Grantee Day

by ecosystem support program
Privacy & Scaling Explorations

What we do & how to get involved

Thore
PSE
What we do
Privacy & Scaling Explorations Team

We explore new use cases for zero knowledge proofs

- We build
  - Circuits
  - Gadgets & Applications

- Other things we do
  - Education
  - Grants
ZKP’s on Ethereum

ZKP: proof that you have computed something correctly (off chain)

- Generate proof (off-chain)
- Verify proof (on-chain)
- Optionally hide the inputs

-> Give privacy and scalability back to Ethereum
zkEVM

- Proof Ethereum transaction
- Useful for zk-rollups or light clients (maybe)
- Community edition
- Github: privacy-scaling-explorations/zkevm-circuits
- Vitalik blog
  - Perfect compatibility
  - Disadvantage: prover time
Semaphore

- Privately prove membership of a group
- Circuits, contracts, js libraries
- Allow people to join groups and signal privately
- Semaphore grants round
- Demo on Devcon: TAZ
- semaphore.appliedzkp.org
MACI

- Bribery resistant voting
- Useful for e.g. quadratic funding
- Users can always override their (encrypted) vote
- Coordinator zk proves that tallied correctly
- Quadratic Funding Devcon, QFI
How to get involved
PSE Grants: Semaphore Community Grants

- Dedicated public grants round
- Projects that build on, or extend Semaphore
- Projects at all stages are welcome
- Deadline: Oct 14th (might be extended :))
PSE Grants: L2 Community Grants

- Support L2 projects
- Rollups, infrastructure, analytics and education
- Projects at all stages are welcome
- Launch Oct 24th
General Grants and Collaboration

- Grants with PSE
  - Who?
    - ZK focussed individuals
  - What?
    - Build on our primitives
    - Come with your own ideas
    - Ask us for ideas

- We are hiring

- Everything is open source
How to get involved

- Check out our projects
  - PSE Website: appliedzkp.org
  - PSE Github: @privacy-scaling-explorations
Thank you!

Thore
Privacy Scaling Explorations (EF)
tg: @zk_th
What Can DAOs Learn From?

Presented by Dream DAO
Introductions

Madison: Co-Founder

Saf: Co-Steward
Dream DAO: We train Gen Z to use web3 for good.

Education
Learning sessions with leaders of web3. Mentorship program.

Internships
Internship program twice per year, at sites like Celo and Regen Network.

Gatherings
Sponsoring conference trips and hosting in-person gatherings.
The Promise of DAOs

Maximizing human coordination
The good news?

We don’t have to reinvent everything.
We are solving human problems.

It’s not all tech

Why repeat mistakes when we can learn from them?
What we took inspiration from: Civics Unplugged

Civics Unplugged trains Gen Z to be “civic innovators”. It was essentially an off-chain DAO before they even knew DAOs existed.

- Elected steering committee with a treasury
- Community votes on youth-led projects to fund
- Sub-groups that work on responsibilities like social media and international student experience
Case Study #1: Boy Scouts

The Boy Scouts of America is one of the largest youth organizations in the United States, with about 1.2 million youth participants.

Recruiting Youth

Recruits from existing, values-aligned organizations. Strong emphasis on word of mouth recruitment as well.

Gamification

- Goals are clear: highest level is “Eagle Scout”
- Badges to reward small steps along the way
Case Study #2: Parks

The foundation of public park design and construction is community involvement and gaining consensus.

“Master Plans”
Creates a detailed plan for how the park will be developed. Serves as a blueprint others can learn from. (Open-source :)

Spokes-Council
- Reps of different groups: police/fire depts, Boy scouts, teacher, etc
- Reps go back to smaller groups for meetings
- Anyone can request, all open to the public

Existing for Users
Goals oriented around serving users and extensive mapping of users
Case Study #3: Ecovillages

Small, sustainable physical/co-living communities with their own work, currency, school, and more.

- **Small Size**: Range from 50 to 250 individuals, because with any more it is hard to form a strong community.

- **Work and Play**: Residents of ecovillages have lots of formal structure to keep it running, but have an equal emphasis on community: work and play are interdependent.

- **Making Money**: Most cannot export because of physical isolation, so some make money off of providing education/consulting to outsiders.
Call to Action

Learn from others, and let others learn from you.
Your turn!

What are some examples you know of?
Ecosystem Support Program

Luc L
Team Lead, ESP
What is ESP?

