REPLY specialises in the design and implementation of solutions based on digital media and new communication channels. Through its network of highly specialised companies, Reply partners with major European corporations in the telecoms and media, industry and services, banking and insurance, and public administration sectors, to devise and develop business models built on the new paradigms of big data, cloud computing, digital media and the Internet of Things. Reply's services include: Consulting, Systems Integration and Digital Services.

QUANTUM BLOCKCHAIN

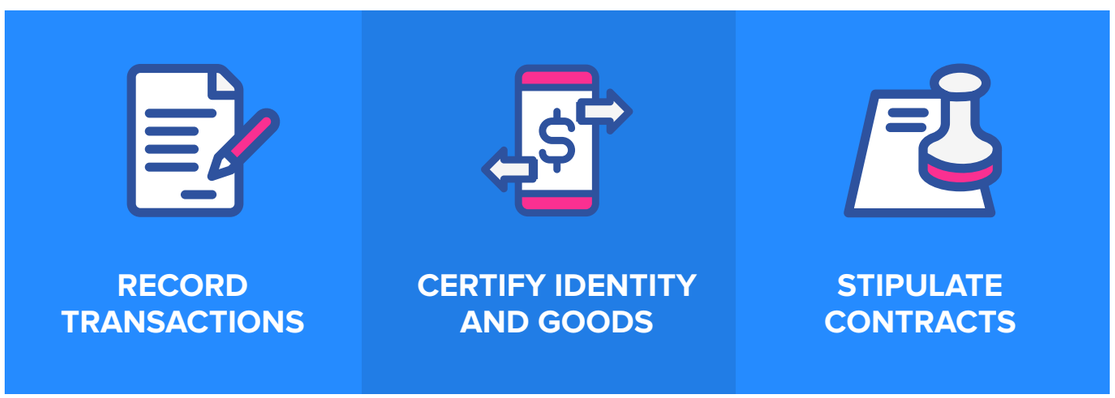
QUANTUM COMPUTING AND THE RISKS FOR BLOCKCHAIN

Blockchain is by now considered mainstream technology, a distributed and encrypted digital register, simultaneously accessible by the participants, which allows data recording, validation, updating and archiving. Data remains unalterable, unchangeable and non-replicable.

TRUST IN TECHNOLOGY

With Blockchain, trust becomes a systemic and financially affordable service and, for the first time in history, it goes beyond brokerage.

Transactions can be recorded, identity and goods certified, contracts entered into remotely without the need to involve institutions, regulatory bodies, banks and insurance companies. It is a trust machine, whose reliability rests upon technology, which is simultaneously a structure and guarantor. It allows for a substantial reduction in transaction and control costs. It is when it comes to money, assets or online purchases, that Blockchain shows its true potential; indeed, the first and best known field of application of this technology is for cryptocurrency, which exploded in the aftermath of the 2008 crisis, a time when capital to invest and trust in third parties responsible for the stability of the financial system had reached historic lows. Blockchain protects the Bitcoin system, thanks to its distributed nature: every single transaction is validated by the interaction of all network hubs, or miners, who participate in data verification activities by making available the computing capacity of the respective computers and by sending the validated information to the next block (securing a block reward or a bitcoin reward in return), within a quite literally “unhackable” chain. The decentralized management Cryptocurrency-like technological paradigm then lends itself to numerous fields of application: from the traceability of supply chains, to logistics, through gaming and up to guaranteeing voting systems and to protecting democracy.



WHY IS THE BLOCKCHAIN SECURE?

In any distributed Blockchain system, security, inviolability and integrity depend on the security of cryptographic algorithms.

Some of these algorithms are based on mathematical properties and on the theory of computational complexity, such as the problem of factorization of integers, a problem considered unsolvable within reasonable time when dealing with very large numbers. The security of cryptographic algorithms is the basis of the security of the network that makes up Blockchain. At present, these algorithms are considered safe: they are used by governments, have been approved by security bodies such as the U.S. NSA and are subject to peer-review by the scientific community.

But what would happen to the Trust Machine if current knowledge were disrupted by new algorithms or new computers with computing capabilities that go beyond “traditional” computer science, capable of solving even the factoring of very large integers in a few weeks, “in the space of one night”, if not within a few minutes? All platforms using encryption technologies, all Blockchains, are vulnerable to Quantum Computing, starting with bitcoin systems.

