LACCHAIN FRAMEWORK FOR PERMISSIONED PUBLIC BLOCKCHAIN NETWORKS

FROM BLOCKCHAIN TECHNOLOGY TO BLOCKCHAIN NETWORKS

IDB IDB | LAB LACCHAIN

LACCHAIN FRAMEWORK FOR PERMISSIONED PUBLIC BLOCKCHAIN NETWORKS

FROM BLOCKCHAIN TECHNOLOGY TO BLOCKCHAIN NETWORKS

Author:

Marcos Allende, Technical Leader of LACChain and IT Specialist
in Blockchain, SSI, and Quantum Technologies at IDB, USA

Supervisors:

Alejandro Pardo, Leader of LACChain and Principal Specialist
at IDB, USA

Marcelo da Silva, IT Principal Specialist at IDB, USA

Design:

.Puntoaparte Editores

This paper has been elaborated by the LACChain DLT working group, which includes international experts in blockchain that participate in the working group in representation of member entities of the LACChain Global Alliance (https://www.lacchain.net/alliance). All the collaborators are acknowleged at the end of the document.

Copyright © 2021 Inter-American Development Bank This work is licensed under a Creative Commons IGO 3.0 Attribution- NonCommercial-NoDerivatives (CC-IGO 3.0 BY-NC-ND) (http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode) and may be reproduced with attribution to the IDB and for any noncommercial purpose. No derivative work is allowed. Any dispute related to the use of the works of the IDB that cannot be settled amicably shall be submitted to arbitration pursuant to the UNCITRAL rules. The use of the IDB's name for any purpose other than for attribution, and the use of IDB's logo shall be subject to a separate written license agreement between the IDB and the user and is not authorized as part of this CC-IGO license. Note that link provided above includes additional terms and conditions of the license. The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

TABLE OF CONTENTS

ACRONYMS

AES	Advanced Encryption Standard
API	Application Programming Interface
Bluzelle	Decentralized Storage Network
CPU	In EOS-based networks, CPU is a time-denominated resource which measures the amount of time an EOS BP should dedicate to a transaction
CBDC	Central Bank Digital Currency
DApp	Decentralized application
DH	Diffie–Hellman key exchange
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DNS	Domain Name System
DoS	Denial-of-Service Attack
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic-Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	Electronic IDentification, Authentication and Trust Services (European Union)
FIPS 202	Specifies the SHA-3 family of hash functions, as well as mechanisms for other cryptographic functions
Gas	Refers to the computational efforts required to execute specific operations on the Ethereum network
GDPR	General Data Protection Regulation (European Union)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDB	Inter-American Development Bank
IPFS	InterPlanetary File System
ISO	International Standards Organization
ISO TC307 WG5 TS23 635	International Organization of Standards Technical Committee 307 Working Group 5 Technical Specification 23636
KPI	Key Performance Indicator
libSSL	Portion of OpenSSL which supports TLS (SSL and TLS Protocols)
NET	In EOS-based networks, NET is a space-denominated resource measuring what share of a blocks' network representation can be used to store a transaction
NIST	National Institute of Standards and Technology
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SHA-2	Secure Hash Algorithm 2
SHA-256	Secure Hash Algorithm 256 bits
SHA-3	Secure Hash Algorithm 3
SSL	Secure Socket Layer
StorJ DCS	Decentralized Cloud Storage
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSS	Trusted Time-Stamping Service
UDP	User Datagram Protocol
X.509	International Telecommunication Union standard defining the format of public key certificates

The world is quickly transforming. The globalization and digitalization that started just a few decades ago has been exponentially accelerated by the COVID-19 pandemic. Each day, electronic communication, transactions, payments, and interactions of all types continue to grow. This growth has further prompted the growth of digitalized, digital, and crypto assets as well as digital information. Additionally, this rapid digital growth has created secondary effects, such as privacy violations, impersonations, hackings, and leaving those lacking access to the Internet without essential online services. The need for a reliable, transparent, private, and trustworthy digital world is clear and blockchain technology is a rapidly developing tool that can help provide these assurances. We believe that in the same way the advent of the Internet enabled worldwide communication and digitalization, blockchain can enable worldwide trust.

The IDB Group has been analyzing blockchain technology since the release of Bitcoin in 2009 and started funding blockchain-based projects in 2017. In 2019, the lessons learned from failure and success in various projects prompted the IDB Lab to launch a Global Alliance in order to develop a blockchain ecosystem in Latin America and the Caribbean: LACChain. LACChain has developed a framework, which is introduced in this paper, that presents a solution to the challenge of building multipurpose blockchain networks for enterprise and government use that allow for scalability of various blockchain-based projects. This framework is agnostic to blockchain protocols as it can and already has been adopted by networks using differing blockchain technologies. Most importantly, it addresses matters related to orchestration, governance, operation, responsibilities, technology, and regulatory compliance across sectors.

A NEXT GENERATION BLOCKCHAIN FRAMEWORK

Eco-Friendly, Multiprotocol, Multipurpose, Neutral, Privacy Preserving, Quantum-Secure, and Regulatory Compliant

Twenty-nine years have already passed since S. Haber and S. Stornetta published the paper "How to Time-stamp a digital document"[1], that proposes the creation of "a distributed network of users, perhaps representing individuals, different companies, or divisions within a company". This distributed network could work as a "digital safety-deposit box" where any of those entities would "transmit the document to a trusted time-stamping service (TSS)" that records the hash of that document together with its date and time and also involving a signature scheme to guarantee authenticity and ownership. With this, Habber and Stornetta wanted to achieve both linking and distributed trust.

Less than 17 years later, Satoshi Nakamoto released Bitcoin, the first network to be considered a blockchain, with the purpose of serving as a peer-to-peer ledger for electronic payments. Bitcoin became the first successful attempt of crypto-cash, after the failures of DigiCash, FirstVirtual, CyberCash, and many others. Previously, important cryptographers such as Chaum, Fiat, and Naor worked since the 1980s in the development of ideas to build e-money systems that allowed for prevention of double-spending without having to rely on a central authority[2]. Satoshi created a decentralized blockchain network that denominates electronic payments into cryptocurrency which only exists in a distributed ledger network and incentivizes participation with the cryptocurrency itself[3].

After the advent of Bitcoin, the creation of blockchain networks has proliferated, allowing users to record and link various types of transactions using hash functions. From 2008 to 2017, the vast majority of these networks were all permissionless and public. Similar to Bitcoin, they had an associated cryptocurrency. In 2013, Vitalik Buterin marked a turning point in this field by releasing the white paper for Ethereum[4], a network that runs programs called smart contract, which was finally released in 2015. People also started exploring commercial use cases for blockchain networks other than for simply backing cryptocurrencies. Before Ethereum, blockchain networks were primarily used for transacting cryptocurrency and time-stamping hashes. Ethereum smart contracts introduced new possibilities such as:

- Automating processes by defining complex functions and relations between them
- Creating several types of digitals assets (both fungible and non-fungible) with specific rules for issuance, ownership, and transference

After Ethereum, other protocols such as EOSIO, IoTA, Cardano, Avalanche, and Symbol have tried to improve the functionalities of permissionless blockchain technology by increasing the number of transactions per second and introducing new consensus protocols, among other features. In a different direction, initiatives such as Hyperledger Fabric, R3, Quorum, Hyperledger Besu, or Hyperledger Indy which have been strongly supported by IBM, Corda, JP Morgan, Consensys, and Hyperledger respectively, have reconsidered the concept of openness in blockchain networks and have come up with new protocols that are focused on permissioned ledgers and private channels, which also aim to maintain decentralization.

Since 2017, all of these blockchain technologies have contributed to the creation of thousands of blockchain networks which have hosted thousands of proofs of concepts and pilots, with generally satisfactory results for stakeholders. However, scalability has been a big roadblock for most of these projects. We believe that the reasons why most blockchain-based solutions do not scale well are that they are built on ledgers that are not properly designed as the instrumental piece of architecture needed by these projects and that it is not clear who is liable for what. There is rarely an upfront discussion about governance, data management and privacy, technical support, operational fees (e.g., tx fees), maintenance, regulatory risks, or sustainability in these decentralized networks.

We believe that there are enough blockchain technologies, such as Ethereum (and Ethereum clients such as Hyperledger Besu or Consensys Quorum), EOS, Hyperledger Fabric, Hyperledger Indy, Avalanche, Symbol, and Corda, with promising roadmaps and great development teams to develop robust blockchain technology that can be used for various applications. However, there is a big difference between blockchain technologies and protocols, and blockchain networks. In LACChain, we believe that there are many aspects that must be developed around any blockchain protocol in order to build a blockchain network that can be suitable for blockchain-based projects. These networks must present robustness, reliability, accountability, sustainability, scalability, affordable costs, and regulatory compliance.

According to the International Standards Organization (ISO), there are three types of blockchain networks[5]: permissionless public, permissioned public, and permissioned private (see Annex I). The LACChain Framework for Permissioned Public Networks presented in this document is focused on blockchain networks that are permissioned and public because we believe that, at present, these are the most suitable for enabling multipurpose applications that establish clear accountabilities, are compliant with regulation, are fully transparent, can have zero transaction fees, are eco-friendly, and respect user's data privacy. We want to emphasize our belief that permissionless public and permissioned private networks are also useful for some specific use cases, but our goal here is to address any government and enterprise use case, for which permissionless public and permissioned private networks have very relevant limitations.

