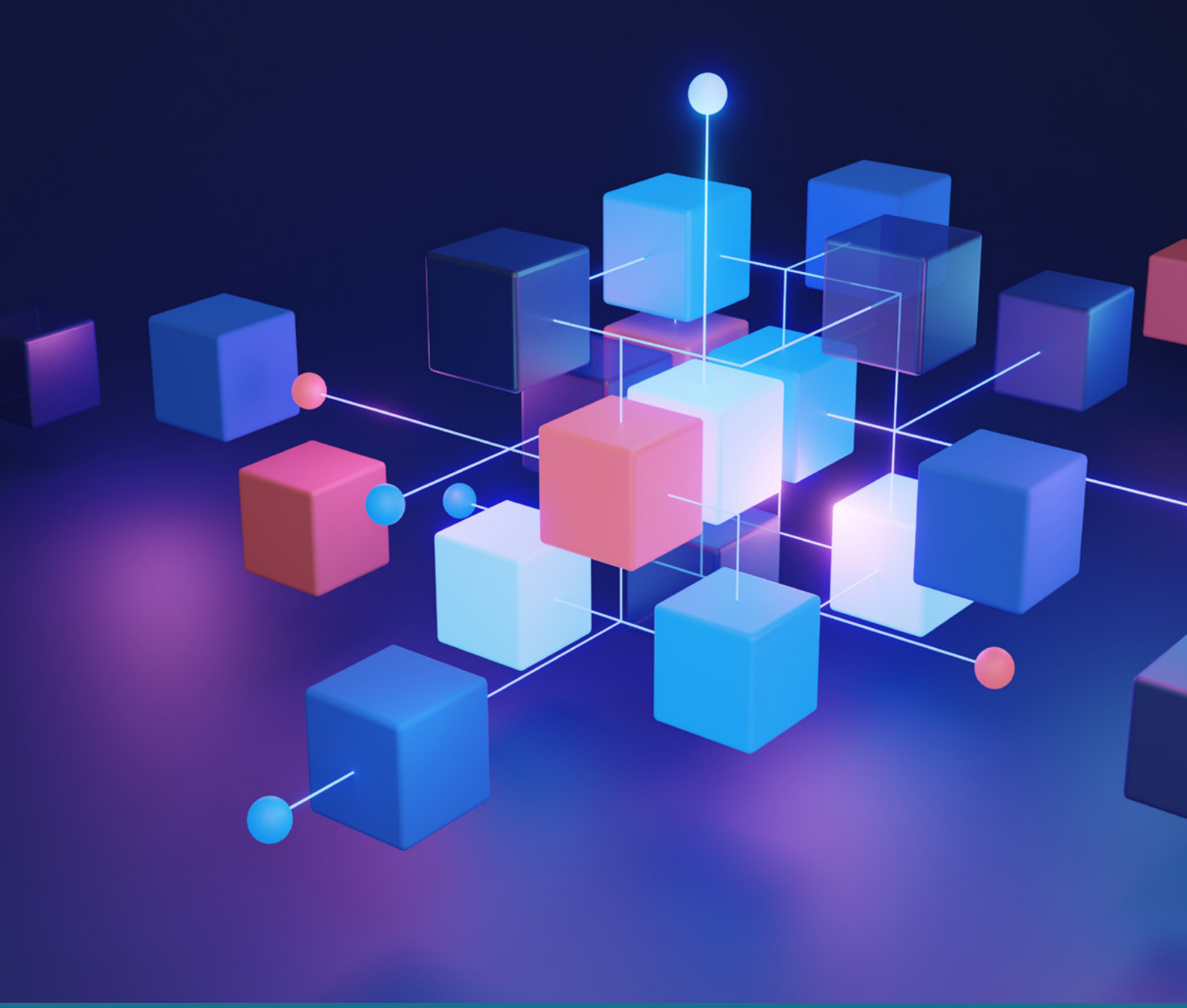


TechREPORT

Blockchain

SEPTEMBER 2023

LACCHAIN IDB IDB LAB

Table of contents

Authors:

Alejandro Pardo
Lucia Latorre
Marcos Allende
Antonio Leal
Mariana Gutierrez
Fernando Puerto

Contributors:

Jennifer Nelson
Sandra Corcuera
David Abensur
Fernando Pavon

TechLab

The TechReports are an initiative of the Emerging Technologies Laboratory of the IDB's IT department, known as TechLab, which is in charge of exploring, experimenting, and disseminating information about new technologies to learn about their impact on the IDB Group and the LAC region.

