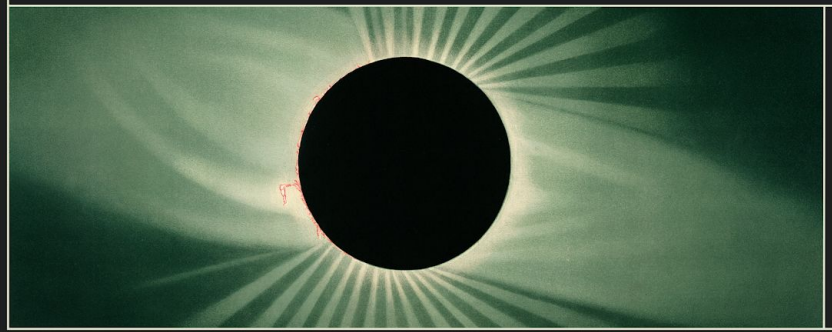
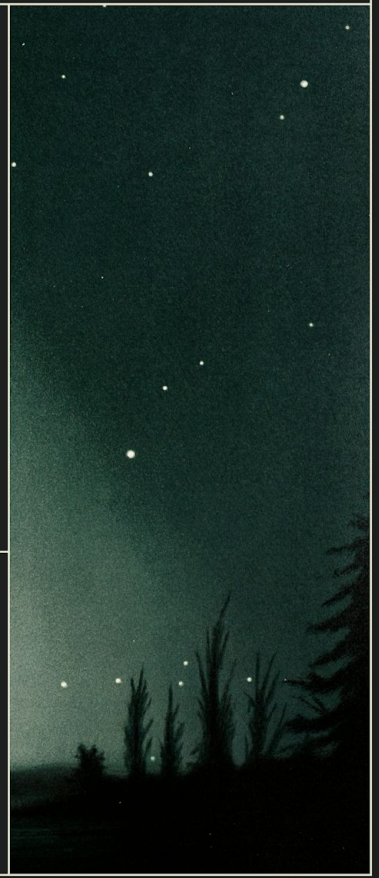
@rachelaux | Design strategy with Privacy & Scaling Explorations

Designing ZK public goods



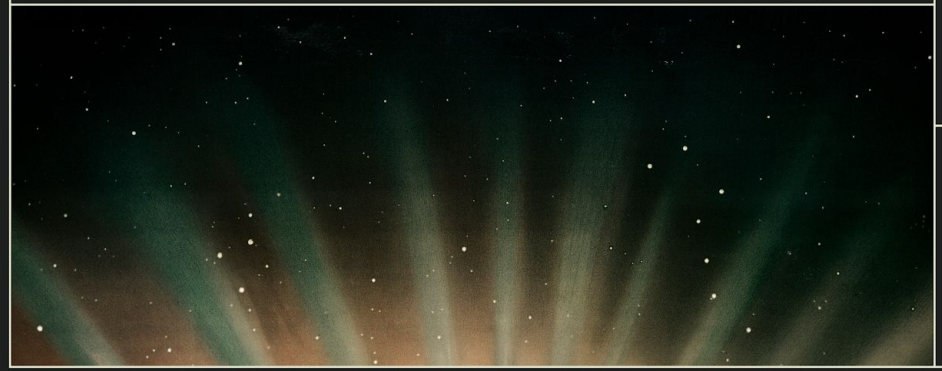


Agenda

- Why design for privacy?
- ZK design challenges
- App interface examples
- Design as a facilitation tool
- Mental models

ZK proofs can give us the ability to select what we reveal or hide in digital interactions.

Why *design* for privacy?



To evolve

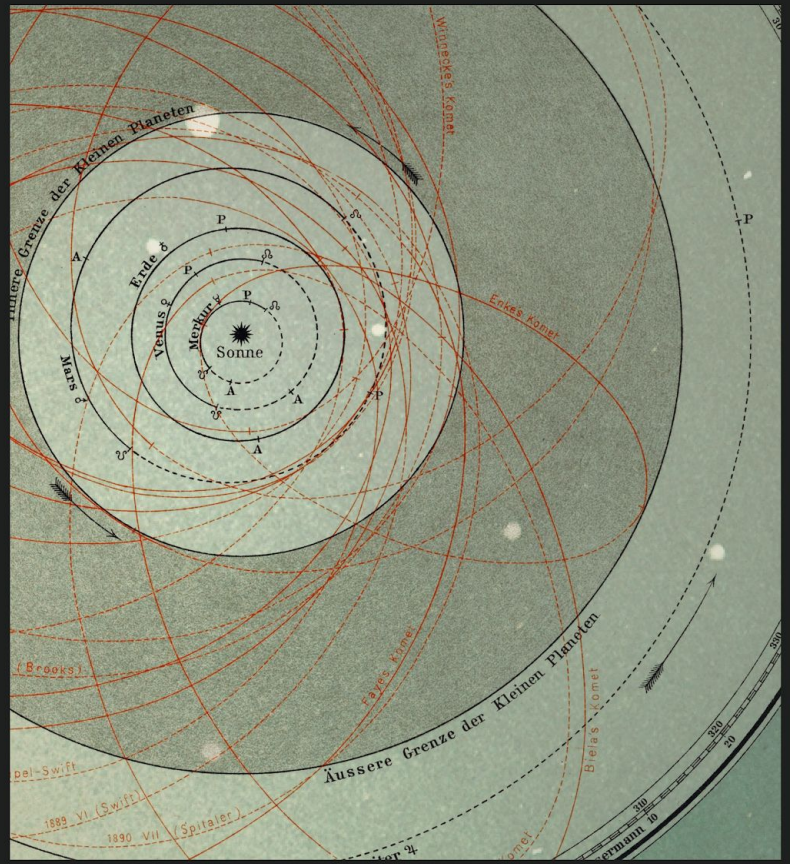
To understand

To foster participation

To fortify privacy

Design to evolve.

Design to understand.



Design to for participation.

Design to fortify privacy.

Do you ever want to prove that something is true without revealing who you are?

Constructing how-might-we questions generates creative solutions while keeping teams focused on the right problems to solve.

