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

See a design response!

unirep.social

Privacy and anonymity by default.

Choose to share more.

- Username (hidden)
- Points (hidden)
- Old posts (shown)
This architecture is in progress - the final design will reflect the feedback collected and lessons learned through implementation and will be posted to the Flashbots documentation.

This document outlines the design for a marketplace for block building (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.

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

See a design response!

interep.link
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.

1. Determine your group by authorizing the provider
2. Generate a Semaphore ID
3. Join social network group

How you qualify

<table>
<thead>
<tr>
<th>Gold members</th>
<th>Followers</th>
<th>Verification</th>
<th>Botometer Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>@alice101</td>
<td>3.2k</td>
<td>Not Verified</td>
<td>2</td>
</tr>
</tbody>
</table>

Twitter Gold

Members

101

Join
How might we represent identity in communities of anonymous individuals?

See a design response!

zkitter.com

Username
Recognizable, static

Reputation
Proves something about them socially

Hash
Obscure, changing
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
# 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

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

What will they name it?
<table>
<thead>
<tr>
<th>Implementation Models</th>
<th>Represented Models</th>
<th>Mental Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflect engineering infrastructure</td>
<td>How designers choose to represent an application</td>
<td>Reflect cognitive shorthand of user</td>
</tr>
<tr>
<td>Logical to developers</td>
<td>Represents function independent of true action (similar but not necessarily accurate)</td>
<td>Only includes info relevant to user</td>
</tr>
<tr>
<td>Do little to help users achieve their goals</td>
<td>AKA representation model</td>
<td>Does not reflect actual inner mechanics</td>
</tr>
<tr>
<td>AKA system model</td>
<td></td>
<td>AKA conceptual model</td>
</tr>
</tbody>
</table>

– 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
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...

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...
When creating mental models ask

- What does this remind me of?
- What do I know that is similar to this?
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...

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

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
<table>
<thead>
<tr>
<th>Approach challenges with curiosity</th>
<th>Align strategy to audience objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get comfy with the unknown</td>
<td>Test potential solutions</td>
</tr>
<tr>
<td>Ask more questions</td>
<td>Iterate!</td>
</tr>
</tbody>
</table>
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!