Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Hybrid Used Car Trading System: Methodology, Security Analysis, and Algorithms

ChunHua Cao
Nanfang College Guangzhou
Chenglian Liu
chenglian.liu@gmail.com

Nanfang College Guangzhou
Sonia Chien-I Chen
Feng Chia University
Andres Arguedas
Universidad Panamericana

Article

Keywords: Blockchain, Used car trading, Cryptographic protocol, Anti-collusion, Terahertz inspection, Security analysis

Posted Date: June 15th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9771304/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Hybrid Used Car Trading System: Methodology, Security Analysis, and Algorithms

ChunHua Cao[1,+], Chenglian Liu[1,3*], Sonia Chien-I Chen[2,+], and Andrés Arguedas[3,+]

[1]Nanfang College Guangzhou, School of Engineering, Guangzhou, 510970, China
[2]Feng-Chia University, Department of International Business, Taichung, 40724, Taiwan
[3]Universidad Panamericana, Department of Cybersecurity and Clouding, San José, 10105, Costa Rica
[*]chenglian.liu@gmail.com
[+]these authors contributed equally to this work

ABSTRACT

The second-hand car market suffers from severe information asymmetry, rampant vehicle condition fraud, malicious data tampering, and frequent collusion among buyers, sellers, and third-party inspectors. Traditional used car trading platforms are mostly built on centralized architectures, which heavily depend on manual detection and subjective evaluation, leading to potential single point of failure, opaque transaction processes, and unreliable vehicle condition records. In recent years, blockchain technology has been gradually applied to build transparent and tamper-resistant transaction systems, and cryptographic protocols have been adopted to enhance transaction security and anti-collusion capabilities. Meanwhile, terahertz (THz) non-destructive inspection has shown unique advantages in detecting hidden damages, repainting, and structural anomalies of vehicles, providing objective and accurate evidence for vehicle condition evaluation. However, most existing studies only focus on a single technology and fail to organically integrate secure transaction mechanisms, cryptographic anti-collusion design, and trusted physical inspection. To fill this gap, this paper proposes a hybrid used car trading system that systematically combines blockchain, cryptographic anti-collusion protocols, and THz non-destructive inspection. The proposed system constructs a complete multi-party message interaction protocol, binds vehicle identity and parameters with on-chain records, and stores the hash values of THz inspection reports on the blockchain to ensure integrity, verifiability, and non-repudiation. The hybrid framework can effectively resist collusion attacks between any two participants, prevent forgery and tampering of inspection data, and eliminate information asymmetry in the trading process. Under standard cryptographic assumptions including discrete logarithm problem and collision-resistant hash functions, formal security analysis proves that the proposed scheme is secure against external attacks, internal fraud attacks, and inspection data forgery attacks. Compared with traditional methods and single-technology solutions, the proposed system achieves higher security, stronger credibility, and better practical deployability, which can serve as a reliable and secure solution for next-generation intelligent second-hand car trading platforms.

Keywords: Blockchain; Used car trading; Cryptographic protocol; Anti-collusion; Terahertz inspection; Security analysis

1 Introduction

The second-hand car market plays an increasingly important role in modern transportation and consumer economies. Compared with new vehicle purchases, secondhand cars offer lower prices and broader accessibility; however, they also introduce significant risks related to vehicle quality, hidden damage, and fraudulent information disclosure. In China, the rapid development of digital commerce has given rise to a range of mainstream second-hand car trading platforms, such as Guazi Used Cars (official website: http://www.guazi.com) – a leading e-commerce platform under the Chehaoduo Group founded in 2015, covering over 200 cities and providing services like 7-day no-questions-asked car returns; Renrenche (official website: https://m.renrenche.com) – the pioneer of the C2C transaction model established in 2014, offering 14-day return policies and a 1-year/20,000-kilometer warranty for core components; and Uxin Used Cars (official website: http://www.xin.com) ?V a brand under Uxin Group focusing on used car retail with both B2B and B2C business segments, implementing strict vehicle quality control through 158 professional inspections. Other notable platforms include Chezhibao (official website: http://www.chezhibao.com), which provides one-stop car-selling services and seamless connection of C2B, B2B, and C2C businesses to ensure high prices via national bidding; Taocheche (official website: https://www.taocheche.com) – a B2C-oriented new retail platform for used cars with strategic investment from Tencent and JD.com, boasting over 70 direct-operated stores nationwide; and Dongchedi Used Cars (official website: https://www.dcdapp.com) – a business segment of ByteDance that leverages its massive content ecosystem traffic and has opened direct stores and franchise stores in multiple regions across the country. Despite the

