zkHub

Year 2026

Aman wants to buy a shirt from menx.com, a D2C website. The website launched very recently and seems to have stellar reviews but Aman wants to know more about the quality of the shirts.

He goes to his favorite fashion subreddit - r/fashionadvice to ask fellow Redditors about menx.com. and the quality of the fabric. A user with the username - u/welldressedbaboon responds, saying - “I was skeptical about the company as well because they are new and make affordable clothes. But I went ahead and bought 2 shirts. I couldn’t be happier with the quality! It’s comfortable and the fabric seems to be getting better with each wash! ”

Aman checks out u/welldressedbaboon’s profile, and it seems like an ordinary Redditor’s profile, with funny answers to some questions asked on r/AskReddit and some comments in tech subreddits about how much he loves his new iPhone and the case he bought from sickcases.com.

Aman, convinced, goes ahead and buys the shirt.

Little does he know that u/welldressedbaboon is actually a bot using generative AI to sell certain brands. A few people have started doubting this, but no one really knows.

This is already starting to happen.

Year 2028

The internet is now riddled with generative bots like u/welldressedbaboon. They are everywhere - in YouTube videos, on Reddit, and google reviews. Shaping the opinions of the world.

It’s become difficult for an average internet user to distinguish bots from humans.

Enter **mandatory digital identity**.

Mandatory digital identity will link a user to their accounts. This could lead to dystopian consequences like penalizing internet users for their opinions.

Zero Knowledge proofs will be an integral technology in implementing mandatory digital identity in a privacy-preserving manner, ensuring that it isn’t misused.

What are ZK proofs?

ZK Proofs are cryptography primitives.

With traditional cryptography techniques, you can only do one of either:

- for something only you know, keep it unknown to others
- for something everyone knows, prove that you own it

That is, you can’t keep something private while at the same time publicly prove that you own it. But with zero-knowledge proofs this is possible.

This enables different kinds of use cases -

Composable Identity Solutions

Social Media users can anonymously prove their age, personal information, and the authenticity of their profiles without revealing sensitive personal data.

DeFi users can prove their creditworthiness without revealing any personal data

Multiplayer Games without servers that stay forever

Typically, “blockchain games" store only a specific part of the game’s mechanics on-chain (in-game items as NFTs). The state and logic of these games still reside on traditional servers.

With advancements in the scalability and speed of blockchains, there are engines like MUD that enable the building of games whose state and logic reside on the blockchain too!

Not only this but multiplayer games can now be built without the need for expensive servers!

Traditionally, multiplayer games are NOT peer-to-peer because a server is responsible for keeping checks on dishonest players and to maintain the same state of the game for all the players. With zero-knowledge proofs, games can verify that the player is not cheating, and the blockchain can maintain the same state for all players, negating the need for servers altogether!

Games like dark forest already have thousands of players demonstrating that this is possible and scalable.

Adding a new meaning to privacy

Imagine if you could fetch all your credit data locally, use a formula provided by a credit score agency resulting in a credit score, and send the credit score with the ZK proof to the credit agency. The credit agency knows none of your credit data but only your score.

It gets even better: the only thing the credit agency needs to post is the verifier function verifying that you used the correct formula when calculating a particular credit score. This eliminates the need for a credit score company almost entirely — anyone can verify your credit score and the fact that you used the correct formula **offline**.

How do zk-proofs work?

Converting a computational problem to a zero-knowledge proof is a mind-bogglingly difficult task, requiring deep knowledge of mathematics and cryptography.

Enter Circom, Arkworks, and Zokrates.

These tools make it relatively easy for programmers to build zero-knowledge provers and verifiers.

On a high level, provers accept *public inputs* and *private inputs (called witnesses)* from a user and generate a proof. This proof can then be verified by the verifier quickly.

