Applied Computer Science, vol. 20, no. 4, pp. 149–174
doi: https://doi.org/10.35784/acs-2024-45

Submitted: 2024-08-07 | Revised: 2024-10-18 | Accepted: 2024-10-28

Keywords: Blockchain, cryptocurrency, database, transaction, database application

Francisco Javier MORENO ARBOLEDA [0000-0001-7806-6278]*,
Georgia GARANI [00000-0003-1892-4183]**,
Sergio Andrés ARBOLEDA ZULUAGA [0009-0008-7560-6345]*

EXPLORING THE EXPEDIENCY OF BLOCKCHAIN-BASED SOLUTIONS: REVIEW AND CHALLENGES

Abstract

A distributed type of database where digital data is stored as blocks chained together is called a Blockchain. Each block consists of several transactions, authenticated using cryptographic keys, and approved by a group of validators. Hundreds of different Blockchain solutions have been proposed over the years, proving that they attract research and business interest. In this article, the authors present a generic vocabulary for unifying different terminologies used by various researchers in the field, followed by a review and evaluation of several research works presenting Blockchain-based solutions. A set of criteria regarding usefulness and suitability of adopting a Blockchain application are distinguished in these works. A method to examine their applicability is also discussed. Cryptocurrencies and supply chains, the two most well-known Blockchain uses, are considered and examined to assess how important these criteria are in these two use cases.

1. INTRODUCTION

Blockchain is a technology that has become popular in the last decade, although its foundations date back to the 1980s (Sherman et al., 2019). Following its success in the management of cryptocurrencies such as Bitcoin, Ethereum, Litecoin, and many others, Blockchain has been applied in a variety of fields including medicine (Shen et al., 2019), supply chains (Groschopf et al., 2021), military affairs (Buenrostro et al., 2019), the sale of goods and services (Ullah & Al-Turjman, 2023), domain name systems (Liu et al., 2018), collaborative forums (Koepsell, 2019), and digital certificates (Bhanushali et al., 2019), among many others. For example, only in the healthcare field, more than 65 Blockchain applications are reported in Agbo et al. (2019), De Aguiar et al. (2020) and in Kassab et al. (2019) 52 primary studies are evaluated and classified.

From a data storage perspective, conventional Blockchain solutions use a replicated and distributed database which offers high data and transaction integrity through cryptographic controls and consensus mechanisms for transaction approval. Thus, this technology is

* Universidad Nacional de Colombia, Sede Medellín, Facultad de Minas, Departamento de Ciencias de la Computación y de la Decisión, Colombia, fjmoreno@unal.edu.co, saarboledaz@unal.edu.co
** University of Thessaly, Faculty of Technology, Digital Systems Department, Larisa, Greece, garani@uth.gr

suitable for applications with this requirement (to guarantee high integrity); users must be aware of its potential disadvantages, e.g., slow transaction processing and high energy and maintenance costs associated with large Blockchain networks, especially those which use PoW (proof of work) as a consensus mechanism (Marr, 2021). For example, in Bitcoin, a transaction is usually confirmed within one hour, and according to the Cambridge Centre for Alternative Finance (https://ccaf.io/cbeci/index), Bitcoin consumes around 0.55% of global electricity production (Carter, 2021). However, these disadvantages are considerably reduced in Blockchain systems such as Ethereum 2.0. (Ethereum Blog Team, 2022), which uses PoS (proof of stake) as a consensus mechanism.

As it usually happens with relatively recent and developing technologies, its use is overhyped, i.e., Blockchain has been implemented in projects in which no major benefits are obtained or the solutions are even inferior to those developed with traditional systems. A particular example is a use case based on a smart contract (a program stored and executed on a Blockchain) for the management of agricultural insurance policies, where payment terms change depending on the state of the weather (Greenspan, 2016). To do this, the smart contract must access an external service that reports the weather and from this information determine the amount to pay for insurance. However, as in Blockchain each transaction is executed on each node of the Blockchain network and not necessarily simultaneously, it is possible that the weather report (external factor) be different between the nodes; for details see (Greenspan, 2016).

In this article, the authors identify from various works a set of criteria against which they analyse the validity of a Blockchain-based solution. Such works usually present a proposal, e.g., a flowchart, to indicate whether a use case is suitable to be implemented using Blockchain. The authors analyze and compare these works. For each one, they consider the following aspects: the technologies it compares, the criteria it uses, and the use cases it considers appropriate to be developed using Blockchain. Hence, from the analysis of these works conclusions are drawn, to identify the common and most relevant criteria in them. The authors also propose a method for determining the relevance of each criterion across all works.

Finally, from the most relevant criteria, two representative use cases of Blockchain, cryptocurrencies and supply chains were considered to assess how important these criteria are in the two use cases. In addition, the authors tried to establish a common vocabulary among the analyzed works, since they often use different terms or expressions to refer to the same concept, e.g., actor, participant, and party.

The article is organized as follows. In Section 2 a generic vocabulary is presented and a number of research works are reviewed and evaluated. Section 3 presents an analysis of two use cases of Blockchain considering the top ten criteria distinguished in the evaluated works. The work is concluded in Section 4 and future research work is briefly discussed in Section 5.

2. REVIEW AND EVALUATION OF WORKS

First, some concepts are presented to identify a common vocabulary for analyzing the works. Additional specific concepts are defined in each work discussed below, see Subsection 2.2.

2.1. Concepts

Terms related to the topic are briefly explained below in alphabetical order.

Actor, participant, or party: a user that interacts with a system, here a Blockchain-based system.

Auditability: a systematic and independent examination of a system with the goal of determining whether its operation is correct (according to its consistency rules) and has been continuously correct (BitFury, 2016).

Blockchain: a distributed database of records of transactions that have been executed and shared among participating actors. Each transaction is verified by consensus of most of the actors (Crosby et al., 2016).

Centralized database: a database that is located, stored, and maintained in a single location, most often in a central computer (Turban et al., 2021).

Consensus: a situation that arises when a group of actors reach an agreement on the state of a system (Ethereum.org, 2023).

Consensus mechanism: a protocol by which a consensus is reached (Ethereum.org, 2023). To maintain the data integrity and the data immutability, Blockchain uses consensus algorithms (see e.g., PoW and PoS) that allow a block to be added to the Blockchain only when it is agreed by the nodes of the network (Hassija et al., 2021). After a block is stored in the Blockchain, its content cannot be altered.

DAO (Distributed Autonomous Organization): a company governed in a decentralized manner through smart contracts (CoinMarketCap, 2023).

Data confidentiality: data access restriction, i.e., the ability to guarantee that only authorized actors can access the data (Ali & Afzal, 2018).

Data immutability: The ability of a system to guarantee that its data remain permanent, indelible, and unalterable (Doubleday, 2018).

Data integrity: degree of data protection, i.e., how protected they are from unauthorized modifications (Wüst & Gervais, 2018).

Data privacy: handling of sensitive data properly and regulating how data are collected, processed, and stored to ensure their proper handling (GeeksforGeeks, 2022).

Data security: a set of measures that prevent unauthorized access to a system (De Wolf, 2024).

Fault-tolerance: the ability of a system (computer, network, database, etc.) to continue operating without interruption when one or more of its components fail (Imperva a Thales Company, 2023).

Intermediary: a trustful actor for other actors. An intermediary must have high availability (hopefully 24/7) and offer responses to the requests of the actors in a satisfactory time, depending on the cost of the services it provides (Greenspan, 2015).

Latency: the delay between the beginning and the end of a transaction (Ma, 2023).

Ledger: a compendium of transactions, a sequence of data records.

Mistrust: a situation that arises when an actor: i) is not willing to let another one modifies data which he/she owns or ii) will not accept the "truth" as reported by another one when reading the database's (Blockchain) contents (Greenspan, 2015).

Open-permissioned or hybrid Blockchain: a Blockchain based on public access but with customizable private-access options.

Permissionless or public Blockchain: a Blockchain that allows any user to become a part of it and to contribute to its upkeep (Freeman Law, 2022).

Permissioned or private Blockchain: a Blockchain where users are assigned permissions according to their role, e.g., writer, transaction validator (Freeman Law, 2022). A private Blockchain is available only to selected users.

Proof of Work (PoW): a consensus mechanism where each node tries to solve a mathematical problem, the first node which solves it has the right to add a new block to the Blockchain (leader node). Its advantages are high node scalability and high security, and the disadvantages are low throughput and high computational power.

