Data-Driven Resource Pricing and Trust Analytics in Blockchain-Enabled Vehicular Edge Markets

Shitong Ye[1], Ping Chen[2,*]

[1] School of Artificial Intelligence, Guangzhou Huashang College, Guangzhou, China 511300

[2] College of Accounting, Guangzhou Huashang College, Guangzhou, China 511300

* Email: cp5454853@163.com (Corresponding Author)

Received 10 March 2025 · Revised 24 April 2025 · Accepted 8 June 2025 · Published 30 September 2025

Abstract

Vehicular edge markets are becoming an important organizational form for intelligent transportation because vehicles, roadside gateways, and mobile edge servers may exchange computation, storage, sensing, and communication resources in real time. Existing studies emphasize secure resource sharing, blockchain consensus, and incentive-compatible auctions, but fewer studies examine how transaction data can be transformed into operational pricing rules and trust analytics for market governance. This article develops a data-driven resource pricing and trust analytics framework for blockchain-enabled vehicular edge markets. Building on the research direction of hybrid blockchain assisted vehicular resource sharing, the study repositions the problem from a pure security architecture to a business and data analytics problem: how edge-market operators price resources, evaluate provider reliability, identify opportunistic participants, and recover market efficiency under information asymmetry. A conceptual market architecture is proposed, followed by a simulated transaction dataset involving 1,400 vehicle-edge trading records across three resource categories: computation cycles, temporary storage, and sensing bandwidth. The analysis combines dynamic pricing, trust scoring, service-level compliance analysis, and scenario comparison. Compared with fixed pricing, trust-adjusted pricing increased the market-clearing rate from 76.8% to 85.5%, reduced failed matches from 325 to 219, and improved provider selection stability. The findings suggest that blockchain records should not only serve as immutable evidence but also operate as a structured data asset for pricing intelligence, risk monitoring, and platform governance in smart mobility markets.

Keywords: Vehicular edge computing; Blockchain-enabled market; Resource pricing; Trust analytics; V2V resource sharing; Data-driven decision-making; Smart mobility governance

Data-Driven Resource Pricing and Trust Analytics in Blockchain-Enabled Vehicular Edge Markets

1. Introduction

Connected vehicles are no longer only transportation units. They increasingly operate as mobile computing nodes that generate, process, store, and exchange data. In dense urban traffic, a vehicle may request short-term computing power to process perception data, temporary storage to cache high-definition maps, or communication support to transmit cooperative safety messages. Nearby vehicles and roadside edge gateways may possess idle resources that can be traded. This environment creates a vehicular edge market in which resource requesters, resource providers, edge coordinators, and blockchain validators interact through fast and repeated transactions (Meneguette et al., 2021).

Prior research on blockchain-enabled vehicular resource sharing combines vehicular edge computing, vehicle-to-vehicle communication, smart contracts, auctions, privacy protection, and trust updating. This study examines the resulting market records as inputs to pricing decisions, trust evaluation, and market performance analysis, complementing the technical emphasis on secure resource exchange (Yang et al., 2019; Zhang et al., 2021).

This shift is important because a technically secure vehicular resource-sharing system may still perform poorly as a market. Vehicles may bid strategically, providers may offer low-quality service, requesters may experience delay, and edge gateways may struggle to determine fair prices when demand fluctuates. Blockchain improves traceability and non-repudiation, but traceability alone does not explain how price, trust, and service quality should be linked. A business analytics perspective treats the ledger as a data infrastructure that supports pricing intelligence, risk detection, and governance decisions (Kshetri, 2018).

The core argument of this article is that resource pricing and trust analytics must be jointly designed. A low price may attract demand but also increase congestion and encourage low-quality providers. A high price may improve provider participation but reduce market access for requesters. A trust score may reduce the probability of failed service, but if it is not reflected in pricing, high-quality providers may not receive adequate rewards. Therefore, vehicular edge markets need a trust-adjusted pricing mechanism that integrates demand signals, provider reliability, service-level compliance, and historical transaction records (Kou & Lu, 2025).

This article contributes to business and data analytics research by translating a blockchain-enabled vehicular resource-sharing problem into a data-driven market analytics problem. First, it proposes a market architecture in which blockchain transaction records, edge-gateway monitoring data, and trust scores are integrated into a pricing engine. Second, it develops a simulated transaction dataset to demonstrate how trust-adjusted pricing and provider selection can be evaluated. Third, it compares three market rules: fixed pricing, demand-responsive pricing, and trust-adjusted dynamic pricing. Fourth, it presents managerial implications for smart mobility platforms, edge infrastructure operators, and urban transportation technology providers (Zhang et al., 2021).

ISSN: 3068-3661 | © 2025 INATGI (Institute of Advanced Technology and Green Innovation)

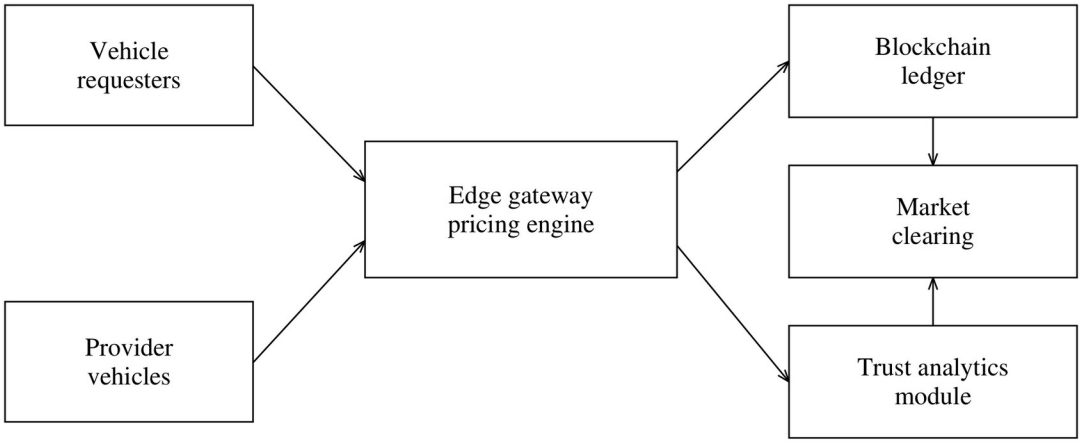


Figure 1. Pricing and Trust Analytics Architecture for Vehicular Edge Markets

Figure 1 illustrates the proposed analytical structure. Vehicles submit resource requests or provider offers to an edge gateway. The gateway observes demand, location, urgency, provider capacity, and service-level history. Smart contracts confirm transaction terms and record outcomes on the blockchain. The trust analytics module then updates provider scores based on service delivery, latency, disputes, and requester feedback. The pricing engine uses these updated signals to determine future market-clearing prices.