For example - a user can input their bank statement to a prover and get a proof stating that the monthly average account balance was greater than INR 50,000. This proof can then be sent to the verifier, and the verifier can verify whether the proof is valid (the verifier can verify the correctness of the statement that the balance was greater than 50,000 and also verify that the statement was generated truthfully)

> *God: “I am thy Lord!”*
> *Human: “Prove it.”*
> *God:*
> *“aec070645fd53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f”*
>
> *Human: “🙏”*

Limitations

Powerful as they are, zk proofs come with their own limitations.

Zero-knowledge proofs are expensive to generate (both in terms of memory and computation)

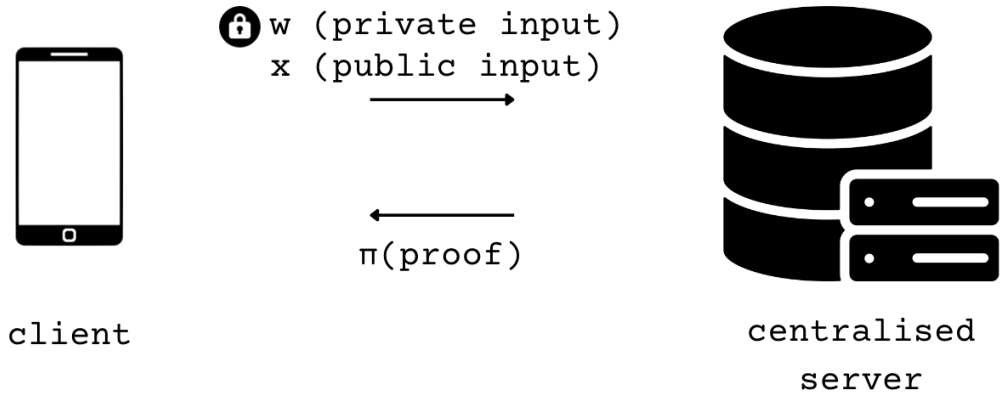
The creation of proofs is often slowed down by the need for numerous complex mathematical operations, such as exponentiations, inversions, FFTs, and bilinear pairing computations.

As the complexity of the computational problem increases, the memory, computation, and time required to generate the zk proof also increases.

A single zk proof can take hours to generate. Proof generation on the phone is next to impossible.

How are companies solving this?

Most companies with intensive resource requiring proof generation needs to set up their own infrastructure for generating proofs.



This has a couple of disadvantages -

- **Expensive to setup securely**
- **Priority shift from building product to setting up infrastructure for the product**
- **Liability of potentially sensitive data required for proof generation**

zkHub

This is where zkHub comes in.

zkHub lets entities with idle computation (or specialized hardware) at their hands plug into its network and connects them with entities who want to generate zk proofs.

The goal of zkHub is to **outsource proof generation while maintaining privacy**.

zkHub takes away the overheads of proof generation for companies. It provides the infrastructure required to generate proofs quickly, and without exposing the sensitive data required for proof generation, hence maintaining privacy.