Acknowledgments: The IDB team would like to thank all the individuals who participated in interviews and provided key information for this document.

1. Executive Summary

Decentralized and immutable digital registers based on blockchain technology make it appealing for the development of applications in the public and private sectors where the integrity of the information needs to be secured and transparent.

The IDB Group has embraced and promoted the adoption of blockchain technology in the region. In order to develop the blockchain ecosystem in Latin America and the Caribbean, IDB Lab and IDB's Technology department founded LACChain in 2019, a global alliance between stakeholders from the public and private sectors to create an enterprise and government grade blockchain infrastructure suitable for real life solutions.

Some of the most relevant applications for the public and private sectors include transparency in procurement processes, transparency and verification of supply chains, health certificates, academic diplomas, and digital assets.

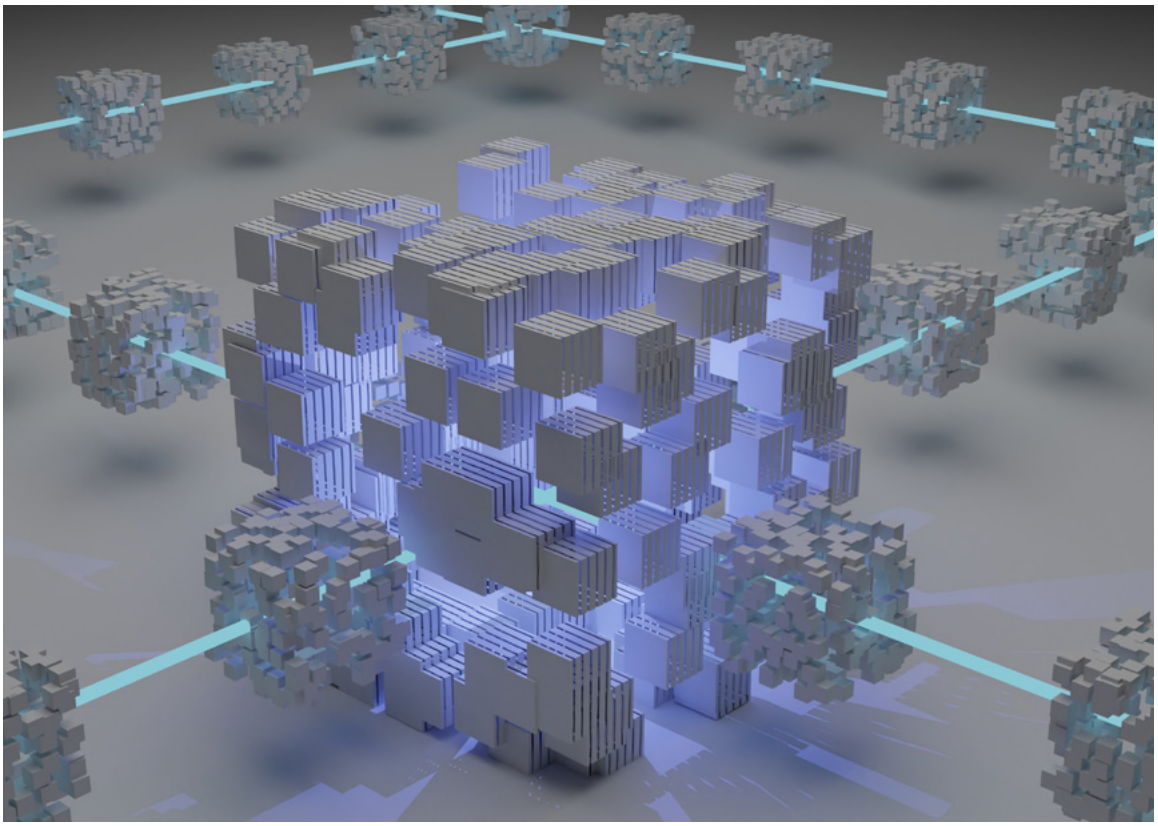
Across the world, institutions and organizations are taking advantage of blockchain technology to move forward their business and development goals. These include the Ministry of Labor in Peru creating a system for the verification of graduate certificates called Certijoven; Climate Trade a company that aims to empower large-scale decarbonization, created a system to track the offsetting of carbon emissions in Bolivia, and Colombia's financial superintendency and central bank approved the issuance of the first blockchain-based bond in the LAC region.

