The Bitcoin Social Network

@everhusk

January 21st, 2024

Abstract

A decentralized system is proposed to resolve the escalating transaction costs for Bitcoin transactions, from increasing demand in extra information being saved on the Bitcoin Network. This system intends to minimize the transaction fee (satoshis/byte), finalty times, and node storage requirements on the Bitcoin network, without a centralized architecture. By utilizing recent Bitcoin Taproot and Ethereum upgrades, transaction can be bundled into succinct zero-knowledge proofs on Layer Two Rollups, dramatically reducing the burden on the Bitcoin blockchain, leading to much faster, more affordable, and much less energy intensive transactions. Additionally, by utilizing Nostr compliant event signatures, a trusted and efficient way of storing large amounts of off-chain data, linked to on-chain transactions on the Bitcoin network can minimize the burden of regular Bitcoin node operators. This is accomplished through a series of already proven cryptographic techniques and audited smart contracts that impose proper behavior and protect against abuse. By integrating Bitcoin, Ethereum, and Nostr, this decentralized system makes every effort to revolutionize the cryptocurrency ecosystem, making it much more scalable, affordable, and resistant to congestion, ultimately unlocking the potential of decentralized social networks on Bitcoin, for a much more united Earth.

1 Bitcoin Mining

In 2009, the Bitcoin [1] consensus algorithm, known as Proof of Work (PoW), unlocked an innovative new decentralized approach to verifying and recording transactions using a blockchain. Miners compete to solve complex mathematical puzzles, and the first to succeed adds a new block to the chain, making it extremely secure against fraudulent activities and coercion. Bitcoin has successfully demonstrated its ability to revolutionize money, finance, and asset ownership for the 21st century. However, this innovation comes with significant energy requirements as miners require substantial computational power which could be used for other societal functions. Although, scaling solutions for Bitcoin like Lightning Network enable faster and cheaper transactions in certain fee rate environments, it does not address the new demands for on-chain media.

Bitcoin's new scalability limitations pose a significant challenge, and opportunity for it to unlock additional utility for humanity scale trust. As more information based applications (i.e. Ordinals), are built on the Bitcoin blockchain, its unaffordability, slower transaction processing times and increased fees, may hamper its effectiveness in serving as a robust platform for these uses. Addressing these scalability concerns will be crucial for unlocking Bitcoin's utility in the 21st century, by ensuring the most valuable resource on the internet, data, can also be available on Bitcoin.

2 Ethereum Staking

In 2022, the second most used blockchain, Ethereum [2], upgraded to a Proof-of-Stake consensus system and now relies on validators, who are selected to create new blocks in a deterministic manner, often based on factors such as their "staked tokens" and performance in validating blocks. Additionally, by using Layer 2 solutions like zero-knowledge rollups, which offload transaction processing from the mainnet, Ethereum has become 99 percent more energy efficient, with lower transaction fees, and now accessible for a wider range of applications.

Since the upgrade, roughly 90 percent of ETH staked is done through 'Liquid Staking' protocols. These protocols enable anyone with any amount of ETH to deposit to a smart contract, and delegate the complexity of running Validator nodes to experienced operators. Layer 2 rollups have further

enhanced the scalability of the Ethereum network by processing over 1B transactions off-chain or on a separate chain at 10-100x lower fees, while still ensuring the security of the Ethereum mainnet.

3 Bitcoin Staking

Bitcoin Staking reduces the sats/byte fees to enable on-chain media without burdening everyday Bitcoin node operators, increases the time to finality to make Bitcoin more acceptable for everyday uses, and removes the high energy demands to satisfy the environmental concerns of Proof-of-Work. This section provides a high level overview of how this can be achieved while maintaining a decentralization.

3.1 Transaction Fees

The fees on the Bitcoin mainnet can fluctuate greatly depending on—depending upon the network's workload and market conditions. These fees are typically expressed in satoshis (0.00000001 BTC) per byte and determine how quickly a transaction is processed. Historically, when the network is peaceful, fees have be less than 10 sats/byte. However, during periods of high demand for Bitcoin blockspace, such as a bull market or heavy network usage, fees can skyrocket, in recent cases with Bitcoin Ordinals, exceeding 1000 satoshis per byte.

