US 20240405998A1

(19) **United States**

(12) **Patent Application Publication**

Naik

(10) **Pub. No.: US 2024/0405998 A1**

(43) **Pub. Date: Dec. 5, 2024**

(54) **MESSAGE SCHEDULING FOR CRYPTOGRAPHIC HASHING**

(71) Applicant: **QUANTUM BLOCKCHAIN TECHNOLOGIES PLC**, London (GB)

(72) Inventor: **Rahul Naik**, London (GB)

(73) Assignee: **QUANTUM BLOCKCHAIN TECHNOLOGIES PLC**, London (GB)

(21) Appl. No.: **18/696,073**

(22) PCT Filed: **Sep. 28, 2022**

(86) PCT No.: **PCT/GB2022/052458**

§ 371 (c)(1),
(2) Date: **Mar. 27, 2024**

(30) **Foreign Application Priority Data**

Sep. 29, 2021 (GB) 2113962.1

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3239*** (2013.01)

(57) **ABSTRACT**

A method of performing cryptographic hashing when mining for Bitcoin comprises causing a message scheduler to calculate a set of partially-calculated input values for a SHA256 (e.g. $SHA256_0$ 424) cryptographic compression function using values which are based on invariable portions taken from an initial input message of the input messages (e.g. 418) to be hashed. For each subsequent input message of the input messages (e.g. 418) to be hashed, a set of fully-calculated input values for the SHA256 (e.g. $SHA256_0$ 424) cryptographic compression function is calculated using the partially-calculated input values and values which are based on variable portions of the subsequent input message to be hashed. The set of fully-calculated input values is then provided for use when performing the SHA256 (e.g. $SHA256_0$ 424) cryptographic compression function in respect of the subsequent input message. This reduces the number of calculations which need to be performed by the message scheduler.