Proof of Stake (PoS): a consensus mechanism where the leader node is chosen based on the amount that each node stakes. To avoid monopolies (i.e., rich nodes have more voting power and may win most of the elections), this consensus can have restricted elections. Its advantages are high node scalability, high throughput, and low computational power and its main disadvantage is that it is probably less secure than PoW (its security is not as proven as PoW).

Public verifiability: a property of a system that allows anyone to verify the correctness of the system state (Wüst & Gervais, 2018).

Scalability: it indicates how system performance is affected as data processing demand increases (Gartner®, 2023).

Smart contract: a program stored and executed on a Blockchain. A smart contract is typically used to automate the execution of an agreement so that all actors can be sure of the outcome, without any involvement of an intermediary (IBM, 2023). Thus, smart contracts could offer several benefits: speed and real-time updates, accuracy, lower execution risk, fewer intermediaries, lower cost, among others (Mohanta et al., 2018).

Throughput: the number of transactions a system can process in a period. Latency and throughput are indicators of the performance of a system (Oracle Corp, 2010).

Traceability: the ability to trace, to follow every single action in the network (Haritonova, 2022). For example, in a supply chain, it allows the actors to follow every step of the transportation process of a product.

Transparency: the ability to make visible every single action in the network to all (authorized) actors (Haritonova, 2022). Transparency provides trust between actors.

Validator: an actor that is responsible for approving transactions on a Blockchain.

Writer: a type of actor who can perform write operations on a Blockchain.

2.2. Evaluation of works

The search and selection of the evaluated works was based on the answers to the following questions:

- When should a Blockchain-based solution be used? When should it not be used?
- Which use cases are appropriate to be implemented using Blockchain? Why are they appropriate and which ones are not? Which ones are not appropriate and why not?
- Which requirements of a use case suggest that a Blockchain-based solution is appropriate and which ones suggest the opposite?

The bibliographic search included scientific databases such as IEEE Xplore and Scopus and the search engines Google and Google Scholar. The authors considered articles published in journals, conferences, and web sites. The search was carried out without time

restriction, since the topic is relatively new, although priority was given to latest works. The identification of the relevant works was based on keywords (string searches) as suggested by (Kitchenham, 2004). The authors considered the following search strings (enclosed in quotation marks for the searches): “when to use Blockchain”, “where to use Blockchain”, and “Blockchain suitability”. For example, in Google Scholar these were the results: “when to use Blockchain”: 238 documents, “where to use Blockchain”: 12 documents, and “Blockchain suitability”: 112 documents.

The authors used the Search and Selection methodology proposed by (Kitchenham et al., 2009). Basically, the authors began the search, identified the sources and candidate papers (based on title and abstract), read and discussed any papers with disagreement on inclusion or exclusion until agreement was reached, checked references for all selected papers, and added any missed papers to the list of selected papers. For complete details of this methodology, see (Kitchenham et al., 2009).

After analysing the results, several papers were found that focus on the topic of interest to the authors, which are analysed here. However, most of the results correspond to works that deal with a variety of topics around Blockchain: surveys, applications in specific domains, consensus algorithms, security issues, smart contracts and their languages, cryptocurrencies, regulations, and so on. On the other hand, the search in the Scopus database generated fewer results: “when to use Blockchain”: 5 documents, “where to use Blockchain”: 0 documents, and “Blockchain suitability”: 5 documents. The search in the IEEE Xplore also generated few results: “when to use Blockchain”: 1 document, “where to use Blockchain”: 0 documents, and “Blockchain suitability”: 5 documents. Hence, in Google Scholar the authors found works most relevant to their analysis. They also found some works on websites through the Google search engine. These websites belong to Blockchain development companies, to official government pages, or to experts in this field. Although these works are not published in journals or conferences, they offer proposals that the authors consider valuable to be incorporated into their analysis.

On the other hand, there are several surveys about Blockchain, e.g., while searching “Blockchain surveys”, the authors got 61 documents in Google Scholar and 14 in Scopus; just to name a few ones (Al-Jaroodi & Mohamed, 2019; Berdik et al., 2021; Fernandez-Carames & Fraga-Lamas, 2018; Guo et al., 2022; Bao et al., 2020). However, to the best of the authors’ knowledge, they did not find specific surveys about when to use Blockchain.

For each work they identified the compared technologies and the criteria for their selection. Most of the works present the criteria in a flowchart, which indicates whether a given technology is appropriate. Some flowcharts are so detailed (e.g., (Belotti et al., 2019)) that they go so far as to indicate, e.g., the type of Blockchain that should be used. Other works do not present a flowchart as such, but they present the criteria and express their importance in certain use cases. In other works, the criteria were implicit, so they were identified from the use cases. We show our Blockchain search and select process in Figure 1. Next, we present the analysed works in ascending order chronologically.

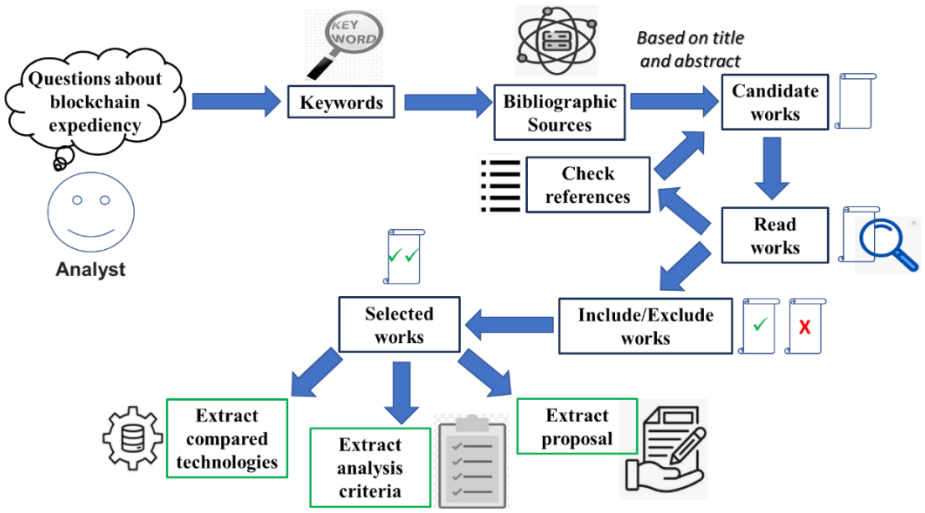

Fig. 1. Blockchain search and select process

2.2.1. Avoiding the pointless Blockchain project (Greenspan, 2015)

Compared technologies

Blockchain, regular file storage, centralized database, master–slave database replication, and multiple databases to which users can subscribe.

Analysis criteria: a) Backing of the assets: i.e., who answers for, supports in the real world the assets that reside on a Blockchain, b) Definition of validators: i.e., define the actors who will be in charge of the consensus, and with which mechanism it will be established (Nguyen et al., 2019), c) Intermediation, d) Number of writers, e) Rules restricting the transactions performed: e.g., in an asset ledger, transactions should be prevented from creating assets out of thin air, i.e., the total quantity of each asset in the ledger must be the same before and after every transaction, f) Storage (shared or personal), g) Transaction interaction: i.e., transactions that record data on the Blockchain usually have dependencies between them, e.g., for a user to make a payment (a transaction) he/she must have sufficient funds; therefore, he/she must have received payments or charges to his/her account (as a result of other transactions), and h) Trust levels.

Proposal

The author states that Blockchains are overhyped and that many use cases are more appropriate for a relational or non-relational database. The author concludes that a viable use case for a Blockchain requires shared storage, multiple actors (writers) who do not trust each other, lack or little availability of trustful intermediaries, and that the transactions that record data in the system depend on one another (interdependent transactions).

2.2.2. Do you need a Blockchain? (Wüst & Gervais, 2018)

Compared technologies

Permissioned and permissionless Blockchain, centralized database.

Analysis criteria: a) Data integrity, b) Data privacy, c) Data redundancy. It occurs when the same piece of data is stored in two or more separate places within a database (Rouse,

2023) In a Blockchain database, data redundancy is inherently provided through replication across the nodes. In a centralized database, redundancy is usually achieved through replication on different disks and through backups, d) Latency and throughput, e) Transparency (process of updating the state of the system), f) Public verifiability, g) Trust anchor. An authoritative entity that is assumed to be trustable, i.e., who represents the highest authority in a system and can grant and revoke access to it, and h) Trust levels.