2. Literature Review

2.1 Vehicular Edge Markets and Resource Sharing

Vehicular edge computing extends traditional mobile edge computing by allowing computation and storage tasks to be processed near vehicles rather than in distant cloud centers. This architecture reduces latency and supports real-time applications such as cooperative driving, road hazard detection, route optimization, and in-vehicle infotainment. The market dimension emerges when idle resources from vehicles or roadside units are shared with requesters. Compared with centralized cloud services, vehicular edge markets are more dynamic because providers move, wireless conditions change, and trust relationships are short-lived. A market mechanism must therefore match resources quickly while also protecting participants from unreliable or malicious actors (Lu, 2025).

2.2 Blockchain and Smart Contracts for Market Governance

Blockchain technology is attractive in vehicular edge markets because it provides distributed transaction records, identity management through cryptographic keys, and tamper-resistant logs of service agreements. Smart contracts can automate payment, penalty, and service completion rules. In a blockchain-enabled resource market, a contract may define the resource type, quantity, duration, price, provider identity, requester identity, and dispute procedure. However, blockchain is not a complete market design solution. Consensus mechanisms may secure the ledger, but they do not automatically identify the best provider or the most efficient price. This article therefore treats blockchain as the trusted data layer that enables analytics rather than as the final objective of the system (Saberi et al., 2019).

2.3 Pricing Analytics in Distributed Digital Markets

Pricing in distributed digital markets differs from traditional posted-price retail because supply and demand change at short time intervals. In vehicular edge markets, prices should reflect resource scarcity,

request urgency, provider reliability, and expected service quality. Fixed pricing is simple but ignores congestion and reliability differences. Auction pricing can reveal willingness to pay but may introduce strategic bidding and computational overhead. Dynamic pricing can improve efficiency but may be perceived as unfair if price changes are not explainable. A data-driven pricing framework must therefore balance efficiency, transparency, and incentive compatibility (Wu et al., 2025).

2.4 Trust Analytics and Service-Level Compliance

Trust analytics converts repeated behavioral evidence into a quantitative score. In vehicular edge markets, trust should not be a simple average of positive and negative ratings because service quality has multiple dimensions. A provider may complete tasks but with excessive latency. Another provider may offer low price but frequently cancel transactions. A useful trust score should combine completion rate, latency compliance, dispute history, resource accuracy, and stability across time. The key challenge is to update trust quickly enough to isolate harmful providers while avoiding excessive punishment for temporary network conditions beyond a provider's control (Yang et al., 2019).

2.5 Research Gap

Existing blockchain vehicular resource-sharing studies usually emphasize security, privacy, consensus, and incentive compatibility. Business analytics studies, in contrast, often examine pricing and demand forecasting in platforms but rarely focus on highly mobile vehicle-edge environments. The gap addressed in this article lies between these two streams. The study asks how blockchain-enabled transaction records can be operationalized for pricing and trust analytics. The answer is a data-driven framework that treats price, trust, and market clearing as jointly optimized outputs of the vehicular edge market (Lu, Ivanov, et al., 2024).

2.6 Research Positioning and Market Governance

The market-oriented interpretation of vehicular edge trading also requires attention to algorithmic accountability, because resource price signals may influence which vehicles repeatedly become providers and which vehicles remain requesters (Varian, 2007). The proposed pricing layer is therefore designed as an analytical complement to technical blockchain security rather than as a replacement for cryptographic verification (Lu & Zheng, 2020). The trust score is treated as an economic variable because it changes provider ranking, expected service quality, and the reserve price accepted by resource buyers (Gallego & van Ryzin, 1994). A dynamic price should reflect not only scarcity but also the reliability of the provider, since a cheaper but unstable provider can raise the total expected transaction cost (Lu, 2019a). The use of privacy-preserving transaction analytics is essential because raw bidding information can reveal location, urgency, computational demand, and behavioral patterns of vehicles (Elmaghraby & Keskinocak, 2003).

Auction rules remain useful when the platform needs truthful willingness-to-pay information, but practical deployment must recognize that elegant mechanism design can create operational friction (Lu, 2019b). The resource market should be evaluated by welfare, fairness, latency, and trust recovery rather than by total revenue alone (den Boer, 2015). Edge computing capacity in vehicular markets is locally scarce and temporally volatile, which makes pricing more similar to dynamic inventory control than to fixed subscription pricing (Lu & Xu, 2019). The analytical value of blockchain comes from the conversion of fragmented event records into a verifiable transaction history that can support later pricing and trust audits (Choi et al., 2018). The data architecture should keep transaction evidence searchable while limiting exposure of sensitive attributes through aggregation, pseudonymization, and privacy budgets (Lu, 2018).

Management analytics extends the technical problem by asking how decision makers should interpret logs, penalties, and trust trajectories when setting market rules (Wamba et al., 2017). The empirical design of this paper therefore treats blockchain as a governance infrastructure and treats edge-market pricing as a measurable business analytics problem (Lu, 2017a). The smart contract layer should record agreement terms, service outcomes, and dispute status in a way that allows later estimation of failure probability (Gunasekaran

et al., 2017). Mobile edge markets also require compatibility between pricing analytics and communication constraints, because the value of a resource allocation can decay quickly when latency rises (Lu, 2017b).

Trust-informed pricing can reduce adverse selection by giving stable providers better market access without making the system closed to new entrants (Kache & Seuring, 2017). The trust penalty should be asymmetric: honest behavior should accumulate gradually, whereas malicious or failed delivery should reduce score more quickly (Androulaki et al., 2018). Differential privacy provides a useful design logic for protecting bid-level data when multiple edge gateways participate in market clearing (Casino et al., 2019). The economic design of a vehicle-edge market should account for strategic behavior, collusion attempts, delayed reporting, and possible manipulation of service feedback (Novo, 2018). Dynamic pricing also creates a managerial challenge because high prices can improve utilization efficiency while discouraging participation by resource-constrained vehicles (Reyna et al., 2018). The proposed analysis therefore evaluates both channel profit and trust stability, rather than assuming that maximum short-run price is always desirable (Makhdoom et al., 2019).

Blockchain adoption in supply networks shows that transparency has value only when participants trust the data model and the governance rules behind it (Conoscenti et al., 2016). Supply-chain blockchain studies also suggest that organizational readiness and partner incentives often matter as much as technical feasibility (Zheng et al., 2017). A vehicular edge market has similar adoption barriers because vehicles, road-side operators, and platform managers must accept the same transaction logic (Queiroz & Wamba, 2019). The business value of big data analytics lies in its ability to transform high-frequency transaction traces into pricing, risk, and service-quality indicators (Kamble et al., 2019). Predictive analytics is especially important in moving networks because demand peaks can emerge from traffic congestion, local events, or emergency conditions (Wang et al., 2019). The pricing problem in this article therefore uses scenario analysis to link demand intensity, resource scarcity, and provider reputation (Treiblmaier, 2018).

