The Truth Social Network: A Decentralized Social Network

>btc_joe
btc_joe@protonmail.com
www.thetruthsocialnetwork.com

Abstract: A decentralized social network would allow participants to engage in social media directly without relying on trusted third parties. The need for permission-based access to various walled garden platforms would be eliminated. Recreating the vast majority of social media functionality largely depends upon solving the problem of decentralized, pseudonymous identity. We propose a solution to the above by utilizing the cryptocurrency Public Key Infrastructure (PKI). By choosing a single public address, participants can create censorship-resistant historical records of content. Content is provably linked to an identity through the creation of digital fingerprints, which are timestamped and committed to blocks (which are themselves timestamped). Participants can reference their own and others content by simply including it's unique fingerprint within their message. Any file that can be hashed (audio, video, zips, pdfs, etc) can be included within messages. While files themselves *are not* stored in these identity blockchains, a record of them *is*, as their hashes are committed to fingerprints.

1. Introduction:

Social Media has come to rely almost exclusively on monopolistic, politically biased technology companies serving as trusted third parties who store, maintain, and curate content. The ability to publish depends upon permission-based access to various walled garden systems each of which authenticates users by storing passwords in centralized databases. Hacks, censorship, and the harvesting of our data have proven these third parties to be security vulnerabilities.

While the system has worked well enough, in recent years our trust has been abused. Critical information which serves the public good is often prevented from trending and reaching the masses. An Orwellian environment has been created where users are forced to curtail their speech or risk permanent banishment from digital society by the various silicon valley ministries of truth. Many would agree the range of allowable discussion, dissent, and discourse has been dramatically reduced. Statistics such as views, likes, followers, etc can all be gamed through the use of bot farms. Attempts to mitigate the above have manifested in the form of know-your-customer like mechanisms for limiting access in conjunction with esoterically written artificial intelligence algorithms serving as judge, jury, and executioner.

To claim that most of the problems incurred by using these platforms can be avoided by creating your own website is some-what true, yet no protocols, systems, or standards exist which allow you to format (and potentially monetize) content in a way that enables interaction, virality, and the ability to create your own historical record. We believe it is time to reexamine the design of social media with a fresh perspective. In our view it is entirely possible to recreate the vast majority of social media functionality with an open-source protocol.

What is needed is a decentralized social media network based on upon cryptographic proof instead of trust, allowing any two willing parties to interact directly with each other without the need for a trusted third party. In this paper we propose a system of write-only (as in only the content-creator can propose blocks to be appended) 'identity blockchains' where users store their own content and concurrently build a public, timestamped historical record of such. Given there is sufficient demand in the form of hash power, content becomes increasingly immutable through 'Merged-merged Mining' (a slight variation of Merged Mining first used in Namecoin [1]).

2. TSN References:

As opposed to financial transactions, identity blocks are populated with content fingerprints called ‘TSN References.’ TSN References are produced using your unique ‘TSN Address.’ A TSN Address is the hash of a public key (as defined by asymmetric cryptography). The ability to sign messages from a public address which *only* you own the private key to is essential. This public address serves as the basis for your ‘TSN Account(s)’. Accounts are used to publish content.

‘TSN Signature Pages’ are pages on your ‘Block Publishing Server’ (BPS) specifically dedicated to each of your digital signatures. By having these dedicated pages you can easily--using a line within your message--reference your own and others past TSN References. Simply provide the fingerprint of the TSN Reference with a link to it's corresponding signature page URL. More importantly, it is on these pages where files are actually stored. When uploading a file your message *must* contain a line with the file name followed by a line with the file hash.

The key concept to grasp here is these links to other signature pages and links to uploaded files exist solely on signature pages, as it is only the raw text of your references which are concurrently added to your candidate block.

3 . TSN Accounts:

TSN Accounts are opened and closed using your TSN Address. An individual TSN Address can have multiple TSN Accounts, although it *must* have a Primary Account.

Opening a TSN Account
Under the directory of "Accounts" a 'mandatory directory' you will create a TSN Reference which:
-Describes the server/domain you wish to open an account from
-Designates >your_blockchain_handle (in the case of your Primary Account)
-States "hello world"

Closing a TSN Account
Under the directory of "Accounts" you will create a TSN Reference which:
-References the "hello world" TSN Reference
-States "denounce" (or as an emergency measure “denounce and replace with” followed by a line describing the new server)

Primary Account
Opening a Primary Account establishes your current BPS (the server from which you will publish blocks). Since this Signature Page was published on your BPS--no further action is required.