It does this by using 2 clever techniques -

- **Distributed Proof Generation**

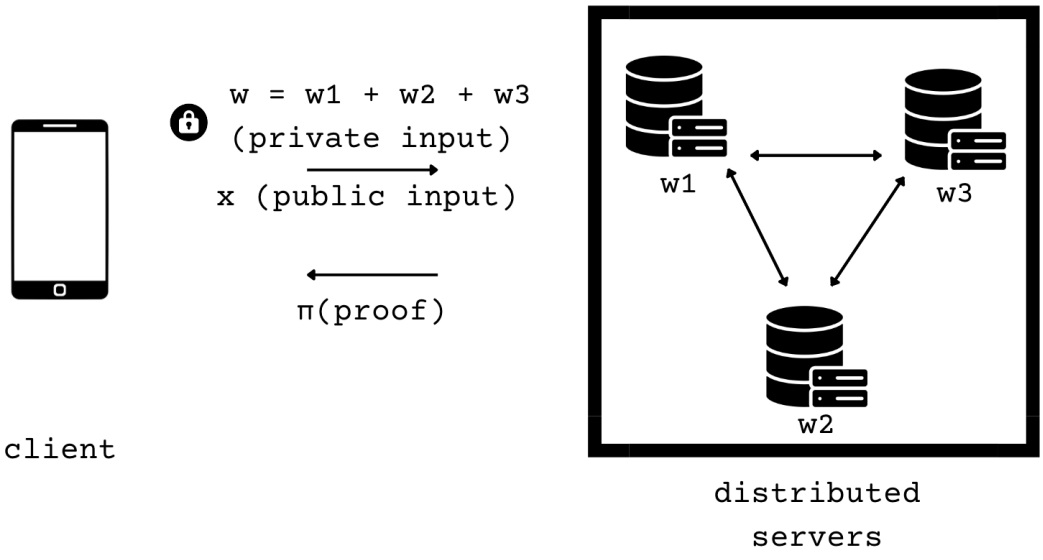
  Instead of sharing the data required for proof generation with a single authority, zkHub splits up the secret inputs into multiple chunks during a pre-processing phase and then distributes the proof generation task to multiple servers, hence resulting in faster proof generation.

- **Multi-Party Computation**

  The proof generators communicate with each other to generate the proof in such a way that each individual prover is obfuscated to the secret input of the other provers.

There are computationally-inexpensive checks done here as well to ensure that each prover is generating its part of the proof honestly.

Privacy is maintained as long as at least 1 prover is being honest.



Features

Marketplace Design

Each system that joins the marketplace as a proof generator will be assigned a rating based on the capabilities and proof generation success rate.

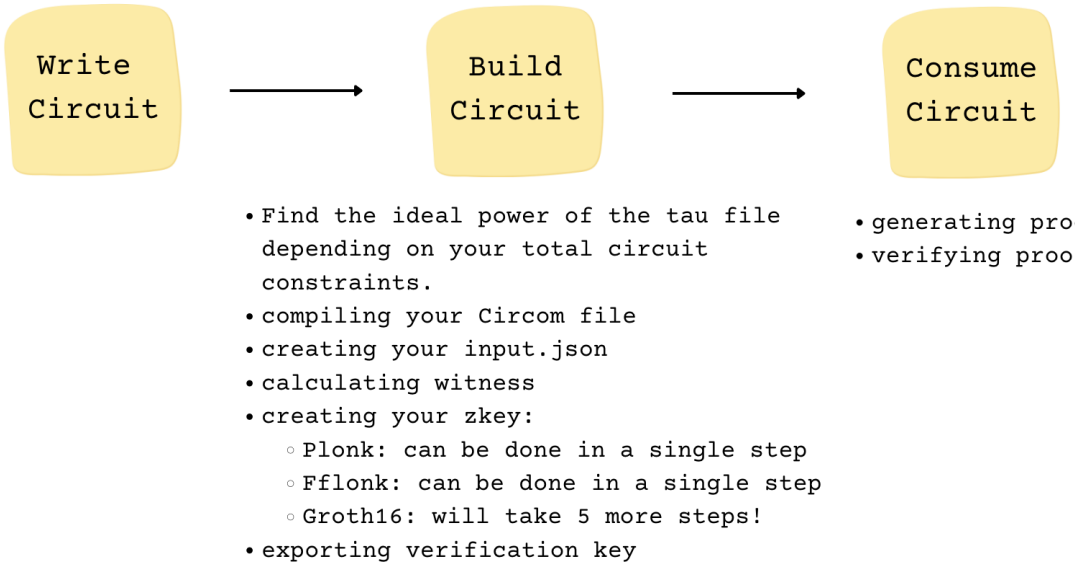
Using a third-party distributed computing solution like ICP, Golem will not give us the desired control over who we can assign these jobs to.

Requestors will then **place bids** and set the **priority** of the proof.

