

Quantum Blockchain Technologies Plc
(“QBT” or “the Company”)

R&D and Business Update

Quantum Blockchain Technologies (AIM: QBT), the AIM-listed investment company focusing on a R&D and investment programme within blockchain technology, is pleased to provide an update of its recent R&D activities for the development of its disruptive Bitcoin mining technologies.

Overview

The R&D activity during the past four months has been focused on two main directions:

- Further improvement in the results obtained in the laboratory for the three Artificial Intelligence (“AI”) Methods: A, B and C, and
- The porting of these Methods onto existing commercial mining hardware.

The short-term strategic goal is to achieve real-time bitcoin mining via one, or more, of the existing Bitcoin mining pools, through a collaboration or in partnership with a leading Bitcoin miner.

In addition, the team is continuing to apply to secure patents for its IP by working with the Company’s Patent Attorney as follows:

- to extend the two existing patent applications by applying for international patents,
- by continuing the work on its third patent application, and
- by defining the scope for a new, fourth patent application.

Finally, Chief Research Officer, Francesco Gardin and senior colleagues have recently attended two of the major US Bitcoin conferences. As well as showcasing QBT’s technology, the Company met with a number of potential North America mining partners and consultants, in order to consolidate its existing business contacts and establish new ones, in preparation for the planned commercial deployment of the three Methods.

R&D Activity

While QBT’s AI-based mining technology has shown consistent results under laboratory conditions, supported by verifiable experimental data, the Company’s research teams are continuously challenging the efficiency of the obtained results to further improve them.

QBT’s software engineers are continuing to attempt to successfully port the Methods to existing commercial ASIC-based mining hardware and software system, via CGMiner. This remains challenging due to the severe limitations of most current ASIC architectures for implementing SHA-256. These limitations are mainly due to the speed and power consumption inefficiencies created by the designers, which impact the ability to use any arbitrary input to SHA-256.

A decision has been taken, therefore, to migrate away from CGMiner to AxeOS (ESP-miner), a more recently developed and, in the Company’s opinion, a better designed public domain operating system software for Bitcoin mining devices. The Company has found that CGMiner, which is considered the leading operating system for Bitcoin mining, added elements of unpredictability to a number of processes, due mainly to the code being developed over the last 13 years by a large number of contributors, each adding a new elements to the mining software. Therefore, while CGMiner was initially used by QBT to achieve the porting of its Methods, its high-level of inefficiency has now been recognised and the change to ESP-miner has been implemented.

ESP-miner was created by Open Source Miners United (OSMU), of which QBT is a sponsor, and incorporates the essential firmware-like functionalities of the FPGA component, which is the second processor of the current mining rigs’ control boards that provides time communication with the hashing boards.

ESP-miner uses the same processor for both the operating system and the firmware-like functionalities: the ESP32-S3 Espressif MCU (micro controller unit).

The combination of ESP-miner and the new family of BM1366 ASIC is now QBT’s new real-time operational environment for porting and testing the three Methods in a real-time mining mode. Other hardware and software platforms from OSMU are currently being assessed.

Method A

The key data from Method A’s neural network training dataset is the accurate real-time measurement of the hashing time; specifically, the more precise the measure, the better the performance of the Method.

The Company’s main objective has been to collect such information in real-time while hashing is taking place on the ASIC chip. This was obtained by developing specific modifications to CGminer, replacing indirect time measure with direct measure.

The same functionalities will be implemented in ESP-miner and the Company believes it will lead to even better real-time hashing time measuring, given the easier access to the firmware-like functionalities of this new software environment.

Method B

The porting of Method B will continue using the new ESP-miner software platform, making the control of the BM1366 chips easier, more efficient, stable and reliable.

In parallel to this, a new tool has been developed by QBT for real-time mining testing which will bypass CGminer and any other mining operating systems, reducing potential errors introduced by the complexity of this mining operating system. This tool is likely to be ported directly onto the ESP32-S3 Espressif MCU.

In addition to the porting activity, a new major alternative performance improvement technique has been developed, based on solid mathematical theory, which has been tested off-line in the laboratory, with consistent positive results. Once the ESP-miner porting has been completed, this new version of Method B will undergo real-time mining testing.

Method C

The laboratory results of Method C continue to be confirmed, while the R&D team is working on perfecting both the underlying AI model used by the Method and the selection of data used for training it.

Tests have been conducted, so far, off-line on historic data, 'ex-post', by using a simulation of a Bitcoin pool operating in the past.

The reason for this approach is due to Bitcoin's current level of mining difficulty; that is, the probability of finding a winning hash is statistically almost impossible, unless using hundreds of mining rigs simultaneously. Therefore, by using the difficulty level of old blocks of the Blockchain, combined with current mining hardware, a real-time testing of Method C would, the Company believes, be possible.

