# How to ethically Build public good Infrastructure

# tl;dr:

Assholes exist; Web3's main primitive is to minimize their influence on everyone else

The ethics of building the infrastructure has a massive impact in our success in doing this

Hi.

corpetty.eth

petty.stateofus.eth

corpetty

status.im

hashingitout.com

# Principled Foundations

Our principles guide us while we design and build.

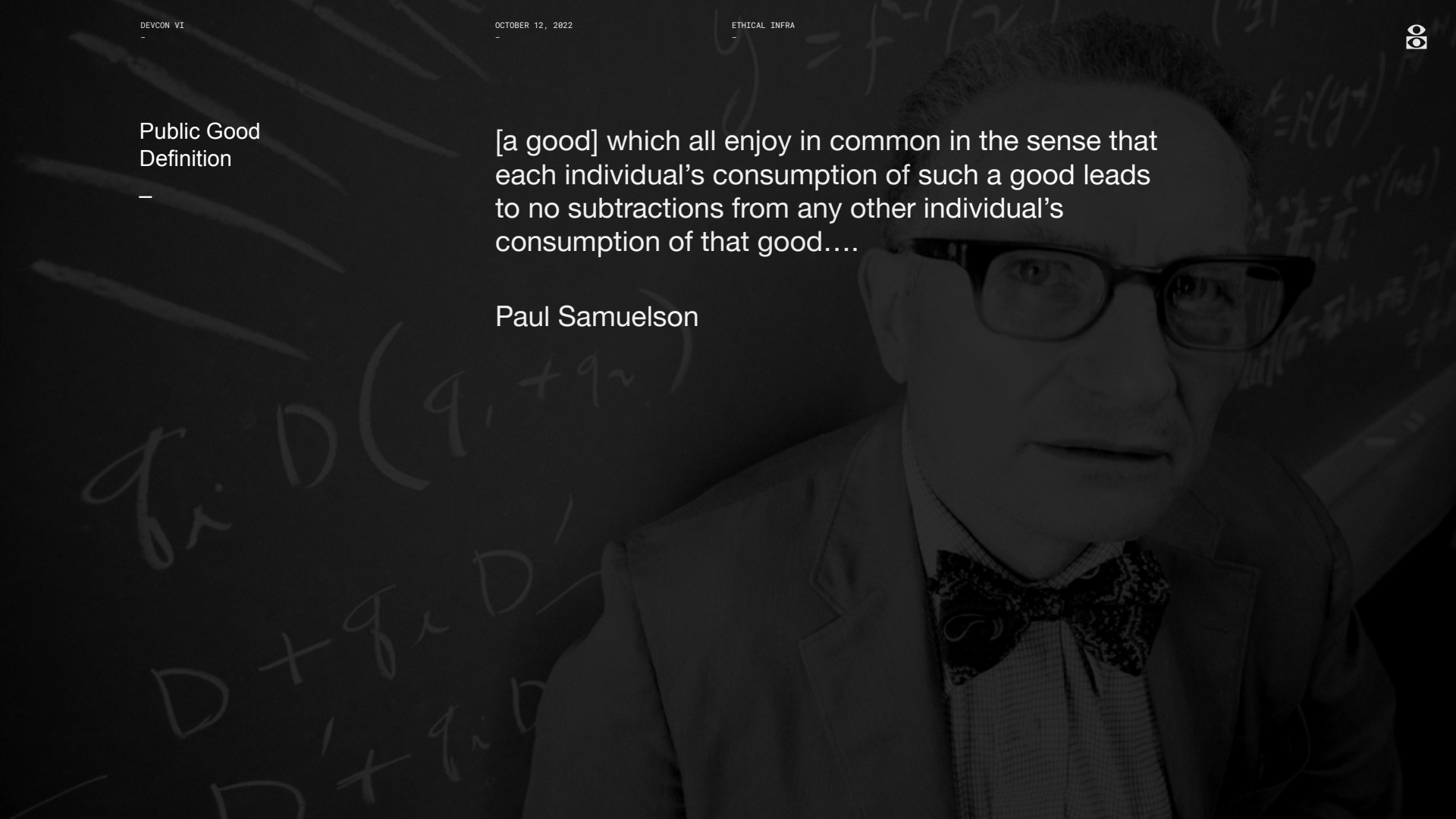
I. Liberty
II. Censorship resistance
III. Security
IV. Privacy
V. Transparency
VI. Openness
VII. Decentralization
VIII. Inclusivity
IX. Continuance
X. Resourcefulness

## Public Good Definition

–

[a good] which all enjoy in common in the sense that each individual's consumption of such a good leads to no subtractions from any other individual's consumption of that good….

