EF's Bug Bounty Program

The past, the present and the future

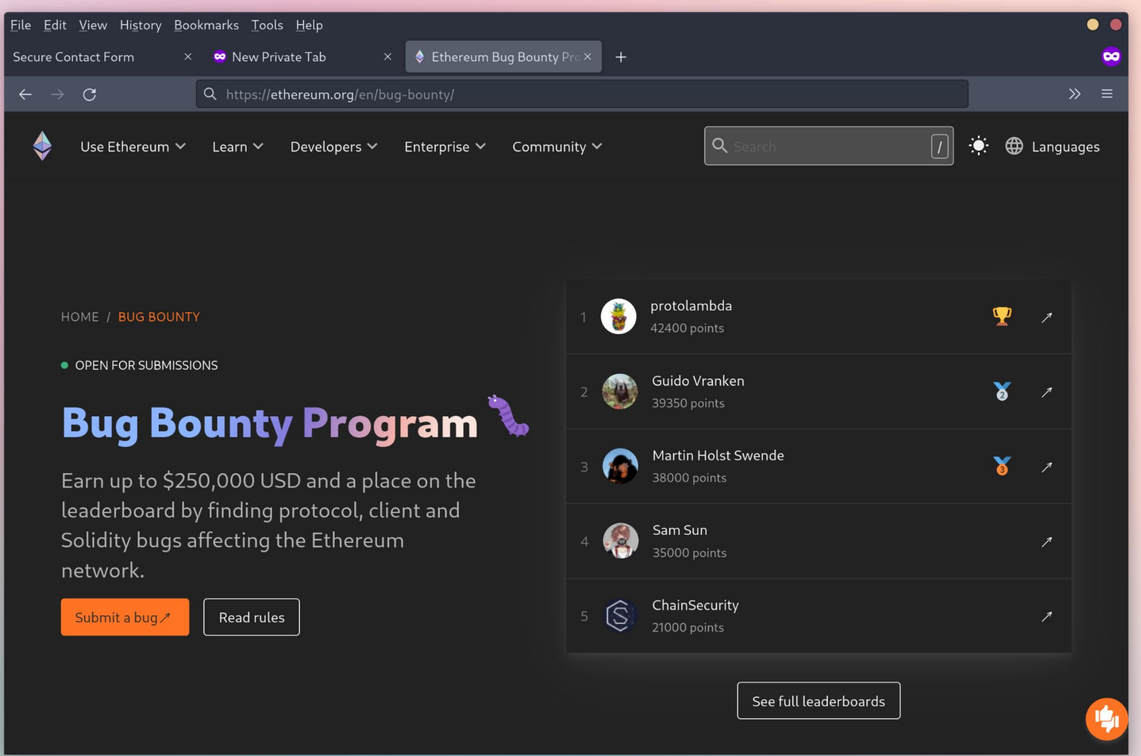
Fredrik Svantes

Security Research, Ethereum Foundation

What is it?

Bug Bounty Program

- Let’s start with the basics
- What’s in scope
- BBPaaS vs. In-house
- https://bounty.ethereum.org

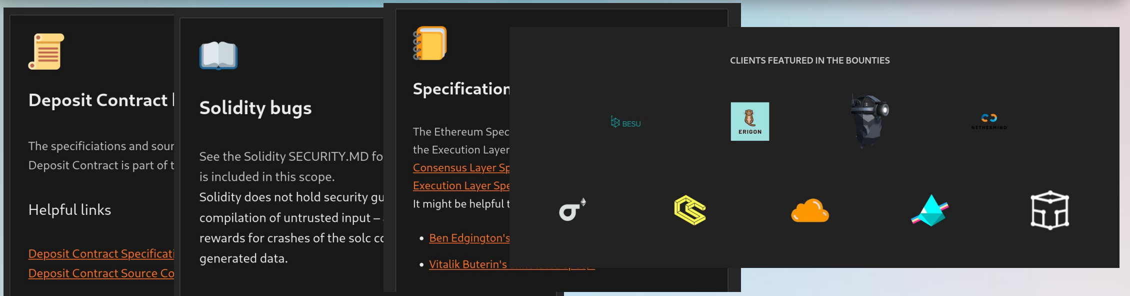


● OPEN FOR SUBMISSIONS

Bug Bounty Program

Earn up to $250,000 USD and a place on the leaderboard by finding protocol, client and Solidity bugs affecting the Ethereum network.

