REALSEC's CEO Interview

What is REALSEC's perception about Blockchain's current status and evolution and growth prospects in general and especially in Spain and Latin America?

By 2020, under the circumstances of the pandemic, the process of digital transformation has accelerated, so what was once an option has become an imperative.

The new economy requires us to adopt new business models with a high component of innovation, purely digital.

Disruptive technologies are today, and are expected to be in the coming years, the fastest and safest way to reclaim the new economy.

Companies and institutions that do not bet on improving their productivity, efficiency and business agility, through new business models (innovation) and betting on digitization, will become a vestige of the past.

Twelve years after the creation of Blockchain technology, announcements such as the launch of the "sovereign yuan" by the Bank of China, have piqued interest from Governments and Central Banks around the world in moving towards a regulatory framework for blockchain technology, including the ECB (European Central Bank) itself.

This new context, away from both cryptocurrencies as a means of enriching itself and the first pilot projects to verify their potential, Blockchain is perceived in 2021 as one of the five main technological strategies for a large number of companies in various sectors, including many Spanish and Latin American companies.

What points would you stand out from this study from the previous one about the State of the Art of Blockchain?

In terms of investment, the State of the Art study report conducted at the end of 2019 estimated that investment in Blockchain in Western Europe, by 2020, it

would reach $1,169 M with a sustained growth trend up to 2023 of 53% and in the case of Latin America, that investment would reach $77 M by 2020 with a sustained growth of 45% by 2023.

Regard to sector-by-sector investment, the 2019 report estimated that the sectors that would lead the largest volume of investment would be the financial sector, industry and distribution.

In the latter study, these predictions are not only maintained, in the case of Western Europe, but are increasing upwards in the case of Latin America.

Regarding the incorporation of Blockchain technology by sector, in addition to the financial sector, industry and distribution, the current study highlights the significant penetration of Blockchain technology in the services sector.

Other highlights of the current study in Spain are: 1) that the penetration of Blockchain into the Spanish business already reaches 11%; 2) that 1 in 4 organizations with more than 50 workers are Blockchain users or have plans to be, and 3) that 46% of large companies think the Blockchain concept associated with cryptographic hardware offers greater guarantees of security and confidence in encryption and electronic signature processes.

Why does encryption and digital signature using cryptographic hardware reinforce Blockchain's presumptive security?

The weaknesses of Software-based cryptography vs Hardware-based cryptography is that, in many cases, the former does not inspire sufficient trust, due to the number of successful and public domain attacks that have occurred against Blockchain systems.

We have seen how some cybercriminals have managed to get hold of users' private keys, breaking the security chain, thus leaving the system compromised.

Essentially, it is worth noting the possible risks in the generation and custody of private keys and/or digital certificates, as well as the secure use of the digital signature necessary to perform the process of authentication and validation of transactions. The power and versatility of a certified cryptographic hardware allows you to issue and use all kinds of secure keys to protect any environment in the most diverse formats.

To all this, we must unite the immutability of the information and cryptographic functions that an HSM possesses, which can be used to perform Hash operations, maintaining integrity and anonymity in the network.

We must not forget that we start from the fact that one of the many advantages and benefits provided by Blockchain technology is trust between the different parts that make up the ecosystem, for which it is vital to maintain a high level of security and reliability in the operations of the system.

Use cases

More and more business projects are growing in production around the world, while use cases, such as pilot projects, are growing in private networks powered by Blockchain. From the emergence of Bitcoin's public network to date, multiple networks and methods have emerged, which far beyond cryptoactives, are used in various business processes.
If we focus on Blockchain's usability by sectors and business processes, we can highlight the following:

- Financial Sector: It is one of the sectors with the greatest projection, whose usability, beyond cryptocurrencies, is geared towards business processes such as: Payment Compensation, Cross-border Payments, Derivative Products, Commercial Registrations, Mortgage and Loan Registrations, International Transfers, Reconciliations, Settlements, Audits, Reporting, etc.

