Blockchain Adoption as a Business Journey: A Thematic Literature Review of Drivers, Strategies, and Regulations

REALB KUSHE [1,a] *, KRESHNIK VUKATANA[2,b]
[1]Department of Informatics,
University "Fan S. Noli" Korçë,
Bulevardi Rilindasit 11, Korçë,
ALBANIA

[2] Department of Statistics and Applied Informatics,
University of Tirana,
Rruga Arben Broci 1 1001, Tiranë,
ALBANIA

*Corresponding Author

Abstract: - This paper presents a literature review of key business needs that remain difficult to address through traditional digital systems but can be effectively supported by blockchain technology. A total of 356 research papers were analyzed using a BERT-based clustering approach, leading to the identification of five major need categories: transparency and trust, data integrity and provenance, fraud prevention in identity management, fractional ownership, and secure cross-border payments. The implementation strategies associated with these needs are linked to practical use cases across sectors such as agriculture, supply chain, fintech, real estate, and e-healthcare. The findings highlight a growing shift from Layer-1 to more scalable Layer-2 solutions, driven by lower costs and increased development flexibility. In addition, performance benchmarks and regulatory developments in the EU, US, Japan, and Singapore are examined. The study concludes by proposing an iterative adoption framework in which business needs, technological choices, and regulatory considerations continuously inform one another.

Key-Words: - Blockchain, Real-World Assets, Fractional-Ownership, Stablecoins, Smart Contracts, Distributed Ledger Technology

Received: November 11, 2025. Revised: December 27, 2025. Accepted: January 19, 2026. Published: May 27, 2026.

1 Introduction

Nowadays, businesses from various sectors deal with clients' data in a consistent manner. Data is a valuable asset for the company, and it should be carefully treated in multiple dimensions: from its storage and privacy to the security of its movements through different systems or platforms (also known as "data interoperability") [1].

Each of these dimensions comes with its own challenges. The system architects who design the system architecture to accommodate business workflows face the old and familiar problem: they have to make a trade-off between privacy, transfer speed, storage capacity, etc., to design sustainable and easy-to-use data systems for businesses. In order to build systems that benefit at the optimal point of this trade-off, without risking the degradation of any of the above-mentioned system features, system architects have shifted their focus from traditional system infrastructures to new and innovative ones. Among them, blockchain technology is one of the most discussed innovations [2], [3]. Still, blockchain adoption is not a simple task, just like adding a new Google Chrome extension. The business workflow has to shift to an entirely new digital infrastructure without risking data leakage during the transition process. Without prior investigation of the principles of how blockchain networks work, the transition could turn into a headache for them.

On the other hand, if the blockchain implementation journey goes well, businesses may benefit a lot from it. The data will eventually gain a safety and privacy boost. Due to the minimization of data redundancy by the blockchain network, they may be served faster per need, and eventually, there will be more room to experiment with new business features on top of them. This motivates us to further investigate the state-of-the-art literature regarding practical use- cases for businesses and extract important and interconnected implementation "mini-themes" along the review process. Our literature review is guided by four research questions, which collectively capture the entire blockchain implementation journey of businesses and their related experiences, as illustrated in Figure 1 (Appendix).

Since "Research Questions" correspond to distinct yet interconnected "mini-themes" within the blockchain implementation process, we decided—for the reader's ease of navigation—to map them to specific Results & Discussion domains.

By following our proposed navigation pathway, presented in Figure 2 (Appendix), the reader can explore the journey of the implementation life cycle and form an authentic, independent perspective by the end of it.

2 Research Methodology

The literature on blockchain for real-world applications is relatively new and constantly evolving. The field is also rich in fresh ideas and diverse strategies, often moving in directions that do not always converge. For this reason, we chose to design a clear methodological framework to identify and analyze the studies most relevant to our research questions.

2.1 Scientific Material Repositories Selection

ACM Digital Library, ScienceDirect, and IEEE Xplore Digital Library are well-established repositories of computer science and engineering research that contain peer-reviewed conference proceedings and journals. ACM publishes specialized blockchain-related conferences, such as the ACM Transactions on Blockchain (TOB) and the ACM Conference on Advances in Financial Technologies (AFT), which naturally makes it a pivotal reference source for our research. IEEE is both an international professional organization that manages IEEE Xplore and the organizing body for the annual IEEE Conference on Blockchain and Cryptocurrency. This highlights the notable contribution of this organization and its corresponding digital library to our research topic.

2.2 Initial Search

We began by exploring the three repositories listed in Section 2.1, using the following search strings:

RQ1- *"Business needs addressed by blockchain"* **OR** *"Core Business needs"*

RQ2- *"Blockchain selection"* **AND {**"criteria" **OR** *"metrics"* **}**

RQ3- *"Blockchain use cases across industries"* **OR** *"blockchain adoption rate"* **OR** "*Impact of blockchain on Real-World Asset (RWA) implementation"*

RQ4- *"Blockchain regulatory"* **AND {** *"framework"* **OR** *"legislation"* **}**

We exported the metadata from each query, including journal and conference papers, into three CSV files, each corresponding to one repository.

2.3 Preliminary Screening of Metadata from Research Papers

The implementation journey starts with the identification of the key business needs that cannot be addressed by traditional digital systems. In this early step of our literature review, we searched for available software tools that can help identify and extract those needs from the research papers. Among them, we consider the Replit development environment to be the most adaptive and user-friendly. It offers a large number of natural-language-processing libraries as well as results-visualization libraries.

For the key business-needs classification task, we employed a Python-based library that implements BERT (Bidirectional Encoder Representations from Transformers). For readers interested in using this library, we note that it is a highly efficient natural-language-understanding model, particularly suited for tasks where contextual interpretation is essential. Initially trained by Google's research team in 2018, BERT now operates in a self-supervised manner [4]. It continuously learns from previous applications, improving over time in recognizing linguistic patterns and performing thematic clustering of metadata. We value this model because it does not require pre-defined labelled data for its classification tasks, which, in our view, significantly reduces the classification bias encountered in earlier language models.

Once the Replit AI agent applied BERT to our dataset, it grouped similar research topics, forming clusters of business needs based on semantic relationships.

The dataset was mapped by the model via self-supervised learning across two key dimensions, on a scale from 0 to 1, based on the metadata mentioning and connections, where this range manifests the transition of topics from the left to the right side of each axis, as illustrated in Figure 3 (Appendix).

The identified key business needs: X-axis: *Technical Complexity → Business Value Impact* and Y-axis: *Infrastructure Investment→Market* Opportunity Transparency and Trust accounted for

15.2% *(55 research papers)* of the total cluster distribution, followed by Data Integrity and Provenance at 14.3% *(52 research papers)*, Fraud Prevention in Identity Management at 13.2% *(48 research papers)* Fractional Ownership at 12.4% (45 research papers), and Secure and Efficient Cross-Border Payments at 11% *(33 research papers).*

While all identified needs are important, to maintain the breadth and depth of this review, only the key needs of businesses included in these five major clusters were taken into consideration in the screening process *(233 research papers).*

2.4 Full-text Screening process

2.4.1 Distribution of research papers across key business sectors and the needs they address

As part of the full-text screening process, we first analyzed how these needs manifest across five key sectors—healthcare (S1), supply chain (S2), real estate (S3), agriculture (S4), and fintech (S5) to highlight both the main areas of interest and the extent to which each sector has been studied. The distribution is summarized in Table 1.

Table 1. Business Needs Across Industry Sectors by Number of Research Papers.

Business Need\Sector	S1	S2	S3	S4	S5	Total
Transparency & Trust	12	16	8	5	14	**55**
Data Integrity & Provenance	11	14	6	6	15	**52**
Fraud Prevention in Identity Management	10	9	5	5	19	**48**
Fractional Ownership	6	4	14	2	19	**45**
Secure & Efficient Cross-Border Payments	4	6	2	0	21	**33**
Total	**43**	**49**	**35**	**18**	**88**	**233**

Source: created by authors.

In supply chains and agriculture, publications addressing transparency and data integrity *(16 and 14 papers for supply chains; 5 and 6 for agriculture)* point to closely connected sectoral needs. The post-COVID-19 pandemic revealed weaknesses in logistics and food supply chains. In addition to this situation, Regulatory initiatives like the EU's Farm to Fork Strategy and US food traceability programs may drive research interest in blockchain.

