Phở Networks Whitepaper

*The very first *instant* decentralized social networking experience*

About

Phở Networks is a decentralized affinity-based social networking platform with ephemeral storage for increased privacy. The software, which is open source and licensed liberally under MIT, allows anyone to create a digital online community hub that is censorship-resilient against government-led content suppression methods. Unlike predecessor software, Phở Networks is:

(a) Instant: doesn't require an app or third-party plug-in to operate.
(b) Truly decentralized: there's absolutely no single point of failure.
(c) Comes with proven incentivization built-in: there's a clear benefit of participating in the network.

Phở Networks is offering this unique value proposition thanks to its novel "camaraderie network" architecture among the servers participating in the platform; as opposed to the typical blockchain, and client-side peer-to-peer approaches.

Motivation

There are two fundamental issues with existing social networks:

1. ***Brain hacking***: Platforms have shown capabilities of manipulating and deceiving people, through fake news, the spread of misinformation and echo chambers.
2. ***Censorship***: Governments all around the world censor social networks when they feel threatened; thus suppressing people's right to access information.

The main benefit of a decentralized social networking architecture would be it could be a recipe to both of the problems mentioned above.

Previous Work

There have been many attempts to create open social networks. From a technical standpoint, they may be categorized as follows:

1. Distributed Data (DD)
2. Distributed Identities (DI)
3. Distributed Communities (DC)

1. Distributed Data (DD)

In the distributed data model, all user-generated-content (including multimedia assets as well as database records) are stored:

(a) in a verifiable ledger such as Ethereum or Blockstack.
(b) peer-to-peer via distributed gossip protocols such as secure-scuttlebut (https://ssbc.github.io/scuttlebutt-protocol-guide/)

1a. Verifiable Ledger

This approach comes with the clear disadvantage of crypto-verification overhead and paying transaction fees for each insert or update operation.

Blockchains are known to be highly inefficient data stores. They are usable only with handful applications where the benefits outweigh the drawbacks; unfortunately, social networking is not one of them. As a consequence, many early attempts like Leeroy have already shut down, and there are only a small number of them like Peepeth which still exist but continue to fizzle.

Besides, with the DD approach, consumers are required to install an additional browser plug-in to use the services. While MetaMask, in the form of a Chrome extension, is the most user-friendly one, time has proven, on multiple occasions, that extra friction, no matter how little it is, never goes welcome with the consumers.

1b. Peer to Peer

Crypto is not the only backend adapter for the distributed data model. There is ongoing research in creating distributed data social networks

- Completely peer-to-peer among the client's browsers [see gun.eco]
- Through public cloud services such as Dropbox and Google Drive, [see POSN**]

but both are far from becoming applicable.

One can develop a peer-to-peer social network without the limitations of the browser; using a distributed gossip protocol such as secure-scuttlebutt*** on a desktop or mobile app similarly to Patchwork, Planetary. A big disadvantage with this approach is that the nicknames (to identify the user) cannot be unique since there is no global registry, and the only solution is to rely on centralized services. Last but not least, the Reddit-like desktop app Aether follows a similar approach but with an ephemeral append-only log (DAG) to store data, rather than relying on ssb.

** https://www.cse.unr.edu/~mgunes/papers/16-ASONAM-POSNapp.pdf
*** https://ssbc.github.io/scuttlebutt-protocol-guide/

2. Distributed Identities (DI)

There are several federated protocols, led by Microformats and Indieweb communities that suggest personal websites to represent one's online digital identity. Accordingly, such sites interact with each other via open pub/sub-protocols such. Even W3C has specific

recommendations that date back to 2017 like WebMention (https://www.w3.org/TR/webmention/)

IndieWeb oversees online activities to be aggregated in open-source silos. For example, micro.blog is one such aggregator that can interact with people's websites via WebMentions.

These small groups of like-minded "distributed identities" advocates gather online and offline sporadically, but they have failed to gain mainstream attention, due to:

- The lack of consistent user-interface
- Difficulty in the adoption of these technologies and launching such personal websites.
- Inefficiencies at the aggregator (newsfeed) level

Although, the distributed identity approach has no or negligible performance drawbacks as opposed to the DD, with a minor exception of "aggregator" level. On a positive note, they are philosophically similar to SMTP and POP3, which constitute the email communications infrastructure.

3. Distributed Communities (DC)

Perhaps the most realistic one among all three approaches is the "Distributed Communities" one, where the social network is not one giant graph (a la Facebook or Twitter) but constitute of many subgraphs around shared topics. Ning and Grou.ps are two such early, yet central examples. On the other hand, the new open-source upcomers such as Mastodon, GNU Social and DiSo do the same, taking a somewhat more decentralized approach where community owners host the open-source software on their own, and there's an underlying open federated protocol (ActivityPub) that connects the subgraphs.