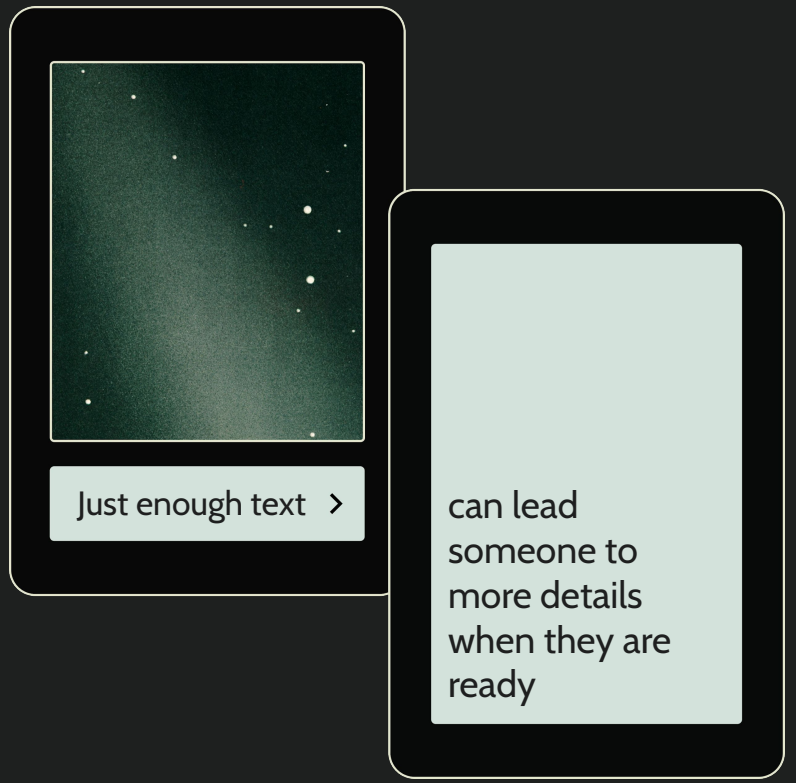
— Nielsen Norman Group

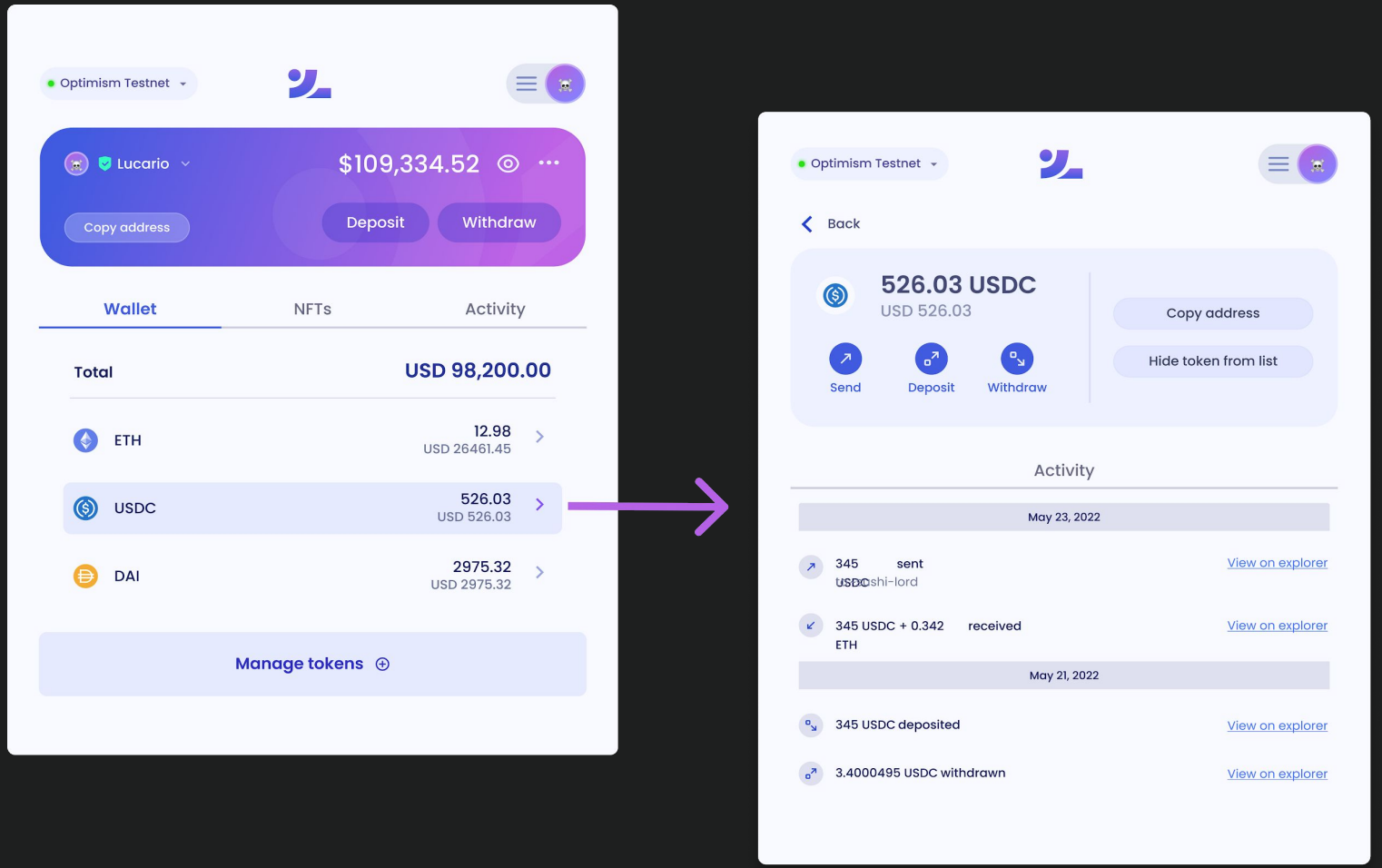
How might we balance approachability and transparency?

