This document is an early draft of an unfinished idea; feedback is appreciated.

Emerald: A Decentralized Imageboard Protocol

Alexander Sellström
alexander@sellstrom.me
May 27, 2025

Abstract

This paper introduces a novel protocol for peer-to-peer social media platforms, leveraging blockchain technology to address limitations of existing social media, such as censorship and privacy concerns. Imageboards are identified as uniquely suitable for such decentralized applications due to their inherently bounded storage requirements. Key technical challenges in developing these applications include content storage, distribution, retrieval, and the design of effective incentive mechanisms for network participants. The proposed protocol, Emerald, combines content-addressable networks and blockchain to establish a secure, scalable, and censorship-resistant platform specifically for imageboards.

1 Introduction

The advent of mainstream social media platforms has brought about a revolution in communication, connecting billions of people worldwide and enabling unprecedented levels of information sharing and social interaction. However, these platforms have also given rise to a host of social challenges. Centralized platforms have wielded significant power over the flow of information, raising concerns about censorship, privacy breaches, and the legal responsibilities of these platforms. Moreover, centralized architectures introduce technical constraints and vulnerabilities, such as single points of failure and susceptibility to various cyberattacks.

In response to the limitations of centralized social media, there is a burgeoning movement toward decentralized social media platforms. These platforms aim to address the shortcomings of their centralized counterparts by distributing control and infrastructure across a peer-to-peer network. By empowering users and communities to govern their own digital spaces, decentralized platforms hold the promise of fostering greater freedom of expression, privacy, and resilience against censorship.

However, the transition to decentralized social media is not without its own set of challenges. Scalability and performance are two key areas where decentralized platforms often struggle to match the user experience offered by centralized alternatives. The protocols powering these decentralized solutions must grapple with the technical complexities of efficiently routing content and managing distributed storage across a network of nodes.

Many blockchain-based projects [1, 2] have emerged as a promising alternative. However, these solutions often lack adequate incentives for nodes to reliably distribute content to end-users, resulting in performance issues. In addition, these protocols are plagued by frustratingly poor performance; their reliance on Distributed Hash Tables (DHTs) for content discovery frequently results in lookup delays of several minutes, rendering such systems practically unusable for dynamic content. To address these shortcomings, some platforms have opted to integrate centralized gateways to facilitate content delivery, reintroducing the very issues that decentralization sought to eliminate, such as single points of failure and control.

Anonymity stands as a cornerstone feature of imageboards, serving as a safeguard against the suppression of free speech and providing protection against legal repercussions for illicit expressions. The blockchain domain has seen the development of protocols such as Zcash [3], which leverages zero-knowledge cryptography, and Monero [4], which employs distinct advanced cryptographic methods like ring signatures and stealth addresses, both aiming to ensure transactional anonymity. Similarly, the Waku messaging protocol employs zero-knowledge cryptography to maintain user anonymity and implement rate limiting. The potential application of such cryptographic advancements to anonymous forums is an area ripe for exploration, with the possibility of enhancing privacy and freedom of expression in the digital realm.

2 Decentralized Storage

One of the main challenges of blockchain technology is scalability. Due to the limited block size and the requirement for all nodes to process all transactions, it is best to store and deliver larger amounts of data using specialized decentralized storage protocols and only store hashes of files on the blockchain. This also reduces the cost of storing data, as on-chain storage is typically much more expensive than off-chain storage.

One such protocol is the InterPlanetary File System (IPFS) [5], a peer-to-peer hypermedia protocol designed to make the web faster, safer, and more open. Content-addressable storage means that data is identified by its content rather than its location, using a unique identifier called a Content Identifier (CID). IPFS uses a Distributed Hash Table (DHT) to store and lookup CIDs and their corresponding network addresses, enabling the routing and discovery of data. A DHT lookup must be done for each file to be downloaded, which can take several minutes [citation needed]. This added latency makes for a jarring user experience. In addition, IPFS does not have a built-in incentive mechanism to encourage nodes to store and share data, which may limit its availability and reliability.

Other protocols, such as Swarm [6], aim to address some of these limitations. Swarm uses a content-addressable storage model similar to IPFS, but with some differences in how CIDs are generated and stored. Swarm also introduces an incentive system based on peer-to-peer accounting and payments to encourage nodes to store and share data. Swarm also offers features such as encryption, erasure coding, mutable resources, and feeds, which can enhance its functionality and usability. Despite these advantages, Swarm's reliance on its DHT for content discovery also results in significant lookup latency, often on a scale that, like IPFS, makes it ill-suited for highly dynamic content.

