JAX coin - Proof of Value Mechanism

Vinod Manoharan *[1]

[1]JaxNet, Kyiv, Ukraine

June 22, 2021

Contents

*vinod@jax.net

1 Introduction

In Jax.Network, we have a mechanism to reuse the security of other SHA256 coins using merged mining without losing the unique value of our native stable-coin. We call this mechanism the Proof of Value mechanism.

2 How does it work?

Whenever someone merge-mines BTC along with Jax.Network beacon and shard chains, they get both BTC and JXN coins. JXN coins are the beacon chain coins of Jax.Network. Since, the main value proposition of the Jax.Network blockchain is the intrinsic stable-coin: JAX, we will need to ensure that it's economics is precise and that it is not printed simply as a part of defending the network. I.e We have to decouple the economics of JAX from the security incentives of the network.

Hence, we only issue JAX coins when the JXN reward and the BTC reward is sent to an invalid address. So, on the JAX shards (transactional shards), JAX block creation rewards can only be issued when the BTC and the JXN rewards are foregone / burnt. By utilizing such a mechanism, we are still able to defend the JAX shards by reusing the hashrate of the beacon shard, BTC (anchor shard) by incentivizing them with JAX tx fees only. In the event of miners wanting to print JAX coins, they will then have to burn BTC and JXN.

3 Technical specification

3.1 Coinbase transaction in Bitcoin block

Whenever a miner merge-mines a BTC block + Jax.Network, he is supposed to structure the coinbase transaction in the following fashion:

IF HE WISHES TO MINE BTC + JXN:

Table 1: Bitcoin block coinbase transaction outputs. Case 1.

Output	Amount of coins	Recipient address
1	0 BTC	https://www.jax.network
2	6.25 BTC	MINER_ADDRESS
3	BTC_TX_FEES	MINER_ADDRESS

IF HE WISHES TO MINE JAX:

Table 2: Bitcoin block coinbase transaction outputs. Case 2.

Output	Amount of coins	Recipient address
1	0 BTC	https://www.jax.network
2	6.25 BTC	JAX
3	BTC_TX_FEES	MINER_ADDRESS

Additional BTC COINBASE Validation:

No additional validation required.

3.2 Coinbase transaction in BC block

IF HE WISHES TO MINE BTC + JXN:

Table 3: BC block coinbase transaction outputs. Case 1.

Output	Amount of coins	Recipient address
1	0 JXN	https://www.jax.network
2	20 JXN	MINER_ADDRESS
3	JXN_TX_FEES	MINER_ADDRESS

IF HE WISHES TO MINE JAX:

Table 4: BC block coinbase transaction outputs. Case 2.

Output	Amount of coins	Recipient address
1	0 JXN	https://www.jax.network
2	20 JXN	JAX
3	JXN_TX_FEES	MINER_ADDRESS

Additional JXN COINBASE Validation:

i) Check if the JXN COINBASE 1st output is our network identifier:

https://www.jax.network

ii) Check if the JXN COINBASE 2nd output is equal to the block reward.

iii) Check if the JXN COINBASE 3rd output equals the sum of transaction fees of the transactions that were included in the block

3.3 Coinbase transaction in the shard block

Key:

- K is a K-coefficient of Jax.Network which can be obtained from the beacon chain. Read our K-coefficient paper for more information.
- D is the difficulty of the current shard chain.

IF HE WISHES TO MINE BTC + JXN:

Table 5: Shard block coinbase transaction outputs. Case 1.

Output	Amount of coins	Recipient address
1	0 JAX	https://www.jax.network
2	$K \cdot D$ JAX	JAXNET
3	JAX_TX_FEES	MINER_ADDRESS

IF HE WISHES TO MINE JAX:

Table 6: Shard block coinbase transaction outputs. Case 2.

Output	Amount of coins	Recipient address
1	0 JAX	https://www.jax.network
2	$K \cdot D$ JAX.	MINER_ADDRESS
3	JAX_TX_FEES	MINER_ADDRESS

Key:

- TRUE - Valid block
- FALSE - Invalid block

Additional JAX COINBASE Validation:

1. Check if the JAX COINBASE 1st output, BTC COINBASE 1st output, JXN COINBASE 1st output is our network identifier: https://www.jax.network
   a) If NO: return FALSE;
   b) ELSE: continue;
2. Check if the JAX COINBASE 3rd output equals the sum of transaction fees of the transactions that were included in the block
   a) If NO: return FALSE;
   b) ELSE: continue;
3. Check if the JAX COINBASE 2nd output was burnt to JAXNET:
   a) IF YES: return TRUE;
   b) IF NO: continue;
4. CHECK IF JXN COINBASE 2nd output was burnt to “JAX”
   a) IF NO: return FALSE
   b) IF YES: continue;
5. Check if BTC COINBASE 2nd output was 6.25 BTC and it was burnt to “JAX”
   a) If YES: return TRUE;
   b) If NO: continue;
6. Check if BTC COINBASE

$$\text{3rd output} \leq 0.5\,\text{BTC}$$

   a) IF YES: return TRUE;
   b) IF NO: return FALSE;

4 Pros & Cons

Table 7: Pros and cons

Pros	Cons
• Reduce the cost of security of Jax.Network. • Jax.Network comes under the control and protection of BTC miners. • Ensures that tx fees will be feasibly set instead of relying on block reward subsidy.	• JXN coin loses uniqueness and its value becomes dependent on the value of BTC. • Network could be attacked by BTC miners (We don't see any reason for a profit-motivated attacker).

5 Conclusions

In this paper, we have proposed a Proof-of-Value mechanism which we use in Jax.Network. We have concluded that:

- Any PoW BTC protocol based blockchain network like Jax.Network, BCH, BSV, etc. could reuse the hashrate of the BTC network without giving up the value of their native digital token.
- This Proof of Value mechanism helps reuse SHA256 hashrate and hence reduce the cost of minimum security of the network under the assumption of 51% honest SHA256 hashrate.
- We have specified how this proposed Proof-of-Value mechanism can be implemented technically.

Should you have any questions, feel free to contact us through our website:
https://www.jax.network