Storing large files on-chain would certainly require substantial transaction fees, making it economically unwise for most users, nonetheless, despite this limitation, there has actually been a clear demand for making use of Bitcoin's blockchain for on-chain media assets (i.e. Bitcoin Ordinals). On-chain media offers distinct ownership records and can represent digital art, collectibles, or other forms of digital assets. These digital assets make use of Bitcoin's security and decentralized nature for provenance and scarcity verification, even if the actual media content is stored off-chain or organized elsewhere.

Nostr[3] provides a simple and functional solution for attaching large scale information storage networks to Bitcoin, allowing creators to utilize the security and decentralization of the Bitcoin blockchain while avoiding the high on-chain storage costs. This approach facilitates the growth and adoption of additional utility on Bitcoin, satisfying the demand for unique digital assets while maintaining the Bitcoin network's performance and cost-effectiveness.

3.2 Finality

On Bitcoin, transactions are considered finalized when they are included in a block by miners. Each additional block added to the blockchain enhances the degree of confidence that a transaction is irreversible, with six confirmations being commonly accepted as a standard for high security. Mainnet block times are on average 10 minutes, and in some cases up to 2 hours, making it unfeasible for most mainstream user applications to use Bitcoin without a scaling solution.

Bitcoin Staking deposits are initiated by making a Taproot transaction [4] with the amount of Bitcoin being staked as the amount sent, a taproot script transaction which includes the users deposit address, the destination chain id, signed with a valid Nostr key which can be submitted to Bitcoin Staking operators via NIP-22. This transaction will take a maximum of 2 hours (worst case Bitcoin block times), and an additional 2 hours x 6 blocks = 12 hours to achieve sufficient confirmations to be deemed finalized.

Once a stake transaction has been safely finalized, this triggers Bitcoin Staking Operators to create a multi-party threshold Schnorr Signature [5] mint request which is submitted via Ethereum Light Client to create a wrapped version of Bitcoin on layer two Ethereum Rollup networks, reducing further transaction finality speeds to under one minute or less, while keeping the same degree of security as the Ethereum mainnet. An implementation of this is provided in later sections.

3.3 Energy Efficiency

The amount of energy used by a single Bitcoin block can differ greatly and is influenced by various factors such as the difficulty level of the network, the effectiveness of the mining equipment employed, and the price of electricity in the mining location. It is generally believed that the energy consumption of one Bitcoin block typically falls between 300 MWh to 500 MWh or even higher. It is important to note that open source incentives to create low cost, self sovereign, off-grid energy systems, will likely

lead to faster solutions for the clean abundant energy, than poorly implemented, designed, yet enforced government based incentives.

Nonetheless, when Bitcoin is staked on a Proof-of-Stake Ethereum rollup, the amount of energy consumed per block is greatly reduced. Researchers estimate that the Ethereum blockchain enhances transaction energy efficiency by around 53,000 times, resulting in an impressive annual energy savings of 149 TWh. Without a functional Proof-of-Stake or another scaling solution for Bitcoin, this figure will keep rising, exerting additional pressure on our energy-limited global economy.

4 Security Requirements

The security model of Bitcoin Staking is dependant on three pillars, transparency, self custody, and decentralization, which are discussed in this section.

4.1 Transparent

Individuals must have the ability to verify that the number of Staked Bitcoin in circulation accurately matches the amount of Bitcoin held in the threshold security deposit address. 24/7 third-party audits and transparency in operations are important for building and preserving user trust.

This is achieved by producing a singular Bitcoin Taproot [4] deposit address, which consists of a multi-party computation of all Bitcoin Staking Operators off-chain. The Bitcoin Staking deposit address will be made transparent, and publically available for tracking over hundreds of open source and free to use bitcoin blockchain explorers and wallets. Along with the addition of tools like Chainanalysis and other on-chain monitoring systems, this address can effectively be actually observed 24/7/365.

4.2 Self Custodial

Staked Bitcoin, must only be accessible to the user holding the keys to the staked bitcoin, or the corresponding staked asset on layer two networks. Staking Validators, must only exist to facilitate the locking/unlocking, but never be able to redeem any assets from the staking pool.

