Don’t record your social life on an append-only social network

2022-11-08
5 minute read

Share

Secure Scuttlebutt (SSB) is an alternative, self-governed, distributed social network without gatekeepers. You only see updates and mentions from people you follow, so moderation isn’t as much of an issue as on Twitter. However, the technology that powers the platform is ill-suited for sharing things with our ever-changing social circles.

Elon Musk’s acquisition of Twitter last week kick-started a customer exodus from the social [Skip to main content] are either fed up with micro-blogging or looking for Twitter alternatives. SSB hasn’t gotten as much attention as Mastodon (the “Fediverse”). However, SSB is worth considering as a serverless, self-governing, and self-hosted Twitter replacement.

The technology that powers SSB is entirely different from Twitter and Mastodon. You don't need to register an account anywhere to get started. Your identity isn't a username and doesn't depend on a domain name or service provider. Instead, your username is a meaningless cryptographic hash that consists of random-looking numbers and letters. Your friends only need to know your hash to follow you, and you can keep it as public or private as you want.[1]

[1] You must arrange a side channel such as QR codes or email to exchange hashes. There's no single global feed in the network, and neither is there a global user directory.

All you need to get started is an SSB-compatible client app; you don't even need an internet connection (except when pushing and pulling updates). Every update you publish, whether public or private, is stored in a local append-only database (AOD). The database exists primarily on your local device.

The network works by having its users synchronize with each other's account databases. The databases get distributed through "pub" servers. Some SSB client apps can also exchange updates using other means, such as directly between devices using distributed peer-to-peer (P2P) connectivity. Users and pubs can pass along updates on behalf of mutual connections, so everyone doesn't need to be online simultaneously for the network to function.

All of this sounds great, and you can completely discard any corporate overlords, censors, and other parties with misaligned incentives. It's just you and your friends or audience talking directly to each other's devices. Everything is encrypted and you can make what you share as private or public as you want.

The AOD functions like a blockchain where every update is cryptographically chained one after the other. This structure makes it easy to synchronize the database across devices.

You must break the blockchain and fall out of sync with everyone who follows you to delepdates on the network. Any modification to existing updates on the blockchain creates a new blockchain where every following update must be re-appended to the new chain. The original will remain just as valid as the new blockchain, which causes conflicts and synchronization stalemates.

Append-only databases are acceptable for financial ledgers, contracts, and things we want to be persistent and immutable. Unfortunately, social graphs aren't immutable. People fall out with each other over time: relationships end, friendships shift, and we change who we are as we age and move through life.

Maybe you posted something you later regretted and wanted to remove from the network. Or perhaps you don't want to be reminded of a former acquaintance or relationship, so you want to remove messages and images with that person. Maybe your device storage is full from all the photos and videos your aunt shares with you.

Whatever the reason, people need to have some control and power to change — or at least delete — things as they move on in life. On SSB, you must create a new identity and start a new blockchain to escape your past mistakes and regrets.

The experimental P2P-focused Beaker Browser project also experimented with building a distributed social network. Beaker uses the Hypercore Protocol which uses an append-only storage system for its P2P network.

The open-source instant messaging client Jami uses P2P and a blockchain to exchange and keep messages in sync between users and your devices. It uses one blockchain per contact or group conversation instead of a single database for everyone.[2]

[2] Jami uses Git — the popular version control utility – for its conversation blockchains.

This design at least lets you unfriend someone and leave them behind when the time comes.

Permanency may sound like a neat feature and it lets developers take shortcuts when creating reliable distributed networks. When deployed correctly, it can help keep politicians and public figures accountable. However, it's definitely not what you should look for in your social network. ■

Privacy P2P

Abbreviations

AOD	append-only database
P2P	peer-to-peer
SSB	Secure Scuttlebutt

Related reading

P2P apps' connection amnesia makes them less fault-tolerant

Why 'IPv6 Control Message' uses so much data in Windows 10

5 options for auto-mounting network shares on MacOS

Are you even trying to fight spam bots, Twitter?

Skip to main content

Follow Ctrl blog on Feedly

Hosting by Hetzner and Linode. CDN by Bunny.