See a design response!

zkopru.network

zkopru



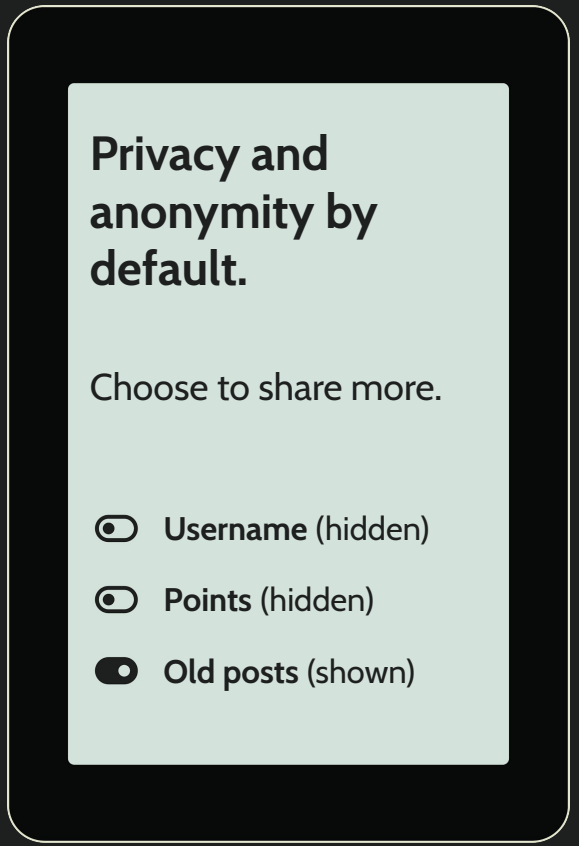

Optimism Testnet
Lucario
$109,334.52
Copy address
Deposit
Withdraw
Wallet
NFTs
Activity
Total
USD 98,200.00
ETH
12.98
USD 26461.45
USDC
526.03
USD 526.03
DAI
2975.32
USD 2975.32
Manage tokens
Optimism Testnet
Back
526.03 USDC
USD 526.03
Send
Deposit
Withdraw
Copy address
Hide token from list
Activity
May 23, 2022
345 sent
View on explorer
345 USDC + 0.342 ETH received
View on explorer
May 21, 2022
345 USDC deposited
View on explorer
3.4000495 USDC withdrawn
View on explorer

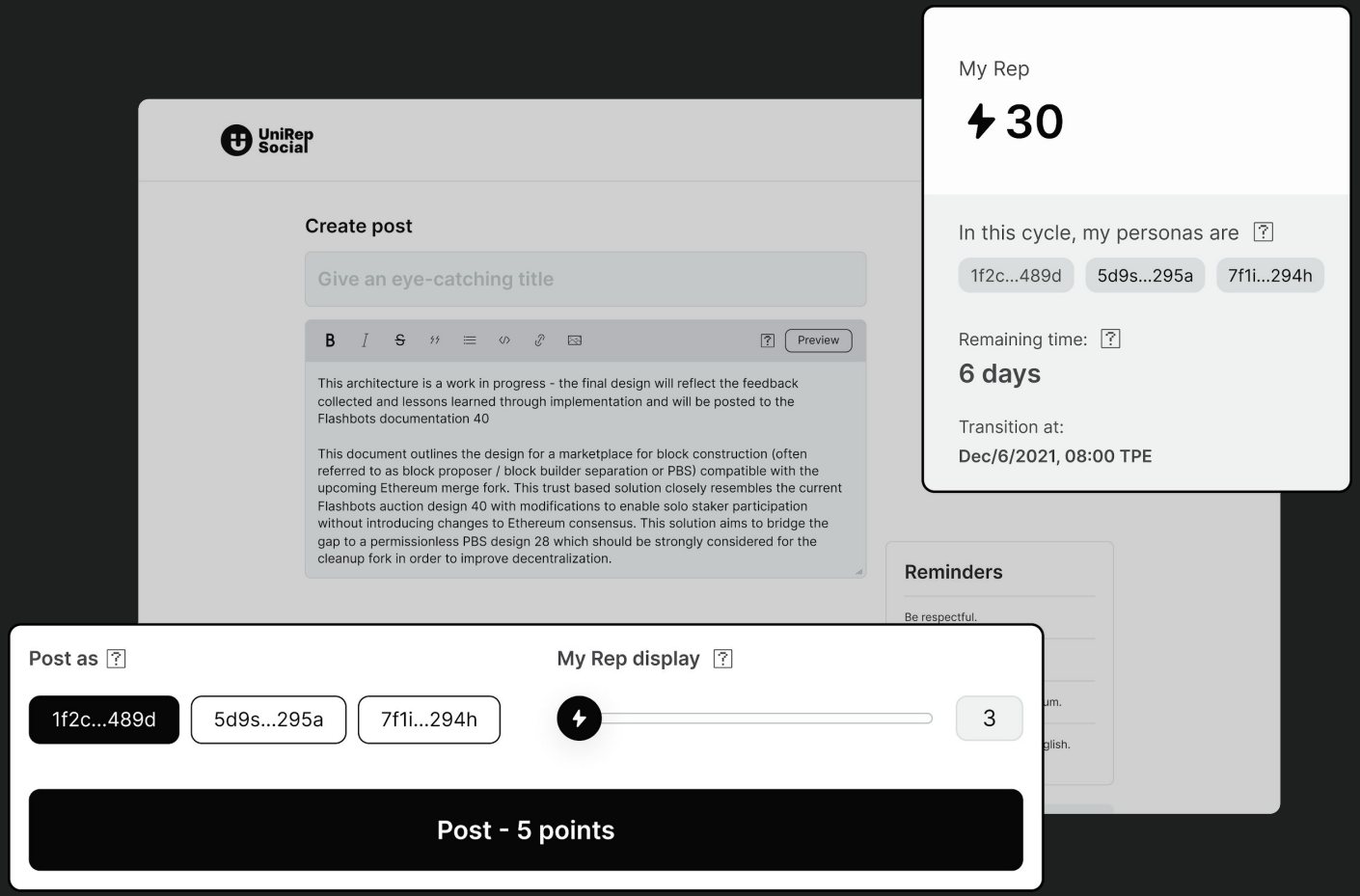
How might we give users the freedom to choose how much they reveal about themselves?