One of the main issues with permissionless public blockchain networks, when considered for multipurpose government and enterprise use cases, is that anyone is allowed to join without any permissioning requirements, which implies that even identification cannot be requested. As a consequence, it is difficult to establish accountabilities in a network where nobody knows who anybody else is. Additionally, the transaction fees that are generally required for incentivizing block producers (a.k.a. validators or miners) and managing the demand are not affordable for most blockchain-based applications. Permissioned private networks, on the other hand, are not open and transparent, and thus, their scope is always limited, the degree of decentralization is generally low, and trust in the network is conditioned to trust in central governing entities.

From our perspective, permissioned public networks bring together different desired features from permissionless public and permissioned private networks that make them ideal for government and enterprise scalable and legally compliant blockchain-based applications. These networks can have the decentralization, transparency, and availability of the permissionless public networks while also allowing for identification of participants, establishment of accountabilities, and elimination of transaction fees.

This LACChain Framework is a set of recommendations that enables the creation of multipurpose network of networks that are robust, reliable, sustainable, compliant, scalable, and have clear accountabilities. The framework can also be applied to both permissionless public and permissioned private blockchain networks, but can only be fully realized in a permissioned public infrastructure. It is important to remark that it is not conditioned to any particular blockchain protocol. Indeed, this framework has already been applied to networks based on Hyperledger Besu and EOSIO blockchain technologies.

Our goal is to contribute to the construction of "the Internet of Value". The Internet, as a network to connect people and entities remotely, in its current form does not allow the transference of either digital (e.g., a digital certificate or a digital currency) and physical (e.g., a painting, a car, or a house) assets electronically with full trust between unknown parties unless there is a trusted third-party involved (e.g., Amazon). We believe the combination of the current Internet with a new robust and reliable blockchain layer properly provided with digital identity and digital money platforms can achieve full trust between remote and unknown parties without intermediaries, leading to a new digital era of digital services and transactions, and constituting the Internet of Value.

Last but not least, we want to highlight our belief that even if one single blockchain network takes regional or global leadership, this network will have to interoperate with other blockchain networks conceived in a totally independent way.

LACCHAIN FRAMEWORK FOR PERMISSIONED PUBLIC BLOCKCHAIN NETWORKS

1

ORCHESTRATION, OPERATION, AND GOVERNANCE

IDB IDB | LAB LACCHAIN

According to ISO TC307 WG5 TS23635, "DLT and blockchain systems governance is an approach that comprises elements of central and decentral decision rights, where the accountability is situated within the network and where incentives are provided to reach consensus […]. The governance of DLT & blockchain systems oversees several key functions during the operational stage of the DLT & blockchain system, such as the enrolment of participatory rights for participants in the DLT & blockchain system and the contracting rules associated with participation in the DLT & blockchain system. All DLT & blockchain systems shall operate within the broader context of external legal and regulatory frameworks; in some cases, DLT & blockchain systems may provide guidance and on-chain mechanisms for managing the operation […].".

We believe that one of the key missing pieces in blockchain infrastructures today is a clear definition of who is responsible for what. Working with decentralized technologies allows for decentralized governance mechanisms, while also facilitating interoperability and increasing transparency along with many other positive aspects. However, working with decentralized technologies does not eliminate the need to assure who will be held accountable when something fails.

It is not only important, but also essential, to know what can fail and who will be responsible for that failure when discussing the use of blockchain networks for government and enterprise use. This is necessary when discussing a university that will certify skills and course completions with blockchain-based certificates, or for an entity issuing a bond or a bank issuing digital money as blockchain tokens. At the end of the day, we see blockchain becoming one more piece of the architecture of digital platforms of all kinds. We envision entities having blockchain nodes that complement their existing databases.

We believe the current conversation taking place regarding the risks in blockchain technology use and regulatory compliance is partially misled. This conversation should not happen around blockchain technology as a whole, but rather around each blockchain network as a specific platform each with a particular framework. With these distinctions in mind, it is essential to evaluate the risks and the ways in which they are addressed and mitigated. Some of the most common risks when working with blockchain networks are illustrated by the following questions:

- What happens if my history is rewritten and my data and assets (e.g., cryptographic proofs of the digital credentials issued, digital bonds, digital money) are tampered with?
- What happens if the network stops generating blocks because validators stop reaching consensus?
- What happens if the network is forked?

- What happens if an entity engages in a denial-of-service attack?
- What happens if someone has registered illegal data (e.g., a link to a child pornography website) and all the nodes have a copy?
- What happens if someone sues "the network"?
- What happens if my smart contracts have bugs that are exploited to hack them?

We believe that the only way to answer these questions is to establish clear coverage for each of the risks. In order to do so while maximizing decentralization in node operation and governance, we have distinguished between three different concepts:

Orchestration: Minimum set of technical and administrative tasks to guarantee that a blockchain network is technically reliable, functions in compliance with regulation, is financially and energetically sustainable, and is scalable. These tasks include establishing contractual relationships with the entities running nodes to define liabilities, accountabilities, and responsibilities (e.g., through SLAs and terms and conditions); permissioning; monitoring; and technical support.

Operation: Tasks strictly limited to the administration of nodes. The operation includes technical tasks such as the deployment and maintenance of a node, which involves security, performance, resilience, and availability. The operation also includes assuming liabilities that the node operator has agreed upon in accordance with the network rules.

Governance: All the decisions that have relevance in the functioning of the network and affect the entities using it. These tasks include updating protocol versions, defining the genesis file, consensus protocol, and block generation, as well as changing the liabilities, permissioning rules, economic incentives, and other relevant decisions.

Block generation is intentionally left out of the orchestration. We believe that the orchestration of the network must not include any type of control or censorship over block generation. Moreover, as we will discuss in Section 2.3, any entity can operate nodes that play a role in block generation -by running validators nodes- provided that they are contractually committed to accept every transaction that is computationally valid and complies with the network rules (such as not exceeding the gas limit or being generated by a permissioned entity), and to ignore and/or report the ones that are not. The block generation should be as decentralized as possible, with identified, authenticated, and authorized entities taking turns to participate in a Proof of Authority consensus protocol following well defined rules (see Section 2.3).

1.1. Orchestration

This LACChain Framework proposes the construction of legal entities that assume responsibility for the orchestration of blockchain networks; a non-profit and non-losses Underlying Orchestration Vehicle plays the role of a neutral entity aimed at ensuring accountability. This framework proposes that the Underlying Orchestration Entity establishes formal best practices with each of the node operators, which we will cover in Section 1.2.

The orchestration vehicle emulates the role of Internet Service Providers in the blockchain world. This must not be confused with a blockchain-as-a-service approach, because it is not. The network orchestrator fosters principles for a social ledger whereby networks are able to achieve benefits by operating in a socially responsible manner, in alignment with ISO 26000[6]. Following the ISO TC307 WG5 TS23635 guidelines, we believe that the specific tasks that comprise the orchestration can be divided into three phases of the lifecycle: establishment, functioning, and termination. This orchestration needs operational executing bodies to execute the different tasks. We propose two executing bodies: a technical team and a permissioning team.

1.1.1. Establishment

The establishment phase is comprised of tasks from design to initialization of the blockchain network. The essential tasks of this phase include but are not limited to the following:

- Define incentives (e.g., economic and operational) that guarantee the blockchain sustainability.
- Define the framework that sets rules and allows for the establishment of technical, legal, and other bodies within the blockchain.
- Design and deploy the first block of the network that contains both soft (e.g., the initial set validator nodes) and hard rules (e.g., the consensus protocol).
- Enable clear and comprehensive documentation.

1.1.2. Functioning

The functioning phase is comprised of tasks related to up and running the blockchain network. The essential tasks of this phase are the following:

- Accomplish identity proofing and certification of nodes.
- Accomplish proactive research and development within the network to improve security, efficiency, scalability, performance, discoverability, and interoperability.
- Allow nodes and accounts to join the network (i.e., whitelisting) and remove them (i.e., blacklisting) when they violate agreements.[1]
- Manage the distribution of resources among writer nodes (see Section 2.6).
- Provide and maintain dashboards and monitoring tools and perform monitoring tasks.
- Serve as an essential legal entity to establish all necessary agreements on behalf of the blockchain network in order to guarantee its reliability, including establishing contractual relationships with node operators and any other institution when needed (e.g., insurance firms).
- Supervise the network and perform maintenance tasks to guarantee the network runs without issues and does not fail, collapse, or die.

1.1.3. Termination

The termination phase is comprised of tasks that take place after a network stops functioning. The essential tasks of this phase are the following:

- Define how data or assets (e.g., smart contracts, tokens, proofs of certificates) can be transferred, destroyed, or disposed of. In other words, provide solutions and mechanisms to manage value that was stored in the network.
- Guarantee access to the transaction history.

1.1.4. Execution

The executing bodies are the executing arms of the Underlying Orchestration Entity and they report directly to that entity. These bodies can be composed of members of the entities with nodes deployed in the network. The Underlying Orchestration Entity is responsible for enforcing delivery of the type of service that the Underlying Orchestration Entity has agreed to with all entities running nodes in the network (see Section 1.2).

[1] The conditions under which a user is given access to a blockchain network (in permissioned networks) is based on the acceptance of the network's terms of use. These access rules are entirely determined by an underlying orchestration entity. All parties behind the system are known and identifiable.