convenience brought by these platforms, one of the core challenges in second-hand car transactions remains the information asymmetry between buyers and sellers: sellers often possess more complete knowledge of a vehicle's history and condition than potential buyers. To address this problem, various information systems and online platforms (including the aforementioned ones) have been developed to support second-hand car trading. Nevertheless, many existing systems – even the well-known ones – rely on centralized databases and third-party authorities, which may become single points of failure or targets of data manipulation[1,2]. For instance, centralized architectures make it difficult to fully eliminate information asymmetry and malicious collusion[3,4].

The main contributions of this paper can be summarized as follows:

- We propose a hybrid second-hand car trading framework that integrates blockchain, cryptographic protocols, and THz non-destructive inspection.
- We design a multi-party cryptographic protocol that prevents collusion among buyers, sellers, and third-party inspectors[5,6].
- We incorporate THz inspection results into the blockchain using cryptographic hashes, ensuring the integrity and verifiability of vehicle condition information[7–9].
- We provide a detailed security analysis demonstrating resistance against external attacks, insider attacks, and inspection data forgery.

2 Related Work

Research related to second-hand car trading systems can generally be divided into three categories: (1) information systems and trading platforms, (2) blockchain-based transaction mechanisms, and (3) vehicle inspection and sensing technologies.

2.1 Second-Hand Car Trading Systems

Early studies on second-hand car markets primarily focused on pricing strategies, market behavior, and information asymmetry between buyers and sellers. Several works analyzed how insufficient or asymmetric information leads to adverse selection and unfair pricing in used car markets[1]. With the development of e-commerce platforms, online second-hand car trading systems have been proposed to improve market efficiency and accessibility. However, these systems often rely on centralized architectures, which raises concerns regarding data integrity and trustworthiness[2,3].

2.2 Blockchain-Based Used Car Systems

To address trust and transparency issues, blockchain technology has been introduced into used car trading systems. Huang et al.[10] proposed a cryptographic framework that applies public-key cryptography and blockchain concepts to prevent collusion among transaction participants. Their work emphasizes anonymous transactions and formal security analysis under discrete logarithm assumptions. Similarly, Ahn[11] explored the use of smart contracts on public blockchains to improve reliability and reduce intermediary costs in used car trading platforms. Other blockchain-based solutions[4,12] focused on traceability and decentralized identity management to enhance transaction credibility.

While blockchain-based systems improve data immutability and traceability, many existing approaches focus primarily on transaction records and ownership transfer. They often assume that inspection results provided by third parties are trustworthy, without addressing the problem of inspection data forgery or collusion between inspectors and sellers[5,6].

2.3 Terahertz-Based Vehicle Inspection

Terahertz sensing technology has emerged as a promising tool for non-destructive vehicle inspection. THz waves can penetrate paint layers and non-metallic materials, making them suitable for detecting repainting, hidden repairs, and structural inconsistencies[7,8]. Shen et al.[13] discussed the application of THz technology in second-hand car inspection and highlighted its advantages over traditional visual inspection methods. Recent advances[9] also extend THz inspection to vehicle component defect detection.

Despite its effectiveness, THz inspection alone does not solve the problem of trust in transaction systems. Inspection results may still be manipulated, selectively disclosed, or replaced if they are not properly protected by secure information systems.

2.4 Motivation for Hybrid Approaches

Recent studies indicate a growing need for integrated solutions that combine secure transaction mechanisms with reliable inspection technologies. However, existing research rarely provides a unified framework that jointly addresses transaction security, anti-collusion requirements, and vehicle condition verification. Motivated by these limitations, this paper proposes a hybrid approach that tightly integrates blockchain-based storage, cryptographic protocols, and THz inspection, providing a comprehensive solution for secure second-hand car trading.