The main benefit of the DC approach is the fact that, besides technical decentralization, more abstract (yet important) aspects of the network such as the governance, moderation and value-creation are also split between multiple parties. This is a positive direction, because otherwise, in a giant decentralized network, it will prove much harder to own, regulate and moderate than one might estimate.

The disadvantage of current DC based software is, while they borrow some ideas from the DI approach, with WebMention allowing Mastodon cross-follows across the networks, they are far from being usable and useful, particularly because the identities are completely isolated from each other. To illustrate it on Mastodon, esokullu@mastodon.social (with the email esokullu@gmail.com) has nothing in common with the same user on a different network, say esokullu@php-enthusiasts.social with the same email esokullu@gmail.com.

Additionally, the architecture they're built with, which is based on traditional MVC and relational databases, makes them impossible to scale out in a way regular people or software developers can.

Last but not least, with their shared-nothing data model, Mastodon and the likes have no answer to the censorship problem.

The Architecture

Unlike any other mentioned before, Phở Networks follows a hybrid of DI, DD and DC approaches. The innovation that makes Phở Networks censorship-resilient is its proprietary camaraderie network.

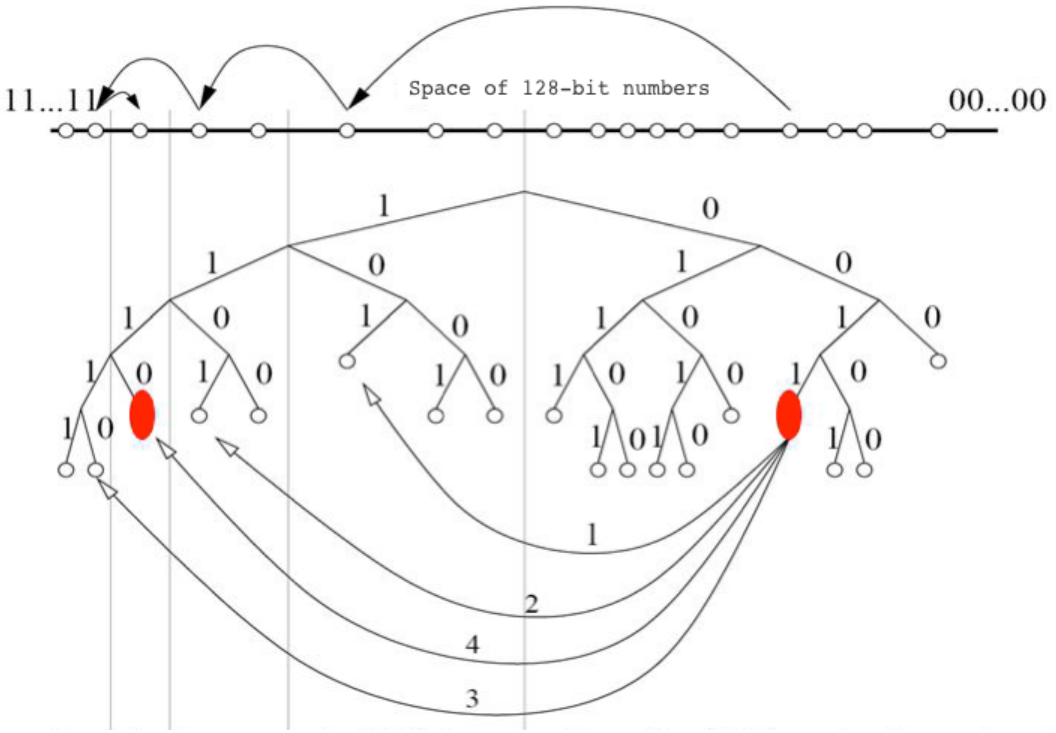
Phở Networks is designed in such a way that, if a part of the network is censored or blocked, all that the responsible party (e.g., community owner) needs to do is to change a single line of code in the client-side, and redirect the queries to some other part(s) of the network. The recipient of the traffic would be able to recognize the site and decipher its legitimacy from its 128-bit unique identifier; and even if it does not have its full information (like IP address and port number), it will still be able to query other neighboring peers. The XOR-distance model guarantees that in no more than 30 hops, it will find the right IP and port, then it can respond the clients by rerouting the queries and acting as a mirror to the original server.

This leaves the governments and bad actors only one choice, and that is letting the site operate or shutting down the whole internet, which is a less feasible action to take.

From a bird-eye view, Phở Networks architecture resembles more to Distributed Communities one, in the sense that we let community owners take charge of regulation and ownership. This constitutes the first layer of the decentralization.

However, unlike current DC approach, Phở Networks also does some data sharing across the network participants. Instead of sharing all the data across a common pool of resources (decentralized data) like DD, we share only some that are crucial; which include basic user and network records only, in a distributed hashtable that comes built-in with the software.

We use a slight derivative of the Kademlia principles in doing so, enabling the network participants to be sorted through a 128-bits-wide binary tree.



The result is; Tor-like censorship-avoidance, but faster and accessible by common web browsers such as Chrome and Firefox.