‘Backwards compatible’ social media Accounts
Since this Signature Page is published from your BPS--a link to it *must* then be published from your backwards compatible social media account (thus proving ownership of the account).
By establishing a Valid TSN Account--one of three major forms of signing is being used--so the decision to sign and record said content in your blocks thereafter is yours to make.

Valid TSN Account(s)
A Valid TSN Account is an account who's status is current (as per >your_blockchain).

4. Three aspects of signing:

There are three different aspects of TSN Signing all of which are *required* for the creation of TSN References:

Digital Signatures
The first aspect is the Digital Signature. Messages are digitally signed using your TSN Address creating cryptographically verifiable fingerprints.

Publishing from a Valid TSN Account
The second aspect is publishing the message and corresponding fingerprint from a Valid TSN Account.

Concurrently including Digital Signatures (as well as Signature Page URLs) in Blocks
The third aspect is the inclusion of the message and corresponding fingerprint in your candidate block. This submits it for inclusion in your historical record of content.

In traditional social media editing or deletion of content is allowed. Similarly, on The Truth Social Network editing or deletion of TSN References is allowed, except in our case the ability to do so is temporary (eventually your candidate block is committed to a hash).

5. Timestamping and The TSN Protocol:

Time is established all throughout the creation of your historical record. Timestamps can be broken down into three categories: publishing timestamps, occurrence proofs, and existence proofs. Unix Epoch Time is used to commit your own publishing timestamp to a message or file. The most famous application of what we call occurrence proofs would be proof of life used by Julian Assange in 2017 [2]. Occurrence proofs state an easily identifiable characteristic of the most recently confirmed block in a blockchain. While the Block Hash is used as a blocks unique identifier, there are other characteristics which would be near impossible to *consistently and continuously* predict without error. For instance, lets take the number of transactions in the most recent block of the Bitcoin [3] and Litecoin [4] blockchain to illustrate an occurrence proof:

Bitcoin block height,# of transactions Litecoin block height,# of transactions
example (at the time of writing):
654927,2196 1938980,273

In our case we can use the universally agreed upon block timestamp for our occurrence proofs. By committing these proofs to a message to be signed, or a file to be hashed, you are to an extent proving that the creation of such occurred *after* a certain time. By ‘establishing the time’ what we really mean is using a combination of your own publishing timestamp followed by an occurrence proof using both Bitcoin *and* Litecoin.

Requiring the use of two separate chains for an occurrence proof keeps the likelihood of *both* chains being reorganized i.e. an invalid proof small. Again editing is allowed before blocks are committed to a hash, so proofs which turn out to be invalid can easily be corrected. Naturally, your publishing timestamp *must* be more recent than either timestamp used in your occurrence proof. Similarly, if referencing your own or others’ TSN Reference—your publishing timestamp *must* be more recent. Finally, your publishing timestamp *must* be less recent than a subsequent TSN Reference (or less recent than the block header timestamp in the case of a candidate block’s last TSN Reference).

On the other hand, existence proofs help prove that a signed message, or a hashed file, existed *before* a certain time. While existence proofs generally have a cost (on-chain transaction fees) the OpenTimestamps protocol [5] is free to use. The first TSN Reference added to your candidate block is a special TSN Reference called ‘The Cloutbase Reference.’ The Cloutbase Reference *must* provide an existence proof of the previous block i.e. it’s message must contain a line for the previous block OTS file and a line for the corresponding file hash.

Your Primary Account opening TSN Reference is the only reference in your genesis block. In this instance, there can be no Cloutbase Reference as there is no prior block for an existence proof. Your Primary Account opening TSN Reference *must* have a bitcoin occurrence proof within 10 blocks of the first Cloutbase Reference (identity block #2) bitcoin occurrence proof.

