Hacash Diamond: A Trustless Store-of-Value System

An anonymous author released Hacash Diamond in a 2018 paper

Summarized by the HACD Art team

Abstract. In 2018, an anonymous author released the white paper titled "Hacash: A Cryptocurrency System for Large-Scale Payments and Real-Time Settlement." The white paper introduces an innovative cryptocurrency system of Hacash, which includes Block Diamond, a currency with a distinctive set of features: a limited supply, indivisibility, and a unique identifier. The mining difficulty of Block Diamond is designed to increase in one direction, ensuring its scarcity and value stability. The production mechanism of Block Diamond adapts to changes in population and technological cycles. It is driven by market competition, increasing the output of new coins with computational power and decreasing or halting production to maintain the currency's supply-demand balance. The Hacash white paper provides a comprehensive monetary theory system, covering payment settlement systems and blockchain design principles. It includes in-depth technical discussions, which, due to their extensive and complex nature, may be challenging to navigate. For a focused understanding of Block Diamond, the relevant sections have been refined and integrated herein. For complete details, readers are encouraged to explore the full Hacash white paper.

1. Introduction

The ideal currency, existing only in theory, features zero transaction costs and a total supply that adjusts in real-time with the growth and consumption of society's overall wealth. It is akin to an infinite reserve of virtual gold, where currency is minted into circulation with increased productivity and production reduces with rising mining costs due to decreased productivity. This system aims to avoid economic harm from dramatic currency fluctuations, such as inflation or deflation. However, achieving this theoretical perfection is challenging due to the harsh reality that such perfection is unattainable.

The bookkeeping rewards and channel interest production quantities are fixed and do not change with variations in productivity or market conditions. A currency growth mechanism that adapts to fluctuations in population and technological cycles is needed. This mechanism should adjust production based on market competition and computational power, with mining difficulty that only increases, ensuring new coin production decreases or stops when computational power drops due to market reasons.

2. Production

Block Diamond is defined as a string of data satisfying specific formatting criteria, generated from a compressed calculation of a 32-bit hash value. Each block can contain at most one Block Diamond, or none, depending on computational power. The production algorithm is as follows:

[hash256((genesis_block_hash ||prev_diamond_block_hash) + belong_user_public_key + nonce_number) ==> length_16_string]

This process involves taking the concatenation of the genesis block hash or the previous block hash containing a diamond, the public key of the target owner, and a random nonce number, performing a hash operation to obtain a 64-character string, similar to:

[35534631f31dfcf12200cdbad65c66ffb9d3fbd3ac985aa8a401bc4c3616bab3]

The result undergoes a special compression operation where every 4 bits are mapped to characters from the list *[0WTYUIAHXVMEKBSZN]*, resulting in a 16-character string such as:

[0NMSAK0ZYNSNBAZM, 00000000IXVKHNHZ, or 0000000000UKNWTH]

When the result satisfies at least the first ten characters as "0" and contains no trailing zeros, a Block Diamond is produced. Each Block Diamond is assigned a

unique literal identifier, such as "*UKNWTH*". Once produced, the Block Diamond is included in a block and broadcasted, prompting producers to calculate the next Block Diamond's identifier using the new block's hash. If multiple Block Diamond is produced within the same block interval, miners decide which one to include in the block, possibly favoring the one with the highest transaction fee.

The total number of Block Diamonds is capped at around 17 million. Each time one is mined, the overall mining difficulty increases exponentially, approaching infinity as the number of diamonds mined increases.

Block Diamond represents a high-dimensional heterogeneous form of currency, capable of achieving dynamic adjustments in currency supply. Their value is determined by mining costs and market recognition.

3. Mining

The literal value of a diamond consists of 16 characters from the set *[WTYUIAHXVMEKBSZN]*. A valid literal value is considered when the final hash value has the last six characters as letters. The total number of possible diamonds is: *16^6 = 16,777,216.*

It takes approximately 25 minutes to mine one diamond every 5 blocks, without considering sharp increases in difficulty. The estimated time to mine all diamonds is approximately 800 years, which means a maximum of about 58 diamonds can be mined each day, resulting in an annual maximum production of approximately 21,000 diamonds.

The mining difficulty adjusts every 3,277 diamonds. When the first 20 bits of a 32-bit hash value are all zeros, the mining difficulty reaches its maximum. However, due to the nature of hash calculations, the mining difficulty will double each time, ensuring that not all diamonds can be mined. There will be a point of equilibrium where mining a new diamond will require the majority of the network's computational power, making the marginal yield of diamond mining increasingly smaller, while the marginal cost continues to rise, thus ensuring the scarcity of diamonds in the market.

Block Diamonds accumulate as surplus production and serve as a wealth repository within the economic system.