RPOW - Reusable Proofs of Work

2004

Archived Website

GitHub

Original Announcement

Reusable Proof-of-Work (RPOW) was an invention by Hal Finney intended as a prototype for a digital cash based on Nick Szabo's theory of collectibles. RPOW was a significant early step in the history of digital cash and was a precursor to Bitcoin. Although never intended to be more than a prototype, RPOW was a very sophisticated piece of software that would have been capable of serving a huge network, had it caught on.

Historical Context

In the 1990s the Cypherpunks began to play around with the idea of a digital cash whose value would not be dependent on an organization issuing it. Following Nick Szabo, this form of digital cash would be recognizable as being limited in supply, and therefore usable as money, by being provably difficult to create. This could be done by defining units of the digital cash in terms of proof-of-work. Some proposals for digital collectibles circulated on the cypherpunk mailing list, including b-money by Wei Dai and Bit Gold by Nick Szabo. RPOW was the only digital collectible to ever function as a piece of software.

How it Works

An RPOW client creates an RPOW token by providing a proof-of-work string of a given difficulty, signed by his private key. The server then registers that token as belonging to the signing key. The client can then give the token to another key by signing a transfer order to a public key. The server then duly registers the token as belonging to the corresponding private key.

The double spending problem is fundamental to all digital cash. RPOW solves this problem by keeping the ownership of tokens registered on a trusted

server. However, RPOW was built with a sophisticated security model intended to make the server managing the registration of all RPOW tokens more trustworthy than an ordinary bank. Servers are intended to run on the IBM 4758 secure cryptographic coprocessor, which is able to securely verify the hash of the software that it is running. RPOW servers are capable of cooperating to serve more requests.

For more information, please see Hal Finney's original page, which includes an overview, an FAQ, a theory page, a presentation, and a very interesting page called World of RPOW which explains how RPOW would have scaled to serve the entire planet.

The original code can be found on GitHub here.

Special thanks to Fran and Jason Finney, Hal's wife and son, for sharing the original RPOW code and website files.

Back