All TSN References *must* establish the time. Each TSN Reference *must* have timestamps within the interval of one TSN Block Header to the next. After creating a block header, blocks are submitted to your ‘Cloutchain Network’ for validation. There is no nonce or proof of work, as long as a block has followed the protocol it will be accepted. TSN Block Headers *must* establish the time and contain the previous block hash. The bitcoin occurrence proof used in your block header *must* be more recent than the Cloutbase Reference OTS bitcoin attestation block number.

Further, by implementing a block publishing time *limit* of say 248 bitcoin blocks, we are ensuring that as long as content is being produced blocks will be produced. To better phrase the rule: the block time limit rule states that you *can not* add a TSN Reference to a TSN block which is greater than 248 bitcoin blocks from your last published block (~two days).

Basically, blocks are published in order to avoid breaking the rule and since this is necessarily accompanied by the creation of a new Cloutbase Reference—existence proofs will be taken nearly as frequently as blocks are published. There is no problem with taking long breaks from creating content, the key is to always begin a new block as soon as an old one is accepted by the network. If you unintentionally break the block time limit rule an exception is allowed. For instance, if immediately after publishing a block you are abducted by aliens, when you return you must reapply the 10 block occurrence proof rule similar to your genesis block, except in this case your first TSN Reference will be a Cloutbase Reference (to be compared with the following Cloutbase Reference) and your header will contain the previous block hash.

This constant alternation between existence proofs and occurrence proofs serves as a check on the system. While it can take a few hours for your OTS to get confirmed by the Bitcoin blockchain, the mere necessity of having to create these existence proofs in order to publish subsequent blocks should foster fairly reliable timestamps. Occurrance proofs keep your publishing timestamps honest, and existence proofs keep your occurrance proofs honest.

6. Directories and Thread Channel Replies

TSN References are published under various directories on your BPS. Mandatory Directories are directories that everyone *must* run, such as Accounts. ‘Common Directories’ are directories with their own agreed upon set of standards. ‘Niche Directories’ are custom directories that anyone can create but no one else has to run.

‘Thread Channel Replies’ enable the creation of a comments section for any TSN Reference. The main difference between a TSN Reference and a reply is that replies use 2/3 aspects of signing, in other words they are not submitted to your candidate block. The initiator publishes their reply on a signature page under a sub-directory dedicated to thread channel replies. Referencing or replying to others requires pinging the recipient the signature page URL, a notification-like feature.

In order to reply to a reply, updating the state of a channel, you must provide the preceding chain of replies on your signature page until you reach a TSN Reference. Aggregation Signature Pages can be used to manage complicated, lengthy threads. You always have the option to include your most recent response on chain thus creating a TSN Reference which has the entire state of preceding replies built into it’s message. You need not include every single reply to a particular reference or reply on your server, but you *must* include every reply that you are replying to. Providing replies that you may not reply to is courteous to their creator as it exposes them to your audience which could lead to tips in the form of 'Clout.'

7. Clout:

Clout is the unit of account and block reward for 'The Cloutchain.' Cloutchain miners process transactions and distribute the supply of Clout. The Clout supply schedule mimics that of Bitcoin although faster confirmation times could be implemented.

On The Truth Social Network, attention is rooted, earned, and measured in hash power. Each and every identity blockchain has it's own Cloutchain and accompanying Proof of Work [6] difficulty. Clout can be used as reward points with the content creator. TSN References and replies can be tipped in Clout. TSN References published under the directory of 'Cloutreon' are priced in Clout. Cloutreon references contain encrypted file containers of which the passwords are only revealed upon payment or using a push-based subscription model. Development bounties could be created for projects under the 'Git Truth' directory. Advertising on a BPS, products, or services could be priced in Clout.

While in general, a particular reference will be most exposed to the audience of the content creator, and in turn, their Clout, a single Address can be tipped on multiple chains. No Cloutchain is aware of the transactions or state of any other Cloutchain, but wallets could be designed to run Simplified Payment Verification applicable to numerous chains. A 'Universal Cloutchain Explorer' could run as many Cloutchain nodes as possible, or above a certain difficulty threshold, which could be queried for the accumulated cross-chain balances of any TSN Reference. This could come into play with the concept of 'Server Feeds' (more on this later).

