From Vehicular Blockchain Trading to Smart Mobility Governance: Institutional Trust, Incentives, and Technology Adoption

Aiman Farhan Ismail[1], Nurul Aina Rahman[2], Mei Ling Tan[3], Hafizah Abdullah[4, *]

[1] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang, Malaysia
[2] School of Technology Management and Logistics, Universiti Utara Malaysia, Sintok, Kedah, Malaysia
[3] Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia
[4] Faculty of Business and Management, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia

* Email: *hafizah.abdullah@uitm.edu.my* (Corresponding Author)

Abstract

Blockchain-enabled vehicular edge markets are usually discussed as technical systems for secure resource discovery, smart-contract settlement, and decentralized trust management. This article reframes that problem as a smart mobility governance issue. It argues that vehicular blockchain trading can support scalable resource sharing only when technical trust is reinforced by institutional trust, fair incentives, privacy assurance, regulatory clarity, and adoption readiness. A conceptual framework is developed to connect vehicle resource markets, blockchain transaction layers, institutional governance, trust analytics, incentive design, and technology adoption. A simulated stakeholder dataset is then used to illustrate how governance variables influence adoption readiness among vehicle owners, fleet managers, platform operators, edge infrastructure providers, municipal officers, and cybersecurity auditors. Results suggest that institutional trust and incentive fairness are the strongest drivers of adoption readiness, while regulatory clarity remains the weakest perceived condition. The article contributes to technology innovation and society research by transforming a blockchain-based vehicular trading architecture into a broader governance model for smart mobility ecosystems. It also provides practical guidance for platform operators and public agencies seeking to deploy secure, accountable, and socially acceptable mobility resource markets.

Keywords: Vehicular blockchain; Smart mobility governance; Institutional trust; Incentive design; Technology adoption; Trust analytics; Edge computing; Privacy assurance

Article History

Received: April 14, 2023

Revised: June 22, 2023

Accepted: August 16, 2023

Available Online: September 30, 2023

From Vehicular Blockchain Trading to Smart Mobility Governance: Institutional Trust, Incentives, and Technology Adoption

1. Introduction

Blockchain-enabled vehicular markets are moving from a narrow engineering problem to a broader governance problem. The original technical question asks how mobile vehicles can exchange computation, storage, bandwidth, sensing, or energy-related resources through secure peer-to-peer coordination. A social-technical interpretation asks a wider question: what institutional conditions make such trading trusted, fair, accountable, and adoptable at scale? This article develops that second perspective by reframing vehicular blockchain trading as a smart mobility governance system. Blockchain provides the transaction layer, but governance supplies the rules, legitimacy, incentives, and accountability needed for public and private actors to accept the system.

The research direction is closely connected to blockchain-enabled information systems, where distributed ledgers are used to create verifiable records among parties that do not fully trust one another（Lu, 2022）. The vehicular edge market is a particularly demanding setting because actors are mobile, interactions are short, resources are heterogeneous, and trust must be updated continuously after each transaction. A vehicle may act as a requester in one period and a provider in another, while the edge gateway coordinates local discovery, smart contract execution, and ledger recording. This role switching makes the market more flexible than centralized road-side infrastructure, but it also exposes the system to manipulation, false identities, opportunistic bidding, and uneven willingness to participate.

The adoption of such platforms cannot be explained by technical capability alone. Information systems adoption research shows that perceived usefulness and perceived ease of use shape initial willingness to adopt new technologies（Davis, 1989）. In smart mobility, however, usefulness is not limited to faster matching or lower latency. Users, vehicle operators, mobility companies, and public agencies also evaluate whether the platform is fair, whether payments are predictable, whether data are protected, and whether the rules can be audited after disputes. Therefore, blockchain trading in vehicular networks should be studied as a combined system of technology performance, institutional trust, economic incentives, and organizational adoption.

Smart contracts are important because they translate governance rules into executable logic. In Internet of Things environments, blockchain and smart contracts have been widely discussed as tools for decentralized coordination, traceable transactions, and programmable trust（Christidis and Devetsikiotis, 2016）. For vehicular edge markets, the smart contract is not only a payment script; it becomes a rule engine that defines provider eligibility, pricing procedure, penalty clauses, privacy boundaries, and post-service trust updates. This article uses that idea to develop a governance-oriented model in which technical trust is combined with institutional legitimacy.

A governance view also complements unified technology acceptance theory, which argues that performance expectancy, effort expectancy, social influence, and facilitating conditions shape technology use（Venkatesh et al., 2003）. In vehicular blockchain trading, performance expectancy refers to efficient resource access, effort expectancy refers to low operational burden, social influence includes platform norms and regulatory expectations, and facilitating conditions include interoperable vehicle systems, edge infrastructure, and clear legal responsibility. This article therefore treats technology adoption as a dependent governance outcome, not merely as an engineering result.

The purpose of this study is to develop a conceptual and data-analytical article titled From Vehicular Blockchain Trading to Smart Mobility Governance: Institutional Trust, Incentives, and Technology Adoption. The study makes three contributions. First, it translates the technical logic of blockchain-based vehicular resource sharing into a governance framework suitable for JTIS. Second, it proposes a trust-incentive-adoption model that links institutional trust, smart contract incentives, privacy assurance, regulatory clarity, and platform readiness. Third, it provides simulated empirical evidence showing how trust scores, incentive fairness, privacy guarantees, and governance clarity affect adoption readiness across stakeholder groups in smart mobility markets.

2. Literature Review

Blockchain has been increasingly embedded into IoT systems to address identity management, data integrity, device authentication, and distributed trust（Xu et al., 2021）. Vehicular networks share many of these characteristics because vehicles behave as mobile IoT nodes with sensing, communication, computation, and storage functions. However, the vehicular setting adds unique governance complexity. Vehicles interact with road-side units, traffic platforms, fleet operators, insurers, logistics companies, and regulators. Thus, the same ledger transaction may carry operational, commercial, and public safety consequences.

Institutional theory helps explain why technical trust is insufficient for long-term adoption. Trust can be produced not only through personal relationships but also through institutions, rules, certifications, and standardized procedures（Zucker, 1986）. In a blockchain-enabled vehicular market, institutional trust emerges when stakeholders believe that the system's rules are stable, auditable, and fairly enforced. A ledger can record transactions, but users still need confidence that identity issuance, smart contract parameters, dispute handling, and data access rights are governed by legitimate authorities.

Supply chain and platform studies show that blockchain may reduce information asymmetry by providing immutable transaction records and shared visibility among authorized participants（Kshetri, 2018）. Similar logic applies to smart mobility. A vehicle owner may not know whether a provider actually delivered the promised resource level, and a provider may not know whether a requester will pay after service. Blockchain records, service evidence, and smart contract escrow mechanisms reduce the need for bilateral trust by creating a shared transactional memory.