3 Methodology

This section presents the proposed Hybrid Used Car Trading System, which integrates blockchain, cryptographic protocols, and terahertz (THz) non-destructive inspection technology to construct a secure, transparent, and tamper-resistant environment for second-hand vehicle transactions. The system is designed to solve critical issues in traditional used car trading platforms, including information asymmetry, data tampering, insider fraud, and collusion among buyers, sellers, and third-party inspectors. By combining distributed ledger technology, formal cryptography, and physical detection means, the proposed framework achieves end-to-end verifiability and strong security guarantees. The proposed framework combines three core components:

- an anti-collusion cryptographic protocol derived from the design in[10], which prevents bilateral or trilateral collusion during message exchange and transaction execution;
- a secure registration and vehicle-parameter binding mechanism inspired by[13], which links vehicle identity, ownership, and technical parameters to immutable on-chain records;
- a trusted evidence storage scheme that converts THz non-destructive inspection reports into cryptographic hashes and uploads them to the blockchain for public verification without leaking raw data[8].

These modules work together to establish a closed-loop security mechanism. The anti-collusion protocol ensures that no participant can forge or alter protocol messages without detection. The parameter binding mechanism fixes vehicle identity and inspection records to avoid identity substitution or parameter tampering. The hash-based on-chain storage preserves the integrity and non-repudiation of THz inspection results. Collectively, the proposed system provides strong security, public verifiability, resistance to internal and external attacks, and effective suppression of information asymmetry and collusion behaviors among transaction participants.

3.1 Notation

Throughout this paper, we use the following notation:

- p: a large prime number, with $|p| \geq 1024$ bits.
- g: a generator of the multiplicative group $\mathbb{Z}_p^*$.
- x_a, x_b, x_c: secret keys of the purchaser, the merchant, and the third-party inspector, respectively.
- $y_a = g^{x_a} \bmod p$: public key of the purchaser.
- $y_b = g^{x_b} \bmod p$: public key of the merchant.
- $y_c = g^{x_c} \bmod p$: public key of the third-party inspector.
- b: vehicle brand.
- t: vehicle type/model.
- p_1: suggested price of the vehicle.
- VIN: Vehicle Identification Number.
- $inspectionID$: index or identifier of the inspection record on blockchain.
- M_i: a query message that combines vehicle and inspection information

$$M_i = b \parallel t \parallel p_1 \parallel VIN \parallel inspectionID.$$

- $m_i \equiv h(M_i)$: a hash of the query message, using a secure one-way hash function $h(\cdot)$.
- THz_Report: the raw THz inspection report for the vehicle.
- $H_{\text{report}} = h(THz_Report)$: the hash of the THz inspection report.
- Blockchain: a distributed ledger that stores registration records, inspection summaries, and transaction logs.
- T_1, T_2, T_3, T_4, T_5: intermediate values produced during the execution of the hybrid protocol.

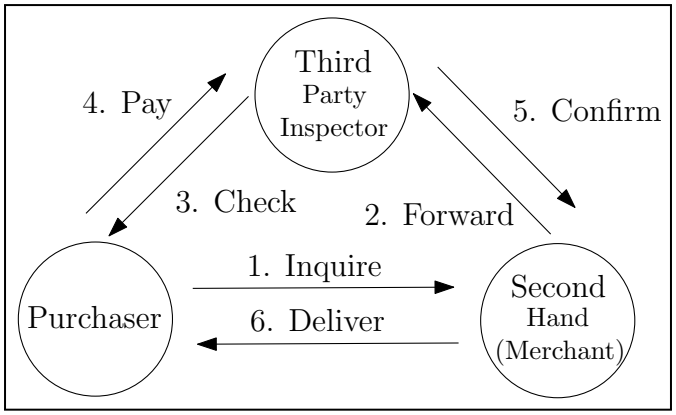


Figure 1. The Diagram of Our Scheme.

