$COLL
If Terrence Tao can't do it, so can't you.

Charles Dana, H24, Discrete Mathematician

February 21, 2024

Abstract

We are in the year 202𝕏, and sha256 has become a running gag, $ETH needs to rely on something like proof of work in order not to collapse and we can mine $DOGE in the blink of an eye. Who's your savior you might ask yourself, the Collatz Conjecture. It is possible to introduce public key cryptography through the un-solvable property of the Collatz Conjecture. The principle is simple, your public key is a sequence of $\omega \in \{0,1\}^{N+1}$ where you decide N and the private key is a pair (n, x) where we assume that the Collatz operator:

$$C(x) = \frac{1}{2}\big([x\%2 == 1](3x+1) + [x\%2 == 0]x\big)$$

can be iterated such that, $\mathcal{C}^n(x) = (C \circ \ldots \circ C)(x)\%2$ follows:

$$N \in \mathbb{N},\ \omega \in \{0,1\}^{N+1},\ n \in \mathbb{N},\ x \in \mathbb{Z}$$

$$\omega = (\mathcal{C}^n(x+k))_{k \leq N}$$

What would a block look like? A simple:

`00110...1110:0110111...01110111:1000:10:101:1:10001001101..1101`

Which would send 2^3 $COLL from 00110...1110 to 0110111...01110111. And 2^1 $COLL from 00110...1110 to the miner of the block, with a decaying difficulty from 5 to 1, starting from the timestamp 10001001101..1101 minute by minute being reduced by 1. The idea is to use sha256 on the block, and the difficulty is about guessing the first D digits of the binary hash.