The concept of institutions is also important because mobility markets operate under formal and informal constraints. Institutions define the rules of the game, shape incentives, and structure economic exchange（North, 1991）. For smart mobility governance, formal rules include data protection law, transport regulation, cybersecurity standards, and liability frameworks. Informal rules include user expectations about fairness, platform reputation, and acceptable uses of vehicle-generated data. A blockchain trading platform must align with both sets of rules to move from experimental deployment to social acceptance.

The literature on Industry 4.0 blockchain applications has emphasized traceability, security, interoperability, and distributed control（Chen et al., 2024）. These themes are directly relevant to vehicular edge markets because the vehicle becomes part of an intelligent industrial ecosystem. Vehicles produce data, request computation, provide temporary resources, and participate in machine-to-machine transactions. The governance challenge is therefore not simply to secure a single exchange but to coordinate many short-lived exchanges within a wider cyber-physical infrastructure.

Institutional isomorphism explains why platforms may converge toward similar governance forms when they face comparable regulatory pressure and legitimacy expectations（DiMaggio and Powell, 1983）. In smart

mobility, blockchain platforms may gradually adopt similar identity standards, data-sharing rules, audit procedures, and dispute-resolution protocols because cities, insurers, manufacturers, and users demand comparable assurances. This convergence may improve interoperability, but it may also reduce experimentation if governance templates become too rigid.

Sustainable supply chain research has argued that blockchain can support transparency and accountability across multi-party systems（Saberi et al., 2019）. In mobility governance, sustainability is not limited to emissions reduction. It also includes efficient use of underutilized vehicle resources, reduced duplication of roadside infrastructure, and improved resilience of mobility services. A decentralized vehicular resource market can reduce waste when idle vehicle resources are temporarily shared, but such sharing will not scale without institutional mechanisms that make participation safe and rewarding.

Legitimacy is particularly important when emerging technologies intervene in public mobility spaces. Organizations and platforms gain legitimacy when their actions are perceived as desirable, proper, and appropriate within socially constructed systems of norms and beliefs（Suchman, 1995）. Vehicular blockchain trading platforms need legitimacy from drivers, manufacturers, mobility service providers, city agencies, and data protection authorities. A purely technical security claim is unlikely to be enough if users view the incentive rules or data practices as opaque.

Blockchain research has emphasized decentralization, immutability, consensus, and smart contract automation as core design features（Lu, 2018）. From a governance perspective, these features should be interpreted as institutional instruments. Decentralization distributes authority, immutability creates accountability, consensus defines accepted truth, and smart contracts embed procedural rules. The question is not whether these features exist technically, but how they are designed to support stakeholder confidence and responsible adoption.

Transaction-cost economics suggests that governance structures are chosen to reduce uncertainty, opportunism, and coordination costs（Williamson, 1979）. Vehicular blockchain trading seeks to lower transaction costs in micro-resource markets where repeated bargaining would be inefficient. Smart contracts reduce negotiation cost, reputation records reduce screening cost, and automated settlement reduces enforcement cost. Yet the technology also creates new costs, including compliance verification, wallet management, data governance, and smart contract auditing.

Empirical studies of blockchain adoption in supply chains show that organizational readiness, perceived benefits, top management support, and partner pressure influence adoption decisions（Queiroz and Wamba, 2019）. Similar conditions apply to vehicular edge markets. A fleet operator will not adopt a blockchain trading system simply because it is decentralized. The operator must perceive economic value, risk reduction, integration compatibility, and legal clarity. Adoption is therefore a governance decision under uncertainty.

Polycentric governance provides a useful lens because smart mobility involves multiple centers of decision making rather than a single authority（Ostrom, 2010）. Vehicle manufacturers, municipalities, telecom operators, cloud providers, insurers, users, and regulators each control part of the system. A blockchain market that ignores this distributed authority may face resistance. A polycentric design, by contrast, can allocate responsibilities across local edge gateways, consortium validators, municipal oversight bodies, and market participants.

Blockchain research challenges include scalability, privacy, consensus efficiency, and governance of protocol changes（Lu, 2019）. These challenges are especially visible in vehicular environments because transactions may be frequent and time-sensitive. A governance model must decide which events require full on-chain

recording, which can be handled off-chain, how identity changes are managed, and who is responsible when consensus delays affect service quality.

3. Conceptual Framework: From Trading Network to Mobility Governance

Mobile edge computing research shows that low-latency computation near users can reduce the burden on centralized cloud systems（Mao et al., 2017）. Vehicular resource markets extend this logic by allowing vehicles themselves to contribute resources to nearby peers. The market becomes a hybrid infrastructure composed of vehicles, edge nodes, base stations, wallets, smart contracts, and governance rules. Figure 1 presents the conceptual transformation from a transaction-oriented trading network to a governance-oriented smart mobility system.

Systematic reviews of blockchain applications show that many successful use cases combine technical traceability with organizational coordination（Casino et al., 2019）. The proposed framework therefore contains six connected layers: the vehicle resource market, the blockchain trading layer, institutional governance, trust analytics, incentive design, and technology adoption. Each layer performs a different function. The market layer handles resource matching. The blockchain layer records and settles transactions. Governance defines rights and responsibilities. Trust analytics evaluates behavior. Incentives motivate honest participation. Adoption reflects stakeholder acceptance.

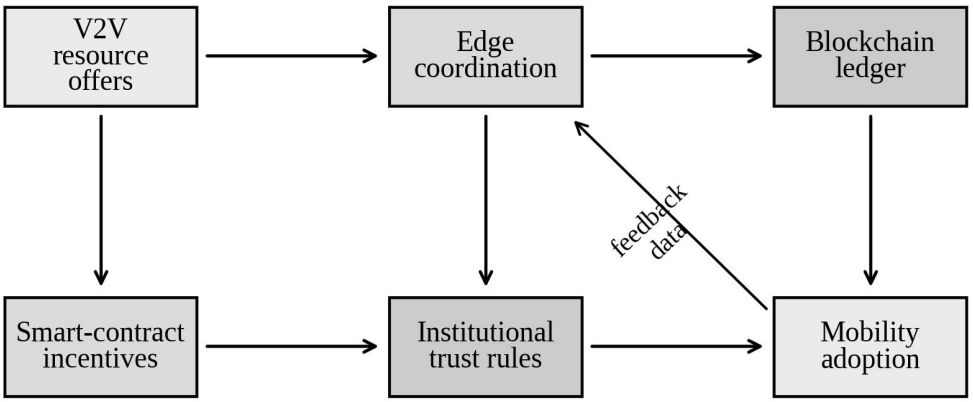

Figure 1. Governance-oriented framework for transforming vehicular blockchain trading into smart mobility governance.

Mobile edge computing has been described as a key technology for bringing computation and storage closer to connected devices（Hu et al., 2015）. In the proposed governance framework, the edge node has a dual role. It is both a technical coordinator and a governance intermediary. Technically, it verifies requests, identifies providers, and monitors service quality. Institutionally, it applies platform rules, filters low-trust nodes, records evidence, and triggers dispute processes when service terms are violated.

