



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.

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.



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.



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**

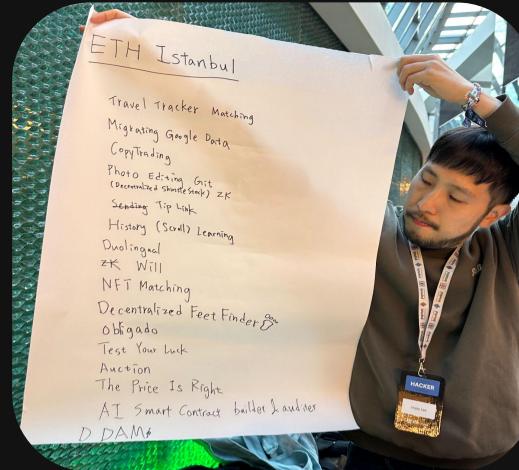
Governments or organizations can store important historical documents to be unlocked at significant future anniversaries or milestones.

- **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.



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.

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



PIVOT!

The Giant Pivot: Let's propose an EIP!

A screenshot of a GitHub repository page for the Ethereum Improvement Proposals (EIPs). The repository name is "ethereum / EIPs". The main navigation bar shows "Code" (1), "Issues" (10), and "Pull requests" (77). A pull request titled "EIP for Time Capsule Encryption via Verifiable Delay Functions (VDFs) #7971" is highlighted. The pull request details show it wants to merge into the "ethereum:master" branch from the "hojayxyz:patch-2" branch. The pull request has 2 conversations, 1 commit, 15 checks, and files changed. A comment from "hojayxyz" is visible, and there is a note to "Add EIP Draft: Time Capsule Encryption via VDFs".

A screenshot of a post on the Fellowship of Ethereum Magicians website. The title of the post is "EIP for Time Capsule Encryption via Verifiable Delay Functions (VDFs)". The author is "hojayxyz" and the post was made 1 hour ago on Nov 18. The post discusses the proposal for Time Capsule Encryption via VDFs, seeking community feedback. It states that the primary goal is to enhance the Ethereum ecosystem by enabling secure, time-locked encryption of data. 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.

The post has 1/1 interaction and was posted on Nov 18 at 1h ago. There are also "Edit" and "Delete" buttons on the right side of the post.



Memento in Action (sending)

Memento Box Send A Memento Contact Us



memento

Welcome To Memento, Where Your Messages Travel Through Time! 

Here, You Can Write Messages, Attach Files, And **Choose When The Notes Get To Loved Ones**.
Send A Birthday Message For Later, A Reminder, Or Keep A Memory Safe. Start Sending Notes To Friends, Family, Or Even To Yourself In A Fun New Way :)

[Write A Memento](#)

Write A Memento To Someone

To Julie, on a Special Christmas Birthday 

Dear Julie, Happy Birthday and Merry Christmas!

Today, as you celebrate 21 years of life and the joy of Christmas, my heart is filled with love and pride. You have blossomed into a remarkable young woman, full of grace, kindness, and endless potential. May this year bring you as much happiness as you've brought into our lives. Embrace your dreams, cherish every moment, and always remember how much you are loved. Wishing you a day as wonderful as you are.

With all my love,
Memento

Seal this Memento until... 

12 25 2023

Date to unseal: 12 / 25 / 2023
Duration: 36 days
Delivery fee: 0.003 ETH

[Sign & Seal](#) 

Memento Box

Title	Date Sent	Date to unseal	Total Duration	Countdown
To Julie, on a...	Nov 19, 2023	Dec 25, 2023	36 days	36 days

Memento in Action (sending)



ⓘ Please don't close or refresh the page, it'll stop your note from being sent.

- Crafting your unique key...
- Securing your Memento...
- Uploading your Memento for safekeeping...
- Confirming in wallet...
- Your Memento is ready! Keep the link safe! 



ⓘ Please don't close or refresh the page, it'll stop your note from being sent.

- Crafting your unique key...
- Securing your Memento...
- Uploading your Memento for safekeeping...
- Confirming in wallet...
- Your Memento is ready! Keep the link safe!