1	protolambda	42400 points
2	Guido Vranken	39350 points
3	Martin Holst Swende	38000 points
4	Sam Sun	35000 points
5	ChainSecurity	21000 points



Deposit Contract

The specificiations and sour
Deposit Contract is part of t

Helpful links

Deposit Contract Specificati
Deposit Contract Source Co

Solidity bugs

See the Solidity SECURITY.MD fo
is included in this scope.
Solidity does not hold security gu
compilation of untrusted input –
rewards for crashes of the solc cc
generated data.

Specification

The Ethereum Spec
the Execution Layer
Consensus Layer Sp
Execution Layer Spe
It might be helpful t

- Ben Edgington's
- Vitalik Buterin's

CLIENTS FEATURED IN THE BOUNTIES

The Past

History

2015

Launch of the Ethereum Foundation Bug Bounty Program.

Max Reward: 5 BTC for consensus issues (~$1500)

2020

CL Program started

Max Reward: $25/50,000 (x2)

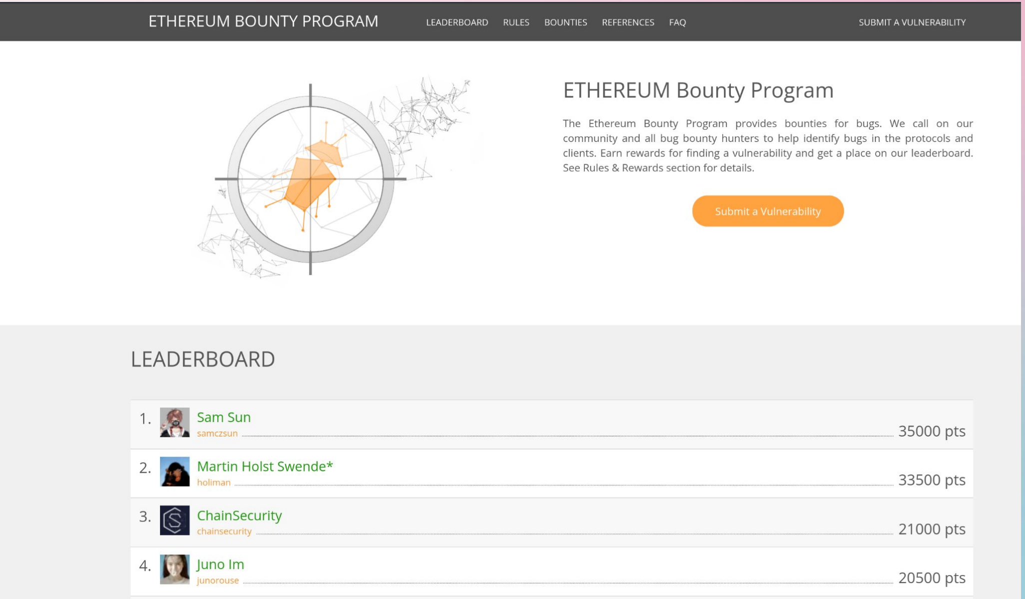
2022

Merge of the two bounty programs.

Max Reward: $250,000 ($1 Million for Merge Related issues)

Ethereum Bounty Program

- Submit via email (PGP)



ETHEREUM Bounty Program

The Ethereum Bounty Program provides bounties for bugs. We call on our community and all bug bounty hunters to help identify bugs in the protocols and clients. Earn rewards for finding a vulnerability and get a place on our leaderboard. See Rules & Rewards section for details.

