > 256 bits to support EVM?

```
 Relies on a lot of mathematical properties.
STARK's paper is a good resource to understand
the underling concepts of choosing the field 252.
```

Can you give an example of a custom gate? I've taken a class "Logic Design of Digital Systems".

```
 I'll get an example for you
```

Can you talk briefly about zk systems and quantum attack resistance? Thanks!

```
 ok
```

For the under constrained code, did the case that you add all the opcode = 1 (like add + sub + ... + call = 1) to ensuring that ONLY one opcode can be called?

```
 yes the idea of the selectors there is to ensure that exactly one is called
```

Given the immense amount of applications for zkEVMs, have there been talks of adding precompiles + trusted setup of a pairing curve with a field > 256 bits?

```
 I believe there are discussion regarding that starting from EIP-197.
```

On zkSync once you deploy a smart contract the compiled bytecode is stored & gas cost is significantly reduced on next deploy. Can you show where it is stored?

```
 Might be because of the factory deps, but not entirely sure. Maybe this can help? https://era.zksync.io/docs/reference/architecture/contract-deployment.html
```

What would the other inputs be other than the execution trace? (sorry for the multiple questions!)

```
 For example it could be the built-ins that has been used during that execution
```

what's withdrawal circuit doing? The sequencer and rollup contract handle L2 interaction, so what is the function of withdrawal circuit in the VM

```
 It is responsible to verify the correctness of withdrawal operations.
```

why the field is smaller than 256 bits?

```
 It is mostly performance and optimization specific. For example STARKs has field252 which allows to be more efficient.
```