The Technical Team

We believe that there must be a Technical Team in a permissioned network. The LACChain Framework proposes the Technical Team as the Body that ensures correct network functioning and provides support over time. Tasks of the Technical Team include but are not limited to the following:

- Develop native tools for developers.
- Expose specific boot nodes available for accepting connections from observer nodes (see Section 2.1 and Section 2.2).
- Incorporate the latest developments to the network in collaboration with the community and the other members of the network
- Maintain a transaction explorer.
- Maintain available complementary off-chain services (e.g., a timestamping service).
- Make data and dashboards available to show performance of the network (see Section 2.10).
- Monitor the network to detect technical malfunctions and identify enhancements.
- Perform periodic stress tests.
- Perform regular technical maintenance.
- Provide availability of back-up nodes in case the core nodes fail.
- Provide technical support to entities aiming to deploy nodes or applications.

The Technical Team is not an entity with any hierarchical power in the network or over other entities; it is only a body that guarantees robust functioning of the network and provides support to participants, according to public and consensuated rules.

The Permissioning Team

The LACChain Framework proposes the Permissioning Team as the Body responsible for a set of essential non-technical tasks that guarantee the permissioned network functions well. These tasks include the following:

- Maintain a public list of permissioned nodes.
- Manage the distribution of resources in the network according to the resource distribution rules (see Section 2.6).
- Monitor the network to identify network rule violations (including violations of regulatory policies) and misbehavior.
- Permission and block nodes according to the public rules (see Section 2.5) and issue certificates for on-chain authentication if necessary.
- Update information about node deployment and permissioning rules.

To us, it is very important that every task carried out by the Permissioning Team is done according to transparent and public processes approved by the Underlying Orchestration Entity. As such, the Permissioning Team is not an entity with a hierarchical power in the network or over other entities; it is only an executor of central tasks that have been previously agreed upon. It is worth emphasizing that different networks that are part of the network of networks can have independent Permissioning Teams, even if all these networks have the Underlying Orchestration Entity in common.

1.2. Operation

This LACChain Framework believes that in a permissioned public blockchain network, any entity should be able to deploy a node, provided that they comply with the permissioning requirements (see Section 2.5). They should also be able to decide whether they want to operate with the network directly or want a third party to operate the node for them as a service. Additionally, each entity should be able to decide whether they want to have their node running on their own premises or on the cloud. As stated before, we are proponents of networks that are as decentralized as possible in both operation and governance. However, if we also wish to have well established accountabilities and to have risks mitigated according to a risk model, it is necessary to set and enforce very clear rights and obligations for each entity participating in the network.

In order to understand the rights and obligations of each entity, it is useful to start by understanding the different roles that entities can play in a blockchain network that applies this framework. Table 1 presents these roles, and we encourage reading Section 2.1 to understand the topology of nodes as well as review a detailed explanation of their purpose before continuing diving into this section.

Role	Main activity	Contractual relationship with the Underlying Orchestration Entity
Validator nodes	Generate blocks	Membership
Boot nodes	Connect validators with writers and boot. Onboard new nodes	Membership
Writer nodes	Broadcast transactions[2]	Membership
Observer nodes	Access the history and state of the blockchain	None
End users	Manage blockchain accounts and digital assets. Interact with smart contracts	None
Apps, DApps, and other services	Connect different type of services to the blockchain network with potential commercial interests	None

Table 1. Available roles in LACChain Permissioned Public Networks and their contractual relationship with the Underlying Orchestration Entity.

Although every role in Table 1 is required to respect the network rules, not all of these roles are accountable for their actions directly upon Underlying Orchestration Entity. Our framework proposes that the Underlying Orchestration Entity only establishes contractual relationships with the entities that are responsible for deploying and maintaining nodes. There is a strong logical basis behind this rationale.

Generally, blockchain transactions are only signed by end-users that send the transactions from apps, dapps, digital platforms, digital wallets, and other interfaces. Under the aim of establishing clear accountability, it is essential that there is always either an entity or a person accountable for each piece of data that goes into the blockchain (thus, each transaction). The approach taken by this framework consists of making the writer nodes, rather than the end-users, accountable for the transactions that writer nodes broadcast to the network, with the understanding that broadcasting is the action of introducing a transaction into the network for the first time. In the end, writer nodes are the ones

[2] Broadcasting refers to a writer node introducing a transaction into the network for the first time. We will use the verb, "replicate," to refer to transactions that are sent between nodes in the network.

broadcasting transactions to the network on behalf of end users, and it is feasible to require the entities behind these nodes to establish a contractual relationship with the Underlying Orchestration Entity and always operate as identified and authenticated. As covered in Section 2.7, this requires writer nodes to co-sign the transactions they broadcast to the network.

1.2.1. Operation of Validator Nodes

The operation of validator nodes under the LACChain Framework should at least include the obligations, liabilities, and rights presented in Table 2.

Obligations and liabilities	Rights
Follow the Routing Rules[3]	Technical support by the Technical Team
Do not connect with any node which is not in the permissioning smart contract	
Execute valid transactions while rejecting and reporting invalid transactions	
Vote for valid blocks	
Do not vote for and report invalid blocks	
Vote for new validator nodes according to the node rotation rules[4]	
Maintain the node resilient	
Do not broadcast transactions	

Table 2. Obligation, liabilities, and rights for entities operating validator nodes.

1.2.2. Operation of Boot Nodes

The operation of boot nodes under the LACChain Framework includes the obligations, accountabilities, and rights presented in Table 3.

[3] See Section 2.2.

[4] See Section 2.3.

Obligations and Accountabilities	Rights
Follow the Routing Rules[5]	Technical support by the Technical Team
Replicate all transactions with their peers	
Maintain the node resilient	
Do not broadcast transactions	

Table 3. Obligation, liabilities, and rights for entities operating validator nodes.

1.2.3. Operation of Writer Nodes

The operation of writer nodes under this framework includes the following obligations, accountabilities, and rights.

Obligations and Accountabilities	Rights
Do not exceed the resource usage/ consumption allowed per block[6]	Minimum use/consumption of the network per block guaranteed
Do not send any transaction that violates network rules (e.g., forbidden use cases and data privacy and protection)	
Co-sign all transactions broadcasted to the blockchain[7]	Technical support by the Technical Team on issues related to the network
Be accountable for all transactions broadcasted	
Do not attempt denial of service attacks	Access to history and status guaranteed by the Technical team in case of failure or termination

Table 4. Obligation, liabilities, and rights for entities operating validator nodes.

[5] See Section 2.2

[6] See Section 2.6.

[7] See Section 2.7.

1.2.4. Operation of Observer Nodes

The operation of observer nodes under the LACChain Framework does not include any obligations, accountabilities, or rights.

1.3. Governance

In a blockchain network in which different entities operate a piece of the decentralized infrastructure, it is important to ensure that all entities are represented in decision making. Otherwise, the network will not be truly decentralized. This is why this framework distinguishes between orchestration and network governance, aiming to maximize the transparency and decentralization of decision making and task execution.

- Orchestration governance refers to all decisions that have relevance in the provision of orchestration of infrastructure services provided by an Underlying Orchestration Entity. These services include, but are not limited to, updates of changes in the statutory, legal and regulatory standards or adjustment in business, and economic incentives. By definition, this governance model must be neutral and accountable. This framework proposes a participatory governance based on representation by participating entities in the sovereign bodies of the Underlying Orchestration Entity. Ultimately, the Underlying Orchestration Entity takes responsibility for the network's establishment, provision of services, and termination.
- Network governance refers to all decisions related to the functioning of the permissioned public blockchain networks. According to this kind of consensus algorithm, the voting power for decision making would depend on the stake of each entity in a proof-of-stake basis. Those entities for which the reliability and well-being of the network is more relevant (e.g., a university registering proofs of thousands of digital diplomas; a bank issuing a million-dollar bond; a health institution registering proofs of vaccination certificates) would have more voting power. This must not be confused with the consensus protocol that governs the block generation and this framework proposes to be based on proof of authority (see Section 2.3). As discussed in Section 1, block generation is intentionally left out of Governance.

2 TECHNOLOGY

IDB IDB | LAB LACCHAIN

This framework addresses twelve elements related to the technology of the blockchain network: topology, routing and connections, block generation (consensus protocol), publicness, permissioning, resource distribution, node signatures, quantum-safeness, scalability, monitoring and evaluation, decentralized storage, and private channels.

2.1. Topology

LACChain encourages a network topology with two categories of nodes: core nodes and satellite nodes. Each category of nodes is also divided into two subtypes.

2.1.1. Core Nodes

Core nodes play an essential role in guaranteeing correct functioning of the network. The network cannot work without them. Core nodes are classified into validator and boot nodes.

Validator nodes: Participate in the consensus protocol and are responsible for the generation of new blocks. Validator nodes must only connect to each other and to the boot nodes. Validator nodes are not allowed to reject or ignore any transaction without notifying the Permissioning Team (See Section 1.1.4.2). If a transaction is not valid according to the network rules, they must reject it. If a block proposed by another node contains invalid transactions, they must report it.

Boot nodes: Act as a liaison between validator and satellite nodes, which implies that:

- They onboard new nodes by sharing the history and state of the blockchain with them in the first place. The state of the blockchain includes information about the other nodes in the network, routing rules, and whitelists and blacklists.
- They must listen to the writer nodes and pass along the transactions broadcasted by the writers to the validator nodes.
- They update the satellite nodes about new blocks generated by the validator nodes.

Boot nodes must be connected to all validator nodes and to the writer nodes they are assigned to (see Section 2.2).