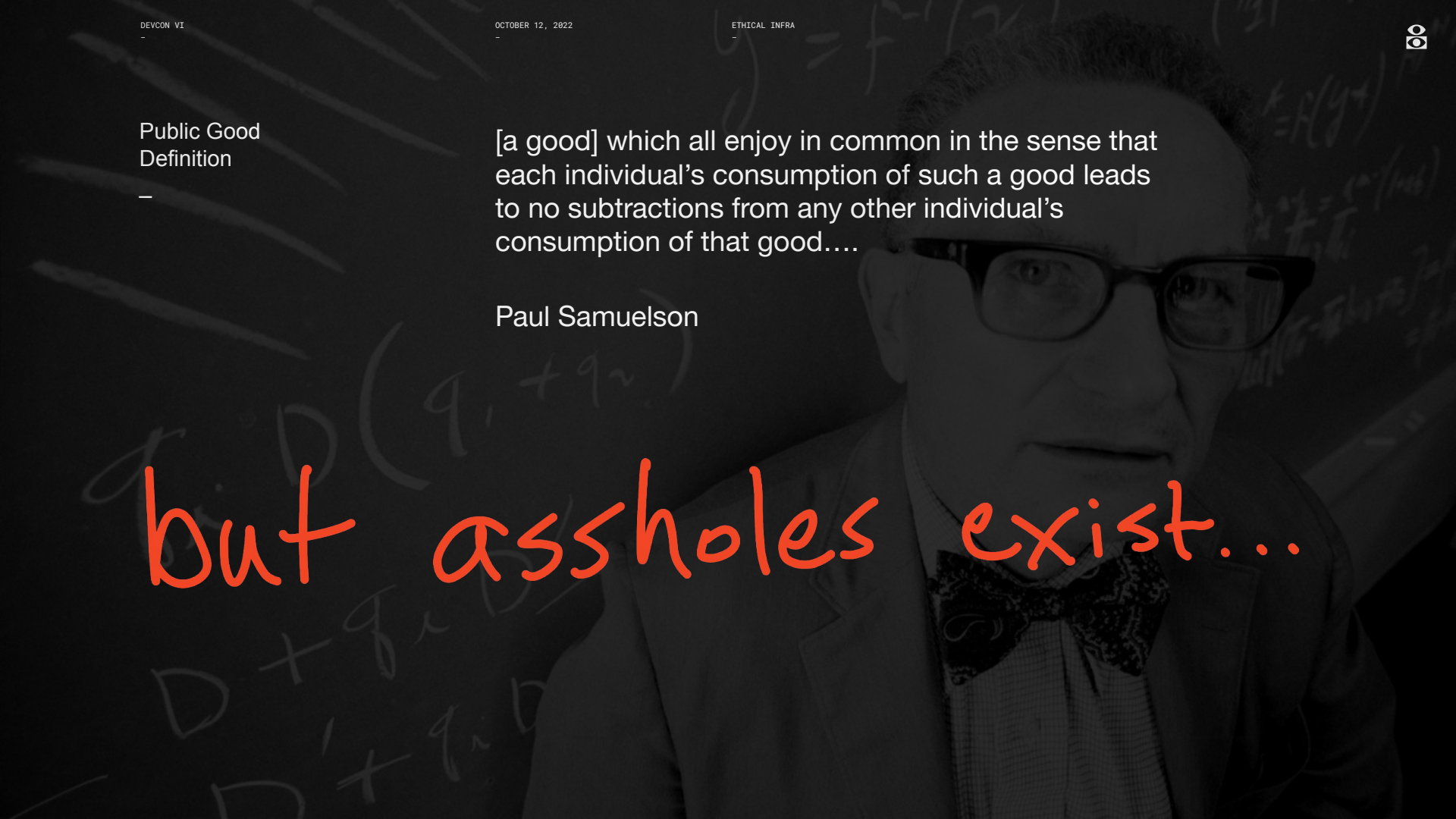
Paul Samuelson



Public Good
Definition

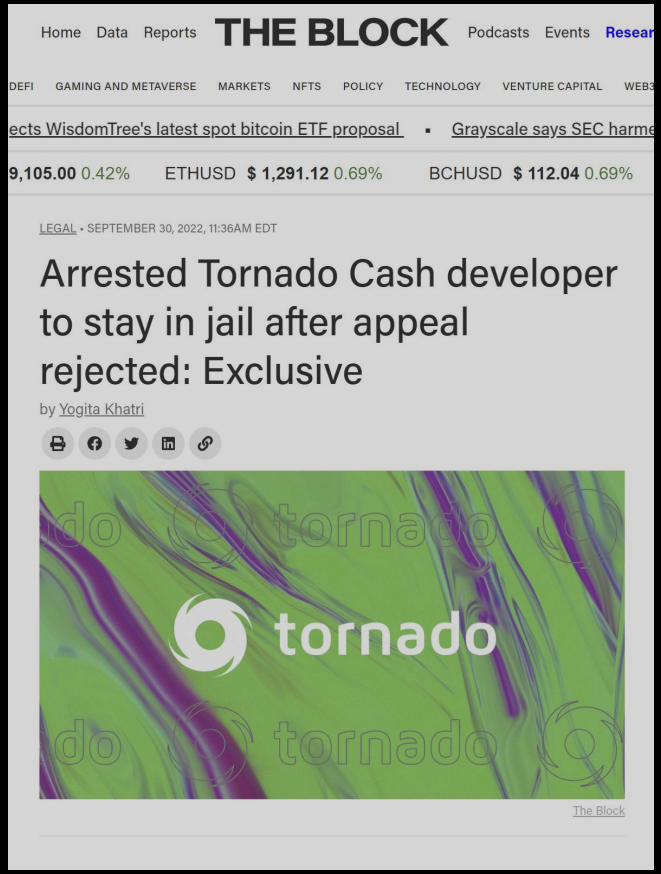
[a good] which all enjoy in common in the sense that each individual's consumption of such a good leads to no subtractions from any other individual's consumption of that good….

Paul Samuelson



# Corey's Law:

Every community has assholes, and they're usually loud



Home Data Reports THE BLOCK Podcasts Events Resear

