

Freebits – A Decentralized Global Public Square

Version 1.0

Dr. Shiva Kintali
shivakintali.org
freebits.app/shiva

Abstract

In this paper, we present Freebits, a decentralized global public square. We discuss how the Freebits [platform](#) and the EulerChain [protocol](#) can solve the ongoing social media censorship crisis. We explain why there is an urgent need for a decentralized, permissionless and uncensorable global public square. This paper is written in a simple language, minimizing the greek symbols, to make it accessible to everyone.

Keywords: bitcoin, blockchain, cryptocurrency, decentralisation, peer-to-peer, social media.

1 Introduction

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

— United Nations

“If freedom of speech is taken away, then dumb and silent we may be led, like sheep to the slaughter.”

— George Washington

“If we don’t believe in freedom of expression for people we despise, we don’t believe in it at all.”

— Noam Chomsky

“I disapprove of what you say, but I will defend to the death your right to say it.”

— Voltaire, (Attributed); written in 1906 by Evelyn Beatrice Hall (pseudonym. S. G. Tallentyre) in the biography “The Friends of Voltaire”.

“The moment you declare a set of ideas to be immune from criticism, satire, derision, or contempt, freedom of thought becomes impossible.”

— Salman Rushdie

“Without freedom of speech there is no modern world, just a barbaric one.”

— Ai Weiwei

Any democracy is impossible without freedom of speech, cross-pollination of ideas and a common understanding of what is true and what is false. In good old days, we had public squares i.e., open public areas in a town where people gather and where public speech, debate and discussion are allowed for everyone. In the last two decades, the rise of social media platforms and online communication tools dwarfed all these physical public squares. We now express ourselves in bits, over the Internet.

Unfortunately, the current social media platforms are not true public squares. Jack Dorsey (co-founder of twitter) frankly **admitted** that *free speech was never a descriptor of twitter*. He is right. Old social media platforms were *not designed* to protect our free speech and first amendment. They are centralized communication platforms where the users are the product and the advertisers are the paying customers. The rules about which content is acceptable and which content is unacceptable are made by the parent company. These rules are often contradictory, unfair, biased and artificial without any consistently solid principles. The enforcement of these rules is not transparent. Corporations regulating online speech is a very **dangerous** precedent, to say the least.

A recent pew survey found that approximately **75%** of Americans believe that social media sites intentionally censor political viewpoints. For example: BLM activists **say** they are being silenced by facebook. Conservatives **say** they are being unfairly censored online. Numerous such examples can be found in several countries across the world. This is creating unprecedented chaos... *left, right and center*.

In the last decade, twitter and facebook have become the default social media platforms across the world. Recently several governments are losing trust in social media because they do not want their democracy and freedom of speech controlled by a few people at tech companies. Some countries are passing laws that would fine tech companies millions of dollars every time they unconstitutionally censor lawful speech online. Governments imposing fines and regulating social media platforms are not long-term sustainable solutions. Tech companies defend themselves saying “we are private companies and we have the right to refuse our services to anyone”. They often ban or censor people with vague explanations. Some countries are developing their own local social media platforms to maintain a sovereign communication channel for their leaders to directly reach their citizens. This is just shifting the problem from one centralized company to another local centralized company. But the issue of *ensorship* and *tech control* is not addressed at all. Also, fragmented local apps cannot enable debates about global problems (covid, climate change etc) and cross-pollination of global ideas and solutions. The world now is more interconnected and interdependent than ever before in the history.

Governments cannot be given the right to control our speech either. There are several instances of governments across the world banning social media access during important elections and protests, to control the narrative to suit their own political agenda.

This raises a very important dilemma. *Who should regulate online speech ?* Is it the governments or the tech companies ? The answer is **no one**. Censoring, banning and de-platforming the speech *you* do not like is not a long-term sustainable solution. They *will* make things much worse and lead us *all* towards a dystopia.

We should never trust any centralized company or government or any group of gatekeepers with our freedom of speech. No one should be allowed to dictate the parameters of acceptable speech and filter what we can think and hide opinions and shadow-ban people. Everyone has the right to freely express their thoughts in text, images, satirical cartoons, videos, symbolic speech, art, animation etc, even if someone else considers them as hate speech.

For decades, we have allowed the banks to control our financial freedom and dictate terms about how we can use our own hard-earned money. 2008 financial crisis opened our eyes. The subsequent adoption of Bitcoin and other cryptocurrencies is giving the control of personal finance back to the individual people. In the last decade, we have allowed tech companies and governments to control our freedom of speech, because it is very convenient to use free centralized platforms and addictive apps. Creators, journalists, global leaders and even satire accounts are getting de-platformed and de-monetized without any valid reasons. Some of the reasons given by the tech corporations are outright silly. This crisis is as serious as 2008 financial crisis, if not more. Now it is high time to build open, transparent, fair and unstoppable protocols and global platforms (built on top of the open protocols) that allow everyone to join in with conversations around the world. The socio-economic, moral and technological rationales to build a decentralized future, are now very obvious.

