



Public Goods and Experiments

the Journey of Zkopru

Wanseob Lim

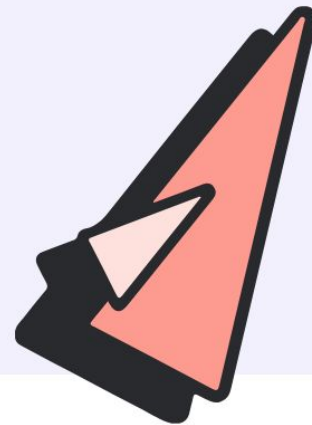
Applied ZKP Dev / PSE



PRIVACY & SCALING EXPLORATIONS

Enhancing Ethereum through cryptographic research.

[Explore our work](#) ↓



We explore new use cases for zero-knowledge proofs and other cryptographic primitives through research and proof-of-concepts.

Public Goods & Experiments



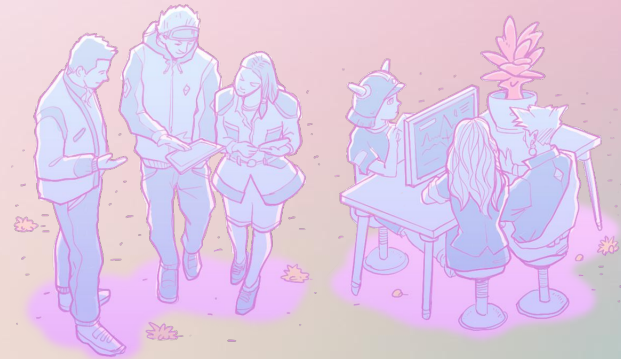
It's hard to keep the faith

De-Fi NFT
Layer N



Love You Goodbye GIF By TruTV's At Home With Amy Sedaris

<https://giphy.com/gifs/athomewithamysedaris-amy-sedaris-at-home-with-ah208-vxNCVFfe0PI9A3YVJEX>



Why are we doing?

2012, my 1st start-up experience

- Founded a startup
- Acquired by another startup in 2014
- I swapped all my equities to the new one

2014-2017, learned about capitalism

- Why others do not work very hard in this team?
- Incentive problems
 - Founder's share: 50%
 - 10th member's share: 0.5%
- Sweet-talks
- Founder is not greedy, because should take all the responsibility.
- It also works well for rocket-speed companies

