memento

EVM TIME CAPSULE

NOVEL ENCRYPTION PROTOCOL VIA VERIFIABLE DELAY FUNCTION (VDF)

ETHGlobal 2023 Hackathon
Istanbul, Turkey

memento

Memento is a dapp for storing private notes and media on a public blockchain to be unlocked in the future.

Powered by a novel EVM time-locking privacy protocol, built from scratch and inspired by Proof-of-Time consensus algorithm.

memento

Potential Use Cases of Time Capsule Encryption - 1

- **Digital Time Capsules**
  Users can create digital time capsules, storing personal memories or significant historical events, to be revealed at a future date.

- **Wills and Inheritance**
  Individuals can use Memento to store their wills or details of inheritance, which can be time-locked to be revealed or accessed only after their passing, ensuring privacy and reducing the risk of premature disclosure or tampering.

- **Future Predictions and Time Capsules**
  Users or groups could store predictions about the future or messages to their future selves, to be unlocked years later to see if they came true.

memento

Potential Use Cases of Time Capsule Encryption - 2

- **Educational Uses**
  Teachers can store educational content, revealing it to students at a predetermined time to align with their curriculum.

- **Confidential Business Agreements**
  Businesses can time-lock sensitive agreements, contracts, or strategic plans, ensuring they remain confidential until a specified future date.

- **Personal Goal Setting**
  Individuals can set goals and lock away messages of encouragement or reminders, which will be revealed at future checkpoints.

memento

Potential Use Cases of Time Capsule Encryption - 3

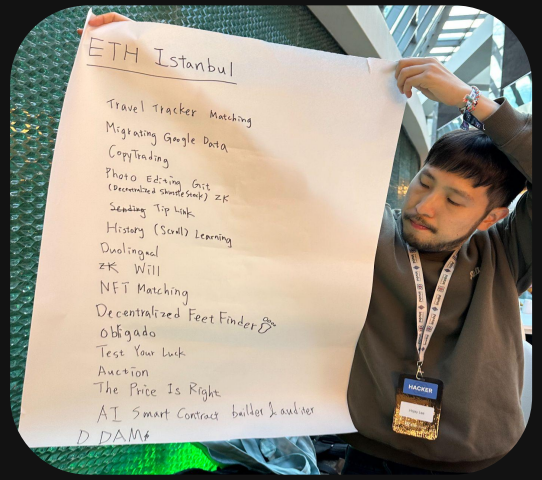
- **Event Planning and Announcements**
  Event organizers can create buzz by time-locking important announcements or details about upcoming events, creating a sense of mystery and excitement.

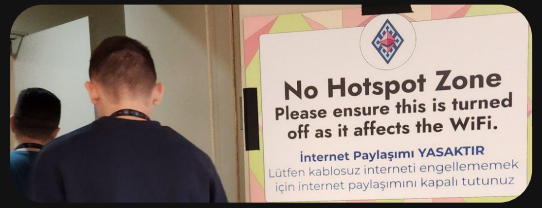
- **Artistic Projects**
  Artists and writers can use Memento to release their works publicly at a future date, adding an element of surprise and anticipation to their art.

- **Historical Record Keeping**
  Governments or organizations can store important historical documents to be unlocked at significant future anniversaries or milestones.
- **Research Data Release**
  Scientists can time-lock their research data or findings to be released in the future, allowing for timed disclosure of sensitive or impactful information.

memento

As most hackers, we just wanted to build some privacy dApps on EVM...





...but, surprisingly there was no tech to time-lock a content fully on chain in Ethereum ecosystem yet.

memento

"The best way to predict the f u t u r e is to invent it."

memento

The Giant Pivot: Let's propose an EIP!

ethereum / EIPs

Code | Issues 10 | Pull requests 77

Edit | Code | Jump to bottom

EIP for Time Capsule Encryption via Verifiable Delay Functions (VDFs) #7971

Open

hojayxyz wants to merge 1 commit into `ethereum:master` from `hojayxyz:patch-2`

Conversation 2 | Commits 1 | Checks 15 | Files changed

hojayxyz commented 53 minutes ago • edited

Add EIP Draft: Time Capsule Encryption via VDFs

ethereum-magicians.org/t/eip-for-time-capsule-encryption-via-verifiable-delay-functions-vdfs/16

✨ Fellowship of Ethereum Magicians ✨

EIP for Time Capsule Encryption via Verifiable Delay Functions (VDFs)

EIPs erc, evm

hojayxyz 1h

EIP for Time Capsule Encryption via VDFs - Seeking Community Feedback

I am excited to share with the community a draft of an Ethereum Improvement Proposal (EIP) that I've been working on, titled "Time Capsule Encryption via Verifiable Delay Functions (VDFs)." This proposal introduces a mechanism to securely encrypt content on the Ethereum blockchain with a time-delayed decryption feature.