See a design response!

unirep.social

UniRep Social




UniRep Social
Create post
Give an eye-catching title
Preview
This architecture is a work in progress - the final design will reflect the feedback collected and lessons learned through implementation and will be posted to the Flashbots documentation 40
This document outlines the design for a marketplace for block construction (often referred to as block proposer / block builder separation or PBS) compatible with the upcoming Ethereum merge fork. This trust based solution closely resembles the current Flashbots auction design 40 with modifications to enable solo staker participation without introducing changes to Ethereum consensus. This solution aims to bridge the gap to a permissionless PBS design 28 which should be strongly considered for the cleanup fork in order to improve decentralization.
My Rep
30
In this cycle, my personas are
1f2c...489d
5d9s...295a
7f1i...294h
Remaining time:
6 days
Transition at:
Dec/6/2021, 08:00 TPE
Reminders
Be respectful.
Post as
1f2c...489d
5d9s...295a
7f1i...294h
My Rep display
3
Post - 5 points

How might we craft environments for anonymous users to build trust with one another?

See a design response!

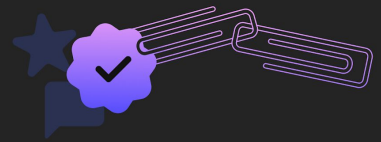
interep.link

interep

interep

Authenticate anonymously on-chain using off-chain reputation

To join Interep groups associated with off-chain applications, authorize the provider to share your credentials with Interep.



Determine your group by authorizing the provider — Generate a Semaphore ID — 3 Join social network group

How you qualify

	Followers	Verification	Botometer Score
Gold members	>500	Verified	<1
@alice101	3.2k	Not Verified	2

Twitter Gold

Members
101

Join

How might we represent identity in communities of anonymous individuals?

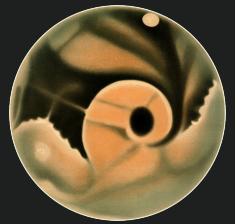
See a design response!