Puchaser	Third Party	Second Hand
$y_a \equiv g^{x_a} \bmod p$	$y_c \equiv g^{k_c} \bmod p$	$y_b \equiv g^{k_b} \bmod p$

Figure 2. Initializing Phase.

3.2 System Initialization

In the system initialization phase, global public parameters and key pairs are generated.

1. The system selects a large prime p and a generator g of $\mathbb{Z}_p^*$.
2. Each participant $i \in \{a,b,c\}$ chooses a secret key $x_i \in \mathbb{Z}_{p-1}$ and computes the public key
$$y_i = g^{x_i} \bmod p. \tag{1}$$
3. For each participant, an identity record is stored on the blockchain:
$$(ID_i, y_i, h(Profile_i)), \tag{2}$$
where $Profile_i$ denotes abstracted identity or profile data. This provides identity binding and non-repudiation for subsequent interactions[4,12].

3.3 THz Inspection and Blockchain Evidence

A trusted third-party inspection center performs THz imaging on the vehicle to detect structural damage, repainting, or other hidden defects[7,9]. The result of this inspection is a detailed report THz_Report. The inspector computes a hash of the report:

$$H_{\text{report}} = h(THz_Report). \tag{3}$$

Then the following tuple is stored on the blockchain:

$$(VIN, b, t, p_1, H_{\text{report}}). \tag{4}$$

This allows any party to verify later that a presented inspection report corresponds to the one recorded on-chain, without revealing all internal details.

3.4 Query Formation

When a purchaser is interested in a specific vehicle, the merchant provides the relevant vehicle information, including $(b, t, p_1, VIN, inspectionID)$. The purchaser forms a query message

$$M_i = b \parallel t \parallel p_1 \parallel VIN \parallel inspectionID, \tag{5}$$

and computes its hash

$$m_i \equiv h(M_i) \bmod p. \tag{6}$$

The value m_i will be embedded into the subsequent cryptographic protocol, which binds the vehicle information and inspection record to the flow of messages.

3.5 Hybrid Cryptographic Protocol

The hybrid cryptographic protocol consists of six logical steps. Intuitively, the protocol ensures that all participants agree on the vehicle information and THz inspection result while preventing any two parties from successfully colluding against the third[5,6].

Step 1: Purchaser Generates Query Parameters

The purchaser chooses a random value k_a and computes:

$$r_a \equiv g^{k_a} \bmod p \tag{7}$$

, and

$$S_a \equiv y_a \cdot r_a \bmod p. \tag{8}$$

The purchaser sends (S_a, m_i) to the merchant.

Step 2: Merchant Forwarding

Upon receiving (S_a, m_i), the merchant uses its secret key x_b to compute:

$$T_1 \equiv S_a^{x_b} \cdot m_i \cdot r_c^{-x_b} \bmod p, \tag{9}$$

where r_c is an appropriate value related to the inspector's public information (depending on the concrete instantiation). The merchant then forwards T_1 to the inspector.

Step 3: Inspector Verification

The inspector first checks the consistency between the THz report and the blockchain record:

$$h(THz_Report) \stackrel{?}{\equiv} H_{\text{report}}. \tag{10}$$

If the check fails, the protocol aborts. If the THz evidence is valid, the inspector uses x_c to compute:

$$T_2 \equiv T_1^{x_c} \cdot m_i^{-x_c} \bmod p. \tag{11}$$

The inspector then sends T_2 back to both the purchaser and the merchant.

Step 4: Purchaser Payment and Authorization

After receiving T_2, the purchaser confirms that the THz result and vehicle information are acceptable. The purchaser then commits to payment and authorization by computing:

$$T_3 \equiv T_2 \cdot (r_b)^{k_a} \bmod p, \tag{12}$$

where r_b is related to the merchant's side (e.g., a value derived using the merchant's public key). The purchaser sends T_3 to the inspector.

Step 5: Inspector Confirmation

The inspector confirms the agreement among all parties by computing:

$$T_4 \equiv T_3^{k_c} \cdot T_2^{-k_c} \bmod p, \tag{13}$$

using a semi-key k_c or similar parameter. Then T_4 is sent to the merchant.