3 Imageboards

Imageboards are online platforms where users can post and discuss various topics anonymously. They are different from other types of forums or social media, as they do not require user registration, and do not store user profiles or histories. Imageboards are characterized by their topical boards, which focus on specific themes or interests, such as anime, video games, politics, hobbies, etc. Users can create new threads by uploading an image and adding a comment, and other users can reply with images or text.

Imageboards have a finite number of threads that can be active simultaneously. When a user creates a new thread, the thread that has been inactive the longest is deleted. This deletion mechanism makes imageboards dynamic and transient in nature, but also limits the storage requirements compared to most other types of social media. With such modest storage requirements, ranging from tens to a couple hundred gibibytes, an entire board could easily fit on a single node in a peer-to-peer network. Node storage and bandwidth requirements can be further reduced with a sharded network architecture, allowing resource-restricted devices, such as smartphones, to participate in the network.

4 General Structure

On Emerald, service providers (back-end servers) can be consumer-grade devices such as desktops, laptops, or even smartphones belonging to any private person, as opposed to a corporate data center. The blockchain only stores the hashes of the media posted on Emerald due to bandwidth constraints inherent to blockchain consensus algorithms. The media itself is stored by the service provider nodes that make the content available to end-users for a small fee.

Emerald differentiates itself from most other blockchain projects in that it has an application-specific blockchain. Other blockchains are often general-purpose blockchains that allow smart contracts to be deployed on-chain, enabling all kinds of decentralized applications to be built on top of them. Smart contracts increase complexity and attack surface, which can expose users to risks such as fraudulent or buggy smart contracts. Transaction fees for using applications on general-purpose blockchains are also subject to sudden increases caused by a surge in the use of a completely unrelated application.

Emerald also differentiates itself from decentralized (federated) platforms like Nostr, Bluesky, and Mastodon, in that the content is globally consistent (*logically* centralized) across all service nodes/servers. The shortcomings of federated protocols boil down to the fact that each individual server is sovereign and essentially centralized, and therefore inherits many of the problems of traditionally centralized networks. Blockchain technology also enables the creation of an incentive layer that compensates nodes that help support the network, and a disincentive layer to deter any would-be malicious nodes.

5 Content Storage

Emerald's data distribution protocol differs from IPFS by not requiring a Distributed Hash Table (DHT) to locate specific data items. Instead, it employs a sharded architecture. Each imageboard can be divided into multiple shards, and node operators may choose to join specific shards, thereby committing to store and distribute the data relevant to those portions of a board. Within a given shard, all participating nodes are expected to eventually hold and distribute all of that shard's data, operating much like a BitTorrent swarm. This full replication within the shard means that once a node is part of a shard's swarm, it obtains data from its peers without needing DHT lookups for individual content items. (Mechanisms for discovering peers to join a shard's swarm are a distinct aspect of the protocol and could potentially utilize a DHT).

A defining characteristic of Imageboards is that threads are pruned when new ones are created. A limit on the maximum number of active threads allows for very modest storage space requirements in the range of 50-150 gibibytes for one board. The rationale behind sharding is to reduce the hardware and bandwidth requirements for individual nodes, thereby making it easier for users to participate in the network by supporting only specific boards or parts thereof. This approach can also allow resource-restricted devices, such as smartphones, to contribute to the network. This selective participation in shards also means that node operators can effectively opt out of hosting content from boards they deem objectionable by choosing not to join those respective swarms.

6 Post Finality

When making a post, the author first submits their post's Content Identifier (CID) to the blockchain, where it is held in a ring buffer (functioning like a mempool) pending finality. Once the CID is in this buffer, the author—already connected to the relevant shards to view and interact with the board (either through their own nodes or via service providers)—can start to broadcast the post's data to their peers within these shards. Peers verify that the received data pieces correspond to the on-chain CID using a Merkle proof. Upon receiving

a complete piece of data, nodes within the shard further distribute it to their own peers, mirroring the data propagation dynamics of a BitTorrent swarm.

After allowing sufficient time for this peer-to-peer propagation, a designated set of blockchain validators, acting as data availability attesters and randomly assigned to specific shards for this duty, will vote on the data's availability using a commit-reveal scheme. If these attestations surpass a predefined threshold, the data is deemed available. The post is then finalized, with its CID being formally moved from the ring buffer to the target thread on the imageboard.

7 Service Contracts

Users who cannot or are unwilling to run their own nodes can enter into a service contract with some nodes to use the network. Service contracts utilize a payment channel to perform many off-chain transactions, allowing the client to continuously pay the node for the services rendered. Such a contract could, for example, require the client to pay a very small sum every second or for every megabyte received. If either party stops upholding their end of the contract, the other can simply terminate the connection.