zkitter.com

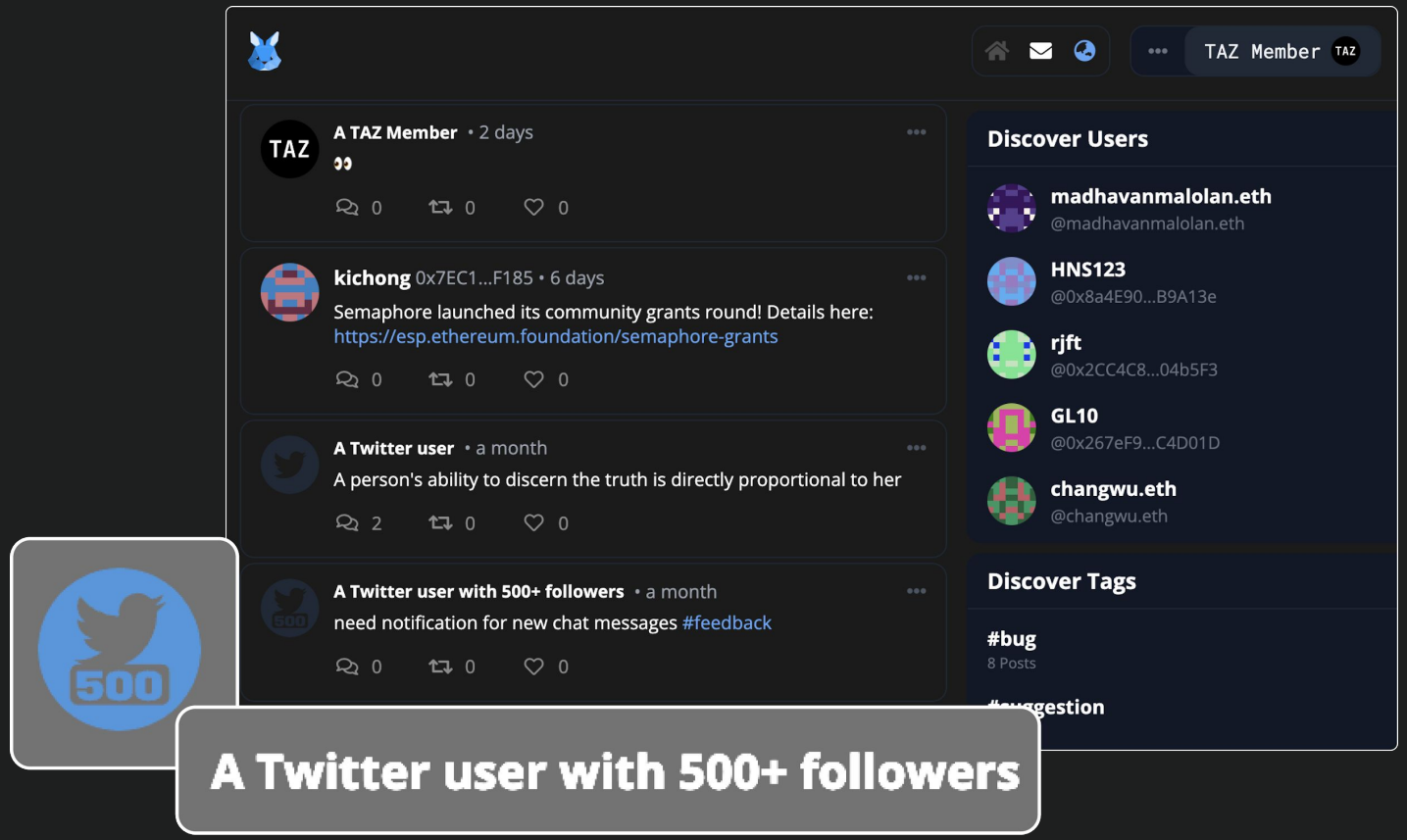
zkitter

Username
Recognizable, static

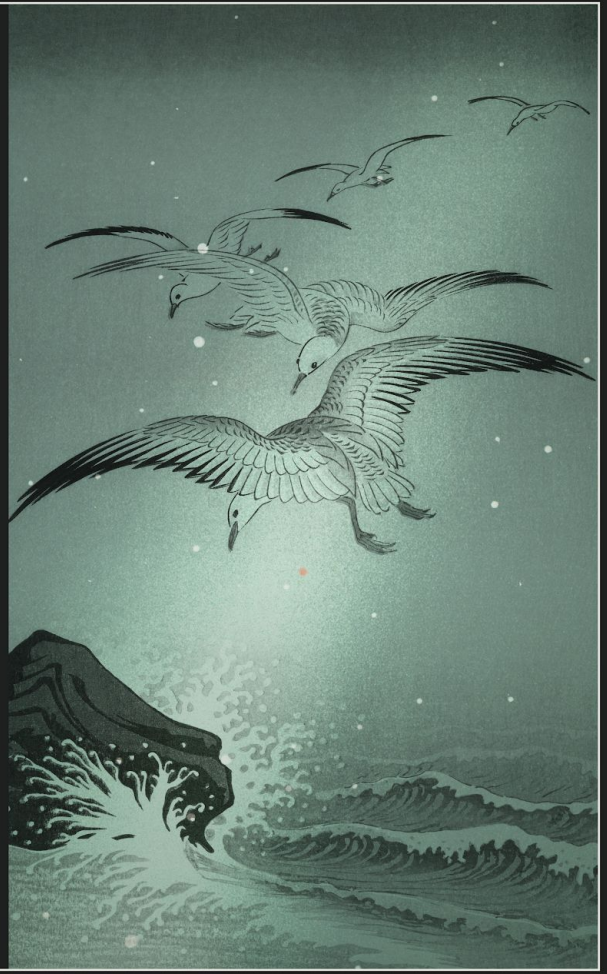
Reputation
Proves something about them socially



Hash
obscure, changing


TAZ Member
A TAZ Member • 2 days
👀
0 0 0
kichong 0x7EC1...F185 • 6 days
Semaphore launched its community grants round! Details here:
https://esp.ethereum.foundation/semaphore-grants
0 0 0
A Twitter user • a month
A person's ability to discern the truth is directly proportional to her
2 0 0
A Twitter user with 500+ followers • a month
need notification for new chat messages #feedback
0 0 0
Discover Users
madhavanmalolan.eth
@madhavanmalolan.eth
HNS123
@0x8a4E90...B9A13e
rjft
@0x2CC4C8...04b5F3
GL10
@0x267eF9...C4D01D
changwu.eth
@changwu.eth
Discover Tags
#bug
8 Posts
500
A Twitter user with 500+ followers

Design begins with **environments** that foster **collaboration** and **processes** that facilitate **conversation**.



Design is really an act of communication, which means having a deep understanding of the person with whom the designer is communicating.

— Donald A. Norman, The Design of Everyday Things

Agenda

then....

10 min: Intro & questions

This

10 min: Write user journey steps in silence

10 min: Review out loud

or

This

20 min: Go through flow together and talk/ write ideas

What is Semaphore?

Semaphore allows Ethereum users to prove their membership of a group and send signals such as votes, endorsements, or feedback without revealing their original identity.

Today's mission!

aphore in physical reality so that we can **communicate** Semaphore's value through an experience, **collect** feedback, and **connect** with curious creators.

Let's brainstorm together how Devcon attendees could learn more about Semaphore through an experience.

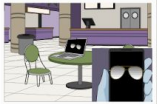
There are a few project constraints including

- timeline (~ 1 month)
- users will need to use their personal laptop
- users will need Meta Mask

Todo

- ~~Need a doc that explains what it would look like whats needed from other apps~~
- ~~Need to clean up board~~
- are we meeting our goals?
- Schedule another workshop for planning the space

Semaphore user flow V1

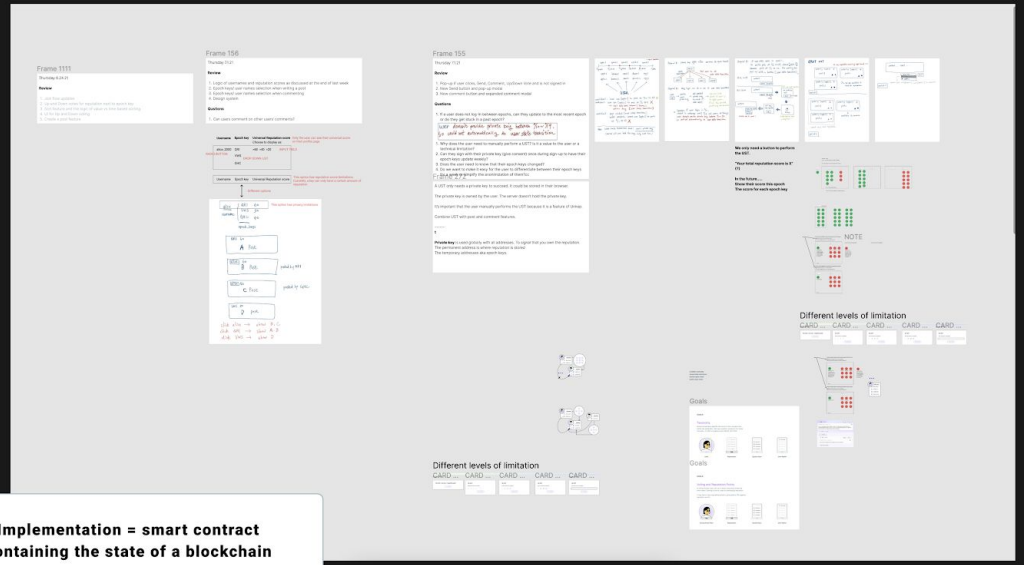
Protocol Steps	Joining the Devcon VI Semaphore Group	Sending a message anonymously	Viewing all group member's signals	People interacting with signals	Take Semaphore Identity to a new place	Follow up/Next steps
						
What the user is doing	The user is on the app and sees groups they can join. Clicks Join and is a member in seconds.	The user is on the app and sees 2 paths: • **Co-creative generative art** • **Q&A**	After sharing, they can see what others have shared	They can even see shared content projected on a white board in the PSE community hub and write on the board	They write their semaphore id on a special card that PSE has designed and take it as a souvenir	
Purpose of the step	To prove they are a Devcon attendee and to trust that all other group members, although anonymous, are Devcon attendees	So that group members can hear each other's thoughts without knowing who they belong to	To view whatever was anonymously shared: feedback, a question, something silly	To make the experience **interactive!** So that people can interact with the anonymously submitted graffiti	To show the value of Semaphore Identities being transportable	
Tools needed	Personal computer Meta Mask POAP stable wifi network	Personal computer stable wifi	Personal computer stable wifi and/or Whiteboard to project onto	Personal computer stable wifi and/or Whiteboard to project onto	other apps that allow user to use their semaphore identity	
Our opportunity	integrate with other project as whole experience?					