2.1.2. Satellite Nodes

Satellite nodes do not play an essential role in guaranteeing the network. The well-functioning of the network does not depend on satellite nodes, so they can join and leave the network with no consequences. Satellite nodes are classified into writer and observer nodes:

Writer nodes: Allowed to broadcast transactions to the network. These nodes generate traffic in the network, usually coming from apps, DApps, end users and other types of services:

- They communicate transactions to the boot nodes, who then pass the transactions along to the validator nodes.
- They can establish private channels and side-chains between one another for private communication, for which they can leverage native tools in the network (see Section 2.12).
- They can share public documents and information using native decentralized storage in the network (see Section 2.11).

Writer nodes can only be connected to boot nodes according to the Routing Rules (see Section 2.2) as well as other writer nodes.

Observer nodes: Can only read the blockchain. They can join the network by connecting to boot nodes that are open for the purpose of reading the blockchain and are maintained by the Technical Team (see Section 1.1.4.2). No permissioning requirements should be imposed on entities or individuals running observer nodes, as the network is public. Additionally, these nodes cannot broadcast transactions nor generate blocks, so they cannot cause any harm.

This topology is motivated by two fundamental reasons, one technological and one legal.

The technological basis for this specific topology is that separating the nodes that generate blocks (validators) from the nodes that broadcast transactions (writers) allows validator nodes to be more isolated because they do not need to be directly exposed to apps, DApps, end users, or other services, and their peer connections are limited to other validators and boot nodes.

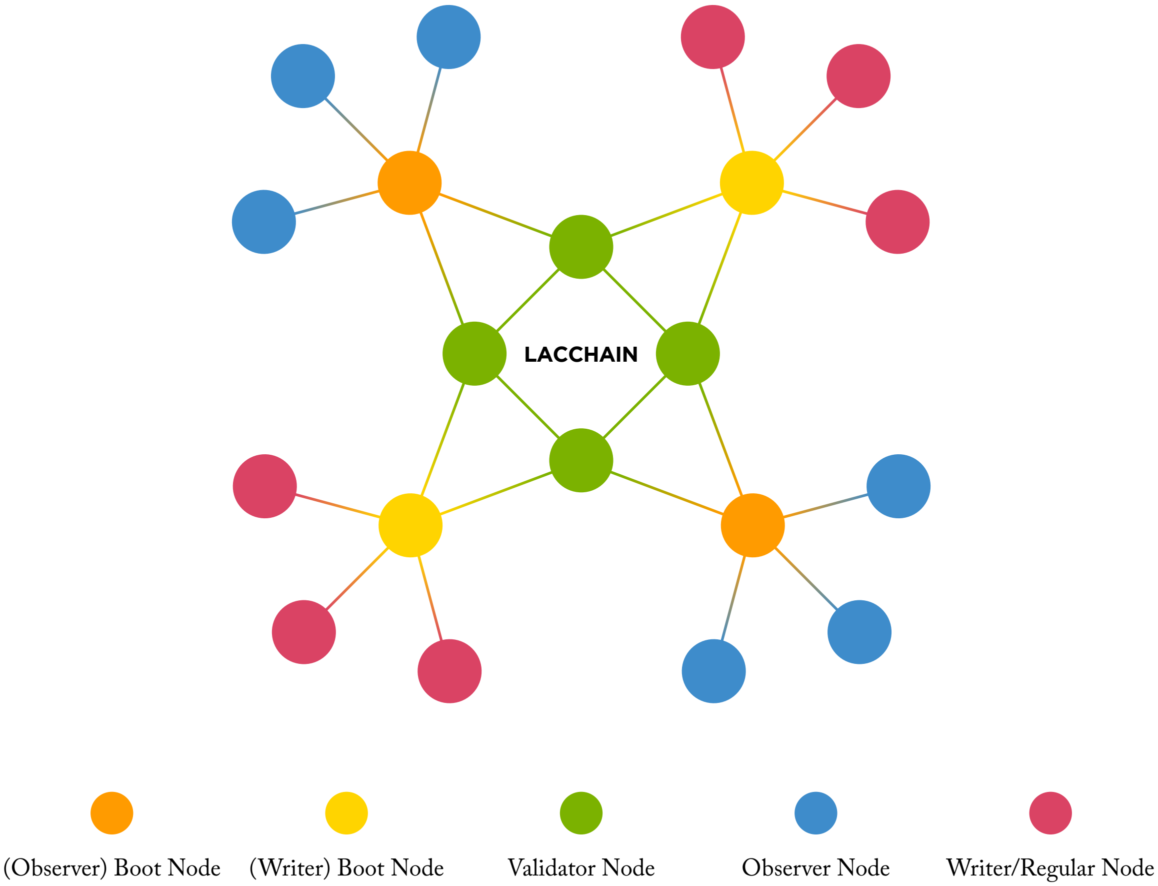

Figure 1. LACChain Network's Topology.

The legal basis for this specific topology is that, from a regulatory perspective, having a network of servers connected through TCP/UDP connections, which are well-known transport protocols, cannot possibly violate any law. Instead, transactions that contain data and information and are registered immutably in all these interconnected servers need to be looked at from a regulatory perspective. In a blockchain network, the data and information shared, which come from the applications on top of it, and not the ledger itself, need to be regulated and/or compliant with regulations.

The rationale discussed in the two paragraphs above leads to the following breakdown of regulatory compliance: a number of validator and boot nodes across the world that are only connected with each other though Internet but that do not hold any data make up a regional blockchain which is perfectly compliant with regulation. Complementarily, each writer node that broadcasts data should be entirely accountable for those broadcasts and should acquire liability associated with it (see Section 1.2.3).

2.2. Connections Between Nodes

In order to guarantee that the topology presented in Section 2.1 is respected by the nodes in the network, the following Routing Rules should be enforced:

- Each writer node can connect to a specific set of boot nodes
- Each observer node can connect to a specific set of boot nodes
- Some boot nodes must be available to connect with a specific set of writer nodes
- Some boot nodes must be available to connect with a specific set of observer nodes
- Each boot node must be available to connect with all the active validator nodes
- Each active validator node must be available to connect with all the boot nodes
- Each active validator node must be available to connect with all the other active validator nodes
- Validator nodes must not connect with writer nodes

The way this framework proposes achievement of these rules is by organizing nodes into groups. For each type of node (observer, writer, boot, and validator) we create sets of sub-groups:

- The O groups (e.g. O1, O2, O3, …) are subsets of observer nodes.
- The W groups (e.g. W1, W2, W3, …) are subsets of writer nodes.
- The B groups (e.g. B1, B2, B3, …) are subsets of boot nodes.
- The V groups (e.g. V1, V2, V3, …) are subsets of validator nodes.

Next, connections are proposed as follows:

- O1 can connect to B1, B2, and B3
- O2 can connect to B2, B4, and B6
- B2 must be available to connect with O1 and O2
- …

As explained in Section 1.2, boot and validator nodes must respect the Routing Rules set by the Permissioning Committee.

2.3. Block Generation (Consensus Protocol)

Block generation is a process executed by validator nodes and consists of proposing and accepting (i.e., voting for) sets of transactions to become new blocks appended to the chain. Every blockchain network has a well-defined mechanism for the nodes to propose and accept blocks, which is known as the consensus protocol. In the most popular permissionless networks, the consensus protocol is generally proof of work, originally proposed and adopted by the Bitcoin network. This consensus protocol introduces a reward for the block producers or validators, which is imperative in stimulating participation in these types of networks. As a trade-off, proof of work leads to the use[8] of amounts of energy equivalent to the energy consumed by medium-size countries[7] and reduces the decentralization of block generation down to only a few people who are in charge of mining pools, which are responsible for deciding which transactions go into the new blocks[8].

However, in permissioned networks there is no need to stimulate validator nodes by rewarding them with a cryptocurrency. In general, in permissioned networks, validator nodes take turns to generate new blocks, and are operated by known entities that maintain these nodes because of their interest in the existence and well-functioning of the network to allow blockchain-based government and enterprise to scale. This framework encourages a consensus protocol consisting of a practical byzantine fault-tolerant proof of authority with the following characteristics:

- Blocks need to be signed by a majority of validator nodes to be valid
- Finality is instantaneous or semi-instantaneous[9].
- History cannot be rewritten.
- Only nodes permissioned as validators can propose and vote new blocks.
- Validator nodes have a time slot to propose a new block. When time expires, the validator is replaced by another available validator.
- Validator nodes must accept any valid transaction and report any invalid transaction.
- Validator nodes must be resilient.

Validators do not compete to produce blocks, but rather take turns. As such, finality is instantaneous and new blocks are always appended at the end, never rewriting the history. If there were an attack by a majority of validator nodes trying to rewrite the history, any

[8] Although some have debated this issue, it does not impact the security of the network. Hash functions are irreversible, even for quantum computing, so there is no gain in security by increasing the difficulty of finding a valid nonce. Additionally, the possibility of rewriting history relies on the finality of the blocks, which is not good enough in networks with proof of work, as repeatedly evidenced in August 2020 with the hacking of Ethereum Classic.

[9] When a transaction is incorporated into a block that has been proposed by one validator and signed by 2/3+1 of the validator nodes, the transaction becomes permanent in the network. It is not necessary to wait until several blocks are added behind the network as is the case with consensus protocols, such as proof of work.

honest node in the network (including validators and not validators) could simply refuse to accept it as soon as the honest node finds that the hash of the block previous to the last proposed block does not match with the hash in the latest version of the chain the honest nodes have.