DEFI GAMING AND METAVERSE MARKETS NFTS POLICY TECHNOLOGY VENTURE CAPITAL WEB3

ects WisdomTree's latest spot bitcoin ETF proposal ▪ Grayscale says SEC harme

9,105.00 0.42% ETHUSD $ 1,291.12 0.69% BCHUSD $ 112.04 0.69%

LEGAL • SEPTEMBER 30, 2022, 11:36AM EDT

# Arrested Tornado Cash developer to stay in jail after appeal rejected: Exclusive

by Yogita Khatri



The Block

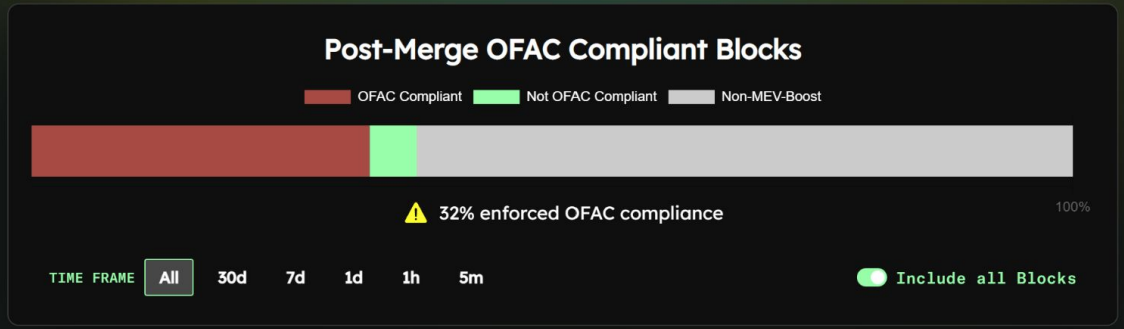
We aren't removing power dynamics, we're flattening its effects