Step 6: Merchant Delivery

Finally, the merchant computes:

$$T_5 \equiv T_4^{k_b^{-1}} \bmod p, \tag{14}$$

where k_b^{-1} is the inverse of a semi-key used by the merchant in the protocol. The merchant sends T_5 to the purchaser along with vehicle delivery.

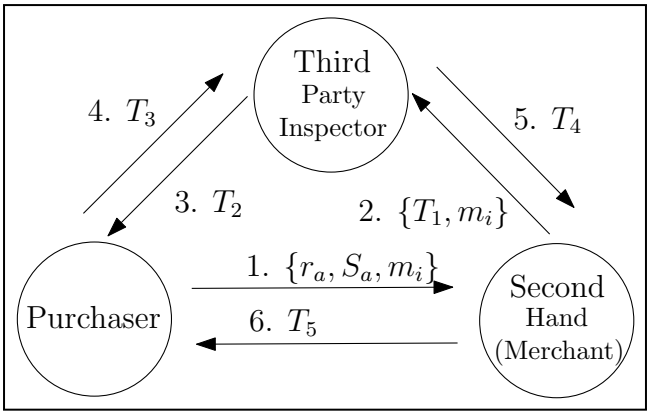


Figure 3. A Concept of Used Car Scheme Based on Cryptographic Protocol.

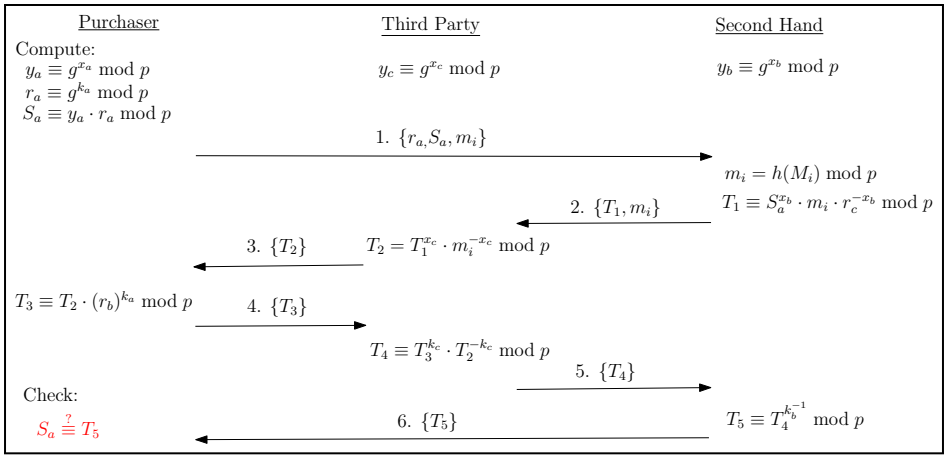


Figure 4. The Parameters Flow of Conception Diagram.

3.6 Purchaser Verification

The purchaser verifies the correctness of the final value:

$$T_5 \stackrel{?}{\equiv} S_a \bmod p. \tag{15}$$

If the equality holds, the purchaser accepts the transaction as valid and complete. A summary of the transaction (e.g., hashes and status) is then recorded on the blockchain.

3.7 Flow Diagram (Informal)

For intuition, the message flow can be summarized as:

3.8 Algorithms

This section presents four algorithms describing the main components of the Hybrid scheme: system initialization, THz inspection and recording, the hybrid protocol, and final verification.