Additionally, this framework also encourages the implementation of the LACChain Scheme for Validator Rotation, a set of rules to score and rotate nodes that maximize decentralization and reliability. The full scheme, which is presented in detail in Appendix II, is based on the following principles:

I. Validator nodes are divided into active and inactive.
II. The number of active validator nodes is fixed to 11, because 11 is the smallest number of nodes to allow for 4 validators down in a BFT/PoA scheme.
III. Any entity that complies with the network requirements to run a validator must be allowed to do it. These requirements must only have the goal of ensuring that an entity is capable of maintaining a reliable validator node.
IV. Validator nodes are graded according to the Node Health Score, which is based on five metrics: blocks generated, block time, online time percent, decentralization, and block propagation time.
V. After well-defined optimal amounts of time, active and passive nodes rotate. Rotation probabilities are calculated according to health scores (i.e., a node with a higher score has lower probability of being rotated out).
VI. The Permissioning Committee supervises the process.

Active validators must enable the rotation with their votes (to add and remove the proposed validators).

2.4. Publicness

The concept of public or private in regard to networks refers to the openness of the access in a network according to the types of blockchain networks defined by ISO TC307 WG5 TS23635 and presented in Appendix I of this document. Access includes privileges such as running a node, broadcasting transactions, participating in the consensus protocol, or accessing the history and the state of the ledger. Therefore, publicness is not a binary quality; blockchain networks are not simply public or private as there are a range of possibilities in between. In order to evaluate how public or private a particular network is, we consider three factors:

- How accessible is the network for writing?
- How accessible is the network for reading?
- How accessible is the network for participating in the consensus protocol / block generation?

Regarding writing, permissioned public blockchain networks should be completely public, allowing any legal entity to deploy any type of node, including observer, writer, boot, and validator (see Section 2.1). Therefore, any legal entity in control of a writer node can broadcast transactions and be part of the consensus protocol.

Regarding reading, permissioned public blockchain networks should be completely public by allowing any person or entity to deploy an observer node without requiring any authentication, enabling them to have access to the history and be posted about the state in the same way as any other node. Additionally, for those uninterested or unable to deploy and maintain nodes, the Underlying Orchestration Entity through the technical Team exposes a broad variety of public dashboards and user friendly interfaces, in addition to a transaction explorer (see Section 2.10).

Regarding participation in block generation, permissioned public blockchain networks should allow any legal entity to participate in block generation, once they have complied with technical requirements to guarantee availability as well as legal requirements that include commitment to not harming the network. In the Proof of Authority consensus protocol proposed by this framework (see Section 2.3), the number of entities that can be part of block generation is unlimited. There could be 10, 20, 50 or any number of entities taking turns to generate blocks, all having equal chances.[10]

2.5. Permissioning

The concept of permissioning refers to the requirements or conditions that either a private or public network might set in order to grant access to participants. A network that is private is always permissioned[9] because if the access is not open to everyone,

[10] Some people might argue that permissioned blockchain networks are less public in the block generation than permissionless blockchain networks. This is not necessarily true and can be disproved by looking at how many entities are responsible for the block generation in a permissionless network like Bitcoin, where there are five mining pools responsible for the 64.6% of the blocks generated, all based in the same country, China. In networks that follow this framework, the number of entities that can participate in the consensus protocol with the same voting power as the others are not limited. Any entity from any country is invited.

there must be conditions entities must satisfy in order to be authorized to join. On the other hand, if a network is permissionless, it must also be public, as a network that has no conditions to join is by definition, not private.

Permissioning means that someone must to give you access to a network, but it does not necessarily mean that the access is restricted. For example, when a person takes a flight or enters a secured building, they need to present some kind identity document and they need to be authenticated and authorized in order to access. However, everyone is allowed to take a flight or enter the building if the access requirements are satisfied. These are examples of permissioned public access spaces.

Unlike publicness, permissioning is binary in the sense that a network is either permissioned or permissionless. There are no options in between. When a network is permissionless, it is public. When a network is permissioned, it can be public or private, as exemplified in the previous section. Additionally, permissioning requirements may vary from one network to another.

This framework pertains to networks that are permissioned, which means there is a set of requirements for entities to comply with in order to be permissioned to the network to deploy a writer, boot, or validator node. As explained in Section 1.1, these conditions are set by the Underlying Orchestration Entity and executed by the Permissioning Team. The permissioning requirements are comprehend presenting identification as a legal entity, assuming responsibility and accountability for the actions performed in the network, respecting terms and conditions, and acting in compliance with regulations.

The main reason behind encouraging permissioned networks for government and enterprise multipurpose applications (and consequently the base of the permissioning requirements) is to be able to enforce a legal framework that ensures that each entity is responsible, accountable, and liable for their actions, and that nobody is responsible for anyone else's actions. This is fundamental in order to have a reliable infrastructure where regulators know how to establish, settle, clear, and resolve any improper behavior, illegality, or felony, whilst ensuring that nobody pays for others' acts in a shared and decentralized network.

Specifically, the permissioning process includes:

- Agreeing with the terms, conditions, and rules of the network.
- Assuming complete accountability for the operation and performance of the node.
- Committing to respecting the forbidden use cases.

- Committing to respecting the liabilities, obligations, and rights associated with the type of node operated (see Section 1.2).
- Establishing focal points.
- Providing information for the Permissioning Team to identity proof the entity operating the node.

If an entity violates the rules and agreements outlined by the Underlying Orchestration Entity (see Section 1.1 and Section 1.2), the Permissioning Team will remove the node's access to the network and initiate a process to clarify the situation with the node operator before granting access again.

2.6. Resource Distribution

In networks with transaction fees, such as the permissionless Bitcoin or Ethereum, the transaction fees regulate the use of the network and serve to avoid DoS attacks; when there is a higher demand, the transaction fee becomes higher, and nobody can provoke a DoS attack to the network without assuming high costs of those transaction fees. However, in networks that are permissioned, there are generally no transaction fees and therefore, it is necessary to develop mechanisms to avoid DoS attacks and maximize network availability for all participants. This is what we call resource distribution, where resources refer to the different elements provided by and consumed in a blockchain network, such as gas, CPU, NET, or RAM[11]. The rules for resource distribution in LACChain are the following:

I. Resources are distributed only among writer nodes by the Permissioning Team (see Section 1.1.4.2). No other node nor account has any resources available to use or spend. Writer nodes decide how they manage their resources and are able to re-distribute them among different accounts and services that the nodes authorize to access the network through the accounts' writer nodes. In all cases, the writer node assumes responsibility for its resources.

II. The distribution of resources depends on network use at any moment. The network is under constant monitoring, which allows for evaluation of whether the network is in a regime of "low consumption" (when blocks are relatively empty in comparison with

[11] In Ethereum-based networks, the only distributed resource is the gas. However, in EOSIO there are three resources: CPU, NET, and RAM.

a threshold) or "high consumption" (when blocks are relatively full in comparison with that threshold). There are also states in between.

III. The threshold that determines when blocks are full or empty is determined by stress tests. The Technical Team performs periodic stress tests to determine at which point blocks are generated with delay because validators have trouble processing too many transactions. That is stablished as the threshold.

IV. If the network is in a "low consumption" regime, the resources available for each writer node are higher. If the network is in a "high consumption" regime, the resources available are lower.

V. If a writer node tries to provoke any attack on the network, such a DoS attack, or behaves inadequately, the node is blacklisted until the behavior is explained to the Permissioned Team.

VI. The distribution of resources is based on public, transparent, and dynamic algorithms executed automatically.

The implementation of this mechanism depends on the blockchain protocol. The LACChain Alliance has developed a solution to implement this resource distribution model in an Ethereum-based network using a rely signer (a component on top of the node that generates a meta-transaction from the original transaction and signs it) and a rely hub (a proxy smart contract that verifies the transaction before sending it to the final contract). It has also achieved a similar implementation in an EOSIO-based network using native abstractions that makes it easier to establish dynamic conditions for resource distribution.

2.7. Mandatory Writer Node Signatures

In Section 1 we introduced the concept of liability for actions in a permissioned public blockchain network and we explained how and why the entities operating writer nodes are the only ones responsible for the transactions broadcasted by their nodes to the network. However, there is a big inconvenience to enforce this liability: many blockchain protocols do not require or even enable the signature of node transactions. Only the blockchain addresses that generate the transactions sign them and send them to the nodes, who simply broadcast them to the rest of the network in a peer-to-peer way. Clearly, if a writer node that broadcasts a transaction does not sign it nor leaves any track on it, it is impossible not only to make it liable for that transaction but to even track through which writer node the transaction entered the network (i.e., which node broadcasted it).

The solution proposed by this framework to be able to comply with the liability structure presented in Section 1 consists of:

- Developing a solution that enables each writer node to sign the transactions they broadcast to the network.
- Making writer nodes transaction signatures mandatory.
- Setting a mechanism to enforce that every validator node verifies that the transactions they receive contain a signature associated with a permissioned writer node.

Additionally, if a permissioned node is detected attempting to broadcast transactions that are not properly co-signed by a permissioned writer node, it will be warned or blocked until the behavior is clarified with the Permissioning Team.

!

As is the case in the model for resource distribution presented in Section 2.6, the implementation of resources in a blockchain network depends on the protocol. The LACChain Alliance has developed solutions to implement resources in Ethereum-based and EOSIO-based technology. In Ethereum-based technology, the co-signing is achieved via a meta-transactions mechanism combined with permissioning smart contracts. In EOSIO-based technology, the networks enabled by the LACChain Alliance leverage the native account permissioning to impose the co-signature of transactions onto writer nodes before the writer nodes can be propagated through the network.