In the last decade, we have witnessed a steep rise in *citizen journalism and pseudonymous journalism* (and pseudonymous researchers and developers). The quality of citizen journalism is often better than the mainstream media. Have you ever noticed that when you visit a big media company's website, only a small fraction of their articles fall in the category of real journalism and the rest of it is some kind of scripted and biased propaganda, click bait articles, affiliate marketing and privacy intrusive ads. But when you subscribe to a citizen journalist's newsletter or a podcast, a large fraction of it has real investigative journalism and genuine discussions between people (displaying mutual respect even when they completely disagree with each other) and only a small fraction of the content has non-personalized ads to support the creator. This is perhaps because media corporations care about their profits first and their journalist employees are often told to align their articles with their profit model. Independent citizen journalists care passionately about other citizens. Decentralized protocols enable citizen journalists and pseudonymous journalists to speak freely to everyone globally, connect with their followers and get tips without any fear of censorship or de-platforming.

Journalism is one of the most dangerous profession. Journalists often get threatened, intimidated, silenced and even killed. The decentralized pseudonymous identities, combined with zero-knowledge-proofs and tamper-proof provenance of photos and videos, help journalists and whistleblowers to fearlessly bring truth to everyone. For example, the entire covid crisis could have been prevented (or made much less severe) if the doctors in China had the ability to securely communicate the early warnings to all the global citizens while simultaneously proving that they belong to the right corporation (hospital or virology department).

[Freebits](#) is a decentralized, permissionless, immutable, uncensorable online public square, globally accessible to anyone with an internet connection. It is *a borderless decentralized bulletin board* for everyone. It is built on top of an open, unstoppable and uncensorable [EulerChain](#) protocol. In the following sections, we discuss the details of the EulerChain protocol and the Freebits platform.

2 EulerChain – The Protocol

The early stages of the Internet started with open protocols such as HTTP and SMTP. Somehow, along the way we have lost our principles, took shortcuts and built centralized services, treating everyone as a product and obsessively maximizing the number of ad clicks. A small number of corporations took control of all aspects of our lives and play anti-competitive games with each other. For example, Google [pulled](#) YouTube off the Fire TV and Echo Show after Amazon stopped

selling the Nest products. Several creators lost thousands of viewers during this period. There are hundreds of such examples. We can avoid such crisis, if we host our content on decentralized storage networks using open protocols, not controlled by any corporation. The recent rise of decentralized protocols gives a new hope to put us on the right track again i.e., building open and decentralized protocols to store and transfer not only *data* but also *value*.

The correct way to enable free speech for everyone is to first build an open protocol. This protocol is like a *public utility* accessible to anyone with an internet connection. Then anyone can build platforms and interfaces on top of this protocol. For example, Bitcoin is an open protocol and we have hundreds of interfaces (wallets, exchanges, explorers) built by independent developers and corporations. No one can unilaterally stop the Bitcoin protocol.

EulerChain is built on Bitcoin source code with only two important changes. The underlying cryptocurrency of EulerChain is *Euler*. It is named after Leonhard Euler, an 18th century Swiss mathematician, physicist, astronomer, geographer, logician and engineer, held to be one of the greatest mathematicians in history. There are more than 96 mathematical terms (theorems, identities, equations and symbols) named after Euler.

Bitcoin blockchain is an elegant decentralized ledger to send and receive bitcoin in a permissionless manner. All the transactions are publicly visible. Similarly, EulerChain is a basic decentralized ledger that allows anyone broadcast their thoughts (in 256 bytes at a time) to the entire world publicly in a permissionless and censorship-resistant manner. The two main differences between Bitcoin and Eulerchain: (i) EulerChain uses an ASIC-resistant hash puzzle to allow anyone with a laptop to mine Euler. (ii) The OP_RETURN field in each EulerChain transaction is 256 bytes long. EulerChain code is intentionally kept very simple and close to Bitcoin code to make it compatible with all the existing open source crypto tools and blockchain APIs and enable quicker global adoption.

