engineering proceedings

MDPI

Proceeding Paper

Transparent Trust Assessment in 6G Using Blockchain †

Ronald Iván Maldonado Valencia *,‡, Elmira Saeedi Taleghani ‡, Jesús Angel Alonso Lopez ‡, Ana Lucila Sandoval Orozco ‡ and Luis Javier García Villalba *,‡

Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), Facultad de Informática, Universidad Complutense de Madrid (UCM), 28040 Madrid, Spain; elmirasa@ucm.es (E.S.T.); jesusaal@ucm.es (J.A.A.L.); asandov@ucm.es (A.L.S.O.)

* Correspondence: ronaldim@ucm.es (R.I.M.V.); javiergv@fdi.ucm.es (L.J.G.V.); Tel.: +34-91-394-7638 (L.J.G.V.)

† Presented at the First Summer School on Artificial Intelligence in Cybersecurity, Cancun, Mexico, 3–7 November 2025.

‡ These authors contributed equally to this work.

Abstract

Trust assurance will be a cornerstone of the security and autonomy of sixth-generation (6G) networks. Traditional trust models focus on data authenticity and integrity; however, 6G systems increasingly rely on autonomous decision-making. This article presents blockchain as a dual function in 6G: first, as a decentralized and immutable ledger, and second, as a trustor, an entity that guarantees the transparency, traceability, and immutability of the trust assessment process itself. A conceptual framework is proposed in which blockchain houses both trust metrics and the logic that governs their assessment using smart contracts.

Keywords: blockchain; trust; 6G networks; transparency

1. Introduction

Sixth-generation (6G) networks promise a paradigm shift toward hyper-connected, intelligent, and autonomous ecosystems. This paradigm encompasses new applications and devices, such as telemedicine, the Internet of Things, autonomous transportation, and smart cities [1]. As new enhancements and connected devices emerge, new security, privacy, and operational challenges inherent to managing these networks arise. These next-generation networks will be able to natively establish trust mechanisms and enable continuous trust verification.

A multi-criteria method was proposed by [2], which takes into account criteria such as network structure, user comments, etc. These criteria are then combined using weights and techniques such as weighted average and weighted moving average to obtain a trust value. Generative Adversarial Networks have also been used for trust management [3]. They first perform a trust assessment using fuzzy logic, the results of which are used to train the neural network. This model allows networks to be classified using medium, high, or low trust. The work carried out in [4] proposes the use of support vector machines to determine whether a node is trustworthy or not in underwater sensor networks. Evaluating trust using fuzzy logic is characterized by its ability to address uncertainty and allow trust information to be represented in linguistic terms, making it a more flexible system. A review of trust evaluation methods is presented in [5], highlighting fuzzy methods as scalable, dynamic, and context-aware. In Blockchain technology, information is stored in different nodes of a decentralized network, and each node has an identical copy of the book. This allows information to be secure, traceable, decentralized, and immutable [6]. Considering

Check for updates

Academic Editors: Héctor Manuel Pérez Meana and Gabriel Sánchez Pérez

Published: 4 February 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

these properties, blockchain technology can ensure that trust-related data is legitimate, thus making the network environment more reliable. A trust evaluation mechanism for dynamic spectrum access for IoT systems is proposed in [7]. This dynamic aspect causes different unrelated services to share information; thus, this method guarantees privacy, information transparency, decentralized access to the spectrum. A review of blockchain technologies to guarantee trustworthy systems is carried out by [8]. Here, a trustor and trustee perspective is presented in which the user can act as a trustor and the blockchain as a trustee. There, the improvement in trust that this scheme provides is discussed, since the blockchain is a trustworthy entity by nature. In the work carried out by [9], some attributes that should be considered when evaluating trust in IoT systems using blockchain are discussed, such as reputation, accuracy, confidence in authentication and authorization. It also discusses how blockchain types influence trust and the challenges of trust in IoT, including trust challenges in privacy, interoperability, and system integration.