Blockchain technology has been recognized as a continuing research trend because it changes how distributed actors coordinate records, incentives, and trust（Zheng and Lu, 2022）. In vehicular markets, the ledger should

not be viewed as a replacement for institutions. Rather, it is an institutional memory that records exchanges, trust updates, and compliance events. The real governance question is how this memory is interpreted and how it affects future eligibility, pricing, and sanctions.

Edge computing research highlights the challenges of resource heterogeneity, mobility, and service latency （Shi et al., 2016）. These challenges produce governance problems. A resource provider may perform well under low traffic density but fail under congestion. A requester may provide unfair feedback after receiving service. A validator may become temporarily unavailable. A governance model must therefore combine automated analytics with institutional safeguards so that temporary performance variation is not confused with deliberate misconduct.

Blockchain for IoT security has been used to illustrate how distributed ledgers can support identity, access control, and privacy in device ecosystems（Dorri et al., 2017）. Vehicular blockchain trading requires similar but more dynamic identity governance. Vehicles need pseudonymous identities to limit tracking, but the platform must still prevent Sybil attacks and ensure accountability after disputes. This requires controlled pseudonymity: identities should be privacy-preserving during normal operation but auditable under legitimate governance procedures.

Mobile edge computing surveys emphasize architecture and computation offloading as core design concerns （Mach and Becvar, 2017）. The present article adds a governance interpretation: offloading is also a trust transfer. When a vehicle delegates a task to another node, it temporarily relies on that node's capability, honesty, availability, and compliance with contract terms. Institutional trust grows when repeated offloading exchanges are evaluated consistently and sanctions are applied predictably.

IoT cybersecurity research has shown that connected devices create broad attack surfaces across sensing, communication, and application layers （Lu and Xu, 2019）. In smart mobility, these risks become public because compromised vehicles and edge nodes may affect traffic safety, service reliability, and personal data. Governance must therefore include security certification, incident reporting, minimum encryption standards, and post-incident accountability rather than treating cybersecurity as a purely technical subsystem.

4. Research Design and Data Analytical Approach

This study develops a conceptual empirical design using simulated stakeholder data rather than direct field deployment. The goal is not to claim observed market behavior but to demonstrate how governance variables could be measured and analyzed in future pilots. The simulated dataset represents 420 stakeholders in a vehicular blockchain market, including private vehicle owners, fleet managers, mobility platform operators, edge infrastructure providers, municipal transport officers, and cybersecurity auditors. Each respondent is assigned scores on institutional trust, perceived incentive fairness, privacy assurance, regulatory clarity, operational fit, interoperability, and adoption readiness.

The design follows the logic that edge computing is becoming an operating model for distributed services rather than a single technical component（Satyanarayanan, 2017）. The simulated variables are measured on five-point Likert scales. Institutional trust measures confidence that rules are stable and fair. Incentive fairness measures whether pricing, rewards, and penalties are perceived as reasonable. Privacy assurance measures confidence that personal and vehicle data are protected. Regulatory clarity measures whether legal responsibility is understandable. Operational fit measures integration with existing mobility operations. Interoperability measures compatibility across vehicles, platforms, and edge networks.

A review of blockchain research in PLOS ONE identified privacy, scalability, consensus, and smart contract quality as recurrent research issues（Yli-Huumo et al., 2016）. These issues are translated here into governance constructs. Privacy becomes perceived privacy assurance. Scalability becomes operational fit and interoperability. Consensus quality becomes institutional trust. Smart contract quality becomes incentive fairness and accountability. The measurement design therefore links technical features to adoption-relevant governance perceptions.

Fog computing was introduced as a way to extend cloud services toward the network edge and support context-aware services（Bonomi et al., 2012）. In the present model, edge gateways are treated as semi-local governance nodes. They record transactions, aggregate QoS feedback, apply risk thresholds, and communicate with consortium validators. This design reflects the reality that smart mobility governance must be partly local because congestion, road conditions, and service availability differ across urban zones.

Table 1. Construct Definitions and Measurement Logic

Construct	Operational meaning	Example indicator
Institutional trust	Confidence that rules are stable, fair, and auditable	Trust in rule enforcement
Incentive fairness	Perceived fairness of payments, rewards, and penalties	Fairness of smart-contract pricing
Privacy assurance	Belief that identity and mobility data are protected	Confidence in pseudonym and data controls
Regulatory clarity	Understanding of legal responsibility and compliance duties	Clarity of liability after disputes
Operational fit	Compatibility with existing mobility operations	Ease of integrating resource trading
Adoption readiness	Willingness to participate in the platform	Intention to use or recommend the market

The 6G vision emphasizes intelligent, ultra-reliable, and highly connected digital infrastructure（Lu and Ning, 2020）. Vehicular blockchain markets can be understood as an early organizational layer for this vision. They convert connectivity into exchangeable resources and convert digital trust into operational coordination. Table 1 summarizes the operationalization of the key constructs used in the simulated analysis.

5. Data Analysis and Results

The Internet of Vehicles literature emphasizes layered architectures, network models, and future challenges for connected vehicular systems（Kaiwartya et al., 2016）. In this article, the analysis focuses on how stakeholders evaluate the institutional and economic conditions of such systems. The simulated descriptive results show that perceived security receives the highest mean score, while regulatory clarity receives the lowest score. This pattern suggests that stakeholders may accept the technical promise of blockchain before they fully trust the institutional environment surrounding it.

Blockchain supply chain frameworks show that distributed ledgers create value only when they are embedded in process redesign and governance alignment（Treiblmaier, 2018）. The same pattern appears in the simulated adoption model. Institutional trust has the strongest relationship with adoption readiness, followed by incentive fairness and privacy assurance. Technical interoperability matters, but it is not sufficient when users are uncertain about accountability and rule enforcement.

Security research on the Internet of Vehicles has emphasized architecture, protocols, and risk control

（Contreras-Castillo et al., 2017）. The trust trajectory simulation in Figure 2 shows how a governance platform can differentiate participants over time. Compliant providers gradually build trust. Non-compliant providers lose trust quickly after repeated failures. Variable providers remain in the middle and require additional monitoring. This pattern supports a governance design that rewards consistency but penalizes harmful behavior rapidly.

Table 2. Simulated Stakeholder Sample and Governance Scores

Stakeholder group	n	Institutional trust	Incentive fairness	Adoption readiness
Private vehicle owners	120	3.72	3.68	3.64
Fleet managers	80	3.96	3.82	3.88
Platform operators	70	4.18	4.05	4.12
Edge providers	55	3.84	3.74	3.79
Municipal officers	55	3.51	3.38	3.42
Cybersecurity auditors	40	4.22	3.91	3.85

Table 2 shows that platform operators and cybersecurity auditors report relatively high institutional trust, while municipal officers report lower adoption readiness. This difference suggests that actors closer to technical operations may recognize the benefits of blockchain more quickly, whereas public-sector actors may require clearer legal mandates and accountability procedures before endorsing deployment.

