Blockchain-Enabled Communication Infrastructures: A Review of Trust, Security, and Resource Orchestration in IoT, Edge, Vehicular, and 6G Networks

Marta Kovacevic[1], Luka Petrovic[2, *]
[1] Faculty of Organization and Informatics, University of Zagreb, Varazdin, Croatia, 42000
[2] Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor, Slovenia, 2000
[*]Email: luka.petrovic.review@proton.me (Corresponding Author)

Abstract

Blockchain has moved from a cryptocurrency infrastructure to a coordination technology for modern communication systems. This review examines how blockchain is being embedded into next-generation communication environments, with particular attention to Internet of Things deployments, edge-cloud collaboration, cyber-physical infrastructures, security and privacy management, smart grids, vehicular networking, and emerging 5G/6G ecosystems. Following the logic of recent survey work on blockchain-enabled communications, the article synthesizes representative peer-reviewed studies, clarifies the blockchain mechanisms that matter for communication engineering, and organizes the literature around application layers rather than isolated protocols. The review shows that blockchain creates value when communication systems require shared trust, auditable automation, decentralized identity, incentive-compatible coordination, or tamper-resistant data exchange across organizational boundaries. At the same time, real deployment remains constrained by throughput, latency, storage overhead, interoperability, privacy leakage, governance complexity, and uneven energy efficiency across consensus designs. Building on both communication-network research and information-systems scholarship, the article develops an integrated analytical view of when blockchain genuinely improves communication architectures and when lighter coordination mechanisms are preferable. The paper concludes by identifying future directions around lightweight consensus, AI-native blockchain orchestration, cross-chain communication fabrics, privacy-preserving verification, and programmable trust for 6G and autonomous infrastructures.

Keywords: blockchain; communication networks; Internet of Things; edge computing; 6G; trust management

Article History
Received March 10, 2026
Revised March 20, 2026
Accepted March 25, 2026
Available Online March 28, 2026

Blockchain-Enabled Communication Infrastructures: A Review of Trust, Security, and Resource Orchestration in IoT, Edge, Vehicular, and 6G Networks

1. Introduction

Blockchain is no longer interpreted only as the ledger behind cryptocurrency. In communication systems, it is increasingly treated as a programmable trust layer that can coordinate devices, users, service providers, and regulators that do not fully trust one another. That shift matters because next-generation communication networks are no longer narrowly concerned with moving packets from source to destination. They now mediate identity, data provenance, spectrum sharing, edge-cloud computation, service monetization, machine autonomy, and cross-organizational auditability. The resulting networked environment is rich in data but poor in shared trust, especially when large numbers of heterogeneous devices produce transactions that influence billing, routing, safety, security, or service-level agreements. In precisely this type of environment, blockchain becomes interesting not because every problem needs a chain, but because some communication problems are fundamentally coordination problems with adversarial incentives (Haber & Stornetta, 1991; Tschorsch & Scheuermann, 2016; Christidis & Devetsikiotis, 2016; Lu, 2018a; Lu, 2019).

The communications field has been transformed by the expansion of the Internet of Things, industrial cyber-physical systems, connected vehicles, UAV swarms, mobile edge computing, and early 6G visions. Each of these environments combines high device density with decentralized data generation and a demand for reliable automation. Traditional centralized architectures remain efficient in many settings, yet they also create bottlenecks, single points of failure, opaque access-control regimes, and dependence on trusted intermediaries. Those limitations have motivated studies on blockchain-enabled device registration, access control, distributed logging, peer-to-peer energy coordination, secure vehicular communications, and auditable edge services. Representative literature shows that the blockchain question in communication systems is less about replacing networking fundamentals and more about embedding trust, verifiability, and incentive logic into them (Xu et al., 2014; Wortmann & Fluchter, 2015; Conoscenti et al., 2016; Panarello et al., 2018; Ferrag et al., 2019; Xu et al., 2021).

At the same time, the enthusiasm surrounding blockchain has often outpaced architectural discipline. Communication researchers sometimes describe blockchain as a universal security primitive, while information-systems scholars warn that governance cost, interoperability limits, and organizational misfit can outweigh the gains from decentralization. Surveys in blockchain, IoT, and Industry 4.0 confirm the breadth of the opportunity, but they also show persistent confusion between problems that require immutable, multi-party coordination and those that can be solved more efficiently with conventional databases, signed logs, or platform governance. That tension is especially

ISSN-3067-7505 https://doi.org/10.63646/jtis.2025.030301

visible in communications, where latency, throughput, bandwidth efficiency, and energy consumption are first-order design criteria rather than afterthoughts (Casino et al., 2019; Wang et al., 2018; Lu, 2022; Zheng & Lu, 2022; Chen et al., 2024; Ali et al., 2021).

The objective of this article (Table 1) is therefore to review blockchain in communication systems through a logic like that of recent survey articles, but with a stronger integration of communication engineering, edge intelligence, and information-systems reasoning. Instead of listing blockchain use cases in isolation, the paper asks four connected questions. First, which blockchain mechanisms are actually relevant to communication-system design? Second, in which communication domains has blockchain produced credible architectural value? Third, what performance and governance trade-offs recur across these domains? Fourth, what research directions are likely to matter as IoT, edge AI, vehicular networking, and 6G infrastructures become more autonomous? By answering these questions, the review aims to move the discussion from hype-driven application catalogues toward a more discriminating analytical framework (Pilkington, 2016; Yli-Huumo et al., 2016; Reyna et al., 2018; Lu, 2018b).

Table 1. Main Information for the Present Review

Description	Results
Timespan emphasized	2016-2025, with foundational pre-2016 concepts only where necessary
Primary focus	Blockchain applications in communication systems and adjacent digital infrastructures
Document profile	Predominantly peer-reviewed journal articles, with selected conference papers
Representative themes	IoT, edge and cloud coordination, security, smart grids, vehicular networking, 5G/6G
Number of references in this paper	69
Review orientation	Narrative synthesis with structured thematic analysis rather than bibliometric exhaustiveness

The rest of the paper is organized as follows (Figure 1). Section 2 discusses related surveys and explains the selection logic used in this review. Section 3 revisits blockchain structure, operational logic, smart contracts, blockchain types, and consensus mechanisms from the standpoint of communication architectures. Section 4 synthesizes blockchain applications across IoT, edge-cloud systems, cyber-physical infrastructures, security and privacy management, AI-assisted networking, network optimization, smart grids, vehicular systems, and 5G/6G environments. Section 5 summarizes the distribution and impact of the reviewed studies. Section 6 discusses recurring challenges. Section 7 outlines future research directions, and Section 8 concludes.

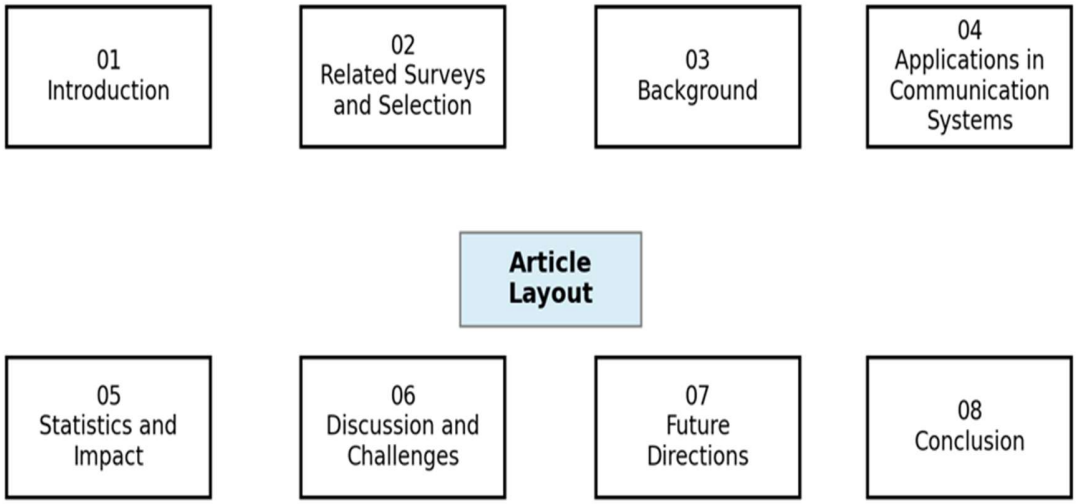

Figure 1. Article Layout

2. Related Surveys and Selection Process

2.1 Related surveys

The literature on blockchain has grown quickly across information systems, industrial engineering, finance, energy, and communication studies. Foundational reviews mapped the conceptual territory by explaining distributed ledgers, consensus, cryptocurrency infrastructures, smart contracts, and early application scenarios. These works were important because they established the vocabulary through which later communication research interpreted decentralization, immutability, and programmable trust. They also revealed a key pattern that remains relevant today: blockchain research often begins from technological novelty but becomes truly useful only when connected to coordination problems involving multiple stakeholders, asymmetric information, or distributed record-keeping (Tschorsch & Scheuermann, 2016; Yli-Huumo et al., 2016; Pilkington, 2016; Lu, 2018a; Lu, 2018b; Yuan & Wang, 2018).

