Enhancing Censorship Resistance in Ethereum's World Computer

Patrick Spiesberger [1]

Abstract: This talk is about censorship resistance within the Ethereum network [1], focusing on mechanisms at both the consensus and network layers. At the consensus layer, we examined how block builders influence transaction inclusion, which can result in delays or exclusions of code execution, particularly for state-sanctioned addresses. We analyzed *Protocol-Enforced Proposer Commitments (PEPC)* [7, 3] and introduced a slightly modified approach: *Protocol-Enforced Requirements (PER)*. This includes the *Anti-Censorship Requirement*, which leverages economic disincentives to make censorship more costly. At the network layer, we plan to investigate encrypted transaction forwarding as a potential method for preventing content-based censorship. While promising, this approach faces challenges such as timeliness and the risk of participant collusion. We intend to explore how combining encrypted transactions with the anti-censorship requirement could address these issues, aiming to ensure both timely inclusion and stronger censorship resistance.

Introduction The collection and processing of digital data are fundamental in many sectors, especially in critical infrastructure services (KRITIS) [5], which are essential for public safety, economic stability, and daily life. Traditional centralized systems, such as local servers and large data centers, depend heavily on trust in operators and security measures. Despite strong cybersecurity measures, these systems remain vulnerable to physical disruptions, as demonstrated by the OVH data center fire [6]. While backups provide redundancy, they also create trust dependencies due to the need for secure and consistent maintenance. Decentralized Peer-to-Peer (P2P) networks offer an alternative by enabling direct communication between nodes. The use of Replicated State Machines (RSMs) in P2P networks supports the execution of code without a single point of failure. While decentralized networks reduce trust dependencies, they are still susceptible to censorship at both the consensus and network layers, which can undermine their reliability.

Consensus Layer Censorship Resistance In Ethereum, transactions are the input of the RSM, also known as the World Computer. However, the inclusion of these transactions in a block is not guaranteed, as block builders control which transactions are included in a block. This creates a potential for censorship, where certain transactions are delayed or excluded entirely by one partie. This issue is particularly evident with transactions related to addresses flagged by the U.S. Office of Foreign Assets Control (OFAC) [11], which experience delays averaging 2.8 times longer than non-flagged transactions [9].

[1] Karlsruhe Institute of Technology, Decentralized Systems and Network Services, Karlsruhe, Germany, patrick@spiesberger.info, https://orcid.org/0009-0006-4746-8868

To address this challenge, *Forward Inclusion Lists* [4] mandate the inclusion of certain transactions in the next block, but they do not eliminate all censorship risks. *PEPC* strengthen this approach by requiring binding agreements between proposers and builders regarding block contents, which helps prevent selective exclusion. We extended PEPC with *PER*, which allows the applicant as well as the block builder and block proposer to express requirements in-protocol. Further enhancing censorship resistance, we introduced the *Anti-Censorship Requirement*, which significantly increases the cost of censorship by necessitating that an attacker compromises at least 156 times more entities compared to scenarios without this requirement. The estimated cost of such censorship is 1.08 Ether every 12 seconds, making it economically unfeasible in most practical scenarios.

Network Layer Censorship Resistance At the network layer, censorship occurs when malicious nodes selectively block or delay transaction propagation based on transaction content. This prevents certain transactions from being included in blocks and, accordingly, processing by the world computer. One possible solution is the encryption of transactions, where the content of a transaction remains hidden until it is included in a block by the block proposer [8, 10]. This prevents content-based censorship by making it impossible for nodes to selectively block transactions based on their content. However, encrypted transaction propagation faces significant challenges, particularly in terms of **timeliness** and the **collusion** between network participants [2]. If malicious nodes and block publisher cooperate, content-based censorship can still take place cost-effectively.

We aim to explore whether integrating encrypted transactions into the Anti-Censorship Requirement can effectively address these two challenges. The core idea is to move away from a purely temporal encryption mechanism — where transaction data becomes visible only at a specific time — and instead bind decryption directly to Anti-Censorship Requirements. In this approach, transactions would remain encrypted during propagation but would be decrypted by the block publisher before inclusion in a block. Crucially, this decryption would obligate the block publisher to include the transaction. Failing to do so would render the published block invalid.

References

[1] Vitalik Buterin. “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”. In: *Ethereum White Paper* (2013).

[2] Arka Rai Choudhuri et al. *Practical Mempool Privacy via One-time Setup Batched Threshold Encryption*. Cryptology ePrint Archive, Paper 2024/1516. 2024. URL: https://eprint.iacr.org/2024/1516.

[3] Diego Estevez. *Commitment-Satisfaction Committees: An In-Protocol Solution to PEPC*. [Online; accessed on November 06, 2024]. Oct. 2023. URL: https://ethresear.ch/t/commitment-satisfaction-committees-an-in-protocol-solution-to-pepc/17055.

[4] Ethereum Foundation. *EIP-7547: Inclusion Lists*. https://eips.ethereum.org/EIPS/eip-7547. [Online; accessed on October 21, 2024]. 2024.

[5] Federal Office for Information Security (Germany). *What are Critical Infrastructures?* [Online; accessed on October 18, 2024]. 2024. URL: https://www.bsi.bund.de/EN/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html.

[6] Peter Judge. *OVHcloud’s data center fire: One year on, what do we know?* [Online; accessed on October 18, 2024]. 2022. URL: https://www.datacenterdynamics.com/en/opinions/ovhclouds-data-center-fire-one-year-on-what-do-we-know/.

[7] Barnabé Monnot. *Unbundling PBS: Towards Protocol-Enforced Proposer Commitments (PEPC)*. [Online; accessed on October 11, 2024]. Oct. 2022. URL: https://ethresear.ch/t/unbundling-pbs-towards-protocol-enforced-proposer-commitments-pepc/13879.

[8] Antoine Rondelet and Quintus Kilbourn. “Mempool Privacy: An Economic Perspective”. In: July 2023. DOI: 10.48550/arXiv.2307.10878.

[9] Soispoke. *Estimating inclusion delays for censored transactions*. https://ethresear.ch/t/estimating-inclusion-delays-for-censored-transactions/15115. [Online; accessed on October 22, 2024]. 2023.

[10] James Stearn. *Cryptographic Approaches to Complete Mempool Privacy*. 2022.

[11] U.S. Department of the Treasury. *Office of Foreign Assets Control - Sanctions Programs and Information*. [Online; accessed on October 21, 2024]. 2023. URL: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.