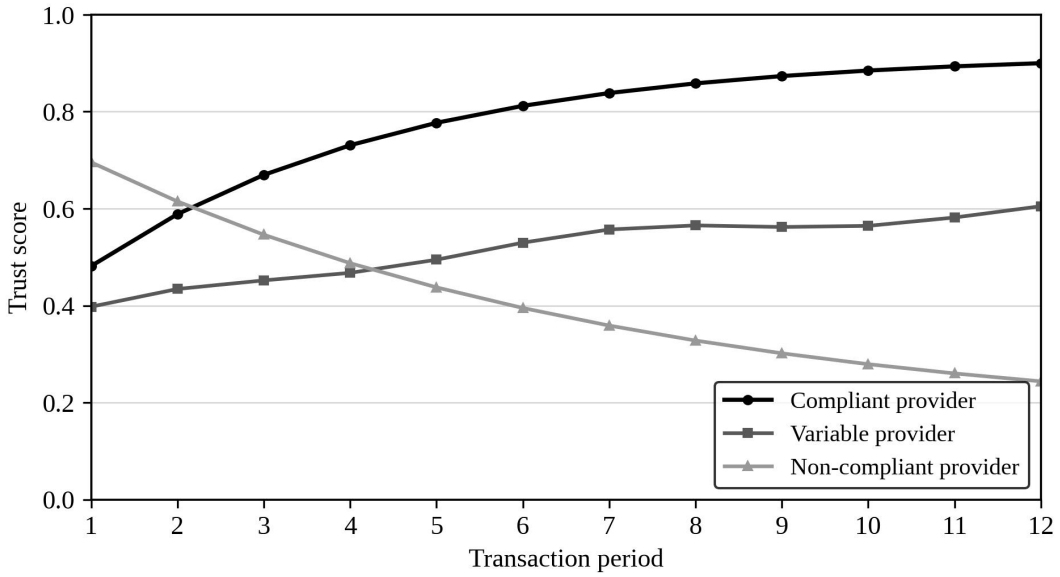

Figure 2. Simulated trust-score trajectories for compliant, variable, and non-compliant vehicular resource providers.

6G research stresses that future systems will integrate communication, computation, sensing, and intelligence across heterogeneous scenarios（Lu and Zheng, 2020）. Vehicular blockchain markets depend on exactly this integration. A vehicle's trust score should not be based only on whether a transaction occurred. It should combine latency, service duration, energy cost, user feedback, dispute status, and contextual risk. Figure 2 illustrates this logic through three simulated trust trajectories over twelve trading periods.

Smart mobility governance research warns that innovation without governance can produce fragmentation, exclusion, and accountability gaps（Docherty et al., 2018）. The adoption-readiness results in Figure 3 support

this warning. Regulatory clarity has the lowest mean score among the six factors, which suggests that users may hesitate even when security and economic incentives are attractive. In other words, regulatory uncertainty can become an adoption bottleneck.

The broader IoT literature shows that connected environments require coordination among devices, applications, network services, and data-management processes（Atzori et al., 2010）. For vehicular blockchain markets, this coordination must be translated into service-level rules. A platform should specify who can provide resources, what minimum performance is acceptable, how rewards are calculated, how complaints are reviewed, and how privacy-preserving identities are managed.

Transport governance scholars argue that policy should not treat mobility innovation as a purely technological process（Marsden and Reardon, 2017）. This insight is central to the proposed JTIS article. A decentralized trading platform still needs governance, and that governance must be legible to users. If smart contract terms are too complex or dispute pathways are unclear, the system may appear unfair even when its technical design is secure.

Industry 4.0 research connects cyber-physical systems, digital platforms, and intelligent decision-making（Lu, 2025）. Vehicular blockchain trading is part of this broader industrial transformation because it turns mobility resources into data-driven and contract-governed services. The system is not only a transportation application; it is an institutional experiment in distributed industrial coordination.

Smart urban mobility research has emphasized that smartness should be aligned with sustainability and social purpose（Lyons, 2018）. The implication for vehicular blockchain markets is that adoption metrics should include more than transaction speed. A platform should also be evaluated according to fairness, inclusiveness, privacy protection, infrastructure efficiency, and contribution to resilient mobility services.

IoT security surveys point to authentication, confidentiality, access control, and data integrity as foundational requirements（Alaba et al., 2017）. In the simulated model, privacy assurance and perceived security are treated as separate constructs. Security indicates whether attacks and manipulation are controlled. Privacy assurance indicates whether stakeholders believe their identities, locations, and transaction histories are not misused. The distinction matters because a system can be technically secure while still creating privacy anxiety.

Mobility-as-a-service research has questioned whether integrated platforms always serve public interest and social equity（Pangbourne et al., 2020）. A vehicular blockchain market raises similar questions. Resource-rich vehicles and large fleets may benefit more than occasional drivers if incentive rules are not carefully designed. Governance should therefore monitor whether rewards concentrate among powerful actors and whether small participants remain able to join the market.

Industry 4.0 research identifies interoperability, openness, and cyber-physical coordination as major open issues（Lu, 2017a）. The simulated path model in Figure 4 shows that interoperability has a positive but weaker direct effect on adoption than trust and incentive fairness. This result does not mean interoperability is unimportant. Rather, it suggests that technical compatibility is a baseline condition, while adoption decisions are strongly shaped by whether the system is viewed as trustworthy and fair.

Urban mobility research warns that smart mobility may be either an opportunity or a threat depending on how it is governed（Papa and Lauwers, 2015）. Blockchain-enabled vehicular trading has the same dual character. It can improve resource efficiency and transparency, but it can also create new exclusion, surveillance, and responsibility problems if governance is weak. The article therefore frames technology adoption as an institutional

outcome.

Security, privacy, and trust are closely linked in IoT networks because device interactions create vulnerabilities across technical and social layers（Sicari et al., 2015）. In the vehicular context, trust analytics should therefore be multidimensional. A high trust score should not only reflect successful delivery but also policy compliance, privacy-respecting behavior, and absence of suspicious identity patterns.

6. Incentive Design, Pricing Fairness, and Institutional Trust

Auction theory provides a useful foundation for incentive-compatible vehicular markets. Vickrey's sealed-bid auction logic shows that carefully designed payment rules can encourage truthful valuation reporting（Vickrey, 1961）. In the proposed governance model, auction-based pricing is interpreted not only as an efficiency tool but also as a legitimacy mechanism. Stakeholders are more likely to accept resource trading when pricing appears rule-based rather than arbitrary.

Cyber-physical systems research shows that Industry 4.0 environments require integration between physical operations and digital intelligence（Lu, 2017b）. In vehicular blockchain markets, the resource itself may be physical or computational, while the transaction is digital. This hybridity means that incentive rules must be tied to measurable service outcomes such as latency, task completion, availability, and response time.