A second stream of surveys focused on blockchain and the Internet of Things. This line of work demonstrated why IoT became one of the earliest non-financial domains to embrace blockchain ideas. Device heterogeneity, weak built-in trust, distributed ownership, and long service chains made IoT a natural setting for immutable logs, decentralized identity, secure update trails, and policy automation. Surveys by Conoscenti et al., Panarello et al., Christidis and Devetsikiotis, Khan and Salah, Reyna et al., and Xu et al. systematically showed that blockchain can improve provenance and accountability in IoT settings, but they also emphasized resource scarcity, throughput constraints, and the cost of running heavyweight validation on constrained devices (Conoscenti et al., 2016; Christidis & Devetsikiotis, 2016; Khan & Salah, 2018; Panarello et al., 2018; Reyna et al., 2018; Xu et al., 2021).

A third stream moved beyond generic IoT and examined blockchain in broader industrial and enterprise architectures. Here, the dominant concern was not merely secure messaging but the integration of blockchain with organizational systems, industrial automation, supply networks, and digital transformation. This body of work is valuable to communication researchers because many communication systems are not standalone technical artifacts; they are embedded within industrial operations, business processes, and regulated service ecosystems. Information-systems scholarship has been especially helpful in identifying when blockchain fits multi-party coordination and when it introduces more governance burden than value (Viriyasitavat et al., 2019; Lu, 2022; Zheng & Lu, 2022; Chen et al., 2024; Alladi et al., 2019).

A fourth stream addressed specific communication environments such as smart grids, vehicular systems, edge-cloud architectures, and 5G/6G infrastructures. These domain-specific studies are often more technically grounded than general blockchain reviews because they treat latency, mobility, spectrum scarcity, reliability, and real-time service constraints as design variables. Reviews of energy-sector blockchain, secure vehicular communications, intelligent transportation, and 6G-envisioned blockchain architectures suggest that the field is converging around a smaller set of credible use cases: decentralized identity, transaction logging, resource reservation, secure data sharing, market coordination, and collaborative model governance. However, many studies remain proof-of-concept exercises or architecture proposals rather than fully validated deployments (Aitzhan & Svetinovic, 2016; Andoni et al., 2019; Mollah et al., 2020; Rahmadika et al., 2021; Aggarwal et al., 2021; Nguyen et al., 2021).

Taken together, the existing surveys provide a rich base but still leave an important gap. Few reviews place blockchain squarely inside the logic of communication-system design while also integrating insights from information systems, edge computing, cyber-physical infrastructures, and AI-assisted network management. Some studies are too broad and treat communication only as one application among many. Others are technically detailed but narrow, focusing on a single domain such as smart grids or vehicular systems. The present review addresses this gap by organizing the field around communication functions and coordination requirements rather than around isolated industrial cases.

2.2 Selection strategy and review scope

This review follows a structured but non-bibliometric selection logic. The intention is not to claim exhaustive database coverage but to develop an analytically coherent synthesis of representative, peer-reviewed work. Literature was prioritized from major venues that frequently publish blockchain or communication-system studies, including IEEE journals and conferences, Elsevier journals, Springer journals, and selected interdisciplinary outlets in information systems, industrial informatics, and digital infrastructure. The review emphasizes work published from 2016 to 2025 because that period captures the transition from foundational blockchain conceptualization to communication-specific

implementations, while earlier work is cited only where it establishes basic blockchain principles or adjacent networking concepts (Haber & Stornetta, 1991; Xu et al., 2014; Gervais et al., 2016; Zheng et al., 2017).

The inclusion logic used four criteria. First, a study had to contribute directly to blockchain-enabled communication, communication-adjacent infrastructure, or a communication-intensive cyber-physical context. Second, the paper had to make a substantive analytical contribution rather than merely mention blockchain as a peripheral technology. Third, both reviews and empirical or architectural studies were retained, because communication-system blockchain research is still maturing and many influential contributions take the form of conceptual architectures, protocols, or system designs. Fourth, work that clarified interaction with IoT, edge computing, AI, transportation systems, smart grids, or identity and access control was treated as relevant because these are the main routes through which blockchain enters communication practice (Abbas et al., 2018; Yu et al., 2018; Roman et al., 2018; Salah et al., 2019; Dinh et al., 2018).

The scope of the review is intentionally thematic (Table 2). It includes blockchain for IoT and device communication, blockchain with cloud, fog, and edge computing, blockchain in cyber-physical systems, security and privacy applications, AI-assisted blockchain uses in communication systems, network and computing optimization, smart grids and energy communication, vehicular and transportation communication networks, and blockchain-oriented 5G/6G research. It excludes purely financial cryptocurrency studies unless they provide foundational insights into consensus, incentives, or distributed trust that have been reused in communication-system designs. This thematic scope makes it possible to mimic the logic of communication-centered survey papers while also retaining stronger conceptual discrimination about where blockchain meaningfully fits.

Table 2. Selected Survey Clusters and Their Analytical Value for the Present Review

Cluster	Representative focus	Contribution to this review	Main limitation
Foundational blockchain surveys	Consensus, ledger architecture, smart contracts	Provide conceptual baseline for later communication applications	Often not communication-specific
IoT and IIoT surveys	Identity, provenance, access control, device trust	Explain why constrained devices motivate lightweight blockchain design	Can understate latency and deployment trade-offs
Industry 4.0 and enterprise IS	Cross-organizational coordination and system integration	Clarify organizational and governance fit	Sometimes treat networking only indirectly

Smart grid and transportation surveys	Resource trading, mobility, infrastructure trust	Show domain-specific architectural opportunities	Many studies remain pilot or conceptual
5G/6G and edge-intelligence literature	Programmable services, slicing, AI-native orchestration	Connect blockchain to future communication fabrics	Empirical validation is still limited

3. Background

3.1 Blockchain structure

At the architectural level, blockchain is a distributed ledger maintained by multiple nodes that agree on transaction validity and ledger evolution through some form of consensus. A block typically contains metadata, a cryptographic link to the previous block, a collection of transactions, and in some platforms a representation of smart-contract state. This chaining structure gives blockchain two features that matter for communication systems. First, it supports tamper-evident storage of events such as device registration, access requests, handoff records, charging events, or service-level updates. Second, it reduces dependence on a single central logging entity, which is useful where participants come from different administrative domains and no universally trusted operator exists (Haber & Stornetta, 1991; Tschorsch & Scheuermann, 2016; Zheng et al., 2017; Wang et al., 2018).

In communication systems, the importance of blockchain structure does not lie in the block format itself but in what the format makes possible. Because each record is linked to prior states and validated by more than one party, the ledger becomes suitable for accountability-intensive communication contexts (Figure 2). Examples include machine-to-machine billing, edge-resource reservation, data provenance across sensor pipelines, delegated access to infrastructure, or cross-operator settlement in mobile environments. At the same time, block-based ledger growth introduces storage overhead and state-replication cost, which means that communication-system designers often have to separate high-rate data traffic from lower-rate blockchain event records. This design distinction between data plane and trust plane is central to successful blockchain deployment in networking environments (Dinh et al., 2018; Viriyasitavat et al., 2019; Xu et al., 2019).