We aren't removing power dynamics, we're flattening its effects

don't be evil → can't be evil

# MEV Watch

Some MEV-Boost relays are regulated under OFAC and will censor certain transactions. Use this tool to observe the effect it's having on Ethereum blocks.




Help us improve this tool for the community

Provide Feedback | Share

**Protocol level censorship = Bad**

Keep Ethereum credibly neutral by adopting a non-censoring mev-boost relay.

# The Medium is the Message

Three Layers of
any Message

The frame message

The outer message

The inner message

Gödel, Escher, Bach: an Eternal Golden Braid by Douglas Hofstadter

Three Layers of
any Message

# The frame message

“I’m a message, decode me if you can”

Implicitly conveyed in the structure of the message

## The outer message

To understand the frame message is to recognize the need for a decoding-mechanism.

## The inner message

Gödel, Escher, Bach: an Eternal Golden Braid by Douglas Hofstadter

Three Layers of any Message

The frame message

The outer message

The medium used to convey of the message

To understand the outer message is to build, or know how to build, the correct decoding mechanism for the inner message.

The inner message

Gödel, Escher, Bach: an Eternal Golden Braid by Douglas Hofstadter

# Three Layers of any Message

The frame message

What is trying to be conveyed in the first place

The real message

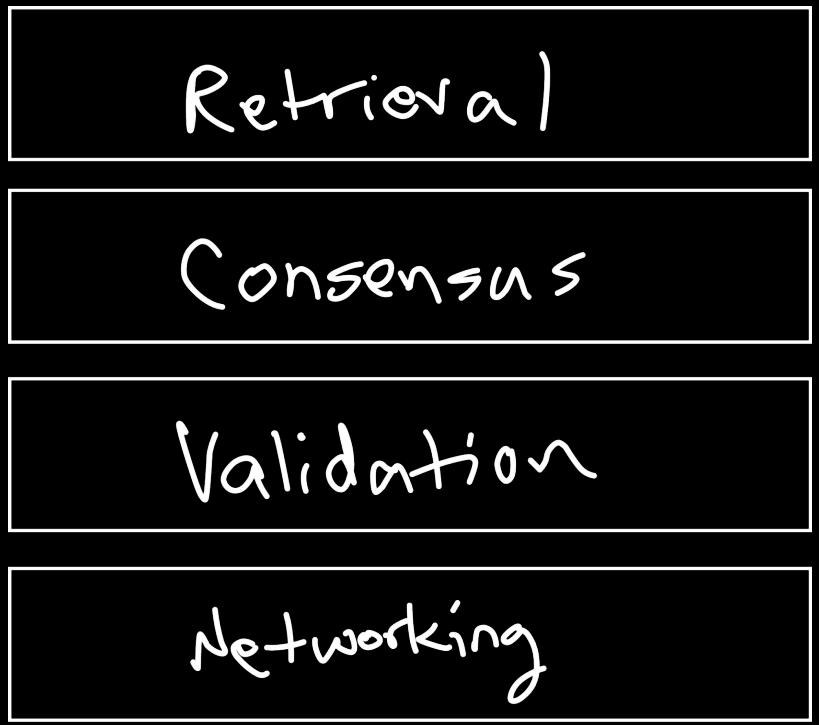
To understand the inner message is to have extracted the meaning intended by the sender