Specifically, IDB Group has supported projects in the region including the issuance of digital diplomas to graduate's digital wallets, self-managed domestic violence evidence collection, improved operations between the custom administrations of the Pacific Alliance and four other countries in LAC, proofs of concept of cross-border payments, and leveraging the LACChain blockchain network as a regional trust registry aligned with WHO[1] standards, enabling LAC countries' the issuance of health credentials and its verification in real-time and in a cross-border manner. ITE's TechLab has made an observatory of solutions available with up-to-date information on projects, vendors, and use cases.[2]

[1] https://www.who.int/
[2] https://idbg.sharepoint.com/sites/tech_lab#/observatory/technologies

As a result of the extensive experience the IDB Group has gained through working on blockchain projects, some key recommendations when starting a new project are: (i) select a blockchain network before a blockchain protocol, (ii) identify the project stakeholders to ensure project completion and solution adoption, (iii) design appropriate application program interfaces to integrate with the blockchain network. When it comes to regulation, it is important to consider the use case rather than the technology.

Lastly, it's important to keep in mind the ethical use of the data involved in the solution. All information registered in a blockchain network is transparent to all participants and immutable. Therefore, no data with a minimum sensitivity should be stored on the network.



2. Definition

Blockchain technology allows the creation of decentralized and immutable digital registers. The decentralized[3] nature of these digital registers comes from the distributed architecture and governance of blockchain networks, where there is no central authority or single point of control, and blockchain's distributed architecture ensures a copy of the chain of blocks[4] is replicated in the network nodes.[5] They are immutable because they only accept new entries and do not allow the editing or deleting of previous ones. These entries are arranged in blocks that get added by consensus and in a sequence to the original chain, each block linked securely to the other.

These characteristics make blockchain networks appealing for the development of applications in the public and private sectors, where the integrity of the information is secured by the cryptography used in the technology.

Depending on the use case and requirements, and according to ISO blockchain networks available today are[6]:

- **Permissionless public**: anyone can join at any time. Most of these networks are generally linked to cryptocurrencies. They are open and transparent but typically have high transaction fees and no privacy. Additionally, as participants are using pseudonymous, it is difficult for transactions and applications to enforce regulatory compliance.

- **Permissioned private:** a consortium of finite and well-defined entities that deploy, run, and maintain all nodes. Generally, these networks are developed and even maintained by a blockchain service provider. In general, private networks do not have transaction fees (although there might be a fixed cost charged by the service provider, if applicable), and allow for high levels of privacy. However, these networks are not decentralized nor transparent, and their scalability is very limited. In addition, they are usually designed for a single use case or application. Examples of permissioned private networks include the hundreds of private blockchain networks behind specific blockchain applications, the IBM

[3] Decentralization: The transfer of authority and responsibility from a centralized organization, government, or party to a distributed network
[4] Block: After a certain number of transactions have been added to the ledger and consensus has been reached among the nodes that the transactions are valid, they are then cryptographically locked into a "block" and officially recorded. This "block" forms the basis for the next one; in this way, they are all linked together in a chain.
[5] Node: Public blockchains consist of a network of computers that synchronize the network's data, coordinate transaction requests, and participate in consensus regarding the validity of those transactions; each one of these computers is called a 'node'.
[6] Source: LACChain Framework for Permissioned Public Blockchain Networks: From Blockchain Technology to Blockchain Networks https://publications.iadb.org/en/lacchain-framework-permissioned-public-blockchain-networks-blockchain-technology-blockchain

FoodTrust, and the blockchain network of the Energy Web Chain by the Energy Web Foundation (EWF) consortium.