Clarke's public-goods pricing logic further demonstrates how payment mechanisms can internalize social effects（Clarke, 1971）. In smart mobility, a resource allocation may affect not only the requester and provider but also surrounding traffic conditions, edge network load, and service continuity. Incentive design should therefore consider welfare beyond a single buyer-seller pair.

Distributed IoT security studies show that privacy and security challenges become more complex when devices are geographically dispersed and administratively heterogeneous（Roman et al., 2013）. Incentive systems must account for this heterogeneity. A uniform reward may not be fair if providers face different energy costs, connectivity risks, or regulatory obligations. Governance rules should permit contextual adjustment while retaining auditability.

Groves mechanisms demonstrate that truthful participation can be induced when payments are linked to the external effect of each participant's report（Groves, 1973）. Translating this logic into vehicular blockchain governance means that smart contracts should not simply reward winning providers. They should also discourage strategic exaggeration, fake availability, and malicious feedback by linking future trust and eligibility to observed service evidence.

Artificial intelligence research highlights the growing role of intelligent models in decision-making across digital systems（Lu, 2019b）. Trust analytics in vehicular markets can use AI to detect abnormal patterns, predict provider reliability, and recommend risk-adjusted prices. However, AI should not replace governance. Its outputs must be explainable enough for dispute resolution and accountable enough for institutional legitimacy.

Optimal auction design emphasizes that allocation rules and payment rules must be considered jointly（Myerson, 1981）. A vehicular market that selects the cheapest provider may reduce immediate cost but harm reliability. A governance-oriented auction should include trust, location, availability, resource quality, and privacy risk as decision variables. This broader design better aligns economic efficiency with safe smart mobility.

IoT research has highlighted many potential applications and challenges, including data management and

network heterogeneity（Miorandi et al., 2012）. In vehicular edge markets, these challenges influence pricing fairness. If one vehicle has better connectivity because of infrastructure advantage, the system should decide whether that advantage justifies higher rewards or whether pricing should also support balanced participation across less connected areas.

Algorithmic mechanism design connects computational feasibility with economic incentives（Nisan and Ronen, 2001）. This is critical because vehicular resource trades must be processed quickly. A theoretically ideal mechanism is insufficient if it cannot operate under mobility and latency constraints. Smart mobility governance must therefore balance truthfulness, computational speed, privacy, and transparency.

The state of artificial intelligence research suggests that model-based decision support is increasingly embedded in business and infrastructure systems（Zhang and Lu, 2021）. In the proposed framework, AI-based trust analytics provides the decision layer that links raw blockchain records to governance actions. For example, repeated late delivery may reduce a provider's score, but a context-aware model can distinguish congestion-related delay from deliberate underperformance.

Selfish routing theory shows that individually rational decisions can reduce system-wide welfare when actors do not internalize congestion effects（Roughgarden and Tardos, 2002）. Vehicular resource trading may face similar externalities. If many vehicles seek the same nearby provider, the platform may create local overload. Pricing and trust rules should therefore discourage behavior that is individually profitable but collectively inefficient.

Internet of Things legal research has noted that privacy and data protection concerns become sharper when physical-world data are continuously collected（Weber, 2010）. Vehicular blockchain trading creates location-sensitive and behavior-sensitive records. Governance must therefore define what data are stored on-chain, what data remain off-chain, and how long audit records should persist.

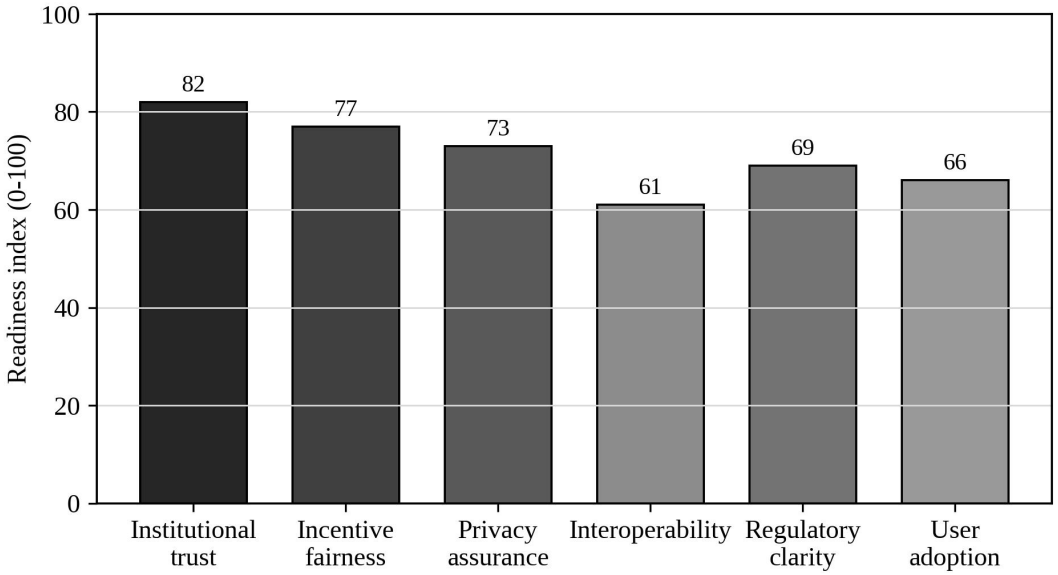

Figure 3. Simulated adoption-readiness factors in blockchain-enabled smart mobility governance.

7. Privacy Assurance and Data Governance

Differential privacy provides a mathematical foundation for limiting the disclosure risk associated with individual data contributions（Dwork, 2006）. In vehicular blockchain markets, privacy-preserving analytics can protect bids, locations, and behavior traces while still allowing the system to compute market-level indicators. This is especially important because mobility data can reveal home locations, work patterns, and personal routines.

Management analytics research shows that decision-making increasingly depends on structured data, models, and interpretive frameworks（Lu et al., 2024a）. A governance system for blockchain mobility should therefore develop dashboards that distinguish operational performance, institutional compliance, and adoption readiness. The ledger provides data, but analytics translates those records into governance intelligence.

The algorithmic foundations of differential privacy clarify that privacy protection requires explicit control over the probability that individual participation changes analytical outputs（Dwork and Roth, 2014）. A smart mobility platform can apply this principle when publishing aggregate trust statistics, regional service quality indicators, or market participation reports. The goal is to support transparency without exposing individual vehicle behavior.

Privacy-preserving machine learning research shows that models can be trained or evaluated while reducing exposure of sensitive data（Shokri and Shmatikov, 2015）. This approach is relevant when mobility platforms use AI to estimate trust or adoption propensity. If the training data include vehicle locations or transaction histories, the governance model should specify privacy-preserving model development practices.

Decision-making analytics research emphasizes that modern organizations need methods that connect data patterns to practical managerial action（Lu et al., 2024b）. For vehicular blockchain governance, this means trust scores should not be abstract numbers. They should feed into clear actions such as provider selection, additional verification, temporary suspension, reward adjustment, and dispute review.