Eulerchain explorer, address generator, seedphrase generator and web wallet are hosted at eulerchain.org. EulerChain mainnet and a mining pool were released on March 14th 2021, Pi Day. Coincidentally, on the same day, there was an [article](#) titled “Control over online speech should be in the hands of users, not the government” published in The Times of Northwest Indiana. It is a short guest commentary written by [Jillian York](#) ([director](#) of International Freedom of Expression at the Electronic Frontier Foundation and author of “Silicon Values: The Future of Free Speech Under Surveillance Capitalism”) and [Karen Gullo](#) (an analyst and senior media relations specialist at Electronic Frontier Foundation). The article’s title and the content perfectly summarizes our mission. We used the title of this article in the EulerChain’s genesis block.

3 Freebits – A Platform

Freebits is a front-end for posting and retrieving content on EulerChain. Each post (at most 256 bytes) can contain any text (in any language), emojis, hashtags, cryptographic hashes and links (URLs or IPFS content hashes). Freebits platform provides a quick and easy onboarding process (with a userid and password) and some well-known social media functionalities such as followers, likes, reshares and comments.

Every time a user posts something, she must enter her seedphrase. A javascript program (running locally in your browser) extracts the private key and public key from the seedphrase. The private key is never sent to any servers. Users are responsible to keep their seedphrases secure and safe. If they lose their seedphrase, no one can recover it. The private key is used to send a very small amount of Euler from the user to herself. The text of the user’s post is stored in the

OP_RETURN field in this transaction. This transaction is broadcast to the EulerChain network. This data is permanently stored on EulerChain and visible to everyone publicly. Your seedphrase is not required when you like or reshare a post.

The first time a user posts something on EulerChain using Freebits platform, the user's *public* key is stored in the user database on freebits servers. This public key is the user's decentralized identity (DID). It is displayed on the user's profile page. Freebits maintains a mapping between the public keys and the userids. This mapping is one-to-one i.e., *one userid one public key*. If the user lost her seedphrase, freebits platform does not allow the user to update her profile with a new seedphrase. This is for security reasons. This mapping is not decentralized, to prevent impersonation scams. If we detect (or get a complaint) that a malicious actor is impersonating a famous influencer (for example, someone other than Elon Musk creating an @elonmusk account on Freebits), then Freebits can delete this userid. The malicious actor can still use his seedphrase to post on EulerChain. but we can stop him illegally using celebrity names and trademarked names to scam people.

Freebits is a free platform for everyone. All services are provided at no cost to the user. The platform gives free Euler to new users and this Euler is used to sign and post the user's content on EulerChain.

As mentioned earlier, Freebits is just a front-end platform. If you do not trust Freebits, you can announce your public key on your personal homepage or blog and use your seedphrase to post anything (256 bytes per post) directly on the EulerChain blockchain. You can implement a widget to retrieve all your posts directly from EulerChain and display them on your website or blog, without using Freebits or any centralized service. You can even use a good old command line interface to post your thoughts on EulerChain. Even a middle-school student can write a simple script to retrieve and analyze all the posts of any user (pseudonymously identified by her public key) from the EulerChain. Journalists, politicians, global leaders and activists can use EulerChain without any fear of censorship or de-platforming. They can choose to be anonymous, pseudonymous or use their real name.

Remember the massive twitter [hack](#) ? A hacker got access to several twitter accounts (including Apple, Biden, Obama, Musk) and posted tweets on behalf of these accounts. That kind of massive centralized attack is impossible on freebits platform, because seedphrases are not stored on any centralized servers. Each user is responsible for securing her seedphrase. There is no centralized database with seed phrases of thousands of users. Do not share your seedphrase with anyone.

Seedphrase also acts as an elegant 2FA. As we all know the 2FA using SMS is broken. SIM hacks have become very common these days, especially in the crypto space. Not everyone uses an encrypted SIM.

All posts are stored permanently on EulerChain. There is no way to delete your posts from the Blockchain. We hope this encourages everyone to be more thoughtful instead of posting something in the heat of the moment. Immutability prevents obfuscation and fake screenshots. This is a very useful feature, especially for public figures and global leaders. See this example of a fake [screenshot](#). EulerChain is a decentralized ledger of all thoughts, ideas and free expressions cryptographically signed by the users, stored on-chain.

3.1 Customization

Anyone can connect their RSS feeds, data APIs, newsletter or podcast feeds to their DID on EulerChain and automate their announcements. Since the entire data is publicly stored on EulerChain,

anyone can develop their own platform, for example: one platform for displaying only images, one for displaying only audio content, one for displaying only education content etc. Any citizen journalist from anywhere on the earth has free access to all these posts. Academic researchers can freely access and analyze all the posts. Search engines can freely access the posts and index them for efficient search. Anyone from any country can develop front-end platforms respecting their own local laws.