The inner message

Gödel, Escher, Bach: an Eternal Golden Braid by Douglas Hofstadter

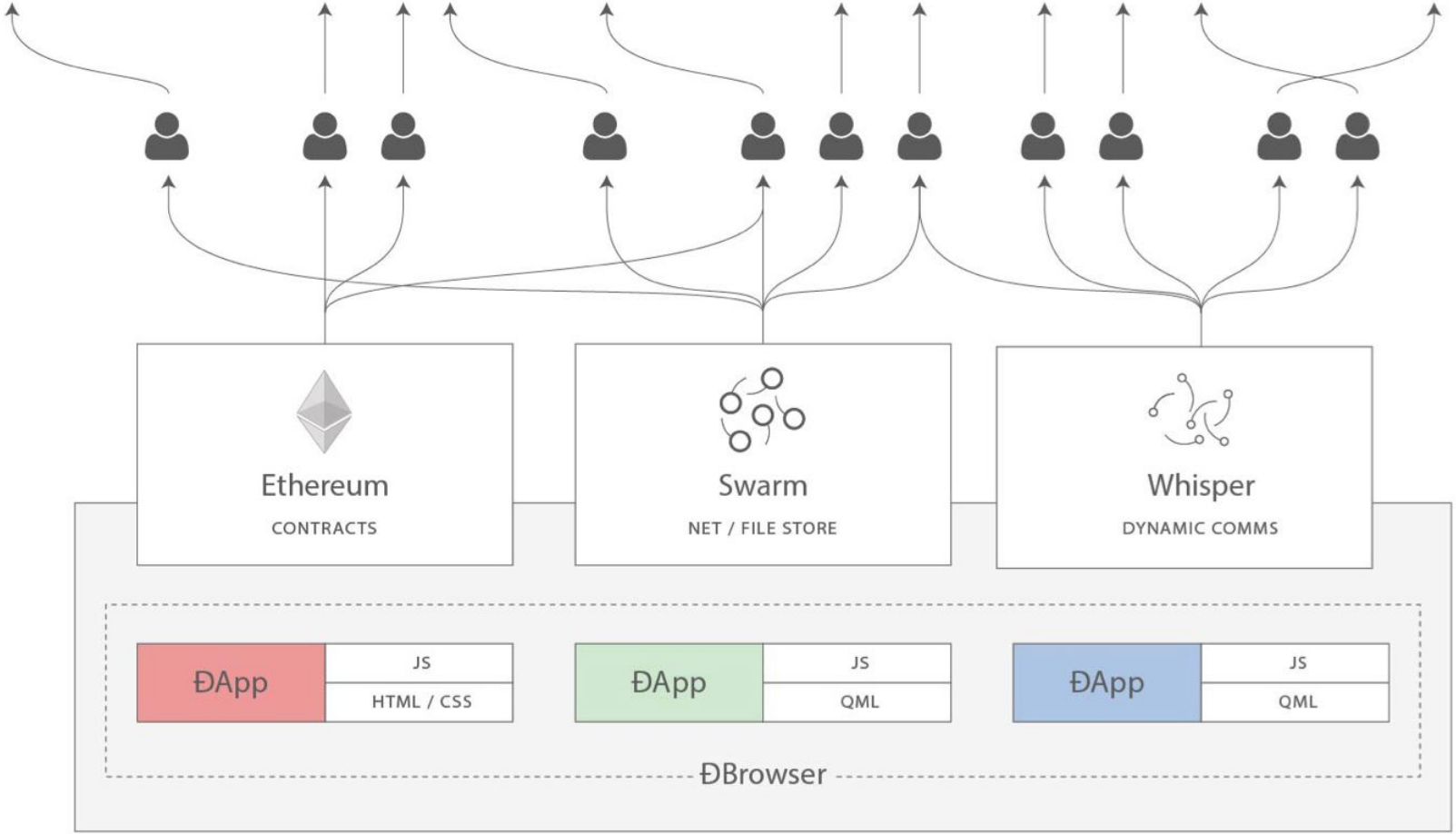
Blockchain networks are coordination mechanisms

with real world value


Retrieval
Consensus
Validation
Networking

# A quick history

whisper → RLN Relay


Ethereum
CONTRACTS
Swarm
NET / FILE STORE
Whisper
DYNAMIC COMMS
ĐApp
JS
HTML / CSS
ĐApp
JS
QML
ĐApp
JS
QML
ĐBrowser

## Socio-economic Networks

Everyone-as-a-stakeholder

What if we could flatten these roles? What if users of social networks possessed a real stake in the networks they participate in? What if we could align incentives for all parties and create a network that naturally promotes behaviours that benefit all participants?