Trust and technology acceptance research demonstrates that trust can mediate the relationship between system characteristics and adoption intentions（Gefen et al., 2003）. This finding supports the model proposed here: perceived security and privacy assurance do not influence adoption only directly. They also build institutional trust, which then increases willingness to participate in the platform.

FinTech research illustrates how digital platforms reshape trust, risk, and transaction governance in financial markets（Kou and Lu, 2025）. Vehicular blockchain markets share this platform logic because they convert temporary resource access into programmable micro-transactions. The difference is that mobility transactions occur in physical space and may interact with public safety, which raises the importance of regulatory clarity.

Mobile payment adoption research shows that perceived security, social influence, and convenience influence whether users recommend digital payment technologies（Oliveira et al., 2016）. Similar dynamics can be expected in vehicular resource trading. If drivers or fleet managers perceive the wallet, bidding, and settlement processes as inconvenient, they may avoid the platform even when economic rewards are available.

Decentralized finance research shows that distributed financial infrastructures can create new efficiencies while also raising governance and risk concerns（Xu et al., 2024）. A vehicular blockchain market is not DeFi, but it uses similar primitives: wallets, smart contracts, programmable payments, and decentralized validation. Lessons from DeFi suggest that transparency must be paired with risk controls and user protection.

Big data analytics research finds that firms benefit when they build dynamic capabilities around data interpretation and action（Wamba et al., 2017）. Mobility platforms should therefore treat blockchain records as

a strategic analytics resource. Transaction data can reveal underserved zones, unreliable provider categories, price volatility, and trust decay patterns. These insights can guide governance revision and infrastructure investment.

8. Technology Adoption and Stakeholder Implications

Blockchain-enabled auditing research demonstrates that distributed ledgers can improve assurance by making records more transparent and tamper-resistant（Wu et al., 2025）. In smart mobility governance, auditing is not limited to financial records. It includes service completion evidence, trust-score changes, validator behavior, and smart contract updates. An auditable market is more likely to gain acceptance from regulators and institutional users.

Digital transformation research stresses that technology changes organizational value creation, operational processes, and structural arrangements（Vial, 2019）. Vehicular blockchain trading would require similar transformation. Fleet operators may need new resource-sharing policies, manufacturers may need wallet integration, telecom operators may need edge service interfaces, and city agencies may need oversight dashboards.

QoS-based auction research is particularly relevant because vehicular resource markets must price quality as well as quantity（Lu et al., 2020）. A low-cost provider with unstable latency may be less valuable than a higher-cost provider with reliable performance. The governance model therefore recommends a trust-adjusted pricing rule in which QoS history influences future market opportunities.

Digital business strategy research argues that firms must integrate digital resources, organizational processes, and external ecosystems（Bharadwaj et al., 2013）. Smart mobility platforms follow this logic because they cannot be built by one actor alone. Adoption requires ecosystem alignment among vehicle manufacturers, platform operators, edge providers, municipal authorities, cybersecurity auditors, and users.

Digital innovation theory shows that digital artifacts are generative and can be recombined across contexts（Yoo et al., 2010）. A blockchain trading layer for vehicles may later support insurance pricing, carbon accounting, emergency service prioritization, parking-resource exchange, or logistics coordination. Governance should therefore be modular enough to support future services without compromising accountability.

Digital innovation management research emphasizes that innovation is increasingly distributed across ecosystems rather than contained within single firms（Nambisan et al., 2017）. This perspective supports a multi-stakeholder governance model. No single participant should define the rules alone because the effects of mobility resource trading cross organizational and public boundaries.

Quantum machine learning research illustrates how advanced computation may expand future decision-making capabilities（Lu et al., 2024c）. While the present article does not rely on quantum methods, it recognizes that future smart mobility governance may integrate more sophisticated optimization and analytics. The key challenge will remain institutional: advanced models must still be explainable, legitimate, and accountable.

Research on organizational change shows that leadership strongly influences how people respond to new technologies（Oreg and Berson, 2019）. In the context of smart mobility, platform sponsors and municipal leaders must communicate the value, limits, and responsibilities of blockchain trading. Without visible leadership support, stakeholders may interpret the system as a risky experiment rather than a trustworthy mobility innovation.

Quantum financing research shows that emerging technologies often create potential scenarios before stable

business models are established（Lu and Yang, 2024）. Vehicular blockchain trading is at a similar stage. It has plausible technical and economic benefits, but its business model depends on stakeholder adoption, governance clarity, and regulatory accommodation.

The duality of technology perspective argues that technologies both shape and are shaped by organizational practices（Orlikowski, 1992）. Smart mobility blockchain systems will therefore evolve as users interact with them. Trust rules, price thresholds, privacy settings, and dispute procedures may need revision after deployment. Governance should be designed as a learning process rather than a fixed protocol.

Quantum science trend research reminds us that emerging technological fields often require cross-disciplinary interpretation to become socially meaningful（Ye and Lu, 2022）. Vehicular blockchain trading similarly requires more than computer science. It involves economics, public administration, transport policy, data ethics, organizational behavior, and user acceptance research.

Information technology and organizational change research cautions against deterministic explanations of technology outcomes（Markus and Robey, 1988）. Blockchain will not automatically produce trustworthy smart mobility. Outcomes depend on governance choices, incentive design, stakeholder power, organizational routines, and regulatory response.

Ecosystem strategy research defines ecosystems as structured sets of partners that must align for value creation（Adner, 2017）. A vehicular blockchain market is an ecosystem because resource trading cannot succeed unless vehicles, edge gateways, validators, regulators, and users coordinate their roles. Failure in one role can reduce the value of the whole system.

Collaborative governance research shows that public and private actors can jointly solve complex problems when they build shared rules, trust, and facilitative leadership（Ansell and Gash, 2008）. This is a useful model for smart mobility. Public agencies can provide legitimacy and oversight, while private actors provide infrastructure, platforms, and innovation capacity.

Interorganizational value co-creation research demonstrates that technology vendors and partners jointly create value through ongoing relationships（Sarker et al., 2012）. Vehicular blockchain trading platforms should therefore be governed as co-created systems. Users, fleet operators, and edge providers should have channels to challenge rules, propose improvements, and participate in governance updates.