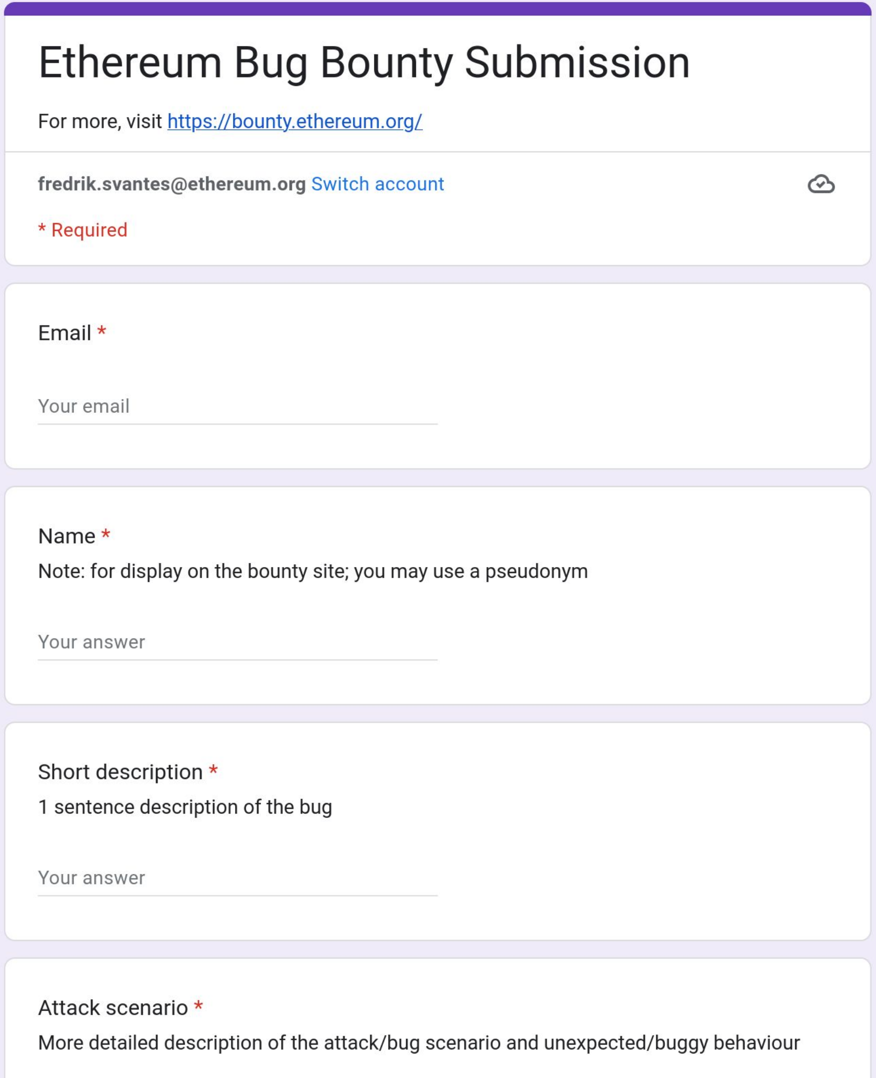
LEADERBOARD

1.	Sam Sun samczsun	35000 pts
2.	Martin Holst Swende* holiman	33500 pts
3.	ChainSecurity chainsecurity	21000 pts
4.	Juno Im junorouse	20500 pts

The Present

Submissions

- Sent via Google forms or Email (PGP)



Ethereum Bug Bounty Submission

For more, visit https://bounty.ethereum.org/

fredrik.svantes@ethereum.org Switch account

* Required

Email *

Your email

Name *

Note: for display on the bounty site; you may use a pseudonym

Your answer

Short description *

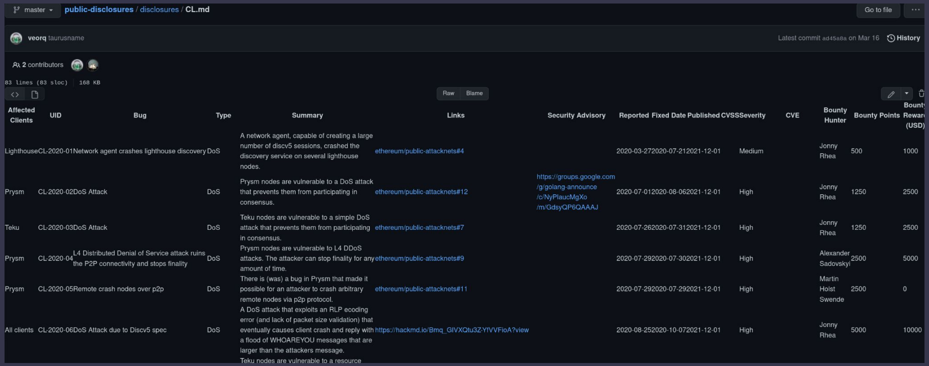
1 sentence description of the bug

Your answer

Attack scenario *

More detailed description of the attack/bug scenario and unexpected/buggy behaviour

200+ vulnerabilities reported and fixed.