Algorithm 1 SystemSetupAndRegistration

Require: Security parameter λ
Ensure: Public parameters (p, g) and key pairs for all parties
1: Select a large prime p and generator $g \in \mathbb{Z}_p^*$
2: **for** each participant $P_i \in \{\text{buyer } A, \text{merchant } B, \text{inspector } C\}$ **do**
3: Choose secret key $x_i \leftarrow \mathbb{Z}_{p-1}$
4: Compute public key $y_i \leftarrow g^{x_i} \bmod p$
5: Upload $(ID_i, y_i, role_i)$ to the blockchain
6: **end for**
7: Publish (p, g) as global parameters

Algorithm 2 THzInspectionAndCommitment

Require: Vehicle information (VIN, b, t, p_1)
Ensure: On-chain THz commitment hash H_{report}
1: Inspector performs THz scanning and obtains *THzReport*
2: Compute $H_{\text{report}} \leftarrow h(THzReport)$
3: Construct record $rec \leftarrow (VIN, b, t, p_1, H_{\text{report}})$
4: Store *rec* into the blockchain
5: Return H_{report} for future verification

Algorithm 3 HybridTransactionProtocol

Require: Public parameters (p, g), public keys (y_a, y_b, y_c), digest m_i
Ensure: Final value T_{final} for verification
Phase 1: Purchaser creates query token
1: Buyer samples $k_a \leftarrow \mathbb{Z}_{p-1}$
2: Compute $r_a = g^{k_a} \bmod p$
3: Compute $u_a = y_a^{k_a} \bmod p$
4: Compute $S_a = h(u_a \parallel m_i)$
5: Buyer sends (r_a, S_a, m_i) to merchant
Phase 2: Merchant transforms token
6: Merchant computes $T_1 = r_a^{x_b} \cdot m_i \bmod p$
7: Merchant forwards (T_1, m_i) to inspector
Phase 3: Inspector checks THz evidence
8: Retrieve $(VIN, b, t, p_1, H_{\text{report}})$ from blockchain
9: **if** $h(THzReport) \neq H_{\text{report}}$ **then**
10: abort protocol
11: **end if**
12: Compute $T_2 = T_1^{x_c} \cdot m_i^{-x_c} \bmod p$
13: Inspector sends T_2 to both buyer and merchant
Phase 4: Buyer adjusts token
14: Buyer computes $T_3 = T_2^{k_a^{-1}} \bmod p$
15: Buyer sends T_3 to inspector
Phase 5: Inspector removes its exponent
16: Inspector computes $T_4 = T_3^{x_c^{-1}} \bmod p$
17: Inspector sends T_4 to merchant
Phase 6: Merchant finalizes token
18: Merchant computes $T_{\text{final}} = T_4^{x_b^{-1}} \bmod p$
19: Compute $T_{\text{tag}} = h(u_a \parallel m_i)$
20: Send T_{tag} back to buyer

Algorithm 4 BuyerSideVerification

Require: (S_a, m_i) kept by buyer, received T_{tag}
Ensure: Accept or Reject
1: Recompute $u_a = y_a^{k_a} \bmod p$
2: Recompute $S_a^* = h(u_a \parallel m_i)$
3: **if** $S_a^* = T_{\text{tag}}$ **then**
4: Accept transaction
5: **else**
6: Reject protocol
7: **end if**

4 Security Analysis

In this section, we analyze the security of the proposed Hybrid scheme. We first recall several standard complexity assumptions and hash properties, and then discuss the correctness of honest participants and the robustness against different types of attacks.

4.1 Definitions

Definition 4.1 (Discrete Logarithm Problem (DLP))**.** Given (p, g, y) with $y = g^x \bmod p$, find x. The DLP is believed to be computationally infeasible for sufficiently large p.

Definition 4.2 (Computational Diffie–Hellman Problem (CDHP))**.** Given (g, g^a, g^b) for unknown $a, b \in \mathbb{Z}_{p-1}$, compute g^{ab}. This problem is assumed to be intractable in $\mathbb{Z}_p^*$.

Definition 4.3 (Decisional Diffie–Hellman Problem (DDHP))**.** Given (g, g^a, g^b, g^c), decide whether $c = ab \pmod{p-1}$, that is, whether $g^c = g^{ab}$ or not.

Definition 4.4 (Pre-image Resistance)**.** A hash function $h(\cdot)$ is pre-image resistant if, for a given output W, it is computationally infeasible to find any input X such that $h(X) = W$.

Definition 4.5 (Collision Resistance)**.** A hash function $h(\cdot)$ is collision resistant if it is computationally infeasible to find distinct X_1 and X_2 such that $h(X_1) = h(X_2)$.

