Semaphore

Social media users are often unsatisfied by existing platforms, which are generally non-responsive to user preferences. The accrual of network effects to specific platforms means that unwanted decisions can be made by platform owners, leaving users with little recourse. We propose a new type of blockchain network, which we call Semaphore, to solve this problem by relocating network effects to a decentralized layer below social apps.

*

Availability of quality content is what attracts users to social media platforms, and availability of quality content on a social media platform is driven by the number of users generating content. The result is a feedback loop that drives users to a particular platform. Metcalf's law suggests that the value of a platform grows in proportion to the square of the number of users. As more users join a particular platform, the value of joining the platform and the cost of leaving the platform both increase. This externality associated with the volume of users participating on the platform is an example of a network effect. With current approaches, every platform accrues its own siloed network effects because each platform has its own infrastructure that makes different platforms non-interoperable. New users are consequently incentivized to choose the most popular platform within a given area because more users on the platform implies more total value from available content. Switching from one platform to another at a later date is costly because the benefits of network effects associated with the initial choice are lost. Because network effects are tied to specific platforms, in general a single platform will eventually obtain near-monopoly status in its area of focus, as the value associated with joining the dominant platform drives an increasing fraction of new users to that platform.

A primary implication of dominant social media applications operating as quasi-monopolies is that user preferences often play a negligible role in the development of the platform because the network effects associated with the platform typically prevent users from leaving the platform. Consequently, there is little user choice in social media platforms and as a result these platforms are able to engage in behaviors actively contrary to the users' interests with relatively little fear of losing meaningful levels of users. For example, social media platforms currently collect large amounts of personal data with relatively little user control over how that data is used, compel users to accept unwanted changes to the platform, recommend content using algorithms that focus on maximum exposure to ads instead of providing efficient access to desired content, and implement moderation policies that upset users both for being too strict and too lenient. These issues and many more undesirable behaviors are a consequence of the reduced user choice caused by network effects accruing to individual platforms.

These issues can be resolved only by breaking the link between platforms and network effects, thereby aligning the incentives of platforms with the desires of users. Decentralization can allow a system to operate smoothly without any single actor controlling its operation. However, a "decentralized social media app" or decentralized file storage does relatively little to resolve the issues associated with network effects. To break the link between social media platforms and network effects, a decentralized layer running below social apps is needed. The only practical way to achieve decentralization is a blockchain network that enables network participants to reach consensus on the state of the system. Additionally, a decentralized network effect layer allows users to make small posts, view the posts of others, and interact with other posts, such as by replying or liking. Higher level functionality can be enabled through social apps. By building on a decentralized layer, a social app can act as a custom front-end with assurance that all other apps remain composable and can access the same content. Apps built on this decentralized layer would not be able to "trap" users because network effects accrue to the decentralized layer rather than to the app itself. Such a system would promote competition between apps on the qualities that users value, such as privacy, content recommendation, user interface design, etc. If a user liked the features of another app better than the one they are currently using, switching would not harm the user's benefits from network effects because the same content would be available through both apps. Because apps could not rely on controlling network effects to keep users, apps would instead compete on offering the best service to users. Given the significant user dissatisfaction with existing social media platforms on many dimensions, it is likely that

introducing the possibility of competition between social apps as a consequence of relocating network effects would lead to innovations inducing new users to join social media altogether.

*

Systemic design choices made existing social media monopolistic. Similarly, existing blockchain solutions have not been able to be the foundation of a decentralized layer for network effects because their tradeoffs make them unsuitable for social apps. A new type of network is necessary. An understanding of the constraints of communication networks is necessary to understand the design space of alternative approaches. Communication networks operating at scale have three desirable properties, but only two are achievable at a time due to bandwidth, computation, and storage constraints.

- The first property is decentralization: The ability for an individual user to inexpensively receive and validate network activity without relying on a central party.
- Second is free broadcasting: The ability for an individual user to broadcast a message to the members of a network at trivial or zero cost.
- Third is free access: The ability for an individual user to be recognized as a participating member of the network and be guaranteed access to the functions of the network at trivial or zero cost.

The choice of which property to exclude yields three distinct types of networks. Type 1 networks, which lack decentralization, include existing social media platforms. For instance, it is free to make a Twitter account and free to send a tweet, but Twitter is not decentralized because it would be unmanageable for individual users to personally run twitter's servers or combat the large amounts of spam that would flood the network.

Existing blockchains are type 2 networks in which broadcasting is not free. For instance, Bitcoin is decentralized and a user can make effectively infinite wallets at no cost, but a fee must be paid to miners to have a broadcast accepted onto the blockchain. If Bitcoin was designed to eliminate miner fees, its blockchain would grow so large that individual users could not run a node, hurting decentralization.

Social media posts are valuable, but users have very low willingness to pay to broadcast social media messages. Users of a social app built on a type 2 network would have to outbid other users of the blockchain, who typically have some expected profit from broadcasting to the blockchain. Therefore, a social media app built on a type 2 network would require unpredictable fees to perform any action, leading to a reduction in content and a worse user experience. A decentralized network effect layer that supports social apps is therefore better suited to be a new, type 3 network in which decentralization and free broadcasting is achieved. By allocating blockspace with methods other than fees, these social applications become viable.

This is the Semaphore approach. To broadcast to the Semaphore network, a type 3 network, a user must own an alias, a non-fungible token that exists on an external, type 2 blockchain. The number of aliases can be increased over time to allow new users to join the network. The Semaphore network periodically checkpoints the state of the alias smart contract into the Semaphore chain so that Semaphore nodes know the ownership status of each alias. When broadcasting to the Semaphore blockchain, messages must be signed with keys bound to the alias. Validator nodes collaboratively produce blocks of broadcasts using an iterated voting process somewhat analogous to some proof of stake systems. This process ensures safety and liveness as long as no more than a third of validators are controlled by a malicious actor, which is standard for Byzantine fault tolerant systems. Blockspace is primarily allocated via a dynamic rate limit, enabled by the alias system. However, aliases that have received sufficient engagement from other aliases are allowed to exceed the rate limit to an extent. Unlike in a proof of work or proof of stake system, validators do not decide the canonical chain history. Instead, users commit to a specific chain history when broadcasting. In a process called proof of engagement, the canonical chain is determined by acquiring more commitments than competing chains. This system means that a majority of users, not validators, produces finality. Proof of engagement is well suited to a type 3 network because the type 3 network is not securing valuable assets, but instead is a means of reaching consensus of social broadcasts.