24 July 2023

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

ASIC EnhancedBoost – Patent Application

QBT (AIM: QBT) is pleased to announce that its cryptography expert and Cryptographic Optimisation team have developed what the Board believes to be an innovative approach to SHA-256 optimised computation for Bitcoin ("BTC") mining. The Company believes that this novel approach, called Message Scheduling For Cryptographic Hashing ("MSFCA"), addresses one of the most challenging problems in BTC mining: partial pre-computing of future blockchains' blocks.

A patent application in respect of MSFCA has been filed at the UK Intellectual Property Office. If the application is successful, the Company intends to apply for the patent to be extended internationally.

SUMMARY

- MSFCA can perform pre-calculations for future BTC blocks before the current block is closed
- Allows miners to use less logic gates, thus lower energy costs
- Implementation can be made to QBT's current SHA-256 architecture with feasible modifications
- Effective potential area saving is around 8%

BACKGROUND

Approximately every ten minutes a block is added to the BTC blockchain. Each new block represents the confirmation of the validity of the encrypted transactions, i.e. transfer of BTCs between senders and receivers, usually between, on average, 2,000 and 3,000. The miner who finds the winning hash for the block within ten minutes, causes the block to be closed and receives the reward; currently 6.25 BTCs, plus the transaction fees. A new block in the following ten minutes can then start to be processed, but only when the previous block has been closed, because the starting information to compute the new blocks, contains information from the previous closed block.

MSFCA

The computational optimisation obtained by MSFCA allows, under BTC mining special conditions, the miner to asynchronously perform (i.e. not within the temporal boundaries of the current block being computed) partial pre-computations of future blocks, before the ten minute computation 'time target' for closing a new block begins. The benefit being that all the logical gates and computation time on the ASIC chip needed for the specific partial pre-computation are saved.

QBT believes this is a novel procedure, potentially capable, in certain conditions, of addressing a key BTC mining limitation that prevents asynchronous pre-computation of a new block in the blockchain prior to the previous block being closed.

Application of MSFCA is not believed to enhance SHA-256's computation performance time; however, by enabling partial SHA-256 pre-processing of the block, it makes it possible to save the hardware resources otherwise necessary for standard SHA-256 computation. From this perspective, it is anticipated that energy would be saved due to less logic gates being present on the ASIC allowing the same chip area to be used to implement additional SHA-256 engines and increasing the overall speed of the process.

The key principle of this approach is that the partial pre-computation can occur asynchronously. Implementation of MSFCA will require a specific ASIC architecture, hence a specific ASIC chip will need to be designed, however the Company believes this would only require a feasible modification of the current SHA-256 proprietary implementation being developed by QBT.

In terms of SHA-256 ASIC chip areas, the projected potential saving would be in the region of 25% for one instance of SHA256 out of the three instances involved in Bitcoin mining. However, because of other well-known optimisation techniques, the effective potential area saving of MSFCA is estimated by the Company's ASIC designer to be around 8% on average.

The handling of pre-processed data requires additional circuitry, the impact of which is expected to be negligible in the near future.

While MSFCA can be implemented with currently available technology, by adding a logical gate overhead, in the near future, the Company believes these overheads will be less relevant, making this approach even more competitive.

Despite present technological limitations, (for example, the limited throughput of memory chips), the Company believes that it is strategically important to file a patent application covering the novel approach created through the use of MSFCA.

Francesco Gardin, CEO and Chairman commented: *"While at this juncture we cannot go into the specific details of what we believe is an innovative solution designed by our R&D cryptography team, suffice it to say that the new concept behind this idea disrupts, under special conditions, a fundamental BTC blockchain paradigm; computation for future blocks can take place before the previous block is mined. This is quite a radical change of the paradigm, and we believe it is well worth a patent application.*

"The current advantage of this approach is the partial pre-processing of a future BTC blocks, thereby potentially making redundant a large number of logic gates of a BTC mining ASIC chip, representing a material cost saving, when considering the hundreds of thousands of ASIC chips used in any mid-to-large sized BTC mining facility."

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
Kasia Brzozowska

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

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.

Asynchronous Pre-Computation: Computation performed in advance of the main computation, reducing therefore the amount of logic gates or software code of the main computation.

Chip Area: The silicon area of a computer chip used by the logical gates, measured in square millimeters. In general, the smaller the area the less energy required.

MSCFA: Acronym of Message Scheduling For Cryptographic Hashing, which is a key part of the SHA-256 Algorithm to be computed before the 64 compression steps.

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.

Ten Minutes Computation Time Target: is the block time on the BTC blockchain, which is 10 minutes. This means that every 10 minutes a new block of transactions is added to the blockchain and transactions within the block are considered to be “processed”.