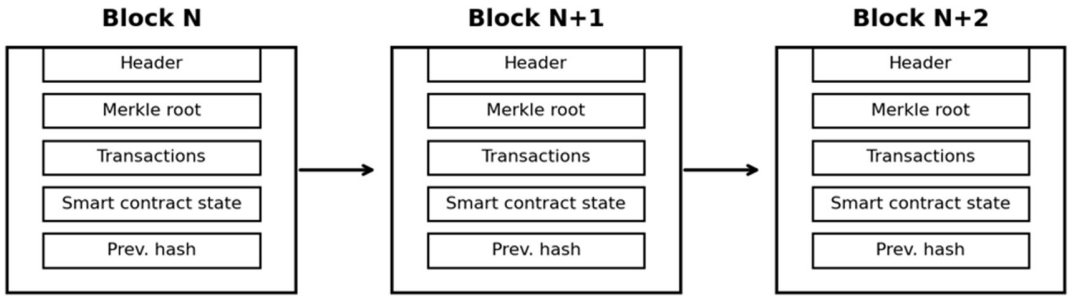

Figure 2. Simplified Operational Mechanism of Blockchain Technology

3.2 Nature of operations

A blockchain transaction is best understood as a state-change proposal rather than simply a message. In a communication architecture, a device or service submits a signed event that requests recognition by the shared ledger: for example, a gateway may register that a sensor produced a verified reading, a vehicle may reserve communication and computing resources for a road segment, or an energy node may publish a demand-response commitment. Once the transaction is validated and included, all relevant participants can treat the event as having a commonly observable status. This common observability is what turns blockchain from a storage mechanism into a coordination mechanism (Aitzhan & Svetinovic, 2016; Tian, 2016; Li et al., 2019).

Operationally, however, communication systems rarely place all raw traffic on chain. Doing so would impose unacceptable delay, throughput loss, and storage burden. Instead, most workable designs adopt a layered model: raw sensor data, streaming traffic, video, or large model parameters stay off chain, while hashes, permissions, settlement events, model updates, audit records, or policy triggers are written on chain. This hybrid pattern appears repeatedly across IoT, edge computing, healthcare communication, and industrial networking. The ledger stores what needs to be trusted and audited; high-volume payloads stay in cloud, edge, or distributed file systems. The recurring architectural lesson is that blockchain works best in communication systems when it verifies the meaning of interactions, not the entirety of their data payloads (Nguyen et al., 2020a; Guo et al., 2019; Tanwar et al., 2020).

3.3 Smart contracts

Smart contracts introduce programmable logic into blockchain operations. In communication systems, they are attractive because they can automate access control, tokenized incentives, resource allocation, billing, and compliance checking without relying on manual intervention from a central operator. Early work on smart-contract vulnerabilities already showed that code execution on chain requires careful formal reasoning, because immutability makes flawed logic difficult and expensive to repair. Yet the promise remains significant: communication infrastructures increasingly require machine-speed execution of rules across organizational boundaries, and smart contracts offer a shared execution environment for these rules (Luu et al., 2016; Christidis & Devetsikiotis, 2016).

In practice, communication-oriented smart contracts often do three kinds of work. The first is authorization, such as deciding whether a device, application, or edge service has the right to access some resource. The second is settlement, such as distributing payments or credits when a service is consumed. The third is coordination, such as reserving spectrum, compute, or mobility support within a shared infrastructure. These uses are common in intelligent transportation, smart energy markets, secure device management, and machine-to-machine service ecosystems. However, the more sophisticated the contract logic

becomes, the more important it is to address execution cost, privacy exposure, oracle trust, and the risk that contractual rigidity may conflict with dynamic network conditions (Huh et al., 2017; Park et al., 2020; Singh & Kim, 2018; Sikorski et al., 2017).

3.4 Types of blockchain

Communication-system studies typically distinguish among public, private, consortium, and hybrid blockchains. Public chains maximize openness and censorship resistance but often perform poorly under strict latency and throughput requirements. They are attractive when open participation, public auditability, or broad token-based incentives are essential, but most communication infrastructures cannot tolerate their performance cost. Private chains are controlled by a single organization and provide efficient access control, yet they reduce decentralization and may replicate what a conventional distributed database could already do. Consortium chains occupy an important middle ground for communication environments shared by multiple operators, manufacturers, service providers, or regulators. Hybrid models combine on-chain transparency with off-chain confidentiality and selective disclosure (Pilkington, 2016; Wang et al., 2018; Ali et al., 2021).

For communication systems, the blockchain-type decision is fundamentally a governance decision (Table 3). A smart city platform, an industrial edge ecosystem, or a multi-stakeholder mobility network often needs more than one party to validate events, but not unrestricted global participation. In such cases, consortium or hybrid models are often superior because they align better with regulated services, contractual partnerships, and quality-of-service obligations. The strongest designs therefore begin by specifying who must trust whom, who is allowed to validate, what data can be public, and how disputes are resolved. Only after those questions are answered does the blockchain type become clear.

Table 3. General Comparison of Blockchain Types in Communication-System Settings

Type	Strengths	Communication-system fit	Main weakness
Public	High transparency and open participation	Open marketplaces and global token ecosystems	Latency, scalability, energy cost, privacy
Private	Fast processing and strong administrative control	Enterprise or campus infrastructures with one authority	Limited decentralization and audit neutrality
Consortium	Balanced governance across multiple operators	Industrial IoT, inter-organizational service platforms, regulated sectors	Requires governance agreements and validator coordination

Hybrid	Selective transparency plus protected data domains	Smart city, healthcare, transportation, and sensitive edge services	Architectural complexity and interoperability cost

3.5 Consensus mechanisms

Consensus determines how blockchain participants agree on ledger state. In communication systems, consensus is not an abstract cryptographic detail; it directly shapes confirmation delay, energy use, node participation cost, and fault tolerance. Proof-of-Work is historically important but rarely appropriate for communication infrastructures because its energy burden and probabilistic finality are difficult to reconcile with real-time service requirements. Proof-of-Stake and BFT-family mechanisms offer more attractive performance profiles, especially in permissioned or consortium settings. Surveys on consensus consistently show that communication-system blockchain design is inseparable from the choice of validator model and failure assumptions (Tschorsch & Scheuermann, 2016; Nguyen & Kim, 2018; Zhou et al., 2020).

This is why many blockchain-enabled communication proposals rely on practical Byzantine fault tolerance, delegated validation, committee-based consensus, or sharded arrangements rather than on open mining (Table 4). When mobility, edge cooperation, or machine-to-machine control is involved, immediate or near-immediate transaction finality is often more valuable than maximal openness. Consensus must therefore be chosen according to service context: industrial coordination and infrastructure governance typically value deterministic finality and controlled membership, whereas open token ecosystems may tolerate slower and probabilistic settlement. The broader lesson is that communication-system blockchain research succeeds when consensus is treated as a systems-engineering parameter, not as a symbolic commitment to decentralization.

Table 4. Consensus Considerations for Communication Systems

Mechanism family	Typical properties	Where it fits	Why it matters
Proof-of-Work	Probabilistic finality, high energy cost	Rarely suitable for operational communication infrastructure	Security through expensive computation but weak efficiency
Proof-of-Stake	Lower energy demand, validator incentives	Tokenized service platforms and some open ecosystems	Better scalability-energy balance than PoW
BFT and variants	Fast finality, permissioned participation	Industrial IoT, smart grid, inter-operator coordination	Useful where validator set is known and regulated

Hybrid/sharded approaches	Performance tuning through hierarchy or partitioning	Large-scale edge or 6G-oriented architectures	Attempts to reconcile scale with trust guarantees

4. Blockchain in Communication Systems

4.1 Blockchain for IoT and device communication systems

IoT is the most persistent application context for blockchain in communications because it combines distributed device ownership with weak native trust. Sensors, gateways, actuators, and embedded devices often operate across multiple vendors and administrative domains, which makes secure registration, device authentication, firmware provenance, and tamper-evident logging difficult to manage through a single central system. Blockchain-based approaches respond by introducing distributed identity, shared event history, and programmable access policies. Early IoT literature framed blockchain as a way to replace centralized trust anchors in smart homes, industrial environments, and machine-to-machine ecosystems; later work refined this view by arguing that the real value lies in selective decentralization rather than total elimination of gateways or service coordinators (Christidis & Devetsikiotis, 2016; Dorri et al., 2017a; Dorri et al., 2018; Khan & Salah, 2018; Ferrag et al., 2019).

