# Bitcoin (Blink) - A Scalable & Adoptable Peer to Peer Cash System

Joby Reuben
jobyreuben@gmail.com

Purva Chaudhari
purva@example.com

**Abstract**

Bitcoin's PoW is replaced with a propagation competition on blocks sent across validators under a certain time interval stamped with cryptographic proofs to claim fees and solve forks as per proof weight. To bring adaptable scalability the block sizes are decided on consensus among elected nodes of specific epochs to decrease waiting transactions. Gossip systems are replaced with a privacy-centered direct messaging system by constructing encrypted paths to deliver unconfirmed transactions & confirmed blocks. Aside from bringing speed, we resolved the need for a single transaction fee token for a blockchain by bringing forth a novel non-custodial per-token staking system to offer users to pay in any token. Bitcoin as a currency will hold the security of the network, Layer-1 tokens with staking and yielding fees. Since Bitcoin script adapts a Turing-incomplete language and doesn't involve loops, the fees are imposed for renting UTXOs which makes transactions cheaper and the chain's ledger size optimized. We propose solutions for regulation revolving around taxation within the self-custody wallet ecosystem without compromising users' privacy.

## 1 Introduction

Bitcoin Network and other altcoin blockchains with newer consensus and programmable money are unable to compete with centralized payment providers in volume due to their sheer nature of inability to scale. Rules imposing heavy reliance on users acquiring chain native tokens are declared to be unuseful and hide the wonders of blockchain technology for different regions of the world. Decentralized networks can effectively adapt to users' needs by 1. Increase Block Size 2. Decrease Block Time 3. Eliminate Low Efficient Nodes 4. Increase Joining Requirement. Retail Staking with non-custodial solutions encourages users to stake their Bitcoin to become a world reserve currency for every financial instrument with an additional decentralized restrictive monetary policy that helps to reduce volatility similar to central bank currencies.

Instead of storing UTXOs for an indefinite time which compromises storage, renting UTXOs and replacing them with a fingerprint without altering the block's Merkle root will provide cheaper fees. With Bitcoin unlocking script developers can create regulatory options involving various types of taxes within its UTXOs, offloading identity verification off-chain, with signatures instructing nodes to validate regulated payments with self-custody of tokens. Basic Banking solutions can be developed in Bitcoin Script whereas common computable programs can be deployed to Layer 2 EVM State Machine which updates the state by providing a Proof-of-Fee-Receipt paid in Bitcoin Layer.

## 2 Block Requirement

Block size, time, VoC, Bandwidth, Election

## 3 Staking

Staking Requirement, Conditions, Non-custodial Delegation, Stake Per token per node, onetime usage, No Pools

## 4 Regulation

UTXO Taxes, Types of Taxes, Script Level, Bitcoin Satoshi Vision Opcodes, sCrypt, Offchain Validation, Client Witness Signing

## 5 Messaging

Unconfirmed Tx, Network Graph, Psedonymous Identities, Path Finding, Encryption, Mempools

## 6 Propagation

Snips, Competition, Kamikaze Proof, Ring Propagation

## 7 Hash-Rewards

How rest Bitcoins are rewarded per hash, 21 million cap

## 8 Renting

Merkle Chain, Fingerprint, Expiry Value, Rent Rates, Transfer Fees

## 9 Tokens

Layer 1 Tokens, Bridging, Efficiency

## 10 Banking

Exchanges, Lending & Borrowing, Insurance, Mirrored Wallets,

## 11 Privacy

Ring CT, Ring Signatures

## 12 Cash

Layer 2 Cash System

## 13 Computing

EVM Layer with unique Proof of Fee receipt consensus model, removing EOAs, Balances, Purely for Logic and State update.

## 14 Maintenance

Active Development Funds, Validators commission, DAO setup