

## **Quantum Blockchain Technologies Plc**

("QBT" or "the Company")

### **Update on FPGA and ASIC Development**

The board of Quantum Blockchain Technologies (AIM: QBT) is pleased to announce that its first phase of the FPGA development has now been completed.

#### **HIGHLIGHTS**

- Disruptive Bitcoin mining technology development is well under way
- QBT researching multiple routes to faster Bitcoin mining
- Bitcoin algorithm core architecture for an FPGA chip has been selected and modification completed
- To keep costs low, initial testing performed on an FPGA chip
- Architecture design work for ASIC prototype to commence before year end
- Testing will commence on the final design of the more expensive / faster ASIC prototype chip by end of Q1 2022
- Ultimate goal is to produce an enhanced 7 nanometers (nm) ASIC chip
- Early internal calculations show a final chip that could perform 24% quicker than current best available ASIC

#### **OVERVIEW**

The goal of the Company is to develop disruptive Bitcoin mining technology, to mine both faster and with less overall energy consumption than current practices. A number of advanced technologies are being used by QBT to achieve this goal; namely, quantum computing, AI Neural Networks - Deep Learning, Algebraic-Boolean reductions, Very Big Data, Cryptography and custom chip programming and design - using GPU, FPGA and ASIC chips.

The current technique used by producers of Bitcoin mining technology on dedicated computers to achieve the fastest performance, is by manufacturing single purpose, customised ASIC chips, which can perform only one wired function, i.e, the computation of the double hashing; the SHA26 cryptographic algorithm used to extract Bitcoins. The simple reality is that the faster the algorithms are computed and the more ASIC chips deployed, the more chances a miner has to extract Bitcoins.

Before manufacturing an ASIC chip, which is an expensive operation, there are usually two initial steps; firstly, to develop the logic gates architecture which will be used by the final ASIC chip – this is performed on a cheaper but slower chip, called an FPGA, which already contains some pre-defined functions - and secondly, by customising the design to take advantage of the greater freedom offered by ASIC technology, initially by manufacturing a prototype in a small batch, to keep costs low. The final stage, manufacturing the completed ASIC chip, is an expensive process, but the end result is a very small scale (currently up to 5nm) processing chip, which is significantly quicker, leading to greater results when mining Bitcoin.

QBT has now completed the FPGA development phase and is moving to develop its ASIC prototype.

Initial estimates derived from the FPGA performance obtained from our internal testing, would indicate that when the final industrial ASIC prototype design is completed it could outperform the fastest ASIC chip, currently being used to mine Bitcoin by at least 24%.

Moreover, early experimental evidence, using AI techniques to multiply by several factors the speed of an FPGA for computing the Bitcoin mining algorithm, would make even an FPGA a competitive Bitcoin mining tool. This same principal would apply to ASIC and other existing commercial mining tools. Tests on this innovative approach, will continue over the next three months.

## **DETAILED VIEW**

Following testing of a variety of design options, an unrolled SHA-256 architecture has now been implemented, with a number of existing optimisations coded, for QBT's FPGA chip prototype.

The Company's patented ASIC ULTRA Boost improvements (patent under application) will be added in the next few weeks, as a result of the close cooperation between the in-house cryptography expert and the Company's FPGA designer.

Current performance of the Bitcoin mining architecture developed by QBT on the FPGA (based on 16nm technology, at 600MHz basic cycle and the average general purpose available coding area) is 2.8 Giga Hash per second (GH/s) with an estimated 50W energy consumption. The ASIC ULTRA Boost optimisation should improve the above performance by 7% as previously reported.

To put things into context, our in-house expert has calculated that, as of today, a top of the range FPGA (using QBT's architecture of the implementation of the algorithm, to make it run at approximately 15 times faster than the standard FPGA), is still approximately 23.4 times slower than the best-in-class existing 7nm ASIC Bitcoin mining chip and much less energy efficient.

It was never the Company's intention to compete on speed and energy efficiency against an ASIC chip, using an FPGA chip but, in order to keep testing costs significantly lower, it has been a necessary step for QBT to take in this phase of its development. As a result, the Company is now in a much better position to assess the performance projection of its SHA256 Bitcoin mining architecture, and therefore the team is confident that it can now transfer this solution over to an ASIC chip.