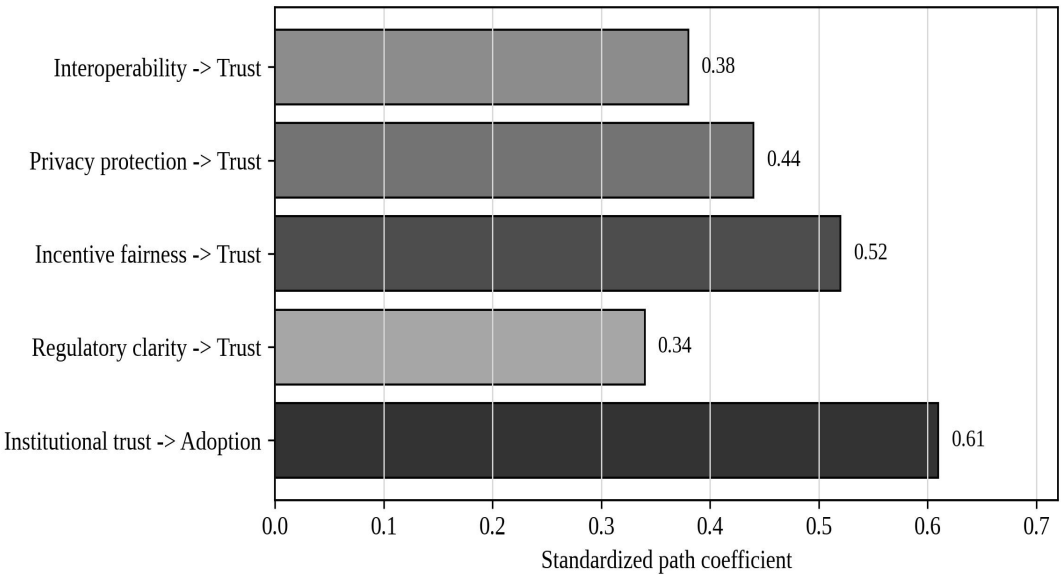

Figure 4. Simulated path coefficients linking governance factors to trust and technology adoption.

Table 3. Governance Implications for Smart Mobility Stakeholders

Stakeholder	Key concern	Recommended governance response
Vehicle owners	Privacy and reward fairness	Use pseudonymous identities and transparent reward rules
Fleet operators	Operational reliability	Apply trust-adjusted provider selection and service-level evidence
Platform operators	Scalability and legitimacy	Combine smart contracts with dispute governance
Municipal agencies	Public accountability	Require audit trails, liability rules, and safety reporting
Edge providers	Infrastructure cost recovery	Design fair pricing for low-latency resource coordination
Cybersecurity auditors	Attack resilience	Verify identity governance, access control, and incident response

9. Discussion

The findings suggest that vehicular blockchain trading should not be assessed only by throughput, latency, or attack resistance. These indicators remain important, but they do not explain whether stakeholders will adopt the system or whether it will be considered legitimate. Institutional trust is the central bridge between technical design and social acceptance. A blockchain ledger can reduce uncertainty, but institutional arrangements decide how ledger evidence is used, how disputes are resolved, and how rule changes are made.

The simulated analysis also shows that incentive fairness is a major adoption driver. Participants are unlikely to share resources if they believe rewards are too low, penalties are arbitrary, or large actors dominate market outcomes. Therefore, smart contracts should include transparent pricing logic, visible reward formulas, and explainable penalties. Trust analytics should be used cautiously because a low score may exclude participants from future opportunities. The platform should allow appeal and correction when a score is affected by contextual factors outside the provider's control.

Privacy assurance is another central concern. Vehicular markets generate sensitive data about movement, transaction history, vehicle capability, and service participation. Even if identities are pseudonymous, repeated patterns can create re-identification risk. The governance model therefore recommends layered data storage, with essential settlement evidence recorded on-chain and sensitive contextual data handled off-chain under privacy-preserving rules. Differential privacy and privacy-preserving learning can support aggregate analytics without revealing individual mobility behavior.

Regulatory clarity receives the weakest score in the simulated adoption data. This is important because smart mobility platforms operate in public spaces and may affect safety, liability, and access. A governance model should identify who is responsible when a service failure causes operational loss, when a smart contract executes incorrectly, when a malicious actor manipulates identity, or when a privacy breach occurs. Without such clarity, technical trust may not convert into institutional adoption.

The article also extends the original technical focus by proposing that edge gateways operate as governance intermediaries. They are not merely routing or computation nodes. They verify participation, apply eligibility thresholds, monitor QoS, coordinate dispute evidence, and communicate with validators. This interpretation makes the edge layer a site of institutional control and not just a network architecture.

For JTIS, the main theoretical contribution is the movement from blockchain trading to smart mobility governance. The original engineering logic emphasizes secure and incentive-compatible resource sharing. This article adds the social-technical logic of institutional trust, adoption readiness, privacy legitimacy, and stakeholder governance. It therefore positions blockchain-enabled vehicular resource trading as a technology innovation that must be socially organized before it can be broadly adopted.

For practitioners, the framework suggests a staged deployment strategy. A pilot should first define identity rules, data boundaries, and service-level indicators. It should then implement transparent incentive rules and trust-score updates. Next, it should evaluate stakeholder adoption readiness, especially among fleet managers and municipal agencies. Finally, it should revise governance based on observed disputes, user feedback, and trust-score behavior. This staged approach reduces the risk of deploying a technically secure but institutionally fragile platform.

For policymakers, the article suggests that regulation should not simply approve or reject blockchain mobility platforms. Instead, regulation should define minimum governance standards for identity assurance, privacy, auditability, dispute resolution, smart contract accountability, and data portability. Such standards would allow innovation while protecting users and public interest.

10. Conclusion

This article has developed a governance-oriented interpretation of blockchain-enabled vehicular resource trading. Building on the research direction of vehicular edge resource sharing, it reframes the technical trading network as a smart mobility governance system shaped by institutional trust, incentives, privacy assurance, regulatory clarity, and technology adoption. The article argues that blockchain creates a useful transactional foundation but does not automatically produce legitimate or widely adopted mobility services.

The proposed conceptual framework links six layers: vehicle resource markets, blockchain trading, institutional governance, trust analytics, incentive design, and adoption readiness. The simulated data analysis indicates that institutional trust and incentive fairness are stronger adoption drivers than purely technical interoperability. Privacy assurance and regulatory clarity are also critical because mobility data are sensitive and

public-facing services require accountability. The trust trajectory analysis demonstrates that dynamic trust scoring can distinguish compliant, variable, and non-compliant providers, but such scoring must remain explainable and contestable.

The study contributes to technology innovation and society research by showing how an engineering framework can be transformed into a governance research agenda. It also offers practical guidance for platform operators, transport authorities, and mobility service providers. Future empirical studies should test the proposed model using pilot deployment data, stakeholder surveys, transaction logs, and real trust-score histories. Further research should also examine legal liability, cross-border data governance, and the social equity effects of resource-sharing markets in smart mobility systems.