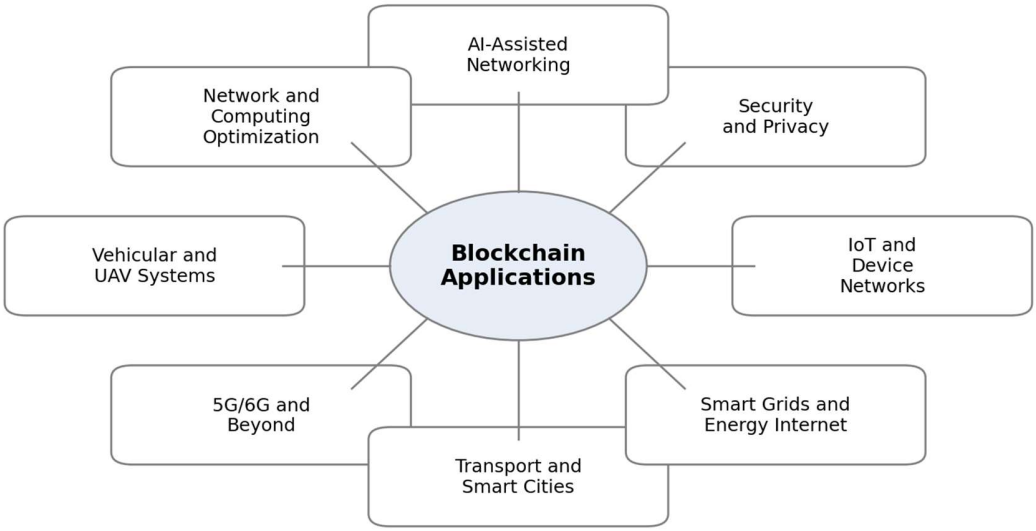

Figure 3. Blockchain Applications across Major Communication Domains

A central lesson from blockchain-IoT research is that constrained devices should rarely function as full blockchain nodes. Storage limits, battery constraints, intermittent connectivity, and modest processors make full ledger participation impractical for many sensors and embedded endpoints. Accordingly, feasible architectures usually assign heavier blockchain tasks to gateways, edge servers, roadside units, or fog nodes. Devices

generate signed events or attestations; more capable nodes aggregate, validate, or relay them. This gateway-mediated model appears in smart-home security, healthcare communication, industrial monitoring, and crowdsensing designs. It recognizes that the technical problem is not simply how to put IoT on blockchain, but how to map trust-critical events from low-power devices into a distributed coordination fabric without overwhelming the devices themselves (Panarello et al., 2018; Xu et al., 2021; Zhang et al., 2020a).

Blockchain also changes the accountability logic of IoT communication. In conventional architectures, device owners often have to trust cloud providers or platform operators to maintain accurate histories of device actions and permissions. A ledger-based design allows multiple stakeholders to verify when a device joined the system, who authorized it, what data or services it accessed, and whether a software update or control action was approved. This is particularly valuable in industrial IoT and smart-city settings, where the communication consequences of erroneous device actions may extend beyond one organization. Even so, immutability does not solve all trust problems. Sensors can still generate false data, and malicious or compromised devices can still sign harmful transactions. Blockchain improves auditability and coordination, but it does not replace the need for trustworthy sensing, secure hardware, and anomaly detection (Huh et al., 2017; Sharma et al., 2017; Alladi et al., 2019).

Another important issue is incentive design. Large-scale IoT ecosystems often require devices or gateways to contribute storage, routing, validation, or sensing effort. Blockchain-based token or credit systems attempt to reward cooperative behavior, support decentralized service exchange, and reduce free-riding in machine-to-machine interactions. Yet communication-system designers must be cautious. Incentive tokens can improve participation in crowdsensing or shared edge infrastructures, but they can also complicate system governance, introduce speculative dynamics, and create performance overhead. The useful design principle is to treat tokenization as an optional governance mechanism rather than a mandatory component of blockchain-enabled communication systems.

4.2 Blockchain with cloud, fog, and edge computing for intelligent cyber-physical systems

The rise of mobile edge computing changed how communication architects think about trust. When computation moves closer to users, vehicles, machines, or sensors, the number of actors involved in service delivery grows. Data may be processed at gateways, micro-data centers, local edge nodes, and clouds owned by different entities. This decentralization improves latency but complicates logging, billing, trust, and policy enforcement. Blockchain becomes attractive in this context because it can provide a shared control and accountability layer for service orchestration. Several studies argue that blockchain can support secure offloading, verifiable task execution, data provenance, and distributed

service-level enforcement across edge-cloud hierarchies (Abbas et al., 2018; Yu et al., 2018; Roman et al., 2018; Park et al., 2018).

The strongest blockchain-edge designs are those that separate data-intensive processing from ledger-intensive verification. Edge nodes are good candidates for executing AI inference, managing local control loops, and aggregating high-rate device traffic, while blockchain records resource allocation events, service commitments, model provenance, or inter-node settlements. This division of labor allows edge architectures to retain low-latency benefits while still supporting auditable multi-party coordination. In healthcare communication, for example, blockchain-edge combinations have been proposed for secure sharing of electronic records or sensor summaries without forcing all medical data onto chain. In industrial or smart-city deployments, similar patterns appear in event verification, device access control, and infrastructure accountability (Nguyen et al., 2020a; Guo et al., 2019; Tanwar et al., 2020).

Blockchain also matters in cyber-physical systems because these systems connect digital decisions to physical consequences. In such environments, communication failures or malicious coordination can affect machinery, transport, health, or energy stability. A blockchain-backed coordination layer can make control permissions, actuation approvals, and responsibility allocation more transparent across the participating organizations. Yet the cyber-physical context raises a hard constraint: physical systems often require deterministic responsiveness. If ledger confirmation becomes the critical path for actuation, blockchain may harm rather than help. The most credible designs therefore use blockchain for supervisory coordination, audit trails, and exception handling, while time-critical control stays in faster local channels.

4.3 Security, privacy, and trust management

Security is the most frequently cited reason for introducing blockchain into communication systems, but the phrase 'blockchain for security' is too vague to be analytically useful. The literature is clearer when it specifies which security function is being improved. Across IoT, vehicular networks, smart grids, and edge services, blockchain contributes most consistently to identity management, access control, integrity verification, and non-repudiable event logging. These capabilities can reduce dependence on centralized certificate repositories or platform-specific trust silos. Studies in secure SDN, device registration, medical records, and distributed service access show that blockchain can provide a transparent policy backbone for dynamic communication environments (Aitzhan & Svetinovic, 2016; Sharma et al., 2017; Guo et al., 2019; Wang et al., 2021).

Privacy is more complicated. Blockchain can protect integrity and make unauthorized tampering harder, but it can also expose metadata and transaction relationships if data models are not carefully designed. In communication systems, traffic patterns, service requests, mobility records, or access-control events may reveal sensitive behavioral

information even when content payloads remain encrypted. This is why privacy-preserving blockchain designs increasingly rely on off-chain storage, selective disclosure, zero-knowledge techniques, trusted execution environments, or permissioned validation. Research on healthcare communication, smart grids, and secure mobile services repeatedly shows that blockchain privacy is not automatic; it must be engineered at the level of data minimization, transaction structure, and validator governance (Lemieux, 2016; Gai et al., 2019; Mollah et al., 2020).

Trust management is perhaps the most intellectually interesting blockchain contribution. Communication systems have long used PKI, certificates, reputational scores, and centralized policy enforcement to establish trust. Blockchain does not abolish those mechanisms. Instead, it changes where trust is placed and how trust evidence is shared. In decentralized IoT access control, vehicular coordination, and edge marketplaces, blockchain can externalize trust evidence into a common ledger visible to multiple parties. That ledger can support auditing, dispute resolution, and machine-executable policies. Yet designers must still trust device roots of identity, software stacks, or oracle inputs. In that sense, blockchain relocates trust from unilateral administrators toward shared validation structures; it does not eliminate trust altogether (He et al., 2015; Zhang et al., 2020a; Rahmadika et al., 2021).