Principles for successful workshops

- Open to different skill sets
- Offer multiple ways to contribute
- Create time for discussion + writing
- Have a dedicated notes taker
- Synthesize *a copy* of the results

For workshops that involve many people or have a tight time limit:

- Coordinate with someone else and divide tasks.
- Have a dress-rehearsal to practice your timing.



Overarching technology is Zkopru. It is open source and any number of programs can be built upon it.

Zkopru

Protocol

Implementation = smart contract containing the state of a blockchain

? ? ?

app

Zkopru wallet

app

? ? ?

app

What if someone else builds a wallet on the Zkopru smart contract?

What will they name it?

Implementation Models

- Reflect engineering infrastructure
- Logical to developers
- Do little to help users achieve their goals
- AKA system model

Represented Models

- How designers choose to represent an application
- Represents function independent of true action (similar but not necessarily accurate)
- AKA representation model

Mental Models

- Reflect cognitive shorthand of user
- Only includes info relevant to user
- Does not reflect actual inner mechanics
- AKA conceptual model

– Ref. Cooper and Reiman, About Face 4th edition

Implementation Models

reflect technology

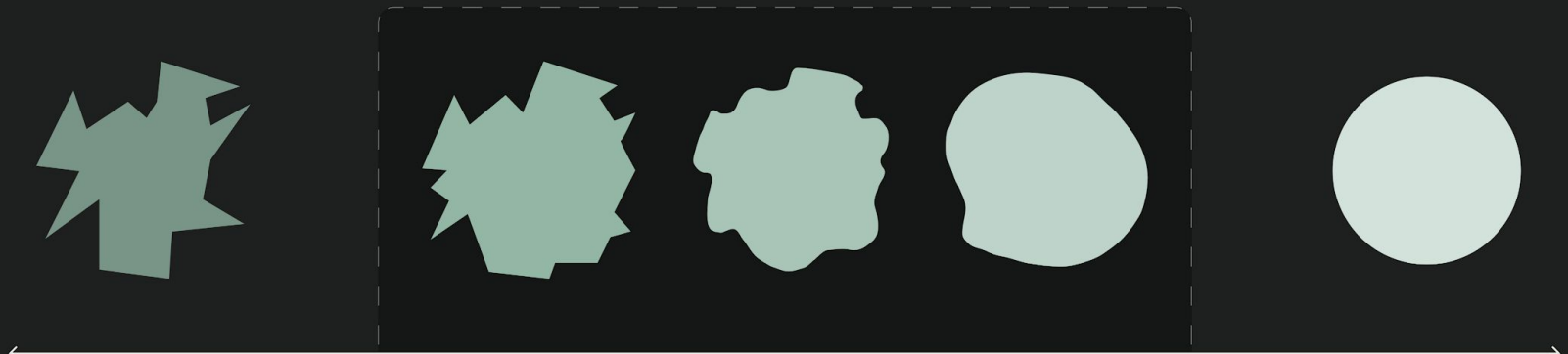
Represented Models

reflect designer's vision

Mental Models

reflect user's vision

– Adapted from Cooper and Reiman, About Face 4th edition



Low-level cryptography

mathematical concepts

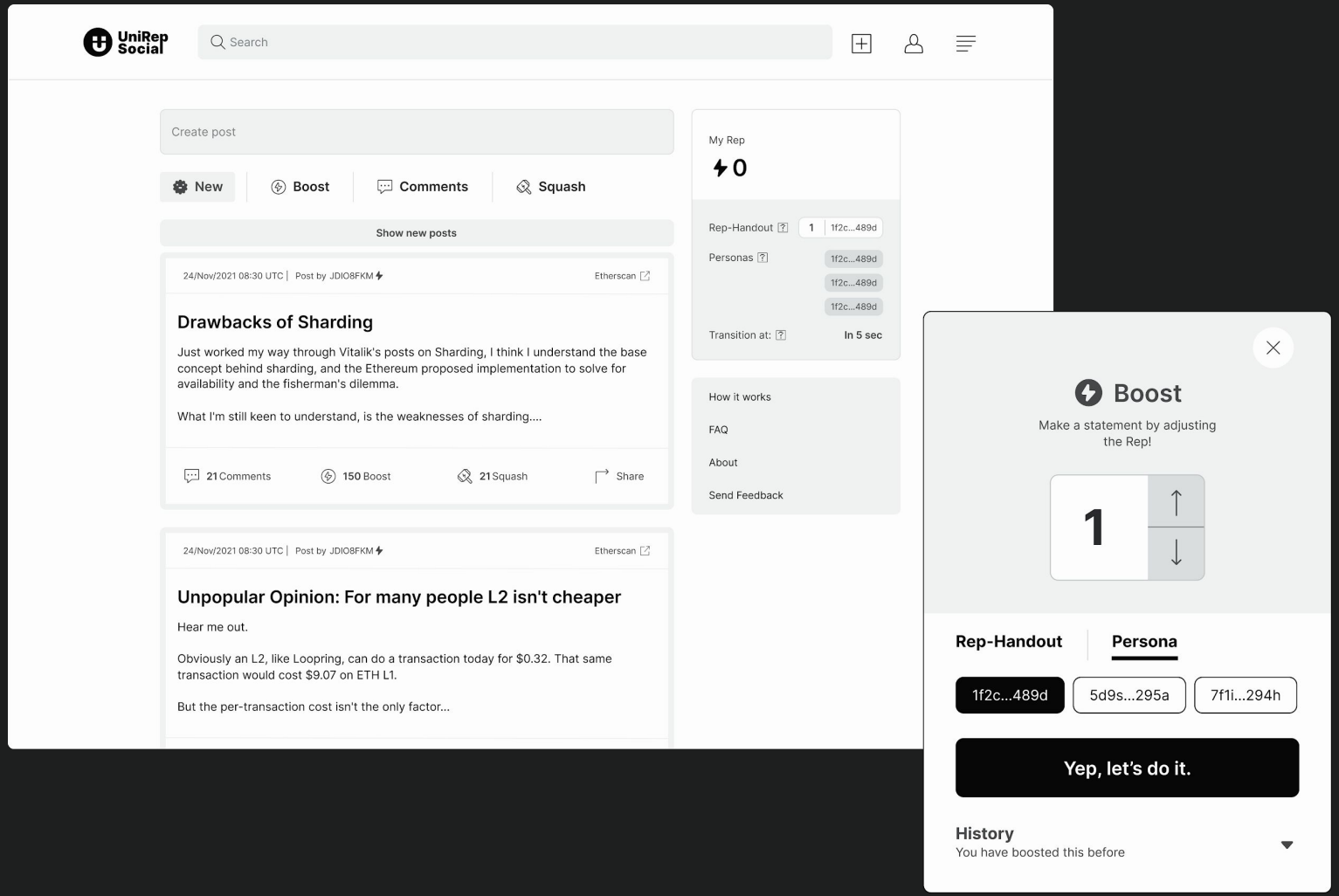
ZK developer's Model

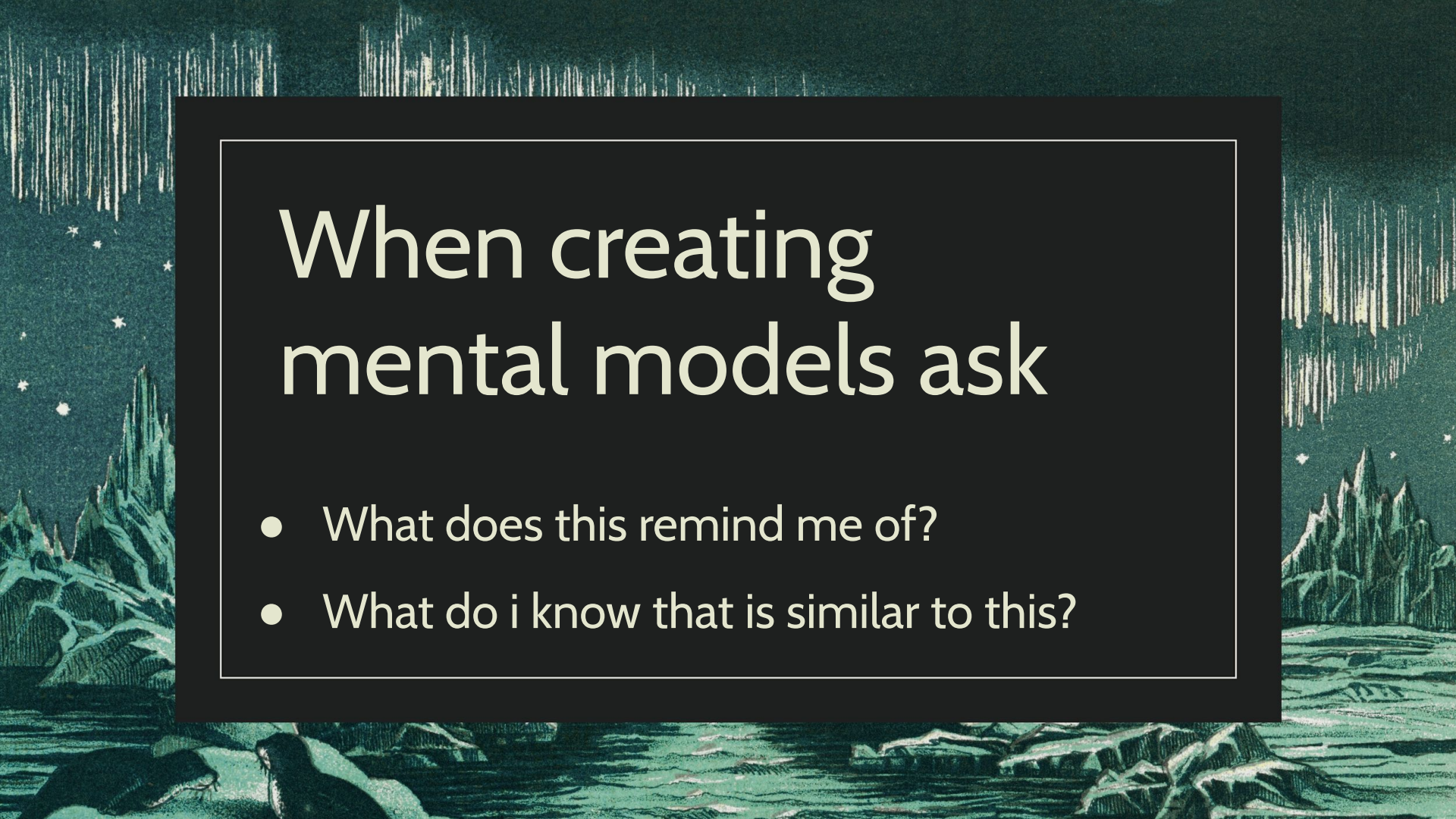
developer's interpretation