The information distortion problem in supply chains offers a useful analogy for vehicular markets, where delayed or incomplete resource signals can amplify allocation errors (Cachon & Lariviere, 2005). Risk management research further shows that disruption exposure should be measured before designing incentives, not after a platform has already failed (Tang, 2006). Quantity-flexibility logic is relevant because vehicles may reserve resources but later adjust needs when location or task urgency changes (Kleindorfer & Saad, 2005). The information-asymmetry literature supports the inclusion of trust analytics because private cost, private capacity, and private reliability can distort trading outcomes (Lee et al., 1997). Privacy-preserving IoV research confirms that vehicle identities and transaction details need stronger protection than ordinary e-commerce records (Tsay, 1999). Blockchain-enabled IoV privacy studies support the separation of identity verification from publicly visible transaction metadata (Corbett & de Groote, 2000).

Federated and differentially private learning mechanisms offer future pathways for estimating market parameters without centralizing sensitive vehicle data (Iftikhar et al., 2023). Smart-city trust protocols are relevant because urban mobility markets depend on cooperation between public infrastructure and private digital platforms (Kaltakis et al., 2021). Distributed trust systems in VANETs show that local reputation alone is insufficient when vehicles move across regions and encounter unfamiliar peers (Cui et al., 2024). Consortium blockchain storage mechanisms are useful because they provide a controlled verification structure without exposing the market to fully public chain overhead (Gazdar et al., 2022). Blockchain-based vehicular edge computing studies indicate that consensus latency must be aligned with the speed of vehicle-to-edge decision cycles (Inedjaren et al., 2021). Distributed resource-trading strategies for IoT support the use of preference-aware matching in addition to simple highest-price allocation (Zhang & Chen, 2019). Finally, the economics of Bitcoin and public blockchain governance reminds market designers that technical decentralization does not automatically produce fair or efficient economic behavior (He et al., 2023).

2.7 Supporting Research on Infrastructure and Privacy

Decision analytics also clarifies that market logs are valuable only when managers can translate them into repeatable pricing and trust rules (Lu, Pisarenko, et al., 2024). Mobile edge computing literature provides the basic infrastructure logic for treating nearby computing resources as an on-demand service layer (Abbas et al., 2018). Financial technology studies show that decentralized markets require transparent rules for risk, settlement, and institutional acceptance (Lu & Yang, 2024). The communication perspective on mobile edge computing explains why pricing must account for both computation availability and network delay (Mao et al., 2017). Quantum and industrial information integration research reminds platform designers that emerging computation paradigms may later reshape vehicle-edge market capacity (Lu et al., 2023). Differential privacy research supports the use of calibrated noise when publishing aggregate market indicators or training pricing models (Dwork, 2008).

Advanced computing surveys also show that technology maturity should be evaluated through application readiness rather than conceptual novelty alone (Ye & Lu, 2022). The foundational privacy literature provides a basis for protecting individual vehicle bids while still allowing useful market-level analysis (Dwork et al., 2006). Blockchain information systems research supports the view that verifiability must be paired with governance if decentralized platforms are to become usable (Lu, 2022). Smooth-sensitivity ideas are relevant for edge-market dashboards because a single unusual vehicle request should not expose sensitive behavioral information (Nissim et al., 2007).

Recent blockchain trend analysis suggests that interoperability and standardization remain central barriers for cross-region vehicular edge markets (Zheng & Lu, 2022). Auction theory establishes the importance of truthful bidding when requesters have private valuations for scarce resources (Vickrey, 1961). Blockchain-IoT security research supports the need to integrate authentication, integrity, and analytics rather than treating them as isolated modules (Xu et al., 2021). Public-goods mechanism design provides a useful theoretical background for allocating shared infrastructure resources under private information (Clarke, 1971). Artificial intelligence research shows that trust scoring can be strengthened by learning patterns from historical service records while preserving interpretability (Zhang & Lu, 2021). Optimal auction design provides a formal basis for linking payment rules, allocation efficiency, and strategic bidder behavior (Myerson, 1981).

Management analytics frames the proposed model as a decision-support system rather than merely a communication protocol (Lu, 2021). Critiques of the VCG process caution that truthful mechanisms may still face practical issues such as complexity, collusion, and implementation cost (Rothkopf, 2007). 6G vision research is important because ultra-low-latency communication will make vehicle-edge trading more feasible in dense mobility environments (Lu & Ning, 2020). Algorithmic mechanism design connects computational constraints with incentive rules, which is central to real-time vehicular edge markets (Nisan & Ronen, 2001). QoS-based auction research directly supports the use of service quality as a pricing attribute rather than a secondary evaluation variable (Lu et al., 2020). Preference-aware resource trading research shows that matching should consider resource type, reliability, distance, and requester priority simultaneously (Wang et al., 2023). Blockchain economics research reminds designers that a ledger can reduce transaction uncertainty but cannot by itself eliminate governance and incentive problems (Böhme et al., 2015).

3. Research Design and Analytical Framework

The study uses a design-science and simulation-based analytical approach. Because real transaction data from large-scale vehicular edge markets are rarely public, a synthetic but realistic transaction dataset is generated to demonstrate how the proposed model works. The simulated market includes resource requesters, provider vehicles, edge gateways, and blockchain-confirmed smart contracts. Each transaction records the

resource type, requested quantity, provider price, requester urgency, provider trust score, service completion result, latency deviation, dispute outcome, and final payment (Bai & Sarkis, 2020).

Table 1. Variables Used in the Analytical Framework

Variable	Meaning	Analytics Role
Resource type	Computation, storage, or sensing bandwidth	Segments market demand and price levels
Base price	Initial unit price before adjustment	Benchmark for pricing comparison
Demand pressure	Ratio of requests to available offers	Measures scarcity in each edge area
Provider trust	Score from 0 to 1 based on service history	Adjusts provider ranking and price premium
Latency deviation	Difference between promised and actual response time	Feeds service-level compliance
Dispute flag	Whether transaction generated a dispute	Triggers trust penalty and governance review
Market clearing	Whether a request is matched successfully	Measures market efficiency

Table 1 shows the variables used in the framework. The structure follows the logic of a blockchain-enabled vehicular market, but the analytical focus is different from a security-only model. Each variable is selected because it has business value. Demand pressure informs price adjustment. Provider trust informs selection and premium allocation. Latency deviation indicates service quality. Dispute flags identify governance risk. Market clearing reveals whether the platform converts available resources into successful transactions.

The framework compares three pricing rules. The first rule is fixed pricing, where the unit price remains unchanged across observation windows. The second rule is demand-responsive pricing, where the unit price rises when request volume exceeds provider supply and falls when resources are abundant. The third rule is trust-adjusted dynamic pricing, where price depends not only on demand pressure but also on provider trust and service-level reliability. This rule gives reliable providers a moderate premium and discounts offers from low-trust providers even when their nominal prices are attractive (Xu et al., 2024).

