Assignment 7

1. Question 1:

Celestia is set out to be the consensus and data availability layer for blockchains. Chains built on top of Celestia can concentrate on execution. Do you think data availability is the true bottleneck to scale blockchain? Argue for and against the need for the data availability layer for blockchain.

[ANSWER]

Yes.

There are 3 major ways to scale a blockchain: increase block size, sharding and rollups. Together, these approaches will end up increasing the chain's size exponentially. It's not technically and economically feasible to store and verify all transaction data in one node or client. It must be stored in distributed manner and is always available to all kinds of clients. As separation of concerns, I believe a dedicate layer (or another block chain) to handle the data availability (DA) is a good design. Such pluggable and modular design could eventually achieve millions of TPS.

I especially like the use case that Celestia (and Polygon Avail) works as transaction storage for rollup solution. Technically, I feel it can be a more scalable and extensible solution for zkSync than its own zkPorter.

I'm enlightened to realize that Celestia is startup and developer friendly. It eliminates the needs to build and incentivize validators' community which is too costly to a small project. This work can be outsourced to Celestia through its own validator network.

However, one could argue that such design is already done in L0 block chain (Comos, Polkadot etc) where the main chain only focuses on communication and DA these core blockchain capabilities. Then, gives L1 chains the flexibility to implement its own execution, scalability solution and tokenomics. It's unclear to me that how much advantage Celestia can gain in this fast-moving field. Or it can just focus on supporting rollup solution?

2. Question 2:

Another popular zero knowledge technology in the market today is zk-STARKs. Starkware uses this technology to power dApps such as DiversiFi, ImmutableX, dYdX, etc. List some advantages of zk-Starks over zk-Snarks. In your opinion, which one is better and why?

[ANSWER]

Advantage

1. zk-Snarks require a trusted setup phase whereas zk-Starks use publicly verifiable randomness to create trustlessly verifiable computation systems.
2. zk-Starks are more scalable in terms of computational speed and size when compared to zk-Snarks.
3. zk-Snarks are vulnerable to attacks from quantum computers due to the cryptography they use. zk-Starks are currently quantum-resistant.

Disadvantage

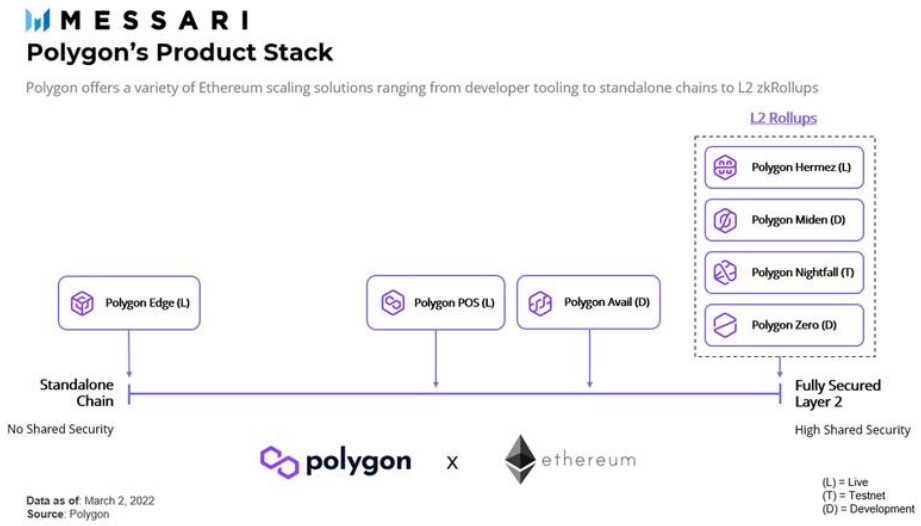
1. The proof size of zk-Starks (> 10KB) is much bigger than zk-Snarks (~0.2 KB), It consumes more gas to verify in smart contract environment and is also limited in mobile use case (that's the reason Celo chose zk-Snarks).
2. Since zk-Starks is younger. The community and tool chain for zk-Snark is more developed than zk-Starks. To highlight, there is no solid implementation for recursion (although possible) which is quite important for bridge and light client project.

I feel zk-Starks is technically superior but for my current project, I would still choose zk-Snarks over zk-Starks to reduce implementation risk.