When interacting with other blockchains like Ethereum, users who cannot run their own node must typically rely on centralized API services. This defeats much of the purpose of using a decentralized network like Ethereum. In August 2022, the US Treasury put a ban on the Tornado Cash smart contract on Ethereum. This caused US-based Ethereum API service providers such as Infura to block users around the world from using it. Such censorship would not work very well on Emerald, since the user's client can simply rent a new service node if one starts acting up.

8 Decentralized Moderation

A complete lack of moderation is unlikely to result in a usable board, but appointing administrators with absolute authority to silence users reintroduces the very same problems inherent to centralized platforms that Emerald is supposed to solve. A solution to this would be to have a permissionless judiciary, similar to Kleros Moderate[7], and other Oracle protocols.

Users willing to help moderate and earn tokens can stake their tokens to become jurors. Jurors vote on whether reported posts comply with the board's established guidelines. The voting process employs a commit-reveal scheme to deter voters from merely echoing the apparent majority. If a post is judged to violate guidelines and is marked for deletion, service nodes are no longer required to serve that content. Jurors who vote contrary to the case's established consensus may face slashing of their stake, whereas those voting with the consensus are rewarded.

Scalability presents a challenge as the number of jurors or reports grows. For juror scalability, one option is to allow only the top N stakers to vote, similar to some proof-of-stake mechanisms; however, a more decentralized approach involves pseudo-randomly selecting jurors for each case from the global pool of all staked jurors. The seed for this selection can be a globally deterministic value, such as a recent block hash. This random selection from a large, common pool provides robust economic security for individual juries: An attacker would need to control a substantial fraction of the total tokens staked globally to have a significant chance of corrupting a specific jury's decision.

To handle a high volume of reports, multiple juries can operate in parallel. This parallel execution of moderation tasks benefits from the shared economic security of the entire system, analogous to how Polkadot[8] achieves scalability with its parachains sharing the security of the Relay Chain. Furthermore, an escalation mechanism can enhance robustness: cases where an initial jury reaches only a weak consensus could be escalated to a larger, potentially randomly selected, panel of jurors, or even the entire juror pool for a final binding decision. This tiered approach is also reminiscent of the dispute resolution pathways seen in systems like Polkadot's ELVES protocol[9].

9 Rate Limiting Nullifier

A defining characteristic of imageboards is that all users are anonymous and do not have accounts. If users use the same identity for many posts, they may end up "doxing" themselves. Simply generating a new key pair and transferring the tokens to the new address would leave an obvious paper trail leading back to the original one. A solution to this is to use a rate-limiting nullifier[10] in place of a transaction fee. This introduces numerous other challenges, such as transaction ordering and accountability. The suitability of rate-limiting nullifiers must be explored further.

References

[1] A. Labs, "Frequency," accessed: 2024-03-31. [Online]. Available: https://www.frequency.xyz/

[2] Subsocial, "Subsocial," accessed: 2024-03-31. [Online]. Available: https://subsocial.network/

[3] D. Team, "Dat protocol," accessed: 2023-11-24. [Online]. Available: https://dat-ecosystem.org/

[4] M. C. T. Nicolas van Saberhagen, "Monero," accessed: 2023-12-14. [Online]. Available: https://www.getmonero.org/

[5] P. Labs, "IPFS," accessed: 2023-11-24. [Online]. Available: https://ipfs.tech/

[6] S. Foundation, "Swarm," accessed: 2023-11-24. [Online]. Available: https://www.ethswarm.org/

[7] C. Kleros, "Kleros moderate," accessed: 2025-05-25. [Online]. Available: https://kleros.io/moderate

[8] W. Foundation, "Polkadot," accessed: 2025-05-25. [Online]. Available: https://polkadot.com/

[9] J. Burdges, A. Cevallos, H. K. Alper, C.-D. Liu-Zhang, F. Shirazi, A. Stewart, R. Habermeier, R. Klotzner, and A. Ordian, "Efficient execution auditing for blockchains under byzantine assumptions," *Cryptology ePrint Archive*, 2024, accessed: 2025-05-27. [Online]. Available: https://eprint.iacr.org/2024/961

[10] A. Revuelta, S. Tikhomirov, A. Challani, H. Cornelius, and S. P. Vivier, "Message latency in waku relay with rate limiting nullifiers," Cryptology ePrint Archive, Paper 2024/1073, 2024. [Online]. Available: https://eprint.iacr.org/2024/1073