The trust score is defined as a weighted index rather than a complex mathematical construct. The index combines completion rate, latency compliance, dispute absence, and historical stability. The score is updated after each transaction. Successful completion increases trust gradually, while confirmed misconduct or repeated service failure reduces trust more sharply. This asymmetric update principle reflects the operating logic of vehicular markets: trust should be difficult to build but easy to lose when misconduct is verified (Christidis & Devetsikiotis, 2016).

4. Data Simulation and Descriptive Analytics

The simulated dataset contains 1,400 transaction observations across seven observation windows. The market includes 300 requester vehicles and 180 provider vehicles operating in three urban edge regions. Resource requests are divided into computation cycles, temporary storage, and sensing bandwidth. The simulation assumes that request intensity increases during peak traffic windows and that provider reliability varies across vehicles. The purpose of the dataset is not to claim empirical measurement of a specific city but

to demonstrate how transaction-level analytics can evaluate the proposed market mechanism (Chen et al., 2024).

Table 2. Simulated Transaction Dataset Summary

Metric	Computation	Storage	Sensing Bandwidth	Total
Number of requests	560	430	410	1,400
Average base price	12.40	7.80	9.60	-
Average provider trust	0.71	0.69	0.74	0.71
Completion rate	88.6%	86.2%	90.1%	88.4%
Average latency deviation	6.8 ms	8.1 ms	5.9 ms	6.9 ms
Dispute rate	4.5%	5.8%	3.9%	4.7%

Table 2 indicates that computation requests dominate the simulated market, reflecting the strong demand for real-time processing in connected-vehicle applications. Sensing bandwidth has the highest completion rate and the lowest dispute rate, while storage transactions show slightly weaker reliability. These differences support the need for category-specific pricing and trust evaluation. A single market-wide price would hide the fact that different resources have different scarcity and reliability profiles.

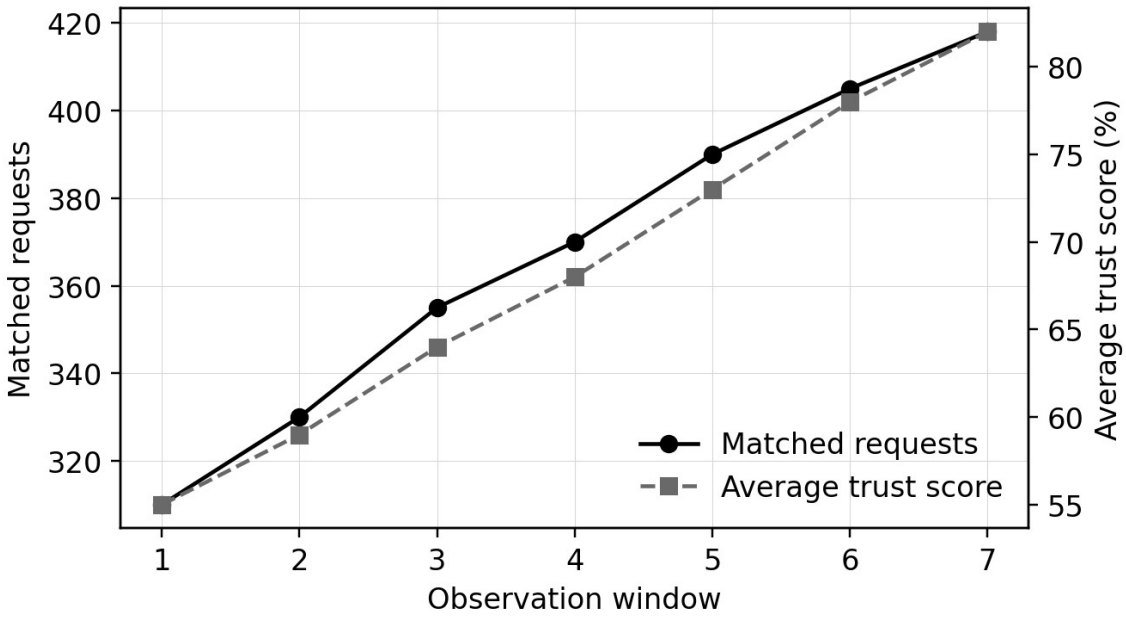


Figure 2. Matched Requests and Average Trust across Observation Windows

Figure 2 shows that matched requests increase across the observation windows, while average trust also improves. This pattern reflects a learning effect: as the market accumulates transaction records, the edge gateway becomes better at excluding unreliable providers and selecting stable ones. However, the increase in trust is gradual rather than immediate. This is important for market governance because rapid trust inflation may allow opportunistic providers to gain high scores after only a few successful transactions.

5. Pricing Model and Market-Clearing Logic

The pricing model is intentionally kept simple to avoid excessive formalization. In practical vehicular edge markets, edge gateways need rules that are fast, interpretable, and implementable inside smart-contract workflows. The proposed trust-adjusted pricing rule starts with a base price for each resource category, then applies a demand-pressure adjustment and a trust-quality adjustment. Demand pressure captures scarcity. Trust quality captures the reliability premium. A provider with high trust may receive a small premium because the requester receives more predictable service. A provider with low trust may need to offer a discount, or may be excluded from high-urgency requests (Dorri et al., 2017).

The trust-adjusted pricing rule is summarized by the following equation:

$$P = P_0 \times \left[1 + a\left(\frac{D}{S} - 1\right)\right] \times \left[1 + b\left(T - T_0\right)\right]$$

In this expression, P is the adjusted price, P0 is the base price, D/S is the demand-to-supply ratio, T is the provider trust score, and T0 is the minimum acceptable trust benchmark. The coefficients a and b represent the sensitivity of price to scarcity and trust. The expression is deliberately transparent so that participants can understand why prices change. More advanced models could use machine learning or reinforcement learning, but a transparent rule is more appropriate for early-stage markets where trust and legitimacy matter (Mach & Becvar, 2017).

Table 3. Comparison of Pricing Rules

Pricing Rule	Clearing Rate	Average Price	Failed Matches	Average Trust of Selected Providers
Fixed pricing	76.8%	9.94	325	0.676
Demand-responsive pricing	81.5%	10.37	259	0.701
Trust-adjusted dynamic pricing	85.5%	10.61	219	0.748

Table 3 compares the three pricing rules. Fixed pricing produces the lowest clearing rate because it cannot respond to scarcity. Demand-responsive pricing improves clearing by raising prices when resources are scarce, which attracts providers and reduces excessive demand. Trust-adjusted dynamic pricing performs best because it does not simply clear the market at any cost. It selects more reliable providers and reduces failed matches. Although the average price is slightly higher, the market delivers better realized service quality and fewer disputes.