Public facing allocation arm of the Ethereum Foundation

Instead of asking “What should we fund?”, we want to know “What challenges are you facing?”

Support is more than just funding

Proactive, rather than reactive
What does ESP support?

- Open source
- Non-commercial
- Benefits
- Ethereum
- Positive sum outcomes
- Projects on the lower end of the development stack
What are we looking for?

Grow usage
Grow community
Grow developer base
Grow research capabilities
Improve developer output
Support R&D that makes Ethereum’s tomorrow a reality
Upkeep, i.e. maintaining today’s crucial projects
What does all of this mean?

Core Development
- Targeted grants
- RFPs
- Challenges

Support Ecosystem
- Non-financial support
- Grants
- Sponsorships
- Mentoring
- Connections

Ecosystem Motivation & Capacity

Core Development
- Low priority (for now)

Support Ecosystem
- Leave Ecosystem to Develop
What do we stay away from?

Projects that can easily raise funds through VCs or other mechanisms
Projects with a planned token launch or public funding round
NFT projects
Financial products (e.g. trading, investment products)
Token or investment focused events
Hobby activities
ESP

Forms of Support
Office Hours

20-minute video calls to offer support in the form of:

- Guidance within the Ethereum ecosystem
- Advice surrounding the grants process
- Feedback on your project before submitting it
- Determining if your project is within the scope of our program
- Identifying other resources and funding opportunities
Sponsorships

Support community events including conferences and hackathons

Capped at $20,000
Sponsorships Evaluation

Are the overall goals of this event Ethereum-aligned?

Is this event hosted in a geographic region that receives limited support?

What speakers will be present at this event?

Can the EF’s support uniquely help this event?
Small Grants

Projects that are smaller, more experimental, in early stages, or have a shorter timeline

Kickstart a project

Capped at $30,000
Project Grants

Projects with a larger scope, more complex needs, thorough research, and clearly defined goals and strategies

Undergo process of collaborative review and feedback with advisors within the ecosystem

No cap on funding requests
Grants Evaluation

**Problem** - how important is the problem to be solved?

**Project** - how does the proposed project push the state of the art forward, is it feasible, does it add something, how does it fit into the landscape of existing approaches?

**People** - is this team capable, are they values aligned?

**Plan** - is the project plan and use of resources sensible?

How do we avoid second order negative impact?
Process

Submit an application via our website

ESP team will get in touch within 1 - 2 weeks

Video call to discuss further
What has ESP been up to?
Applications Received
## Academic Grants Round

More than $2 million allocated across 39 grants in 7 categories

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th># OF PROJECTS</th>
<th>AMOUNT (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economics</td>
<td>9</td>
<td>$222,067.00</td>
</tr>
<tr>
<td>Consensus Layer</td>
<td>9</td>
<td>$483,477.81</td>
</tr>
<tr>
<td>P2P Networking</td>
<td>5</td>
<td>$386,592.00</td>
</tr>
<tr>
<td>Maximum Extractable Value</td>
<td>5</td>
<td>$351,659.00</td>
</tr>
<tr>
<td>Formal Verification</td>
<td>4</td>
<td>$283,165.51</td>
</tr>
<tr>
<td>Cryptography and zero knowledge proofs</td>
<td>2</td>
<td>$120,000.00</td>
</tr>
<tr>
<td>Other domains</td>
<td>5</td>
<td>$194,807.00</td>
</tr>
</tbody>
</table>
Merge Data Challenge

Document your best Merge data insights in the most readable blog post possible

Up to $30,000 in prizes to be won

Deadline for submission is October 31, 2022

Learn more and apply here!
Semaphore Grants

Submit your proposals for privacy-preserving applications built with Semaphore

Wishlist includes a wide range of domains, including medical, government, and cybersecurity

Deadline for submission is October 28, 2022

Learn more and apply here!
Stay in touch!

ESP Blog

Twitter
Find us at our booth in Devcon on Floor 3!
Web3 is Going Great

Panelists
- Brian
  OxpARC Foundation
- Eda
  BuidlGuidl
- Jacob
  ETHGlobal
- Romina
  ETHLatam

Moderator
- Mauricio
  TRU, Tropkyus
Anukriti Kunwar

- Product Manager at Spruce
- Prev. Data Program Manager
- Based out of NYC
About Spruce

Spruce was founded in 2020 and is a globally distributed team of 20.