master public-disclosures / disclosures / CL.md

veorq taurusname   Latest commit ad45a8a on Mar 16   History

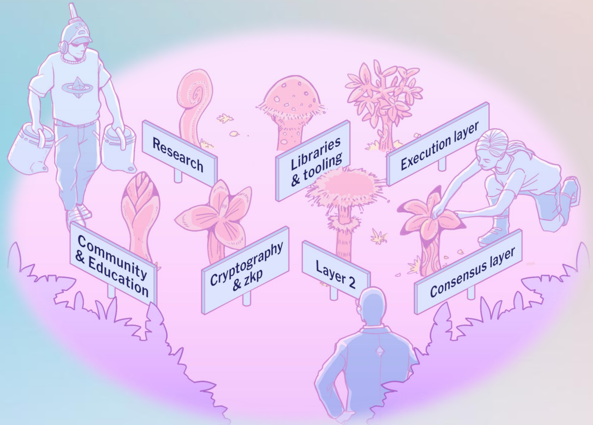
2 contributors

83 lines (83 sloc) | 168 KB

Affected Clients	UID	Bug	Type	Summary	Links	Security Advisory	Reported	Fixed Date	Published	CVSS	Severity	CVE	Bounty Hunter	Bounty Points	Bounty Rewar (USD)
Lighthouse	CL-2020-01	Network agent crashes lighthouse discovery	DoS	A network agent, capable of creating a large number of discv5 sessions, crashed the discovery service on several lighthouse nodes.	ethereum/public-attacknets#4		2020-03-27	2020-07-21	2021-12-01		Medium		Jonny Rhea	500	1000
Prysm	CL-2020-02	DoS Attack	DoS	Prysm nodes are vulnerable to a DoS attack that prevents them from participating in consensus.	ethereum/public-attacknets#12	https://groups.google.com/g/golang-announce/c/NyPlaucMgXo/m/GdsyQP6QAAAJ	2020-07-01	2020-08-06	2021-12-01		High		Jonny Rhea	1250	2500
Teku	CL-2020-03	DoS Attack	DoS	Teku nodes are vulnerable to a simple DoS attack that prevents them from participating in consensus.	ethereum/public-attacknets#7		2020-07-26	2020-07-31	2021-12-01		High		Jonny Rhea	1250	2500
Prysm	CL-2020-04	L4 Distributed Denial of Service attack ruins the P2P connectivity and stops finality	DoS	Prysm nodes are vulnerable to L4 DDoS attacks. The attacker can stop finality for any amount of time.	ethereum/public-attacknets#9		2020-07-29	2020-07-30	2021-12-01		High		Alexander Sadovskyi	2500	5000
Prysm	CL-2020-05	Remote crash nodes over p2p	DoS	There is (was) a bug in Prysm that made it possible for an attacker to crash arbitrary remote nodes via p2p protocol.	ethereum/public-attacknets#11		2020-07-29	2020-07-29	2021-12-01		High		Martin Holst Swende	2500	0
All clients	CL-2020-06	DoS Attack due to Discv5 spec	DoS	A DoS attack that exploits an RLP ecoding error (and lack of packet size validation) that eventually causes client crash and reply with a flood of WHOAREYOU messages that are larger than the attackers message.	https://hackmd.io/Bmq_GIVXQtu3Z-YfVVFioA?view		2020-08-25	2020-10-07	2021-12-01		High		Jonny Rhea	5000	10000
				Teku nodes are vulnerable to a resource											

Public Disclosures

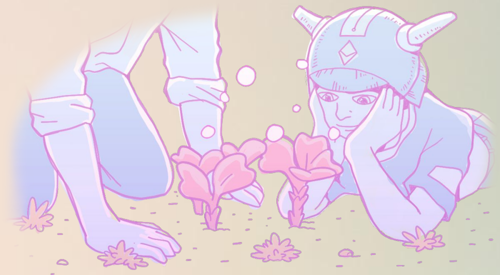
https://github.com/ethereum/public-disclosures/