Proposal

The authors analyze when to use each of the compared technologies. According to the authors, a Blockchain only makes sense when the actors are multiple, do not trust each other (mistrust), need to interact with each other to change the state of the system, and are not willing to agree on an intermediary (to entrust the changes they make). A flow chart is proposed that takes these aspects into account and indicates which of the three technologies is appropriate.

2.2.3. A framework for determining Blockchain applicability (Scriber, 2018)

Compared technologies

Blockchain

Analysis criteria: a) Data immutability, b) Transparency, c) Intermediation, d) Users' anonymity, e) Distribution: fault tolerance, security, public verifiability, and network threats, f) Compatibility with other systems, g) Easiness of migration, h) Data privacy, i) Number of organizations (that maintain the Blockchain), and j) Performance.

Proposal

The author states that a Blockchain application is not always appropriate or optimal: in many cases a (relational or non-relational) database might be better. The author proposes a framework for determining whether a Blockchain is appropriate for a system architecture. The framework is based on ten criteria (see previous paragraph). These criteria can be evaluated based on five fundamental questions: 1. Will the project require updates or deletion of records?, 2. Is there agreement that all validators should be able to view and validate transactions?, 3. Does this Blockchain application fit well with other company systems?, 4. Are there adequate incentives for validators to support the Blockchain indefinitely?, and 5. From a performance perspective, are enough validators and sufficient infrastructure to buoy the consensus mechanism and validate all transactions and authorization processes?

2.2.4. A ten-step decision path to determine when to use Blockchain technologies (Pedersen et al., 2019)

Compared technologies

Permissionless public Blockchain, permissionless private Blockchain, permissioned Blockchain, and relational and non-relational databases.

Analysis criteria: First, to define whether a Blockchain is used: a) An objective immutable log is required, b) Conflicting interests/trust issues, c) Frequency and ease of changing transaction rules over time, d) Intermediation, e) Number of actors, f) Storage (shared or personal), g) Trust levels, and variety of access rules. Second, to define the type of Blockchain: a) Consensus determination (inter-organizational or intra-organizational), b)

Need for public access, and c) Public nature of the transactions, i.e., are the transactions public.

Proposal

It is stated that Blockchain is a booming technology in the supply chain sector, however, it is a challenge to determine which type of Blockchain to use. A flow chart is proposed that considers these criteria and indicates whether a Blockchain is required. According to the authors, the use of a public Blockchain is justified when the following conditions are met: a) A shared database is required, b) An objective immutable log is required, c) The actors are multiple, do not trust each other, and are not willing to agree on an intermediary, d) The rules governing system access are different between the actors, and e) Transaction rules do not change over time. Finally, the type of Blockchain is decided by considering the privacy level of the Blockchain: permissionless public Blockchain or permissionless private Blockchain.

2.2.5. A vademecum on Blockchain technologies: When, which and how (Belotti et al., 2019)

Compared technologies

Open-permissioned Blockchains, private Blockchain, permissionless Blockchains, traditional central database, off-chain storage.

Analysis criteria: a) Adaptability to different use cases (flexibility), b) Cost, c) Data integrity, d) Data privacy, e) Fault-tolerance, f) Group of selected actors: need for a group of actors to be in charge of read and write operations, g) Intermediation, h) Number of actors, i) Performance (throughput), j) Operational platform: it allows the distribution of digital data with interactions between the actors and automate the business, k) Primary adoption: i.e., do the actors want to use Blockchain as a system of records (a data history preservation system) or as an operational platform?, l) Public community: responsible for the proper functioning of the system, through defined protocols and rules, m) Public verifiability, and n) Storage (shared or personal).

Proposal

The authors propose a decision model to answer the questions: when to use a Blockchain? and what type of Blockchain to use? It is based on a review of several use cases. According to the authors, Blockchain should be used when a shared ledger is needed, there are multiple writers, and the maintenance of the ledger is not the responsibility of an external third entity. If these conditions are met, then a decision should be made based on the group in charge of maintaining the ledger: if it is a public community, a permissionless Blockchain should be used; if it is a group of actors and, in addition, the ledger needs to be publicly verifiable, an open-permissioned Blockchain should be used. Otherwise, the pros and cons of using a Blockchain or a traditional database should be evaluated, see Table 1.

Tab. 1. Pros and cons of a Blockchain and a traditional database according to (Belotti et al., 2019)

Technology	Pros	Cons
Blockchain	Authenticity Data confidentiality Data immutability Data integrity Data privacy Decentralization Fault tolerance	Low performance.
Traditional database	Easy to use High performance Simple architecture (compared to a Blockchain)	According to the authors, the pros of Blockchain are absent in a traditional database.

If it is concluded that a Blockchain should be used, it should be analyzed which type should be used. If the application is a system of records, the level of confidentiality (high, medium, low, where confidentiality refers to the non-disclosure to the public of the transactions performed by Blockchain users) should be considered. For a high confidentiality level, a full-permissioned Blockchain should be chosen, otherwise, the pros and cons of a permissionless Blockchain and an open-permissioned Blockchain should be evaluated.

Tab. 2. Pros and cons of a permissionless Blockchain and an open-permissioned Blockchain according to (Belotti et al., 2019)

Technology	Pros	Cons
Permissionless Blockchain	Any user can become a member and contribute to its maintenance. Auditability Data privacy High security and robustness (it is quite robust against any type of failure, if 50% of the system nodes are honest). It requires less configuration (when compared to a permissioned Blockchain). Public verifiability Robustness	Little or no flexibility Little or no customization Low performance, especially in those Blockchains based on PoW. Low confidentiality of the Blockchain transactions.
Open-permissioned Blockchain	Greater flexibility and customization. High performance (throughput): it offers good performance due to their restricted nature; thus, data validation, verification, replication, and modification are faster with respect to a permissionless Blockchain. Medium confidentiality (restricted to a group of selected actors).	Less security and robustness because a restricted group of selected actors controls the system instead of a bigger public community. They are not fully private, therefore; they are not fully auditable. They require more configuration (when compared to a permissioned Blockchain).

The off-chain storage option (EBSI European Blockchain, 2023) is considered when there are large non-transactional data and it is preferred to store them outside the Blockchain (e.g., video files). The authors also propose the use of off-chain storage to improve the performance of the Blockchain.

If the application is a platform, its purpose must be identified: if it is for the exchange of digital resources, the choice depends on the privacy of these resources, if they are sensitive data and must be private, full permissioned Blockchain should be chosen, otherwise the costs and benefits between permissionless Blockchain and open-permissioned Blockchain must be evaluated. On the other hand, if the application is for automation of business functionalities, confidentiality should be re-evaluated, if required, full permissioned Blockchain should be chosen, otherwise the costs and benefits between permissionless Blockchain and open-permissioned Blockchain should be evaluated, see Table 2.

2.2.6. The revolution will be memorialized: Selected Blockchain-bases smart contract use cases (Catanzaro & Kain, 2020)

Compared technologies

Blockchain

Analysis criteria: a) Automation of processes, b) Data immutability, c) Data integrity, d) Data privacy, e) Decentralization, f) Multiple actors, g) Fault-tolerance, and h) Public verifiability.

Proposal

An appropriate use case for Blockchain must involve multiple actors and take advantage of decentralization. For those use cases that also involve automation of processes, smart contracts are of great help.

In this proposal, Blockchain is considered for the following use cases: a) Asset-based payment contracts (royalty payments for the sale of products), b) DAOs, c) Digital rights management, d) Domestic relations and probate (legal disputes about processes such as divorces, paternity, adoptions, among others), e) Investment contracts, f) Supply chain, g) Secured transactions: transactions with defined procedures to be executed in case of defaults, breach of contracts, pawns, mortgages, among others, and h) Securitized assets, replevin (claim and delivery, revendication), and attachment (rights over digital or tangible resources, with legal character).

No justification is offered for each of these cases; the assumption is that all cases correctly meet the qualities provided by a Blockchain. For most of the cases, the verdict is to use Blockchain with smart contracts.

2.2.7. When do we need the Blockchain? (Puthal et al., 2021)

Compared technologies

Blockchain.