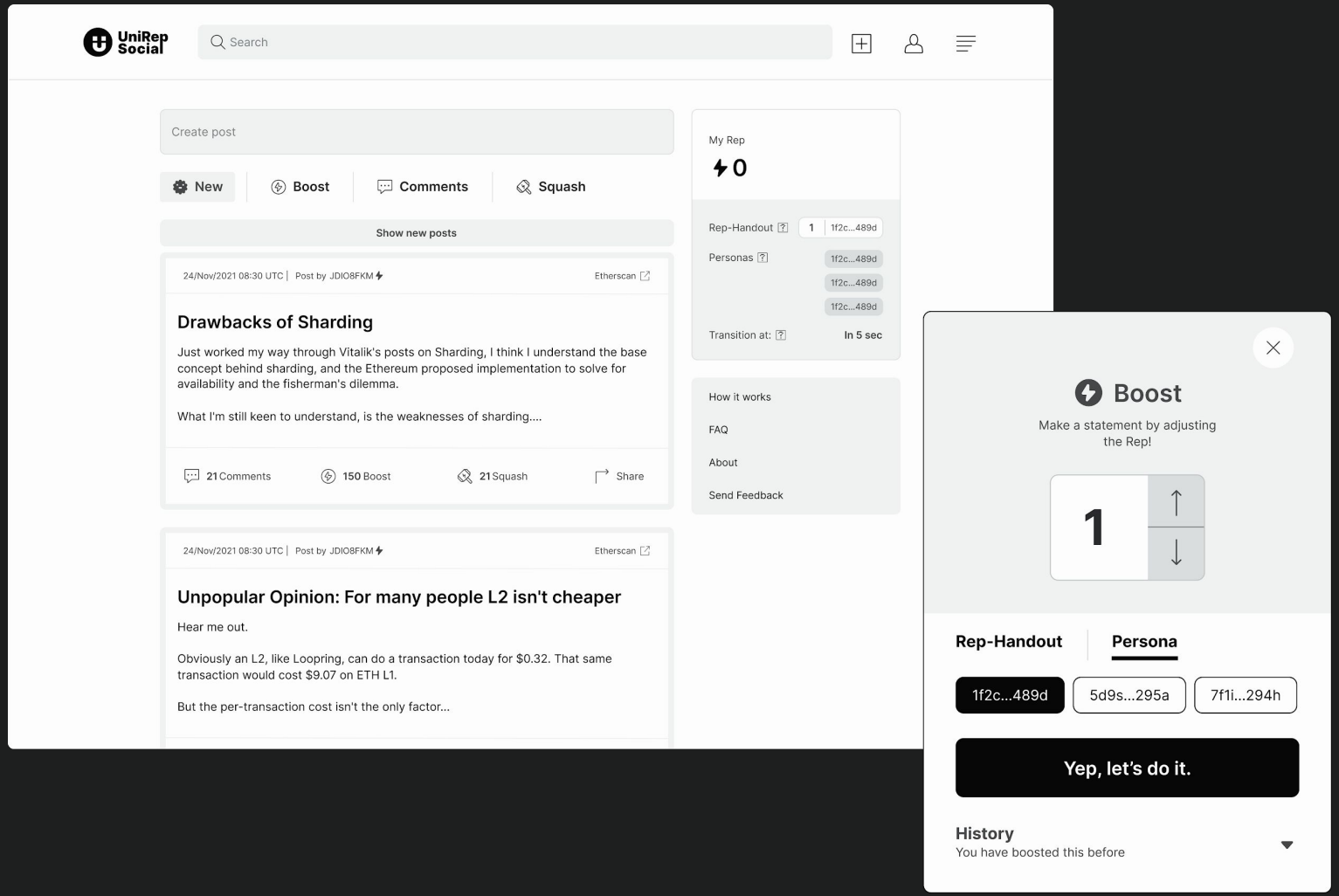
Implementation Models

simple and familiar code

~~— Adapted from Cooper and Reiman, About Face 4th edition~~


UniRep Social
Search
Create post
New
Boost
Comments
Squash
Show new posts
24/Nov/2021 08:30 UTC | Post by JDIO8FKM
Etherscan
Drawbacks of Sharding
Just worked my way through Vitalik's posts on Sharding, I think I understand the base concept behind sharding, and the Ethereum proposed implementation to solve for availability and the fisherman's dilemma.
What I'm still keen to understand, is the weaknesses of sharding....
21 Comments
150 Boost
21 Squash
Share
24/Nov/2021 08:30 UTC | Post by JDIO8FKM
Etherscan
Unpopular Opinion: For many people L2 isn't cheaper
Hear me out.
Obviously an L2, like Loopring, can do a transaction today for $0.32. That same transaction would cost $9.07 on ETH L1.
But the per-transaction cost isn't the only factor...
My Rep
0
Rep-Handout
1
1f2c...489d
Personas
1f2c...489d
1f2c...489d
1f2c...489d
Transition at:
In 5 sec
How it works
FAQ
About
Send Feedback
Boost
Make a statement by adjusting the Rep!
1
Rep-Handout
Persona
1f2c...489d
5d9s...295a
7f1i...294h
Yep, let's do it.
History
You have boosted this before


When creating mental models ask
What does this remind me of?
What do i know that is similar to this?


UniRep Social
Search
Create post
New
Boost
Comments
Squash
Show new posts
24/Nov/2021 08:30 UTC | Post by JDIO8FKM
Etherscan
Drawbacks of Sharding
Just worked my way through Vitalik's posts on Sharding, I think I understand the base concept behind sharding, and the Ethereum proposed implementation to solve for availability and the fisherman's dilemma.
