The Color Consensus Mechanism Beige Paper: Color Prism

Version 0.9-1

November 24, 2018

The Color Platform Team

1.0 Purpose

The purpose of this paper is to explain the Color Consensus Mechanism at length at a more in depth manner. This paper will explain the ecosystem and how the consensus is achieved, and how it differs from existing platforms.

2.0 Introduction

The Color Prism Consensus algorithm will be the backbone of the Color Platform, ensuring dApp and Core transaction flows happen accordingly. Using the Color Consensus we believe it will achieve two main things:

1. Achieve Transaction Confirmation Speeds at **twice** the rate of EOS through concurrent transaction confirmation.
2. More Decentralized than EOS, thus being more Robust and harder to bribe the mining consensus participants.

3.0 Technical Details

Color Prism Abstract

Consensus Algorithm Type:	Modified DPoS
Number of Consensus Participants:	49 (Main) 28 (Backup)
Block interval:	0.5 Second
Block Confirmation:	1.0 Second
Maximum Block Size:	1.0 Mega byte
TPS (Transactions per second):	*Faster than EOS[1] (See footnote)

[1] EOS need 402 communications per block confirmation
20 x 20 + 2 = 402
Color need 132 communications per block confirmation
6 x 6 + 6 x 6 = 72

4.0 Color Prism Participants

Participant	Number	Selection And Role
Block Builders	**49 (7 from 7 leagues)**	**Provides Consensus actively, selected by vote & performance metrics (See Below).**
Backup Block Builder	**28 (compensated)**	**Steps in for active Block Builders in same league when they fail to provide consensus for a Block. Selected by vote & metrics.**
Prime and Lead Block Builder	**7 (at any one time)**	**Block Builders who are actively providing consensus for the current round. 1 Prime and 6 Lead Block Builders from 7 leagues**
Logic Runners	**>1,000**	**Will contribute CPU power and computing power and be compensated accordingly. Anyone can become.**
Council Members	**>1,000**	**Will vote on the Treasury Proposals and be compensated accordingly.**

Table 1: 4 Color Prism Participants

4.1 The Consensus Leagues

The motivation behind dividing consensus into leagues may be new in the blockchain world, but parallel computing and load balancing based on geographic locations is the norm in the blockchain world. The idea behind the Leagues is for each league to be able to handle the traffic for that specified region up-front, and then get consensus from the other nodes after the heavy lifting is done. Imagine a league in each country and each of the Block Builders in that league potentially geographically spread out as well.

4.2 Selecting a Block Builder

Consensus is divided amongst seven different groups of Consensus Providers (henceforth referred to a **Block Builders**) that operate in seven different groups (called **leagues**). Similar to most DPoS systems, Block Builders are elected. How they are elected however is not based on the amount of coin holder votes they amass, but rather on a formula that combines reputation and performance as well how many coins they are personally putting at stake for the network. It is assumed that the more coins a user has at stake, means the less likely they are to do “bad

things” in fear of getting their coins confiscated (explained in section 5). This formula is applied every 7200 blocks, or about once an hour. The tentative figures to describe the weight of what goes into choosing a Block Builder is below:

- **40%** Based on number of **C**oins **S**taked that are voting for each candidate.
- **30%** Based on a **C**ontribution **I**ndex, which will have many ways to be increased systematically such as referrals.
- **30% S**ystem **P**erformance **I**ndex. The further away from 100% the block confirmation is, the score will drop exponentially, thus replacing this participant with a backup until they can recover their score.

The various indexes are then aggregated and compared against each candidate and the tops from each section are weighted and selected accordingly. Using this method, let's imagine we can only choose two of the following four Block Builder Candidates:

Block Builder Candidate	**Coins Staked (CS)**	**Contribution Index (CI)**	**System Performance Index (SPI)**	**Total Score**
Color_Korea	100,000	16	96.8	1(40) + 3(30) + 1(30) = 160
Color_Dltto	80,000	34	94.2	3(40) + 1(30) + 3(30) = 240
Color_Argentina	78,000	20	95.4	4(40) + 2(30) + 2(30) = 280
Color_Italy	90,000	1	90	2(40) + 4(30) + 4(30) = 320

Table 2: 4-2 Block Builder Election Scores

In the above table the lower the score, the more likely they will be elected. For example, even though the Color_Italy has a higher **CS** (meaning more people voting for it) it has a lower **CI** and **SPI**, meaning that it won’t be elected. Similarly, even though Color_Argentina has a higher **SPI**, it falls short in **CS**, and **CI**, meaning that it too, won’t be chosen.