THE RUSH TO QUANTUM COMPUTING

Although, in some ways, Quantum Computing is still a frontier issue, there are several studies that estimate that in a few years, probably 10 or 15 years, it will be possible to have a sufficiently stable, mature and powerful hardware, which exploits the laws of quantum mechanics and can be used for processing that is unthinkable with standard computers. The affirmation of this technology will be definitive when quantum computers will reach at least 1000 qubits stable, with high fidelity gates. Google is currently the closest to the goal, with its 72 qubit Bristlecone processor, but the Californian giant is not alone.

There are many large hardware and software players that invest large sums of money in experimenting on Quantum Computing and have announced the imminent release of beta versions of their respective cloud services for Quantum Computing: from IBM to D-wave, all the way to Microsoft, Amazon and Alibaba.

RED ALERT: QUANTUM COMPUTING

Blockchains such as bitcoin and others use many encryption technologies that, to simplify, can be divided between three categories.

SYMMETRIC KEY ALGORITHMS

CRYPTOGRAPHIC HASHING ALGORITHMS

PUBLIC KEY ALGORITHMS

Bitcoin uses the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm, a public key algorithm based on Elliptic Curves. This algorithm is used in the latest https certificates, which are used in most websites around the world. To crack this algorithm with a traditional computer it is necessary to perform a number of operations that grows exponentially with respect to the size of the key. Asymmetric key technology (or public/private key cryptography) represents one of the most vulnerable elements in the set of technologies used by bitcoin. With a sufficiently powerful quantum computer, the number of operations required to overcome the inviolability of the key and substantially crack the ECDSA is greatly reduced, thus transforming the problem from exponential to polynomial. Scientific studies estimate that a quantum computer that is powerful enough to crack an ECDSA key in less than 10 minutes may become available in 2027. Another element of Blockchains threatened by Quantum Computing is the mining problem. Mining refers to a shared “challenge” between all peers of a Blockchain network, upon which the construction of the Blockchain is based. In bitcoin the mining problem uses cryptographic hashing functions, such as SHA256.

Thanks to Grover’s algorithm, quantum computers have a quadratic advantage in compromising some properties of cryptographic hashing algorithms. This advantage may compromise the neutrality of the Blockchain, if a node equipped with a sufficiently powerful quantum computer participates in the peer network. This threat could expose the system to the risk of producing a non-neutral block sequence or even allowing the double-spending of cryptocurrencies or their destruction, therefore undermining the foundations of this digital economy.

BLOCKCHAIN TECHNOLOGY IS FOREVER?

For every cryptographic technology there are post-quantum solutions.

1 **SYMMETRIC KEY ALGORITHMS**

It may be sufficient to further increase the key size, thus increasing the level of complexity in such a way as to make the problem almost unsolvable even on quantum computers.

2 **CRYPTOGRAPHIC HASHING ALGORITHM**

The solution is to stop using them, implementing an alternative mining strategy, such as the “Proof-of-stake” strategy.

3 **PUBLIC KEY ALGORITHMS**

Important scientific research has been developed on public key algorithms and dozens of post-quantum algorithms that cannot be cracked by quantum computers, but which are not yet widely used (for example, in https certificates), because they are still the subject of research or because they have significant disadvantages when used on traditional computers.

A hard fork of the Blockchain is required to implement these solutions in the public chain model, which means, in turn, that the majority of peers participating in the network must share these new rules.

CHANGE TO KEEP UP WITH TIMES

If Blockchain has spread and become so important it is because it is considered immutable and guaranteed, just like the deed by a notary or an insurance contract; therefore, the expectation is that Blockchain will be considered safe for a very long period of time, going so far as to guarantee immutability, even in a remote future.

Distributed, shared and systemic trust is at the base of the success of this technology (and economy). Blockchain can be a reliable and safe technology even in the era of Quantum Supremacy. To preserve it, it must be re-designed in a post-quantum perspective with a sense of responsibility and foresight. The experience honed in the areas of Security, Blockchain and Quantum Computing (with practices created in partnership with Google, Amazon, Microsoft and many others...) and the specific skills developed in each industry are the background and tools by which Reply designs solutions that are effectively safe and perform within a long-term perspective, for and with its Customers.

WHERE REPLY CAN MAKE A DIFFERENCE

For over two years, Reply has been working with multidisciplinary teams, exclusively dedicated to Quantum Computing, to develop quantum algorithms and translate some machine learning algorithms into quantum optics.

Reply adds its consolidated experience in the finance arena to its expertise in Quantum Computing, as it pertains to the use of blockchain applications and the hardening of security, in order to support and prime its Customers for the advent of the quantum revolution.