What I'm still keen to understand, is the weaknesses of sharding....
21 Comments
150 Boost
21 Squash
Share
24/Nov/2021 08:30 UTC | Post by JDIO8FKM
Etherscan
Unpopular Opinion: For many people L2 isn't cheaper
Hear me out.
Obviously an L2, like Loopring, can do a transaction today for $0.32. That same transaction would cost $9.07 on ETH L1.
But the per-transaction cost isn't the only factor...
My Rep
0
Rep-Handout
1
1f2c...489d
Personas
1f2c...489d
1f2c...489d
1f2c...489d
Transition at:
In 5 sec
How it works
FAQ
About
Send Feedback
Boost
Make a statement by adjusting the Rep!
1
Rep-Handout
Persona
1f2c...489d
5d9s...295a
7f1i...294h
Yep, let's do it.
History
You have boosted this before

A paradoxical, but perhaps realistic, view of design goals is that their function is to motivate activity which in turn will generate new goals.

— Herbert Simon, *The Sciences of the Artificial* (Third Edition, 1996)

Impact of public goods fortified by design

Builders and product teams empowered by educational content

Reduced stigma of online privacy and anonymity

Transparent protocol resources informed by user research

Decreased friction during user on-boarding

Approach challenges with curiosity	Align strategy to audience objectives
Get comfy with the unknown	Test potential solutions
Ask more questions	Iterate!

Say hi:

@rachelaux #🎨designing-public-goods

Get involved:

TAZ Community Hub

Adoption Day UX Unconference
Th 10-6 @ Workshop 4 - Floor 3

Design for ZK learning group

PSE website

appliedzkp.org

PSE Discord

@chiali | @beyondr | @kichong

@althea | @jchance | @cedoor.eth

@bigkat | @tsukino | @atheartengineer

Thank you!