Once the Block Builders are selected, they will remain in that spot as long as they can keep their score high enough and are not missing above a certain threshold of blocks, provided a Backup Block Builder does not surpass their rating and “dethrone” them from the active Block Builder’s league.

4.3 Selecting a Backup Block Builder

Selecting a Backup Block Builder happens in exactly the same way the Block Builders are selected. Additionally, Backup Block Builders have all the same requirements and scores as the Block Builders, and are still rewarded at 50% the rate of the Block Builders for their services. Twenty eight Backup Block Builders, 7 per each league, will be selected by Color Council before MainNet launches. The specifics of selection process will be announced in later time.

4.3.1 Missed Blocks

A missed block occurs when a Block Builder does not build a block within the time allotted. This could be because it is having trouble connecting to the network, it doesn't have the proper hardware to handle the load, or any number of reasons. When this occurs, those transactions will still need to be confirmed, and after a certain time passes, another block Builder will be chosen to perform that action. Missed blocks will not be sent to the Backup Block Builders, instead they will be sent to the next in line and that builder will take a hit to their System Performance Index. If their score gets low enough then a Backup Builder may replace them.

4.4 Selecting a Prime and Lead Block Builders

Each Block Builder has an ID(BBID), 0-48. The way the numbering works is that they count upwards 1-by-1 as you get to the next league. If we number leagues from 0 to 6, the league 0 consists of 7 BBID's such as 0,7,14, 21, 28, 35, and 42. So as the league 1 with BBID's 1,8,15, 22, 29, 36, and 43.

For a given round (which we will call 12 blocks), a Prime Block Builder(PBB) and six Lead Block Builders(LBB's) will provide the consensus for that round, and at the end of the round, a new Prime Block Builder is pseudo-randomly selected based on a MOD 49 of the last 4 hex digits of the previous block's hash value (which will give us a Block Builder ID between 0-48, selecting the new leader). The formula to calculate the ID of the new PBB is as follows:

```
PBB_ID = (last_block_hash & 0xFFFF) mod 49,
```

where last_block_hash is the hash value of the last confirmed block, `&' is the bit-wise AND operation and `mod' is modulo operation.

A Prime Block Builder will produce 12 consecutive blocks (or 1 round) with approximately a 0.5 second interval between blocks. A new PBB is chosen every 12 blocks. The current PBB was self-decided by Modulo function of the hash value of a block in the past round. For example, all block builders take last 4 bytes of the hash value of the 10th block(a value with 4.3 billion combinations) mod 49 (the number of Block Builders). The mod 49 function will give them a number between 0-48 that correspond to each "seat" across all Block Builder leagues. When the number matches its BBID, it becomes the PBB for the next round. This way, there is no

need to communicate further amongst 49 BB's to elect the next PBB - no Proof of Work, no redundant message passings.

Lead Block Builders are then chosen based on which Prime Block Builder is chosen. Once the next Prime Block Builder's ID(PBBID) is calculated, each Block Builder can immediately decide whether it will also participate in next round of LBB's or not. If its own BBID falls between {(PBBID+1) Mod 49} and {(PBBID+6) Mod 49}, inclusive, it will do. If 44 is elected to be the Prime for the next round, then 45, 46, 47, 48, 0, and 1 will be be the next Leads. If 48 for the next Prime, then 0, 1, 2, 3, 4, and 5 for the next Leads.

When a PBB completes building a block, it broadcasts the fresh block to 6 LBB's. Then each Lead works the consensus amongst its own league to validate the Prime's work in parallel with other 6 leagues. Whenever a transaction occurs, it sends back a small boolean True or False packet, for the other nodes to validate that transaction.