2.8. Quantum-Security

The advent of quantum computing will bring forth a new paradigm in which digital technologies will endure both challenges and opportunities. Security threats in the digital space will come up in a variety of forms, especially when robust quantum computers will have the ability to break several important cryptographic algorithms that are currently used. Blockchain, as a technology that strongly relies on cryptography, is not safe from these threats. In a paper published by the IDB in 2019, it was presented the conjunction of blockchain technology and quantum computing in the following four areas[10].

- **Digital signatures** are one of the most essential components of blockchain technology. Bitcoin and Ethereum use elliptic curve cryptography (ECC), particularly the ECDSA signature schemes on curvesecp256k1. Others, such as EOSIO, use the NIST standard secp256r1 curve. NIST recommends that ECDSA and RSA signature schemes be replaced due to the impact of Shor's algorithm on these schemes.[11]
- **Communication over the Internet** relies on protocols such as HTTP. Communication security happens in HTTPS within the SSL/TLS protocol stack. TLS supports one-time key generation (which is not quantum-safe) with AES for symmetric encryption and several non-quantum-safe algorithms for exchange and authentication, such as RSA, DH, ECDH, ECDSA, and DSA. This means that all internet communications, including transactions and messages sent between applications and nodes in a blockchain, will not be quantum safe when robust quantum computers become fully operational.
- **Block mining** is the basis of blockchain networks that use proof-of-work, as the consensus mechanism relies on finding nonces. Quantum computers will be able to find these nonces (i.e., mine) quadratically faster using Grover's algorithm[12]. However, this does not pose a major threat to the security of blockchain networks because the solution will be as easy as quadratically increasing the difficulty to compensate for the quantum advantage. In networks with consensus protocols that do not promote competition between nodes, such as the proof-of-authority proposed in this framework (see Section 2.6), this threat does not exist.
- **Hash functions** take an element from a set of infinitely many elements and give an output from a finite set of elements, as is the case for the SHA-256 function that is used by most blockchain networks today. Thus, from a hash value stored in the blockchain, it is statistically impossible to obtain the element that resulted in that value. This property, known as irreversibility or pre-image resistance, guarantees the security of these operations even in the presence of quantum computers. Additionally, hash functions are continually evolving for increased security. For example, if quantum computers evolve to the point of posing a threat to SHA-2, then SHA-3 is already standardized as an alternative that offers a higher level of security in NIST standard FIPS202[13].

As a result of this high-level analysis, it becomes clear that the threat blockchain networks face with respect to quantum computers is primarily related to vulnerable digital signatures of blockchain transactions and vulnerable key-exchange mechanisms used for peer-to-peer communication over the network.

In a paper published by the IDB, Cambridge Quantum Computing and Tecnologico de Monterrey[14], it is presented a solution developed for the LACChain Alliance that allows blockchain networks to resist attacks by quantum computers. This solution does not require modification of the algorithms used by Internet or blockchain protocols but creates a layer on top that which provides quantum security. This solution consists of the following two elements:

- **Encapsulating the communication between nodes using post-quantum X.509 certificates** to establish TLS tunnels. As part of the on-boarding process, nodes receive a "post-quantum X.509 certificate", which is an extension of an X.509 certificate using the v3 extension specification that allows for incorporation of new fields into the credential, such as complementary cryptographic algorithms; in this case, post-quantum. Using these certificates and a version of libSSL with proper capabilities, nodes can establish secure post-quantum connections that encapsulate data sharing over the communication protocol set by default by the blockchain technology.[12]

[12] In the case of Ethereum, the communication protocol is RLPx, which enables nodes to transfer encrypted and serialized data through encrypted multiplexed messaging leveraging Elliptic Curve Integrated Encryption Scheme (ECIES).

- **Signing the transactions with a post-quantum signature** along with the regular signature defined in the blockchain protocol and establishing on-chain verification mechanisms. This framework enables a second-layer cryptography scheme that allows writer nodes that broadcast transactions to sign these transactions with a post-quantum signature that can be verified on-chain, in addition to the signature that comes by default with the blockchain protocol (e.g, ECC in the case of Ethereum). If the default signature becomes compromised by a quantum-computer, integrity is preserved by the post-quantum signature. It is possible to use post-quantum keys related to the post-quantum X.509 certificates for this.

The post-quantum algorithms chosen should follow guidelines by NIST[15] and other standards organizations that are carrying out standardization processes.

Blockchain networks must take into account the threat posed by quantum computers and incorporate quantum-resistant cryptography and mechanisms. Otherwise, blockchain networks will become the easiest target for robust quantum computers as data and assets are recorded immutably and exposed publicly. When private keys can be derived from publicly exposed public keys, assets and encrypted data will be hacked. The best way to do this is by updating blockchain protocols to incorporate post-quantum cryptography algorithms.

2.9. Scalability

Scalability in blockchain networks is limited by three parameters: block size, processing capacity, and storage. Block size is set in the genesis file of the network and is the first limitation to the number of transactions that can fit in each block. The block size can be increased, but at some point, the processing capacity of the network will emerge as the second limitation. Blockchain networks are asynchronous, transactions are replicated peer-to-peer between nodes, and the consensus protocol requires validator nodes to execute new transactions and vote for new blocks. This implies that the networks' throughput processing as a whole is limited and depends on nodes' hardware. The network's throughput processing can be increased by upgrading the machines' hardware, but at some point the cost of maintaining a node is not worth the increase in throughput. Additionally, different blockchain software also present intrinsic limitations to the throughput. Finally, a third limitation is the storage. As nodes keep a copy of the full history, the storage requirements become very relevant over time.

At present, scalability in blockchain networks is an open problem being addressed by several different approaches. As discussed in the introduction, this framework targets highly decentralized permissioned public networks that can respond and perform well under high demand. We envision large permissioned public networks becoming an instrumental architectural piece for any digital solution that may benefit from using a decentralized ledger. In order for blockchain networks to become such a thing, it is necessary to guarantee that any entity using these networks can increase their throughput in line with the demands of the application or platform on top of them.

State channels, plasma, and sharding, among others, are solutions under development today by the blockchain community currently. These approaches face significant issues, including the process of verifying the integrity of the state, as transactions are not executed in the main network. The community has established roll-ups as a workaround for this challenge. Roll-ups allow for the avoidance of executing all transactions in the main network by executing them in layer-2 networks. Additionally, they allow for verification of integrity by registering the results of the computation in the main network as Merkle trees.

This framework proposes the use of roll-ups and similar approaches to enable scalability. Roll-up layers can be developed both by the node operators themselves or by the Underlying Orchestration Entity. In a multipurpose enterprise network, an outstanding Underlying Orchestration Entity shall enable mechanisms for writer node operators to satisfy the throughput needed by the applications and services on top. These mechanisms may include roll-up layers.

2.10. Monitoring

Monitoring is essential for many reasons. It is useful in detecting malfunctions, analyzing performance, identifying irregularities, and presenting metrics and dashboards. This framework proposes the use of different tools for the Technical Team (see Section 1.1.4.1) to constantly monitor the network. The tasks associated with monitoring and evaluation should at least include the following:

- Analyze data captures with monitoring tools
- Develop and maintaining monitoring tools that capture infrastructure and performance metrics
- Generate public reports on the stats of the network
- Maintain a node status dashboard
- Maintain a transaction explorer
- Set alerts for under performance (e.g., node is down or not synchronizing) and for misbehavior (e.g., a writer node is attempting to send more transactions than it is allowed)

We classify information into five categories: infrastructure, nodes, smart contracts, transactions, and blockchain accounts. The information about infrastructure allows us to know the resources (e.g., gas, RAM, CPU, NET) used by each node. The information about the nodes allows us to understand the performance of the ledger. The information about the smart contracts, transactions, and blockchain accounts allows us to understand the applications' usage of the ledger. It is important to at least evaluate the following KPIs:

Node KPIs

- Information about the routing/connection between nodes
- Latency and performance of validator and boot nodes
- List of nodes, types of nodes, location of nodes, and entities behind each node
- Number of transactions generated by each writer node
- Number of transactions rejected by a node and reason for rejection
- Percentage of available resources used by each writer node
- Score of the validator nodes according to performance
- Software versions used by each node

Smart Contracts, Transactions, and Blockchain Accounts KPIs

- Individual monitoring of key smart contracts (e.g., DID registries, on-chain DNS, resource distribution, permissioning smart contract, and stable-coins, among others)
- List of most active recipients
- List of most active senders
- List of most called smart contracts
- List of transactions per block, hour, day, and averages
- Number of smart contracts
- Number of unique senders
- Number of unique recipients
- Percentage of resource consumption per block, hour, day, and averages

!

Notably, monitoring also aids in measuring the social and financial impact of the applications running on top of the infrastructure, which is one of the main goals of LACChain as the Global Alliance for the development of the blockchain ecosystem in Latin America and the Caribbean. LACChain Alliance's main goal is to enable a regional infrastructure that is leveraged for multipurpose enterprise use cases that can enable social, economic, and financial impact. In order to measure the impact, the LACChain Alliance has developed a solution that promotes the use of tags in smart contracts to associate transactions with indicators that allow for classification of the transactions by topic and to evaluate their impact on development.

2.11. Decentralized Storage

In general, blockchain networks must not be used to store sensitive data because they are immutable, especially if they are public. Blockchain networks must also not be used to store documents, files, or large amount of data because storage requirements become unpractical. In general, blockchain networks should be used to store cryptographic proofs of off-chain data and well-selected public metadata.

