Azim Coin: Ring-based value over IP

shahiN Noursalehi
Private Curiosity Lab
coin.mixoftix.net

ABSTRACT

The human brain contains the most advanced consensus model, which is highly decentralized through its parallel processing neural units. Instead of competing to determine who solved the task first, these units share their jobs and solve them together, using dynamic routes among nodes with minimal power consumption. Although migrating completely from Proof-of-Work to a new proof model with such characteristics is challenging, drawing inspiration from the back-propagation process in training neural networks can guide us towards an innovative feed-forward approach. In this approach, each entity finalizes its duty and relays the result to the next step in the protocol, which we call Proof-of-Consistency. With these predefined conditions, there will be a virtual ring among master nodes for each block, responsible for continuously validating and broadcasting agreed transactions.

TYPE OF PAPER AND KEYWORDS

Short Communication: *blockchain, consensus, Persian Generals Problem, Zero Carbon Footprint*

1 INTRODUCTION

When people decided to enhance their commercial activities from basic bartering [1] by inventing money as a medium of exchange [2], they quickly discovered the problems associated with personal and social payment costs [3]. To address these issues, financial institutions were established to facilitate the process. However, this led to the emergence of payment providers within these institutions, exacerbating the problem. High social costs result in inflation, over-production, lower prices, unsold goods, and ultimately, increased unemployment rates in society. Therefore, an effective solution is needed.

Bitcoin also addresses this problem in its whitepaper [4], but nowadays the Proof-of-Work (PoW) model it employs involves significant power consumption by ASIC miners. This raises the question: what if there could be a peer-to-peer network of nodes that also targets payment costs, but achieves this with an almost zero carbon footprint?

Furthermore, central banks have made numerous attempts to introduce a digital version of fiat money (CBDC) [5] to reduce the aforementioned costs. However, these efforts often result in new forms of trust and related expenses, ultimately bringing us back to the same challenges.

2 ROOTS IN PSYCHOLOGY

The mediums of exchange we use stem from fundamental human needs that are not directly exchangeable. By examining Maslow's hierarchy of needs [6] and aligning its different stages with the evolution of mediums of exchange, we can see how money has facilitated transactions. For instance, exchanging a weather forecast for a farmer's milk addresses safety needs in stage 2. It is assumed that in the age of digital transformation, innovative mediums are needed to address the needs in stages 3 and 4.

Table 1: Maslow's hierarchy of needs

Stage	Needs	Example
1	Physiological	Air, Water, Food
2	Safety	Health, Finance
3	Social	Intimacy, Connection
4	Esteem	Strength, Freedom
5	Self-actualization	Goals, Talents

Table 2: Align proper mediums to needs

Stage	Needs	Medium of Exchange
1	Physiological	Bartering
2	Safety	Money
3	Social	Money over IP
4	Esteem	Cryptocurrency
5	Self-actualization	Curiosity

3 STRUCTURE OF NETWORK

PoW plays a crucial role in preventing Denial-of-Service attacks, but its use as a consensus mechanism needs to be re-evaluated. In Proof-of-Consistency (PoCo), we still utilize PoW as a safeguard at the infrastructure layer, but miners are no longer in competition to solve difficulties first. Instead, end users will specify their preferred miner entity and then sign their raw transactions. Once a miner solves the difficulty, it simply relays the result to a trusted master node. As a result, miners in idle time do not consume energy without having a job and reward.

3.1 Block Structure

To achieve the desired consistency, we have made four minor changes to the block structure: 1- Wallet Format 2- Flash Back Pinning 3- Ring Data 4- Shahin Go Round.

3.1.1 Wallet Format

Rapid advances in technology often carry consequences that can put older systems at risk of instability. To address this, we have included an identifier in wallets, as shown in the table below, to adopt new resistant cryptographic algorithms suited against AI and Quantum Processors:

Table 3: Wallet Format

Part	Contains	Meaning
1	azm	Azim Chain
2	A,B,C,..	RSA, secp256k1, nistp256,..
Upper Case = Main Net Lower Case = Test Net		
3	Integrity	Left 11 char of MD5
4	Public Key	Base58 (Sha256)

Table 4: Sample Wallet Address

```
azmC76df55329c3BW5FFbsBt5ruidwXqn43
      7H8xMaaXLqmEdPcdL2T6kUoN
```

3.1.2 Flash Back Pinning

An experiment about 51% attacks in blockchains reveals that the mempool is particularly vulnerable, as it allows for the misuse of raw transactions to generate fake blocks. In Azim Coin's flash-back-pinning [7], the hash value of the last known block must be included in the signing process. This ensures that all involved entities can detect any possible fork in the network and secure sufficient confirmation blocks in advance.