Status uses
Whisper

Proof of Work anti-spam mechanism
Dead batteries, Hot phones

Gossip / bloom filters giving sender anonymity
Empty mobile data plans

Discovery v4 for finding peers
High churn devices rely on centralized nodes

## Fixing Whisper with Waku

*Dec 03 2019* - by *oskarth*

This post will introduce Waku. Waku is a fork of Whisper that attempts to addresses some of Whisper's shortcomings in an iterative fashion. We will also introduce a theoretical scaling model for Whisper that shows why it doesn't scale, and what can be done about it.

### Introduction

Whisper is a gossip-based communication protocol or an ephemeral key-value store

Waku

Attempt to patch Whisper for our operational environment

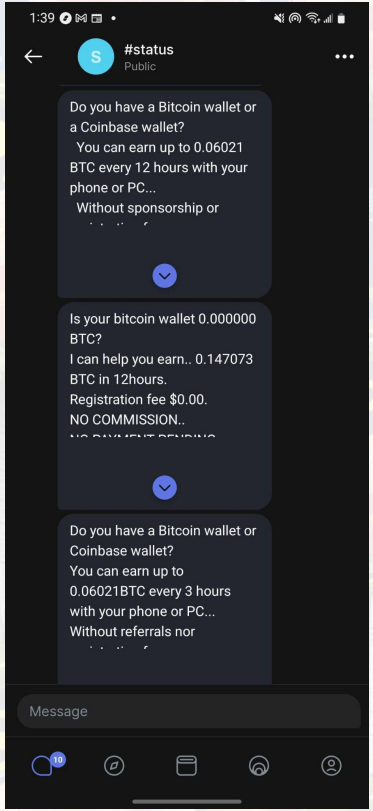
Take responsibility and apply attention to our required infrastructure

Openly research, build, and publish. Created Vac to focus specifically on private, p2p ephemeral messaging

Specifications available at https://rfc.vac.dev

# Issues

–


1:39
#status
Public
Do you have a Bitcoin wallet or a Coinbase wallet?
You can earn up to 0.06021 BTC every 12 hours with your phone or PC...
Without sponsorship or
Is your bitcoin wallet 0.000000 BTC?
I can help you earn.. 0.147073 BTC in 12hours.
Registration fee $0.00.
NO COMMISSION..
Do you have a Bitcoin wallet or Coinbase wallet?
You can earn up to 0.06021BTC every 3 hours with your phone or PC...
Without referrals nor
Message

## What's the Plan for Waku v2?

*Jul 01 2020* - by *oskarth*

**tldr: The Waku network is fragile and doesn't scale. Here's how to solve it.**

*NOTE: This post was originally written with Status as a primary use case in mind, which reflects how we talk about some problems here. However, Waku v2 is a general-purpose private p2p messaging protocol, especially for people running in resource restricted environments.*

### Problem

The Waku network is fragile and doesn't scale.