In fintech, the focus on fraud prevention, cross-border payments, and transparency *(19, 21, and 14 papers)* mirrors the rise of digital payment systems and stricter regulations such as the EU's PSD2 directive and US anti-money laundering frameworks.

In the healthcare sector, large-scale regulations, such as the EU's GDPR and the US's HIPAA, play a key role in identifying and addressing gaps or weaknesses that could lead to patient data breaches. We strongly believe that this proactive approach has triggered increased research interest in how blockchain applications can ensure data transparency *(12 papers)* and integrity *(11 papers).*

Among the most discussed topics in these papers are the development of unified blockchain network protocols for inter-hospital data exchange and the level of controlled access to clinical trials by participating patients. In this way, even within telemedicine platforms, patients should be able to choose which sensitive data to share with other involved entities. Blockchain can not only address these challenges but also improve liquidity in the real estate sector by attracting younger generations and tech enthusiasts to invest in this traditional market.

2.4.2 Distribution of the research papers According to their year of publication

Over the past few years, blockchain-related publications have steadily increased across nearly all business sectors. Between 2019 and 2025, this trend is evident in healthcare, supply chain management, real estate, agriculture, and especially fintech, as shown in Figure 4.

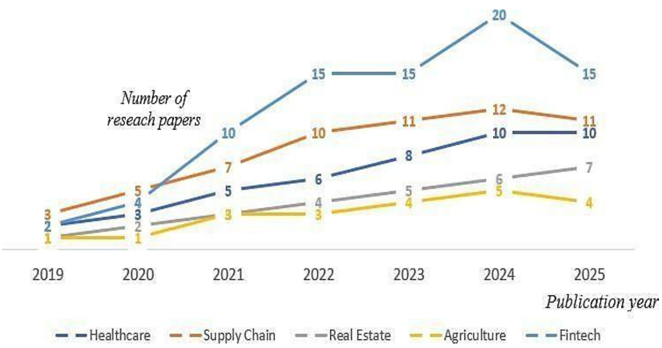

Fig 4: Trend of blockchain-related research papers by industry sector (2019–2025).
Source: created by the authors through the processing of the literature.

The close connection between the fintech sector and digital innovation and rapid technological change has naturally positioned it to explore and experiment with blockchain solutions earlier and more decisively than other sectors.

2.4.3 Application of Exclusion Criteria during Manual Screening

To make sure that only relevant studies aligned with our research questions were further analysed, we also carried out a manual screening phase.

Under the umbrella of the first exclusion criterion were all research papers that discussed purely theoretical blockchain models or conceptual frameworks *(n = 35 excluded research papers).*

Secondly, studies that did not examine key blockchain selection factors—such as scalability, security, transaction costs, interoperability, or governance models—were excluded from further review *(n = 28 excluded research papers)*. During our review, research papers that did not address regulatory and compliance aspects of blockchain implementation—such as Know Your Customer (KYC), Anti-Money Laundering (AML) requirements, or alignment with the existing legal framework were excluded *(n = 29 excluded research papers).* The PRISMA flow diagram for the complete selection process of the literature review is presented in Figure 5.

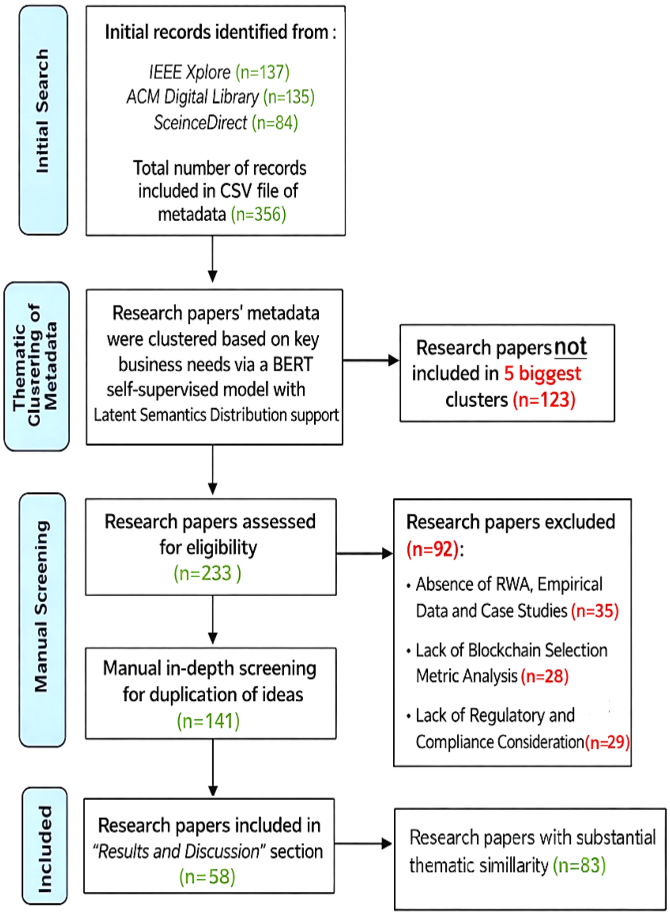

Fig 5: PRISMA flow diagram for the complete selection process of the literature review. *Source: created by authors.*

3 Results and Discussion

3.1 Core Business Needs Addressable by Blockchain - Based Solutions

3.1.1 The Need for Transparency and Trust.

With the explosion of digital marketing, a field that strongly appeals to younger generations, a considerable portion of business funds is directed toward targeting potential clients through digital channels. Conversely, some media influencers and digital marketers have engaged in practices that undermine trust with their clients, such as purchasing fake followers and using bots to comment on their posts [5].

Establishing a reputable digital identity is far more complex than simply purchasing the X.com verification mark for one's profile. The authenticity of posts and even the sponsorship of digital campaigns should be transparent to earn the trust of a large-scale audience and stakeholder businesses. Consequently, interest is growing in building digital identities on blockchain infrastructures [6]. Their credibility depends on designs that apply NFT logic, allowing them to inherit the same transparency.

From another business sector perspective, today's supply chains are complex because products pass through many hands before reaching the final consumer. The legislation, such as the EU's "from farm to fork" concept, aims to assign the appropriate responsibility to each actor in the supply chain [7].

From food harvesting to processing, storage, and transport, blockchain technology can be used to securely store the data related to all these processes.

This should increase overall transparency across the entire supply chain and make it easier for legal bodies to audit the implementation of the law among the involved parties.

3.1.2 The Need for Data Integrity and Provenance

Data integrity and Provenance are two vital components, let's say the fuel and battery that drives the workflow machinery of many business models. Sensitive business models, such as pharmacies, require the highest degree of provenance for their medical products. Those products, by nature, are parts of multi-party production lines, starting from raw material compounding to clinical trials and mass distribution. Whether there is a shortage or any event that targets specific products, the end sellers should be notified to take proactive steps. The data lineage should be fully preserved and audited, even by legal bodies, such as the FDA and EMA.

Financial institutions, such as banks, hedge or investment funds, connect clients to a broad, dynamic financial market. When it comes to the integrity of the information from such a valuable market, it is a must to provide only real-time verified information. A mismatch between actual stock prices and those given to clients can result in a huge financial loss and damage to the trust of stakeholders in the market. Blockchain may adequately meet that need by offering reputable mechanisms for the distribution of financial operations.

The need for data integrity is crucial even in business models that aim to optimize traditional state processes, where the election case is the most representative one. As digital voting systems emerge worldwide, so does the need for vote integrity [8]. In this context, a notable study proposes a blockchain-based voting system called *"Next-Gen Voting"* [9]. It combines asymmetric encryption and digital signatures to ensure both anonymity and integrity of each vote, making the entire process immune to silent alteration.

3.1.3 The Need to Prevent Fraud in Identity Management

The online job market is a complex and not very bright landscape. There are tons of daily job seekers who tend to fake their CVs, letters of reference, and qualification reports to gain an unfair edge over legitimate candidates. This problem is amplified for large-scale companies that rely on third-party HR agencies [10], [11]. In this context, the validation of real data for job seekers could become easier and safer if their past employment and academic data were mapped on a blockchain by their previous employers or educational institutions.