4.5 Logic Runners and Council Members

Although not directly involved with Consensus in and of itself, they provide an important role and are part of the compensation structure, and recipients of a portion of the Block Reward based on their contributions within their respective ecosystems. Each Council Member is compensated based on their participation in the treasury voting system, which they can only do if they have enough coins. Logic Runners on the other hand are compensated based on the amount of storage and computing power they are providing with reliable and low latency averages in requesting that use of storage. The exact mechanisms to determine these are still under development.

5.0 Consensus Process

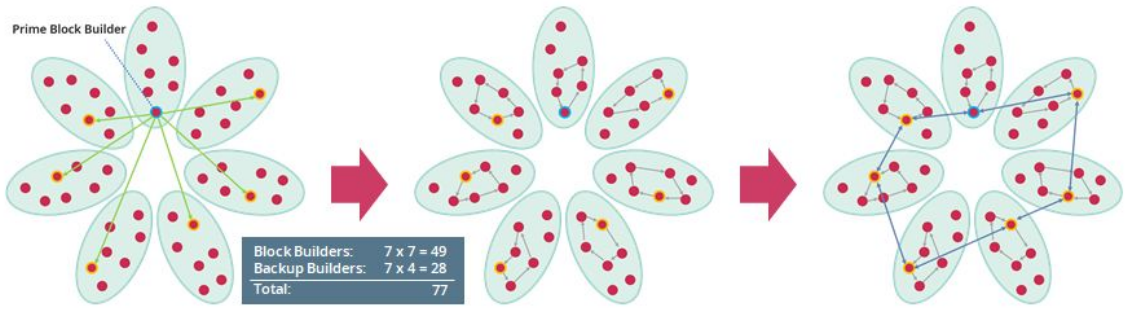
5.1 Building a Block

Building a Block consists of a five step process which we will outline below:

1. The Prime Block Builder will build blocks from the transaction data merkle tree and send the hash value to six other 'Lead' block builders, one from each other league. (A lead block builder is essentially a Block builder in another league that is selected at the time of consensus).

2. The seven Block Builders across the seven leagues will begin the consensus process in parallel, within their own leagues. The Block Builder then sends the Block out to the other leagues and awaits a confirmation.

3. The seven block builders confirm the block simultaneously, and once five of seven blocks confirm this effort by sending a small boolean ‘True/False’ packet back to the network, the block is considered confirmed, starting the process for the next block.



[Figure 1-5.1 - Block Building Illustration]

Through this process our theoretical ‘top speed’ for Consensus is roughly twice that of EOS. See the confirmation speed chart below for details.

Step	EOS	Color Prism
Producing Block	**10ms**	**10ms**
Sending/Receiving Block	**To 20 BPs - 200ms**	**To 6 LBB’s in 6 Leagues - 150ms**
Sending/Rec Second Block	**n/a**	**To 6 BB inner league 50ms**
Consensus Confirm	**Among 21 BP 80ms**	**Inner League 20ms**
Consensus Second Confirm	**n/a**	**Among League 50ms**
Total:	**480ms**	**270ms**

[Figure 2-5.1 - Confirmation Speed Comparison Chart]

5.2 Block Builder (& Backup Block Builder) Requirements

1. All Block builders should prepare servers and run real-time with enough bandwidth in their league.

2. Block Builders are expected to provide adequate low latency confirmations within each league.
3. All Block Builders are required to have a Secure Element chip installed on their machine in order to assist in the processing of offline and P2P payments. For more information on the Secure Element Chip, please see the Color Pay Beige Paper.
4. Block Builders, in order to maintain their position must maintain a high contribution index. A contribution index is a sort of community rating that calculates a whole suite of metrics from reputation to referrals, activity and merit worthy contributions to the platform.
5. All Block Builders must prepare a “campaign” and run to be elected to provide consensus. A Block Builder must first be a regular council member and will then stake their coins while providing consensus.