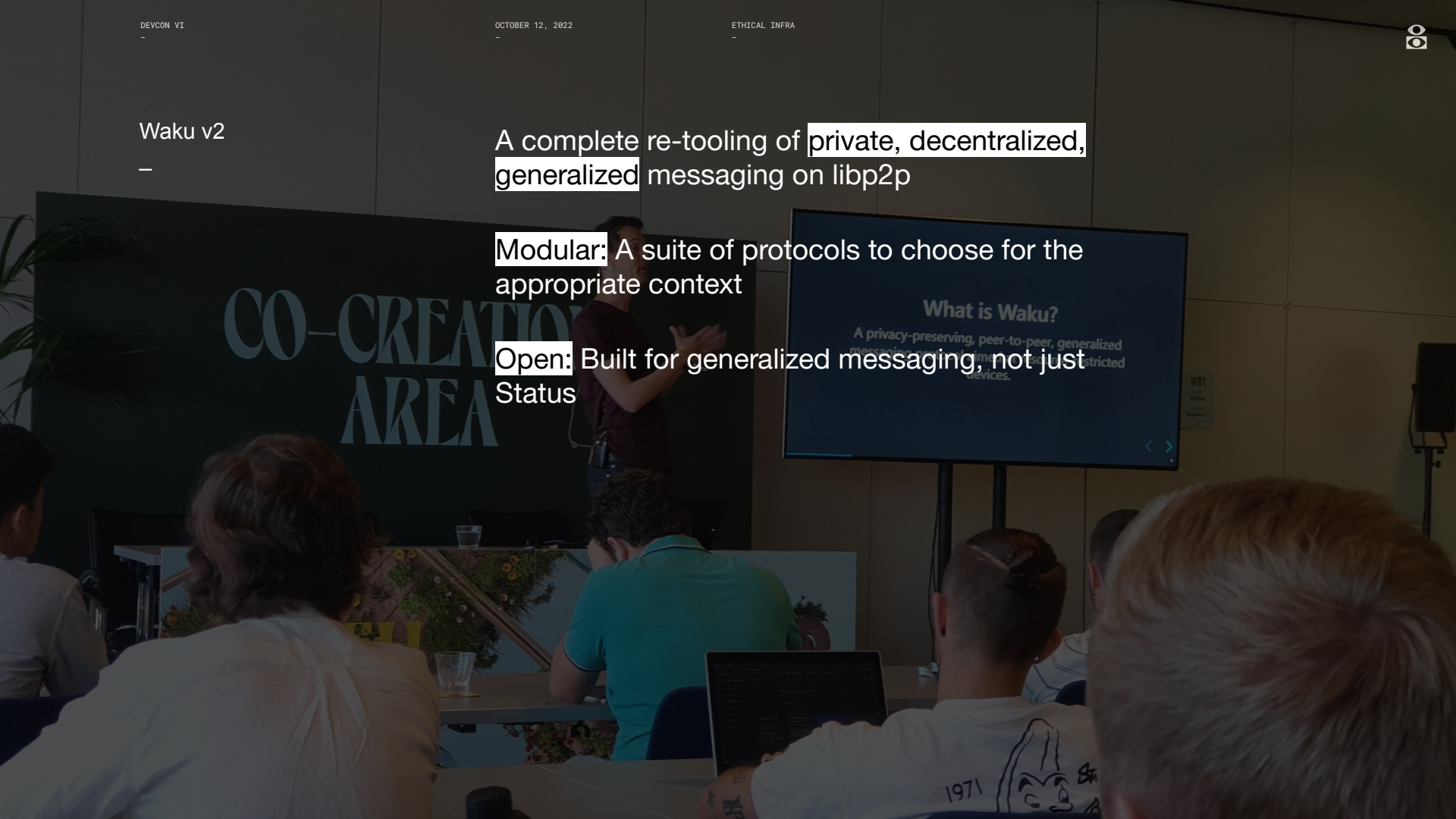
## Waku v2

–

A complete re-tooling of private, decentralized, generalized messaging on libp2p

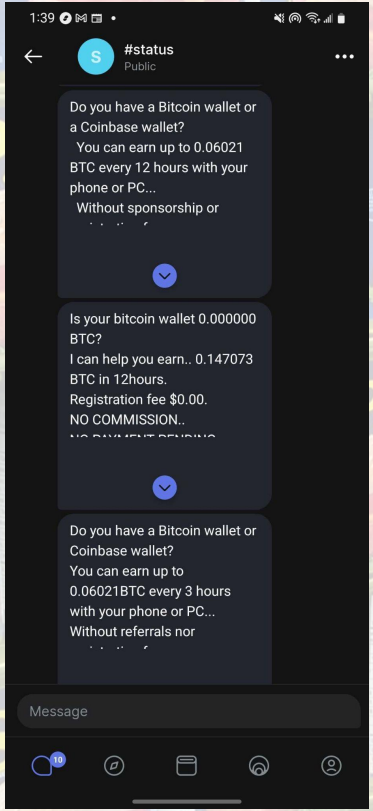
Modular: A suite of protocols to choose for the appropriate context