Integrate with Developer Workflows

Though tools like Circom and Arkworks are great for writing zk-circuits(programs), the process of building and consuming these circuits is rough.

This is what the workflow looks like -



To test these circuits during the development phase could again take hours, depending on the number of constraints.

zkHub also comes with an SDK which helps in the testing and automation of these workflows.

It also comes with the tools required for sharing proof generation data to the marketplace in a privacy-preserving manner, hence making developer workflows faster as well.

zkHub aims to be the natural choice for developers building circuits.

Reusability of proofs

There will be times when proofs for the same inputs might have to be generated multiple times. For example -

- Proving that a person is older than 18, would require the person to input their birth date into the prover.
- The next time someone with the same birthday comes along to generate a proof of the age, they will be generating the same proof again.

zkHub will store such proofs on a database, along with the encrypted inputs and the proof, so that when someone wishes to generate the proof for the same data again, instead of computing the proof, they can instantly get the proof from the zkHub database.

Repository of common proofs

There are some proofs that are very common for multiple use cases. For example, checking if an element is a member of a merkle tree.

zkHub will have a repository of optimized versions of common proofs like this.

What does zkHub enable?

Using the features mentioned above and DIZK (Distributed ZK)

- Up to **40x** increase in **proof generation times** compared to generation times on mobile phones.
- Build up to **250x** larger circuits in terms of size and complexity.

All of this without sacrificing privacy!

Monetization

Marketplace Fee

zkHub will take a 1% cut for proof generation.

Proof Generation

As mentioned before, when proofs are delegated to multiple nodes, we would require at least 1 node to behave honestly for privacy to be maintained. zkHub will provide that honest node and ensure that at least 1 part of the proof is always generated on a trusted node.

Reusable Proofs

As mentioned above, there is scope for reusing some proofs. These proofs will not have to be regenerated, hence saving on compute power and increasing speed.

zkHub will get revenue for such proofs for facilitating quick proofs.

Unit Economics

Based on the sheet below(sources provided), dark forest - a game built with zk-snarks generated proofs costing USD 2340 in the 9 days that it was live for (around 2 million transactions on Ethereum).

zkSync, a zk-evm generates proofs costing USD 720,000 per month.

> https://docs.google.com/spreadsheets/d/1aZCEEaS04PIjsytJbnKOq_NtJEfc2T67ZqF0R9b7SJI/edit?usp=sharing

Initial Customers

We are initially targeting to pilot with building consumer applications like

- ZK games
- ZK financial applications

- ZK identity solutions

This is because applications like bridges and rollups don't really require privacy for proof generation and can generate proofs on central servers as well.

We also foresee a big influx of developers building zk applications in the next 2 years.

Roadmap

The first version of the product will target Arkworks, a rust library for building generalized circuits.

Building distributed zk-circuits will require some modification in the way circuits are developed.

Owing to the novelty of this idea of distributed zero-knowledge proofs, there is a white space on the educational content side.

The first version of the product will launch in September 2023. It will have the following features:

- Marketplace
- Preprocessor for Distributed Proof Generation
- SDK for developers - simplifying build processes and generation
- Efficient set up of environment with a VM for GPU providers to run proofs

Till then, the product will be built out and tested. We will also be posting educational content for developers during this time.

We will also build a community of zk-builders and GPU providers.

First Hires

Cryptography Engineer for optimizing distributed proof generation

Growth for building marketing & social media campaigns

Technical Content Writer for writing tutorials and documentation

Competitor Analysis

Nil Foundation

NIL Foundation announced that they are building a marketplace for proof generation recently.

Their documentation and discord servers reveal that they are building the marketplace specifically for generating state proofs for zk-rollups on Solana and Mina.

They are also incapable of producing private proofs since they do not delegate proofs to multiple nodes.

[Recent Fundraise $22 Million]

ZeFi

ZeFi is building a simple proof generation in the cloud solution.

They are also incapable of generating private proofs since they have their own centralized servers which generate zk-proofs.