



Project Blink

Decentralized World Bank

Blinkchain - Proof of Concept

<https://blinkchain.org>

[WORKING-DRAFT]

Joby Reuben, Auguth Tech Pvt Ltd

Contents

1 Objectives	1
2 Time Architecture [2.1]	1
3 Epoch Election	2
3.1 Bandwidth & IHR Proofs	2
3.1.1 Creating Proof (Node)	2
3.1.2 Attesting Proof (Script)	2
3.1.3 Selection of Proof (Node)	4
3.2 Vote of Confidence (Removal of Nodes)	4
3.2.1 Selection of Un-fit Nodes (Node)	4
3.2.2 Participation by Voting (Script)	4
3.2.3 Elimination & Result (Chain)	4
3.3 Producer Arrival	4
3.3.1 Repeated (Bandwidth Proof)	4
3.3.2 Selection of Proofs (Node)	4
3.3.3 Contestant Results (Chain)	4
3.4 Allocation of Leaders	4
3.5 Stake UTXO Creation	4
3.6 Block Size & Time	4
3.6.1 Proof Selection (Node)	4
3.6.2 Block Size per sec Fixing (Chain)	4
3.6.3 Block Time Fixing (Chain)	4
3.6.4 Per Block Size Fixing (Node)	4
4 Parent-Child Script	4
4.1 Price Oracles	4
4.2 Stake UTXO	4
5 Block Minting	4
5.1 Packet Clock	4
5.2 Collateral Snip	4
5.3 Transaction Snip	4
5.3.1 Local Mempool	4
5.3.2 Tx Validation	4

5.3.3	Vanity Addresses	4
5.3.4	Transaction Fees	4
5.3.5	Taxes	4
5.4	Coinbase Snip	4
5.5	IHR Verification	4
5.5.1	Hash-reward	4
5.6	Snip Messaging	4
6	Snip upon Receiving	4
6.1	Genesis Clock Spaces	4
6.2	Collateral Validation	4
6.3	Fee Validation	4
6.4	Tax Validation	4
6.5	Hash-reward Validation	4
6.6	CT Deal Validation	4
6.7	Position Update Validation	4
6.8	Kamikaze Proof	4
6.8.1	Pattern Identification	4
6.8.2	Construction	4
6.8.3	Attesting	4
6.8.4	Validation	4
7	UnConfirmed Tx	4
7.1	Propagation to Leader	4
7.2	Leader Segregation	4
7.3	Leader Transmission	4
8	Pruning UTXOs	4
8.1	Expiration & Fingerprint Replacement	4
8.2	Centralized Storage Boilerplate	4

1 Objectives

1. Whitepaper Section, Passive or Active Program & Level
 - Chain - Ledger,Consensus and Core Implementations
 - Script - UTXO scripts/proofs construction and attesting
 - OffChain - Client Side construction/propagation
 - Node - Validation, Ledger Outlook & Parameter construction
- 2.
3. Process, Algorithm and Mathmatical Data
4. Existing Implementations and Documentation References
5. Feasibility of Development & Notes
6. Technical & Non-Technical Challenges
7. Alternatives Offered and Outcome

2 Time Architecture [2.1]

- The Time Architecture in Blinkchain is segregated into Epoch = 10,000 blocks; Slot = 400 blocks ; Packet = 1 block.
- These time frames are not correlated to the ledger, as it only knows block heights. It is only taken in the following area
 - Election conducted every epoch (10,000 blocks)
 - Announcing Leaders for every Epochs, Slots and Packets
 - Taking Variable Data to form constraints in the consensus e.g., Total Volume in an Epoch, Each individual block time in an epoch/slot, etc
- Cardano, a UTXO based blockchain uses these timeframes, thus it is implemented and running <https://developers.cardano.org/docs/stake-pool-course/introduction-to-cardano/#slots-and-epochs>
- Its feasibility is proved with previous implementations and it does not affects or changes consensus protocols. As block heights are only taken for constraints, these time frames
 - Epoch, Slots and Packets are quasi and can be much more human readable. The alternatives would be reciting all constraints in block heights which cannot be developer friendly. The outcome can be achieved seamlessly.

3 Epoch Election

3.1 Bandwidth & IHR Proofs

3.1.1 Creating Proof (Node)

3.1.2 Attesting Proof (Script)

Legates

- 3.1.3 Selection of Proof (Node)
- 3.2 Vote of Confidence (Removal of Nodes)
 - 3.2.1 Selection of Un-fit Nodes (Node)
 - 3.2.2 Participation by Voting (Script)
 - 3.2.3 Elimination & Result (Chain)
- 3.3 Producer Arrival
 - 3.3.1 Repeated (Bandwidth Proof)
 - 3.3.2 Selection of Proofs (Node)
 - 3.3.3 Contestant Results (Chain)
- 3.4 Allocation of Leaders
- 3.5 Stake UTXO Creation
- 3.6 Block Size & Time
 - 3.6.1 Proof Selection (Node)
 - 3.6.2 Block Size per sec Fixing (Chain)
 - 3.6.3 Block Time Fixing (Chain)
 - 3.6.4 Per Block Size Fixing (Node)

4 Parent-Child Script

- 4.1 Price Oracles
- 4.2 Stake UTXO

5 Block Minting

- 5.1 Packet Clock
- 5.2 Collateral Snip
- 5.3 Transaction Snip
 - 5.3.1 Local Mempool
 - 5.3.2 Tx Validation
 - 5.3.3 Vanity Addresses
 - 5.3.4 Transaction Fees
 - 5.3.5 Taxes
- 5.4 Coinbase Snip
- 5.5 IHR Verification
 - 5.5.1 Hash-reward
- 5.6 Snip Messaging

6 Snip upon Receiving

- 6.1 Genesis Clock Spaces
- 6.2 Collateral Validation
- 6.3 Fee Validation