2. Materials and Methods

Through the dual vision of leveraging blockchain technology, a system is proposed to evaluate trust. The DLT performs two fundamental functions: the first is the decentralized recording of trust-related data, which then acts as a trustor, evaluating trust through a smart contract. The blockchain as a trustor implies that it will be the entity in charge of estimating the trust of other entities, and these other entities known as trustees will be continuously evaluated and the trust values will be stored in the DLT. Blockchain as a trustor implies that it will be the entity responsible for estimating the trust of other entities. These other entities, known as trustees, will be continuously evaluated, and the trust values will be stored in the DLT. This approach provides a significant differentiation by ensuring that the trustor is trustworthy in and of itself, and also by ensuring that the trustor is decentralized, immutable, and transparent. The information needed to calculate trust is collected through an independent module that can query external APIs and manage events. This information will be used as input to calculate the trust level. The proposed system will collect this information and process it using a fuzzy logic algorithm, in conjunction with the blockchain, where the input information will be stored in the DLT. This algorithm will be executed in a smart contract. The proposed architecture is shown in Figure 1.

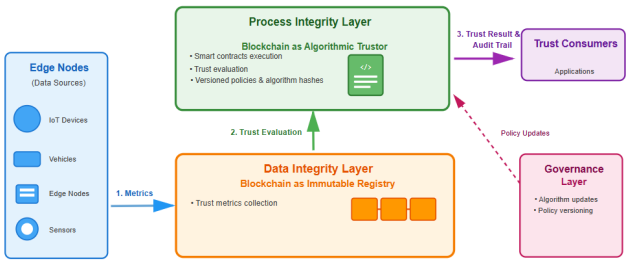


Figure 1. Trust Assessment Architecture.

2.1. Data Integrity Layer

This is responsible for collecting and recording information. To do this, it will consult other algorithms to obtain information related to trust. This information will then be used in another stage to obtain a final trust value. The algorithms will be responsible for generating values that indicate how the nodes behave in a system. In addition, in this stage, the input data will be processed so that it can be used to calculate the trust level. This processing consists of giving the information a uniform structure, in addition to handling values that are not available at a given time. Finally, since the information will depend on

multiple different sources, this module will ensure that the input attributes have the same format and are associated with a specific service or node at a given time.

2.2. Process Integrity Layer

As seen in Figure 1, there is a processing layer to calculate trust values. In this layer, the DLT technology to be used and the protocols implicit in this technology must be taken into account. This is because, depending on the DLT selected, it is easier to control costs or even transact without incurring fees, as occurs in certain blockchains such as Ethereum. An example is permissioned systems, which guarantee that network participants are trustworthy and, likewise, the transactions executed will be more reliable. Furthermore, since they are private, information will remain confidential. Another consideration is the consensus protocols for approving transactions. There are many consensus protocols [10], such as Raft, which consumes few resources but is not tolerant to Byzantine faults, or PoW, which is decentralized and provides great security but presents scalability issues and high consumption of computational resources. A smart contract will be deployed in the DLT that will perform different functions. The first is that for each attribute, a value will be calculated that indicates how good or bad that attribute is for the system. This can be done with an artificial intelligence algorithm, fuzzy logic, weighted sum, etc. Algorithm 1 shows some of the smart contract's functions. It shows that for each dimension (attribute), a fuzzy logic calculation is performed. These results are then processed again to obtain a final confidence value. In addition, methods that allow information to be queried from the DLT are necessary.

Algorithm 1 Smart Contract (Chaincode) of the Trust Assessment System

```
1: function TrustAssessment (dimensions...)
2:     Attestation ← trustByDimension (atestacionInputs)
3:     SaveAssessment (dimension, Attestation)
4:     finalTrust ← TrustAssessment (Attestation, CTI, ...)
5:     SaveAssessment (finalTrust)
6:     return finalTrust
7: end function
```

3. Results

The results obtained using blockchain to evaluate trust are now shown. We focus on the performance of the functions for calculating and reading information. The experiment was conducted on a Hyperledger Fabric network, using the Raft protocol as a permissioned, private network. The performance indicators presented were obtained using Caliper. The results of performing the TrustAssessment transaction are shown in Table 1.

Table 1. Trust Assessment Performance.

Tx	Rate (TPS)	Latency (s)	Throughput (TPS)
10	133.3	0.23	37.2
100	73.7	0.28	59.6
1000	76.5	0.20	73.7

Tx: Transaction number. **Rate**: Send rate from client **Throughput** The actual confirmation rate. **Latency** expresses the response time per transaction.

