MEV Roast- Privacy

Date: 2023-01-11T16:00:00Z

Start: 11:00am ET / 8:00am PT / 4:00pm UTC / 12:00am China Standard Time

Estimated runtime: approximately 2.5 hours

Roast master: Justin Drake (Ethereum Foundation)

Event type: virtual, Zoom link, Meeting ID: 246 680 5965

MEV Roasts were a monthly tradition from the MEV Pi-rate Ship. You can see a past MEV Roast agenda here. Flashbots Research plans to bring back occasional roasts, and we will start on January 11th with a MEV Roast on privacy. For each roast we invite researchers to present insights from MEV-related research they are working on or interesting early stage proposals for community feedback.

Stream: (MEV Roast - Privacy | January 11th, 2023 - YouTube) / Link to join (Launch Meeting - Zoom)

Pt 0: Introduction & Memes

Pt 1: Why and Where- Why and where do we want privacy?

In MEV markets, a user's information is valuable. Supporting privacy for users in MEV means empowering them and shielding them from value extraction due to information asymmetry. Are there additional motivations to protect privacy? Also, privacy is differently impactful depending where it is protected within the transaction supply chain stack. In which areas should privacy be protected? Where may privacy be undesirable?

- Why Privacy in MEV
- Quintus Kilbourn (Flashbots)- Slides
- Privacy Tradeoffs
- Phil Daian (Flashbots)- Slides

Pt 2: How- How can we provide privacy?

For each part of the transaction supply chain, privacy can be offered with different techniques making different trust assumptions. Which privacy-preserving tools best serve our needs, and what are the best practices for their use? What are the limitations of current privacy-preserving techniques?

- Encrypted Mempools
- Justin Drake (Ethereum Foundation)- Slides
- TEE Smart Contracts: Pitfalls and Best Practices
- Andrew Miller (UIUC)- Slides
- Private Searching on Private Transactions: From Covert Channels in SGX to MPC (and Back to SGX?)
- Robert Annessi (Flashbots)- Slides
- Minimizing MEV on Penumbra
- Henry de Valence (Penumbra)- Slides
- The Joys and Challenges of Adopting PETs - Present and Future Applications of Privacy Enhancing Techs at Flashbots
- Jonathan Passerat-Palmbach (Flashbots)- Slides
- Spicy SGX Panel

(Moderated by Justin Drake; Panelists Andrew Miller, Jonathan Passerat-Palmbach, Phil Daian)

Roast panel questions from the Roast Master (with purposefully abrasive language to fit the "roast" theme

):

• Intel has deprecated SGX on consumer CPUs. What if Intel fully deprecates SGX in 2023?

• MEV is in large part about low latency. How can SGX be competitive on latency?

• SGX is known for being leaky. Is SGX suitable for mempool privacy?

• SGX has a terrible reputation. Isn’t this a massive headwind for adoption?

• What if an unpatchable critical SGX vulnerability is discovered after the launch of SUAVE?

We will update this post to include the slides used once they are available.

Please reply to this thread if you have suggestions for this agenda and want to participate in the creation of this event.