Actually, there are many attempts and successful startups developing previous job or study experience verification tools on L2 blockchain networks built on top of the Ethereum mainnet [12], [13]. These tools, if proven sustainable over time, may be used by human recruitment companies, in the form of a node on the blockchain, to verify applicant data. We find it particularly valuable—especially for the theme of merit-based recruitment—if universities were allowed to upload their verified degrees and certificates directly onto these L2 blockchain platforms. Some experiments have already started at MIT, the University of Nicosia, the University of Bahrain, and the University of Lille. Still, these pilot projects remain confined to their own academic ecosystems, with very little interaction with HR companies. All actors involved in this process could gain much more if there were a shared, well-integrated framework that linked these blockchain applications under a single verification standard.

Identity management, though it sounds corporate, happens quietly in every daily exchange—from buying coffee to boarding a train. As clients, we should have the full right to decide what personal information to share with those services. The level of privacy in data sharing should always be proportional to the situation. For instance: *"Why should a messaging app need access to the camera or photo gallery if its main purpose is just to send and receive text messages?"*

The same principle applies to so-called "self-sovereign systems". Self-sovereign systems are also well-suited to meet strict GDPR requirements, especially in healthcare, where protecting patient data is crucial. Information such as diagnoses or previous treatment plans can be shared on-demand with hospitals or medical centers through cryptographic private-public key pairs, without needing a central repository. Similarly, the fintech sector could benefit greatly from self-sovereign systems.

3.1.4 The Need for Fractional Ownership

Many individuals or companies worldwide are interested in acquiring portions of valuable assets, such as precious metals. They typically do not seek to evade taxes, but they also prefer not to be publicly identified [14]. Smart contracts can address these two main concerns: 1) they can provide a unified, widely accepted notary system that is low-cost as well as private and highly accessible, and 2) they can enable the division of asset holdings into smaller portions, similar to the issuance of digital tokens.

Along the same lines, a tangible portion of the middle and upper classes in countries with high inflation, such as Argentina and Turkey, looks to diversify part of their investments into real estate as a way to preserve purchasing power over time. Yet, the high cost of property makes such investments difficult, particularly for younger investors [15]. Every day, bureaucracy and notary fees weigh heavily on how many companies operate. Blockchain may offer a simpler alternative that is capable of transforming the traditional business model of real estate. Countries such as Singapore and Japan are among the first countries to actively implement blockchain technology for fractional ownership of properties. Fractional ownership has become essential for attracting global liquidity in many markets.

3.1.5 The Need for Secure and Efficient Cross-Border Payments.

Cross-border transactions often pass through several intermediaries, such as correspondent banks, clearinghouses, and payment processors. This multistep chain slows settlements and raises costs through added transaction fees, as in the case of SWIFT.

Blockchain simplifies payment systems that have long depended on layers of intermediaries. It enables parties to transact directly through a decentralized ledger, replacing multiple verification steps with one shared record of trust [16]. This reduction in intermediaries naturally accelerates transaction time and lowers operational costs, while also strengthening the overall Quality of Service (QoS) delivered to users.

3.2 Business-Driven Blockchain Selection Through Metric Evaluation

Selecting an appropriate blockchain network for business use is rarely straightforward. It is less a sprint and more a marathon that unfolds through several small yet telling checkpoints [17], [18], [19].

3.2.1 Scalability

Scalability has always been a concern for information systems, and the same issue extends naturally to blockchain. Since these systems belong to the wider family of distributed networks, their scalability should be examined through three lenses: network throughput, data storage, and communication efficiency [20]. Each of these dimensions matters, yet users tend to feel the impact of “network throughput” most strongly when congestion occurs. The Bitcoin network is penalized for “Real-World-Applications” due to its limited throughput. Its internal architecture supports only blocks with a size of up to 1 MB, and it also employs a 10-minute interval between consecutive blocks. This turns the network into a non-feasible Solution for real-time applications, such as financial ones. The VISA network, which relies on traditional financial technology and protocols, can comfortably process up to 2,000 transactions per second [21]. With the focus on filling the network throughput limitation gaps, several promising initiatives have been introduced to the blockchain development community.

The most effective ones, especially for large-scale Layer-1 Proof-of-Stake networks, are “sharding” and “the use of off-chain channels” to distribute computational workload [22]. This helps blockchain networks scale well horizontally without degrading overall performance. Sharding increases fault tolerance because data processing is shared concurrently among independent pieces of the network called “shards”. Other blockchain networks are natively designed with scalability in mind. Hyperledger Fabric responds faster and more reliably to transactional loads compared to Ethereum, and comparative benchmark studies confirm this finding [23].

However, as Ethereum is constantly upgraded to improve its internal scalability mechanisms, the gap tends to narrow over time. Companies, especially fintech ones that are easily adaptive to innovation, are turning to another group of Layer-2 blockchain networks that have reported fewer scalability issues [24]. Among them, blockchain networks that rely on ZK- Proofs and Optimistic Rollups for transaction validation are the lightest yet very accurate. Optimistic Rollups, for instance, assume transactions are valid and verify them only if a dispute occurs. This shift greatly improves speed while lowering implementation costs [25].

3.2.2 Security

Cybersecurity is making headlines not only for traditional systems but even for blockchain-based ones. Nowadays, attacks combine different strategies to DDoS blockchain networks (and take down their services as a consequence) or intercept data. Proof-of-Work networks may impose a security layer that is not easy to break through, due to the high computational cost of the mining process. After all, it is nearly impossible and extremely costly to own 51% of validator nodes in large-scale networks such as Bitcoin. On the other hand, this added security comes at the expense of reduced scalability.

A more balanced trade-off between security and scalability appears in those blockchain networks that rely on the Proof-of- Stake consensus mechanism. Ethereum 2.0’s Beacon Chain, for example, combines slashing penalties for validator misbehavior. It applies penalties respecting an axiom: “Multi-layer attacks should be handled with multi-layer solutions.” In the case of Ethereum, hybrid protocols are used — “Casper FFG” for transaction finality and “LMD-GHOST” for fork choice [26]. This way, threats are adequately addressed, and the overall blockchain network remains stable over time. In smaller Proof-of-Stake ecosystems, especially those with weak tokenomics, validator attacks are not unheard of.

If someone manages to purchase a large portion of the circulating native coins of a blockchain network, they may easily compromise the validators [27]. Likewise, Proof-of-Space and Proof-of-Capacity systems risk security imbalance when a few nodes control the majority of storage [28].

Validator compromise is just one side of the coin. The other includes the compromise of smart contracts, bridges, channel attacks, and many other targeted types of attacks [29]. On behalf of added security for their smart contracts, the Tezos and Polkadot networks apply formal verification to each smart contract prior to its deployment. The added overhead is insignificant compared to the additional security provided to the overall network.

Polkadot uses its Nominated Proof-of-Stake mechanism (NPoS) to validate transactions via distributed parachains [30]. This drastically improves the decentralization and security of the Polkadot blockchain network because under these conditions, there does not exist a single node or major cluster of nodes to attack. Mutual trust is also strengthened through the use of parachains [31].

3.2.3 Interoperability

From our standpoint, the Web 3.0 era is very different from the ".com Bubble" era. The blockchain infrastructure has created immense possibilities for developers to turn their ideas into useful products within a maturing ecosystem. The family of already published applications in the Web 3.0 ecosystem is large and still expanding every day: ranging from DeFi apps (Uniswap and Aave) to NFTs (OpenSea) and digital metaverse platforms (Axie Infinity, Decentraland, The Sandbox).

The infrastructure behind these apps is also progressively expanding, and with that, a recurring Need continues to emerge: the need for interoperability in data exchange between different networks. Business interests change dynamically, and so do their chosen blockchain networks. These networks should be flexible enough to migrate data from third parties and integrate it smoothly on-chain. Polkadot achieves a high degree of interoperability through its relay chain, while Cosmos uses the Inter-Blockchain Communication (IBC) protocol [32], Ethereum and Tezos leverage the infrastructure of existing Layer-2 solutions built on top of them to maintain interoperability and sustain smooth interactions with each other [33].

3.2.4 Governance Model

The blockchain network governance model significantly impacts its overall performance. In the context of large-scale Layer 1 blockchains, any governance change is a major and possibly disturbing event.

On the other hand, businesses do not want the headaches caused by the transitional states of blockchain networks or hard forks. Tezos and Polkadot use on-chain governance, where coin holders vote on whether to implement new features for the network [34]. This minimizes the risk of fragmenting the network through hard forks.