Link to the Memento

www.example.com/memento 

Password for the recipient

Pass1234! 





Memento in Action (receiving)



memento

Enter The Password To Unseal The Memento.

From	Date Sent	Date to unseal	Duration	Countdown
Memento.eth	Nov 19, 2023	Dec 25, 2023	36 days	0 day

***** ➔

From Memento.eth

To Julie, on a Special Christmas Birthday

Dear Julie, Happy Birthday and Merry Christmas!

Today, as you celebrate 21 years of life and the joy of Christmas, my heart is filled with love and pride. You have blossomed into a remarkable young woman, full of grace, kindness, and endless potential. May this year bring you as much happiness as you've brought into our lives. Embrace your dreams, cherish every moment, and always remember how much you are loved. Wishing you a day as wonderful as you are.

With all my love,
Memento

 Download the File



memento

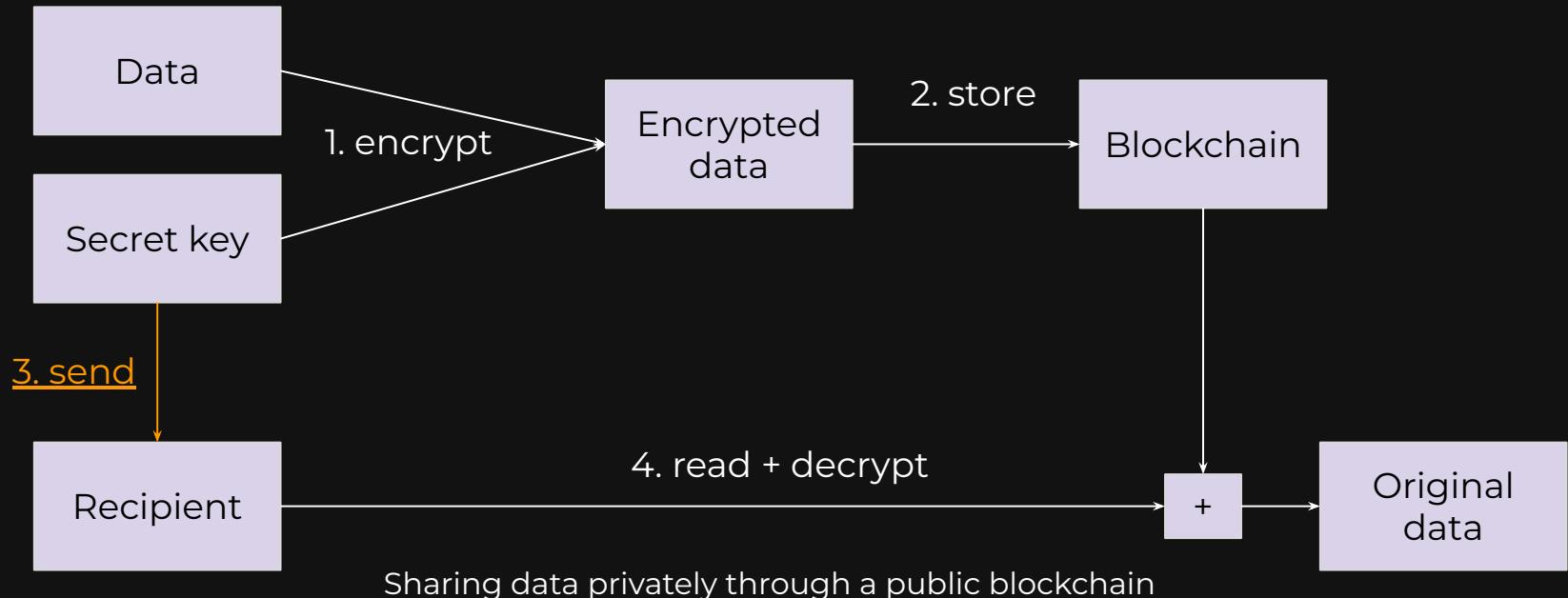
Unsealing The Memento...