Analysis criteria: a) Data integrity, b) Data privacy, c) Data security, d) Latency, e) Mining threats: because of the consensus mechanism, a Blockchain is exposed to threats such as selfish mining, block-withholding attack, and > 50% attack. Selfish mining: cryptocurrency mining strategy where groups of miners collude to increase their profits and exert power over a Blockchain (The Investopedia Team, 2023), block-withholding attack:

cryptocurrency mining strategy where a group of miners can withhold their verifications so that the profitability of the mining pool declines (Bag et al., 2016), > 50% attack: vulnerability of a Blockchain in which a group of miners greater than 50% of the total number of validators agree to commit fraud (Digital Currency Initiative, 2023), f) Network threats: attacks related to the system's telecommunications infrastructure, g) Performance, h) Scalability, i) Size, j) Smart contract threats: vulnerabilities in the smart contracts code, see, e.g., (Mehar et al., 2019) or the infamous The DAO hack (Austin & Lang, 2020), and k) Storage (shared or personal). Additional criteria are mentioned in their proposal, see next paragraph.

Proposal

A flowchart is proposed that considers the above listed criteria and indicates whether a Blockchain is required. According to the authors, the use of a public Blockchain is justified when a) A permanent use of shared data is required, b) Data privacy is not required, c) Data should not be modified after being recorded, and d) The actors are multiple, are the source of the data, and do not trust each other (mistrust).

2.2.8. Blockchain implementation opportunities and challenges in the Latin American and Caribbean logistics sector (Díaz et al., 2021)

Compared technologies

Blockchain.

Analysis criteria

The same as (Pedersen et al., 2019) (they use the same flowchart); however, additional criteria are mentioned in their proposal, see next paragraph.

Proposal

The authors use the same flowchart proposed by (Pedersen et al., 2019). However, they stated that i) if it is determined, from such flowchart, that a Blockchain should be used, it is still necessary to consider the computing infrastructure (see next paragraphs), the regulatory framework (see next paragraphs), and the development methodologies for a Blockchain project, ii) the lack of an exhaustive analysis of the requirements of Blockchain technology (e.g., its exponential growth in resource consumption), may lead to incorrect choices, and iii) as with any technology, Blockchain on its own is not a direct benefit to a company.

Computing infrastructure: a) Network structure: it includes the number of nodes, storage capacity, security issues, e.g., which information can be shared with the entire network and who owns the network generated information and b) Performance.

Regulatory framework: a) Data integrity and data security: it includes ownership and data access, rules for dealing with incorrect stored data in the Blockchain (because Blockchain data are immutable, then, how to proceed in such cases), b) Logistics business: cost and return on investment (ROI), and c) Market regulations: adoption of national/regional standards among the business actors, incentives to encourage a Blockchain solution.

The authors consider Blockchain for use cases relating to international trade and supply chains, where they highlight the following benefits: shorter delivery times, lower delivery costs, checks improvements, reduction of paper documents, dispatch errors, and trade disputes.

2.2.9. Blockchain reference guide adoption and implementation of Blockchain technology for the Colombian State (Espinosa, 2021)

Compared technologies

Blockchain

Analysis criteria: These criteria are generated from the questionnaire, see proposal: a) Intermediation, from question 4, b) Latency, from question 3, c) Public verifiability, from question 6, d) Storage (shared or personal), from question 1, e) Traceability, from question 5, and f) Trust levels, from question 2.

Proposal

The author presents a questionnaire developed by the Inter-American Development Bank (Serale et al., 2019) that seeks to answer whether it is advisable to use Blockchain:

1. Do you need all the involved actors to keep record of information and to access it?, 2. Does anyone involved have an interest in falsifying the registry information?, 3. Do you need to validate the registration of new information in real time or near real time?, 4. What do you think about of a central entity that validates/verifies all the information?, 5. Do you need a reliable historical record of the information to audit or track it?, and 6. Do you need to follow any validation process or get any permission to access the registered information?

In addition, the author also highlights the following criteria: a) Data immutability, b) Democratization of access to services: Blockchain enables more persons and institutions to access services, e.g., financial ones. However, this is a controversial point: not all citizens are prepared to use and to believe in this technology, c) Transparency, and d) Users' anonymity: it means that users' identity is hidden from the outer world. Although their online activity is still visible, it cannot be traced back to them (Immunebytes, 2023)

2.2.10. Framework for determining the suitability of Blockchain: criteria and issues to consider (Hassija et al., 2021)

Compared technologies

Centralized database, public Blockchain, private Blockchain (controlled by a single organization), consortium Blockchain (a hybrid Blockchain controlled by several organizations).

Analysis criteria: a) Data confidentiality, b) Data integrity, c) Data privacy, d) Intermediation, e) Number of organizations (that maintain the Blockchain), f) Number of writers, g) Storage (shared or personal), and h) Trust anchor.

Proposal

The authors state that due to the hype surrounding Blockchain, it is often suggested as a solution for almost any application. The authors propose a set of guidelines (a framework), along with a flow chart, to answer these questions: 1. Is Blockchain suitable for an area?, 2. How to assess if Blockchain is suitable to use or not?, and 3. What kind of "tests" can be used to determine if Blockchain will be good to use for an application?

Their flow chart allows the user to choose the type of Blockchain: private, public, or consortium. The authors conclude that a Blockchain only makes sense when a) A shared database is needed, b) There are multiple writers, and, c) There are untrusted stakeholders involved and there is not a trusted intermediary or there are not untrusted stakeholders, but the data is prone to attacks. Finally, if a Blockchain is needed, depending on the needs of

data privacy, permissions, and the number of organizations that maintain the Blockchain, the type of Blockchain is defined.

2.2.11. When you need Blockchain for your project and when it is not the best option (Haritonova, 2022)

Compared technologies

Blockchain

Analysis criteria: a) Digital assets management: i.e., to host, buy, and sell digital assets, b) Improved data security: enhanced security by storing data in a decentralized way. The author states that when a system is decentralized, the nodes are usually located in different places, making them much more difficult to hack. This helps to guarantee data immutability, c) Intermediation, d) Need to create your own cryptocurrency or tokens, e) Traceability, f) Transparency, and g) Trust levels.

Proposal

The author states that Blockchain is so popular that many companies simply follow the trend without conducting a feasibility analysis. Because of Blockchain's trust, transparency, and traceability, it is especially useful in transportation and supply chain, healthcare, and government (especially for elections) applications.

The author also presents some reasons for not using Blockchain: a) Scaling issues: Blockchain-based solutions may not be as fast as traditional systems because many nodes in different locations are involved in the transaction validation process, b) Immutability challenges: immutability could be an advantage or a disadvantage. It depends on your needs and requirements. if reversibility is a desirable feature, Blockchain is not an option, and c) Difficulty of development: developers need to know a certain programming language, e.g., Solidity for Ethereum, and write smart contracts extremely carefully: once they are deployed, they cannot be fixed, and mistakes will then cost money (Austin & Lang, 2020).

2.2.12. Blockchain vs Relational Database: Which is right for your application (Martin, 2023)

Compared technologies

Blockchain, relational database

Analysis criteria: a) Data integrity, b) Data security, c) Fault-tolerance, d) Intermediation, and e) Performance.

Proposal

The author states that: a) the high level of fault-tolerance of a Blockchain is hardly achievable with a relational DBMS, b) if an application with high performance (latency and throughput) is required then, a relational database should be used, c) there is no clear advantage for a Blockchain in terms of data security and data integrity, since a relational DBMS also offers cryptographic capabilities and usually provides audit tools to verify the traceability of transactions, and d) dispensing with an intermediary is not a significant advantage, because what is saved by not paying it, may be less than the costs involved in maintaining a platform such as Blockchain. A Blockchain excels when robust storage with high fault-tolerance is required, while a relational DBMS excels for its performance.

Regarding the other criteria evaluated, there is no clear advantage between one or the other technology.

2.3. Proposed use cases

We present in Table 3, in alphabetical order, the use cases described in the evaluated works, specifying which technology was recommended for each of them and stating the reason given by the author(s).