5.3 Reward & Penalty Structure

In the reward structure it can be thought of as a splitting of 1000 shares. Each time someone produces a block they are rewarded with roughly 6.66% of the total block reward, splitting 200 shares of the Network Support Block Reward with the Logic Runners and Backup Block Builders. Although the act of consensus is extremely important, without a healthy treasury and incentives to hold the currency as well, the Pixel Program, the cornerstone of Color’s economic incentive, wouldn’t be able to flourish.

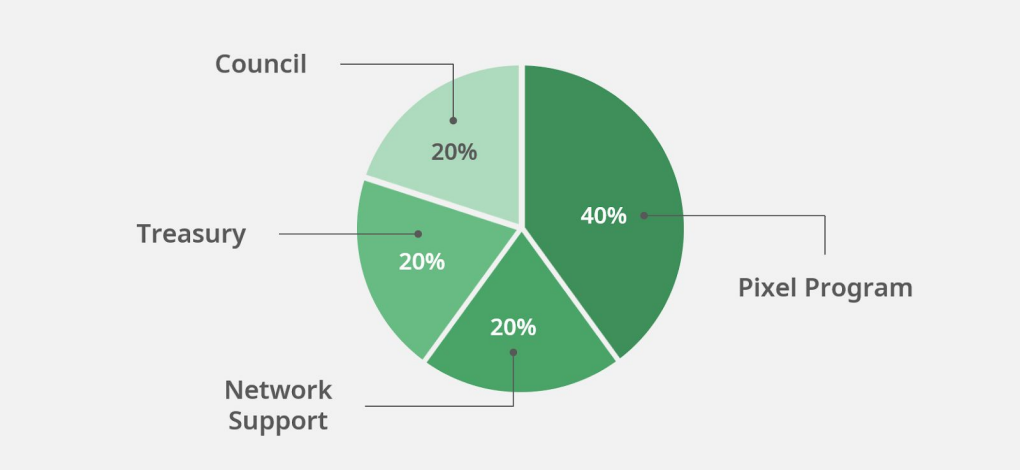


Figure 3-5.3 Reward distribution

When a Block Builder is elected from the pool of eligible Council Members (a Block Builder must have enough Coins to be a council member before becoming a Block Builder), they must stake their coins in their while providing consensus. This stake can be **confiscated** if the network determines malicious intent or does not effectively enforce the rules of the system. For example

if a block builder is sending out mixed messages about a block to the other leagues, that could be grounds for confiscation.

5.4 Nothing at Stake Problem

The nothing at stake problem is a notorious one amongst Proof of Stake Coins. That is to say, if a coin forks, miners have no incentive to “resolve” the fork, and don’t lose anything by committing to both. In Proof of Work, miners would have to point their mining power at a particular fork, so their electricity and mining capacity for the duration of the fork are pointed at a particular chain, which if another chain becomes the main chain, they lose mining time and electricity on mining a chain that isn’t worth anything.

Delegated Proof of Stake solves this by putting the role of the delegate (which earns money for being a trusted actor) on the line. However, this is problematic in that the delegates themselves often form cartels and are either bribing voters to stay in power, or the need of a central body to prevent the formation of cartels[2].

In Color, the selection of Block Builders is pseudo-random and is organized in leagues making it harder to form cartels. In order to prevent bribery, the community will have control over a reputation score (to be discussed in more detail in the future), that community members will be able to suss out bad actors and effectively make them lose their **eligibility** as a potential Prime Block Builder, and likely ultimately, as a Block Builder of any kind.

6.0 The Parallel Consensus

6.1 How It Works (Coming in Next Version)

-To do list to describe this in more detail -> Coming in Next version.

7.0 Conclusion & Summary

7.1 Conclusion

The Color consensus algorithm is essentially a hybrid Tendermint algorithm that uses a unique Parallel Consensus algorithm. Color Prism works in randomly selected leagues to prevent cartels, improve security and lower the amount of unnecessary chatter. Coupled with the parallel processing of transactions instead of a mempool processed one-by-one, Color Prism

[2] https://www.ccn.com/block-one-vows-to-use-its-eos-tokens-to-prevent-voting-cartels/

has potential to be one of the fastest consensus algorithms, beating EOS by nearly 2x the speed.