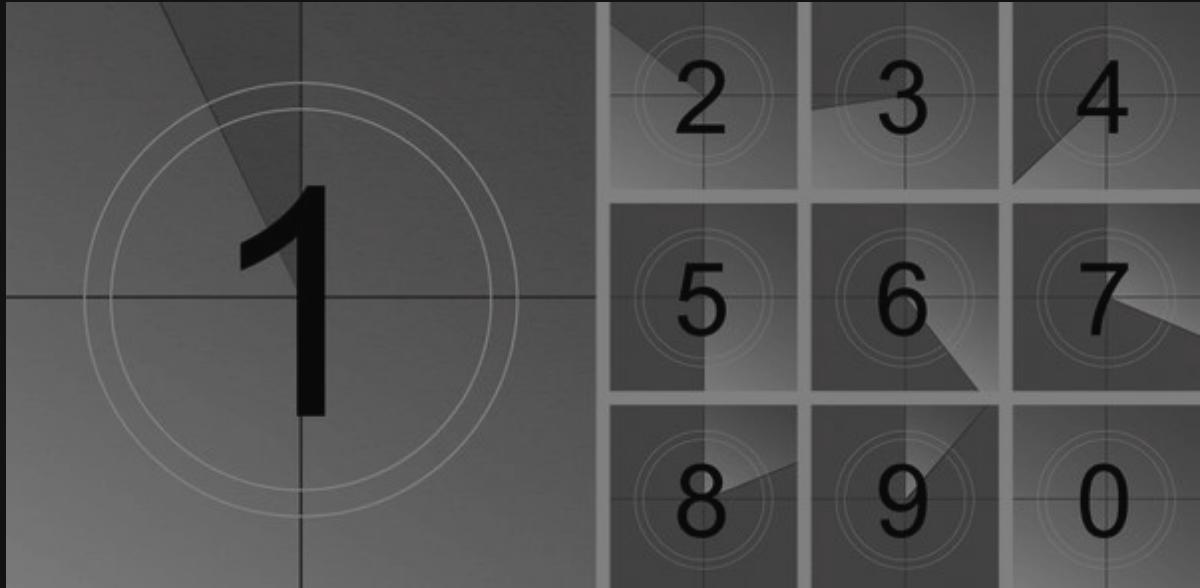
The tech under the hood



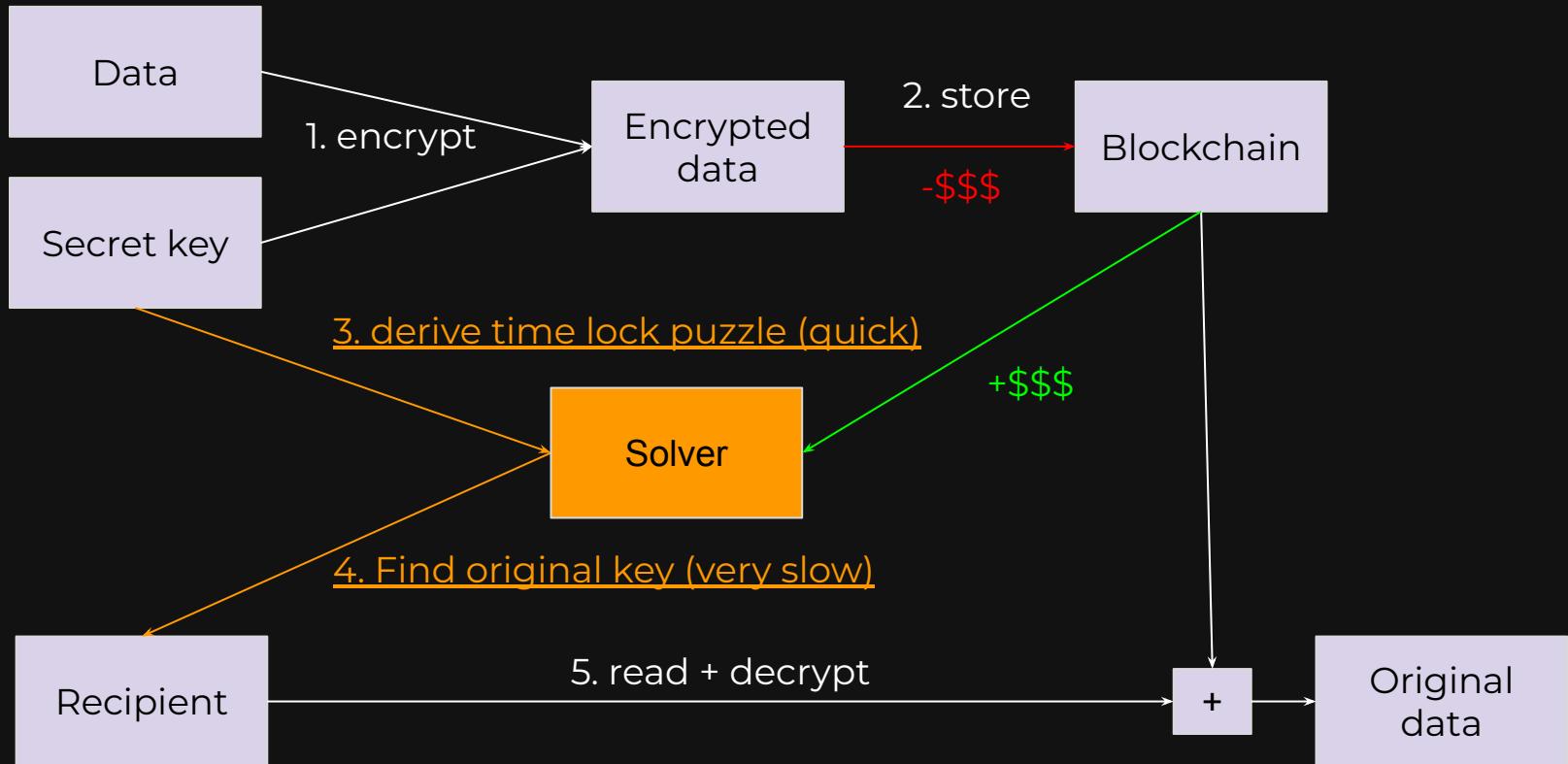
The concept of time-locking puzzles - 1