Tab. 3. Use cases described in the evaluated works

Use case	Reference	Recommended technology	Reason
Cryptocurrencies	(Martin, 2023)	Blockchain	It is the typical application in a public Blockchain.
	(Belotti et al., 2019)	Permissionless Blockchain	It is the typical application in a public Blockchain.
DAOs	(Wüst & Gervais, 2018)	Public Blockchain	Actors in a DAO usually do not trust each other or even know each other. A DAO has a decentralized nature and tends to be established on a public Blockchain and thus, provides an easy access point for actors.
Detection of discriminatory measures	(Díaz et al., 2021)	Blockchain	Blockchain encourages auditing; thus, businesses processes are more transparent and ethical.
Digital identity	(Espinosa, 2021)	Blockchain	Blockchain's data immutability and improved security for citizens (from birth to death certificates) allow public administrations to identify citizens unambiguously.
Education	(Espinosa, 2021)	Blockchain	Blockchain's data immutability prevents falsification of study certificates.
Healthcare	(Haritonova, 2022)	Blockchain	To create, store, and update electronic health records and give patients more control over their own health data.
	(Espinosa, 2021)	Blockchain	Protection against counterfeiting of clinical history and of the supply chain of medicines.
Interbank payments	(Wüst & Gervais, 2018)	Private Blockchain	A Blockchain for an interbank payment system is feasible, given the digital origin of the information and the need for interaction between multiple actors. It must be private, since the actors know each other and are restricted to a group.
Internet of things (IoT)	(Puthal et al., 2021)	Unspecified	The consensus mechanism (in particular, PoW) of a Blockchain tends to be computationally expensive for an IoT application, since IoT devices

Use case	Reference	Recommended technology	Reason
			usually have limited computational resources.
Ledger	(Puthal et al., 2021)	Blockchain	A shared ledger is the typical example of a shared database with interdependent transactions generated by multiple writers who do not trust each other.
Maritime transportation industry	(Pedersen et al., 2019)	Permissioned public Blockchain	This use case meets the conditions for a permissioned public Blockchain.
Multidrone network	(Hassija et al., 2021)	Public Blockchain	Communication between drones and charging stations is needed and information related to transactions needs to be shared. There is no need for a third party to maintain the ledger.
Orange economy applications	(Espinosa, 2021)	Blockchain	Blockchain can support the protection of artists' musical creations and allows the elimination of intermediaries.
Product provenance and traceability	(Díaz et al., 2021)	Blockchain	Greater accuracy in the management of product certificates, reduce the risk of provenance frauds, establish standards for certification of origin.
Proof of membership and voting	(Wüst & Gervais, 2018)	Public Blockchain	Through a Blockchain, it is possible to eliminate the intermediaries that oversee the certification of patents, memberships, and voting results. This system is decentralized and must be accessible to any actor.
Property registration systems	(Espinosa, 2021)	Blockchain	Blockchain's data immutability and improved security can help to secure land titling, or in general to secure any object's ownership.
Shared calendars, wiki-style Collaboration forums (Xu et al., 2021)	(Greenspan, 2015)	Blockchain	These applications are based on the verification of data that is recorded by multiple writers who do not trust each other.
Smart contracts	(Wüst & Gervais, 2018)	Unspecified	The recommended technology depends on the nature of the smart contract.
	(Díaz et al., 2021)	Blockchain	It would increase transaction efficiency: lower administrative costs and less delays because a smart contract executes automatically when its conditions are met.
Streamlining of commercial operations	(Díaz et al., 2021)	Blockchain	Secure information sharing, paperless trade, traceability (which favours better planning).
Supply chain	(Wüst & Gervais, 2018)	Centralized database	A Blockchain for a supply chain faces a barrier between the physical and digital

Use case	Reference	Recommended technology	Reason
			worlds, i.e., data integrity depends on the data digitalization of the physical world that will be stored.
	(Haritonova, 2022)	Blockchain	Blockchain helps track where goods come from and record all data in chronological order.
	(Hassija et al., 2021)	Private Blockchain	Blockchain can improve the transparency in a supply chain by providing information about the life cycle of a product to all actors. The system is managed by a single organization.
Trade finance	(Díaz et al., 2021)	Blockchain	Transparency, efficiency, and security of processes. Faster and cheaper transactions when compared with those of the banking.
	(Hassija et al., 2021)	Centralized database	According to the author, Blockchain still lacks scalability because it can process only a few transactions per second (however e.g., Ethereum 2.0 has improved a lot in this regard).
Voting	(Haritonova, 2022)	Blockchain	Trust and transparency for the voters. Immutability of their votes.
	(Espinosa, 2021)	Blockchain	Blockchain offers unique transparency that limits possible illegal practices during election times. Democratization of access to services.

Next, the authors summarized some findings from the evaluated works. 44 criteria were identified, 24 were mentioned in more than one work and 12 in at least 4 works. No criterion was mentioned in all the works. 20 criteria were mentioned in just one work. Of the 44 criteria, 20 were considered at least once as decisive in defining whether a Blockchain should be used, and 24 were considered at least once as decisive in defining the type of Blockchain to use. The five most mentioned criteria were intermediation, number of actors, storage type, trust levels and data integrity. The two most important criteria were intermediation and number of actors, both are thought to be critical in determining whether a Blockchain should be used. Criteria related to performance (including latency and throughput) tended to be less important than criteria related to non-negotiable requirements of the use cases, e.g., the number of actors is non-negotiable, i.e., it cannot be reduced due to the nature of the use case; in other use cases, it is unacceptable that data can be altered or lost (data integrity). On the other hand, different levels of latency can be accepted. The criterion of trust levels was highlighted in several works, although it had a lower average importance than other criteria (see Table 4).

In the works where the number of actors, intermediation, and storage type criteria were mentioned, they were always considered decisive in determining whether a Blockchain should be used. Only three of the twelve works indicated the type of Blockchain to be used

and only four use cases were mentioned at least twice: supply chain, healthcare cryptocurrencies, smart contracts, and voting.

21 use cases were identified, and for the 18 of them a Blockchain was considered suitable. No contradictions were found between the works, except for the supply chain use case verdict, which occurred between (Haritonova, 2022; Hassija et al., 2021; Wüst & Gervais, 2018). In Wüst & Gervais (2018) it is stated that a barrier to the use case lies in the digitization of the information, and because of this, no real benefit of using a Blockchain is observed. In Haritonova (2022) and Hassija et al. (2021) this barrier is not considered. For every verdict of each use case, it was indicated whether the verdict suggests a public or private Blockchain. We noticed that 11 verdicts recommend the use of public Blockchain, 3 private, 5 are inconclusive (private or public), and 1 hybrid.

For each criterion, we obtained the following metrics: the number of mentions it had in the various works (NM), the number of times it was considered decisive for Blockchain (ND), and its average importance (AI). To determine the importance of a criterion, we considered the priority given to the criterion in each work, i.e., how soon the criterion is considered in the decision stage (e.g., in a flowchart) to define whether to use a Blockchain. Finally, we obtained an impact ratio (IR) that quantifies the impact of the criterion with respect to the decision to use a Blockchain. This ratio is a weighted average of the NM (20%), ID (20%), and AI (60%). We gave more weight to AI, since NM and ID are co-dependent metrics, thus we prevented the sum of their weights from being greater than that of AI. However, the analyst could set other weights for these factors. Thus, IR = 0.2 * NM + 0.2 * ND + 0.6 * (1/AI). In Figure 2 we represent this process. In Table 4 we show the top ten criteria based on the highest IR.

The five criteria with the highest IR (intermediation, number of actors, trust levels, storage type, and public verifiability) coincide with the five most mentioned criteria in the works (with trust levels and storage type with exchanged positions).

