# Proof of Perfect White Paper

Joel Carter, Arie Trouw, Matt Jones, Jordan Trouw [*]

March 2025

**Abstract**

In areas of life where multiple parties interact to achieve an ideal outcome, from those as mundane as choosing where to go for dinner to those as weighty as voting on elected officials, the need for a clear and deterministic distributed consensus algorithm underlies the stability of the system. This need, and the associated solutions, have recently been of pioneering interest in the blockchain space.

# 1 Current Landscape

There exist several recognized and widely adopted solutions for coming to distributed consensus in the blockchain space.

## 1.1 Proof of Work (PoW)

### 1.1.1 Benefits

Revolutionized decentralized consensus by using computational puzzles to secure networks, ensuring trust without a central authority.

### 1.1.2 Limitations

- High energy consumption.
- Slow transaction speeds.
- Centralization risks due to mining pools.
- Vulnerability to 51% attacks.
- Risk of a single entity controlling the network with enough compute power.

## 1.2 Proof of Stake (PoS)

### 1.2.1 Benefits

Pioneered a more energy-efficient consensus model by leveraging stakeholders' assets, reducing energy use and offering faster transaction speeds. Encourages diversification of producers through random shuffling algorithms.

[*] XYO - arie.trouw@xyo.network, joel.carter@xyo.network, matt.jones@xyo.network, jordan.trouw@xyo.network

### 1.2.2 Limitations

- “Nothing at stake” problem.
- Centralization risk with large stakeholders.
- Vulnerability to long-range attacks.
- Challenges in ensuring network security without high energy costs.

# 2 Characteristics of an Ideal Algorithm

Given the existing shortcomings of the current consensus algorithms it becomes advantageous to envision a more ideal algorithm that maintains the guarantees of the existing solutions while addressing their shortcomings. Paramount to any distributed consensus algorithm for a blockchain is the ability to, given two equally valid uncles, choose the best one. Moreover, for an algorithm to be ideal it must not just meet the goal of consensus or even meet it well, but it must be antifragile-–resilient and gaining in positive attributes–when subject to the hostile entropy of the real world use cases it is subject to. The table below lists several metrics across which an algorithm which arrives at that end might be evaluated.

| **Metric** | **Good** | **Better** | **Best** |
|---|---|---|---|
| Consensus Mechanism | Independently verifiable | Simple to calculate | Hard to manipulate |
| CAP Theorem Balance | Chooses a balance of Consistency, Atomicity, and Partition Tolerance | Has an ideal balance for the network participants across conditions | Network partitions introduce minimal disruption due to constantly choosing best uncle, even when not partitioned |
| Scale | Does not fail as the network scales | Handles all reasonable scales across which the network will encounter without degrading in performance or increasing in cost | Gains in efficiency, robustness, & decentralization as the network scales |
| Network Participation | Allows users of a sufficient threshold (financial, technological, etc.) to participate | Allows all users to participate | Encourages decentralization and variety of participants at the protocol level |

Table 1: Tiered Comparison of Sample Blockchain Characteristics

## 2.1 For a Single Block

Towards the goal of arriving at consensus, given N number of potential blocks for inclusion in the blockchain which are all individually valid, it becomes desirable to have a mechanism for comparing blocks to provide an unbiased and impartial way for determining whether a block is more ideal for inclusion in the blockchain. This provides a tie-breaker of sorts when deciding which previous blocks to build on for block producers and an evaluation criteria for validators to decide which of the candidate chains to work on as it likely has the highest probability of being accepted. Existing mechanisms for this are the first produced block in PoW or the block produced by the next elected producer in PoS.

Of paramount importance to selecting the next block is the effect that a single block can have in influencing the direction of a blockchain which leads to the following maxims.

- It is not acceptable for the next block in a blockchain to have an outsized influence on the chain, such as forcing an uncle to be accepted as the new chain, as it allows a single network actor such a block producer with sufficient computational power to manipulate the entire network.
- It is permissible for the cumulative effect of older blocks, which are already included in the chain to have an outsized influence on the future of the chain so long as there was no way during the production of the blocks for any of the network actors to have known they would influence events.