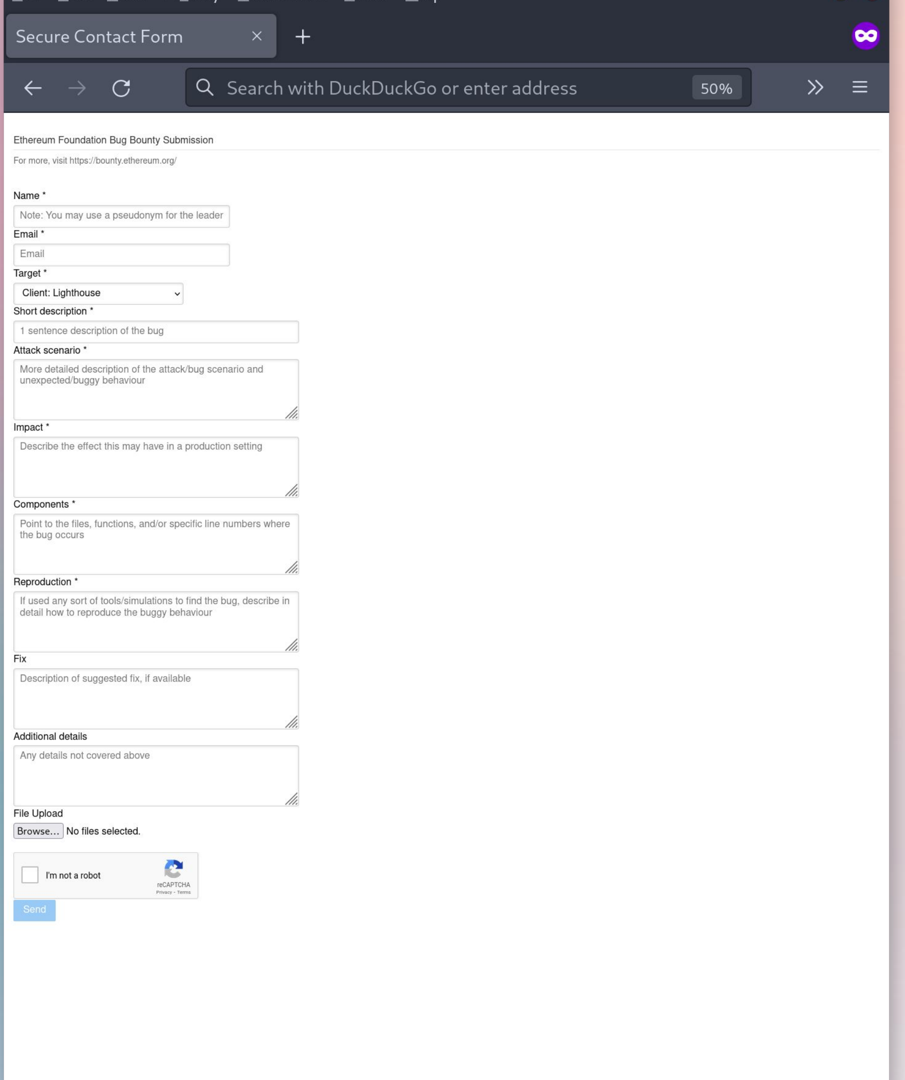


The Future

Secure Submission Form

- Client side encryption in browser
- OpenPGP.js
- Modular
- Small server side app handling transfer of data to destinations
- Soon™ available in a public repository





Ethereum Foundation Bug Bounty Submission

For more, visit https://bounty.ethereum.org/

Name *
Note: You may use a pseudonym for the leader

Email *
Email

Target *
Client: Lighthouse

Short description *
1 sentence description of the bug

Attack scenario *
More detailed description of the attack/bug scenario and unexpected/buggy behaviour

Impact *
Describe the effect this may have in a production setting

Components *
Point to the files, functions, and/or specific line numbers where the bug occurs

Reproduction *
If used any sort of tools/simulations to find the bug, describe in detail how to reproduce the buggy behaviour