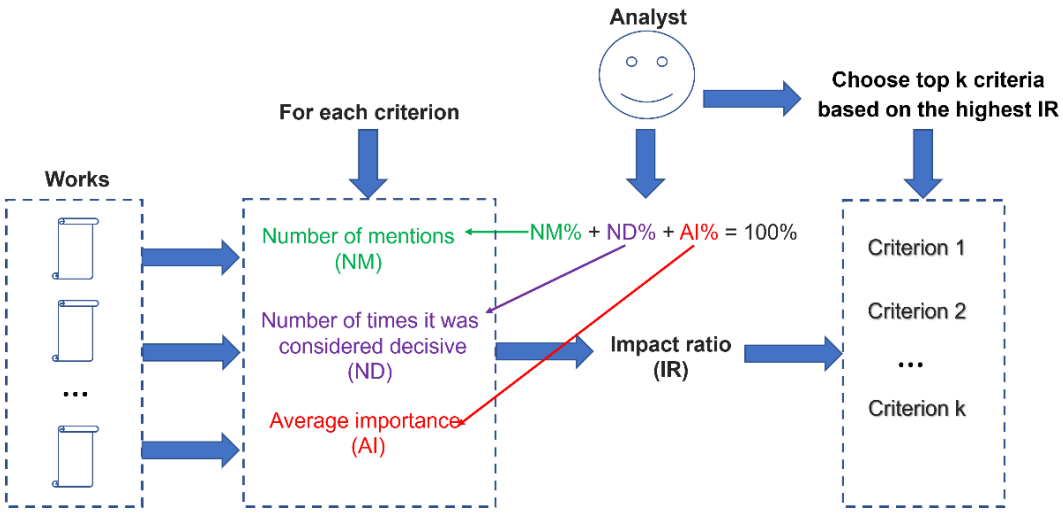

Fig. 2. Process for obtaining the top k criteria based on the highest IR

Tab. 4. Top ten criteria based on the highest IR

Position (according to IR)	Criterion	Number of mentions	AI	Is Blockchain decisive?	IR
1	Intermediation	10	2.75	9	4.01
2	Number of actors	9	4	9	3.75
3	Trust levels	7	1	7	3.4
4	Storage type	7	8	4	2.275
5	Public verifiability	7	7.3	5	2.48
6	Data integrity	7	3.43	7	2.98
7	Data immutability	7	6.25	3	2.1
8	Data privacy	6	6.5	3	1.89
9	Data security	5	7.5	2	1.48
10	Performance	5	7.5	2	1.48

In Table 5 we show which criteria are considered in each evaluated work; they are presented in descending order according to number of mentions.

Tab. 5. Criteria and evaluated works in descending order by number of mentions: a. (Greenspan, 2015), b. (Wüst & Gervais, 2018), c. (Scriber, 2018), d. (Pedersen et al., 2019), e. (Belotti et al., 2019), f. (Catanzaro & Kain, 2020), g. (Puthal et al., 2021), h. (Díaz et al., 2021), i. (Espinosa, 2021), j. (Hassija et al., 2021), k. (Haritonova, 2022), and l. (Martin, 2023)

Position*	Criterion	Number of mentions	a	b	c	d	e	f	g	h	i	j	k	l
1	Intermediation	10	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
2	Number of actors	9	✓	✓		✓	✓	✓	✓	✓	✓	✓		
3	Storage type	7	✓			✓	✓		✓	✓	✓	✓		
4	Trust levels	7	✓	✓		✓			✓	✓	✓		✓	
5	Public verifiability	7		✓	✓	✓	✓	✓		✓	✓			
6	Data integrity	7		✓			✓	✓	✓	✓		✓		✓
7	Data immutability	7			✓	✓		✓	✓	✓	✓		✓	
8	Data privacy	6		✓	✓		✓	✓	✓			✓		
9	Data security	5			✓				✓	✓			✓	✓
10	Performance	5			✓		✓		✓	✓				✓
11	Transparency	4		✓	✓						✓		✓	
12	Fault-tolerance	4			✓		✓	✓						✓
13	Transaction rules	3	✓			✓				✓				
14	Latency	3		✓					✓		✓			
15	Access rules	3				✓	✓			✓				
16	Number of organizations that maintain the Blockchain	3			✓		✓					✓		
17	Traceability	2									✓		✓	
18	Cost (logistics business)	2					✓			✓				
19	Scalability	2							✓				✓	

Position*	Criterion	Number of mentions	a	b	c	d	e	f	g	h	i	j	k	l
20	Throughput	2		✓			✓							
21	Validators	2	✓				✓							
22	Users' anonymity	2			✓						✓			
23	Trust anchor	2		✓								✓		
24	Network threats	2			✓				✓					
25	Consensus determination	1				✓								
26	Data confidentiality	1										✓		
27	Transaction interaction	1	✓											
28	Network structure	1								✓				
29	Automation of processes	1						✓						
30	Market regulations	1								✓				
31	Primary adoption	1					✓							
32	Flexibility (use cases)	1					✓							
33	Mining threats	1							✓					
34	Backing of the assets	1	✓											
35	Smart contract threats	1							✓					
36	Data redundancy	1		✓										
37	Size	1							✓					
38	Compatibility with other systems	1			✓									
39	Easiness of migration	1			✓									
40	Operational platform	1					✓							
41	Decentralization	1						✓						
42	Need to create and operate with a cryptocurrency	1											✓	
43	Democratization of access to services	1									✓			
44	Difficulty of development	1											✓	

*(according to the number of mentions)

To conclude, this study is beneficial for specialists dealing with Blockchain-based solutions, assisting them to decide which one is most suitable according to the application scenario they need to develop. This is achieved by distinguishing, evaluating, and ranking the criteria and by quantifying the average importance of each criterion and its impact,

factors which are considered critical in determining whether a Blockchain should be used or not.

3. USE CASE ANALYSIS

Next, the authors analyze two representative use cases of Blockchain considering the top ten IR criteria of Table 4 to verify their applicability in these cases.

3.1. Decentralized Currency

This use case is a currency that does not depend on a government or a central entity, but on the same actors that use it; this is the use case from which cryptocurrencies arise. In Table 6 we analyze this case against the top ten IR criteria.

Tab. 5. Analysis of case study: decentralized currency

Position (according to IR)	Criterion	Conclusion
1	Intermediation	A currency usually depends on a central entity that backs it, gives it value, and controls its issuance. With Blockchain, this entity can be disregarded, where the currency becomes the responsibility of the actors in the network. This use case requires that there be no such central entity.
2	Number of actors	The purpose of a currency is that it can be used as an exchange mechanism for valuables. This only makes sense if multiple actors can use the currency: a currency without a market in which it can be used is meaningless. Thus, the number of actors is much greater than one.
3	Trust levels	It is unusual to trust in unknown actors; thus, mistrust is high.
4	Storage type	For the system to remain decentralized, storage is usually shared and replicated.
5	Public verifiability	A centralized currency usually allows transactional information to be viewed by its stakeholders or by the government entities. However, a decentralized currency requires that this transactional information is available to any actor.
6	Data integrity	For a currency it is necessary to ensure the data integrity; therefore, the system must ensure that the transactional data cannot be altered or lost.
7	Data immutability	It is essential to prevent currency transfers' data from being altered.
8	Data privacy	The ability to maintain privacy in a monetary system is desirable because it allows actors to keep their identities hidden in the real world. Blockchain provides privacy to its actors by associating them with a unique address rather than personal contact data, which helps actors to keep their anonymity.

Position (according to IR)	Criterion	Conclusion
9	Data security	For a currency it is essential to prevent unauthorized users from accessing user accounts; otherwise, e.g., identity theft and improper transfers (which are practically irreversible) may occur.
10	Performance	In a traditional monetary system (banks), it is common to have interbank transactions to take hours or even days. In Blockchain systems, transactions usually take minutes (e.g., about 1 hour in Bitcoin and 5 minutes in Ethereum 2.0).

3.2. Supply chain

This use case is the correct flow of information between all parties interested in and responsible for the life cycle of a product or resource; it is a contentious case in terms of whether a Blockchain should be used. In Table 7 we analyze this case against the top ten IR criteria.

Tab. 6. Analysis of case study: supply chain

Position (according to IR)	Criterion	Conclusion
1	Intermediation	The management of the traceability of a resource in a supply chain can be accomplished through i) an intermediary and a centralized system agreed upon by a group of actors, or ii) a decentralized system without an intermediary. Users must consider the costs of each option. When the number of actors is small (e.g., less than 20) and trust levels are high, the first option is preferred; when the opposite is true, a decentralized system is preferred. This is a contentious criterion that is heavily influenced by the type of supply chain.
2	Number of actors	A supply chain has multiple actors who interact with one another at various points throughout the supply chain; thus, the number of actors is much greater than one.
3	Trust levels	The supply chain's actors use to have different levels of trust.
4	Storage type	Actors need to share information with each other to run their operations.
5	Public verifiability	The public's verification depends on the type of supply chain. The information could be confidential or public.
6	Data integrity	The data managed by the system must be highly accurate, as it may be critical to the compliance with regulations.
7	Data immutability	It is essential to avoid, e.g., altering the values of the life cycle records of a product (changes in numbers of units, prices, storage temperature, among others).
8	Data privacy	The level of privacy is determined by the type of supply chain. The information could be confidential or public.