Our Mission:
To enable users to control their data across the web
What We’ll Cover

- Decentralized Identity
- Big Login Today
- SIWE Crash Course
- SIWE Support & Community
- The Future of SIWE
What is Decentralized Identity?
Statements about reality by anyone,

**On-Chain**
- ETH Balance = 2.4
- Unisocks Holder
- Spent 3 ETH in Gas
- DAO Hack Victim

**Off-Chain**
- Email = ethlad@gmail.com
- Twitter handle = @handle, have over 2,000 followers
- Discord Handle = @sprucewayne#1452
- SoundCloud Handle = WaynePlaysGuitar

anukriti.eth
Approaches: Off-Chain Statements

Issuer → Holder

Issues Credentials

Registers Identifiers and Uses Schemas

Verifiable Data Registry

Verifier → Holder

Sends Presentation

Verifies Identifiers and Uses Schemas

Verifiable Data Registry

Verifies Identifiers and Uses Schemas
The Goal

User

Application

Database

User

Database

Application
Goal: Defeat Big Login

Just as cryptography can be used to disintermediate large banks, adding transparency and user control, the same can be done for our digital identities, allowing those who want more ownership to have it.
Not Your Keys, Not Your Crypto
Not Your Keys, Not Your Identifier
Ethereum Users HAVE Keypairs

- Key management is already being actively solved by multiple wallets.
- Today, they are used mainly to sign blockchain transactions.
- With these keys, we can also move far beyond Web2 identity and simple SSO.
But what’s the first step?
Sign in with Ethereum
Sign-In With Ethereum Support

ethereum foundation

Spruce

ENS
Sign-In with Ethereum - How Did We Get Here

- Public standardization process with community calls
- Ongoing recordings, available minutes, continued iteration
- Combined effort: wallets, dapps, engineers, security engineers
Sign-In with Ethereum Crash Course

Connect Wallet
Sign-In with Ethereum Crash Course

1. Connect Wallet
2. Sign Message
3. Authenticated!
Sign-In with Ethereum Crash Course

**LOGIN**

```
eutioqqufiwqafbh <- here is your magic phrase!
```

**Sign-in to my site!**

SECRET MESSAGE! DON'T TELL ANYONE THIS MESSAGE - THIS PROVES YOU OWN YOUR WALLET.

---

login.xyz wants you to sign in with your Ethereum account:
0x225e...44c9b772

**Sign-In With Ethereum Example Statement**

URI: https://login.xyz
Version: 1
Chain ID: 1
Nonce: 1cjg29m4
Issued At: 2023-05-15T19:51:51.354Z
Expiration Time: 2023-07-17T19:51:51.351Z
Sign-In with Ethereum Crash Course

login.xyz wants you to sign in with your Ethereum account:
0x225e...44c9b772

Sign-In With Ethereum Example Statement

URI: https://login.xyz
Version: 1
Chain ID: 1
Nonce: 10jgz9m4
Issued At: 2023-05-15T19:51:51.354Z
Expiration Time: 2023-07-17T19:51:51.351Z

login.xyz wants you to Sign-In with Ethereum
Click Sign-In to complete this request!

See details.

[Cancel] [Sign-In]
Phishing scam posing as login.xyz

Woah - hold up, this isn't login.xyz!
You might want to double-check that, chief.
See details.

Cancel  Sign-In
Sign-In with Ethereum Crash Course

$(domain) wants you to sign in with your Ethereum account: $(address)

$(statement)

URI: $(uri)
Version: $(version)
Chain ID: $(chain-id)
Nonce: $(nonce)
Issued At: $(issued-at)
Expiration Time: $(expiration-time)
Not Before: $(not-before)
Request ID: $(request-id)
Resources:
- $(resources[0])
- $(resources[1])
... 
- $(resources[n])
Sign-In With Ethereum Support

- Wallets
  - WalletConnect
- Applications
  - Unlock
  - Tally
  - rainbow
- Even Enterprises
  - CyberConnect
  - Auth0
  - boardroom
  - GameStop
  - NFT
  - nfty chat
The Future of SIWE

Link social media accounts to addresses

On-chain, cross-chain, and off-chain data are blended

Web2 APIs become trusted data faucets in Web3

Surface Data

Maturity of Web3 Identity

Deep Data
We will sign in with Ethereum to the key-controlled revolution.