3.2.5 Transaction Speed and Latency

When livestreaming exploded worldwide, it changed the way people communicate and interact in real time. For a livestream to function effectively, video data packets must travel across the internet with very low latency, ideally within a few hundred milliseconds to a few seconds [35].

If next-generation media platforms were to move onto blockchain infrastructures, network speed would quickly become the decisive measure of performance. Developers have wrestled with the limits of transaction speed for years, often trying to fix it piece by piece rather than through a single breakthrough.

Ethereum 2.0 improves on its predecessor by using "sharding" [36]. Solana reaches even higher speeds through a hybrid of Proof of History (PoH) and Proof of Stake (PoS). Together, these mechanisms make it one of the few blockchains able to handle continuous, real-time activity.

3.3 Comparative Performance Synthesis of Major Blockchain Networks

Validating theory through practice marks a decisive moment in any system's journey from concept to implementation. Because blockchain networks evolve constantly, and business requirements change with them, we turned our attention to studies that report practical, tested benchmarks across major networks.

To keep the review current, we restricted it to the state-of-the-art benchmarks published between 2023 and late 2025. Readers interested in the full dataset can find it under "Observed Blockchain Performance Benchmarks" in References.

Table 2 (Appendix) presents the blockchain performance benchmarks, including network/layer type, observed throughput and finality, average transaction fees, key advantages, observed challenges, and benchmark references.

While we examine those benchmark results, we can draw some valuable insights:

1. HyperLedger Fabric and Solana dominate the field when it comes to the highest throughput (up to 3000 Transactions per Second for HyperLedger and up to 5000 TPS for the Solana network). This makes them the most suitable networks for applications that rely heavily on data, such as those transmitted by IoT devices. E-healthcare and agriculture are among the top beneficiaries if implemented on one of these two blockchains. Their system sensors continuously send data periodically (patients' health data in the case of e-healthcare systems, or harvesting data in the case of agriculture).

2. Between HyperLedger Fabric and Solana, the former offers a thicker layer of security. Businesses that want to seriously invest long-term in the blockchain implementation of their workflow should consider private or consortium (in the case of large corporations) HyperLedger Fabric networks. That way, they have the flexibility to design their own private policy regarding the tokenomics of the cryptocurrency that will operate in their private chain.

3. The math behind blockchain networks that are on testnet and development mode is a bit different. Those businesses that want to deploy their workflow in a mature form should first experiment with less expensive blockchain networks that provide a similar level of scalability and processing speed. Polygon is a cheaper (with a transfer fee of around 0.005 USD per transaction) and lighter blockchain network.

Even startups that typically do not possess huge development funds may experiment with Polygon. Tezos and Solana cost at least twice as much per transaction, while HyperLedger may require an initial upfront implementation cost. These are reasonable arguments why startup interest may naturally shift toward Polygon.

4. **The gap in features between Layer 1 and Layer 2 solutions is projected to narrow over a 1–2 year timespan.** As both the developer community and traditional investors still believe in the reputation of big players (such as Ethereum and Solana), funds will continue to flow into the development of new libraries and mechanisms related to Layer-1 PoS blockchains. On the other hand, Bitcoin will remain a symbolic network, mainly used for trading or speculative purposes rather than practical business use cases. This dynamic is expected to further reinforce the dominance of established ecosystems while gradually improving the competitiveness of Layer 2 solutions.

3.4 Blockchain Implementations Across Industries and Their Business Impact

3.4.1 Retail Sector and Supply Chain

The retail sector is the broadest market with the largest consumer base worldwide. The mismatch between supply and demand is an old yet persistent problem. In U.S. supermarkets alone, one-third to two-fifths of stored food is wasted annually. This phenomenon has lasting negative effects, ranging from financial losses for supermarket owners and

Food producers are aware of the environmental footprint caused by the disposal of food waste. Recent blockchain initiatives such as “InstaMart” and “Mobile Edge Computing (MEC)” aim to strengthen coordination among all actors involved in the supply chain [37], [38], [39]. Their design focuses on capturing the entire process, from food harvesting to its final serving on the dinner table of the end customer. These statistics may guide producers and resellers to produce and sell the products that consumers actually need.

3.4.2 Agriculture

An even more alarming indicator comes directly from the primary production areas where fruits and vegetables are cultivated. Supermarket waste accounts for only 8% of annual food waste, and the rest comes directly from “ready-to-harvest” field products. These do not match the market need, and as a result, their life cycle starts and ends in the same field.

Farmers should have access to real-time market data to make informed decisions about what to cultivate based on actual retail demand. Such data alignment would reduce surplus and converge balance production and consumption more effectively [40].

As we explored the literature on further improvements to blockchain networks in the retail industry, a clear trend emerged: distributed applications that employ the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism are considered reliable by consumers [41], [42], [43].

A bit costly to implement but still very beneficial for reliability among participants would be mapping the food data coming from RFID and GPS technology directly to blockchain [44], [45]. This would definitely create a transparent and verifiable tracking path for food—from land to the kitchen table. Truly organic and well-stored food would have enough room to distinguish itself from other food qualities on a merit-based blockchain system. The origin of halal food and product-related claims could be resolved on blockchain through verification smart contracts [46], [47]. All involved parties in the supply chain and the interconnected retail sector, through IoT devices, would be more engaged in cooperating within a safer and more trustworthy food industry [48], [49], [50].

3.4.3 Fintech ID Solutions

Fintech companies are among the fastest runners toward blockchain technology implementation. They are, by nature, more privileged than other sectors because they have been familiar with computer systems for a long time. Their focus has now moved beyond simple database storage toward embedding client biometrics directly on-chain. BioZero, for example, is an application that stores facial recognition data on a Layer 2 network built on top of blockchain [51].

The storage of such sensitive data comes with an inherent risk of breach, as identity information acts as "fuel" for hackers worldwide. If they manage to obtain sensitive data, they could target several services that the victim client uses and execute a financial attack. Consequently, the biometric details, by standard procedure, are salted and encrypted before being stored on the blockchain. Blockchain bridges are audited and tested consistently by Fintech companies in order to maintain a safe environment for their applications.

To achieve full anonymity and ensure the authenticity of each vote, blockchain-based voting systems— similar to those employed in Fintech— use SHA3 hashing algorithms before recording individual votes on the chain [52]. At a broader level, "self-sovereign" digital systems show promising results in applications that facilitate interaction between citizens and government institutions.

3.4.4 Real Estate

Globally, the retail industry has the biggest consumer base and the broadest market. Among the most appealing investment strategies is the one that involves shared rental properties. Existing fintech platforms such as "Rently" offer this possibility. They are constantly expanding to new territories (with eligible legislation) and new blockchain infrastructures.

By taking advantage of smart contracts, the process of yield distribution among shared property investors can be automated. The distribution can be sent to investors' crypto wallets in the form of stablecoins (like Tether-USD) that are proportional to their investment percentage. Another problem arises with shared properties. As is known, property maintenance comes with utility costs: electricity and gas bills, annual property taxes, etc. Blockchain projects such as *"The TransActive Grid"* measure and notify rental investors in real time about the energy consumption costs associated with their properties [53]. These initiatives may be further expanded to include automated billing for other shared property services through smart contracts in the future.

3.4.5 E-Healthcare

E-healthcare is a leading sector that may be mapped to blockchain networks [54], [55], [56]. Hospitals communicate with clinics, clinics pass information to doctors, and doctors share it with pharmacists, insurers, and, of course, with the patients themselves. This communication flow demonstrates the idea of distinct yet interconnected entities. These entities can be mapped onto consortium networks such as HyperLedger Fabric. Since the data exchange is both sensitive and essential for the operation of such businesses, they should invest in the extra layer of security that HyperLedger Fabric provides. Through HyperLedger's X.509 certificates, all involved nodes in the consortium network can be double- verified periodically to minimize the risk of fraudulent nodes entering the consortium [57].

The pharmaceutical supply chain faces its own variation of the same "trust" challenge. By using the above group of certificates, manufacturers and pharmaceutical distributors can be verified on- chain [58], [59]. This may also serve as a digital audit mechanism even for drug administration agencies such as the EMA or the FDA [60].

3.5 The Rise of the Global Regulatory Frameworks: Implications for Business Adoption

When a company begins experimenting with blockchain, the law is never far behind. It appears in conversations, in paperwork, and sometimes even before the code exists.