Open: Built for generalized messaging, not just Status



# Issues

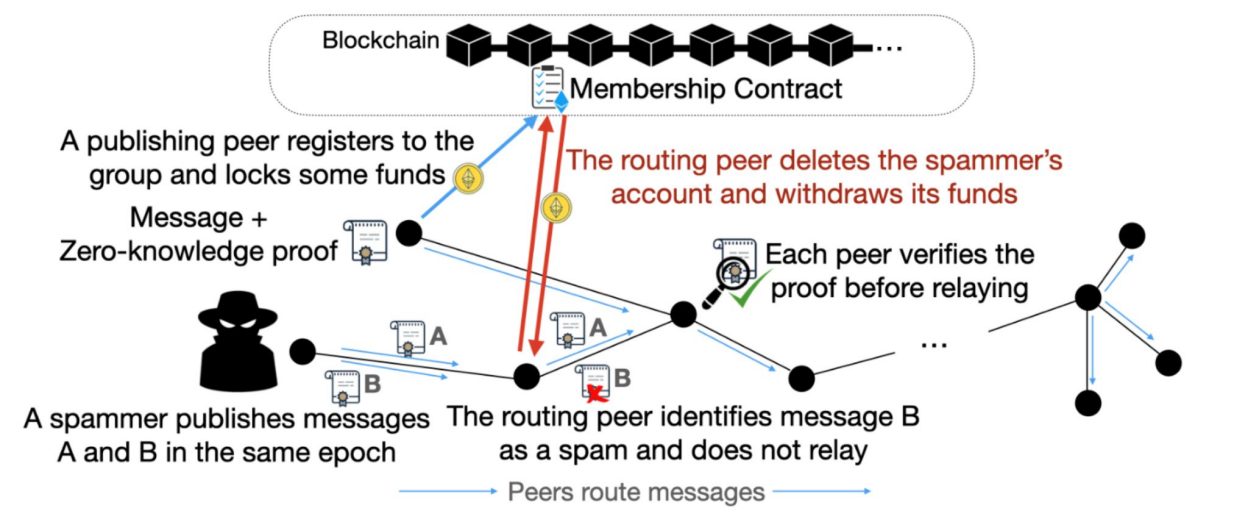
–


1:39
#status
Public
Do you have a Bitcoin wallet or a Coinbase wallet?
You can earn up to 0.06021 BTC every 12 hours with your phone or PC...
Without sponsorship or
Is your bitcoin wallet 0.000000 BTC?
I can help you earn.. 0.147073 BTC in 12hours.
Registration fee $0.00.
NO COMMISSION..
Do you have a Bitcoin wallet or Coinbase wallet?
You can earn up to 0.06021BTC every 3 hours with your phone or PC...
Without referrals nor
Message

The Fruits:
RLN-Relay

Privacy preserving, spam protecting, messaging network leveraging zero-knowledge cryptography, Shamir secret sharing, and economic (dis)incentives

Built on top of the Waku v2 - Relay protocol



It's All
Published,
For Everyone

Specifications at https://rfc.vac.dev

RLN-Relay papers are now available on arXiv
https://arxiv.org/abs/2207.00038
https://arxiv.org/abs/2207.00117
https://arxiv.org/abs/2207.00116

Go play with it

## Wrapping it up

Principles are priority

Publish openly, implement, iterate

Using old tools leads to old things

Assholes are everywhere, think about how they can manipulate the intended messages

Conform technology to relationships, not the other way around

# (Stolen slide) The Sovereign Stack

What we build & how we build it matters

Collective Built
Disintermediated Access
Network Level Privacy
Integrated Decentralised File Storage
Hetereogenous Multi-chain Network
Native Private & Public Smart Contracts
Resource-Restricted Devices

There's work to be done,
and we're hiring