Wallets can generate a new Clout Address for each reference or reply which is then committed to the last line of its' message. Tipping content is a fun way to measure success, and is harder to manipulate than any traditional social media metric as all Clout emanates from Proof of Work. In terms of privacy, your identity is pseudonymous. Clout transactions have the same anonymity heuristics and trade-offs as Bitcoin, there is no way to tell if Clout tips are subsequently swept to an address the identity owns, another entity, etc.

The amount of likes, shares, or engagement with regard to a particular reference is less important than the balance it has received in Clout. The amount of followers a particular content creator might have is less important than the difficulty of their Cloutchain. Each of the aforementioned traditional social media functionalities (followers, likes, etc) can easily be implemented but they are less relevant.

8. Merged-merged Mining

Merged-merged Mining is nearly identical to Merged Mining, a configuration of mining which allows for the application of hash power geared towards a Parent blockhain to be simultaneously used as proof of work towards on one or more Auxiliary blockchains.

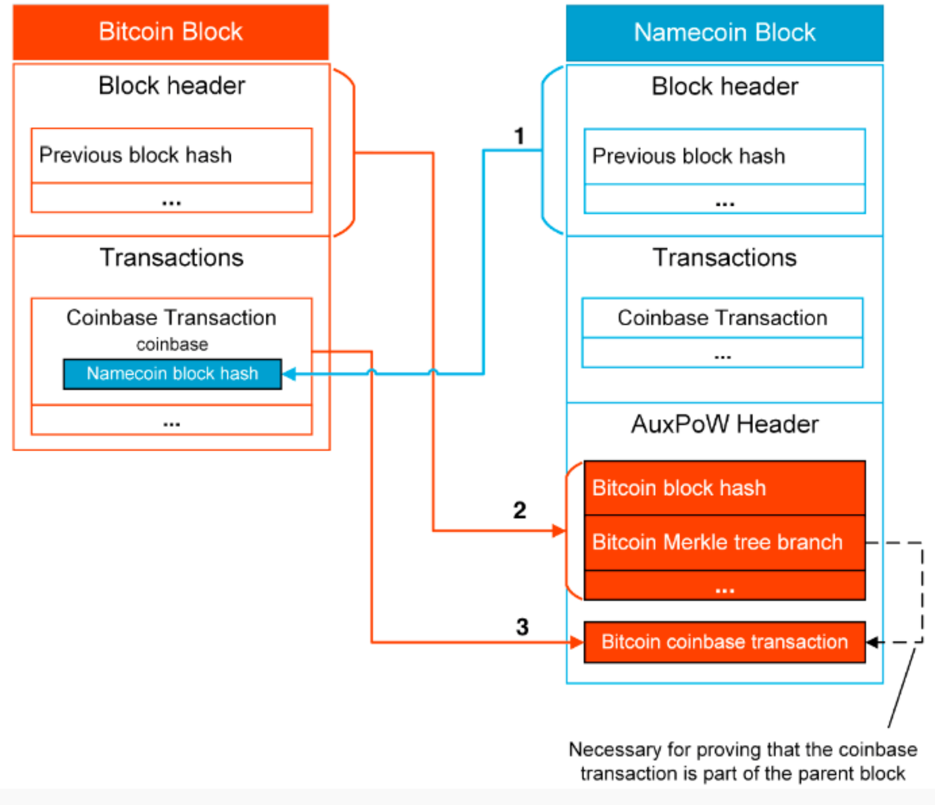
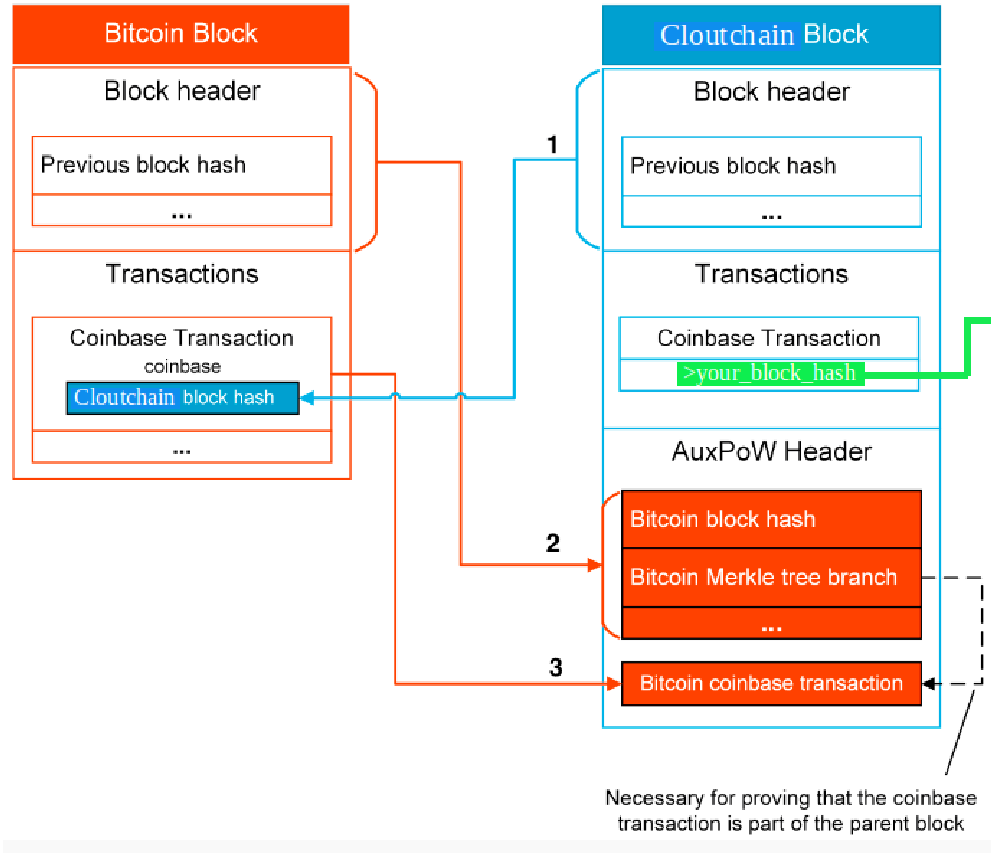