This is achieved using the following 2-Phase Bitcoin Taproot Script, which ensures that Bitcoin Staked assets are accounted correctly by indexers.

```
OP_FALSE
OP_IF
  OP_PUSH sn
  OP_PUSH 7
  OP_PUSH [stake || unstake]
  OP_PUSH 0
  OP_PUSH [event_id]
OP_ENDIF
```

Indexers MUST listen to blocks for these events, ensure user signatures are valid, and commit their part of the MPC signature to earn Bitcoin Staking incentives. This protocol remains compliant with Bitcoin Ordinals indexers, increasing data availability to the end users, discussed in Section 7.

4.3 Decentralized

At it's peak, the demand for Bitcoin linked to other consensus algorithms reached a total amount of over 400,000 BTC, or nearly 10B at the time of writing. The majority of these Bitcoin were linked largely making use of centralized custodians or falsely marketed decentralized 'bridges'. Centralized options for Bitcoin Staking are simple in nature, however pose systemic risk to the future of decentralized money and finance. These links work by sending Bitcoin to a single entity, who operates exclusive rights to mint and and burn a wrapped Bitcoin on the destination network.

To date, several billions of dollars of users BTC has been lost to centralized custodians and or in-sufficiently secure, decentralized linking of Bitcoin to other networks. Poorly architected bridges have accounting for 70 percent of all hacks in the Decentralized Finance (DeFi) in 2022 alone, and remain the number one security priority of cross-chain digital assets. Some examples of this include,

WormHole (300 million), Harmony Bridge (100 million), Ronin Bridge (625 million), and the Binance Bridge (100 million—thousand). Additionally, centralized staking operations would result in potential coercion of staked assets by unaligned actors.

Bitcoin Staking, utilizes Threshold Schnorr Signatures (TSS) to attain sufficient decentralization of asset control, TSS over schnorr signatures makes it possible for a network to collectively generate a digital signature without revealing the private keys to each, and efficiently scale the number of participants in this signature up to a desired level of decentralization. This cryptographic technique is used widely in production by the worlds largest Bitcoin custodians and exchanges, which removes the need for a additional op-codes, hard forks, or use of experimental cryptographic zk schemes on Bitcoin.

5 Security Analysis

We assume the hardness of the discrete logarithm problem in a cyclic group G of prime order q. That is, given g and h in G, it is computationally hard to find x such that $g^x = h$

```
Bitcoin Threshold Schnorr Signature Scheme:

Setup:

Choose a large prime q.
Select a generator g of the cyclic group G of order q.
Randomly choose private keys x_1, x_2, ..., x_t for t participants.
These keys are kept secret.
Compute the corresponding public keys
y_1 = g^(x_1), y_2 = g^(x_2), ..., y_t = g^(x_t).

Signing Phase:

Given a message m to be signed, each participant i computes the following:
Choose a random nonce r_i from a uniform distribution in the range [1, q-1].
Compute R_i = g^(r_i) mod q.
Compute e_i = H(m, R_i) for a random oracle H.
Compute s_i = (r_i + x_i * e_i) mod q.

Combine Signatures:

The combined signature (R, s) is computed as follows:
R = R_1 * R_2 * ... * R_t (mod q).
s = s_1 + s_2 + ... + s_t (mod q).

Verification Phase:

To verify the combined signature (R, s) for a message m:
Compute e = H(m, R) for a random oracle H.
Verify that g^s = R * y_1^e_1 * y_2^e_2 * ... * y_t^e_t (mod q).
```

To prove the security of this threshold Schnorr signature scheme, we need to demonstrate two properties, unforgeability, and privacy.

The scheme preserves the privacy of the private keys of individual participants. Even when multiple participants collaborate, they do not reveal their private keys. Additionally, an adversary cannot forge a valid signature without access to the private keys of at least one participant. This property relies on the hardness of the discrete logarithm problem.

These properties have been proven for the Schnorr signature scheme in general, and the threshold Schnorr scheme maintains these properties as long as the underlying discrete logarithm problem remains hard.