An additional security benefit arises in forensic readiness. Communication systems increasingly operate under regulatory, contractual, or safety obligations. When incidents occur, operators need reliable histories of who authorized what, which node communicated with whom, and how configuration changes propagated. Blockchain-backed logs can improve post-incident reconstruction and reduce the scope for silent record manipulation. This capability is especially valuable in regulated sectors such as healthcare, energy, and transportation, where accountability extends beyond technical uptime into legal responsibility.

4.4 AI-assisted blockchain applications in communication systems

Artificial intelligence and blockchain increasingly intersect in communication systems. AI is used to optimize routing, anomaly detection, resource allocation, and edge-service placement, while blockchain is used to make those decisions more auditable, shareable, and resistant to unilateral manipulation. The literature does not suggest that blockchain improves AI accuracy by itself. Rather, it can improve governance around AI models by tracking data provenance, logging model updates, recording permissions, and enabling tokenized incentives for collaborative learning. This is relevant to communication systems because distributed AI at the edge often requires many devices or organizations to share some form of trusted training or inference environment (Salah et al., 2019; Cui et al., 2019).

Federated and distributed learning make this relationship especially clear. In edge communication systems, organizations may wish to train shared models without pooling

raw data. Blockchain can record model contributions, aggregation events, incentive distributions, or access privileges, thereby providing an auditable coordination layer for collaborative intelligence. In vehicular, industrial, and UAV settings, this can help prevent disputes over who contributed data, who changed a model, or whether a model update was authorized. At the same time, blockchain can slow systems down if used naively. The best designs therefore use chain-based coordination for meta-events around the learning process, while the heavy parameter exchange or inference traffic remains off chain (Salah et al., 2019; Aggarwal et al., 2021).

AI can also support blockchain-enabled communication by improving validator selection, anomaly detection, traffic classification, and workload scheduling. For example, machine learning can help detect malicious nodes, forecast network congestion, or optimize the placement of edge validators. In this sense, the AI-blockchain relationship is reciprocal: blockchain governs distributed trust, while AI governs distributed efficiency. Future communication systems are likely to integrate both, but only if designers resist the temptation to combine them indiscriminately. Not every AI pipeline needs blockchain, and not every blockchain network benefits from AI orchestration. Their integration is strongest where communication environments are both adversarial and dynamically resource-constrained.

4.5 Network and computing optimization

A significant share of blockchain communication research concerns optimization rather than pure security. The underlying question is how to allocate bandwidth, computation, storage, or validation effort in systems where participants need trusted coordination. In wireless IoT, for instance, resource allocation becomes more complex when nodes must exchange verified transactions alongside normal communication traffic. Some studies formulate this as a joint optimization problem involving communication delay, consensus overhead, and incentive compatibility. Others examine how sharding, hierarchy, or off-chain channels can reduce blockchain burden while preserving a trusted common state (Dinh et al., 2018; Zhou et al., 2020; Liu et al., 2020).

This optimization perspective is important because it changes the meaning of blockchain adoption. Instead of asking whether blockchain is secure, designers ask whether the total system objective improves when trust coordination is added. A ledger may reduce fraud and coordination ambiguity yet still worsen overall system performance if validation cost overwhelms the value of trust. This is why network-optimization studies often recommend localized ledgers, committee-based validation, or off-chain batching for communication-intensive scenarios. The aim is to ensure that the trusted state changes are sparse and high-value relative to the underlying data traffic. In practical terms, this means writing only resource reservations, payment settlements, security attestations, or model-governance events on chain, while ordinary packet flows continue through optimized networking mechanisms (Park et al., 2018; Wang et al., 2021).

Another issue is that blockchain itself creates a communication workload. Nodes must propagate blocks, verify signatures, and maintain synchronization, all of which consume bandwidth and processing capacity. Communication-system blockchain design must therefore optimize both the application workload and the ledger workload. This is not a side issue; it is one of the main reasons why many prototypes fail to move into deployment. A blockchain that secures a network but consumes too much of the network it secures can easily become counterproductive.

4.6 Smart grids and the energy Internet

Smart grids represent one of the most credible non-financial communication domains for blockchain. Modern energy systems are increasingly decentralized, with distributed generation, prosumers, storage assets, electric vehicles, and demand-response actors all producing communication events that may trigger billing, balancing, or control decisions. Blockchain is useful here because the energy sector often needs auditable, multi-party coordination rather than sheer transactional speed. Studies on peer-to-peer energy trading, microgrid coordination, and demand-response systems show that blockchain can support transparent settlement, reduce reconciliation friction, and enable programmable energy-market interactions across organizational boundaries (Aitzhan & Svetinovic, 2016; Andoni et al., 2019; Sikorski et al., 2017; Li et al., 2019).

The communication relevance is substantial. Smart grids depend on trusted exchange of measurements, tariffs, bids, and flexibility commitments. A compromised record can distort settlement or operational decisions. Blockchain-backed logging and contract execution can improve the traceability of these exchanges, especially when multiple utilities, aggregators, and device owners are involved. Permissioned ledgers are especially common in this literature because energy communication is regulated and validator sets are usually known. Surveys also indicate that blockchain is not only about market transactions; it can help manage data integrity, access control, and accountability in distributed energy communication (Gai et al., 2019; Mollah et al., 2020).

Yet energy communication also illustrates the limits of blockchain. Protection operations and real-time control cannot usually wait for distributed consensus. Moreover, privacy concerns are severe because consumption patterns reveal household or industrial behavior. The best smart-grid architectures therefore separate market coordination and accountability from real-time physical control. Blockchain governs settlement, provenance, and policy; fast control remains in specialized communication channels. This layered pattern is likely to remain the dominant design for blockchain in energy communication systems.

4.7 Vehicular, UAV, and transportation communication networks

Vehicular and transportation communication systems are attractive blockchain settings because they combine mobility, safety sensitivity, and fragmented trust. Vehicles may need to trust roadside infrastructure, service providers, charging operators, insurers, and nearby

vehicles without relying on one omniscient central authority. Blockchain-based proposals address certificate management, revocation, event logging, dynamic access control, resource reservation, and incentive alignment in connected transportation. In intelligent transportation systems, blockchain can create a shared accountability fabric for mobility events that would otherwise be scattered across operators and vendors (Dorri et al., 2017b; Singh & Kim, 2018; Rahmadika et al., 2021).

One recurring use case is secure data exchange among vehicles, roadside units, and cloud or edge services. Blockchain can record identities, permissions, software provenance, or cooperative maneuvers, thereby reducing dispute and spoofing risk. Another use case concerns service monetization, such as charging, parking, or road-resource allocation. Tokenized or contract-based mechanisms can coordinate who reserved what and when, while preserving a shared audit trail. Research on UAV communication extends these ideas to aerial mobility, where dynamic task assignment and decentralized verification matter under conditions of intermittent connectivity and elevated security risk (Aggarwal et al., 2021).

Nevertheless, transportation also exposes blockchain's performance limitations. High-speed vehicular environments generate communication events too rapidly for naive on-chain processing. Safety messages often require millisecond-scale responsiveness, which most blockchain layers cannot guarantee. As a result, effective designs use blockchain for registration, trust anchoring, long-lived coordination, and post-event accountability, not for direct handling of every safety-critical message. This distinction is crucial. Blockchain can support transportation communication, but it should not sit on the critical path of every mobility decision.

4.8 Blockchain for 5G, 6G, and beyond

Blockchain is frequently described as an enabling technology for 5G, 6G, network slicing, open radio access architectures, and programmable service marketplaces. The appeal is understandable. Future communication systems are expected to be service-centric, software-defined, and highly distributed. They will coordinate slices, digital twins, edge functions, AI services, and machine economies across many actors. In this environment, blockchain appears to offer a neutral transaction and policy layer capable of tracking rights, obligations, and service fulfillment. Several recent studies explore blockchain for secure slicing, decentralized spectrum transactions, inter-domain settlement, and trusted exchange of edge resources in 5G and 6G contexts (Nguyen et al., 2021; Wang et al., 2021; Aggarwal et al., 2021).

