This article is devoted to the implications of the development of quantum computing technologies for distributed ledgers.

At the beginning of the article the authors give a brief information of the key principles of blockchain technology and its importance in the modern world. (By 2025 about a 10% of global gross domestic product will be stored in blockchains. That fact highlights the vitality of data security and transparency for blockchain).

First of all, I would like to argue about the possibility of breaking modern cryptographic algorithms with the help of quantum computers. The crucial part of today's bitcoin defense is one-way functions, for example it's easy to multiplicate two large prime numbers, but finding the prime factors of a given product could take many years for conventional computers. In addition, bitcoin requires that the hash, which is a one-way function used to creation a digital signature for everything, meets a mathematical condition. Anyone who wishes to add a block to the ledger must keep their computer running a random search until that condition is reached. However, within 10 years quantum computers will be able to calculate one-way functions each way and that method of encryption will instantly become obsolete. (It will be another mass extinction of information security, such as the cracking of Enigma or DES.)

The advantage of quantum computers is that they use physical effects such as superposition of states and entanglement to perform computational tasks. That provide quantum computers the ability to execute certain types of work much faster than conventional computers. Thus, wrongdoer equipped with a quantum computer could forge any digital signature, impersonate that user and appropriate their digital assets. Furthermore, quantum advance could give a few users who have use it possibility to monopolize the whole process of adding new blocks to the bitcoin ledger and sabotage any transaction. If nothing is done to update the protocols, cryptocurrencies will crash at moment.