Twitter: @spruceid / @bebaakbeyou
https://docs.login.xyz
Building a Post-Merge World

Panelists

Diego
Ethereum on ARM

Nixorokish
ETHStaker

Kris
L2BEAT

Paul
Sigma Prime

Moderator

Mario
EF
Account Abstraction

Making accounts smarter

Dror Tirosh & Liraz Siri

Gas Station Network
What is Account Abstraction
Accounts in Ethereum

- Externally Owned Account (EOA) - controlled by an ECDSA key
- Smart Contract - controlled by code

Your current wallet is probably an EOA
The limitations of EOAs - key management is hard

- Tightly coupled with a single key
- Hard to secure - keys get stolen
- Hard to recover - keys get lost
The limitations of E0As - access control

- No access control granularity - same for all E0As
- No multisig
- No roles
- No spending policies
The limitations of EOAs - gas payment

- Gas is paid directly by the EOA
- Must maintain ETH balance to pay gas
- No privacy
The limitations of EOAs - efficiency & usability

- No way to batch operations
  - approve+transferFrom - two transactions
- Expensive on-chain reverts
What is account abstraction?

Smart Contract account managed by the user

- Flexible key management and recovery
- Arbitrary access control mechanisms
- Gas payment can be abstracted
- Better efficiency and usability
- Opportunity to innovate where it matters most: UX
Use cases: recovery

- Social recovery
- Dead man’s switch
Use cases: signature abstraction

- Multisig
- Per-device keys
- BLS aggregation
- Quantum resistant signatures
Use cases: roles & policies

- Spending limits
  - Small payments? Seamless from your wallet.
  - Sending $1M? Go get your ledger.

- Multiple roles, delegating specific actions.
  - Payroll can pay employees once a month, with a spending limit and a signature from the controller.
  - Legal can perform on-chain votes with the company’s tokens, but can’t transfer them.
  - CFO can transfer any sum with 24 hours delay and a signature from another C-level executive.
  - External auditor monitors delayed payments and can veto them, but can’t initiate transfers.

- Session keys
  - Ephemeral key kept in the browser can perform less-sensitive operations.
Use cases: gas abstraction

- Gas sponsorship models
- Pay gas with ERC20 tokens
- Privacy - interacting with the blockchain without buying ETH
- Cross-chain operations
Use cases: batching & automation

- Batching and atomicity
- Automating time-delayed and event-driven flows
ERC 4337 - why make it a standard?
ERC-4337 - first step toward protocol level Account Abstraction

- Shared mempool for arbitrary contract wallets
  - A single network of bundlers can serve everyone
- Make contract-wallets a 1st class citizen
  - No need to keep an additional EOA funded to use the wallet
- Separate validation from execution
  - Enables efficient block-building and prevents DoS attacks
- Efficient batching and aggregation
  - Makes rollups cheaper
- No protocol changes
  - Start experimenting now on any EVM chain
What’s next?

- Enshrine AA into the protocol without enshrining a particular wallet
- Seamlessly convert existing EOAs to smart contracts
- User can choose the implementation and enjoy new AA features
- Default implementation should emulate an EOA
  - Backward compatible with existing wallets
- Can be achieved in a few ways - still in discussion
  - New transaction type for calling account code - account pays gas
  - New transaction type just for setting account code
  - EIP-3074+EIP-5003 (AUTH+AUTHUSURP)
  - Set default proxy contract for all addresses
  - ...
How do I join the AA revolution?
Build wallets

● Start experimenting with ERC-4337
● Add useful features like batching and key recovery
  ○ Try some ideas from the first part of this presentation
● Innovate: build cool new features that were not possible with EOAs
● Building a cool ERC-4337 project? Consider applying for an EF grant!
  ○ https://esp.ethereum.foundation/
Building a DApp? Consider AA implications

- Consider contract wallets a 1st class citizen
- Do not assume that accounts can sign messages directly
  - Use ERC-1271 to check for signatures if the caller has code
- Start supporting batching in your UI when connected to a contract wallet that supports it
- Consider gas sponsorship models that suit your DApp.
  - Got a token? Your users could pay gas with it when using your dapp.
- Collaborate with wallet devs on ways to improve DApp UX through wallet innovation
Useful links

- ERC-4337 SDK
- ERC-4337
- Account abstraction discord

Where can I learn more?
Thank you!