References

[1] Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

[2] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340. https://doi.org/10.2307/249008

[3] 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

[4] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478. https://doi.org/10.2307/30036540

[5] 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

[6] Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840-1920. Research in Organizational Behavior, 8, 53-111. https://doi.org/10.1016/B978-0-89232-601-7.50021-7

[7] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[8] North, D. C. (1991). Institutions. Journal of Economic Perspectives, 5(1), 97-112. https://doi.org/10.1257/jep.5.1.97

[9] 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

[10] DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147-160. https://doi.org/10.2307/2095101

[11] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

[12] Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, 20(3), 571-610. https://doi.org/10.5465/amr.1995.9508080331

[13] Lu, Y. (2018). 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

[14] Williamson, O. E. (1979). Transaction-cost economics: The governance of contractual relations. Journal of Law and Economics, 22(2), 233-261. https://doi.org/10.1086/466942

[15] Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of

the main drivers in India and the USA. International Journal of Information Management, 46, 70-82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

[16] Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. American Economic Review, 100(3), 641-672. https://doi.org/10.1257/aer.100.3.641

[17] 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

[18] Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 19(4), 2322-2358. https://doi.org/10.1109/COMST.2017.2745201

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

[20] Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile edge computing: A key technology towards 5G. ETSI White Paper, 11, 1-16. https://doi.org/10.1007/s11036-015-0581-1

[21] 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

[22] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. D. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

[23] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. Proceedings of IEEE PerCom Workshops, 618-623. https://doi.org/10.1109/PERCOMW.2017.7917634

[24] Mach, P., & Becvar, Z. (2017). Mobile edge computing: A survey on architecture and computation offloading. IEEE Communications Surveys & Tutorials, 19(3), 1628-1656. https://doi.org/10.1109/COMST.2017.2682318

[25] Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

[26] Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30-39. https://doi.org/10.1109/MC.2017.9

[27] 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

[28] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 13-16. https://doi.org/10.1145/2342509.2342513

[29] Lu, Y., & Ning, X. (2020). A vision of 6G-5G's successor. Journal of Management Analytics, 7(3), 301-320. https://doi.org/10.1080/23270012.2020.1802622

[30] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of Vehicles: Motivation, layered architecture, network model, challenges, and future aspects. IEEE Access, 4, 5356-5373. https://doi.org/10.1109/ACCESS.2016.2603219

[31] Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management, 23(6), 545-559. https://doi.org/10.1108/SCM-05-2018-0195

[32] Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibanez, J. A. (2017). Internet of Vehicles: Architecture, protocols, and security. IEEE Internet of Things Journal, 5(5), 3701-3709. https://doi.org/10.1109/JIOT.2017.2690902

[33] Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. https://doi.org/10.1016/j.jii.2020.100158

[34] Docherty, I., Marsden, G., & Anable, J. (2018). The governance of smart mobility. Transportation Research Part A, 115, 114-125. https://doi.org/10.1016/j.tra.2017.09.012

[35] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[36] Marsden, G., & Reardon, L. (2017). Questions of governance: Rethinking the study of transportation policy. Transportation Research Part A, 101, 238-251. https://doi.org/10.1016/j.tra.2017.05.008

[37] Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

[38] Lyons, G. (2018). Getting smart about urban mobility: Aligning the paradigms of smart and sustainable. Transportation Research Part A, 115, 4-14. https://doi.org/10.1016/j.tra.2016.12.001

[39] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

[40] Pangbourne, K., Mladenovic, M. N., Stead, D., & Milakis, D. (2020). Questioning mobility as a service: Unanticipated implications for society and governance. Transportation Research Part A, 131, 35-49. https://doi.org/10.1016/j.tra.2019.09.033

[41] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

[42] Papa, E., & Lauwers, D. (2015). Smart mobility: Opportunity or threat to innovate places and cities? Transportation Research Procedia, 10, 543-550. https://doi.org/10.1016/j.trpro.2015.09.090

[43] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[44] Vickrey, W. (1961). Counterspeculation, auctions, and competitive sealed tenders. Journal of Finance, 16(1), 8-37. https://doi.org/10.2307/2977633

[45] Lu, Y. (2017). Cyber physical system (CPS)-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. https://doi.org/10.1142/S2424862217500142

[46] Clarke, E. H. (1971). Multipart pricing of public goods. Public Choice, 11(1), 17-33. https://doi.org/10.1007/BF01726210

[47] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018

[48] Groves, T. (1973). Incentives in teams. Econometrica, 41(4), 617-631. https://doi.org/10.2307/1914085

[49] Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

[50] Myerson, R. B. (1981). Optimal auction design. Mathematics of Operations Research, 6(1), 58-73. https://doi.org/10.1287/moor.6.1.58

[51] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016

[52] Nisan, N., & Ronen, A. (2001). Algorithmic mechanism design. Games and Economic Behavior, 35(1-2), 166-196.

https://doi.org/10.1006/game.1999.0790

[53] Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

[54] Roughgarden, T., & Tardos, E. (2002). How bad is selfish routing? Journal of the ACM, 49(2), 236-259. https://doi.org/10.1145/506147.506153

[55] Weber, R. H. (2010). Internet of Things: New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

[56] Dwork, C. (2006). Differential privacy. In Automata, Languages and Programming (pp. 1-12). Springer. https://doi.org/10.1007/11787006_1

[57] Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

[58] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407. https://doi.org/10.1561/0400000042

[59] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310-1321. https://doi.org/10.1145/2810103.2813687

[60] Lu, Y., Pisarenko, Z. V., Yang, L., & Ye, C. (2024). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

[61] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51-90. https://doi.org/10.2307/30036519

[62] Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

[63] Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Computers in Human Behavior, 61, 404-414. https://doi.org/10.1016/j.chb.2016.03.030

[64] Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. https://doi.org/10.1080/17517575.2024.2397630

[65] Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

[66] Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003. https://doi.org/10.1080/17517575.2024.2448003

[67] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

[68] Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334-351. https://doi.org/10.1080/17517575.2019.1669827

[69] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471-482. https://doi.org/10.25300/MISQ/2013/37.2.3

[70] Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary: The new organizing logic of digital innovation. Information Systems Research, 21(4), 724-735. https://doi.org/10.1287/isre.1100.0322

[71] Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. MIS Quarterly, 41(1), 223-238. https://doi.org/10.25300/MISQ/2017/41.1.03

[72] Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

[73] Oreg, S., & Berson, Y. (2019). Leaders' impact on organizational change: Bridging theoretical and methodological chasms. Academy of Management Annals, 13(1), 272-307. https://doi.org/10.5465/annals.2016.0138

[74] Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

[75] Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. Organization Science, 3(3), 398-427. https://doi.org/10.1287/orsc.3.3.398

[76] Ye, Z., & Lu, Y. (2022). Quantum science: A review and current research trends. Journal of Management Analytics, 9(3), 383-402. https://doi.org/10.1080/23270012.2022.2089064

[77] Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. Management Science, 34(5), 583-598. https://doi.org/10.1287/mnsc.34.5.583

[78] Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39-58. https://doi.org/10.1177/0149206316678451

[79] Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543-571. https://doi.org/10.1093/jopart/mum032

[80] Sarker, S., Sarker, S., Sahaym, A., & Bjorn-Andersen, N. (2012). Exploring value cocreation in relationships between an ERP vendor and its partners. MIS Quarterly, 36(1), 317-338. https://doi.org/10.2307/41410419