Overview of the EIP

The primary goal of this EIP is to enhance the Ethereum ecosystem by enabling secure, time-locked encryption of data. This would be particularly useful for applications requiring time-bound confidentiality, such as sealed bidding, timed message releases, or digital inheritance.

Key features of the proposal include:

- **Secure On-chain Encryption:** Users can encrypt content (text or files) and upload it to the blockchain.
- **Time-Delayed Decryption:** Decryption is only possible after a pre-defined period, using Verifiable Delay Functions (VDFs).
- **Integrity and Authenticity:** Ensures that the content remains secure and unaltered until the specified unlock time.

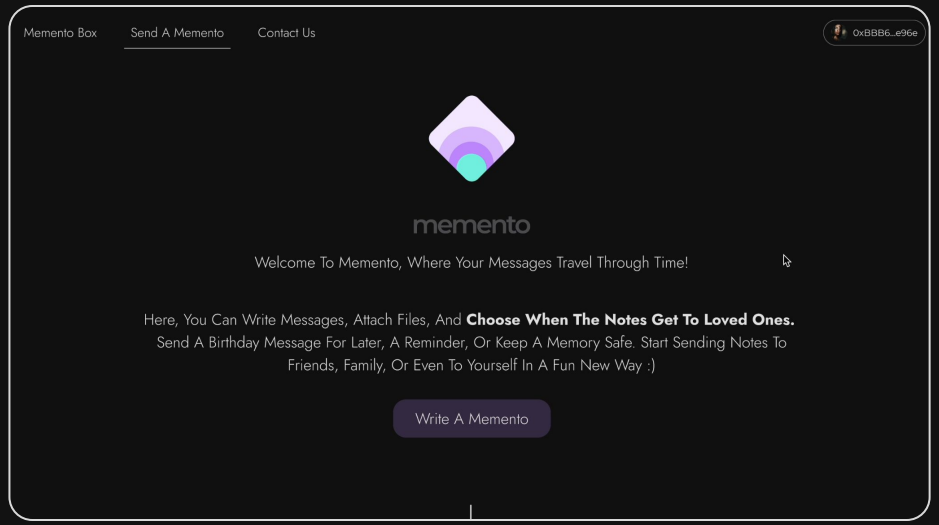
Nov 18

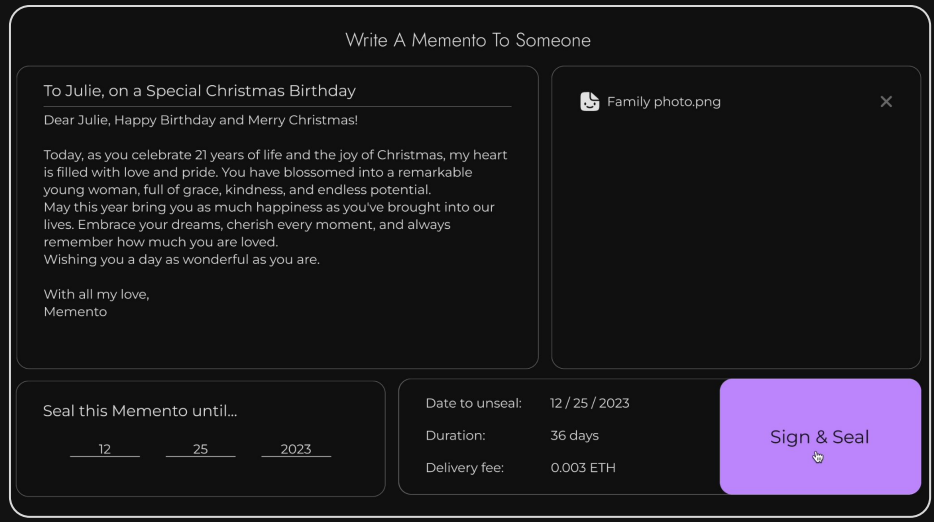
1 / 1
Nov 18

1h ago

memento

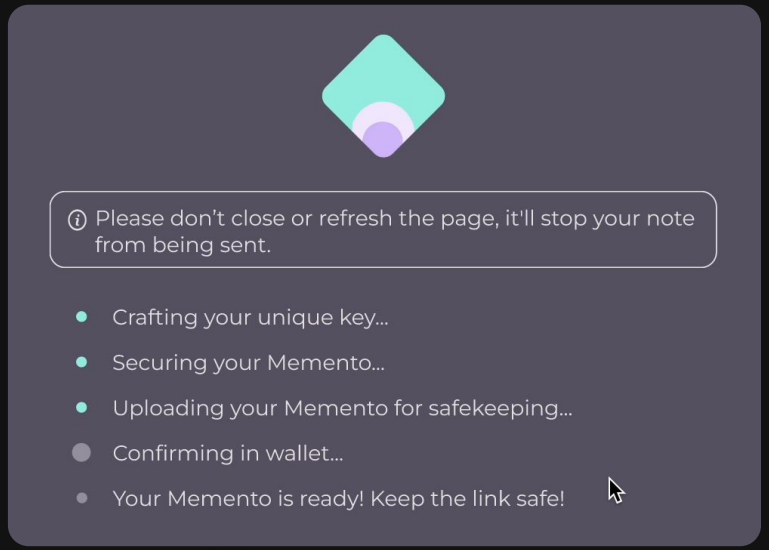
Memento in Action (sending)

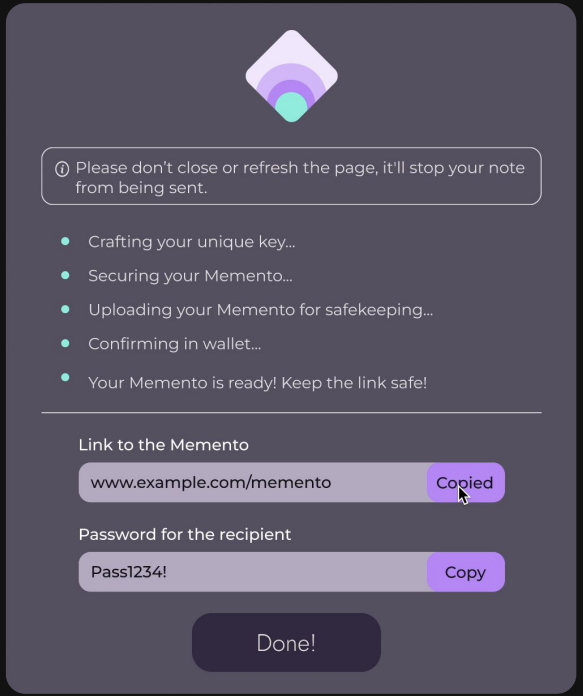




memento

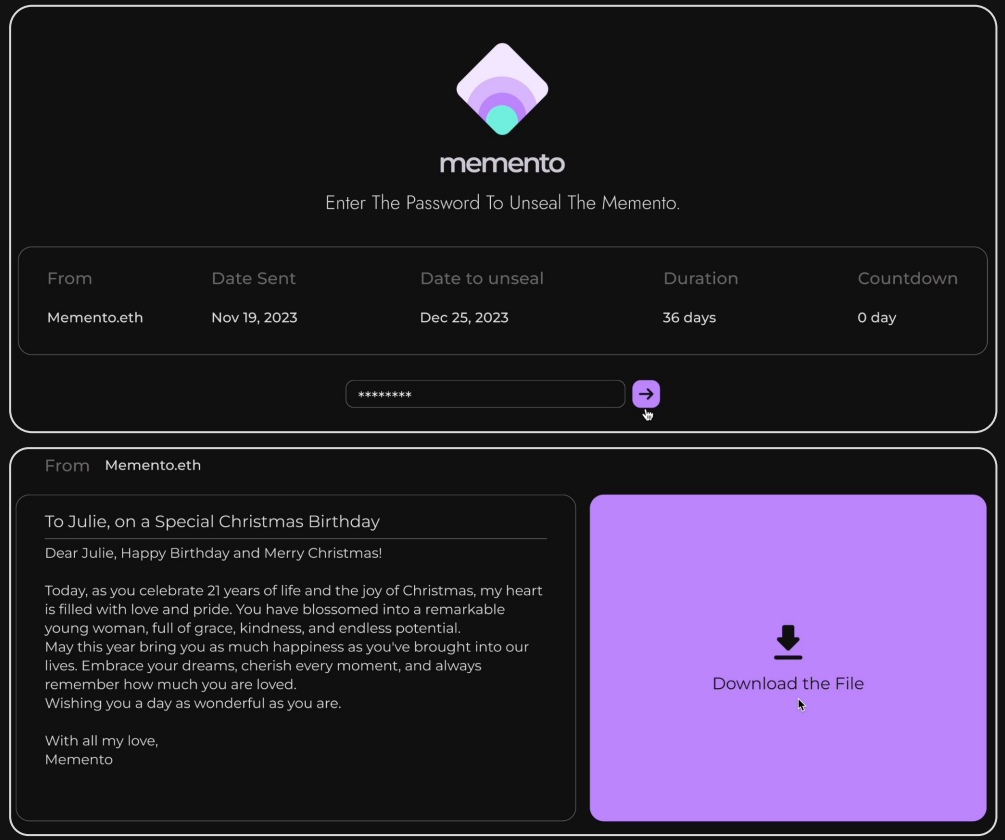
Memento in Action (sending)