The first question most companies face when issuing digital assets sounds simple, but rarely is: *"Does this token count as a security ?"* In the United States, the Securities and Exchange Commission (SEC) still relies on the "Howey Test" for guidance. Many blockchain startups claim that their associated cryptocurrency is merely a payment medium for their services. From a different perspective, the SEC classifies those tokens as securities issued for capital raising. This conflict in principles has been evident in many disputes between blockchain projects and the SEC, the most famous being "Ripple vs. SEC." After five years, the court ruled that XRP is not a security [61].

When sold publicly through centralized crypto exchanges. This marked a noteworthy achievement for blockchain adoption in the U.S. Since the case concluded, multiple blockchain projects have applied for Exchange-Traded Funds (ETFs), with Ethereum-related applications being among the most successful in attracting investor interest.

Under the EU MiCA (Markets in Crypto-Assets) legislative umbrella, token classification is clearer and more modular. This regulation categorizes tokens into three groups: "asset-referenced tokens," "e-money tokens," and a residual category for everything that does not fit between them. For each category, a distinct license must be issued by ESMA before the token can be offered to the public. Auditing of these tokens is closely monitored by the European Banking Authority across all member states, ensuring that all jurisdictions remain aligned with regulatory expectations.

Similarly, Japan's Financial Services Agency (FSA) and Singapore's Monetary Authority (MAS) divide the regulatory pathway into two tracks: one applying to payment and utility tokens, and another applying to tokens used for investment purposes. The former must be fully backed, at least in a 1:1 ratio, with real- world assets such as bonds or fixed-term deposits, while tokens falling into the latter category are subject to dividend taxation, similar to traditional stock markets.

A second important theme in the context of legislation—especially after the "Terra scandal" in May 2022—is the regulation of stablecoins. A brief reminder: the algorithmic stablecoin that was supposed to be pegged 1:1 to the USD collapsed, causing a shocking loss of approximately $50 billion in total market value. This was followed by a cascade of negative events, including the fall of the FTX crypto exchange in the United States. The old postulate re-emerged: "*Not your keys, not your coins!*" Since then, regulatory bodies around the world have taken serious steps to win the battle against financial fraud: The lending of crypto-related assets is partly prohibited, and the use of cryptoassets as collateral is restricted.

Algorithmic stablecoins now represent only 0.2% of the total stablecoin market value [62]. Singapore's Monetary Authority (MAS) has tightened requirements for stablecoin issuers: they must hold full backup reserves in safe, low-risk assets to maintain public trust. These reserves are audited and reported to financial agencies every quarter. Japan's Financial Services Agency (FSA) follows an even stricter approach, recognizing only bank-issued stablecoins under its 2023 amendments to the Payment Services Act.

All jurisdictions are on the same page when it comes to implementing PSD2/AMLD6 "Anti-Money Laundering" (AML) and Know-Your-Client (KYC) procedures. The "travel rule" is enforced across all major regions: in EU countries, it applies even to self-hosted wallets above €1,000; in Singapore, it applies above 1,500 SGD. In the United States, "client diligence" is required for every blockchain transaction above $3,000 or for repeated transactions just below $3,000. Japan strictly prohibits privacy coins, as do France, Spain, and Italy through their local regulations implemented alongside MiCA.

4 Conclusions and Future Research Directions

4.1 How the Pieces Fit Together? A Circular Blockchain Adoption Framework

Now that we have examined the key points in the business implementation of blockchain technology, starting from the definition of needs and continuing through the legislative framework, we reach a final point of reflection. The full implementation flow functions, as illustrated in Figure 6, is more of a circular process rather than a straight line.

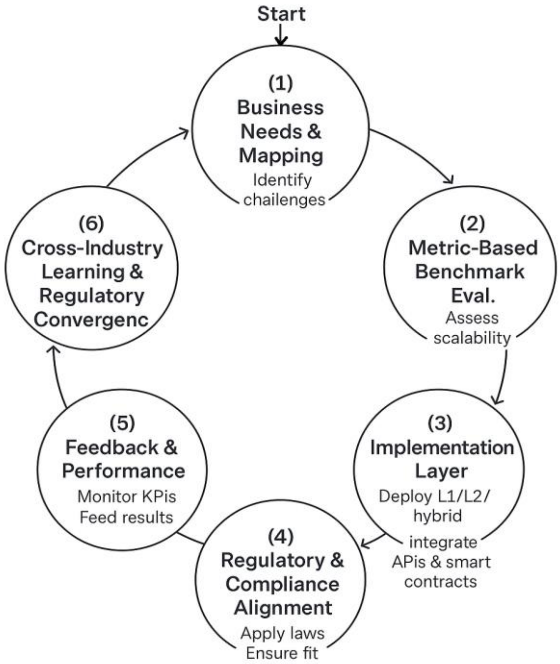

Fig. 6: A Circular Framework for Future Blockchain Implementations derived from our literature review. *Source: created by authors.*

The connections between these nodes become stronger with every successful implementation. The final connection between the first node, meaning businesses and regulatory bodies, is inherently symbiotic. Businesses contribute their practical experiences as invited stakeholders in legislative discussions. In this way, the circular implementation flow develops a feedback loop that allows it to learn and improve with each iteration.

4.2 Gaps in Implementation that Need to Be Addressed by Future Research

Many businesses still don't have the privilege to invest in implementing their workflows on Layer 1 solutions. It is costly in terms of development and requires training employees to use the upgraded service. Naturally, as attention shifts toward Layer 2 blockchain networks, so should the tested benchmarks and research. There is actually little evidence supporting the development of low-to medium-sized businesses on L2 blockchains. Even legislation remains somewhat in a grey area regarding what is allowed and what is not on L2 blockchains. More research could remove the dust and boost business interest in these reasonable alternatives.

Development and legislation do not move at the same pace. Development is mostly achieved in "circles," while legislation slowly chases it. Research related to blockchain implementation should be carried out not only by academics or business R&D teams. Governments should also have special units dedicated to crypto legislation and applications. A good starting point would be a public repository where all existing and new blockchains upload their whitepapers. The whitepaper itself should include tested benchmarks that can be easily reproduced by the general public. This would clear a lot of doubts among interested businesses.

Last but not least, studies should examine how financial initiatives impact business adoption of blockchain solutions. Strategies such as reduced taxes for businesses that implement blockchain workflows (which would naturally include an audit trail) may further increase interest and awareness of this new technology. Japan and Singapore are experimenting with digital startups of this form, but the idea is still in its infancy and yet to be proven by major industry players. By the end of this literature review, we would like to emphasize that as businesses grow in number and form, so will their needs. The demand for blockchain technology will grow over time, serving as motivation for both future research and development in this applied field.

References:

[1] Sunny, F. A., Hájek, P., Munk, M., Abedin, M. Z., Satu, S., Efat, M. I. A., Islam, M. J., A systematic review of blockchain applications, IEEE Access, Vol. 10, 2022, pp. 59155–59177. https://doi.org/10.1109/ACCESS.2022.3179690

[2] Xu, J., Wang, C., Jia, X., A survey of blockchain consensus protocols, ACM Computing Surveys, Vol. 55, 2023, Article 278. https://doi.org/10.1145/3579845

[3] Akanfe, O., Lawong, D., Rao, H. R., Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities, International Journal of Information Management, Vol. 76, 2024, Article 102753. https://doi.org/10.1016/j.ijinfomgt.2024.102753

[4] Aftan, S., Shah, H., A survey on BERT and its applications, Proceedings of the 20th Learning and Technology Conference (L&T), 2023, pp. 161–166. https://doi.org/10.1109/LT58159.2023.10092289

[5] Wang, L., Wang, Z., Wu, L., Liu, A.-A., Bots shield fake news: Adversarial attack on user engagement-based fake news detection, Proceedings of the ACM International Conference on Information and Knowledge Management (CIKM), 2024, pp. 2369–2378. https://doi.org/10.1145/3627673.3679583

[6] Thakre, N. K., Navaneetha, T., Bhasin, N. K., Samudrala, K., Rao, V. S., Karthik, M., Blockchain-enabled trust and transparency in influencer marketing on social media platforms, Proceedings of the Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), 2024, pp. 1–7. https://doi.org/10.1109/ICEEICT61591.2024.10718613

[7] Nirantar, K., Karmakar, R., Hiremath, P., Chaudhari, D., Blockchain-Based Supply Chain Management, Proceedings of the 3rd International Conference for Emerging Technology (INCET), 2022, pp. 1–8. https://doi.org/10.1109/INCET54531.2022.9824449

[8] Jafar, U., Aziz, M. J. A., Shukur, Z., Blockchain for Electronic Voting System - Review and Open Research Challenges, Sensors (Basel), Vol. 21, 2021, Article 5874. https://doi.org/10.3390/s21175874

[9] Shakir, H. S., Abdullah, A. A., A blockchain-based e-voting system for fast and secure digital elections, IEEE Access, 2024. https://doi.org/10.1109/IJCC64742.2024.10847284

[10] Salem, S. H. G., Hassan, A. Y., Moustafa, M. S., Blockchain-based biometric identity management, Cluster Computing, Vol. 27, 2024, pp. 3741–3752. https://doi.org/10.1007/s10586-023-04180-x.

