

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. Altcoins can be bridged one-way and collateralized for a stable coin directly used for staking and yielding fees along with Bitcoin bringing utility. 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. 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. As Bandwidth plays major role in scalable infrastructure, nodes are required to have better of it to achieve maximum 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 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. As slashing is done directly to fees, delegators won't loose their stakes. Bitcoins can be staked to a specific node which choses to include the stake by collateralizing or locking in its allocated block. In this way, for a specific token's transaction to be included in a block, the first transaction should prove the collateral. Additionally a new collateralized stable coin can be issued which can be used for staking where other decentralized altcoins can be utilized to receive yield benefits.

4 Regulation

Regulating cryptocurrencies via centralized exchanges & custodians risk funds and doesn't encourages self-custodial ecosystem. A regulator must have authority to sign/approve transactions. Whitelisting specific hashed addresses belonging to specific countries verified and signed by Government assigned Client Wallets or Regulators by either doing full KYC or minimal such as Mobile Number based OTP verification could work with maximum privacy. UTXOs are stamped with region proof on its unlocking script based on specific spending conditions that will only allow a transaction onchain if a taxes are deducted properly. Bitcoin scripts can work efficiently and securely as opposed to Turing complete smart contracts in this case. Tax models such as Capital Gains Slabs can be issued by governments independantly trustlessly and is validated in script execution. External taxes such as TDS, Sales tax can be imposed offchain independantly as its flexible to do so.

5 Messaging

Delivery of unconfirmed transactions to nodes play important role in finality. Shared Mempools colludes the network with duplicated data that results in poor choice of transactions to include in a block. Miners take only transactions with higher fees, hence deploying

a direct-messaging system with messaging instructions specific for each party as opposed to a gossip network. Paths are attached with unconfirmed transactions directly from the constructed network graph available to all nodes with publickeys as identities. Two peered parties mutually sign a 2-2 random message for every x blocks are gossiped across network and indentify the connection as online. From all the signed random messages proving each pubkeys signature can display a network topology map from the point of reference node. Paths have encrypted instructions and a secret number associated to each party's publickey that economically incentivizes (pay routing fees) and routes the transaction between the origin and the destination where the nodes can attach the transaction in their allocated block. Since the stake information are available publicly client Wallets constructing the transaction with path shall assume and select possible blocks that will add the transaction to it at the earliest. Nodes only receive the transactions which they need to include and client wallets should construct shorter paths to provide best user experience.

6 Propagation

A Block is collectively validated but constructed as snips - divisible block chunks by the producer and directly messaged to most of the current epoch's producer nodes with routing instructions to gossip across the network. Each snip references previous snip's hash similar to chain of blocks for proper identification of each block's snips. For a block of an epoch, a competition to deliver all snips under x time interval is required to win rewards and avoid slashing of fees. When a block fails to win shall be minted until its last snip which may contain rewards. VDF proofs are attached for every snip during routing to declare the state of each blocks competition after resolving forks based on proofs weights. Failed blocks fees are slashed by sending to a burn address by next block height producer in his first transactions before proving collateral for the block. For each failed block with various categories shall result in decreased block production for the node in next epochs indirectly slashes bandwidth costing capital which instructs nodes to act honestly with performance required for the epoch. Some of these negative weights are temporary, permanent and some weights are incentive as it increases its maximum achievable block production in next epochs. To synchronize time, each node's hashrate per second of a specific hash-function is proved cryptographically onchain and taken in multiples of a common hardware's hash-rate. This Individual hash-rate proof is also provided along with bandwidth proof for every epoch which trustlessly synchronizes all nodes as a single hardware producing continuous hashes concated with all snips provide cryptographic timestamped proofs to announce each epoch's block time under which all snips has to arrive and win the time-based propagation competition.

7 Rewards

Rewards are given for each snip hash as block time varies in this implementation to provide faster finality of transactions. Since a year's total newly minted bitcoins are definite and the common hardware's hash-rate per year is also definite used to synchronize various nodes hash-rates, new bitcoins can be supplied for each allocated blocks. From origin snip hash to final snip of a block, the total index of hashes is taken to validate total bitcoins the block can issue. While Tax outputs are attached as zero input transactions within the snip it contains, the fee outputs when accounted marks the end of the block. During staking producers announce their accepted tokens for which it will directly withdraw the commission. For other tokens, delegators can stake with a condition that their stake in bitcoins or the accepted stake token will be traded for the collected fees. During commission withdrawal of non-accepted tokens, the producer will deposit collected fees to delegators and inflate

the stake to LP token 1:1 ratio to withdraw the collateral. Users can pay in any token, delegators incur the risk and producers get paid to validate transactions.

8 Renting

Instead of taking merkle roots of all the transactions inside a block, a snip's merkle root is taken and linearly hashed to find the Merkle Chain root. Since, a snips can be rejected by validators, it is unsure to predict a merkle chain root gives it a purely randomized value. Inside a snip contains parsed transactions whose hashes are taken to find the snip's merkle root can be pruned if the UTXOs are spent, burnt, or expired. Each UTXOs expiry block height is embedded in its script, can be scanned by nodes, prune them to optimize their data storage. Client Wallets can store each of their users transaction history and can be audited onchain using merkle chain roots. Renting rates can be given in exchange rates (usd) independantly voted by producer nodes for every epoch per byte per block. Users cannot directly pay for rent, but rather each new UTXO created charged a transfer fee in range of 0.05% - 0.005% decided based on total volume settled on previous epochs. Transfer fee charges more fees for higher value utxos and less for lesser value utxos bringing ease of transacting for retailers. According to how much each utxo pays for transfer fee, an expiry date is set. UTXOs doing state updates will not be charged, and can combine UTXOs to single for increasing expiry value. This encourages users to store single UTXO per wallet reducing transaction fees and also incentivizes nodes, clients, etc.

9 Oracles

10 Tokens

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

11 Banking

Exchanges, Lending & Borrowing, Insurance, Mirrored Wallets

12 Privacy

Obscuring Amounts, Ring Signatures decryption by government

13 Cash

Layer 2 Cash System

14 Computing

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

15 Maintenance

For sustainability of the project and active development, the developers of project blink can set up a DAO for decisions involving protocol changes and softforks to register government tax wallets. Developers can be actively rewarded similar to a centralized organizations by levying a 15% commission on producer commissions where it is only charged when a producer wins the rewards. Only the accepted tokens and staked tokens are sent to DAO treasury.

References

Appendix

- A Bandwidth Proof
- B VoC Vote
- C Hashrate Proof
- D Election Seed
- E Tax Scripts
- F Block Requirement
- G Stake Script
- H Whitelisted PubKeys
- I Network Graph
- J Encrypted Path
- K Routing Reward
- L Destination Block
- M Time Proof
- N Slashed Fees
- O Resolving Forks
- P ●