Preliminary approximate calculations indicate that on a 12nm ASIC chip, extrapolated by comparing it to a commercial mid-range 16nm ASIC Bitcoin mining chip (with circa 300 million gates), our ASIC could achieve a double hash rate of 392 GH/s, with the ASIC ULTRA Boost optimisation adding an extra 7% as previously announced, reaching 419 GH/s, which would still be 2.26 times slower than the fastest ASIC commercially available.

However, the Company strongly believes that when compared with the best commercial 7nm ASIC chip for Bitcoin mining available on the market today, an industrial production of QBT's ASIC at 7nm, would indicate a double hash rate of 1.19TH/s, hence 24% faster.

This performance of QBT's architecture on the 7nm ASIC, doesn't yet include the 7% efficiency achieved by the optimisation of the patent application filed in September, which is still to be implemented. The current work on a second patent by the Company's cryptography expert will hopefully lead to further material optimisations.

Detailed simulations on energy consumption will be run as soon as our ASIC gate design layout is completed.

ASIC programming will start this month, and we estimate that by the end of Q1 2022 we will be able to announce when the first batch of prototype chips will be available for in-house testing. Following the completion of testing, the Company envisages that chip production, for QBT's own use, will commence by the end of 2022.

Concurrently, QBT's R&D team is also considering an alternative SHA256 computing approach (which is categorised as the basic Bitcoin mining algorithm), and this will be tested within the next three months. The joint effort by the members of our AI team and the Company's FPGA expert, could improve the current FPGA hash rate of 2.8GH/s by a highly material multiple factor, making mining by the slower FPGA chip potentially competitive against the best-in-class ASIC chip. Should this route be successful, mining via this method could commence as early as Q2 2022.

These AI techniques, if successful, could also improve the performance of current commercial ASIC Bitcoin miners.

The Company's new R&D IT infrastructure, which will also allow for Bitcoin mining tests to be carried out, will be operational in five weeks' time. The wait has been due to the serious worldwide shortage of silicon chips, which is delaying the expected delivery of the hardware. However, the Company has adopted the heavy use of cloud resources in order to avoid any interruption in the R&D activities to the various groups.

The Company remains very confident on the R&D strategy it has adopted which it believes could result in disruptive Bitcoin mining. It is worth noting that the Company's R&D programme is fully funded until the end of 2022.

**Francesco Gardin, CEO and Chairman of QBT, commented,** "Our R&D has delivered some very impressive results in a very short time: In only four months since the programme commenced, we have filed a patent application where we believe the ASIC ULTRA Boost has improved the standard mining algorithm, after five years of little or no progress following the publication in 2016 of the ASIC Boost paper.

"We will soon be ready to start the design of our ASIC Bitcoin mining chip which, on paper, already outperforms, in speed, the current best in class ASIC Bitcoin mining commercial solution. This significant improvement is before the implementation of the new optimisation from ASIC ULTRA Boost and we are confident that our second patent application, which is under development by our cryptography expert, will add a further radical improvement to the process, including also a reduction in energy consumption.

"All our other teams are working extremely hard on the other R&D fronts: Quantum computing and AI Neural Networks-Deep Learning and algebraic-Boolean optimisation. Meanwhile an AI accelerator will be tested within the next three months, which we believe could radically improve the performance of existing commercial miners, as well as our GPU, FPGA and, in the near future, our AISC chip. We consider that the R&D activity undertaken by our group of 15 experts is unbelievably exciting and, if successful, could potentially be radically innovative for the industry."

**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:**

**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

**FPGA:** A field-programmable gate array is an integrated circuit designed to be configured by a customer or a designer after manufacturing – hence the term "field-programmable". The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC).

**GPU:** A graphics processing unit (GPU) is a computer chip that renders graphics and images by performing rapid mathematical calculations.

**Nanometer:** A nanometer is a unit of measurement that is equivalent to one billionth of a meter. It is widely used as a scale for building tiny, complex, and atomic-scale computing and electronic components, such as ASIC chips.

**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.