6 Data Availability

Once Bitcoin has been staked to the destination layer two rollup, the remaining challenge becomes how to ensure rollup transactions are made available for fraud proofs, without relying on centralized sequencers. This data availability problem is a fundamental challenge in the context of Zero Knowledge (zk) rollup scaling solutions. zk-Rollups aim to improve the scalability of blockchains by offloading most of the computation and transaction processing to a secondary layer while maintaining the security and decentralization of the underlying network consensus.

In a zk-rollup, only the proof of the correctness of transactions is actually submitted to the main blockchain. The actual transaction data, including the inputs, outputs, and state changes, is actually not featured on the main blockchain. Similarily, the Bitcoin Social Network makes uses of this, and expands data availability problem by creating a robust network for any types of blockchain data storage including media, and simply provides the correct guarantees and pricing mechanisms for any type of transaction linked data on Bitcoin, which can extend to any Ethereum virtual machine. The primary aim of the Bitcoin Social Network, therefore is to ensure transaction linked data is not lost, unavailable, or tampered with, as it becomes impossible to reconstruct the state of the zk-Rollup as well as verify its correctness.

6.1 Decentralized Data Availability

To solve the data availability problem, The Bitcoin Social Network makes it possible for anyone to append any type of arbitrary data based on the users Staked Bitcoin balance, and data will continue to be available for as long as the Bitcoin is staked, if demand is sizable enough for accessing this data, determined by the incentives, it will earn the Bitcoin Staking Operators additional staking revenue based on the highest value network operations, ensuring it remains accessible with the correct free market mechanics.

Bitcoin Staking reduces the costs of storing data on the Bitcoin Social Network by at least 3 orders of magnitude, scaling Bitcoin to support fully on-chain social networks would require a substantial increase in its data storage capacity as well. To do so Bitcoin Staking deposits are linked with a Nostr compliant event signature, and by doing so, instead of using the Bitcoin blockchain directly, Bitcoin is used to record metadata about the stored data, such as timestamps, owner addresses, and references to where the data is available, in a Nostr compliant signature.

6.1.1 Staking Event

When a user makes a sn stake signature and submit it to the relayer to increase HEART balance, the relayer must submit it to the bitcoin node and wait for indexer to confirm it, which triggers the ERC mint threshold signature. Wait for 7 blocks to confirm.

6.1.2 Post Event

When a user submits a sn store event signature and event data linked to the tx. Relayer confirms validity, submits tx to BTC, and stores event to local db with a free storage budget maximum of 7 megabyte-days. Stored items budgets will be updated daily and deleted if the budget ¡0. Heart type events must be stored and never deleted, unless included into Ethereum mainnet (event type of delete).

6.1.3 Delete Event

When a user submits a sn store event signature and event data linked to the tx. Relayer confirms validity, submits tx to BTC, and stores event to local db with a free storage budget maximum of 7 megabyte-days. Stored items budgets will be updated daily and deleted if the budget ¡0. Heart type events must be stored and never deleted, unless included into Ethereum mainnet (event type of delete).

6.1.4 Heart Event

When a users submit sn heart events which includes the event to heart, requires evm signature, the relayer submit heart events to Ethereum rollup sequencer.

6.1.5 Unstake Event

When a user makes a sn stake signature and submit it to the relayer to increase HEART balance, the relayer submits to bitcoin node and wait for indexer to confirm it, which triggers the ERC mint threshold signature. Wait for 7 blocks to confirm.

The benefit to this architecture is that users can easily migrate their data and profiles between different decentralized social networks, reducing the risk of vendor lock-in and giving users more freedom to choose where they want to engage online. It also enables different fee markets to be created around Bitcoin Staking and Nostr Relay networks, such that no central entity is ever in control of the network, limiting the ability for anyone to censor or control the entire network, and for countries or communities to create their own private social networks while using the same public infrastructure.

7 Incentives

As the world's foremost decentralized ledger, Bitcoin offers to optimal market for global information. Its resistance to coercion means that we can establish a market where data is valued and exchanged based on its true worth, free from external manipulation, with no pricing disparity across the vast array of human social structures. By linking Bitcoin to decentralized social networks, it can ensure data is not only secure but also valued accurately. This system would empower all races, religions, and conscious actors on Earth, giving any actor in the global economy control over their data and its worth. This section overviews the incentives of Bitcoin Staking, HEART, and the Social Network, EARTH, where value of data is determined by the collective, unfettered by the constraints of traditional centralized systems.