memento

Memento in Action (receiving)

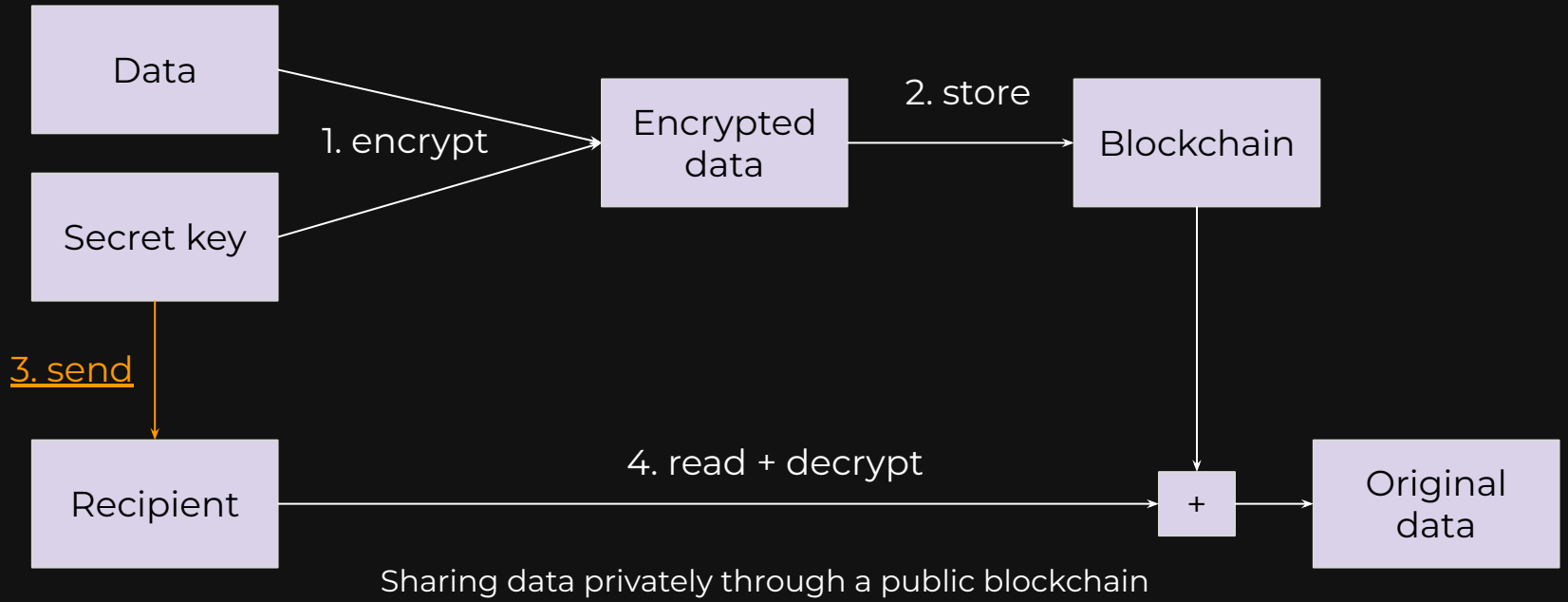


memento

The tech under the hood

memento

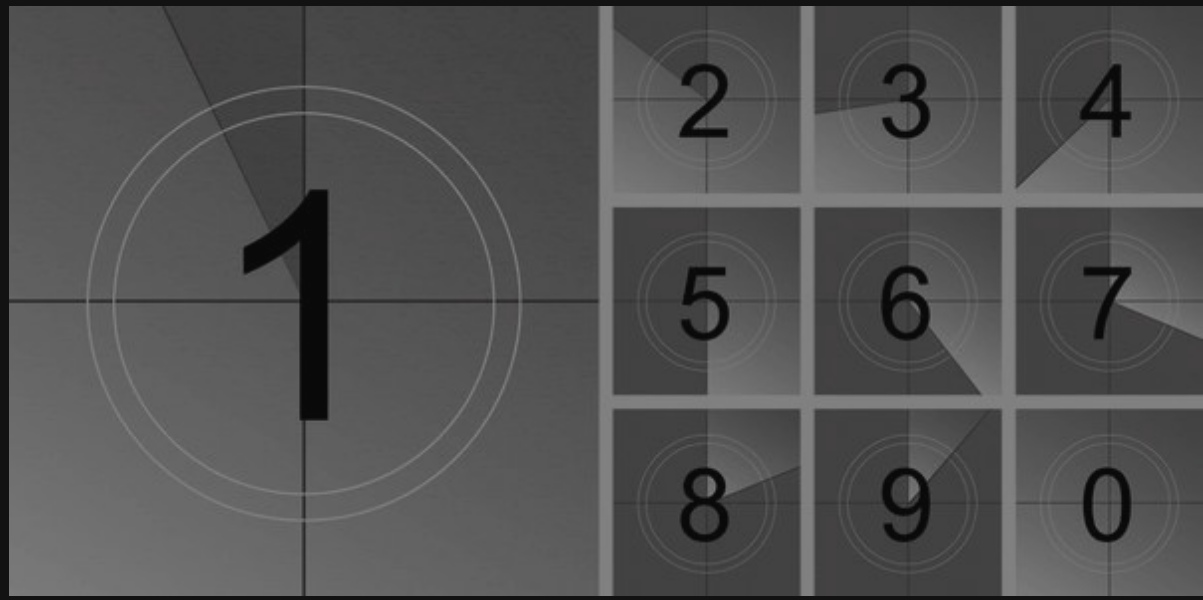
The concept of time-locking puzzles - 1