Fix
Description of suggested fix, if available

Additional details
Any details not covered above

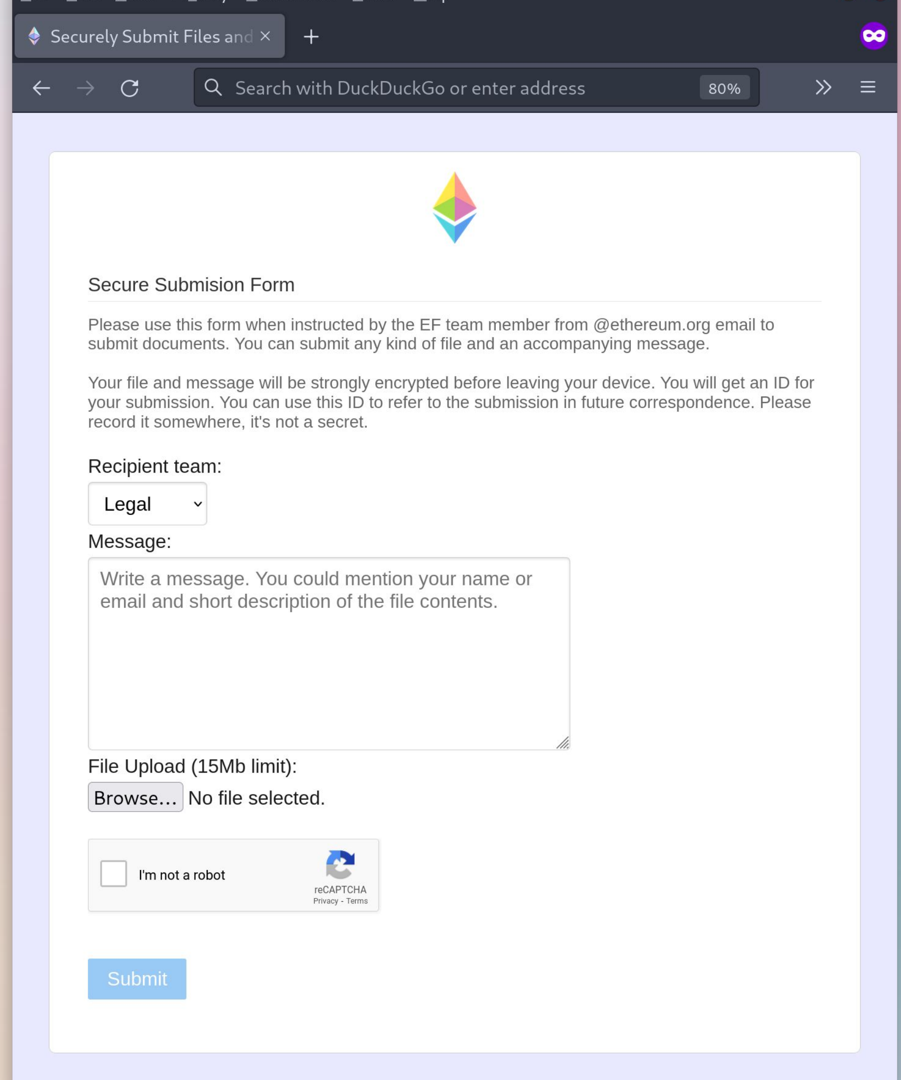
File Upload
Browse... No files selected.

□ I'm not a robot
reCAPTCHA
Privacy - Terms

Send

Secure Drop

- Built on Secure Submission Form
- Easy way for users to submit data that must be kept confidential
- Available at https://github.com/ethereum/secure-drop/


Securely Submit Files and
Search with DuckDuckGo or enter address
80%

Secure Submission Form

Please use this form when instructed by the EF team member from @ethereum.org email to submit documents. You can submit any kind of file and an accompanying message.

Your file and message will be strongly encrypted before leaving your device. You will get an ID for your submission. You can use this ID to refer to the submission in future correspondence. Please record it somewhere, it's not a secret.

Recipient team:

Legal

Message:

Write a message. You could mention your name or email and short description of the file contents.

File Upload (15Mb limit):

Browse... No file selected.

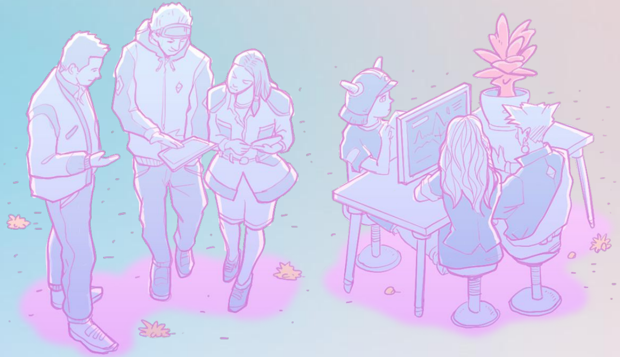
□ I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

Looking ahead

- Encrypted vulnerability lifecycle system
- Additional incentives for bounty hunters
  - Remix Team



Thank you!

Fredrik Svantes

Security Researcher, Ethereum Foundation

fredrik@ethereum.org

@fredriksvantes