other participating nodes. The absence of a single point of failure (meaning that there is no central entity to hack) makes it difficult to compromise the entire network. However, a 51 per cent attack, in which the majority of nodes is compromised, remains possible in theory, particularly in the case of permissioned blockchains, which count a much more limited number of nodes than public ones – although relatively difficult in practice. Vitalik Buterin's release of a new consensus algorithm in August 2018, that would require an attacker who wants to control the network to control 99 per cent of the nodes of the blockchain instead of just 51 per cent, could change the playing field (Buterin, 2018) and make attacks even more difficult to conduct. The highest vulnerability comes, in fact, from smart contracts, as the 2016 DAO* attack demonstrated, and from user interfaces (mobiles, laptops, etc.).

Another important point to bear in mind is that Blockchain's resilience relies on encryption* and algorithms, whose strength is based on computing power. Advances in technology, in particular quantum computing, could, in the long term, represent a threat to blockchain technologies. For the time being, current experimental quantum computers do not have sufficient computing power to break cryptographic algorithms. However, the community of cryptographers is getting ready. "Post-quantum" algorithms that would be resistant to quantum computing are being actively researched.

These challenges are significant, but the technology is still maturing and technological solutions are being investigated and developed.

(b) Interoperability challenges

The advent of Blockchain raises issues of interoperability both at a technical level (how various technical interfaces talk to each other) and at a semantic level (how information exchanged is understood by the various parties involved). Such challenges are not peculiar to Blockchain, but, as with other digital technologies, failing to address them would negate many of the benefits that Blockchain could bring.

(i) The digital island problem

An important challenge is that of the interoperability of the different existing blockchains, a problem made more acute by the search for alternatives to develop applications that meet the specific needs of various industries and that often follow different algorithmic approaches. Many platforms are being built that "do not talk to each other". For example, IBM's pilots use Hyperledger Fabric, while Microsoft's blockchain offer is built on the Ethereum blockchain. As for the R3CEV consortium,