[11] Careja, A.-C., Tapus, N., Digital Identity Using Blockchain Technology, Procedia Computer Science, Vol. 221, 2023, pp. 1074–1082. https://doi.org/10.1016/j.procs.2023.08.090

[12] Lodha, G., Pillai, M., Solanki, A., Sahasrabudhe, S., Jarali, A., Healthcare system using blockchain, Proceedings of the 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 274–281. https://doi.org/10.1109/ICICCS51141.2021.94

32157
[13] Yadav, P., Chandak, R., Transforming the Know Your Customer (KYC) Process using. Blockchain, Proceedings of the International Conference on Advanced Computing (ICAC), 2019, pp. 1–6. https://doi.org/10.1109/ICAC347590.2019.9036811
[14] Chen, S., Jiang, M., Luo, X., Exploring the security issues of real-world assets (RWA), Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2024. https://doi.org/10.1145/3689931.3694913
[15] Swinkels, L., Empirical evidence on the ownership and liquidity of real estate tokens, Financial Innovation, Vol. 9, 2023, Article 45. https://doi.org/10.1186/s40854-022-00427-5
[16] Li, X. H., Blockchain-based cross-border E-business Payment Model, Proceedings of the 2nd International Conference on E-Commerce and Internet Technology (ECIT), 2021, pp. 67–73. https://doi.org/10.1109/ECIT52743.2021.00022
[17] Li, G., Fan, Z.-P., Zhao, Q., Sun, M., Blockchain Technology Application in an E-Commerce Supply Chain: Privacy Protection and Sales Mode Selection, IEEE Transactions on Engineering Management, Vol. 71, 2024, pp. 8060–8074. https://doi.org/10.1109/TEM.2024.3386575
[18] Murad S. B., Kia Chiam, Y., Identification of selection criteria for blockchain platforms, Proceedings of the International Conference on Frontiers of Communications, Information System and Data Science (CISDS), 2022, pp. 8–13. https://doi.org/10.1109/CISDS57597.2022.00009
[19] Smetanin, S., Ometov, A., Komarov, M., Masek, P., Koucheryavy, Y., Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective, Sensors (Basel), Vol. 20, 2020, Article 3358. https://doi.org/10.3390/s20123358
[20] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., Liu, Y., A Survey on the Scalability of Blockchain Systems, IEEE Communications Surveys & Tutorials, Vol. 21, 2019, pp. 2799–2830. https://doi.org/10.1109/COMST.2019.2917082
[21] Guo, Y., Liang, C., Blockchain application and outlook in the banking industry, Financial Innovation, Vol. 2, 2016, Article 24. https://doi.org/10.1186/s40854-016-0034-9
[22] Hewa, T., Ylianttila, M., Liyanage, M., Survey on blockchain-based smart contracts: Applications, opportunities and challenges, Journal of Network and Computer Applications, Vol. 177, 2021, Article 102857. https://doi.org/10.1016/j.jnca.2020.102857
[23] Casino, F., Dasaklis, T. K., Patsakis, C., A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics, Vol. 36, 2019, pp. 55–81. https://doi.org/10.1016/j.tele.2018.11.006
[24] I. Bashir, Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 2nd ed., Packt Publishing, 2018. [Online]. Available: https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/Mastering_Blockchain_2nd_Edition.pdf. (Accessed Date: April 17, 2026).
[25] Nguyen, Q. K., Blockchain - A Financial Technology for Future Sustainable Development, Proceedings of the 3rd International Conference on Green Technology and Sustainable Development (GTSD), 2016, pp. 51–54. https://doi.org/10.1109/GTSD.2016.22
[26] D'Amato, F., Zanolini, L., Recent Latest Message Driven GHOST: Balancing Dynamic Availability With Asynchrony Resilience, arXiv preprint, 2023. https://doi.org/10.48550/arXiv.2302.11326
[27] Al-Jaroodi, J., Mohamed, N., Blockchain in industries: A Survey, IEEE Access, Vol. 7, 2019, pp. 36500–36515. https://doi.org/10.1109/ACCESS.2019. 2903554
[28] Park, S., Kwon, A., Fuchsbauer, G., Gaži, P., Alwen, J., Pietrzak, K., SpaceMint: A Cryptocurrency Based on Proofs of Space, Proceedings of Financial Cryptography and Data Security (FC), Lecture Notes in Computer Science, Vol. 10957, 2018, pp. 480–499. https://doi.org/10.1007/978-3-662-58387-6_26
[29] Atzei, N., Bartoletti, M., Cimoli, T., A Survey of Attacks on Ethereum Smart Contracts (SoK), Proceedings of Principles of Security and Trust (POST), Lecture Notes in Computer Science, Vol. 10204, 2017, pp. 164–186. https://doi.org/10.1007/978-3-662- 54455-6_8
[30] G. Wood, Polkadot: Vision for a Heterogeneous Multi-Chain Framework,

White paper, 2016. [Online]. Available: https://www.allcryptowhitepapers.com/wp-content/uploads/2019/08/PolkaDotPaper.pdf.
[31] Belchior, R., Vasconcelos, A., Guerreiro, S., Correia, M., A Survey on Blockchain Interoperability: Past, Present, and Future Trends, ACM Computing Surveys, Vol. 54, 2022, Article 168. https://doi.org/10.1145/3471140
[32] Li, W., Liu, Z., Chen, J., Liu, Z., He, Q., Towards blockchain interoperability: a comprehensive survey on cross-chain solutions, Blockchain: Research and Applications, Vol. 6, 2025, Article 100286. https://doi.org/10.1016/j.bcra.2025.100286
[33] Anthony Jnr, B., Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise -a standardized architecture perspective, Enterprise Information Systems, Vol. 18,2024. https://doi.org/10.1080/17517575.2023.2296647
[34] M. A. Saleh, S. Amanzholova, Z. Zhetekbay, M. Dauletbek, and A. A. Almisreb, Blockchain interoperability: challenges and solutions for a connected future, CEUR Workshop Proceedings, Vol. 3966, 2023. [Online]. Available: https://ceur-ws.org/Vol-3966/W4Paper3.pdf. (Accessed Date: November 14, 2025).
[35] Timmerer, C., Griwodz, C., Dynamic adaptive streaming over HTTP: From content creation to consumption, Proceedings of the 20th ACM International Conference on Multimedia, 2012, pp. 1533–1534. https://doi.org/10.1145/2393347.2396553
[36] Soumyajit Sarkar, A Comprehensive Analysis of Transaction Speeds, Costs, and Real-World Applications of Solana, Ethereum, and SUI, International Journal for Research in Applied Science and Engineering Technology (IJRASET), Vol. 13, Issue VIII, Aug. 2025, pp. 1103–1106. https://doi.org/10.22214/ijraset.2025.73717
[37] Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C., A Survey on Essential Components of a self-sovereign Identity, Computer Science Review, Vol. 30, 2018, pp. 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
[38] Y. Le, X. Chen, Z. Li, and H. Zhang, "Age-of-Information Analysis for Blockchain-Based Mobile Edge Computing," IEEE Transactions on Communications, vol. 73, no. 12, pp. 13953–13966, Dec. 2025. https://doi.org/10.1109/TCOMM.2025.3597823
[39] A. Preukschat and D. Reed, Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Manning Publications, 2021. [Online]. Available: https://www.manning.com/books/self-sovereign-identity (Accessed Date: November 20, 2025).
[40] Kamilaris, A., Fonts, A., Prenafeta-Boldú, F. X., The rise of blockchain technology in agriculture and food supply chains, Trends in Food Science & Technology, Vol. 91, 2019, pp. 640–652. https://doi.org/10.1016/j.tifs.2019.07.034
[41] Ghode, D. J., Yadav, V., Jain, R., Integrated Framework for Supply Chain with Blockchain Technology: a manufacturer's perspective, Journal of Innovation and Entrepreneurship, Vol. 14, 2025, Article 62. https://doi.org/10.1186/s13731-025-00553-1
[42] Zhao, M., Impact assessment of blockchain-based improved PBFT consensus mechanism for Supply Chain Efficiency and Security, IEEE Internet of Things Journal, 2025. https://doi.org/10.3233/IDT-240619
[43] Pournader, M., Shi, Y., Seuring, S., Koh, S. C. L., Blockchain applications in supply chains, transport and logistics: a systematic review of the literature, International Journal of Production Research, Vol. 58, 2020, pp. 2063–2081. https://doi.org/10.1080/00207543.2019.1650976
[44] Hayashi, T., Ishimura, G., Ohsawa, Y., Structural Characteristics of Stakeholder Relationships and Value Chain Network in Data Exchange Ecosystem, IEEE Access, Vol. 9, 2021, pp. 52266–52276. https://doi.org/10.1109/ACCESS.2021.3070017
[45] Varriale, V., Cammarano, A., Michelino, F., Caputo, M., Sustainable Supply Chains with Blockchain, IoT and RFID: A Simulation on Order Management, Sustainability (Basel), Vol. 13, 2021, Article 6372. https://doi.org/10.3390/su13116372
[46] Yakubu, M. M., Hassan, M. F. B., Danyaro, K. U., Yakubu, B. M., Alabdulatif, A. A., Beevi, S. Z., Garba, A., HalalChain: A decentralized blockchain model for enhanced data integrity, real-time compliance, and automated verification in halal food supply chain, Results in Engineering, Vol. 27, 2025, Article 106591. https://doi.org/10.1016/j.rineng.2025.106591
[47] Ali, M. H., Chung, L., Kumar, A., Zailani, S.,