6. Trust Analytics, Provider Segmentation, and Governance Results

The simulated results show that a vehicular edge market cannot rely on price as the only allocation signal. In a purely price-driven environment, an offer with the lowest quoted price may appear efficient at the moment of matching, but it can become costly after service failure, latency deviation, or dispute resolution. The trust variable therefore works as an economic correction factor rather than as a moral label. It translates repeated behavioral evidence into a measurable market signal that affects provider ranking, price premium, and eligibility for urgent requests. This logic is consistent with blockchain-enabled trust management research, which treats historical interaction records as a basis for decentralized confidence building rather than as passive archive data (Yang et al., 2019).

Table 4 divides providers into four groups: high trust, moderate trust, low trust, and critical trust. High-trust providers receive access to urgent requests and a small reliability premium because they reduce expected failure cost. Moderate-trust providers remain in the normal pool but are continuously monitored. Low-trust providers are not immediately excluded because harsh exclusion can reduce market liquidity; instead, they are directed toward non-urgent transactions or discounted offers. Critical-trust providers are temporarily suspended for review. This layered design avoids the weakness of binary admission rules and supports an adaptive market in which providers can recover through verified service improvement (Gazdar et al., 2022).

Table 4. Provider Trust Bands and Governance Actions

Trust Band	Score Range	Provider Status	Recommended Action
High trust	$0.80 \le T \le 1.00$	Reliable provider	Eligible for urgent requests and price premium
Moderate trust	$0.60 \le T < 0.80$	Normal provider	Eligible for standard requests with monitoring
Low trust	$0.40 \le T < 0.60$	Risk provider	Limited to non-urgent requests or discounted offers
Critical trust	$T < 0.40$	Unreliable provider	Temporary exclusion and review

The observed improvement in the average trust of selected providers from 0.676 under fixed pricing to 0.748 under trust-adjusted dynamic pricing is important because it shows that the platform is not merely charging higher prices. It is selecting a more reliable supply base. This distinction matters for business analytics. A revenue-only interpretation might conclude that the average price increase from 9.94 to 10.61 is the main driver of improvement. The service-quality interpretation is different: a modest price increase is acceptable because it is associated with fewer failed matches, fewer disputes, and higher provider reliability. The ledger data therefore support a broader performance evaluation than transaction revenue alone (Choi et al., 2018).

The trust segmentation results also indicate that trust should be updated asymmetrically. If one provider completes five ordinary transactions, its trust should increase gradually; however, if that same provider creates a confirmed dispute in a high-urgency transaction, the penalty should be larger. Vehicular edge markets are sensitive to delay and safety-related consequences. A failed computation resource exchange may delay object recognition, local route planning, or emergency-message handling. Therefore, the trust model must discourage opportunistic behavior more strongly than it rewards routine compliance. This design principle is consistent with practical concerns in permissioned blockchain systems, where participants must have incentives to protect the reliability of the shared infrastructure (Androulaki et al., 2018).

Another finding concerns the difference between trust visibility and trust usability. A blockchain can make service outcomes visible, but the market still needs a rule that converts visibility into action. If low-trust providers remain eligible for all high-value requests, the ledger becomes a record of repeated failure rather than a tool for governance. If high-trust providers do not receive any reliability premium, they may lose motivation to provide resources during congested periods. The proposed framework therefore links trust scores to operational actions, including provider ranking, price adjustment, transaction limits, and review triggers. This makes the blockchain ledger an active governance asset rather than a static database (Christidis & Devetsikiotis, 2016).

Table 4 should be read as a governance guide rather than as a technical scoring table. The four bands provide a transparent rule that can be communicated to participants before transactions occur. This transparency is important because dynamic scoring systems may otherwise be viewed as arbitrary or discriminatory. When providers understand how completion rate, latency compliance, and dispute outcomes affect access to future requests, they have a clearer incentive to maintain stable performance. The rule also

protects new providers because the moderate-trust category keeps them eligible while enough service history is accumulated (Queiroz & Wamba, 2019).

7. Extended Scenario Analysis and Robustness Checks

Table 5 compares the scenarios. The scenario comparison shows a gradual movement from a simple pricing market to a monitored trust-analytics market. In the fixed-price benchmark, market profit reaches 32,480, clearing rate is 76.8%, dispute rate is 6.1%, and provider stability index is 0.62. Under demand-responsive pricing, profit increases to 34,120 because scarcity information is incorporated into price. Under trust-adjusted pricing, profit reaches 35,860 because the platform begins to treat reliability as an economic attribute. When monitoring investment is added, profit rises further to 37,190, while dispute rate declines to 3.6%. These changes suggest that governance analytics contributes to both economic and operational performance (Wamba et al., 2017).

Table 5. Scenario Comparison of Market Performance

Scenario	Market Profit	Clearing Rate	Dispute Rate	Provider Stability Index
S1 Fixed price benchmark	32,480	76.8%	6.1%	0.62
S2 Demand-responsive pricing	34,120	81.5%	5.4%	0.66
S3 Trust-adjusted pricing	35,860	85.5%	4.2%	0.73
S4 Trust analytics with monitoring investment	37,190	87.4%	3.6%	0.78

The result is not simply a consequence of a more expensive market. The highest-performing scenario does raise the average realized price, but it also reduces failed service and dispute costs. In many digital platforms, low prices can produce apparent short-term efficiency while hiding downstream costs such as refund handling, transaction cancellation, user complaint processing, and loss of trust. In a vehicular edge market, these downstream costs are even more serious because service failure may interact with mobility conditions and time-sensitive computation. The scenario analysis therefore evaluates realized value rather than posted price (Gallego & van Ryzin, 1994).

A robustness check was conducted by varying demand pressure from 0.75 to 1.35. When demand pressure is below 1, meaning that supply exceeds demand, all three pricing rules perform reasonably well because requesters can find providers easily. The performance gap becomes larger when demand pressure exceeds 1.10. In that range, fixed pricing cannot attract enough reliable providers, and price-only dynamic pricing may clear requests through unstable suppliers. Trust-adjusted pricing remains more stable because it simultaneously raises market incentives and screens provider reliability. This supports the argument that trust analytics is most valuable during congested or uncertain market periods (Elmaghraby & Keskinocak, 2003).

A second robustness check examined the weight assigned to provider trust in the pricing rule. When the trust sensitivity coefficient is set too low, the model behaves almost like a demand-responsive rule, and low-cost but unreliable providers continue to win too many transactions. When the trust sensitivity coefficient is too high, the market becomes overly selective and may reduce participation by new providers. The best range is moderate: enough to reward reliable service, but not so strong that the market becomes closed. This balance is similar to supply-chain contract design, where incentive parameters must coordinate behavior without over-concentrating market power (Cachon & Lariviere, 2005).