A simple but robust accounting system could be derived for a single block giving each potential block a score such that the block score is the weighted sum of the positive aspects to be encouraged minus the weighted sums of the negative aspects we wish to discourage. For example, for a blockchain which that only desires to encourage decentralization, the following would apply.

$$Score_{Block} = Score_{Decentralization} - Score_{Centralization}$$

Combining multiple desired/undesired traits with respective weights gives the following.

$$Score_{Block} = \sum_{i \in Q} Weight_i(Score_i - Score_{i'})$$

| | |
|---|---|
| Q | Set of all qualities to emphasize |
| $Score_i$ | The measure to which the block exhibits the desired quality |
| $Score_{i'}$ | The measure to which the block exhibits the inverse of the desired quality |
| $Weight_i$ | The weight at which the quality should be emphasized |

Table 2: Single Block Scoring Key

## 2.2 Across Multiple Blocks

> “The test of a first-rate intelligence is the ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function.”
>
> — F. Scott Fitzgerald, The Crack-Up

Building on individual block evaluation, it becomes necessary to have a method of evaluating N potential chains which are all independently valid for determining which chain is more ideal for defining and furthering the blockchain. Mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) allow for comparing multiple chains to provide an unbiased and impartial means for achieving this but have some shortcomings as address previously.

One of the most ubiquitous and well proven models for arriving at a desired state across discrete data, like blocks in a blockchain, is a Control System. Control systems, of the architecture shown in Figure 1, exist for applications as varied as thermostats to self-driving vehicles and can be adapted to model blockchain consensus.

A familiar Control System is a car’s shocks and struts which work together to absorb bumps and steady the suspension, keeping the ride smooth by controlling how much the vehicle moves and how quickly it settles. In a similar fashion, a blockchain can be viewed as a continuously correcting system across which producers, users, and cryptographic algorithms constantly interact with each other to achieve consensus. For PoW chains the Control System can be modeled as the simplified Controls System in Table 3.

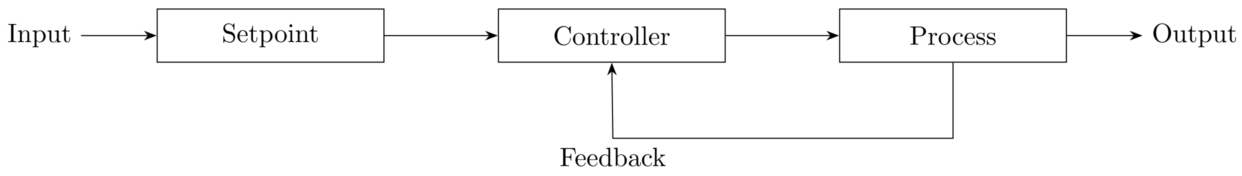

Figure 1: A Control System

| | |
|---|---|
| Input | Difficulty Level |
| Setpoint | Block interval |
| Controller | Difficulty adjustment |
| Process | Miners generating blocks |
| Output | Actual time to mine next block |
| Feedback | Difference between actual & desired block time |

Table 3: PoW Control System

For PoS chains the Control System becomes more complex implementing multiple logical Control Systems for things like network throughput, gas economics, etc. PoS chain Control Systems, while more complex than those of PoS, underscore the need for optimizing the for more than just a single blockchain metric.

An ideal Control System for a blockchain would produce an optimal chain by continuously evaluating and controlling for multiple metrics while also including mechanisms to prevent participants from manipulating or negatively influencing the blockchain.

- Prevent immediate correction (limit influence of a single block)
- Amplify/attenuate across multiple blocks to achieve desired setpoint
- Use randomness and decentralization to prevent deterministic attacks

# 3 Features

## 3.1 Dampening Effect

Longer than just previous block

## 3.2 Amplify/Attenuate

$$\sum_{W-N}^{N} N\, x_i$$

# 4 Proof of Perfect

$$\sum_{i=W-N}^{N} ((P-N)\,(W-i))/(W-i)$$

Weighted contributions to rolling average with past counting for more Emphasize the value of randomness to prevent deterministic attacks notes on - Kalman filters as options - Bayesian Probabilistic feedback - or even an appropriately bounded Markov models