However, in some cases, blockchain-based solutions require the exchange of documents, and would benefit from decentralized storage. This decentralized storage would allow end users to share off-chain information that is linked to transactions in the blockchain in either a permissionless or permissioned way. We encourage the use of solutions, such as the Interplanetary File System (IPFS), StorJ, or Buzelle, to run a decentralized storage alongside the blockchain nodes. This storage should be available for both permissioned and permissionless sharing. However, it is important to highlight that:

- If the information is stored in permissionless mode, anyone can have access to it
- Even if the information is stored in permissioned mode, once it is shared with other permissioned nodes, it could also be shared with entities that are not permissioned
- Once the information has been shared, each storage node needs to delete the information from their own copy in order to remove it; there is not a central unit of control

Interactions with the decentralized storage should at least be available via API and command line. It should be possible to store or get a file, and set options, such as the time a file will be stored, before being deleted. When a document or a file is stored in the decentralized storage, a hash of the document or file is returned. This hash is used to be linked with a transaction in the blockchain. In this way, information can be retrieved by viewing the hash stored in the smart contract and using the hash to access the decentralized storage and obtain the content of the file. In some decentralized storages, the content is addressable, which means the hash of the document guarantees its immutability as well as its location in the storage network.

2.12. Private Channels

Privacy is the ability to keep transactions private between a set of participants, in a way that other participants cannot access the transaction content or list of participants in the private channel. Many blockchain-based applications require the exchange of sensitive information between parties. In some cases, even with the possibility of having decentralized storage in a permissioned mode (see Section 2.11), it is more convenient to enable a private side-channel where some entities can set access rules and create and eliminate members, each of them having their centralized storage for the information exchanged. In a multipurpose enterprise blockchain infrastructure, easy mechanisms for the generation of private side channels by sets of writer nodes should be enabled by the Technical Team (see Section 1.1.4.1).

LACCHAIN FRAMEWORK FOR PERMISSIONED PUBLIC BLOCKCHAIN NETWORKS

3 REGULATORY COMPLIANCE

IDB IDB | LAB LACCHAIN

This framework is designed to enable permissioned public blockchain networks to be fully compliant with the regulations of all countries in Latin America and the Caribbean, as well as European policies, such as eIDAS and GDPR. This is achieved though the following:

- All the transactions broadcasted to the network are signed with digital signatures that are linked to well identified node operators (see Section 1.2.3), and therefore can be recognized and enforced in any country that recognizes the use of electronic signatures by law (in Latin America and the Caribbean, 31 of the 42 countries have regulations on electronic signatures and transactions).
- The contractual relationship between validator, boot, and writer nodes with L-Net via SLA (see Section 1) and the permissioning rules that require identification and authentication for each node (see Section 2.5) make every node in the network responsible for their actions and link those liabilities to well identified legal entities.
- The node topology (see Section 2.1) allows for establishment of a network with four types of nodes, where all legal accountability related to data registered in the blockchain is isolated in the writer node operators, as these are the only nodes allowed to broadcast transactions (see Section 2.1, and Section 1.2).
- The required transaction co-signatures by writer nodes (see Section 2.7), which establish that no transaction can be propagated if it does not have the signature of a permissioned writer node, creates a legally enforceable liability for the writer nodes on the transactions they broadcast to the network and isolates the responsibility of each bad transaction in a particular writer node.
- The Underlying Orchestration Vehicle acts as a central point of contact for any claim.

A very important topic that has been intentionally left out of this framework is the liability for smart contracts. There have been debates in recent years regarding who should be liable for a hacked or failed smart contract. The liability could fall to the developer of the smart contract, the person or entity using it, the person or entity offering services on top of it, a node operator offering services based on it, or the Underlying Orchestration Vehicle, among other options. In this framework, we have presented a solution to establish liabilities for all actions related to participating in a permissioned public blockchain network and we believe that it is necessary to establish liabilities for each smart contract as well.

We do not think these liabilities fall at a network level. On the contrary, we believe that these liabilities are application- and end-user-related. When an application or end user uses a smart contract that someone else has developed and/or deployed in the network, they are trusting a third-party for the code in that smart contract. If, for example, an entity creates a digital bond, issues a CBDC, or issues digital diplomas that rely on one or several smart contacts deployed in a blockchain network, they will want to point to a responsible party should something fail. Just as this framework establishes liabilities for situations that can go wrong in the network, it is important that either the entity that develops a smart contract, the entity that deploys it, or a third party, develops a model surrounding assumptions of liabilities for smart contracts used by end-users and applications.

APPENDIX I.

Types of Blockchain Networks According to ISO TC307 WG5 TS23635

Permissionless public: Permissionless public networks are those that anyone can join at any time, such as Bitcoin or Ethereum. Most of these networks are generally linked to a crypto-currency[13]. They are open and transparent, but typically have high transaction fees, no privacy[14], and all users are pseudonymous. Additionally, as participants are not identified, it is difficult for transactions and applications to be forced to be compliant with regulations.

Permissioned private: Permissioned private networks consist of 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 the 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 FoodTrust[16], and the blockchain network of the Energy Web Chain by the Energy Web Foundation (EWF) consortium[17].

Permissioned public: Permissioned public networks are open, transparent, decentralized, and generally do not have transaction fees. At the same time, every participant is identified, so 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).

[13] Pegged to a cryptocurrency.

[14] Permissionless networks are not private because all the information recorded on them is publicly accessible. However, in principle, it is not possible to know who is behind each transaction because accounts are pseudonymous. In practice, pseudonymity does not guarantee privacy because identities can be disclosed in various ways.

Table 2. Main differences between the three ISO TC307 WG5 TS23635 types of blockchain networks.

	Permissionless public	Permissioned private	Permissioned public
Right to join open to everyone	✓	✗	✓
History and state available for observers	✓	✗	✓
Requires identification, authentication, and authorization	✗	✓	✓
Governed by an underlying orchestration entity	✗	✓	✓
Responsibilities and accountabilities can be established	✗	✓	✓

APPENDIX II.

LACChain Scheme for the Rotation of Validator Nodes

II.1. Scoring of Validator Nodes

In order to rotate nodes in a way that maximizes the performance and decentralization of the network, it is necessary to first understand the health and contribution of active validator nodes. This framework proposes doing this by calculating a Node Health Score, based in the following 5 metrics:

Table 1. KPIs evaluated in validator nodes.

Metric	Definition	Importance (1-5, 5 is most important)
Blocks generated	Node is proposing blocks as expected (compared to other nodes)	5
Block time	Node is proposing blocks within the expected time specified in the genesis file (2 seconds)	4
Online time percent	Node is online as expected	4
Decentralization	Node location is adding decentralization to the network (based on distance to other nodes and number of other nodes in the same location)	3
Block propagation time	Node is proposing blocks that are propagating to other nodes as expected compared to other median of nodes and to previous performance	2

The Node Health Score algorithm is as follows:

- **blocks_score:** blocks_generated / max of blocks_generated across all nodes.
- **block_time_score:** 1 / (block_time / 2).
- **decentralization_distance:** avg distance to every other node / number of nodes in same location.
- **decentralization_score:** decentralization_distance / max of decentralization_distance across all nodes.
- **online_score:** online_time_percent / 100.
- **propagation_avg_score:** propagation_avg_time / propagation_time. if the result is greater than 1, score is 1.
- **propagation_time_score:** propagation_time / median of propagation_time across all nodes. if the result is greater than 1, score is 1.

Table 2 shows an example of 3 nodes being scored according to the Node Health Score algorithm. Table 3 shows the overall score for the same set of nodes and performances.

Table 2. Example of scoring for three nodes.

node	node1	node2	node3
blocks_generated	90	90	90
block_score	**1.00**	**1.00**	**1.00**
block_time	2	2	4
block_time_score	**1.00**	**1.00**	**0.50**
online_time_percent	100%	80%	100%
online_score	**1.00**	**0.80**	**1.00**
decentralization_distance	454.90	206.78	78.13
decentralization_score	**1.00**	**0.45**	**0.17**
propagation_time	3.72	552.34	772.87
propagation_time_score	**1.00**	**1.00**	**0.73**
propagation_avg_time	3.72	510.21	773.20
propagation_avg_score	**1.00**	**0.92**	**1.00**

Table 3. Example of overall score.

node	node1	node2	node3
block_score	1.00	1.00	1.00
block_time_score	1.00	1.00	0.50
online_score	1.00	0.80	1.00
decentralization_score	1.00	0.45	0.17
propagation_time_score	1.00	1.00	0.73
propagation_avg_score	1.00	0.92	1.00
overall_score	**1.00**	**0.86**	**0.74**

II.2. Rotation of Validator Nodes

The validator node health scores are useful to monitor the health of the network, and they are used as inputs to determine the rotation of active and inactive validator nodes. Active validator nodes can be rotated out under two circumstances:

- Health check round
- General rotation round

II.2.1. Health Check Rounds

The health check rounds are periodical checks on the validators' performance. They are intended to identify validator nodes that are underperforming and rotate them before they lead to a malfunction of the network (e.g., delaying or interrupting block generation). The rules applied are the following:

- Every 30 minutes, the scoring methodology will run to 1) calculate an overall health score for each active node and 2) identify any nodes that are performing below thresholds. Thresholds are presented in Table 4.

- If a node is performing below threshold in the 30 minutes check, a report and an alert are sent to the Permissioning Committee which will decide if the node should be immediately rotated out.[15]
- If the node continues to perform below thresholds for 24 hours, the node will be flagged for rotation out and rotation will be triggered automatically.