It's important to note that, with the Kademlia approach, even at the scale of billions of users, we can ensure a performance of no more than 30 hops. Since 5G is already guaranteed to make latency and internet performance 800% better than LTE, 30 hops will be virtually equal to the same level of user experience with today's Facebook.

The governance of the networks are secured in the Ethereum blockchain. As a consequence, only the community owners require a web browser plug-in (MetaMask) to be installed, to manage their network (such as approving a content, or banning a member) and all other users can interact with the network simply as they do on today's popular social networks.

Please note, Kademlia is susceptible to certain types of attacks, particularly Eclipse and Sybil, both caused by a number of adversary nodes to join the network and control certain parts of overlay tree. We encounter these attacks by (i) bootstrapping the network with a high number of "trusted" nodes. (ii) with user IDs that require a crypto-puzzle challenge to be solved in order to join, thus proof-of-work.

The crypto-challenge at Phở Networks is the following;

1. When the user joins the network, they are assigned a key, that will be used to encrypt and decrypt all their communications for added privacy.
2. A random word selected by the server is double key-hashed via HMAC method 1000 times on the client side, as many times as it takes until a node ID with 8 succeeding zeros are found.

3. The key is never transferred outside the client's computer.
4. The key-hash algorithms are distinct for further resistance to potential future vulnerabilities. They would be sha512 and ripe160.

```php
<?php

$t1=\microtime(true);
$i=0;

while(true) {
    $key = uniqid("", true);
    for($j=0;$j<1000;$j++){
        $x = hash_hmac("sha512",
                hash_hmac("ripemd160",
                                "phonetworks", $key),
                                 $key);
    }
    $i++;
    if(substr($x, -8)==str_repeat("0", 8)) {
        echo $key."\n";
        echo "in {$i} attempt\n";
        break;
    }
}

$t2=microtime(true);
echo $t2-$t1;

/**
 * Output as follows:
 * 5d883d226b0ad3.37367810
 * in 8252 attempt
 * 41.089943885803
 */

```

Such an algorithm allows a regular user account to be created within 30-40 seconds on a 2018 Macbook Pro hence can deflect brute-force attacks for a foreseeable future by fine-tuning the number of zeroes required, and still accommodating a user-space of 2^{96} (= 8 e^{28}) or more than a trillion trillions.

On the assets side, we use IPFS, which is already backed by IBM and Cloudflare . This removes the burden of CDN management by the participants of the network. IPFS does not require a third

party add-on for the client to install, and its decentralized underlying resemble to that of Phở Networks'.

Incentivization

In any decentralized project, incentivization is a crucial dilemma to crack for the success of the network. If there is no incentive for a user to join the network, there is no way for the network itself to reach the critical threshold. Bitcoin solved this dilemma with its cash-pegged currency as a value of store, and incentivizing miners with a ticket to earning some.

With Phở Networks, there are two incentivization models built-in:

1. The Intrinsic Incentive of Community Ownership
2. Securitization

1. The Intrinsic Incentive of Community Ownership

The sheer number of installations or subscriptions at Ning, Grou.ps, and other online community software all reach millions cumulatively. Community owners are rewarded by the appreciation of championing a cause, or more directly by charging members a subscription fee, or advertising. We also know that the number of Groups at Facebook surpassed 100,000,000.

2. Securitization

Phở Networks will "securitize" each network with its proprietary tokens (built on Ethereum ERC-1155) and operate a crypto exchange where community builders can buy & sell the ownership and control of their work in a marketplace-like setting.

Conclusion

Phở Networks will provide strong resilience against government censorship methods such as:

- Common ones: IP blocking, DNS filtering and redirection,
- URL filtering --by encrypting the graph's unique identifier with the user's private key—
- Packet filtering (with neutral headers)

Plus, Phở Networks has a strong incentivization model built-in.

It is important to note that Phở Networks is not a decentralized social network by itself, but underneath there is a general-purpose decentralized application platform that may be opened to third parties. Its RAM-first async design makes it very fast, and the fact that it is written in PHP will allow it to be embedded in the web's most popular CMS frameworks such as Drupal and Wordpress. For early results that prove 200% performance gains, even with no libevent or any

other such event-driven backend use, can be found at
https://github.com/phonetworks/benchmarks

Future Work

It is important to note that the encrypted and government-resistant nature of Phở Networks may render it a natural target for criminal use.

In the initial stages of Bitcoin, BTC was largely used for money-laundering and illegal activities (drug trafficking etc.,) but with strong KYC and AML rules, it is now widely used as a value-of-store for the average tech-savvy investor.

On the other hand, the social-media has already become an amplifier for the communication of most extreme thoughts and ideas with masses. Thus, an upgrade in the form of all-encrypted and government-resistant social-media platform poses the threat of adoption by pedophiles or extremists.

The future work should focus on this problem, and how to deal with it without sacrificing free-speech.