These assumptions are standard for public-key cryptosystems and hash-based constructions.

4.2 Correctness of Honest Participants

Lemma 1 (Honest Purchaser Correctness)**.** *If the purchaser follows the protocol honestly, and both the merchant and the inspector are also honest, then the final equality*

$$T_{final} = S_a \tag{16}$$

holds with overwhelming probability.

Sketch of proof. Under honest behavior, each step of the protocol (from S_a to T_{final}) is computed using consistent algebraic operations that preserve the intended relation. At the end of the protocol, reversing these operations leads back to S_a. Any deviation will destroy this equality. □

Lemma 2 (Honest Merchant Correctness)**.** *If the merchant behaves honestly, and if the inspector and purchaser follow the protocol, then any forgery attempt on T_1 or T_4 will be detected and will cause the final equality $T_{final} = S_a$ to fail.*

Lemma 3 (Honest Inspector Correctness)**.** *If the inspector behaves honestly, then invalid THz reports or inconsistent vehicle information will be detected by checking $h(THz_Report)$ against H_{report} and comparing hashes of M_i. Any manipulation will prevent a consistent set of T_1, T_2, T_3, T_4 from being produced.*

4.3 Attack Scenarios

Scenario 1: External Attacker. An external attacker observing the protocol transcript attempts to recover any secret key x_a, x_b, x_c. This implies solving DLP or CDHP in $\mathbb{Z}_p^*$, which is assumed to be infeasible. Thus, the attacker cannot impersonate participants or forge valid protocol messages.

Scenario 2: Insider Attack (Dishonest Merchant Employee). Suppose a dishonest employee of the merchant attempts to replace T_1 with a forged T_1', or modify later messages (T_2', T_3', T_4'). Because the purchaser's final check requires the strict equality $T_{\text{final}} = S_a$, any incorrect algebraic relation will break this equality. Therefore, such insider manipulation is detected and the protocol aborts.

Scenario 3: THz Report Forgery Attack. An attacker attempts to present a fake THz report THz_Report' inconsistent with the blockchain record. Since the blockchain stores $H_{\text{report}} = h(THz_Report)$, and $h(\cdot)$ is collision resistant, the probability that

$$h(THz_Report') = H_{\text{report}} \tag{17}$$

holds for a different report is negligible. Consequently, any tampering with the THz report is detected.

4.4 Security Advantages of the Hybrid Scheme

Table 1 summarizes the advantages of the Hybrid scheme compared with previous schemes.

Table 1. Security properties comparison

Property	Huang et al.'s scheme[10]	Shen et al.'s scheme[13]	Hybrid Scheme
Anti-collusion	Strong	Medium	**Strongest**
Cryptographic soundness	Strong	Strong	**Strong**
Vehicle condition trust	Low	Medium	**High (THz)**
Tamper resistance	Medium	Medium	**High (Blockchain)**
Practical deployability	Medium	Medium	**High**

5 Conclusion

This paper proposed a hybrid used car trading system that integrates blockchain technology, cryptographic anti-collusion protocols, and terahertz (THz) non-destructive inspection. By combining secure multi-party cryptographic message flows with on-chain storage of inspection hashes, the proposed system addresses critical challenges in second-hand car markets, including information asymmetry, inspection result forgery, and collusion among transaction participants. Compared with existing blockchain-based used car trading systems, the proposed scheme provides stronger security guarantees by explicitly modeling and preventing collusion between buyers, sellers, and third-party inspectors[5,6]. Furthermore, by incorporating THz inspection technology, the system enhances the reliability of vehicle condition assessment[7–9], enabling objective and verifiable inspection evidence that cannot be modified after being recorded on the blockchain. Formal security analysis demonstrates that the proposed hybrid scheme is resistant to external attacks, insider manipulation, and inspection data forgery under standard cryptographic assumptions. The proposed system is practical and extensible. It can be integrated into existing second-hand car trading platforms and adapted to different inspection technologies or blockchain implementations[4,12]. Future work will focus on performance evaluation, implementation on real-world blockchain platforms, and the integration of additional sensing technologies and smart contracts to further enhance automation and scalability.