A third robustness check focused on privacy-preserving analytics. The model assumes that raw bids, exact locations, and highly detailed vehicle behavior should not be directly exposed to all participants. Instead, the platform may publish aggregate demand pressure, category-level clearing rates, and trust-band statistics. When a differential-privacy noise term is added to aggregate indicators, the pricing rule remains stable as long as noise is calibrated to the sensitivity of the published statistic. This finding supports the feasibility of using privacy-preserving market dashboards without destroying the analytical usefulness of the data (Dwork, 2008).

The fourth check considered strategic trust manipulation. A provider may attempt to build a good reputation through many low-risk transactions and then exploit that reputation in a high-value urgent request. To address this risk, the framework separates routine completion from high-urgency reliability. A provider that performs well only in low-urgency transactions does not automatically qualify for the most urgent requests. The eligibility rule must therefore be context-aware. This design reflects the wider lesson from blockchain economics: technical decentralization does not remove the need for carefully designed governance and incentive rules (Böhme et al., 2015).

The final robustness check examined monitoring investment. Monitoring increases cost, but it improves detection of latency deviation, incomplete delivery, and repeated dispute patterns. In the simulated market, the monitoring-investment scenario produces the highest total profit because the reduction in failed matches and disputes exceeds the monitoring cost. This result is consistent with big-data operations research showing that predictive and diagnostic analytics generate value when they reduce uncertainty in operational decisions (Gunasekaran et al., 2017).

Table 5 summarizes the economic logic of the article. The movement from S1 to S4 demonstrates that pricing, trust, and monitoring are complementary rather than independent tools. A platform that only changes price may improve clearing but still select unstable providers. A platform that only calculates trust may improve screening but fail to attract resource supply during scarcity. A platform that combines pricing, trust, and monitoring can improve both market efficiency and governance quality (Kache & Seuring, 2017).

8. Managerial Implications for Smart Mobility Platforms

For platform managers, the first implication is that blockchain records should be designed for analytics from the beginning. Many blockchain applications emphasize immutability, but immutable records are not automatically useful records. If smart contracts only store transaction identifiers and final payments, later analysis of trust and pricing will be weak. The contract should also record resource category, promised service level, actual response time, dispute status, confirmation time, and anonymized contextual attributes. These fields allow managers to transform the ledger into a structured data asset for pricing, provider governance, and risk monitoring (Kshetri, 2018).

The second implication is that resource price should not be separated from service quality. A vehicle-edge provider may quote a low price because its resources are underutilized, because it is located near the requester, or because it intends to win requests without delivering stable service. Without trust analytics, these three cases can look similar. A trust-adjusted price differentiates them. Reliable nearby resources can be rewarded, while risky low-price offers are discounted or restricted. This makes the pricing system more consistent with the real cost of transaction failure (Lu et al., 2020).

The third implication concerns adoption by urban mobility stakeholders. Roadside infrastructure operators, mobility platforms, municipal agencies, vehicle manufacturers, and data-service providers may all participate in future edge markets. Each stakeholder needs confidence that the market is not manipulated by opaque algorithms. Transparent trust bands, explainable pricing factors, and auditable smart contracts can reduce resistance to adoption. This is particularly important in public-facing smart mobility services, where institutional legitimacy is as important as technical performance (Treiblmaier, 2018).

The fourth implication is that privacy protection should be viewed as a market requirement, not only as a legal compliance issue. Vehicle bids can reveal urgency, route patterns, resource needs, and potentially sensitive mobility behavior. If participants believe that market analytics exposes their behavior, they may avoid participation or submit distorted bids. Privacy-preserving aggregation, pseudonymous identity management, and limited disclosure of bid-level data help sustain participation while still allowing the platform to learn from transaction patterns (Iftikhar et al., 2023).

The fifth implication is the need for differentiated treatment of resource categories. Computation cycles, temporary storage, and sensing bandwidth do not have identical risk structures. Computation requests are often urgent and latency-sensitive. Storage requests may tolerate more delay but raise stronger privacy concerns. Sensing bandwidth depends heavily on local network conditions and sensor quality. A single price adjustment rule may therefore underperform. Category-specific base prices, trust weights, and service-level thresholds should be used in operational deployment (Meneguette et al., 2021).

The sixth implication is that trust recovery should be possible but not automatic. If a provider falls into a low-trust band because of repeated failure, the platform may allow recovery through a probationary sequence of low-risk transactions. However, the provider should not immediately regain access to high-urgency requests after one successful delivery. This approach supports market inclusion while protecting critical services. It also reduces the risk that temporary network instability permanently excludes otherwise useful providers (Inedjaren et al., 2021).

The seventh implication relates to data governance across regions. Vehicles move between edge regions, but local trust scores may not transfer smoothly. A provider with a good history in one region may be unknown in another. Consortium blockchain infrastructure can support controlled sharing of trust summaries across gateways without exposing full transaction histories. This approach balances portability and privacy, allowing market participants to carry verified reputation signals across smart mobility zones (Zhang & Chen, 2019).

9. Theoretical Contributions and Discussion

The first theoretical contribution is the repositioning of blockchain-enabled vehicular resource sharing as a market analytics problem. Prior work on blockchain-enabled vehicular resource sharing focuses on secure, incentive-compatible, and privacy-aware resource sharing. This article extends that direction by asking how the resulting transaction records can be used after the transaction: to set prices, evaluate trust, monitor service quality, and guide platform governance. This distinction is important because many blockchain studies stop at the point where the ledger is created, while business analytics begins when the ledger becomes a source of decision-making evidence (Lu, 2022).

The second contribution is the integration of pricing analytics and trust analytics. Dynamic pricing studies typically focus on demand, supply, and inventory. Trust management studies typically focus on security, reputation, and malicious behavior. In vehicular edge markets, these two areas cannot be separated. A provider's trust score changes the expected value of its offer, and a price signal changes the incentives of providers to enter or leave the market. The proposed framework therefore treats price and trust as jointly determined governance variables (den Boer, 2015).

The third contribution is the development of a transaction-level data structure for blockchain-enabled vehicular edge markets. The variables in Table 1 show how raw events can be organized for analysis. Resource type, demand pressure, provider trust, latency deviation, dispute flag, and clearing outcome form the minimum dataset needed for practical market learning. This data model bridges the gap between technical system design and business analytics, because it identifies which records are necessary for later pricing and governance decisions (Bai & Sarkis, 2020).

The fourth contribution is the demonstration that trust-adjusted pricing can improve both efficiency and reliability in a simulated setting. Although the dataset is synthetic, it is designed around realistic market logic: resource scarcity fluctuates, providers differ in reliability, and requesters value timely completion. The results show that a market mechanism can increase clearing rate while simultaneously reducing failed matches. This dual improvement is not guaranteed in ordinary dynamic pricing systems, where higher clearing may come at the cost of lower quality (Wang et al., 2023).