3. Question 3:

Write in brief (1- 2 line for each) about the polygon's product stack. Refer this [Polygons ZK Product Overview]

[ANSWER]



1. Polygon PoS Sidechain (in production): a layer-1 and EVM-compatible block chain. It helps conducts transaction at a fraction of the gas cost required by Ethereum.
2. Polygon Hermez (in production): zk-Snarks based ZK Rollup without ZK EVM (until 2.0). It emphasizes decentralization and does not need a centralized operator.
3. Polygon Zero (in development): zk-Snarks based ZK Rollup that emphasizes on speed by leveraging recursive ZK proofs and Plonky2. It can generate a recursive proof in 0.17 seconds.
4. Polygon Miden (release in 2023): zk-Starks based ZK Rollup and have a EVM compatible Miden VM.
5. Polygon Nightfall (in production): optimistic rollup that serves enterprises. It focuses on legal and KYC compliance for corporate transactions.
6. Ploygon Avail (in development): data availability-specific blockchain (like Celestia) designed for standalone chains, sidechains, and other scaling technologies.
7. Ploygon Edge (Polygon SDK): an open-source modular blockchain development framework built for engineers who want to create their own blockchains.

4. Question 4:

Write in brief (at least 4 -5 lines) about your learnings throughout the course.

[ANSWER]

Before joining this course, I was new to block chain technology stack. I didn't have any experience on Solidity, very shadow understanding on how Ethereum works, not to mention any concept of ZKP. What I have learned in the past 2 months are amazing and way above my expectation. To summarize, this course:

- Give me a good understanding on the block chain infrastructure, challenges, and potential solutions.
- Master the skills to build Web3 application with cutting-edge technology.
- Specially, lays a solid foundation on ZK technology and expands my technical vision. I'm convinced ZKP is the future of block chain and very excited to start my own journey on this direction.

5. Question 5:

Provide 2 - 3 ideas for your final project. Explain the pros and cons of each idea. Also, provide a draft proposal for the idea of your liking. Refer here for samples.

[ANSWER]

HongBao (Red Packet)

Goal

Express good will without social pressure.

Problem Statement

When people ask friends to do a favor on emergent finance need (for example: curing a disease) or organize a group donation (for example: wedding wish list). Such donation activities are done publicly, i.e., the requester and (probably) the donators can see who and how much each friend donate. This causes social pressure on some friends, who for some reason, may either don't want to give or can't afford the amount other friends give. It also introduces unhealthy competition environment and encourage displaying of loyalty by money.

ZK Solution

By leveraging block chain and ZK technology, HongBao is a web3 application that anyone can setup a donation campaign based on social network relationship while keeping the donors' activities completely anonymous.

Specifically, the requester uses this app to setup a campaign and selectively set an amount goal, then send the campaign link to friends via social network. Her friends can then follow the link to transfer fund anonymously. The requester can see how many people and how much in total made to this campaign but can never find out individual donation (who and by how much).

Technically, HongBao uses ZKP to verify friend inclusion (to support the case that only friend can make such donation) without revealing the donor's identity. To hide fund transfer, a Tornado Cash like shield transfer is implemented.

Open Questions

- The identity verification is inspired by InterRep. But HongBao needs more granular info. We probably can check friends by calling Facebook Graph API but how can we construct a proof to verify friend relation?
- HongBao may only support fixed amount since given the limited friend number (~250 in average), variable amount could make it easier to link transactions by matching the amount number, this defeats the anonymous purpose. How can we workaround this problem?

About the Name

Hongbao means red packet in Chinese. It's a red envelop with cash inside and usually without any written names and amount on it. It's a tradition in Chinese community that

people give it to friends or younger generation during some happy events for good will, for example: wedding ceremony, Chinese New Year family reunion.

Confide

Goal

Enable domain expert express opinion without worrying about punishment.

Problem Statement

Due to social status, concerns on job security and avoids conflict, it’s hard for people with certain domain knowledge to express their true opinions publicly.

ZK Solution

Make use of ZK identity service to mark specialties of a user. Thus, the user can post messages anonymously with proven specialties.

The ZK identity can be as simple as how many followers in Twitter or member of certain group (both are implemented by InterRep), or as sophisticated as academic degree/reward the user received and working experience.

Message can also be supported by other qualified users to gain further credit.

Open questions

- ZK identity is the core of this service. How useful it is before the availability of Polygon ID like service and a board range of trust services?
- More of a social question, without revealing identity, would it encourage people to speak up irresponsibly? Could such service cause more chaos and confusion to public?