There is a growing distrust of the ranking and recommendation algorithms implemented by mainstream social media networks. They often manipulate users' behavior to maximize their profits. EulerChain stores all the data publicly and Freebits platform shows only the content from the people you follow, in a reverse chronological order. Anyone can develop open-source recommendation algorithms and "plug them" into freebits and extend the platform. These plug-ins are similar to browser extensions, first pioneered by Firefox browser.

3.2 Decentralized blue checkmark

Tech corporations maintaining, controlling and verifying our online identity is a dystopian mess. The best solution is to decentralize i.e., any university, employer, organization can issue credentials, badges and achievements to your EulerChain DID in a completely decentralized manner. For example: Non-profit organizations can issue volunteering badges. Video game companies can automatically send your in-game achievements to your DID. All these badges and credentials represent your online persona. Your DID is a digital wallet for all your credentials, achievements and badges. It is your *decentralized* blue checkmark. These credentials can be verified instantaneously without requiring any intermediary. Since all the posts are public, anyone can analyze your posts and determine your credibility on certain topics: Politics, Science, Healthcare, Technology, Entrepreneurship and whatever.

We have already developed a credential platform (internal codenamed TrueCerts) to enable anyone issue, verify, send, receive credentials on EulerChain. We will be integrating this into freebits soon.

3.3 Fact Checking

Freebits analyzes articles from fact-checking websites and scientific journals and displays the relevant facts next to the relevant posts (containing potential misinformation). These articles are only displayed on the freebits website. They are not stored on the blockchain.

3.4 Tamper-proof Provenance

We have developed a data integrity platform (internal codenamed TrueDat) to track the provenance of any digital content from its origin. Freebits iOS app (with TrueDat APIs) tracks the authenticity of photos and videos (captured using the mobile camera) and stores the metadata (depth information, location, timestamp etc) on EulerChain. This metadata can be used to detect data tampering. TrueDat APIs enables creators to track the ownership and transfer of digital rights of their creations (digital art, photos, videos and music).

3.5 Decentralized creativity economy

We respect the relationship between the creators and their fans by connecting them directly without any intermediaries. Users can tip other creators on freebits, using Euler, the underlying cryptocurrency of EulerChain. Freebits platform takes no commission from these transactions. In future versions, artists can create NFTs directly on the platform. It is as easy as posting an image (or a gif or a video) and setting up simple parameters.

We are implementing *paid DMs* i.e., creators, influencers and anyone can set a price (in Euler) to receive DMs from unknown users. The unknown user must send the required Euler to DM those users.

3.6 StreamerAI

We have developed an AI-powered news analysis engine (internal codenamed StreamerAI) and integrated it into the Freebits platform. It analyzes hundreds of thousands of news articles daily and organizes them into streams. It allows anyone to consume news they care about, without creating hundreds of keyword alerts. Here are some examples of streams: [~ArtificialIntelligence](#), [~Blockchain](#), [~Bitcoin](#), [~DeFi](#), [~FactCheck](#), [~FactCheckIndia](#), [~arXiv.cs.CC](#) and many [more](#).

3.7 FreeSearch

We are currently developing a search engine (internal codenamed FreeSearch) to crawl, retrieve and index all the content stored on decentralized storage networks. It is an efficient discovery platform to search for all global voices from all decentralized media ecosystems.

4 Future

In the future versions of this paper, we will discuss new features in the EulerChain protocol (support for native tokens, metadata, NFTs) and Freebits platform (support for images, videos, audio, ownership economy using a digital collectible marketplace, video-game collectibles integration, tokenizing yourself). These features are currently under development. EulerChain browser extension and our iOS app (with a built-in wallet and support for tamper-proof photos, videos and audio) will be released in the next couple of months.

Note: I respect what Jack and Zuck have built, but I don't want to become the next Jack or Zuck. Nobody should be the next Jack or Zuck. I strongly believe that we need unstoppable protocols, decentralized storage and user-customizable browser-based platforms to reduce our dependency on centralized services. No one should be the arbiters of free speech and free expression. Not governments, not tech companies.

My political beliefs are neither left nor right. I take sides on specific issues. The only maximalism I believe in, is *free speech maximalism*. I am a technologist with a mission to build a decentralized future for every global citizen, encourage cross-pollination of global ideas, reduce misinformation, fraud and corruption by simplifying the flow of free speech, trust and truth in the digital world. If you want to join us in this exciting journey, please contact us.

Acknowledgements : To all the cypherpunks, anonymous and pseudonymous developers... *May the hash be with you.*

Anyone that makes up their mind before they hit a issue is a f***ing fool. Everybody is so busy wanting to be down with a gang... I am a conservative.... I am a liberal.... bulls**t. Be a f***ing PERSON. LISTEN. Let it swirl around your head. THEN form your opinion.

— Chris Rock