- **Permissioned public**: these networks are open, transparent, decentralized, and generally do not have transaction fees. At the same time, every participant is identified so that both privacy and compliance with regulations can be achieved. Examples of these networks are Alastria in Spain, led by an association of over 500 members; EBSI in Europe, led by the European Union; and LACChain in Latin America and the Caribbean led by the Laboratory of Innovation of the Inter-American Development (IDB Lab).

The IDB Group has embraced and promoted the adoption of blockchain technology in Latin America and the Caribbean to empower vulnerable populations, improve digital security, and strengthen trust in the economy. As a result, LACChain was created in 2019 by BID Lab to develop the blockchain ecosystem in the Region. Forging an alliance with stakeholders from the public and private sectors, LACChain blockchain infrastructure is ideal for governments, international organizations, and organizations, in general, that seek to use the technology in a regulated space.

Within the LACChain project, LACNet was created as a non-profit independent legal entity based in Uruguay to serve as an orchestrating vehicle for the networks developed under the LACChain framework as well as other networks developed in Latin America and the Caribbean.

3. Applications

Blockchain has many uses, the widely known is the use of cryptocurrencies, as for example Bitcoin or Ether, among others. In this report, we are going to deep dive in the blockchain enterprise use cases where IDB is fostering different use cases that will impact the lives of vulnerable populations in Latin America:

A. Digital Identity: Nowadays everyone has digital profiles on different platforms, but this information is owned by the platform owner and used according to their terms of service. Using blockchain technology to implement Self-Sovereign Identity digital identity (DIDs) credentials can be stored in digital wallets that are trusted, fraud-resistant, portable, interoperable, and privacy-preserving. A digital identity owned by an individual can streamline the process of obtaining benefits for citizens while enhancing privacy by curating personal information to be shared with others.

B. Verifiable Credentials: Built on top of digital identity, a verifiable credential (VCs) can be issued, held, and verified as a digital version of a title, such as an employee identification card, digital birth certificate, and digital educational certificate. Today, as an example, the diploma mill industry is worth more than $200 million a year, issuing fake diplomas for an average cost of $1,000 for a master's or PhD degree. With a verifiable process on a blockchain network, credentials are verified instantly without sharing personal data and ensuring tamper-proof and decentralized information.

C. Cross-Border Payments: International money and value transfer demands transactions to be settled and cleared in different trust registries, which in most cases involves manual processes. These reconciliations usually take days and lead to inefficiencies, risks, and higher fees. Blockchain technology allows to represent value and assets on-chain using smart contracts, which allow to automate the lifecycles of value and asset transfer. When value is exchanged over blockchain networks, transactions can be settled and cleared in real-time without any post-trade processes. This increases efficiency and reduces costs, while also allowing for more transparency and auditability. Blockchain can also be very helpful to enable better means for transferring international aid in the form of official development assistance and conditional cash transfers, having an impact on development and financial inclusion.

---

[7]https://www.researchgate.net/figure/Some-Estimates-of-the-Business-of-Fake-Degrees-Worldwide_tbl1_235976192
[8]Smart Contracts: automated actions that can be coded and executed once a set of conditions is met.
[9]https://publications.iadb.org/en/cross-border-payments-blockchain[8]https://makeavideo.studio

D. Traceability: Supply chain and international exchange of goods can sometimes be challenging due to the number of actors and validations involved. Technology currently appears as a disruptive instrument to favor this relationship of trust, by providing mechanisms of verification and traceability[10]. Blockchain technology at the end-to-end supply chain logic can be programmed into smart contracts among participants, keeping a tamper-proof record of activities along the supply chain for accurate, actionable, and immediate transparency along the process[11].

E. CBDC: Central Bank Digital Currencies are the digital version of a country's fiat currency that is issued and backed by a central bank. Unlike decentralized cryptocurrencies like Bitcoin, CBDCs are centralized and controlled by a central authority. CBDCs are being explored and developed by several central banks around the world, including the People's Bank of China, the European Central Bank, and the Federal Reserve.