In the example scores presented in Tables 2 and 3, node #2 would be identified as not hitting the online time percent threshold and node #3 would be identified as not hitting the block time threshold.

Table 4. Thresholds of minimum performance accepted.

Metric	Rotation Threshold
Blocks generated	Node is proposing 85% or fewer blocks than expected
Block time	Node is proposing blocks with an average time greater than 4 seconds
Online time percent	Node is online 95% or less
Decentralization	N/A
Block propagation time	N/A

II.2.2. General Rotation Round

The general rotation round is the process established to organically rotate out active and rotate in inactive validator nodes. The purpose of this rotation is to allow any entity capable of maintaining a reliable validator node to participate in the block generation while keeping the number of validators set to the optimal number 11 (see Section 2.3). This allows for a high degree of decentralization. The rules applied are the following:

- Every 2 weeks, there will be a general rotation round where 2 active nodes are flagged for rotation out and 2 inactive nodes are proposed for rotation in.

[15] Monitoring tools shall allow to detect malfunctions or misbehaviors of validator nodes instantly. The 30-minute check allows to detect validator nodes that are performing according to the rules established but lacking reliability.

- The algorithm selects the 2 nodes to be rotated out based on rotation probabilities that are based on the Node Health Scores. The lower the score, the higher the rotation probability. The algorithm for the adjusted overall score is 1 / (1+EXP(-20*(overall_score-0.9))) and for the rotation probability. is (1 - Adjusted overall score) / Sum of adjusted overall scores.
- When an active node is rotated out during general rotation, they will keep their historical health scores and be put in a pool of inactive nodes ready for rotation back in. Active nodes that have been rotated out due to poor performance will not keep their historical health scores and instead be flagged for review by the Permissioning Committee; after review, the node will start from a clean slate and be put into the pool of inactive nodes ready for rotation in.
- The logic for inactive nodes chosen for rotation in are as follows depending on how many nodes need to be rotated in is:

    - 1st replacement node: If available, a node with historical health scores chosen based on the probabilities determined by their average health scores.
    - 2nd replacement node: If available, a node with no previous health scores (e.g., either a complete new node or a previously poorly performing node that was reviewed and cleared by the Permissioning Committee).
    - Continued, flipping between nodes with scores and nodes without scores as available.

REFERENCES

[1] S. Haber and W.S. Stornetta. (1991) How to timestamp a digital document. Journal of Cryptology, Vol. 3, No. 2, pp. 99-111. Retrieved from https://www.anf.es/pdf/Haber_Stornetta.pdf

[2] D. Chaum , A. Fiat, and M. Naor. (1990) Untraceable Electronic Cash. In: Goldwasser S. (eds) Advances in Cryptology — CRYPTO' 88. CRYPTO 1988. Lecture Notes in Computer Science, vol 403. Springer, New York, NY. https://doi.org/10.1007/0-387-34799-2_25

[3] S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[4] V. Buterin (2013) Ethereum whitepaper. Retrieved from https://ethereum.org/en/whitepaper/

[5] ISO Technical Committees. Blockchain and distributed ledger technologies. ISO TC307 WG5 TS23635.

[6] ISO Technical Committees. (2019) Discovering ISO 26000: Guidance on social responsibility. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100258.pdf.

[7] C. Barainuk. (2019) Bitcoin's energy consumption equals that of Switzerland. BBC. Retrieved from Bitcoin's energy consumption 'equals that of Switzerland' - BBC News.

[8] J. Tuwiner. (2021) Bitcoin Mining Pools. Retrieved from https://www.bbc.com/news/technology-48853230#:~:text=Currently%2C%20the%20tool%20estimates%20that,sa

[9] Inclusive deployment of blockchain for Supply Chains. A framework for blockchain interoperability. World Economic Forum. http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

[10] M. Allende-López and M.M. Da Silva. (2019) Quantum technologies: Digital transformation, social impact, and cross-sector disruption. Inter-American Bank , pages 1–94, 2019. DOI: http://dx.doi.org/10.18235/0003313

[11] L. Chen, S. Jordan, Y-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. (2016) Report on post-quantum cryptography-nistir 8105. Technical report, NIST, April 2016

[12] L. K. Grover. (1996) A fast quantum mechanical algorithm for database search. Proceedings of the 28 the annual ACM symposium on the Theory of Computing, pages 212–219, 19966

[13] Information Technology Laboratory. (2015) Sha-3 standard: Permutation-based hash and extendable-output functions. Technical report, NIST, August 2015.

[14] M. Allende et al. (2021) Quantum-resistance in blockchain networks. Inter-American Development Bank. DOI: http://dx.doi.org/10.18235/0003313

[15] G. Alagic et al. (2020) NISTIR 8309: Status report on the second round of the NIST Post-Quantum Cryptography Standardization Process. Retrieved from https://csrc.nist.gov/publications/detail/nistir/8309/final

[16] https://www.ibm.com/blockchain/solutions/food-trust

[17] https://www.atlassian.com/

ACKNOWLEDGEMENTS

Adrian Pareja, Blockchain Lead Architect, LACChain, Perú.

Albi Rodríguez, Head of Ecosystems and Communities, LACChain, Spain.

Anantharaman Iyer, Lead - Strategy Partnerships and Alliances, Tata Consultancy Services, India.

Andres Gomez Ramirez, Blockchain Security Researcher, EOS, Costa Rica.

Annamalai (Anbu) Anbukkarasu, Head, Digital & Emerging Technology, Banking Financial Services and Insurance, Tata Consultancy Services, India.

Antonio Leal Batista, Head of Project Pipeline, LACChain, Perú.

Blanca Sandoval, Communication Manager, LACChain, Mexico.

Bob Trojan, President & CEO, Token Insights / Financial Services Insights / DC Insights, LLC, USA.

Brian Desiderio, Technical Leader, Extrimian, Argentina.

Carlos González, Product Manager, RedCLARA, Colombia.

Chris Fergus, Analytics, Metrika, USA

Daniel Zárate, Communication associate, LACChain, Mexico.

David Ammouial, Blockchain & Digital Identity Expert Architect, NTT Data, France.

Diego López León, Blockchain Architect, LACChain, LACChain, Argentina.

Drummond Reed, Chief Trust Officer, Evernym, USA.

Edgard Espinoza, Lead Software Architect Backend, Everis-NTTData, Perú.

Eduardo Lemp, Operations Advisor, LACChain, Chile.

Eduardo Marchena, DevOps, LACChain, Perú.

Erick Pacheco Pedraza, Blockchain Architect, Everis-NTTData, Perú.

Gene Vayngrib, CEO & Co-founder, Tradle, USA.

Guillermo Villanueva, Founder and CEO, Extrimian, Argentina.

Ilán Meléndez Lugo, Regional Lead, LACChain, Costa Rica.

Ismael Arribas, Owner, Kunfud, Spain.

Itzel Nava, Executive Coordinator, LACChain, Mexico.

Iván Castelán, Software Development Engineer, OS.City, Mexico.

Jaime Alberto Centellas, Chief Technology Officer, World Data Inc., USA.

Juan José Miranda, Director Digital Technology Innovation and Labs Blockchain Everis-NTTData, Perú.

Lucía Latorre, Marketing and Commercial Advisor, LACChain, USA.

Mahesh Chandrahas Karajgi, Senior IT Officer, ITS Technology & Innovation, World Bank Group, USA.

Marcela Ribeiro Gonçalves, Diretora de Desenvolvimento Empresarial e Sócia, Multiledgers, Brazil.

Martin Hargreaves, Chief Product Officer, Quant Network, UK.

Máximo García Martínez, Blockchain Developer, Inetum, Spain.

Moisés Menéndez, Principal Advisor in Legal and Economics, LACChain, Spain.

Oscar Bazoberry, CEO & Founder, World Data Inc., USA.

Pablo Luna, Devops, Extrimian, Argentina.

Pablo Mosquella, Chief of Staff, Extrimian, Argentina.

Pabo Raices, Regional Lead for the Southern Cone, LACChain, Uruguay.

Pallavi Kumari, Tata Consultancy Services, India.

Pamela Martínez Licona, Full Stack Developer, OS City, Mexico.

Pedro Perrotta, Co - Founder and Chairman, Grupo Sabra, Argentina.

Raunak Mittal, IT Officer, ITS Technology & Innovation Lab, World Bank Group, USA.

Rocío Murillo Mora, IT Coordinator, LACChain, Costa Rica.

Saurabh Nagesh,Delivery Manager - Cloud, Tata Consultancy Services, India.

Sergio Cerón, Blockchain Architect, LACChain, Mexico.

Sergio Bazoberry, Head of Operations & Co-founder, World Data Inc., USA.

Simon Wilkinson, Operations Director, Tradle, USA.

Sooin Yoon, Product, Metrika, USA

Sosu Alex,Associate Consultant - Blockchain Architect, Tata Consultancy Services, India.

Suzana Maranhão Moreno, Co-founder, BNDES Digital Innovation Lab, Brazil.

Urko Larrañaga, Lead of Blockchain, Izertis, Spain.

Venu Reddy, Blockchain Consultant, Digital Solutions, BFSI US East, Tata Consultancy Services, USA.

Yusuf Karacaoglu, Chief Technology Advisor ITSVP, Director of Technology and Innovation, World Bank, USA.

LACCHAIN FRAMEWORK FOR PERMISSIONED PUBLIC BLOCKCHAIN NETWORKS

IDB IDB | LAB LACCHAIN