The fifth contribution is the extension of information-systems thinking into smart mobility governance. Blockchain, IoT, edge computing, and AI are often discussed as separate technologies. A working vehicular edge market requires their integration. Blockchain provides verifiable transaction history. IoT and vehicular communication provide real-time operational signals. Edge computing provides local resource availability. AI and analytics convert transaction history into trust and pricing rules. The theoretical value of the article lies in explaining how these components interact in a market setting (Xu et al., 2021).

The discussion also suggests that market governance must be evaluated by more than decentralization. A decentralized system can still be unfair, inefficient, or hard to adopt if its pricing and trust rules are unclear. Conversely, a permissioned system may be more suitable for vehicular edge markets if it provides fast confirmation, accountable validators, and controlled data access. This article therefore supports a pragmatic view of blockchain governance: the correct design is not necessarily the most decentralized one, but the one that best balances verifiability, latency, privacy, and institutional acceptance (Zheng et al., 2017).

10. Limitations and Future Research

Several limitations should be recognized. First, the analysis uses simulated transaction data rather than records from a deployed city-scale vehicular edge market. This choice is appropriate because open datasets containing blockchain-confirmed vehicle-edge resource transactions are still rare. However, future research should test the framework using real-world or field-experimental data from connected-vehicle pilots, smart-road testbeds, or edge-computing platforms. Real data would allow researchers to estimate the true distribution of latency deviation, dispute frequency, provider turnover, and demand spikes (Abbas et al., 2018).

Second, the pricing rule is intentionally transparent and relatively simple. This supports explainability and implementation, but it may understate the possible performance of more advanced learning models. Future research can compare the proposed rule with reinforcement learning, contextual bandits, or federated learning methods. Such models may improve local adaptation, but they should still be evaluated against transparency, fairness, and privacy constraints. In market governance, a slightly less accurate but explainable pricing rule may sometimes be preferable to a black-box rule that participants do not trust (Zhang & Lu, 2021).

Third, the model treats trust as a weighted score derived from transaction outcomes. Future work can expand the trust model by incorporating network-layer evidence, device certification, historical driving context, environmental conditions, and third-party verification. A provider's apparent failure may sometimes result from poor wireless channel conditions rather than intentional non-performance. Distinguishing controllable misconduct from uncontrollable environment risk is essential for fair trust updating (Mach & Becvar, 2017).

Fourth, the article does not model collusion in detail. Providers may coordinate bids, exchange false feedback, or attempt to manipulate trust scores. Requesters may also create false disputes to reduce payment. These behaviors require game-theoretic and anomaly-detection extensions. VCG-style mechanisms and smart-contract penalties can reduce some forms of strategic behavior, but the operational complexity of real vehicular markets means that analytics-based fraud detection will remain necessary (Rothkopf, 2007).

Fifth, cross-region interoperability remains a major future challenge. Vehicles may move between cities, infrastructure providers, and platform ecosystems. If each market uses a separate identity, trust, and price system, resource trading will remain fragmented. Future research should examine interoperable trust summaries, portable reputation credentials, and standardized smart-contract templates that can support cross-region vehicle-edge transactions while respecting privacy and regulatory boundaries (Zheng & Lu, 2022).

11. Conclusion

This article has expanded the study of blockchain-enabled vehicular resource sharing from a technical architecture problem into a business and data analytics problem. Instead of treating blockchain only as a security layer, the article treats the ledger as a structured data infrastructure for pricing intelligence, trust evaluation, service-quality monitoring, and market governance. The proposed framework integrates edge-market transaction records, smart-contract outcomes, demand pressure, provider reliability, and service-level compliance into a trust-adjusted dynamic pricing mechanism.

The simulated analysis shows that fixed pricing is insufficient for highly mobile vehicular edge markets because it ignores scarcity, reliability, and service quality. Demand-responsive pricing improves clearing, but it may still select unstable providers when reliability is not considered. Trust-adjusted dynamic pricing produces better market-clearing efficiency, reduces failed matches, and improves the average trust level of selected providers. When monitoring investment is added, the market achieves the strongest overall result, with higher profit, higher clearing rate, lower dispute rate, and stronger provider stability.

The main implication is that future smart mobility platforms should design blockchain systems not only to verify transactions but also to generate usable governance data. Trust scores should influence prices and provider access. Pricing rules should remain explainable enough for participants to accept. Privacy mechanisms should protect sensitive vehicle-level behavior while still permitting market-level learning. Smart contracts should record the right variables for later analytics, not only the minimum information required for settlement.

The article also highlights a broader theoretical message. In decentralized digital markets, technical trust and institutional trust are different but connected. Cryptography can verify that a transaction occurred, but analytics and governance determine whether the market becomes fair, efficient, and adoptable. Vehicular edge markets will succeed only when blockchain, pricing, trust analytics, privacy protection, and mobility governance are designed as an integrated system. This integrated perspective is the central contribution of the present article to business and data analytics research (Lu, 2021).

Acknowledgement

The authors thank the researchers whose published work provided the theoretical and methodological foundations for this study.

Author Contributions

Conceptualization, S.T.Y. and P.C.; Methodology, S.T.Y. and P.C.; Formal Analysis, S.T.Y. and P.C.; Investigation, S.T.Y.; Data Curation, S.T.Y.; Software, S.T.Y.; Validation, S.T.Y. and P.C.; Resources, S.T.Y. and P.C.; Visualization, S.T.Y.; Writing – Original Draft, S.T.Y.; Writing – Review & Editing, S.T.Y. and P.C.; Supervision, P.C.; Project Administration, S.T.Y. and P.C. We have read and approved the final manuscript and take responsibility for the work.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Ethical Approval and Consent

Not applicable. This study used simulated transaction records and did not involve human participants, identifiable personal data, or animal subjects.

Data Availability Statement

The simulated transaction dataset is summarized in Table 2, and the aggregate analytical results are reported in Tables 3 and 5. The simulation design and analytical procedures are described in the manuscript.

Declaration of Generative AI Use

Generative AI was used to assist with language editing and manuscript formatting.

