30 September 2021

**Quantum Blockchain Technologies Plc**
("QBT" or "the Company")

**ASIC UltraBoost:**
**Filing of the Company's first breakthrough patent application on Bitcoin mining algorithm optimisation**

The board of Quantum Blockchain Technologies (AIM: QBT) is pleased to inform shareholders that, as an initial result of its new research and development ("R&D") strategy in respect of disruptive proprietary techniques for Bitcoin mining, the Company, following the outstanding research work of its cryptography expert, has filed an application for its first patent– the ASIC UltraBoost.

The application made to the UK patent offices (then to be extended internationally while maintaining the priority date, set via the UK application) represents a major breakthrough in Bitcoin mining, as a result of a very material optimisation of the mining algorithm.

The ASIC UltraBoost can be described as an improvement of the Bitcoin mining process (building on all other existing optimisations in the market, including ASIC Boost) eliminating redundant computation of a key part the Bitcoin mining algorithm, resulting in a faster and more efficient mining process.

The optimisation starts from the initial consideration that currently, Bitcoin miners attempt to find the winning hash acceptable to the Bitcoin Network by calculating multiple midstates (by rolling the Version), passing them through further hashing (by rolling the Nonce) to obtain a final hash value that is less than or equal to the Target.

ASIC UltraBoost looks to improve the algorithmic efficiency of Bitcoin mining by proposing 3 specific variants to the SHA256 message scheduler for the 3 instances of SHA256 in Bitcoin mining. These Optimal SHA256 Message Schedule Variants result in faster and more efficient Bitcoin mining by eliminating the redundant computations within the SHA256 message schedule specific to Bitcoin mining.

As such, the calculation of the midstates alongside the calculation of the message digest is significantly optimised.

ASIC UltraBoost reduces the Message Schedule calculations for the 3 iterations of SHA256 by approximately 20%.

The SHA256 function being a combination of the message schedule and the compression function, when considering the optimisations of ASIC UltraBoost for the entire SHA256 function, the number of operations across the 3 iterations of SHA256 are reduced by approximately 7%.

More accurate results, including an overall percentage improvement will be available when ASIC UltraBoost is implemented in hardware.

The Company, following the research programme of the cryptography expert, and other members of QBT's R&D team, is working on other findings that are expected to be patentable in the coming months.

**Francesco Gardin, CEO and Chairman commented**: "Filing the ASIC UltraBoost patent application is the first milestone resulting from our R&D programme, achieved in just four months. It is the first of many patents the Company is working on and plans to file. This breakthrough result, which we believe has the potential to be game changing, will be used for the deployment of our proprietary FPGA and ASIC implementations of the Bitcoin mining algorithm.

A nearly 7% efficiency in running the Bitcoin mining algorithm can be used to increase mining speed or save energy. On the massive numbers of iterations involved in mining, this level of saving represents, either a 7% increase in the mining probability, or a 7% energy saving at the existing mining probability. In both cases, for large mining facilities this optimisation corresponds to significant mining revenues, or saved energy bills, all leading to increased profit. We are very optimistic on the future results of our R&D efforts, as this first patent application has shown.

Finally, I'd like to thank the whole R&D team of QBT, with a special mention to our cryptography expert, who has been key to this first important success of the R&D programme."

*This announcement contains inside information for the purposes of Article 7 of the Market Abuse Regulation (EU) 596/2014 as it forms part of UK domestic law by virtue of the European Union (Withdrawal) Act 2018 ("MAR"), and is disclosed in accordance with the Company's obligations under Article 17 of MAR.*

**For further information please contact:**

**Quantum Blockchain Technologies Plc**
Francesco Gardin, CEO and Executive Chairman +39 335 296573

**SP Angel Corporate Finance** (Nominated Adviser & Broker)
Jeff Keating +44 (0)20 3470 0470

**Leander** (Financial PR)
Christian Taylor-Wilkinson +44 (0) 7795 168 157

**About Quantum Blockchain Technologies Plc**
QBT (AIM: QBT) is an AIM listed investment company which has recently realigned its strategic focus to technology related investments, with special regard to Quantum computing, Blockchain, Cryptocurrencies and AI sectors. The Company has commenced an aggressive R&D and investment programme in the dynamic world of Blockchain Technology, which includes cryptocurrency mining and other advanced blockchain applications.

**Glossary of Terms:**

**AsicBoost:** AsicBoost is a patent-pending method to speed up Bitcoin mining by a factor of approximately 20%. The performance gain is achieved through a high level optimization of the Bitcoin mining algorithm (SHA256) which allows for a drastic reduction in gate count on the mining chip.

**Hash function:** A hash is, in general, a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Thus, regardless of the original amount of data or file size involved, its unique hash will always be the same size

**Message Schedule:** Is a function that generates sixty-four words from 16 words input message block (a word is represented by 32 bit, hence a total of 512 bit). The message scheduler is a key part of the bitcoin mining algorithm: it is computed three times for each winning hash generation attempt, i.e., trillions of times per second.

**Nonce:** The Nonce is a random whole number, which is a 32-bit, which is adjusted by the miners, so that it becomes a valid number to be used for hashing the value of a Block.
A typical Miner tests and discards trillions of Nonce per second until they find that Golden Nonce which is valid. In order to complete the verification faster than other miners, miners compete with each other using their computer hashing power. Once the Golden Nonce is found, they can complete the Block and add it to the Block Chain and there by receive the Block reward, i.e., reward bitcoins.

**SHA256:** Secure Hashing Algorithm (SHA) -256 is the hash function and mining algorithm of the Bitcoin protocol, referring to the cryptographic hash function that outputs a 256 bits long value.

**Version rolling:** Miners can inspect the nVersion field (32 bit) of a block, by rolling the nVersion field. A typical Miner tests and discards more than a billion of random bits activated by the rolling, until a winning hash is found. The method is also referred as Overt-AsicBoost.