Tan, K. H., A sustainable Blockchain framework for the halal food supply chain: Lessons from Malaysia, Technological Forecasting and Social Change, Vol. 170, 2021, Article 120870. https://doi.org/10.1016/j.techfore.2021.120870

[48] Rejeb, A., Keogh, J. G., Treiblmaier, H., Leveraging the Internet of Things and blockchain technology in supply chain management, Future Internet, Vol. 11, 2019, Article 161. https://doi.org/10.3390/fi11070161

[49] Idrissi, Z. K., Lachgar, M., Hrimech, H., Blockchain, IoT and AI in logistics and transportation: A systematic review, Transportation Engineering, 2024. https://doi.org/10.1016/j.team.2024.09.002

[50] Kumar, S., Raut, R. D., Agrawal, N., Cheikhrouhou, N., Sharma, M., Daim, T., Integrated blockchain and internet of things in the food supply chain: Adoption barriers, Technovation, Vol. 118, 2022, Article 102589.https://doi.org/10.1016/j.technovation.2022.102589

[51] Lai, J., Wang, T., Zhang, S., Yang, Q., Liew, S. C., BioZero: An Efficient and Privacy-Preserving Decentralized Biometric Authentication Protocol on Open Blockchain, arXiv preprint, 2024. https://doi.org/10.48550/arXiv.2409.17509

[52] Aruna, S., Maheswari, M., Saranya, A., Highly Secured Blockchain-Based Electronic Voting System Using SHA3 and Merkle Root, IOP Conference Series: Materials Science and Engineering, Vol. 993, 2020, Article 012103. https://doi.org/10.1088/1757-899X/993/1/012103

[53] Natural Resources Canada, The Transactive Grid – Enabling an End-To-End Market Services Framework Using Blockchain 2019. [Online]. Available: https://natural-resources.canada.ca/funding-partnerships/transactive-grid-enabling-end-end-market-services-framework-blockchain. (Accessed Date: November 23, 2025).

[54] Bazel, M. A., Mohammed, F., Ahmad, M., Blockchain technology adoption in healthcare: an integrated model, Scientific Reports, Vol. 15, 2025, Article 14111. https://doi.org/10.1038/s41598-025-95253-x

[55] Chen, J., Ueyama, J., Blockchain and IoT-Based Health Monitoring System Design and Implementation, Proceedings of the ACM Conference on Computing and Sustainable Societies, 2025. https://doi.org/10.1145/3779153.3779175

[56] A. Koulianos, P. Paraskevopoulos, A. Litke, and N. Papadakis, “Towards Enhanced Data Integrity and Accountability: Leveraging Blockchain Technology in Healthcare,” in Proceedings of the 17th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA ’24), ACM, New York, NY, USA, 2024, pp. 587–592. https://doi.org/10.1145/3652037.3663889

[57] Hyperledger Fabric Documentation, “Identity and Membership Service Provider (MSP),” 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/identity/identity.html (Accessed Date: November 24, 2025).

[58] Akram, W., Joshi, R., Haider, T., Sharma, P., Jain, V., Garud, N., Singh, N., Blockchain technology: A potential tool for the management of pharma supply chain, Research in Social and Administrative Pharmacy, Vol. 20, 2024, pp. 156–164. https://doi.org/10.1016/j.sapharm.2024.02.014

[59] Tseng, J. H., Liao, Y. C., Chong, B., Liao, S. W., Governance on the Drug Supply Chain via Gcoin Blockchain, International Journal of Environmental Research and Public Health, Vol. 15, 2018, Article 1055. https://doi.org/10.3390/ijerph15061055

[60] U.S. Food and Drug Administration (FDA), “Drug Supply Chain Security Act (DSCSA) Pilot Project Program,” 2023. [Online]. Available: https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program (Accessed Date: December 1, 2025).

[61] Investopedia, “SEC v. Ripple: Key Court Decision and Impact on Cryptocurrency Regulation,” 2025. [Online]. Available: https://www.investopedia.com/sec-vs-ripple-6743752 (Accessed Date: April 17, 2026).

[62] Brookings Institution, “What are stablecoins, and how are they regulated?”, 2025. [Online]. Available: https://www.brookings.edu/articles/what-are-stablecoins-and-how-are-they-regulated/ (Accessed Date: April 17, 2026).

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)
The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself
No funding was received for conducting this study.

Conflict of Interest
The authors have no conflicts of interest to declare that are relevant to the content of this article.

I. Observed Blockchain Performance Benchmarks:

PB1. CoinMetrics, "Ethereum post-Merge network metrics report 2024," 2024. [Online]. Available: https://coinmetrics.io/charts. *(Accessed Date: April 2, 2026).*

PB2. European Blockchain Observatory and Forum, "Post-Merge Ethereum energy consumption update 2024," European Commission, Brussels, 2024. [Online]. Available: https://blockchain-observatory.ec.europa.eu/index_en *(Accessed Date: April 3, 2026).*

PB3. Polygon Technology, "Polygon Proof-of-Stake and zkEVM overview," 2024. [Online]. Available: https://polygon.technology. *(Accessed Date: April 3, 2026).*

PB4. Messari, "State of Polygon: Key metrics and insights," 2024. [Online]. Available: https://messari.io/research. *(Accessed Date: April 3, 2026).*

PB5. Solana Foundation, "Solana Network Performance and Energy Usage Report 2025," Geneva, March 2025. [Online]. Available: https://solana.com/news. *(Accessed Date: April 4, 2026).*

PB6. CoinDesk Research, "Solana throughput and latency benchmark analysis 2024," New York, NY, 2024. [Online]. Available: https://www.coindesk.com/research *(Accessed Date: April 4, 2026).*

PB7. Web3 Foundation, "Polkadot relay chain performance assessment 2024," Zurich, 2024. [Online]. Available: https://web3.foundation/research/ *(Accessed Date: April 4, 2026).*

PB8. Messari, "Polkadot network metrics update Q3 2024," 2024. [Online]. Available: https://messari.io/article/state-of-polkadot *(Accessed Date: April 4, 2026).*