Declarations

Funding: The authors received no financial support for the research, authorship, and/or publication of this article.
Conflict of interest / Competing interests: The authors declare that they have no conflict of interest.
Ethics approval and consent to participate: This study does not involve human participants or animals. Therefore, ethical approval and informed consent are not applicable.
Consent for publication: Not applicable.
Data availability: No datasets were generated or analysed during the current study.
Materials availability: Not applicable.
Code availability: The code used in this study is available from the corresponding author upon reasonable request.

Data Availability

All data generated or analysed during this study are included in this published article. Additional information is available from the corresponding author on reasonable request.

Author contributions statement

Author Contributions: Conceptualization, C. Liu and Sonia Chen; methodology, C. Liu and Sonia Chen; validation, Sonia Chen and Andres Arguedas; formal analysis, C. Liu and Sonia Chen; resources, C. Liu and Sonia Chen; data curation, Sonia Chen and C. Liu; writing-original draft preparation, C. Liu; writing-review and editing, C. Liu and Sonia Chen; supervision, Sonia Chen and Andres Arguedas. All authors have read and agreed to the published version of the manuscript. All authors read and approved the final manuscript.

References

1. Yu, Y., Yao, C., Zhang, Y. & Jiang, R. Second-hand car trading framework based on blockchain in cloud service environment. In *2021 2nd Asia Conference on Computers and Communications (ACCC)*, 116–120 (IEEE, 2021).
2. Zhang, J., Zhao, H., Yang, Y. & Yan, J. Towards transparency and trustworthy: A used-car deposit platform based on blockchain. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 96–100 (IEEE, 2019).

3. Ko, T. *et al.* A secure used car trading system based on blockchain technology. In *Proceedings of the 21st International Conference on Information Integration and Web-based Applications and Services*, 646–651 (2020).
4. Zhang, W., Guo, L. & Li, Y. Used car traceability system based on blockchain. In *2021 International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, 235–240, DOI: 10.1109/ISPDS54097.2021.00053 (2021).
5. Ali, M. *et al.* Scalable blockchain framework for trust management in the internet of vehicles. *J. Distributed Parallel Comput.* **189**, 104568 (2024).
6. Tao, Y., Liu, X. *et al.* A lightweight anonymous authentication scheme with dual blockchain and self-sovereign identity for vanets. *Peer-to-Peer Netw. Appl.* **17**, 1–18 (2026).
7. Niemann, R. *et al.* Non-destructive characterization of automobile car paints using terahertz pulsed imaging and infrared optical coherence tomography. In *40th International Conference on Infrared, Millimeter, and Terahertz Waves (IRMMW-THz)*, 1–2 (IEEE, 2015).
8. Dash, J. *et al.* Terahertz technology for non-destructive testing applications: A comparative study of continuous wave and time-domain spectroscopy systems. *J. Non-Destructive Test. Eval.* **21**, 49–55 (2024).
9. Research on terahertz detection method for layered defects in vehicle cable terminals based on fdtd. *IEEE Transactions on Instrumentation Meas.* **74**, 1–12 (2025).
10. Huang, C., Liu, C. & Chen, S. C. Research on the used car system based on blockchain and cryptographic technology. *WSEAS Transactions on Comput. Res.* **10**, 105–111 (2022).
11. Ahn, B. Implementation for used trading management system based on blockchain (case: Used car). In Chang, J.-W., Yen, N. & Hung, J. C. (eds.) *Frontier Computing*, vol. 747 of *Lecture Notes in Electrical Engineering*, 405–412 (Springer Singapore, Singapore, 2021).
12. Ko, T. *et al.* Car-story: A decentralized vehicle information storage system based on blockchain. In *2024 IEEE Region 10 Symposium (TENSYMP)*, 1–6 (IEEE, 2024).
13. Shen, H., Liu, C., Chen, S. C. & Xu, R. The second-hand car system based on terahertz and blockchain technology. In *ITM Web of Conferences*, vol. 77, 01050 (EDP Sciences, 2025).