Dror Tirosh & Liraz Siri
Gas Station Network

@opengsn
Break!
Solidity Dev to ZK Dev

Why and How You Should Start ZK Dev Now

Jack Gilcrest - Ian Brighton
BattleZips - ZK Battleship
What is Web3?
What Does Satoshi Nakamoto Think?

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."
What Does Vitalik Buterin Think?

"What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create 'contracts' that can be used to encode arbitrary state transition functions"
What Does Nick Szabo Think?

“The obscurity of a large random number, so vast that a lucky guess is unlikely in, if desired, the lifetime of the universe, is the foundation upon which cryptographic protocols, and in turn smart contracts, are built.”
"In short, we engineer the system to mathematically enforce our prior assumptions, since no government or organisation can reasonably be trusted."
Web3 is Sovereignty in Cyberspace

Cryptography is Authority in Cyberspace
State of Web3

- Zealous conviction in tokenization/financialization of all assets
- Prioritization of financial prosperity over Web3’s core tenants
- Dwindling interest in enterprise use-cases
- Limited throughput contends with unbounded blockspace demand
Decentralized Finance “Lost the Plot”

- Cryptocurrency is seen as a mechanism for profit rather than financial agency
- Capital allocation focused on chasing gains over innovation
- Receding decentralization due to increased government ire
Can We Break Web3 Out of DeFi?

Cue Zero Knowledge Cryptography...
Semaphore

Anonymous Social Coordination?
ZK Proofs of KYC/AML Compliance?
That’s up to you…

Semaphore Community Grant
Round Ends October 28th, 2022

https://esp.ethereum.foundation/semaphore-grants
The Growth of Zero Knowledge Cryptography

1985
First ZK Proof (Goldwasser, Micali, Rackoff)

2013
First zkSNARK
Pinocchio
TinyRAM (First ZK VM)

2016
Groth16
(First practical zkSNARK)

2018
First ZK-Rollup
Barry Whitehat
Circom (Iden3)
First zkSTARK
Starkware

2019
PLONK (AIR/RAP vs R1CS)

2020
StarkEx (Cairo ZK VM)
Halo 2 (ZCash)

2021
Mina (Snapps ZK VM)
Circom 2.0 (Iden3)

2022
Plonky2 (100x faster than PLONK)
zkEVMs (Hermez, Scroll, zkSync)
ZPrize (XPrize for ZK)
Applying ZK Cryptography to the EVM

An Exploration of Privacy and Scalability on Ethereum
Domain-Specific Languages

- Scaling requires expertise
- Computation verified on L1
- Consensus from root Ethereum Network
- SDK abstracts as much ZK complexity as it can
- ZK circuit/ proof agnostic to underlying chain

Virtual Machines In ZK

- Highly scalable with no effort
- Computation verified on L2
- Separate security/ validator set from root Ethereum network
- VM Language built specifically abstracted for ZK dev paradigm
- Vendor lock-in risk*
Circom

2022 Gold Standard
For ZK DSL's
Jumpstart Your Circom Dev

https://battlezips.com/resources
Circom Topics

Powers of Tau, Groth16 vs PLONK
Multiplexing to Evaluate Conditionals
Circuit-friendly Hashing & Signing
Merkle Trees
First and Third Party Dev Tooling
Implementation Demonstration
BattleZips Road Map

V1 (Feb 2022)
- Private state on public EVM
- No focus on scalability
- Intermediate state is public (even though ships are private)

V2 (EoY 2022)
- State generation & consensus off-chain (state channel)
- ZK-shielded summary of State Channels roll up full game in one on-chain tx
- Intermediate state is shielded
- ZK ELO Score demo

Maturity (2023)
- “Zips” zk state channel pattern
- Application to real-world use cases
- Exploration of multiple layers of Zips
BattleZips V2

State Channel ZK Receipt/ Summary

Generic Proof Types & Their Application

Proof of a Valid Battleship Game where Alice won and Bob lost

Proof of a Valid Delivery (IoT sensors + chain of custody maintained)

Proof of a vote on PROPOSAL where X% of participants ratified the proposal

Uses zcash/halo2 instead of iden3/circom for recursion
Thank you!

BattleZips
Please contact us if you want help starting your ZK Dev journey - we are just paying it forward!

@jp4g_  
@brightir2025
Education across Cultures

Panelists
Camila
Women Build Web3
Divyanshu
Devfolio
Ulaş
ITU Blockchain
Yan
Dapp Learning

Moderator
Luka
EF
Thank you for joining us at Grantee Day!