Sharing data privately through a public blockchain

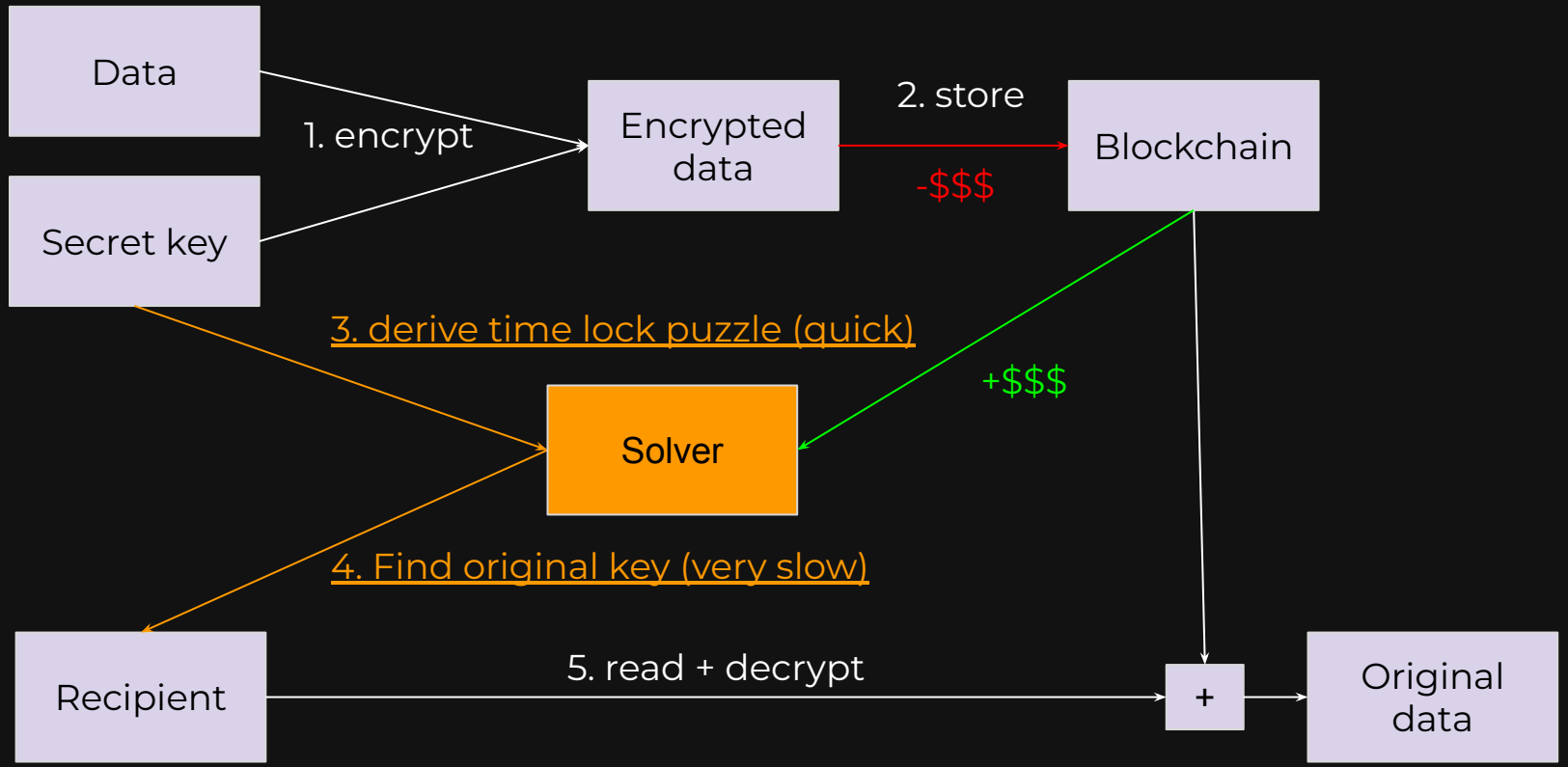
memento

How can we prevent the recipient from reading the message **until a certain moment in the future?**