Opensource



Source code is one of the most powerful means of production

Freedom

Run the software

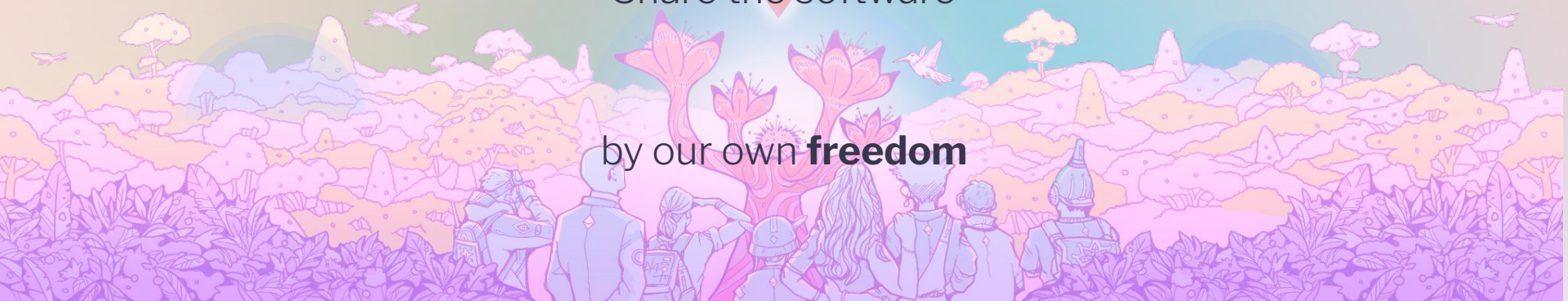
Study the software

Modify the software

Share the software



by our own **freedom**



Value-driven Community



Ethereum

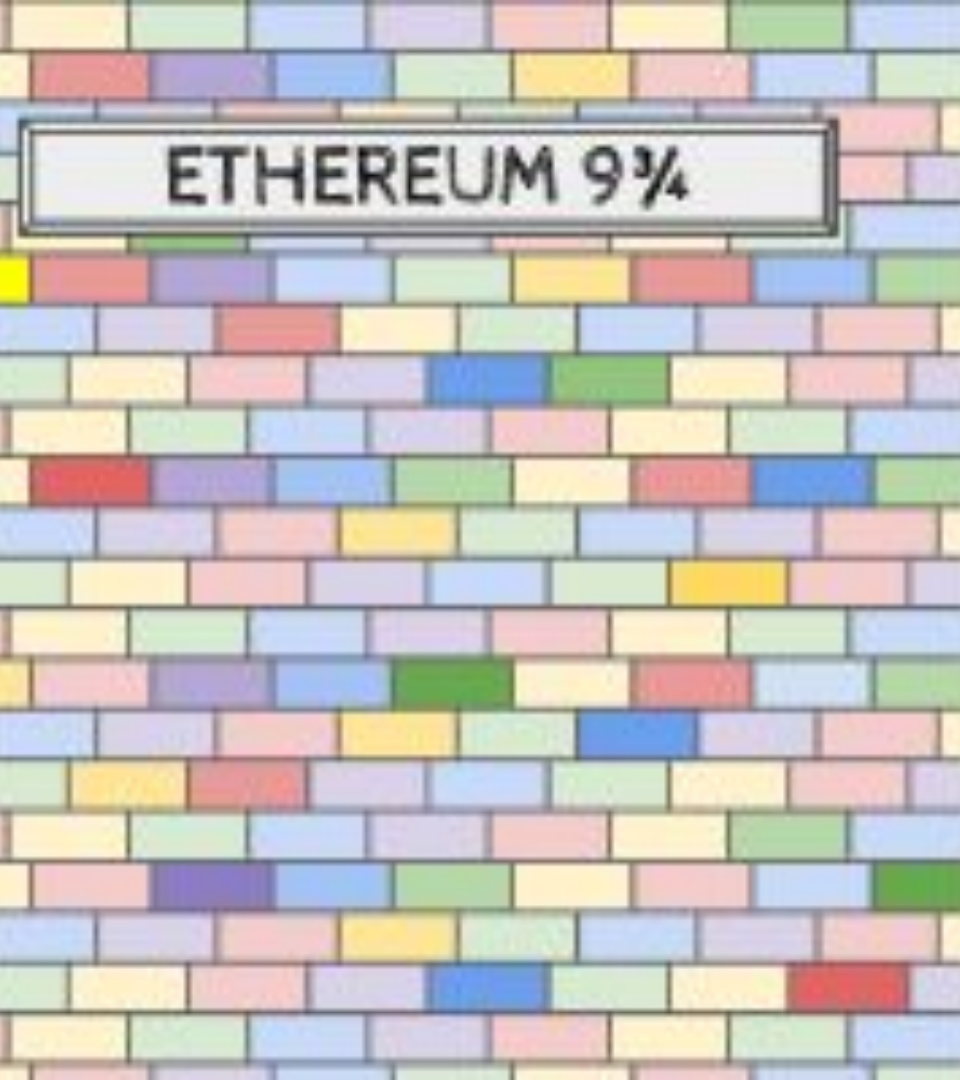
the world of freedom

Public Goods & Experiments for the freedom





**The right of persons to be free
from unwarranted publicity**

The image shows a close-up of a brick wall. The bricks are in various colors including red, yellow, green, blue, and purple. A white rectangular sign with a black border is mounted on the wall. The sign contains the text 'ETHEREUM 9 3/4' in a bold, black, sans-serif font.

ETHEREUM 9 3/4

Ethereum 9 3/4

- Project to implement Mimblewimble on Ethereum
- With the Optimistic Rollup approach
- Schnorr Signature
- But not enough privacy - transaction graph problem
- Added zkSNARK
- Need an interactive transaction

Zkopru

- Implementation of ZCash on Ethereum
- Using Optimistic Rollup
- 4K-9K gas / private tx
- Compliance compatibility
 - Viewing Key / Spending Key system

Wanseob Lim / Barry Whitehat / Chance Hudson / Koh
Wei Jie / Kobi Gurkan / Thore Hildebrandt / Geoff
Lamperd / Jinhwan Shin / Rachel Akerley / Takamichi
Tsutsumi / Chiali Tsai / Jeo Beyonder / Kimi Wu

ZKOPRU

Zero-Knowledge Optimistic RollUp

ZKOPRU

Zero-Knowledge Optimistic RollUp

Growth Strategy



Growth Strategy - Spin Out

- “We do public goods & researches what others will never do if we don’t do”
- There were already many teams trying to ship the private transaction service. (Aztec, Tornado, Polygon Nightfall, and so on...)

What others will never do?

- Other teams have their shareholders. Many things are related to the business
- Sometimes the source code becomes the means to maximize the profit only for some people.

Shipping the reference

- Reference Specification
- Reference Implementation
- Reference Example Applications

**We encourage you to fork our protocol and ship your own
private transaction project**

The reason why you fork and ship?

- Crypto Payment in our daily lives
- Compliance compatibility
- Ship a nation-wide crypto payment network using Ethereum Layer 2

Zkopru's Version 3 built by everyone



Zkopru V3

Specification



- Recursion
- Better membership proof
- Support various types of token
- Hybrid finalization with zk & op

Reference Implementation



- Ship the reference implementations
- Rust version
- Typescript version
- Etc

Shipping to the users



- Shipping this protocol to the local economy



PSE team's ethos

Public Goods

Experiments

Value Driven - Ethereum (maybe freedom)

Thank you!

Wanseob Lim

Applied ZKP Dev, PSE
wanseob.lim@ethereum.org



@wanseoblim