The Company has therefore adapted Method C to enable live demonstrations, by finding winning hashes at lower levels of difficulty, i.e. in the old blocks of the Blockchain, in order to give real time evidence to potential partners, or clients, within the average ten minutes new block hashing time to prove the hashing advantage of Method C, compared to standard non-AI-based hashing.

Patents

Both existing patent applications have been filed internationally. As a result, UK patent protection can be sought through the European Patent Office rather than through the UK Patent Office.

The first international patent application has already been filed at the European Patent Office. If granted, the patent will include UK protection and the original priority date will not be affected. The first international patent application has also been filed in the US, Canada, Australia and South Korea. When the deadline for the national phase of the second international application approaches, the Company will file that international application at the European Patent Office and will decide on any additional jurisdictions to choose.

Drafting of the third patent application, the proprietary quantum version of SHA-256, continues. The subject matter is particularly complex, hence the delay in finalising the document.

A fourth patent application, related to Method C, but not on the nature of the Method, will start to be drafted very soon, with a filing expected to be made by the end of 2024.

The Company's decision for the IP protection of Methods A, B and C is to keep them as industrial secrets, although patent applications which preferably make use of those methods could be filed, as in the case the one related to Method C, without the need to reveal those Methods.

Business Developments

Over the past few months, the Company has continued its discussions with the major Bitcoin sector companies, which are mainly located in North America. These discussions have now reached a level where the Company is looking to provide live mining test demonstrations, as soon as any one of the Methods is available for real-time mining, as confirmed by recent meetings in the US at Mining Disrupt 2024 in Miami and Bitcoin 2024 in Nashville.

The Company believes the recent decision to migrate onto the ESP-miner operating system, running on ESP32-S3 Espressif MCU and using Bm1366 ASIC chips, is expected to achieve successful real-time mining testing of methods A, B and C.

Once this technical milestone has been completed, the Company expects to commence conversations with the small number of companies who have developed their own versions of the mining operating system, firmware and drivers, that operate the current crop of commercial mining rigs. The plan is to port QBT's client version of its Methods to the miners' proprietary software environments, providing access to a potential market of millions of currently operational mining rigs.

Francesco Gardin, CEO and Executive Chairman of Quantum Blockchain Technologies commented: *"Most of the current and recent efforts of the Company are focused on the porting of the Methods on to commercial hardware mining platforms.*

"The skill set for the porting projects is completely different from AI know-how used in the design and development of the three Methods by our R&D teams.

"A very experienced software engineer from Milan University joined the core software engineers' group nine months ago, and we feel this group now has all the necessary skills to successfully undertake the porting task to a real-time Bitcoin mining environment.

"This complex technical step of the process is the precondition for deploying QBT's technology and entering into pragmatic partnership and commercial discussions with the major players of the sector, all of whom are very aware of QBT's technology and all of whom are just waiting for real-time.

"The decision to switch to the ESP-miner operating system, running on ESP32-S3 Espressif MCU and using Bm1366 ASIC chips, will definitely accelerate moving in this direction."

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
John Mackay

+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 with a strategic focus on technology related investments, including a special regard towards Quantum Computing, Blockchain, Cryptocurrencies and AI sectors. The Company has 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

ASIC: An Application-Specific Integrated Circuit is an integrated circuit chip customized for a particular use, rather than intended for general-purpose use. ASIC chips are typically fabricated using metal-oxide semiconductor (MOS) technology, as MOS integrated circuit chips.

Bitcoin Mining: Bitcoin mining is the process of using computer hardware to do mathematical calculations for the Bitcoin network in order to confirm transactions. Miners collect transaction fees for the transactions they confirm and are awarded Bitcoins for each block they verify.

CGminer: Is the most popular software system for GPU/FPGA/ASIC based miners. CGminer is an open-source GPU miner written in C available for several platforms like Windows, Linux and OS X.

Hash: A hash is the output of a hashing function, which is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length.

Method A: A Machine Learning based development by QBT R&D team, aimed at reducing the SHA-256 search space, compared to the brute force method used by BTC mining rigs today.

Method B: A Machine Learning and statistical optimisation technologies developed by QBT R&D team, reducing the SHA-256 search space, but radically different from Method A.

Method C: A Machine Learning based development QBT R&D team is an AI Oracle with to assess in real time the likelihood of an input to SHA-256 to generate a winning hash. (Method A, Method B and Method C, collectively, the Methods.)

Neural networks: A neural network is a machine learning program, or model, that makes decisions in a manner similar to the human brain, by using processes that mimic the way biological neurons work together to identify phenomena, weigh options and arrive at conclusions.

Porting: In computer science, it is a process of adapting, sometimes with modifications, a software component to enable its use on a platform different from the original one. Porting is done when the software is somehow adjusted, not when the source code is completely rewritten in a different programming language.

SHA-256: 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.