memento

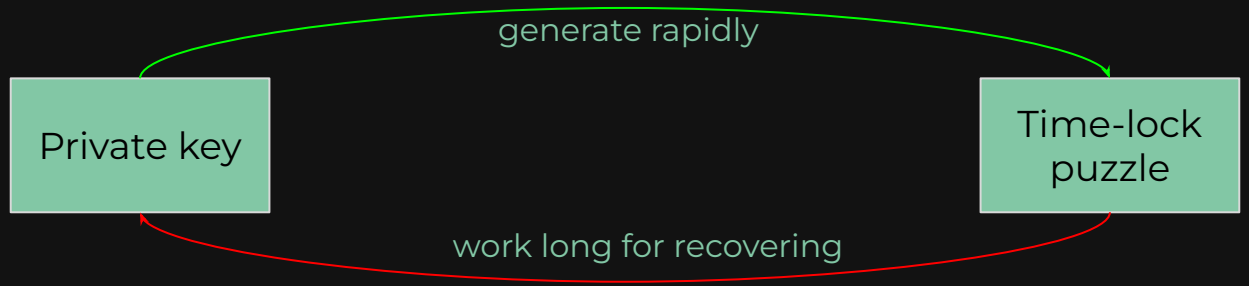
The concept of time-locking puzzles - 2



memento

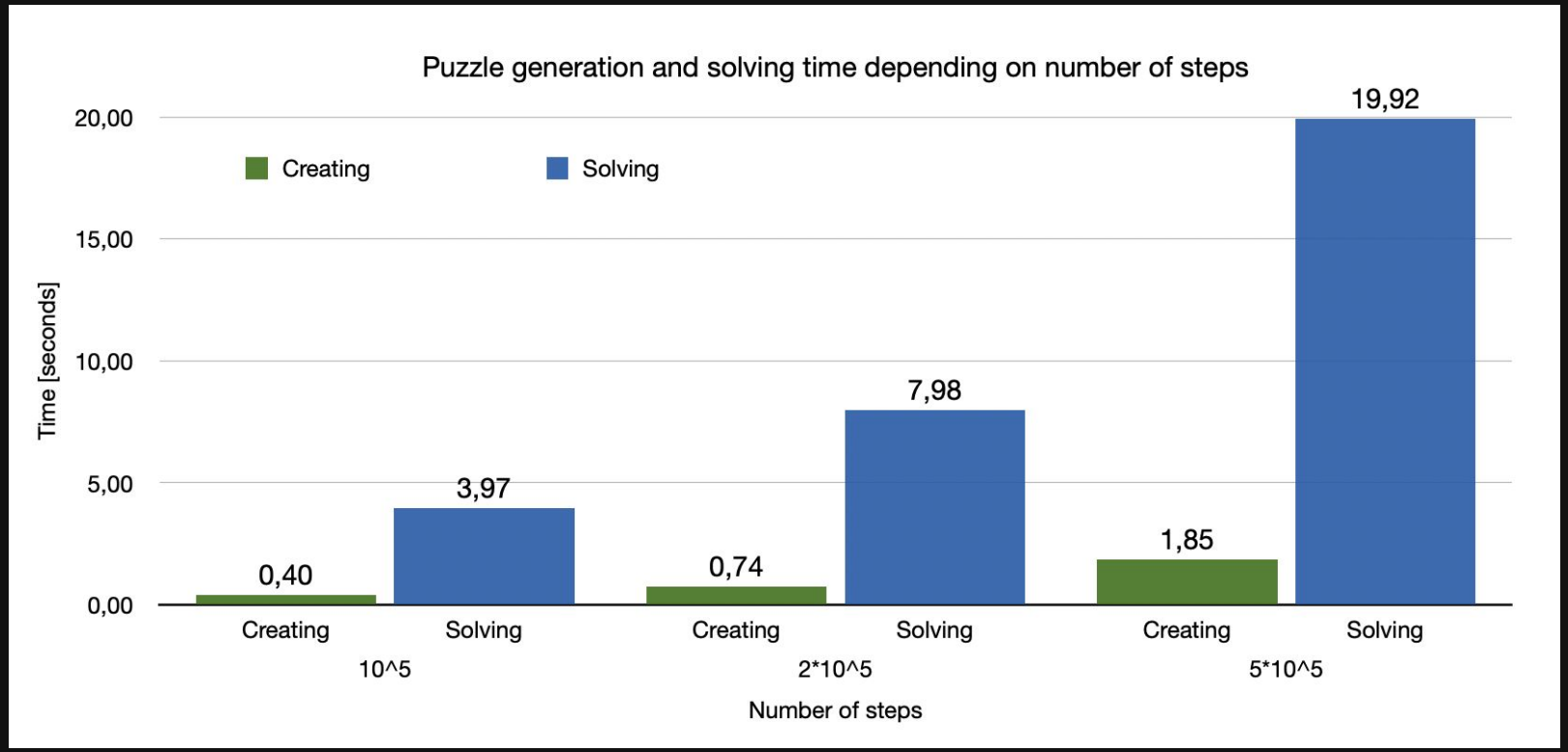
Verifiable Delay Function (VDF)

- Used in Proof-of-time consensus mechanism.
- Can be used for delaying the key delivery
  - Sender generates an encryption secret Y, very rapidly derives X from it and broadcasts it
  - Recipient recovers Y very slowly by recursively running N steps of VDF(X(t)) = VDF(X(t-1)) for the starting value VDF(0) = X