F. Digital Assets: Blockchain technology enables the tokenization of assets using smart contracts to define their features, rules, and permissions. These tokens[12] could be identical to each other in value, such as cryptocurrencies, or unique such as non-fungible tokens (NFTs).

[10] http://www.revistasice.com/index.php/ICE/article/view/7291/7327
[11] https://hbr.org/2020/05/building-a-transparent-supply-chain
[12] Token: a token represents an asset issued on an existing blockchain.

4. Blockchain projects throughout the world

1. Across the world, institutions and organizations are taking advantage of blockchain technology to advance their business and development goals. In Peru, the Ministry of Labor launched a solution called Certijoven[13] that allows beneficiaries under 29 years of age to issue certificates for non-criminal backgrounds, judicial, police, academic degrees obtained, or formal work experience.

2. In Bolivia, Zero Hunger in Pando seeks to offset carbon emissions with afforestation by issuing of SDG Corporate Securities based on Forest Carbon Bonds, recognized by the United Nations Collaborative Programme on Reducing Emissions from Deforestation and Forest Degradation in Developing Countries (UN-REDD)[14].

3. Similarly, Banks are testing the technology for potential mainstream uses in the future. The Asian Development Bank will seek to develop ways to directly connect in a blockchain network central banks and securities depositaries in the ASEAN+3 region[15], while Banco Santander issued the first $20 million end-to-end blockchain bond[16] opening the potential for a secondary market for mainstream security tokens in the future.

4. The World Food Program's Building Blocks[17] enables the secure access of multiple forms of assistance from different organizations via one access point to one million people in Bangladesh and Jordan, making it the world's largest implementation of blockchain technology for humanitarian assistance.

[13] https://lacnet.lacchain.net/certijoven-eng/
[14] https://market.climatetrade.com/projects?id=386
[15] https://www.adb.org/news/adb-develop-prototype-cross-border-securities-transaction-system-using-blockchain
[16] https://www.santander.com/en/press-room/press-releases/santander-launches-the-first-end-to-end-blockchain-bond
[17] https://innovation.wfp.org/project/building-blocks

5. Blockchain Solutions from IDB Group

The IDB has encouraged and supported projects across the Region. The following are featured projects that showcase different use cases. For a complete list of projects, please contact the Tech Lab or visit our Observatory of Emerging Technologies.[18]

Blockcerts Caribbean

Blockcerts in the Caribbean leverages blockchain technology for the issuance and management of digital diplomas in the Caribbean using digital wallets. The IDB is working with the Caribbean Examinations Council (CXC), responsible for the issuance of diplomas in 16 countries of the Caribbean, to enable digital issuance, management, and verification of digital diplomas.

Ni1 +

Ni1+ facilitates the collection and self-management of administratively valid evidence of violent acts to mitigate the effects of gender violence. This application is accessible from a mobile device to record evidence and online notarization, enabling administrative processes, and civil or penal complaints in Colombia.

Proyecto Cadena

The CADENA Project is a blockchain-based solution for real-time exchange of information regarding Authorized Economic Operator (AEO) certificates among customs administrations. It involves customs agencies from the Pacific Alliance countries (Colombia, Mexico, Peru, Chile), as well as customs agencies from Costa Rica, Bolivia, Ecuador, and Guatemala. The CADENA project has gained recognition from various international organizations and publications as an innovative initiative in the use of blockchain within customs and international trade. CADENA enables real-time interoperability between customs agencies, enhancing efficiency and security in the supply chain. Currently, efforts are underway to transition to production environments and to establish interoperability with other public and private entities.

LACPass

LACPass initiative aims to implement a regional pilot in Latin America and the Caribbean countries that enables all countries, independently of their level of digital maturity, to issue digital health certificates and records that are recognizable and verifiable in every other participant country. The project is working with LACCHAIN to learn about decentralized identifiers (DIDs) and how to send vaccine certificates to digital wallets based on the verifiable credentials standard.

Trazabilidad Fibra de Alpaca

Trazabilidad Fibra de Alpaca is the implementation of a traceability system for the production, processing and commercialization of Alpaca fiber in Peru using blockchain technology and digital wallets.