Diagram [7]

In Merged-merged Mining there are 3 different blockchains running in parallel: The Parent Blockchain, The Cloutchain, and The Identity Blockchain. The slight nuance is that the Auxiliary Blockchain (The Cloutchain in this case) is *in a sense*, itself Merged mining an identity blockchain. The way in which The Cloutchain Network accepts a valid identity block is by including it's hash within a Clout blocks' coinbase transaction, or 'The Cloutbase Transaction.'

For clarity's sake we'll illustrate the concept using Bitcoin as the Parent Chain, the identity block hash is labeled >your_block_hash (in green):



(Previous diagram slightly altered to illustrate Merged-merged Mining)

There is a 6 block (bitcoin) differential between the submission of an identity block to The Cloutchain Network and the collective updating of Cloutbase Transactions to include an identity block's hash. This differential rule ensures that determining the validity of an identity block is binary, and easily agreed upon by all miners, as the block header's timestamp is either valid or not.

That is to say, Cloutchain miners must wait until they are working on exactly the Clout candidate block who's timestamp is more than *6 bitcoin confirmations* ahead of the identity block header bitcoin occurrence proof before updating their Cloutbase Transaction with the proper hash. If a miner solves a Clout block without updating their Cloutbase Transaction when they should have, their block will be rejected by the network.

While Cloutchain miners must initially wait for two valid identity blocks to begin (they must validate the genesis block rule), mining becomes fluid thereafter. If an invalid identity block is submitted, then miners simply do not update their Cloutbase Transactions. Invalid identity blocks do not impede the processing of Clout transactions. Similarly, if the exception to the block time limit rule is ever needed, Cloutchain mining continues using the last valid identity block hash until two more valid blocks are submitted and the second block hash is to be used.

The significance of The Cloutchain Network can not be understated. More important than the distribution of the supply of Clout or processing of Clout transactions is the networks consensus as to the validity of identity blocks. The Cloutchain Network attests to the fact that the TSN Protocol rules were followed in the process of building an identity blockchain. As a byproduct of the acceptance of identity blocks, content is buried under proof of work which would be nearly impossible for a content creator to attempt to undo. This is also another existence proof.

9. Lightweight Addresses and Server Feeds:

TSN Addresses require a Block Publishing Server. Alternatively, ‘Lightweight Addresses’ do not and provide a quick and easy way to get involved in The Truth Social Network. Lightweight Addresses are server-less, use as needed addresses. They can be used as throwaway accounts, reused to develop a reputation, or even eventually used as a TSN Address.

