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

[WORKING-DRAFT]

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 with centralization issues. Rules imposing heavy reliance on users acquiring chain native tokens are adoption diminishing requirements which hide users 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 restrictive monetary policy that helps to reduce volatility at time of recession.

Instead of storing UTXOs for an indefinite time which compromises storage, renting UTXOs and replacing them with a fingerprint after it expires without altering the block's Merkle root, thus providing cheaper fees. With Bitcoin's unlocking script and use of sCrypt - a high level language, developers can create custom scripts with -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 Election

Block size denotes the size of data that can be propagated across every producer node on the Bitcoin network, hence it's success rate directly dependant on the Bandwidth each node allocates for confirmed blocks transmission. Block size is not capped, but fixed every n epoch which validates that every producer node on the network can send and receive the data size. Variable Block Size helps in scaling the network by increasing transactions per block if nodes upgrade and announce their bandwidth. Bandwidth's can be proved...@Purva

A vote can be taken across producer nodes if there are increase in unconfirmed transactions cannot fit into a block. The network in consensus can forbid low bandwidth producer nodes participating the election, thus increasing the joining requirement and capacity to hold more transactions. Votes can be published onchain by...@Purva

As Bandwidth plays major role in scalable infrastructure, nodes are required to have better of it to achieve maxium production rate per epoch, as elections will be conducted based on it and each node's honesty weight. Every Node willing to participate in the next epoch block production, identity is given in its public keys published to the ledger onchain for definite calculations.

To randomize the random seed which commences election, shall be identified from epoch's range of block's (n-m) Block Merkle Chain Root which is constructed by validators

Predictable Election Result, Producer Signature

3 Staking

Bitcoins can be staked for node public keys with specified token id where the collateral can be used only once for a block. This results in stake per token per block. Each tokens per block collateral requirement is given in exchange rates by taking the median volume of all the blocks of the previous epoch. Staked Bitcoins can be withdrawn anytime, without vesting period except at the time of producing block bringing retail and non-custodial solution as opposed to security deposit type PoS chains. Bitcoins can be staked to a specific node which choses to include the stake by collateralizing or locking in its allocated block. Additionally a new collateralized stable coin can be issued which can be used for staking benefits where other decentralized altcoins can be utilized to receive yields.

4 Regulation

UTXO Taxes, Types of Taxes, Script Level, Offchain Validation, Client Witness Signing, Oracles

5 Messaging

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

6 Propagation

Snips, Blinks, Legates, Blink time, Competition, Kamikaze Proof, Hash clocks, Ring Propagation, Node Weight

7 Rewards

How rest Bitcoins are rewarded per hash, 21 million cap. Rewards limited for each hash, no tx no reward.

8 Renting

Merkle Chain, Fingerprint, Expiry Value, Rent Rates, Transfer Fees, Single UTXO, State Update

9 Tokens

Layer 1 Tokens, One-way Bridges, Proof of Burn, Creation of new tokens to transact one should stake for it.

10 Banking

Exchanges, Lending & Borrowing, Insurance, Mirrored Wallets, Decentralized Stable Coin

11 Privacy

Obscuring Amounts, Ring Signatures decryption by government

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. NFTs,

14 Maintenance

Active Development Funds, Validators commission, DAO setup, sustainability.