BME, BBVA and IDB Issue Spain's First Blockchain-Based Regulated Bonds

The Iberclear subsidiary of Bolsas Mercados Españoles (BME), along with Banco Bilbao Vizcaya Argentaria (BBVA) and the Inter-American Development Bank (IDB), have issued the first bonds in Spain to be listed on a regulated market and also registered.This platform opens the door for similar bond issues in Spain and Latin America and the Caribbean.

6. Recommendations for the development of blockchain projects

According to LACChain, blockchain technology should be used to register proof of the information that exists somewhere else. Blockchain is not optimized or meant to store sensible data nor large amounts of data and if large data is stored in the network, it would overload the servers resulting in a poor user experience.

When starting a new blockchain project, the LACChain team recommends following these steps:

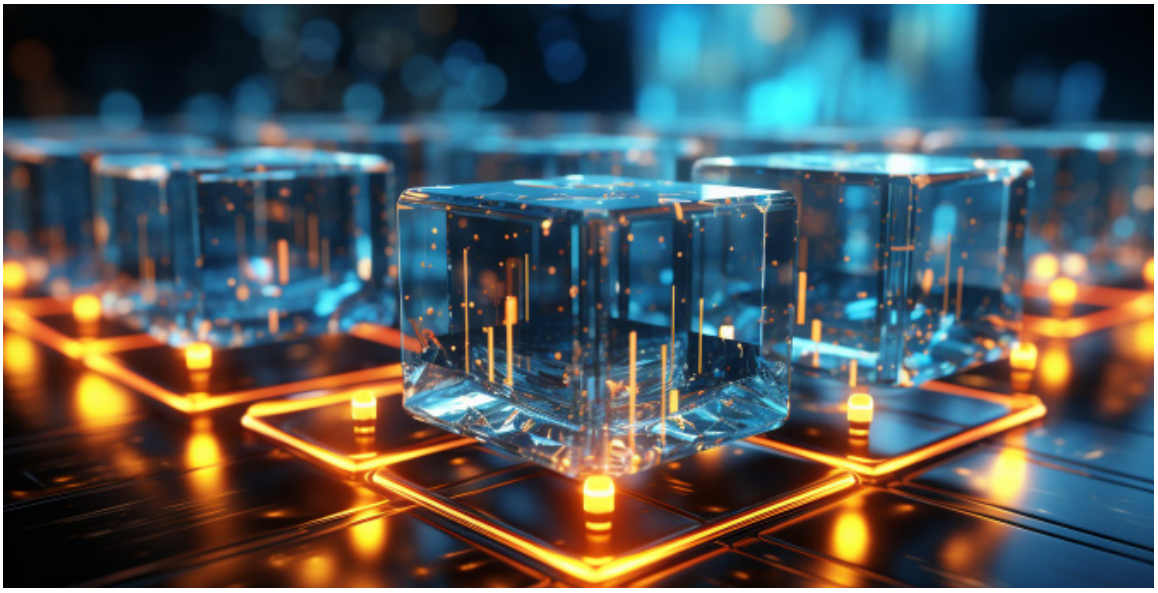
1. Define the scope and use case of the solution in order to select the type of network.

2. Identify the stakeholders and entities that will be part of the solution.

3. Identify the stakeholders and entities role in the solution.

4. Deploy the nodes and build the APIs and interfaces in a layered fashion.. Each node should have an identified owner and its own interface and API.

According to specialists in the Bank using blockchain in their projects, mention that it is extremely important to ensure that the counterpart has the technical and financial capability, to develop and maintain a blockchain solution over the long term. Knowledge transfer is an important component in any kind of project, but when the solution is based on an emerging technology, it's imperative to have the support of an expert willing to train stakeholders and the technical team responsible for the solution moving forward.



7. Best Practices for Blockchain Projects

1. Select the blockchain network before the blockchain protocol

It's important to understand the difference between blockchain protocols and a blockchain network. Currently, there are several blockchain networks available to choose from, but each has different protocols for specific use cases.