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

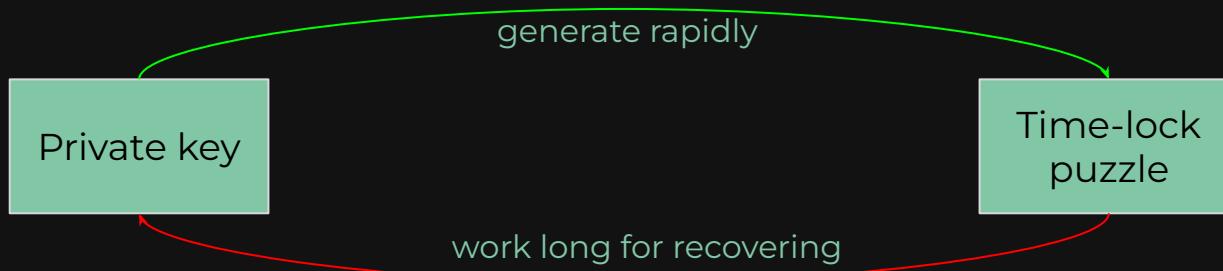


The concept of time-locking puzzles - 2

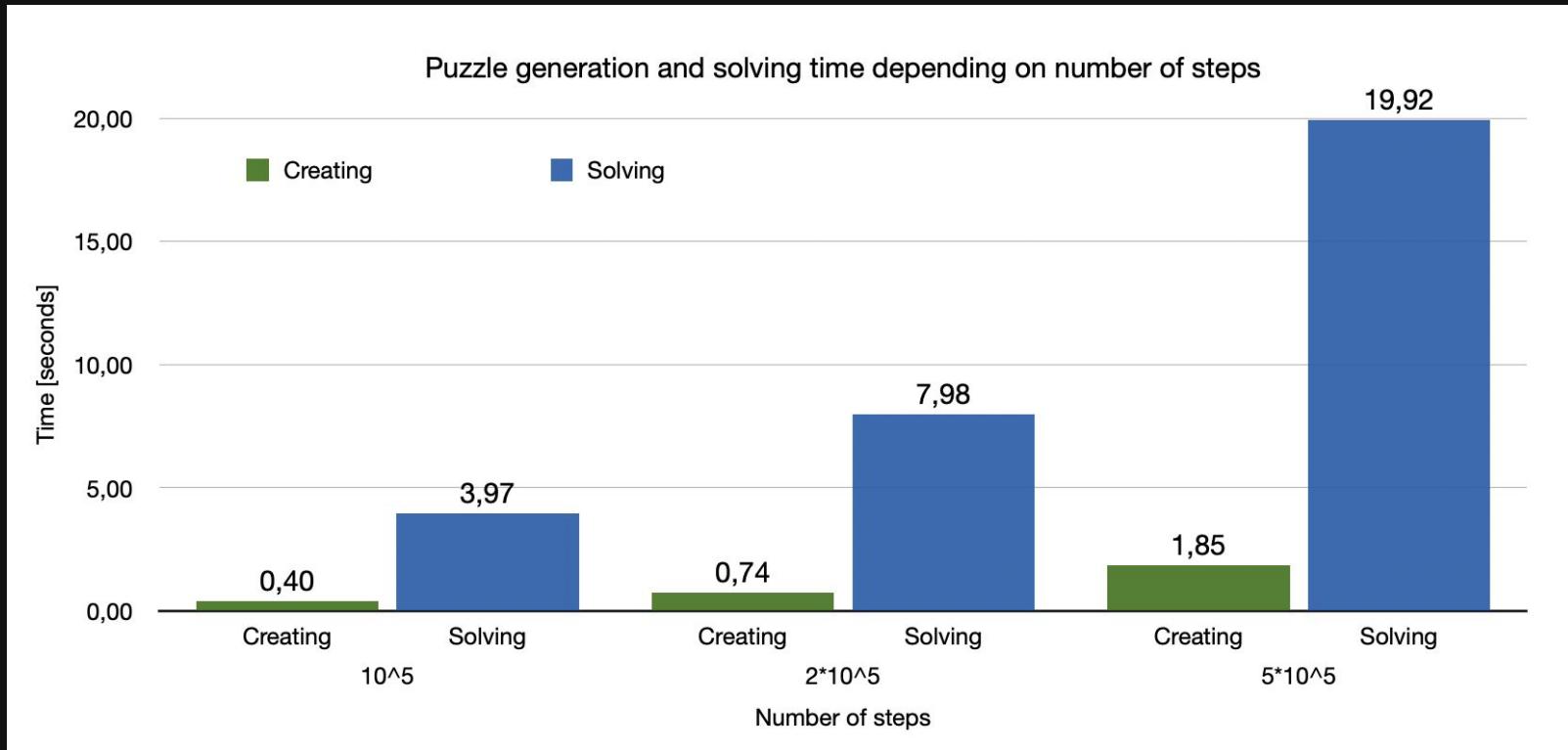


Verifiable Delay Function (VDF)

- 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 $VDF(X(t)) = VDF(VDF(X(t-1)))$ for the starting value $VDF(0) = X$