memento

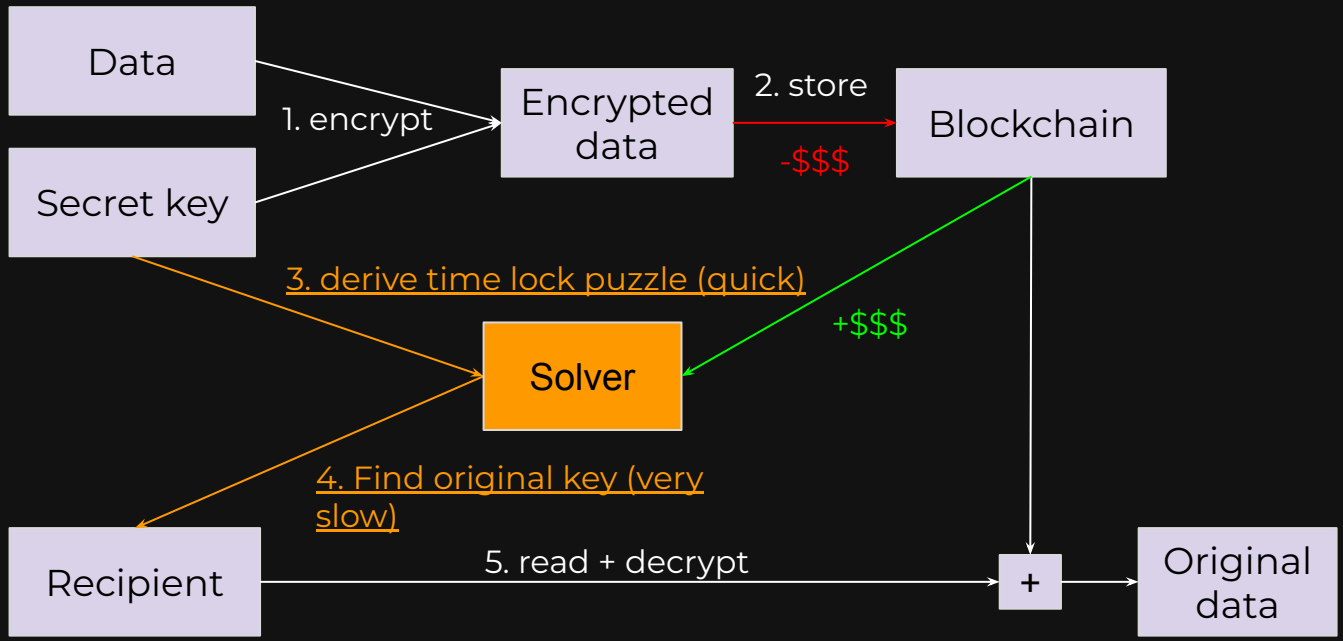
Our Verifiable Delay Function



memento

Memento Solver's bounties

- Solvers will be paid to compute small increments of M steps, where M is much smaller than N
- After each small computation the **checkpoint** is made so any other solver can take the computation from there
  - This is the moment the Solver gets a small part of the bounty



memento

Roadmap

Functionality Implemented In This Hackathon

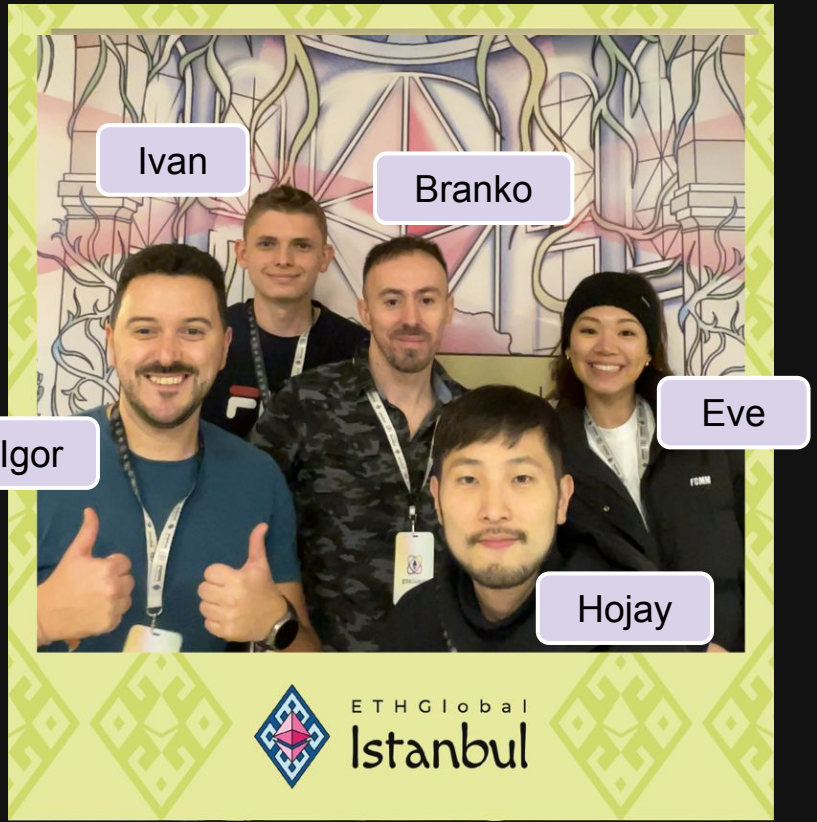
- Built fully functional Next.js frontend
- Hosted on NEAR x BOS distributed frontend
- Encrypted note and media upload to IPFS fully working
- Rust time-lock puzzle solver implemented in Rust
- Designed a robust protocol with economic incentive for solving time-lock puzzles
- Submitted EIP for it

Future Plans

- Multiple recipients
- Other triggers (proof of life, oracle-driven triggers and others)
- Mobile friendly version
- Implementation of reward distributions to puzzle solvers

memento

Meet Our Team



memento

Thank you!