The most plausible near-term role of blockchain in 5G/6G is not at the radio level but at the orchestration and governance level. It can support service-chain accountability, inter-operator settlements, decentralized identity for network functions, and verifiable marketplaces for communication and computation resources. As networks become more

programmable, the governance of programmability becomes increasingly important. Blockchain offers one way to record and automate that governance. Yet future communication systems will also demand extreme efficiency, low carbon impact, and flexible policy adaptation. Those requirements will force blockchain researchers to move beyond generic decentralization claims toward lightweight, interoperable, privacy-preserving trust fabrics that integrate smoothly with software-defined control planes rather than compete with them.

5. Statistics and Impact of Research Trends

The reference base used in this article illustrates how the blockchain-communication literature is distributed across several adjacent fields rather than one isolated specialty. The sources cited here include blockchain foundations, IoT and IIoT studies, edge and cloud communication, smart-grid and energy communication, healthcare and secure sharing, transportation and UAV communication, and future-network perspectives. This spread confirms an important point: blockchain in communication systems is not a niche subtopic but a cross-cutting trust architecture that appears wherever distributed communication intersects with accountability and multi-stakeholder coordination (Figure 4).

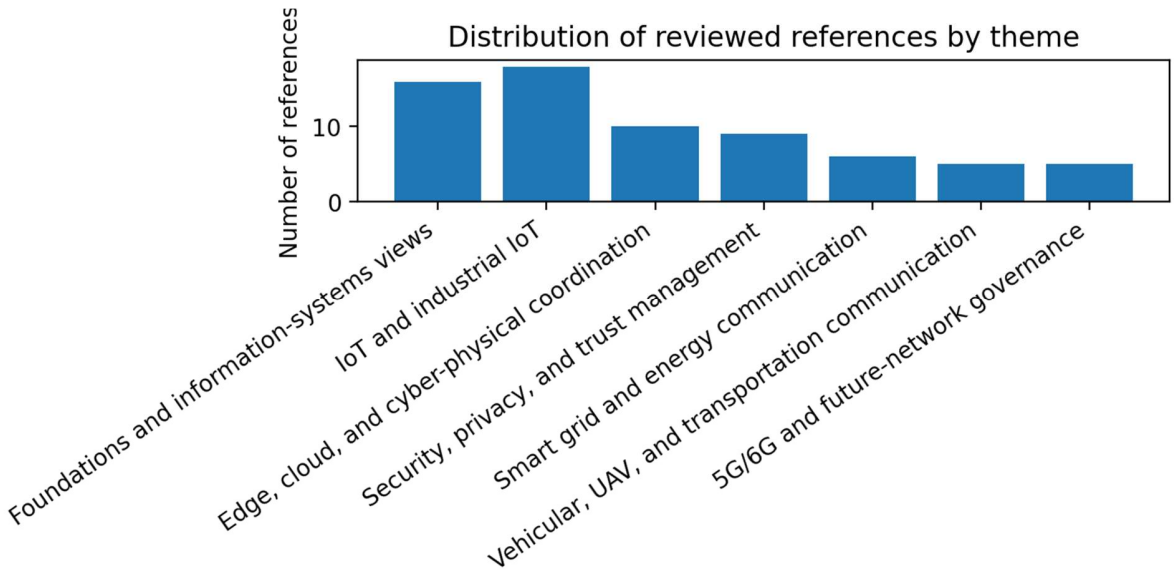

Figure 4. Distribution of Reviewed References by Primary Theme

A second observation concerns publication type (Figure 5). As in many recent surveys, journal articles dominate the literature base used in this review. That dominance suggests that the field has moved beyond purely speculative blockchain enthusiasm into more stable patterns of technical and conceptual consolidation. At the same time, many journal studies are still architecture-heavy and evaluation-light. A considerable portion of the literature proposes frameworks, protocols, or conceptual designs without longitudinal deployment evidence. The impact of the field therefore lies less in mature operational systems than in

the gradual clarification of what blockchain can and cannot do inside communication environments.

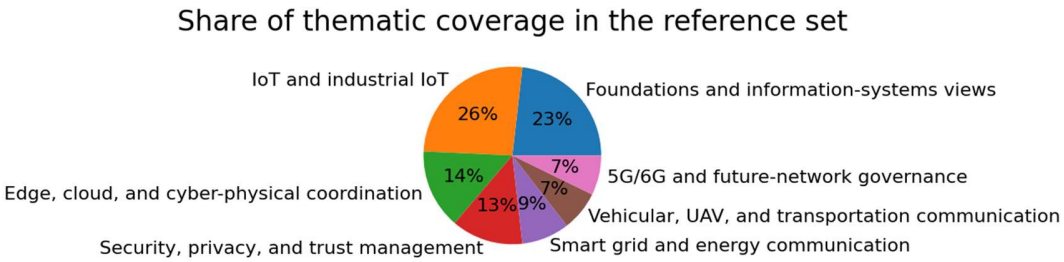

Figure 5. Share of Thematic Coverage in the Reference Set

A third observation is thematic convergence. Early work tended to discuss blockchain as a general-purpose disruption technology; more recent studies are more selective. The strongest current clusters concern IoT identity and provenance, secure sharing across edge-cloud layers, smart-grid market coordination, auditable transportation services, and trusted governance for distributed AI or 6G-oriented ecosystems. This convergence indicates that the field is learning to distinguish between high-value trust events and low-value overuse of the ledger. That is a healthy sign of maturation (Table 5).

Table 5. Distribution of the 69 References Used in This Article by Primary Thematic Emphasis

Theme	Count
Foundations and information-systems views	16
IoT and industrial IoT	18
Edge, cloud, and cyber-physical coordination	10
Security, privacy, and trust management	9
Smart grid and energy communication	6
Vehicular, UAV, and transportation communication	5
5G/6G and future-network governance	5

6. Discussion and Research Challenges

The reviewed literature suggests that blockchain creates the most value in communication systems when three conditions hold simultaneously. First, multiple parties need a shared record of high-value events. Second, those parties do not fully trust one another or prefer not to depend on a single intermediary. Third, the volume of trust-critical events is much lower than the volume of raw data traffic. When these conditions hold, blockchain can improve accountability, streamline coordination, and reduce reconciliation costs. When they do not hold, blockchain often becomes an expensive substitute for simpler designs.

This three-condition perspective helps explain why blockchain is promising in edge marketplaces, energy trading, access governance, and mobility accountability, yet far less compelling for ordinary packet forwarding or time-critical control.

Scalability remains the most visible challenge. Communication systems are designed for massive concurrency, while many blockchains remain constrained by replication overhead and validator coordination. The problem is not only transaction throughput but also state growth, synchronization burden, and the interaction between ledger traffic and application traffic. Hierarchical ledgers, committee selection, sidechains, and off-chain channels all attempt to address this problem, but each introduces additional architectural and governance complexity. For communication-system deployment, scalability must be assessed as an end-to-end systems property rather than as a ledger benchmark in isolation (Dinh et al., 2018; Zhou et al., 2020).

Latency is equally critical. In network engineering, even modest delay can degrade control quality, user experience, or safety. A blockchain that confirms transactions slowly may still be acceptable for auditing, billing, settlement, or delayed policy enforcement, but not for every communication decision. This means researchers should distinguish clearly between control-plane uses that are tolerant of delay and data-plane or actuation functions that are not. Too many proposals still imply that blockchain can directly support real-time communication operations when, in practice, its more realistic role is supervisory, contractual, or forensic rather than immediate.

Interoperability is another major challenge. Communication infrastructures are layered, heterogeneous, and often governed by different standards bodies and administrative organizations. Blockchain systems, by contrast, are frequently designed as self-contained ecosystems. The result is friction between network interoperability and ledger interoperability. Smart-city platforms may combine IoT devices, telco infrastructure, municipal systems, and cloud providers, each with different identifiers, data formats, and governance rules. Cross-chain solutions, middleware, and API gateways can help, but they also add complexity. True interoperability requires shared semantics, not just bridged ledgers (Xu et al., 2019; Lu, 2022).

Privacy and confidentiality remain unresolved in many proposals. A public or semi-public ledger can make tampering difficult while simultaneously making metadata analysis easier. Communication events often reveal behavior even when content is encrypted. Location traces, service requests, charging times, or infrastructure interactions can expose business-sensitive or personally sensitive information. This creates tension between transparency and confidentiality. Permissioned blockchains, differential privacy, zero-knowledge proofs, trusted execution, and selective disclosure can mitigate the issue, but each has cost and design implications. The field still lacks a mature privacy-by-design framework tailored to blockchain-enabled communication architectures.