Position (according to IR)	Criterion	Conclusion
9	Data security	In a supply chain, unauthorized users must be prevented from accessing the life cycle records of a product to avoid, e.g., espionage by competitors.
10	Performance	Since the time between their processes can be hours or even days, performance is not usually a priority in a supply chain.

On the other hand, NFTs are a specific use case for Blockchain that has received little attention in the works. NFTs are tokens that can be used to represent the ownership of a unique resource. NFT is a term in economics that describes items that do not have a fixed exchangeable value like a currency, because these items have unique properties. Examples of NFTs are a) Digital collectibles, b) Internet domains, c) Video game items, d) Tickets and coupons, and e) Unique digital artwork.

In the context of Blockchains, NFTs make it possible to represent a wide variety of digital items and replicate the properties of items in the physical world, such as scarcity, uniqueness, and proof of ownership (Ethereum.org, 2022).

NFTs are a use case that fits well with the established criteria for a Blockchain; they involve multiple actors exchanging these resources with each other, preferably without an intermediary, and the actors involved are not restricted to one group, so there is mistrust between them.

4. CONCLUSIONS

In this article, several works were analysed that evaluate the expediency of using Blockchain based on given criteria and use cases. Such criteria were compiled and evaluated according to an IR; the ten most important ones were determined and validated with two typical Blockchain case studies. The results can serve the analyst as a first step in determining whether a Blockchain-based solution is appropriate for his/her use case. However, the particularities of each case determine the final decision.

A Blockchain database is ideal for applications where data must be highly secure and unalterable, e.g., supply chains and decentralized currencies and transparency and trust are paramount, e.g., public voting systems and DAOs. Note that these two items are in accordance with the top ten criteria we identified based on the highest IR. On the other hand, there are applications where a conventional database (relational or non-relational) is more suitable than a Blockchain database, e.g., an ERP (Enterprise Resource Planning) system where frequent updates (to previous records) are needed along with thousands of instant operations. In a Blockchain the consensus mechanism adds overhead to the real-time, high-throughput needs of an ERP system. A second example is an online banking system where real-time transaction processing and immediate updates to accounts are required. A third example is a graph application, e.g., a social network where a graph database is highly optimized for traversing relationships between nodes, making it suitable for answering queries like “what is the shortest path between two nodes in a network?”. Performing such a query in a Blockchain system would be cumbersome since this type of database is not optimized to such use cases.

To conclude, it became evident that Blockchain stands out as a storage technology with shared storage and high data integrity; it should not be considered as a replacement or a competition with respect to conventional databases (relational or non-relational), but rather as an alternative for use cases that demand such requirements, i.e., applications that deal with digital goods and services and that require trust.

5. FUTURE WORK

Blockchain technology remains a hot research field and this is evidenced by the plethora of research papers published in this field nowadays. There are many research directions as future work. So, we plan to analyze the advantages of Ethereum 2.0, a Blockchain system that promises to improve performance and reduce the energy cost that some of these systems demand. Another work is the definition of a methodology to quantify the benefits of a Blockchain solution versus a conventional solution, accompanied by the development of one or more case studies, implemented in both solutions to determine the advantages and disadvantages of each one in a real environment. An additional research line is to define an assessment method regarding the usefulness of each proposal, i.e., a "gold standard" methodology for evaluating the actual usefulness of proposals that focus on when to use Blockchain. This assessment could consider factors such as the ones we mentioned at Section 2, along with the definition of some metrics.

Although our work was not focused on developing a framework for assessing when to use Blockchain, it could be beneficial for database designers and developers to have a well-defined framework for assessing when Blockchain is genuinely advantageous over other alternatives. Indeed, although we found and reported some flowcharts and frameworks, with that of Scriber (2018) being the most complete, we did not find any interactive tool for accomplishing this goal. The development of such tools complemented with the assistance of chatbots and generative IAs could hopefully lead to the choice of an appropriate database for an application.

An additional interesting research direction is the study of various distributed consensus algorithms used in Blockchain technologies (Guru et al., 2023; Lashkari & Musilek, 2021), their advantages and disadvantages in terms of data integrity, as well as their computational and communication costs. On the other hand, (Hassija et al., 2021), discusses briefly some challenges for Blockchain-based applications related to security issues. One is quantum attacks, i.e., quantum computers could break existing encryption techniques and may perform 51% attacks in the future. Another challenge are intelligent attacks, i.e., advanced attacks based on machine learning and game-theory attacks. Therefore, the level of security required by an application should be a factor to consider when considering a Blockchain-based solution. Blockchain-based applications face several attacks (Aggarwal & Kumar, 2021), such as user wallet attacks (phishing, dictionary attack), smart contracts attacks (vulnerabilities in their source code, malware), transaction verification attacks (51% attack, Finney attack), and network attacks (denial of service, sybil attack), among others.

Finally, we hope to identify use cases that are not fully adapted to either technology, but that through a collaboration of both achieve the desired goals, i.e., a hybrid solution that captures the best of both worlds. For example, Tian (2017) proposes a food supply chain traceability system for real-time food tracing based on Blockchain and Internet of things and

which relies on BigchainDB (https://www.bigchaindb.com). BigchainDB combines a distributed database (DDB) with Blockchain characteristics. In particular, from DDB, BigchainDB takes scaling in throughput, capacity, and efficient querying and from Blockchain, BigchainDB takes decentralized, immutability, creation and movement of digital assets.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

REFERENCES

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, *7*(2), 56. https://doi.org/10.3390/healthcare7020056

Aggarwal, S., & Kumar, N. (2021). Attacks on Blockchain. In *Advances in computers* (Vol. 121, pp. 399-410). Elsevier. https://doi.org/10.1016/bs.adcom.2020.08.020

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access*, *7*, 36500-36515. https://doi.org/10.1109/ACCESS.2019.2903554

Ali, A., & Afzal, M. M. (2018). Confidentiality in Blockchain. *International Journal of Engineering Science Invention*, *7*(1), 50-52.

Austin, R. D., & Lang, H. (2020). *The DAO Hack: A Blockchain Dilemma*. Ivey Publishing.

Bag, S., Ruj, S., & Sakurai, K. (2016). Bitcoin block withholding attack: Analysis and mitigation. *IEEE Transactions on Information Forensics and Security*, *12*(8), 1967-1978. https://doi.org/10.1109/TIFS.2016.2623588

Bao, J., He, D., Luo, M., & Choo, K.-K. R. (2020). A survey of Blockchain applications in the energy sector. *IEEE Systems Journal*, *15*(3), 3370-3381. https://doi.org/10.1109/JSYST.2020.2998791

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A vademecum on Blockchain technologies: When, which, and how. *IEEE Communications Surveys \& Tutorials*, *21*(4), 3796-3838. https://doi.org/10.1109/COMST.2019.2928178

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on Blockchain for information systems management and security. *Information Processing \& Management*, *58*(1), 102397. https://doi.org/10.1016/j.ipm.2020.102397

Bhanushali, H., Arthena, A., Bhadra, S., & Talukdar, J. (2019). Digital certificates using Blockchain: An overview. *2nd International Conference on Advances in Science & Technology (ICAST)*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3372133

BitFury. (2016). *On Blockchain Auditability*. https://bitfury.com/content/downloads/bitfury_white_paper_on_Blockchain_auditability.pdf

Buenrostro, E. D., Rivera, A. O. G., Tosh, D., Acosta, J. C., & Njilla, L. (2019). Evaluating usability of permissioned Blockchain for internet-of-battlefield things security. *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 841-846). https://doi.org/10.1109/MILCOM47813.2019.9020736

Carter, N. (2021). *How Much Energy Does Bitcoin Actually Consume?* Harvard Business Review. https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

Catanzaro, Z. L., & Kain, R. (2020). The revolution will be memorialized: Selected Blockchain-based smart contract use cases. *The Florida Bar Journal*, *94*(5), 52-56.

CoinMarketCap. (2023). *Decentralized Autonomous Organizations (DAO)*. https://coinmarketcap.com/alexandria/glossary/decentralized-autonomous-organizations-dao

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, *2016*(2), 6-10.