Since Lightweight Addresses can not produce signature pages, instead they ping digital signatures themselves to a TSN Address as replies. There is of course, no guarantee that replying to a reference will make it onto the recipient’s BPS, but if it does you will gain exposure to their audience. If your reply merits interaction, there’s a decent chance it could eventually lead to the creation of a TSN Reference by the recipient, thus forever embedding the state in their historical record. Further, you will always have proof of the thread, which could be published to a Server Feed. There are various different kinds of feeds that could be created, each of which would fulfill a different role.

The first kind is a link-based feed. These feeds are low-overhead servers dedicated to sharing and curating TSN References. These servers could simply provide screenshots which directly link to TSN Reference signature pages. You would not need to have a TSN Address to run one as the references are already embedded in the historical records of their creators. References could be tipped with *anyone’s* Clout. With that said, it wouldn’t be surprising to see TSN Addresses run these as a separate part of their BPS, or simply share individual references on their own feed in this manner from time to time.

File-based Server Feeds could enable the aggregation and indexation of content in a searchable database. These servers would be expensive to run and thus would be mainly profit motivated. There are many benefits to these servers as compared to traditional social media. They would have their own identity blockchain and Cloutchain, thus by uploading content to these servers, the record of such would be embedded in their historical record. No password-based authentication would be necessary. And there would be a competing marketplace offering a range of services.

In terms of the mechanics of it, file-based servers could create a placeholder TSN Reference each day. Prospective users would be provided with a page which contains a Clout Address for proof of payment, a drop-in space to upload their file, and the ability to enter a refund address. After completing those steps (price would likely be based upon size and filetype), users simply reply to the placeholder reference including the file name and hash within their message. Administrators would then verify the integrity of the file, that it adheres to their user agreement, and that the Clout payment was received. Finally, administrators reply to the reply with a TSN Reference.

TSN Addresses get the benefit of backing up their files on a separate server. Lightweight Addresses additionally get the benefit of embedding a record of their content in an identity blockchain. It could be a great way to seek out up and coming users of the network and allows those users to be tipped in the Clout of the feed.

Node-based Server Feeds, in a sense, run a node of a collection of TSN References on a separate server. In the case of Git Truth, these could be community oriented feeds which mirror projects or repositories. On the other hand, there could be nodes of encrypted references hosted for use in for-profit apps. Or a node-based feed could possibly be used for something like a podcast index.

10. Conclusion

We propose a system where content creators designate a Public Address to serve as the basis for their online identity. Digital signatures provide message integrity and ensure that all content is irreversibly and provably attributable to a particular identity. There is no need for trusted third parties who authenticate users by storing passwords in centralized databases. Accounts are opened, closed, and managed from this identity enabling the creation of a known, public record updated in real time and observable by all. The ability to manage traditional social media Accounts using this identity lowers the reward for hacking as those accounts can be denounced from a separate server. The application of protocol rules such as the alternation of existence proofs and occurrence proofs as well as other nuances help foster fairly reliable timestamps. Content fingerprints are committed to blocks which are proposed to an independent network of miners. This network of miners attests to the fact that all the protocol rules were followed and buries content under proof of work making it nearly impossible for a content creator to attempt to alter or modify their past historical record.

References

[1] Merged-Mining.mediawiki,
https://github.com/namecoin/wiki/blob/master/Merged-Mining.mediawiki.

[2] A. Hertig, “Julian Assange Just Read Out a Bitcoin Block Hash to Prove He Was Alive,”
https://www.coindesk.com/julian-assange-just-read-bitcoin-block-hash-prove-alive.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer Electronic Cash System,”
https://bitcoin.org/bitcoin.pdf, 2008.

[4] C. Lee, “Litcoin,”
https://litecoin.org, 2011.

[5] P. Todd, OpenTimeStamps
https://OpenTimeStamps.org, 2012.

[6] A. Back, "Hashcash - a denial of service counter-measure,"
http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] Tari Labs University “Merged Mining Introduction”
https://tlu.tarilabs.com/merged-mining/merged-mining-scene/MergedMiningIntroduction.html