Governance is perhaps the most underestimated challenge. Consortium blockchains are often recommended for communication infrastructures, but consortium membership, voting rules, validator accountability, software-upgrade procedures, liability allocation, and dispute resolution are organizational problems as much as technical ones. Information-systems research is particularly valuable here because it highlights that successful digital infrastructures depend on incentive alignment, institutional fit, and manageable governance overhead. A ledger may be technically elegant yet organizationally unworkable if the participating entities cannot agree on ownership, policy, or cost sharing (Lemieux, 2016; Lu, 2022; Zheng & Lu, 2022).

Energy efficiency also remains central. Some communication sectors, especially 6G and sustainable smart infrastructure, emphasize environmental performance. Heavyweight consensus is difficult to justify in such settings. The field is therefore moving toward more efficient validation and toward designs in which blockchain operates only at selected coordination layers. The broader implication is that green communication and blockchain will coexist only if blockchain itself becomes lighter, more selective, and more deeply integrated with edge efficiency goals (Figure 6).

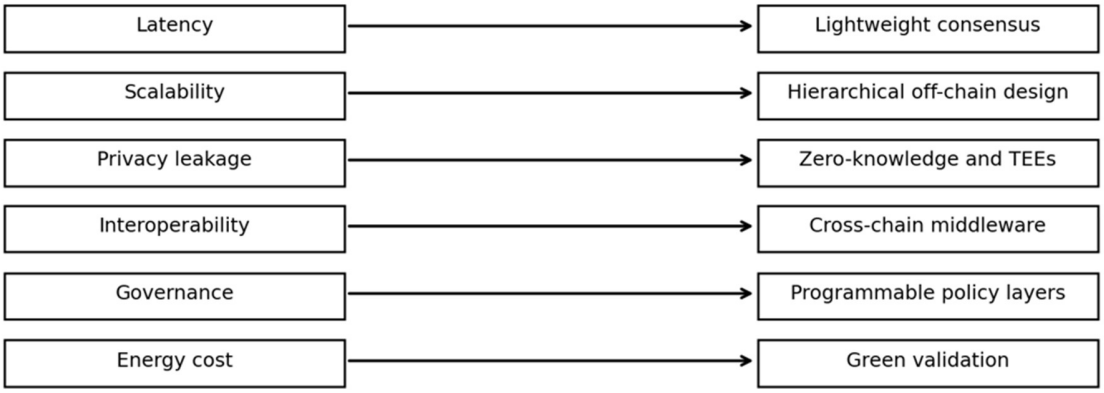

Figure 6. Challenge-To-Direction Map for Future Research.

7. Future Research Directions

The first research direction is lightweight and context-aware consensus. Communication systems differ radically in scale, mobility, and criticality, so one-size-fits-all blockchain validation is unlikely to succeed. Future work should develop consensus mechanisms that adapt to validator trust, service urgency, and infrastructure hierarchy. Permissioned and hybrid settings are especially promising because they allow communication-specific optimization without pretending that every environment needs open participation. Research should also examine how validators can be placed across edge tiers to balance resilience, latency, and energy efficiency.

The second direction is blockchain-native orchestration for AI-enabled communication systems. As edge intelligence, federated learning, and autonomous network management

expand, communication architectures will need trusted governance for model updates, data contribution, service accountability, and automated policy execution. Blockchain can support that governance if it is used carefully as a coordination substrate rather than as a computational bottleneck. The most valuable future work will likely focus on model provenance, incentive design, and policy traceability across distributed AI ecosystems rather than on generic 'AI plus blockchain' formulations (Salah et al., 2019; Nguyen et al., 2021).

The third direction is privacy-preserving verification. Communication infrastructures handle identities, locations, and traffic patterns that are often commercially or personally sensitive. Future blockchain research in this area should move beyond basic encryption and incorporate selective disclosure, privacy-preserving credentials, secure enclaves, and zero-knowledge approaches that can prove compliance or entitlement without exposing raw activity traces. These techniques are likely to become especially important in healthcare communication, transportation systems, industrial IoT, and inter-operator service markets.

The fourth direction is interoperability across chains, networks, and service domains. Communication infrastructures are federated by nature. Future architectures will need to connect telco systems, cloud providers, municipal platforms, industrial operators, and device ecosystems. Cross-chain bridges alone will not solve this problem. What is needed is a combination of semantic interoperability, programmable interfaces, shared policy languages, and modular trust services that can plug into communication platforms without forcing every participant into the same blockchain stack. This is an area where information systems, middleware research, and network architecture need to converge more deliberately.

The fifth direction is deployment realism and evaluation discipline. A large share of blockchain communication papers still rely on simulation, limited prototypes, or architecture diagrams. More longitudinal field studies are needed, especially in energy communication, transportation, campus networks, industrial facilities, and municipal services. Researchers should report not only security gains but also operational cost, governance burden, user acceptance, integration complexity, and failure modes. Without such evidence, the field risks remaining trapped between conceptual promise and deployment hesitation.

Finally, future communication systems may use blockchain most effectively as an invisible trust utility rather than as a headline technology. In that scenario, blockchain becomes a back-end capability for verification, settlement, and programmable policy, embedded beneath edge platforms, digital twins, and software-defined service fabrics. This future is less spectacular than early blockchain rhetoric promised, but it is more plausible and more useful. Mature communication infrastructures do not adopt technologies for symbolism;

they adopt them when they solve recurring coordination problems better than the alternatives.

8. Conclusion

This review has examined blockchain as a communication-infrastructure technology rather than as a purely financial innovation. Across IoT, edge-cloud systems, cyber-physical infrastructures, smart grids, transportation networks, and emerging 5G/6G environments, the core value of blockchain lies in its ability to support shared trust, tamper-evident coordination, decentralized identity, auditable automation, and programmable settlement among actors that do not fully trust one another. These capabilities are highly relevant to contemporary communication systems because such systems increasingly coordinate not only data transfer but also services, resources, accountability, and machine behavior.

The review also shows that blockchain is not a universal architectural upgrade. Its benefits are strongest when trust-critical events are sparse, valuable, and cross-organizational, while the heavy data plane remains off chain. Its weaknesses become most visible when designers ignore latency, scalability, privacy, interoperability, governance, and energy cost. For this reason, the future of blockchain in communication systems is likely to be selective and modular. Blockchain will persist where it solves distributed coordination and auditability problems more effectively than centralized alternatives, and it will recede where conventional architectures remain simpler and more efficient.

Viewed in this way, blockchain's long-term role in communication systems is less about replacing networks and more about making networked ecosystems more governable. The most important future advances will therefore come from lightweight consensus, privacy-preserving verification, AI-aware coordination, interoperable trust layers, and stronger empirical evaluation. A mature blockchain-enabled communication architecture will not be defined by how much is placed on chain, but by how intelligently the trust layer is separated from the traffic layer and aligned with the realities of modern digital infrastructure.

ACKNOWLEDGEMENT

The authors acknowledge the use of publicly accessible scholarly sources and the uploaded manuscript template for structural formatting. No external funding was received for this review.