Figure 1: Making Mempool Useless for Attack

An attacker can't misuse mempool data to perform a 51% attack, and any such attempt would be immediately detected by the protocol.

3.1.3 Ring Data

In PoCo, a draft of raw block data is synchronized among participating master nodes through a temporary virtual ring. The protocol then asks each involved master node to generate its own edition of the new block. Since master nodes must sign system transactions (such as fees, parity, rewards, etc.) using a general system account, they should maintain the same structure in user transactions but have different structures for system transactions.

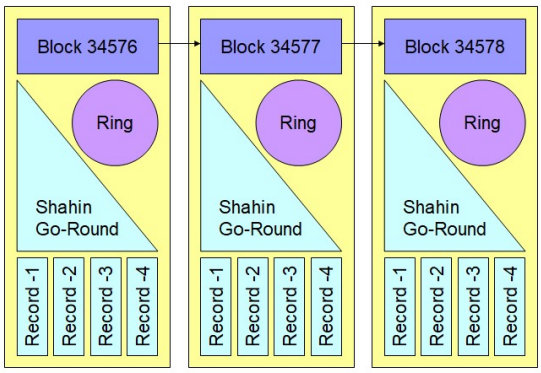

Figure 2: Block structure in Azim Coin

The section in each block that contains the list of signatures by master nodes will provide ring data for identifying the winning block among orphan blocks when a fork occurs. Different valid system signature values come from a unique predefined private key and its padding in the protocol layer.

Table 5: Protocol Built-in Private Key

```
Ba7jr3UZQDMY6HDPyDPuJPSLQRYQk3iZiadcZ9MGDcNf
```

This approach introduces a form of quantization, which can cause distortion among block data. In practice, we observe the Dither-Effect [8] across the entire blockchain, enhancing accuracy and consistency.

3.1.4 Shahin Go-Round

To handle a large number of transactions per block and higher block times, Azim Chain utilizes Shahin Go-Round instead of a Merkle Tree [9] for data chaining purposes. Shahin Go-Round employs a dual-linear flow that is also used in other parts of the project. For example, it can be used to sign values that represent a $20 transaction from Atoosa to Babak:

Table 6: Quantum Resistant Hash

Data	Positive	Negative
From	`Atoosa`	`20 USD`
To	`Babak`	`Babak`
Value	`20 USD`	`Atoosa`
Hashes	`8fda7fa2be025f..`	`cea136f7137755..`
Hash	`feb5fb76c478272d6a08d898ac1e7d42..`	

Now you sign the last hash (order hash) generated by a list of positive and negative hashes from the same data, making it more robust against collision attacks [10][11]. This can be compared to the differences between insertion sort (which takes time equal to C1 x N^2) and merge sort (which takes time equal to C2 x N x LOG[N]) algorithms for sorting N items. While insertion sort is typically quicker than merge sort for small input sizes, as the input size N grows, merge sort's factor (LOG[N]) increasingly outweighs the linear factor (N), eventually overcoming the constant factor differences (C1, C2). C1 and C2 represent the processing power of two different machines [12].

3.2 Structure of Transactions

In PoCo, there are three types of transactions that occur before becoming an approved transaction in a valid block: 1- Raw Transactions 2- Immature Transactions 3- Mature Transactions

3.2.1 Raw Transactions

To generate a valid raw transaction, you need to provide the following data and sign it:

```
(1){wallet_from}
(2){wallet_to}
(3){wallet_miner}
(4){dawn_script}
(5){the_order_amount}
(6){the_order_utc}
(7){flash_back_id}
(8){flash_back_md5}
```

Whoever mines this raw transaction will receive the protocol's reward. The dawn script refers to the capability of smart contracts in Azim Coin.

3.2.2 Immature Transactions

To generate a valid immature transaction, you need to provide the following data:

```
(1){the_order_hash}
(2){wallet_ring}
(3){block_difficulty}
```

Next, you need to find a `nonce_value` that, when appended to the `the_order_hash` and `wallet_ring` strings, satisfies the block_difficulty according to the principles of Proof of Work (PoW). Miner entities are responsible for finding the best route to the master nodes with better service stability, otherwise, they risk losing their rewards.

3.2.3 Mature Transactions

To generate a valid mature transaction, you need to provide the following data:

```
(1){proof_of_fork}
(2){ring_sign}
```

The `proof_of_fork` value could be the most remarkable aspect of the PoCo model. With this feature, after syncing all available immature transactions through a virtual ring among candidate master nodes, each one should then build its own version of the block data. They should sync the ring data with different `proof_of_fork` values derived from the protocol transactions and their signatures.

