32bitcoin - A Sane Hash Cash

T. Harm Gustav

Abstract

People don't know what they are doing on their computer. Names and numbers are important, especially identity. The problem of number identities is so important, that no matter the certificate your bank shows you, it can always be man in the middled. Now some numbers are easier to remember and look good in IPv4 notation, making them easy to remember and undoing the need to keep a book that matches names to numbers (DNS). 32bitcoin proposes a number distribution system that, while centralized as a database, is open and recoverable, in case of data loss.

Introduction

32bitcoin proposes to utilize a 32-bit range for their number system, specifically between 0 and 4294967296, which may vary slightly depending on implementation details.

System Design

We build on the cornerstones of hashcash and bitcoin but aim to make it sane by keeping time, energy, and greenhouse gas emissions to a minimum, while also maintaining total security, depending on which implementation one chooses to trust.

Concept of Hoheit

A new concept introduced by 32bitcoin is *Hoheit*. Numbers can be claimed by submitting data to the Hoheit. The Hoheit then decides if it likes the data and will reveal a secret to the submitter, which it does not save. This secret gives the user power over their number. Simultaneously, a public database is updated with the number, the hashed secret, and the current timestamp. When a user submits their claimed number and secret to Hoheit again, it will change the secret and give a new one, updating the database in the process.

Ownership Proof

This mechanism serves the purpose of proving ownership by enabling users to change the hashed value of the number, which is a relatively straightforward process.

Trustworthiness of Hoheit

Can Hoheit be trusted? Essentially, it acts as a central authority. It could potentially store the secrets it distributes to number claimers and then take over the numbers for itself. However, this would likely be detrimental to its business, as people would stop using a system perceived as fraudulent. Furthermore, the ease of implementation makes it quite simple to become a new Hoheit.

Value of the Magic Numbers

Certain numbers have an allure, like 1.1.1.1 or repeating digits if you will, doubles, toofers, triples even, numbers can be represented in many shapes and forms and some are definitely more valuable. We propose a simple cost function, valueing lower values higher, and not caring about magic numbers. But that is again up to the implementation of this protocol.

Cost function for the proof of work hash

32 bits can be at maximum 32 zeros. In IPv4 notation they are grouped in 4 bytes. Simple mattehmatiks will give a cost function that requries as many leading zeros as the number wants.

Fairness

Many thinkeres, especially Renee Gueneonon said that capabilities in people are different, not in a racist kind of way, Julius Evola said even something like a teenager when he said skincolor dont matter its about the spirit. Hence, to not beg the question it will be very easy to get a number if you want one, becaus