PB9. P. Thakkar, S. Nathan, and B. Vishwanathan, "Performance benchmarking and optimizing Hyperledger Fabric blockchain platform," 2018. https://doi.org/10.48550/arXiv.1805.11390 *(Accessed Date: April 5, 2026).*

PB10. H. Sukhwani, B. Wester, A. Singhal, C. Murthy, and O. Rana, "Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)", *2018 IEEE International Symposium on Network Computing and Applications (NCA)*, 2018. https://doi.org/10.1109/NCA.2018.8548070 *(Accessed Date: April 5, 2026).*

PB11. Tezos Foundation, "Tezos on-chain governance and performance report 2024," Lausanne, 2024. [Online]. Available: https://tezos.foundation/reports *(Accessed Date: April 4, 2026).*

PB12. Messari, "State of Tezos Q4 2024," 2024. [Online].Available:https://messari.io/report-pdf/199cdbd1fc76bf5162d862008b3fa1170f8df1e8.pdf *(Accessed Date: April 6, 2026).*

II. Legislative Documents:

European Union :

- European Parliament and Council, "Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA)," 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng . *(Accessed Date: April 7, 2026).*
- European Parliament and Council, "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD5)," 2018. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng. *(Accessed Date: April 7, 2026).*

United States:

- Financial Crimes Enforcement Network (FinCEN), "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (FIN-2013-G001)," March 18, 2013. [Online]. Available: https://www.fincen.gov/system/files/shared/FIN-2013-G001.pdf *(Accessed Date: April 7, 2026).*
- U.S. Food and Drug Administration, Drug Supply Chain Security Act (DSCSA), 2025. [Online]. Available: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa. *(Accessed Date: April, 8, 2026).*

Japan :

- Financial Services Agency (FSA), Payment Services Act (Act No. 59 of 2009, as amended by Act No. 32 of 2020), 2020. [Online]. Available: https://www.japaneselawtranslation.go.jp/en/laws/view/3078/en *(Accessed Date: April, 9, 2026).*

Singapore :

- Monetary Authority of Singapore (MAS), Project Guardian: Exploring Decentralised Finance and Asset Tokenisation, 2023. [Online].Available: https://www.mas.gov.sg/ *(Accessed Date: April, 9, 2026).*

APPENDIX

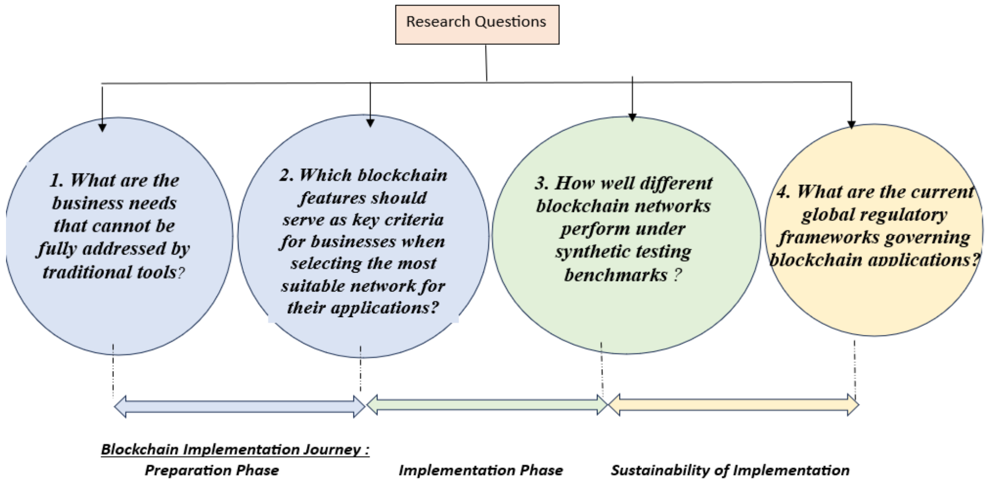

Fig.1: Overview of research questions that capture the full blockchain implementation journey.
Source: created by authors.

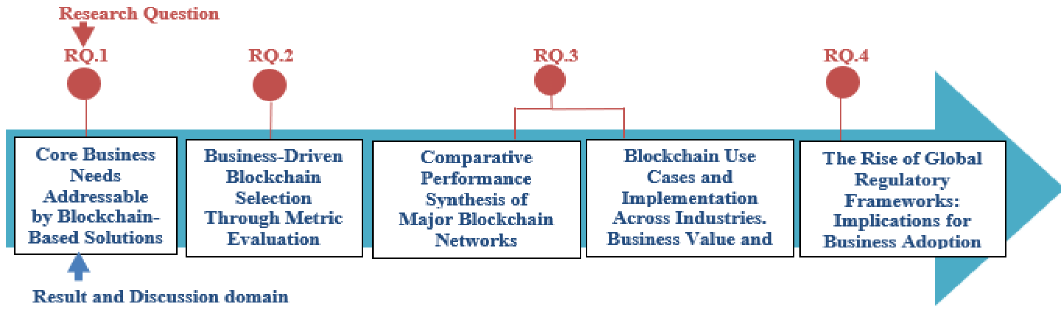

Fig. 2: Navigation pathway of the literature review through the research questions and their related domains.
Source: created by authors.

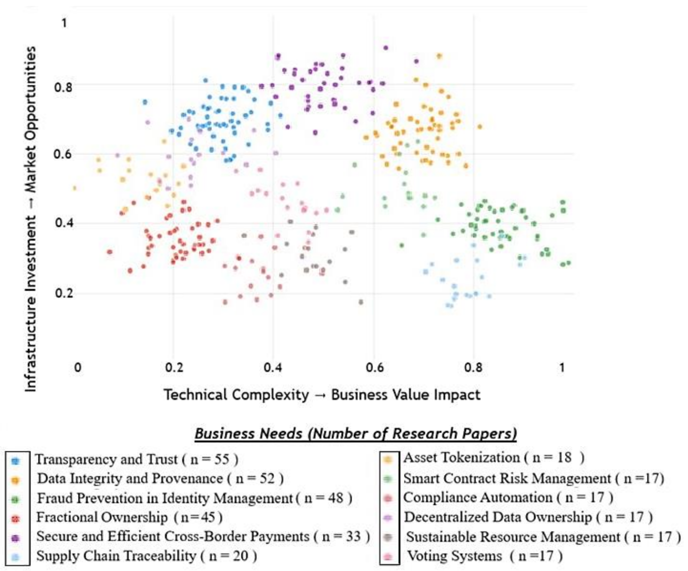

Fig.3 : Thematic clustering of research papers metadata to identify key business needs using BERT model.
Source : created by the authors using research paper metadata mapping via a self-supervised BERT classification algorithm in Replit IDE.

Table 2. Blockchain performance benchmarks.

Network / Layer	Observed Throughput (TPS) & Finality	Avg Fee (USD) / transaction	Key Advantages	Observed Challenges	Benchmark Refs
Ethereum (L1 PoS)	13 – 16 TPS · Finality ≈ 12 min	≈ 0 .38	Mature ecosystem; robust security; wide DeFi integration	High gas fees during congestion; limited scalability on L1	PB1, PB2
Polygon (PoS / zkEVM L2)	≈ 70 TPS · Finality < 10 s	≈ 0 .005	Low fees; fast confirmations; broad EVM compatibility	Bridging security risks; periodic validator centralization	PB3, PB4
Solana (L1)	3 000 – 5 000 TPS · Finality ≈ 0 . 4 – 12 s	< 0.01	High throughput; sub-second latency; efficient PoH design	Validator hardware demand; network instability under load	PB5, PB6
Polkadot (Relay + Parachains)	≥ 1 000 TPS (practical) · Finality ≈ 16 s	≈ 0 . 02	High interoperability; scalable via parachains; energy-efficient NPoS	Complex architecture; governance coordination across chains	PB7, PB8
Hyperledger Fabric (Permissioned)	500 – 3 000 TPS · Finality < 2 s	No token fees	Deterministic finality; enterprise grade privacy controls	Setup complexity; limited public interoperability	PB9, PB10
Tezos (LPoS)	200 – 400 TPS · Finality ≈ 1–2 min	≈ 0 . 01	Formal verification; self-amending governance; energy efficient	Lower TPS than newer L2 chains; slower adoption curve	PB11, PB12

Source: Benchmark metrics, summarized and compared by the authors.