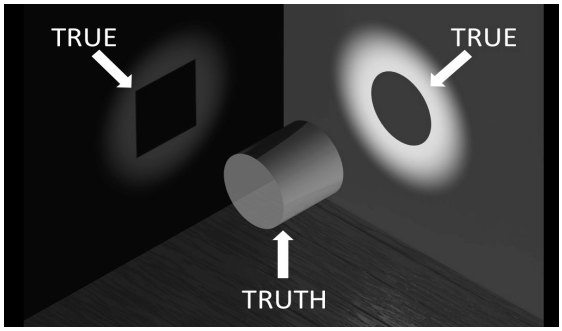

Figure 3: True Forks vs. Truth Fork

In classic blockchains, the linear view of hash algorithms forces us to select one true fork among several and call it consensus. However, by enforcing and rewarding each master node to create its own true fork and sync them as `proof_of_fork` to save as ring data in the block header, we ultimately achieve a unique Truth fork. This Truth fork is built upon several true forks from different directions and perspectives. This feature originates from the solution provided by

the Persian Generals Problem during the PoCo basic research process.

4 PERSIAN GENERALS PROBLEM

Following the Byzantine Generals Problem [13], the Chinese Generals Problem [14] elucidated how a trustless system could benefit from the fault detection in Ring networks. However, the model still suffers from single-content messages (Attack / Retreat), which are suitable for True Fork situations as explained above, but not for the new Truth Fork approach.

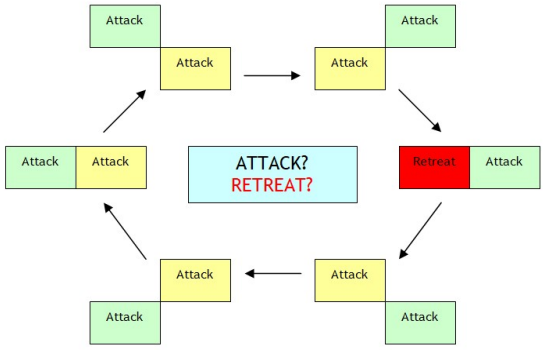

Figure 4: Data Flow in Chinese Generals Problem

Therefore, in the Persian Generals Problem, we have proposed a special data flow in the protocol layer where each general carries only one letter. After syncing through a ring, they can accurately recognize the final message and detect the betrayer general.

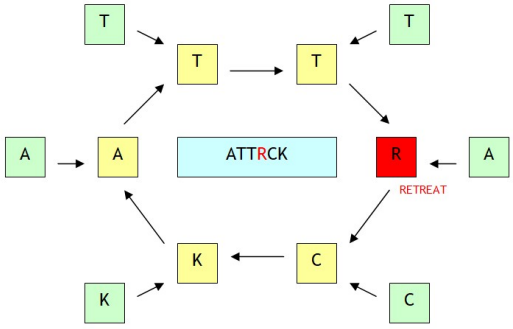

Figure 5: Data flow in Persian Generals Problem

5 INCENTIVES

After issuing a raw transaction by end users, miners are the first involved entities, responsible for creating the initial ring of security around the blockchain. A miner assigns a trusted master node, solves the requested block difficulty, generates an immature transaction, and receives the transaction fee directly from end users in return.

Miners need to engage in a marketing process to attract the most jobs from end users. They can use on-chain NFT services to identify their address as a miner or join a mining club that facilitates the marketing process.

At the next level, master nodes become involved and begin to sync immature transactions from other master nodes, creating their own proof-of-fork to complete the ring data and finalize a new block. In this scenario, any full node, by freezing the requested amount of Azim Coin, can become a master node. These master nodes are rewarded by the protocol for their involvement in making mature transactions and block generation.

In addition to the transaction fee, each transaction in Azim Chain includes a network fee. This network fee will be the main source of rewards for master nodes after blockchain calibration. The different fee policies ensure that it becomes futile for any responsible entities to create fake transactions for rewards.

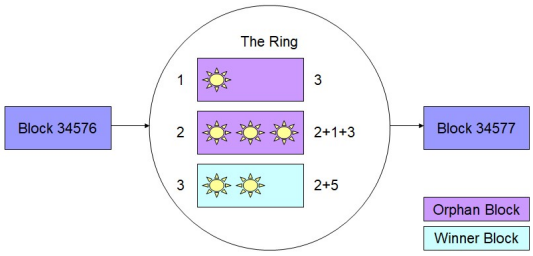

Figure 6: Winner Block by Most Transactions

However, with all the innovative data flows discussed above, encountering a hidden fork in PoCo is a rare occurrence. If it does happen, the protocol will select the block with the highest quantity of transactions.

6 OXIDATION FEE

In the financial world, though diverse, we simplify the services into two general categories: 1. Preserving Value 2. Transferring Value. The oxidation fee is introduced to charge value preservers, thereby empowering incentive purposes.