In addition, trading, clearing and settlement functions can be automated on a Blockchain network using Smart Contracts.

- Logistic Sector: Blockchain allows usability for International Trade, Ground Freight Transport, Product Traceability or Last Mile Distribution.

- Public Sector: In this case, although subject to current legislation, its usability could be oriented to verify the Digital Identity of citizens, the use of secure electoral voting, etc.

- Energy Sector: Blockchain facilitates the increase of operational efficiency, expanding visibility and speeding up compliance with reporting obligations.

- Healthcare Sector: Its usability can be oriented to the management of controlled clinical histories, patient confidentiality, new knowledge and research, drug control, etc.

- Food Sector: Use in this sector can bring high value to traceability and verification of product authenticity to prevent fraud, as well as improve food integrity and transparency.

- Real Estate/Construction Sector: Blockchain is ideal in this sector for the management of the entire value chain.

From land valuation to design, construction, marketing, delivery and maintenance of buildings.

- Education Sector: The use of Blockchain aimed at verifying the authenticity of academic degrees, masters, doctorates, certifications..., is a reality that provides a high value to prevent counterfeiting and fraud.

In short, the potential usability of blockchain technology is applicable to a broad spectrum of business processes and provides multiple benefits, including cost savings, efficiency, and increased security.

REALSEC has an important presence in the financial sector, a sector in which Fintechs have burst strongly. What advantages does Blockchain technology bring to the Fintech ecosystem?

Fintechs, in many cases, are an extension of traditional Banking itself and, in other cases, compete against it, taking advantage of its digital technology infrastructure.

In the first case, Blockchain was able to help both and other transaction networks to reduce their costs as much as their risks. We are talking about a technology that makes it easier for financial market participants to directly access dematerialized assets without having to go through other participants.

Currently, most financial market participants are disconnected from their asset deposits and settlement transactions require them to participate in a flow that is often costly, slow, and inefficient. Having a shared repository makes it easy for participants to interact directly with the depositary without having to involve third parties, allowing operations to be cheaper and more agile.

Regarding the second case, currently exists on the market Fintechs that use Blockchain technology directly in processes such as:

- Exchange from cryptocurrencies to money in circulation to make card payments on conventional terminals.

- Smart payment platforms for digital businesses: crowdfunding, second-hand sales, etc.

- Wallets for transactions with digital or virtual currencies, etc.

As for cybersecurity, what is REALSEC's value offering for the Blockchain environment?

The development of Blockchain in regulated markets, as is the case in the financial sector, requires a robust cryptographic technology similar as they have been relying on until now and whose level of reliability cannot provide the encryption and signature made by software, even if we make use of the same algorithms.

We believe that the keys used in Smart Contracts signing processes should be generated on certified cryptographic devices, both the generation and storage and custody of keys; as well as having the necessary mechanisms and tools for key management and recovery. (KCMS).

Blockchain technology is quite secure in its design and possibly suitable for usability in certain business processes, but for its incorporation into certain Banking processes, as well as in Defense or Government it requires certain changes, including improving cryptography layers to make them more resistant to current cyberattacks and those who will come, not taking many years, as a result of quantum computing.

For this reason, REALSEC proposes a platform that allows secure interconnection between "Peer to Per" networks and nodes (whether public or private) as well as hosting critical applications (BTC, ETH, Hyperledger and Corda). This platform, in appliance format, internally hosts the REALSEC HSM "Cryptosec-DEKATON" to perform cryptographic operations.

Applications can be virtualized and hosted in the cloud, so we can have a hybrid cloud scheme.

The HSM acts as a cryptographic engine, integrated with a quantum generator of random numbers, on which the post-quantum signature algorithms that NIST (CRYSTALS-DILITHIUM, FALCON and RAIBOW) or any other alternative algorithm that is certifiable to resist future attacks can be incorporated in the future.