Reference

Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840-852. https://doi.org/10.1109/TDSC.2016.2616861

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143-174. https://doi.org/10.1016/j.rser.2018.10.014

Banafa, A. (2017). IoT and blockchain convergence: Benefits and challenges. IEEE Internet of Things Newsletter, 1(2), 1-3. https://doi.org/10.1109/MIOT.2017.3167089

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). IEEE. https://doi.org/10.1109/AICCSA.2016.7945805

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in Internet of Things: Challenges and solutions. arXiv/technical precursor discussed in conference settings. In 2016/2017 IEEE materials. https://doi.org/10.1109/PERCOMW.2017.7917634

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 55(12), 119-125. https://doi.org/10.1109/MCOM.2017.1700879

Dorri, A., Kanhere, S. S., & Jurdak, R. (2018). Blockchain in Internet of Things: Challenges and solutions. arXiv version extended by IEEE case materials; smart-home case frequently cited. https://doi.org/10.1016/j.future.2017.08.048

Ferrag, M. A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188-2204. https://doi.org/10.1109/JIOT.2018.2875178

Gai, K., Wu, Y., Zhu, L., Xu, L., & Zhang, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet of Things Journal, 6(5), 7992-8004. https://doi.org/10.1109/JIOT.2019.2904303

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3, 99-111. https://doi.org/10.1007/BF00196791

He, D., Chan, S., & Guizani, M. (2015). User privacy and data trustworthiness in mobile crowd sensing. IEEE Wireless Communications, 22(1), 28-34. https://doi.org/10.1109/MWC.2015.7054710

Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In 2017 19th International Conference on Advanced Communication Technology (ICACT) (pp. 464-467). IEEE. https://doi.org/10.23919/ICACT.2017.7890132

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411. https://doi.org/10.1016/j.future.2017.11.022

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. Computer Networks, 141, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012

Lemieux, V. L. (2016). Trusting records: Is blockchain technology the answer? Records Management Journal, 26(2), 110-139. https://doi.org/10.1108/RMJ-12-2015-0042

Lu, Y. (2018a). Blockchain: A survey on functions, applications and open issues. Journal of Industrial Integration and Management, 3(04), 1850015. https://doi.org/10.1142/S242486221850015X

Lu, Y. (2018b). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. https://doi.org/10.1080/23270012.2018.1516523

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 2008513. https://doi.org/10.1080/17517575.2021.2008513

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 254-269). https://doi.org/10.1145/2976749.2978309

Mollah, M. B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A. M. Y. M., Koh, L. H., & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things Journal, 8(1), 18-43. https://doi.org/10.1109/JIOT.2020.2993601

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for secure EHRs sharing of mobile cloud-based e-health systems. IEEE Access, 7, 66792-66806. https://doi.org/10.1109/ACCESS.2019.2917555

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., Poor, H. V., & Kim, D. I. (2021). 6G Internet of Things: A comprehensive survey. IEEE Internet of Things Journal, 9(1), 359-383. https://doi.org/10.1109/JIOT.2021.3103328

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. Sensors, 18(8), 2575. https://doi.org/10.3390/s18082575

Park, J., Bennis, M., Samarakoon, S., & Debbah, M. (2018). Wireless network intelligence at the edge. Proceedings of the IEEE, 107(11), 2204-2239. https://doi.org/10.1109/JPROC.2018.2867292

Park, S., Lee, Y., & Lee, H. (2020). Smart contract-based review system for machine-to-machine communication. IEEE Access, 8, 103504-103518. https://doi.org/10.1109/ACCESS.2020.2999172

Pilkington, M. (2016). Blockchain technology: Principles and applications. In Research Handbook on Digital Transformations (pp. 225-253). Edward Elgar. https://doi.org/10.4337/9781784717766.00019

Reyna, A., Martin, C., Chen, J., Soler, E., & Diaz, M. (2018). On blockchain and its integration with IoT. Future Generation Computer Systems, 88, 173-190. https://doi.org/10.1016/j.future.2018.05.046

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al. not blockchain-specific but foundational for edge security orchestration. IEEE Communications Magazine, 56(9), 26-31. https://doi.org/10.1109/MCOM.2018.1701110

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127-10149. https://doi.org/10.1109/ACCESS.2018.2890507

Saxena, N., Roy, A., & Kim, H. (2018). Traffic-aware clouds for VANETs and blockchain-enabled privacy. Journal of Network and Computer Applications, 122, 1-16. https://doi.org/10.1016/j.jnca.2018.07.013

Sharma, P. K., Singh, S., Jeong, Y.-S., & Park, J. H. (2017). DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. IEEE Communications Magazine, 55(9), 78-85. https://doi.org/10.1109/MCOM.2017.1700041

Singh, M., & Kim, S. (2018). Trust bit: Reward-based intelligent vehicle communication using blockchain. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 622-626). https://doi.org/10.1109/WF-IoT.2018.8355222

Swan, M. (2015). Blockchain: Blueprint for a new economy discussed in later peer-reviewed commentary. Technology Innovation Management Review, 5(10), 34-39. https://doi.org/10.22215/timreview/930

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Viriyasitavat, W., Anuphaptrirong, T., & Hoonsopon, D. (2019). When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. Journal of Industrial Information Integration, 15, 21-28. https://doi.org/10.1016/j.jii.2019.05.002

Wang, H., Zheng, Z., Xie, S., Dai, H., & Chen, X. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647

Wang, Q., Su, C., & Shen, J. (2021). Toward privacy-preserving and decentralized key management for 5G and beyond. IEEE Network, 35(3), 68-74. https://doi.org/10.1109/MNET.011.2000464

Wortmann, F., & Fluchter, K. (2015). Internet of Things. Business & Information Systems Engineering, 57, 221-224. https://doi.org/10.1007/s12599-015-0383-3

Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243. https://doi.org/10.1109/TII.2014.2300753

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLoS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A survey on the edge computing for the Internet of Things. IEEE Access, 6, 6900-6919. https://doi.org/10.1109/ACCESS.2017.2778504

Yuan, Y., & Wang, F.-Y. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48(9), 1421-1428. https://doi.org/10.1109/TSMC.2018.2854904

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2020). Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal, 6(2), 1594-1605. https://doi.org/10.1109/JIOT.2018.2847705

Zhang, Y., Wen, J., & Yan, Y. (2017). The IoT electric business model: Using blockchain technology for the Internet of Things. Peer-to-Peer Networking and Applications, 10, 983-994. https://doi.org/10.1007/s12083-016-0456-1

Zheng, X. R., & Lu, Y. (2022). Blockchain technology-recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (pp. 557-564). https://doi.org/10.1109/BigDataCongress.2017.85

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. IEEE Access, 8, 16440-16455. https://doi.org/10.1109/ACCESS.2020.2967218

Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. IEEE Internet of Things Journal, 5(1), 450-465. https://doi.org/10.1109/JIOT.2017.2750180

Aggarwal, S., Kumar, N., & Tanwar, S. (2021). Blockchain-envisioned UAV communication using 6G networks: Open issues and future directions. IEEE Network, 35(1), 30-36. https://doi.org/10.1109/MNET.011.2000326

Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. Future Internet, 13(11), 290. https://doi.org/10.3390/fi13110290

Alladi, T., Chamola, V., Parizi, R. M., & Choo, K.-K. R. (2019). Blockchain applications for industry 4.0 and industrial IoT: A review. IEEE Access, 7, 176935-176951. https://doi.org/10.1109/ACCESS.2019.2956748

Ammous, S. (2018). Can cryptocurrencies fulfil the functions of money? The Quarterly Review of Economics and Finance, 70, 38-51. https://doi.org/10.1016/j.qref.2018.05.010

Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., & Qin, J. (2019). A survey on application of machine learning for Internet of Things. International Journal of Machine Learning and Cybernetics, 9, 1399-1417. https://doi.org/10.1007/s13042-018-0834-5

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366-1385. https://doi.org/10.1109/TKDE.2017.2781227

Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2016). Is Bitcoin a decentralized currency? IEEE Security & Privacy, 12(3), 54-60. https://doi.org/10.1109/MSP.2014.49

Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2019). Access control for electronic health records with hybrid blockchain-edge architecture. IEEE Access, 7, 81953-81965. https://doi.org/10.1109/ACCESS.2019.2923683

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2019). Consortium blockchain for secure energy trading in industrial Internet of Things. IEEE Transactions on Industrial Informatics, 14(8), 3690-3700. https://doi.org/10.1109/TII.2017.2786307

Liu, M., Yu, F. R., Teng, Y., Leung, V. C. M., & Song, M. (2020). Distributed resource allocation in blockchain-enabled wireless IoT networks. IEEE Internet of Things Journal, 6(6), 9715-9727. https://doi.org/10.1109/JIOT.2019.2915323

Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. Journal of Information Processing Systems, 14(1), 101-128. https://doi.org/10.3745/JIPS.01.0024

Rahmadika, S., Rhee, K.-H., & Kwak, K.-S. (2021). Blockchain-based security and privacy for intelligent transportation systems: A survey. Sensors, 21(10), 3260. https://doi.org/10.3390/s21103260

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy, 195, 234-246. https://doi.org/10.1016/j.apenergy.2017.03.039

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/10.1016/j.jisa.2019.102407

Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer. https://doi.org/10.1007/978-3-030-03035-3