zk-patent

presented by
Ajlal and Ehteshaam Paracha

The Problem

How do you prove you had an idea first without revealing it?

Key Facts:

- $1.7-4.5 trillion USD piracy annually
- $20, 000 USD patent application process
- 1-3 years timeline
- 88% rejection rate
- No ZK

We need something better...

The Solution

AI-Powered Summarization

An LLM extracts the core essence of your uploaded document.

Zero-Knowledge Proof

Generate a cryptographic proof that you possess without reavling the idea itself.

On-Chain Timestamp

Proof is verified with a smart contract, which then mints an NFT to your wallet.

Youtube Link

Video Tutorial

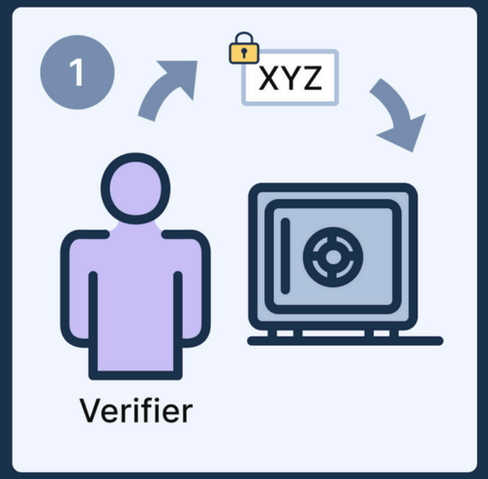
Next Steps and Q&A

- *zk ecosystem; open-source companies (e.g. Vercel, Docker)*
- *Making it easier to build zk applications and improving environment*
- *Applications:*
  - *Decentralized identification*
  - *Privacy-preserving finance*
  - *...*

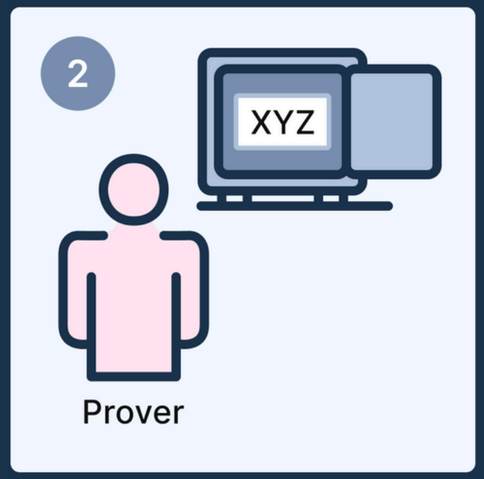
How a zero-knowledge proof works

CIRCULARISE

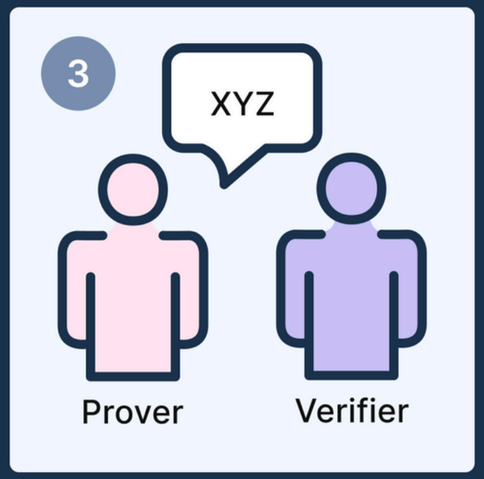
Prove that you know the combination code to a safe without revealing the code



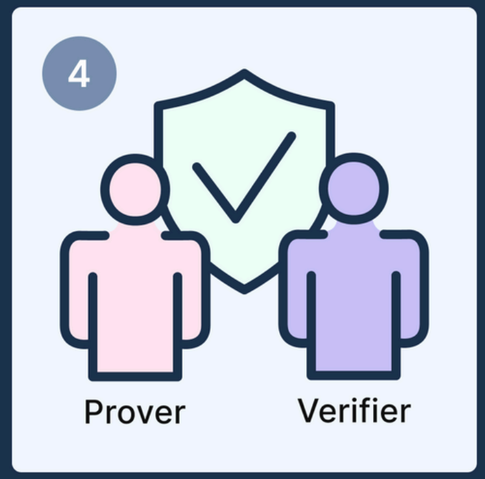
Verifier writes a secret message and put it in a locked safe.



Prover who fulfils the requirements has knowledge of the combination code and opens the locked safe.



Prover returns the secret message to Verifier.



Verifier is convinced that the prover knows the combination and can be trusted.

Importance of zk

- Hashes alone only prove you knew the hash, not the idea behind it without revealing it later.
- ZKPs cryptographically link you to the original idea (the hash's "preimage") without ever disclosing the idea itself.
- This enables verifiable prior art timestamping while maintaining complete privacy – a hash alone cannot.

- Problem with just a hash: You hash your idea (Idea X -> H(X)) and timestamp H(X) on-chain. Later, someone claims Idea X. You say, "I have H(X) timestamped earlier!" They respond, "Prove H(X) is your Idea X without showing it." You're stuck.

- ZK-Patent's Solution: We create a ZKP that says, "I know the secret Idea X whose hash is H(X)." The blockchain verifies this ZKP.

- Result: You prove possession of Idea X without ever revealing it, securing your prior art privately.