2. Establish stakeholders for each component of the solution

Blockchain-based solutions are meant to be decentralized, but that doesn't mean that it doesn't require human intervention in key processes such as technical and legal support. It's important to do a stakeholder mapping exercise when starting a project to identify key people, organizations, and processes and how that translates to each component of the solution.

3. Design APIs to integrate with the blockchain network

Transparency happens as long as every actor in the network can interface with the solution without intermediaries. This requires designing APIs to integrate the designed solution with the blockchain network and leverage the decentralized capabilities of the technology.

4. Regulate based on the use case

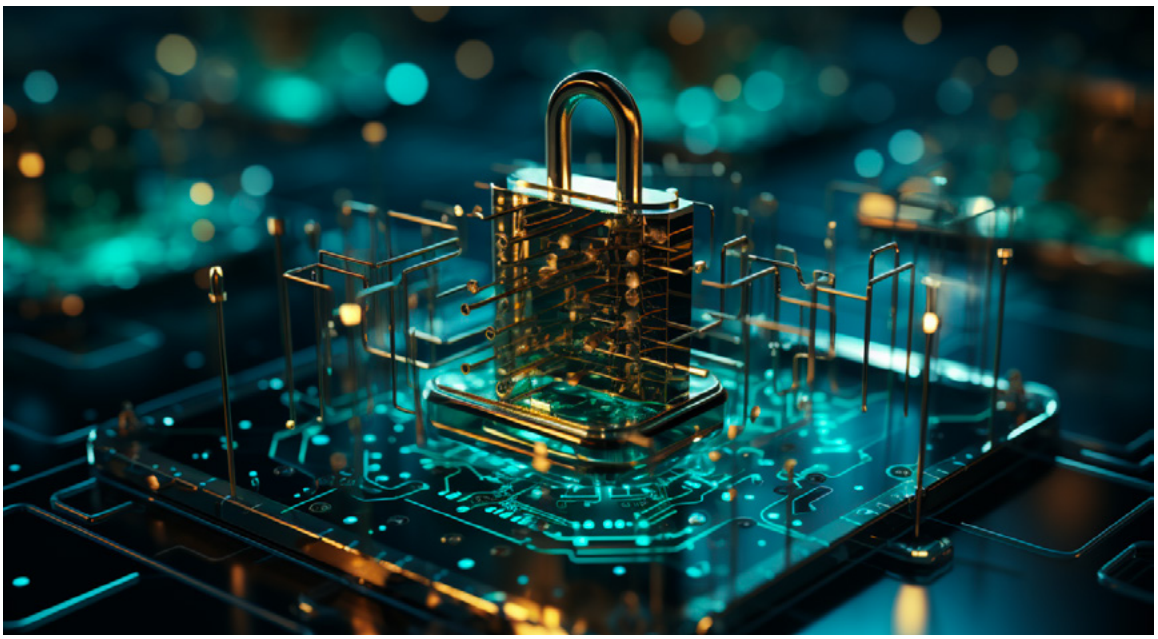
Blockchain simply registers the proof that information exists somewhere else. How that information is used is what needs regulation. For example, how data is being handled, depending on the type of data, privacy concerns, traceability rules, etc. Blockchain as a technology does not need regulation.

8. Security and Privacy

The Security team within the IDB's IT department recommends that users validate the supply chain of software components and assess the risk of using third-party software components or libraries that may have inherent deficiencies, such as encryption libraries or wallets with backdoors. Additionally, users should follow recommendations for securely managing encryption keys or passwords to prevent theft or other malicious uses.

On the other hand, everything that is registered in the network is immutable and public to all participants. Therefore, no data with a minimum level of sensitivity should be stored in the network. Instead, the blockchain only stores proof of the validity of the information in the form of "hashes."[19]

Lastly, it is important to note that the operation of blockchain relies on cryptography, which may become vulnerable due to obsolescence caused by the possible increase in computing capacity through emerging technologies like AI and quantum computing, posing future challenges and potential risks. Once quantum computing becomes real the cryptographic algorithm will be updated (and be more difficult) to handle computing power.



[19] Hash: In computing, 'hashing' is an operation performed on lists or sets of data to create a reliable index for that data.

TechREPORT

Blockchain

September 2023

LACCHAIN IDB IDB LAB