De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A survey of Blockchain-based strategies

for healthcare. *ACM Computing Surveys*, *53*(2), 1-27. https://doi.org/10.1145/3376915
De Wolf, M. (2024, December 16). *Data Security*. Techopedia. http://www.techopedia.com/definition/26464/data-security
Díaz, R. M., Valdés Figueroa, L., & Pérez, G. (2021). *Blockchain implementation opportunities and challenges in the Latin American and Caribbean logistics sector*. *387*(3), 1-16.
Digital Currency Initiative. (2023). *51% Attacks*. https://dci.mit.edu/51-attacks
Doubleday, K. (2018). *Blockchain Immutability-Why Does it Matter?* Fluree PBC. https://medium.com/fluree/immutability-and-the-enterprise-an-immense-value-proposition-98cd3bf900b1
EBSI European Blockchain. (2023). *EBSI Glossary*. European Commission. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Glossary
Espinosa, S. (2021). *Blockchain reference guide adoption and implementation of projects with Blockchain technology for the Colombian State*. https://gobiernodigital.mintic.gov.co/692/articles-161811_pdf.pdf
Ethereum.org. (2022). *Non-fungible tokens (NFT)*. https://ethereum.org/en/nft/#what-are-nfts
Ethereum.org. (2023). *Consensus mechanisms*. https://ethereum.org/en/developers/docs/consensus-mechanisms
Ethereum Blog Team. (2022, January 24). *The great renaming: what happened to Eth2?* Ethereum Foundation Blog. https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming
Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A review on the use of Blockchain for the Internet of Things. *IEEE Access*, *6*, 32979-33001. https://doi.org/10.1109/ACCESS.2018.2842685
Freeman Law. (2022). *Permissioned and Permissionless Blockchains*. https://freemanlaw.com/permission-and-permissionless-Blockchains
Gartner®. (2023). *Scalability*. https://www.gartner.com/en/information-technology/glossary/scalability
GeeksforGeeks. (2022). *Blockchain and Data Privacy*. https://www.geeksforgeeks.org/Blockchain-and-data-privacy
Greenspan, G. (2015, November 22). *Avoiding the pointless Blockchain project*. MultiChain. https://www.multichain.com/blog/2015/11/avoiding-pointless-Blockchain-project
Greenspan, G. (2016, April). *Beware the impossible smart contract*. MultiChain. https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract
Groschopf, W., Dobrovnik, M., & Herneth, C. (2021). Smart contracts for sustainable supply chain management: Conceptual frameworks for supply chain maturity evaluation and smart contract sustainability assessment. *Frontiers in Blockchain*, *4*, 506436. https://doi.org/10.3389/fbloc.2021.506436
Guo, Y., Wan, Z., & Cheng, X. (2022). When Blockchain meets smart grids: A comprehensive survey. *High-Confidence Computing*, *2*(2), 100059. https://doi.org/10.1016/j.hcc.2022.100059
Guru, A., Mohanta, B. K., Mohapatra, H., Al-Turjman, F., Altrjman, C., & Yadav, A. (2023). A survey on consensus protocols and attacks on Blockchain technology. *Applied Sciences*, *13*(4), 2604. https://doi.org/10.3390/app13042604
Haritonova, A. (2022, March 3). *When you need Blockchain for your project and when it is not the best option*. https://pixelplex.io/blog/why-use-blockchain-and-when-not-to/
Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V., & Gupta, S. (2021). Framework for determining the suitability of Blockchain: Criteria and issues to consider. *Transactions on Emerging Telecommunications Technologies*, *32*(10), e4334. https://doi.org/10.1002/ett.4334
IBM. (2023). *What are smart contracts on Blockchain?* https://www.ibm.com/topics/smart-contracts
Immunebytes. (2023, January 23). *Pseudonymity and anonymity: Be untraceable in the Blockchain world*. https://www.immunebytes.com/blog/pseudonymity-and-anonymity-be-untraceable-in-the-Blockchain-world
Imperva a Thales Company. (2023). *Fault Tolerance*. https://www.imperva.com/learn/availability/fault-tolerance
Kassab, M., DeFranco, J., Malas, T., Laplante, P., Destefanis, G., & Neto, V. V. G. (2019). Exploring research in Blockchain for healthcare and a roadmap for the future. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1835-1852. https://doi.org/10.1109/TETC.2019.2936881
Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews; Keele University Technical Report TR/SE-0401*. NICTA.
Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, *51*(1), 7-15. https://doi.org/10.1016/j.infsof.2008.09.009
Koepsell, D. (2019). Blockchain, Wikis, and the ideal science machine: With an example from genomics. *Frontiers in Blockchain*, *2*, 25. https://doi.org/10.3389/fbloc.2019.00025

Lashkari, B., & Musilek, P. (2021). A comprehensive review of Blockchain consensus mechanisms. *IEEE Access, 9*, 43620-43652. https://doi.org/10.1109/ACCESS.2021.3065880

Liu, J., Li, B., Chen, L., Hou, M., Xiang, F., & Wang, P. (2018). A data storage method based on Blockchain for decentralization DNS. *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)* (pp. 189-196). IEEE. https://doi.org/10.1109/DSC.2018.00035

Ma, J. (2023). *Latency*. Binance Academy. https://academy.binance.com/pl/glossary/latency

Marr, B. (2021). *The 5 Big Problems With Blockchain Everyone Should Be Aware Of*. Bernard Marr & Co. https://bernardmarr.com/the-5-big-problems-with-Blockchain-everyone-should-be-aware-of/

Martin, L. (2023). *Blockchain vs. relational database: Which is right for your application?* https://techbeacon.com

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in Blockchain: The DAO attack. *Journal of Cases on Information Technology, 21*(1), 19-32. https://doi.org/10.4018/JCIT.2019010102

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An overview of smart contract and use cases in Blockchain technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCCNT.2018.8494045

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future Blockchain networks: fundamentals, applications and opportunities. *IEEE Access, 7*, 85727-85745. https://doi.org/10.1109/ACCESS.2019.2925010

Oracle Corp. (2010). Chapter 11: Berkeley DB transactional data store applications. *Transaction throughput*. https://docs.oracle.com/cd/E17276_01/html/programmer_reference/transapp_throughput.html

Pedersen, A. B., Risius, M., Beck, R. (2019). A ten-step decision path to determine when to use Blockchain technologies. *MIS Quarterly Executive, 18*(2), Article 3.

Puthal, D., Mohanty, S. P., Kougianos, E., & Das, G. (2021). When do we need the Blockchain? *IEEE Consumer Electronics Magazine, 10*(2), 53-56. https://doi.org/10.1109/MCE.2020.3015606

Rouse, M. (2023, June 17). *Data Redundancy*. Techopedia. https://www.techopedia.com/definition/18707/data-redundancy

Scriber, B. A. (2018). A framework for determining Blockchain applicability. *IEEE Software, 35*(4), 70-77. https://doi.org/10.1109/MS.2018.2801552

Serale, F., Redl, C., & Muente, A. (2019). Blockchain en la administración pública:¿Mucho ruido y pocos bloques? *Banco Interamericano de Desarrollo*. https://doi.org/10.18235/0001951

Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via Blockchain. *Applied Sciences, 9*(6), 1207. https://doi.org/10.3390/app9061207

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of Blockchain technologies. *IEEE Security & Privacy, 17*(1), 72-77. https://doi.org/10.1109/MSEC.2019.2893730

The Investopedia Team. (2023). *Selfish Mining Definition*. https://www.investopedia.com/terms/s/selfish-mining.asp

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, Blockchain & Internet of things. *2017 International Conference on Service Systems and Service Management* (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2017.7996119

Turban, E., Pollard, C., & Wood, G. (2021). *Information Technology for Management: Driving Digital Transformation to Increase Local and Global Performance, Growth and Sustainability*. John Wiley & Sons.

Ullah, F., & Al-Turjman, F. (2023). A conceptual framework for Blockchain smart contract adoption to manage real estate deals in smart cities. *Neural Computing and Applications, 35*(7), 5033-5054. https://doi.org/10.1007/s00521-021-05800-6

Wüst, K., & Gervais, A. (2018). Do you need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE. https://doi.org/10.1109/CVCBT.2018.00011

Xu, Z., Liu, C., Zhang, P., Lu, T., & Gu, N. (2021). WikiChain: A Blockchain-based decentralized Wiki Framework. *Computer Supported Cooperative Work and Social Computing: 15th CCF Conference, Chinese (CSCW)* (pp. 46-57). Springer. https://doi.org/10.1007/978-981-16-2540-4_4