As can be seen in Table 1, several experiments were performed varying the number of transactions to measure the impact on latency and throughput. It can be observed that

the throughput is maintained for a large number of transactions. Considering this, we can say that it is a viable way for many services, since trust does not necessarily have to be evaluated in real time; however, the capacity to process a large number of transactions is evident.

The results obtained demonstrate the feasibility of using blockchain technology for trust in 6G networks, as they demonstrated the ability to use smart contracts to execute complex calculations, such as the implementation of the fuzzy logic engine. This, coupled with the immutability and transparency inherent in DLT (for both data and smart contracts), provides a solid foundation for a robust trust system. We can also say that the inclusion of an external database makes data available for real-time decision-making.

4. Conclusions

The Trust Trustee stands as a cornerstone for achieving the integrity and accountability of algorithms in 6G trust evaluation systems. It designates the blockchain not only as a support layer, but also as a trusted authority for the trusted algorithms themselves. The blockchain-based trust evaluation algorithm provides guarantees that make trust mechanisms much more robust. First, it allows the trust logic to be immutable, since modifying it requires a process that will always be verified and traceable. By storing each entry and its logic, transparency can be guaranteed, allowing us to understand at any time how certain trust values were obtained. A third point is that the trustor will no longer be a central authority, which allows for greater trust.

By proposing a multi-stage system, we have a trust assessment that is more resilient to failure and can work for applications that require real-time results, as we include a decentralized application and an event-based system. The use of blockchain provides an additional level of trust in the assessment system itself, ensuring that the records stored there are transparent and authentic.

Author Contributions: R.I.M.V., E.S.T., J.A.A.L., A.L.S.O. and L.J.G.V. contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the PRIVATEER EU project, Grant agreement N 101096110, by the Programme UNICO-5G I+D of the Spanish Ministerio de Asuntos Económicos y Transformación Digital, the European Union - NextGeneration EU in the framework of the ”Plan de Recuperacion, Transformación y Resiliencia” under reference “TRAZA5G (TSI-063000-2021-0050)”, by the Recovery, Transformation and Resilience Plan, financed by the European Union (Next Generation EU), through the Chair “Cybersecurity for Innovation and Digital Protection” INCIBE-UCM and by Comunidad Autonoma de Madrid, CIRMA-CM Project (TEC-2024/COM-404). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data is already avaliable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wang, C.X.; You, X.; Gao, X.; Zhu, X.; Li, Z.; Zhang, C.; Wang, H.; Huang, Y.; Chen, Y.; Haas, H.; et al. On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 905–974. [CrossRef]
2. Gao, Y.; Li, X.; Li, J.; Gao, Y.; Philip, S.Y. Info-trust: A multi-criteria and adaptive trustworthiness calculation mechanism for information sources. *IEEE Access* **2019**, *7*, 13999–14012. [CrossRef]
3. Yang, L.; Li, Y.; Yang, S.X.; Lu, Y.; Guo, T.; Yu, K. Generative adversarial learning for intelligent trust management in 6G wireless networks. *IEEE Netw.* **2022**, *36*, 134–140. [CrossRef]

4. Han, G.; He, Y.; Jiang, J.; Wang, N.; Guizani, M.; Ansere, J.A. A synergetic trust model based on SVM in underwater acoustic sensor networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11239–11247. [CrossRef]
5. Saeedi Taleghani, E.; Maldonado Valencia, R.I.; Sandoval Orozco, A.L.; García Villalba, L.J. Trust evaluation techniques for 6G networks: A comprehensive survey with fuzzy algorithm approach. *Electronics* **2024**, *13*, 3013. [CrossRef]
6. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open J. Commun. Soc.* **2020**, *1*, 957–975. [CrossRef]
7. Ye, J.; Kang, X.; Liang, Y.C.; Sun, S. A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks. *IEEE Internet Things J.* **2022**, *9*, 13263–13278. [CrossRef]
8. Yavaprabhas, K.; Pournader, M.; Seuring, S. Blockchain as the "trust-building machine" for supply chain management. *Ann. Oper. Res.* **2023**, *327*, 49–88. [CrossRef] [PubMed]
9. Kumar, R.; Sharma, R. Leveraging blockchain for ensuring trust in IoT: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 8599–8622. [CrossRef]
10. Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A Systematic Review of Consensus Mechanisms in Blockchain. *Mathematics* **2023**, *11*, 2248. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.