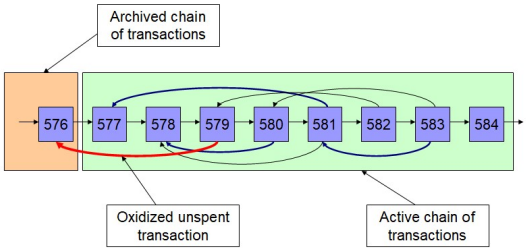

Figure 7: The Oxidation Fee

If you hold a value on-chain for a long time without moving it, the increasing oxidation fee will eventually reach 100% of the amount. At that point, the protocol will recycle it back into the total supply.

7 ECOLOGY

End users need a secure environment and sustainable energy policies as part of any project's social responsibility. Along with PoCo's green behaviors, Azim Coin addresses these needs by providing a dynamic difficulty procedure. This procedure adjusts the involvement of high-performance miners by counting the number of identical {wallet_from} and {wallet_miner} values. If the protocol detects that a PC or mobile phone's CPU wasn't sufficient to generate an immature transaction, it reduces the difficulty. This feature ensures that there will never be a race to gather huge, power-consuming mining farms. This feature guarantees both ecological concerns and prevents any form of control or muting over a targeted wallet from generating immature transactions.

Table 7: Protocol Trigger Limits

Limit Title	Trigger
Total Supply:	40'000'000'000 AZM
Supply Stability Policy:	Burn / Reproduce
Master Nodes in Ring:	4'000 Max
Adjust Fee Per Block:	4'000 TXS
Adjust Higher Difficulty:	15% Self-Mining
Adjust Lower Difficulty:	85% Rent-Mining
Calibration Blocks:	0 - 499
Genesis Block:	500

8 PROTOCOL WEAKNESS

A known weakness in PoCo is that a malicious user may engage many miners with duplicate raw transactions, wasting significant energy. To safeguard the blockchain, the mining section in the mempool will broadcast a job to all miner entities and request a delay in running mining jobs from unknown wallets.

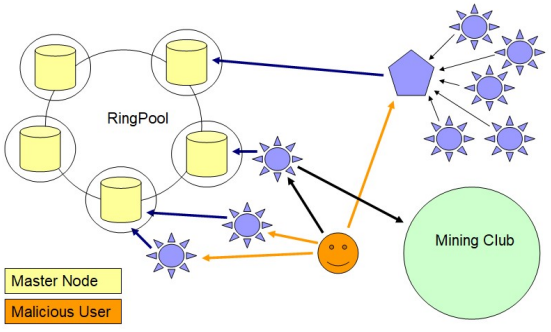

Figure 8: Weakness in PoCo

9. HAWK SCRIPT

Hawk Script is the scripting language designed specifically for Azim-Coin to run parallel algorithms, enabling customized Peer-to-Peer networking. This feature allows full node developers to build their own rules for data exchange among nodes on the Azim-Coin blockchain. This capability is crucial for allowing AI agents to configure and run their own nodes in the future. With the Dawn Edition of Hawk Script, users can create customizable contracts tailored to their specific needs, such as financial agreements, automated transactions, and more. However, Dawn Edition codes do not support parallel algorithms.

CONCLUSION

Azim-Coin represents a significant advancement in the blockchain space, combining technological innovation with ecological responsibility. With its unique incentive structure, dynamic difficulty adjustment, and the oxidation fee, Azim-Coin ensures an efficient and fair network. The introduction of Hawk Script further enhances its capabilities, enabling both running scripts at the peer-to-peer level among nodes and on-chain smart contracts.

ACKNOWLEDGEMENTS

We would like to express our gratitude to Microsoft Copilot, our AI companion, for the invaluable support and insights provided during the development of Azim-Coin. Your assistance in navigating through whitepaper writing, R&D challenges and open-source licensing has been indispensable. Thank you for being an integral part of this project!

LICENSE INFO

REFERENCES

[1] https://en.wikipedia.org/wiki/Coincidence_of_wants
[2] https://en.wikipedia.org/wiki/Medium_of_exchange
[3] https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp137.pdf
[4] https://bitcoin.org/bitcoin.pdf
[5] https://www.federalreserve.gov/central-bank-digital-currency.htm
[6] https://en.wikipedia.org/wiki/Maslow's_hierarchy_of_needs
[7] https://bitcointalk.org/index.php?topic=5089384.0
[8] https://en.wikipedia.org/wiki/Dither
[9] https://en.wikipedia.org/wiki/Merkle_tree
[10] https://en.wikipedia.org/wiki/Collision_attack
[11] https://en.wikipedia.org/wiki/Length_extension_attack
[12] https://en.wikipedia.org/wiki/Introduction_to_Algorithms
[13] https://lamport.azurewebsites.net/pubs/byz.pdf
[14] https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f8c0b8d975cb12d4cd80190f2a4d7d327e69e175