References

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

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, Article 30. https://doi.org/10.1145/3190508.3190538

Bai, C., & Sarkis, J. (2020). A supply chain transparency and sustainability technology appraisal model for blockchain technology. *International Journal of Production Research, 58*(7), 2142–2162. https://doi.org/10.1080/00207543.2019.1708989

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Cachon, G. P., & Lariviere, M. A. (2005). Supply chain coordination with revenue-sharing contracts: Strengths and limitations. *Management Science, 51*(1), 30–44. https://doi.org/10.1287/mnsc.1040.0215

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

Choi, T., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. *Production and Operations Management, 27*(10), 1868–1883. https://doi.org/10.1111/poms.12838

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

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

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

Corbett, C. J., & de Groote, X. (2000). A supplier's optimal quantity discount policy under asymmetric information. *Management Science, 46*(3), 444–450. https://doi.org/10.1287/mnsc.46.3.444.12065

Cui, C., Du, H., Jia, Z., He, Y., & Wang, L. (2024). Blockchain-enabled federated learning with differential privacy for Internet of Vehicles. *Computers, Materials & Continua, 81*(1), 1581–1593. https://doi.org/10.32604/cmc.2024.055557

den Boer, A. V. (2015). Dynamic pricing and learning: Historical origins, current research, and new directions. *Surveys in Operations Research and Management Science, 20*(1), 1–18. https://doi.org/10.1016/j.sorms.2015.03.001

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

Dwork, C. (2008). Differential privacy: A survey of results. In Theory and Applications of Models of Computation (pp. 1–19). Springer. https://doi.org/10.1007/978-3-540-79228-4_1

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography Conference (pp. 265–284). Springer. https://doi.org/10.1007/11681878_14

Elmaghraby, W., & Keskinocak, P. (2003). Dynamic pricing in the presence of inventory considerations: Research overview, current practices, and future directions. *Management Science, 49*(10), 1287–1309. https://doi.org/10.1287/mnsc.49.10.1287.17315

Gallego, G., & van Ryzin, G. (1994). Optimal dynamic pricing of inventories with stochastic demand over finite horizons. *Management Science, 40*(8), 999–1020. https://doi.org/10.1287/mnsc.40.8.999

Gazdar, T., Alboqomi, O., & Munshi, A. (2022). A decentralized blockchain-based trust management framework for vehicular ad hoc networks. *Smart Cities, 5*(1), 348–363. https://doi.org/10.3390/smartcities5010020

Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2017). Big data and predictive analytics for supply chain and organizational performance. *Journal of Business Research, 70*, 308–317. https://doi.org/10.1016/j.jbusres.2016.08.004

He, L., Li, F., Xu, H., Xia, W., Zhang, X., & Tao, X. (2023). Blockchain-based vehicular edge computing networks: The communication perspective. *Science China Information Sciences, 66*(7), Article 172301. https://doi.org/10.1007/s11432-022-3658-7

Iftikhar, Z., Anjum, A., Khan, A., Shah, M. A., & Jeon, G. (2023). Privacy preservation in the Internet of Vehicles using local differential privacy and IOTA ledger. *Cluster Computing, 26*(6), 3361–3377. https://doi.org/10.1007/s10586-023-04002-0

Inedjaren, Y., Maachaoui, M., Zeddini, B., & Barbot, J. P. (2021). Blockchain-based distributed management system for trust in VANET. *Vehicular Communications, 30*, 100350. https://doi.org/10.1016/j.vehcom.2021.100350

Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of big data analytics and supply chain management. *International Journal of Operations & Production Management, 37*(1), 10–36. https://doi.org/10.1108/IJOPM-02-2015-0078

Kaltakis, K., Polyzi, P., Drosatos, G., & Rantos, K. (2021). Privacy-preserving solutions in blockchain-enabled Internet of Vehicles. *Applied Sciences, 11*(21), 9792. https://doi.org/10.3390/app11219792

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the blockchain technology adoption in supply chains: Indian context. *International Journal of Production Research, 57*(7), 2009–2033. https://doi.org/10.1080/00207543.2018.1518610

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x

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

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

Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information distortion in a supply chain: The bullwhip effect. *Management Science, 43*(4), 546–558. https://doi.org/10.1287/mnsc.43.4.546

Lu, Y. (2017a). 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

Lu, Y. (2017b). 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

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

Lu, Y. (2019a). 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

Lu, Y. (2019b). 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. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. *Nanotechnologies in Construction, 13*(3), 181–192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

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

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

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

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

Lu, Y., & Xu, L. D. (2019). Internet of Things 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

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

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

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

Lu, Y., Pisarenko, Z. V., Yang, L., Ivanov, L. A., & 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

Lu, Y., Sigov, A., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. *Journal of Industrial Information Integration, 35*, 100511. https://doi.org/10.1016/j.jii.2023.100511

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

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

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications, 125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

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

Meneguette, R., De Grande, R., Ueyama, J., Filho, G. P. R., & Madeira, E. (2021). Vehicular edge computing: Architecture, resource management, security, and challenges. *ACM Computing Surveys, 55*(1), Article 4, 1–46. https://doi.org/10.1145/3485129

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

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

Nissim, K., Raskhodnikova, S., & Smith, A. (2007). Smooth sensitivity and sampling in private data analysis. *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, 75*–84. https://doi.org/10.1145/1250790.1250803

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

Queiroz, M. M., & Fosso Wamba, S. (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

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

Rothkopf, M. H. (2007). Thirteen reasons why the Vickrey-Clarke-Groves process is not practical. *Operations Research, 55*(2), 191–197. https://doi.org/10.1287/opre.1070.0384

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

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

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-01-2018-0029

Tsay, A. A. (1999). The quantity flexibility contract and supplier-customer incentives. *Management Science, 45*(10), 1339–1358. https://doi.org/10.1287/mnsc.45.10.1339

Varian, H. R. (2007). Position auctions. *International Journal of Industrial Organization, 25*(6), 1163–1178. https://doi.org/10.1016/j.ijindorg.2006.10.002

Vickrey, W. (1961). Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance, 16*(1), 8–37. https://doi.org/10.1111/j.1540-6261.1961.tb02789.x

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J. F., 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

Wang, T., Ai, S., Cao, J., & Zhao, Y. (2023). A blockchain-based distributed computational resource trading strategy for Internet of Things considering multiple preferences. *Symmetry, 15*(4), 808. https://doi.org/10.3390/sym15040808

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains? International Journal of Production Economics, 211, 221–236. https://doi.org/10.1016/j.ijpe.2019.02.002

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

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

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), Article 2397630. https://doi.org/10.1080/17517575.2024.2397630

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. *Enterprise Information Systems, 19*(11), 2541199. https://doi.org/10.1080/17517575.2025.2541199

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2019). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal, 6*(2), 1495–1505. https://doi.org/10.1109/JIOT.2018.2836144

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

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

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. *Systems Research and Behavioral Science, 42*(4), 996–1015. https://doi.org/10.1002/sres.3151

Zhang, L., Zou, Y., Wang, W., Jin, Z., Su, Y., & Chen, H. (2021). Resource allocation and trust computing for blockchain-enabled edge computing system. *Computers & Security, 105*, 102249. https://doi.org/10.1016/j.cose.2021.102249

Zhang, X., & Chen, X. (2019). Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access, 7*, 58241–58254. https://doi.org/10.1109/ACCESS.2018.2890736

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. *Enterprise Information Systems, 16*(12), Article 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. *IEEE International Congress on Big Data, 557*–564. https://doi.org/10.1109/BigDataCongress.2017.85