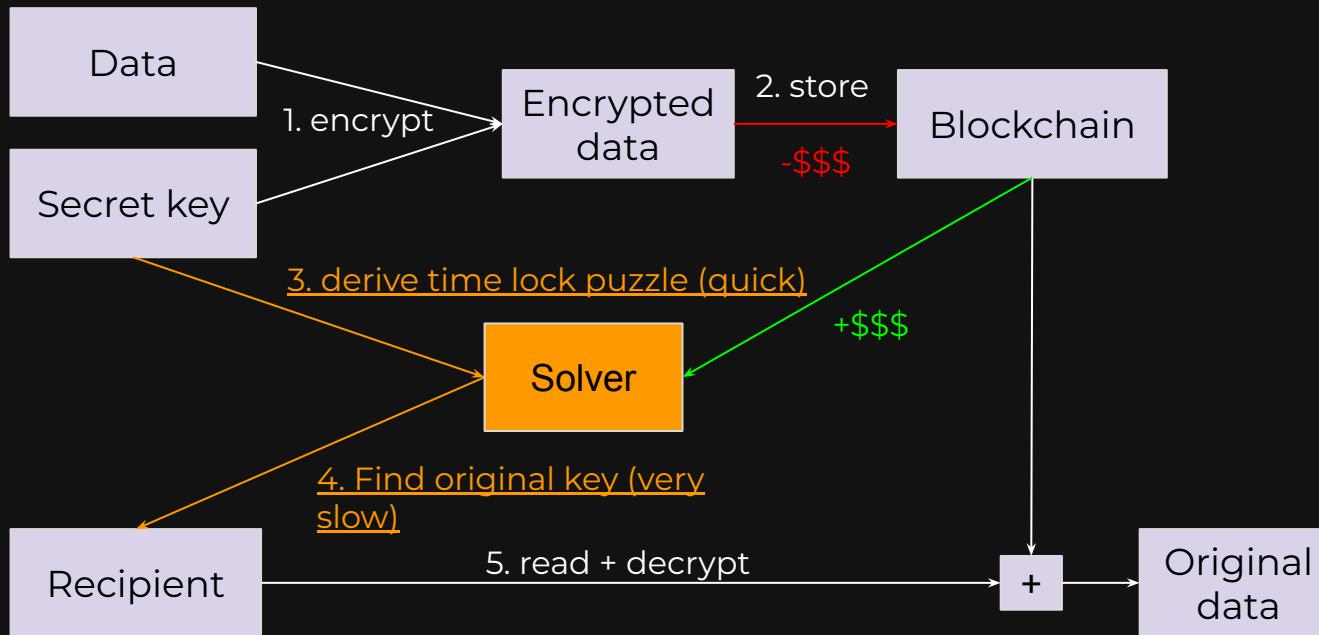


Our Verifiable Delay Function



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



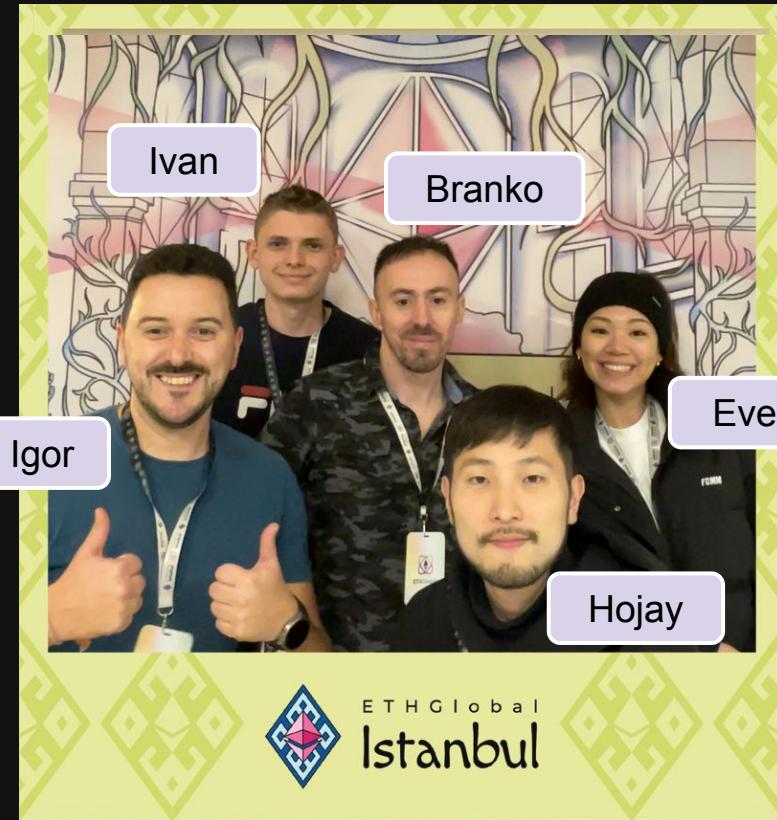
Functionality Implemented In This Hackathon

- 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

Meet Our Team



Thank you!