7.1 Staked Bitcoin (stBTC)

The loss of trust in global financial and governance systems can, in extreme cases, lead to social chaos. As the fundamental value of currency and the reliability of economic, governance, and other critical social institutions come into question. The balance lies in ensuring that inflationary policies are transparent, accountable, and reflect the needs and desires of the broader society. For Bitcoin to prove its utility beyond a store of value, it should also be able to solve the real world global social problems that humanity faces today and will face in the future.

When a user stakes Bitcoin, they recieve Staked Bitcoin (stBTC) for every BTC staked to the Social Network, which can be used to pay for inscriptions (images, videos, and other media) to Bitcoin via Earth Nodes. In addition to new stake Bitcoin events, stBTC token will rebase the total supply based on the revenue generated to the network, which can come in many forms, initially via data storage fees, and other rewards. This architecture can easily expand to additional functions of the decentralized markets, such as BTC, ETH, and other token swaps as required. Additional use cases for stBTC token such as can be unlocked via full EVM compatibility on the Ethereum blockchain, which has surpassed over 1 Trillion in DeFi trading volume, and a growing Regenerative Finance industry as well.

7.2 Social Network (EARTH)

The major limitations of data availability networks are that data may be removed from the network if there are no active nodes storing it, retrieving data can be slower compared to centralized CDNs, and replication of data globally requires higher costs, to pay for global data replication and additional bandwidth associated with distributing data across multiple locations. The Social Network solves this by keeping data localized to where the users have chosen to stake their Bitcoin, ensuring they do not require the entire network to be online, only those local to them. This data architecture allows global societies to store data important to their culture, by creating content policies of their own choosing, and avoiding control and information manipulation by social network platform operators.

As a public good, the Social Network (EARTH) will be fair launched, no venture capital or presale was conducted. 1/3rd of rewards will be available to Bitcoin stakers, 1/3rd to Earth Node Operators, and 1/3rd available to early Social Network app developers and creators, who can help build new incentive systems to re-connect humanity with nature, and regenerate planet Earth.

8 Conclusion

Today, humanity stands at a the precipice of a new digital era, facing a very real challenge of how we manage, share, and connect to stay grounded in reality. The current landscape of social networks is fragmented and often under the influence of centralized entities. However, the Bitcoin Social Network proposes a revolutionary solution: leveraging the power of Bitcoin to create a truly free and transparent market for data.

As the world's foremost decentralized ledger, Bitcoin offers us an unprecedented opportunity. Its resistance to government intervention and coercion means that we can establish a market where data is valued and exchanged based on its true worth, free from external manipulation. And similarily as a beacon of innocation, Ethereum can help ensure that data is not only secure but also valued accurately. This system would empower users, giving them control over their data and its worth. It's a vision of a digital ecosystem where value is determined by the collective, unfettered by the constraints of traditional centralized systems.

In addition to reducing Bitcoin transaction fees by 2 orders of magnitude, increasing finality by an order of magnitude, and reducing the energy consumption of Bitcoin transactions by 99.9 percent, the Bitcoin Social Network represents a significant breakthrough by uniting both the Bitcoin, and Ethereum communities, in a decentralized and secure manner, to expand the potential of decentralized money to all forms of decentralized information, and present a new solution to very real societal problems.

In this new era, the power shifts back to the individual. Your keys, your coins, your data. Let us embrace this opportunity to redefine the digital landscape, and unite around a new system - one which promotes fairness, freedom, and peace for all life on Earth.

References

[1] S. Nakatmoto, "Bitcoin: A peer to peer monetary system." https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform." https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf.

[3] Nostr, "A simple, open protocol that enables a truly censorship-resistant and global social network." https://nostr.com.

[4] P. Wuille, J. Nick, and A. Towns, "Taproot: Segwit version 1 spending rules." https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki.

[5] P. Wuille, J. Nick, and T. Ruffing, "Schnorr signatures for secp256k1." https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki.