JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

DYNAMIC AND SECURE TRANSACTION VALIDATION USING AN ADAPTIVE BLOCKCHAIN ARCHITECTURE

[#1]SD. KHAJA PASHA, ***Assistant Professor,***
[#2]PADALA BHARATH KUMAR, ***B.Tech Student,***
[#3]MUNUGURI PAVANI, ***B.Tech Student,***
[#4]MITTA JYOTHI, ***B.Tech Student,***
[#5]NILUGONDA RAVALI, ***B.Tech Student,***
[#6]NUKA RADHAKRISHNA, ***B.Tech Student,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: The most substantial impediment to ubiquitous data interchangeability is trust. Despite the fact that data consumers have expressed concerns regarding the quality of the shared data, a multitude of data proprietors are unable to share their data due to a lack of infrastructure for establishing data trust. Blockchain technology facilitates decentralized and transparent governance by allowing multiple parties to agree on an unalterable ledger. This program enhances the integrity of data transmission by establishing a comprehensive architecture for data trust through the use of blockchain technology. Additionally, we provide a versatile method for determining the number of transaction validators by utilizing the approximated trust value.

Keywords: Distributed, access control, data trust, and blockchain are all keywords.

1. INTRODUCTION

The sharing of personal information has become a contentious subject due to concerns about privacy, abuse of data, and potential violations of ethical and legal standards. Because data trust isn't well-established, many data owners are wary of giving it out. Several research goals may rely heavily on this data. Concerns over the integrity and precision of the data at its origin point are shared by data owners and consumers. Consequently, consumers and data owners alike face issues with trust. With the new concept of data trust, individuals are more likely to trust one another when they exchange data, which in turn stimulates more data sharing. There are several facets to data trust, including technical requirements for data transfer, ethics, governance, law, and organizational structure.

Adapting existing auditing procedures and automating the deployment of smart contract logic are two ways in which blockchain technology could provide the necessary features for a data trust framework to function, cutting out intermediaries. Research on blockchain's potential applications in data interchange, trust development, and access management has increased substantially. Data controllers and data consumers can build trust with blockchain technology. The data trust system may gain credibility due to blockchain's distributed nature, security features, and reliability.

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

The blockchain-based architecture for data trust presented in this paper protects the ethical and secure use of data by owners while guaranteeing the integrity and quality of data at the source for consumers. To determine the reliability of input data sets, our trust model takes into account the following three factors: the data owner's faith in the data set, the endorsement of the data asset, and the reputation and endorsement of the data owner. With every new transaction, these parameters are updated in the ledger. Depending on the reliability of the dataset, Hyperledger Fabric uses state-based endorsement and adaptive transaction validation. To demonstrate our system's efficacy in managing massive transactional databases across several organizations, we conduct a comprehensive performance analysis. As far as we are concerned, our system possesses all the necessary characteristics for data trust. Furthermore, it

Both the blockchain and the smart contracts it supports have many positive qualities, such as being transparent, secure, and unchangeable.

2. LITERATURE REVIEW

Zavolokina et al. provided valuable information for vehicle dossiers and compensated network members monetarily for their participation. The system is under the impression that if it punishes bad conduct, things would improve. Incentives are calculated and implemented automatically using smart contracts.

Data owners were able to share their research data with Shrestha et al. using smart contracts and blockchain technology, preserving ownership and control. The system incentivizes users to sign up for the network by providing them with aggregated, anonymized data.

A subjective logic model was used to quantify the reputation of nodes in order to guarantee high-quality data transmission over the vehicular network. A trust model was developed by Dedeoglu et al. to verify the veracity of the data collected by IoT sensor nodes. The model takes into account the reliability and trustworthiness of the data source in addition to the results from nearby sensor nodes. Additionally, they use blockchain to detect inaccurate or dubious data acquired by mobile crowd sensing or Internet of Things devices, so they can monitor the quality of shared data.

Choudhury et al. safeguarded personal information while ensuring high-quality data. As nodes in the network, regulatory bodies verify the data's veracity. In order to safeguard sensitive information, certain operations can have their own dedicated private channels. Delegated proof of reputation (DPoR) is a lightweight consensus mechanism developed by An et al. to address the issue of costly computation in crowd sensing node data quality monitoring.

The data collected from the sensor nodes of the crowd sensing network was double-checked for quality by Huang et al. using smart contract verification procedures. To promote the exchange of high-quality data, Su et al. developed a reinforcement learning (RL)-based reward system with two levels. Based on game theory, Casado et al. presented a cooperative edge computation layer methodology to improve data quality and enable false data

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

detection.

Peers in IoT networks that lack trust might be incentivized to improve things through a new incentive scheme developed by Shala et al. The system's ability to keep users going is largely due to its control cycles, which include a goal trust score. A bundle of incentives, including discounts on other services, will be offered to service providers with poor trust ratings in exchange for the promised advantages, in the hopes that they can improve their performance. The developers devised a system that rewards both the owners of high-quality (real and practical) medical data for sharing their data and the miners that take part in and validate transactions with cryptocurrency.

Wang et al. developed a plan for a privacy-preserving incentive to encourage outstanding performance among crowd sensing participants. The trust mechanism incentivizes individuals to trade superior sensing data for Bitcoin or Monero. Verifying the accuracy of data is another way data miners can earn a living.

In their proposal for a trust model to assess the reliability of data collected by IoT sensor nodes, Dedeoglu et al. Evidence from observations of surrounding sensor nodes and the data source's reliability and reputation form the basis of the model.

3. SYSTEM ARCHITECTURE

A data trust architecture that benefits data creators and consumers is the goal of our suggested approach. We will accomplish this by explaining two key components of our system design. A trustworthy model that can evaluate the reliability and quality of input data sets and a dependable system that can monitor and record access are necessary for secure and verifiable access control management.

In Figure 1, you can see our data trust framework in action. Our trust model is built using the information we currently have. To verify the validity of an initial dataset, our approach use a blockchain-based software. Using this identifier, the system can verify that the ledger contains only trustworthy data assets and that validation is performed on only trustworthy data sets. The mathematical concepts and parameters that were considered in determining the trust value are discussed in Section V. More checks are needed because the data sets may not be correct with a low confidence level.

A data set can be lawfully requested by anyone who wishes to obtain it, provided that the ledger contains all the necessary information and saves it as data assets. Once the data owner receives the request, they will determine the terms and conditions of access. There is no longer any need for an intermediary to enforce transactions thanks to blockchain and smart contract technology. A smart contract built on the blockchain allows resource owners to grant access to other parties. In addition, data owners can instantly verify the immutable record on the blockchain to view who has or is attempting to access their dataset, regardless of the displayed response.

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

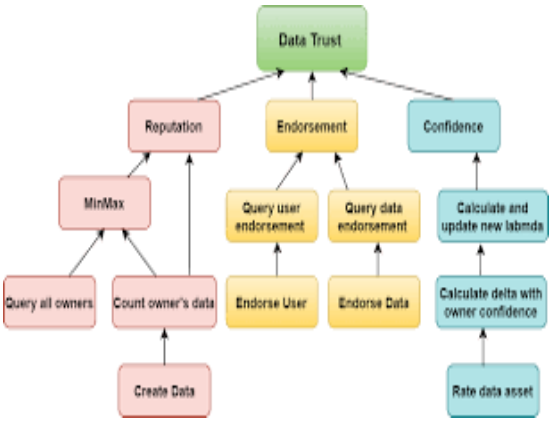

Fig 1: Presents our data trust framework architecture

TRUST MODEL

The steps that need to be carried out in order to compute the reliability score by making use of the data that has been provided are as follows. Those individuals and organizations that have demonstrated an interest in acquiring the data collection that was discussed earlier will be able to gain access to this value at a later point in time. In addition, this value is taken into consideration in real time by the system when it is determining the number of auditors that are required to guarantee the accuracy of the data that has been gathered. If the trust rating is higher, then the number of verifiers that are required to validate the data set will be lowered, which will result in a procedure that is completed more quickly.

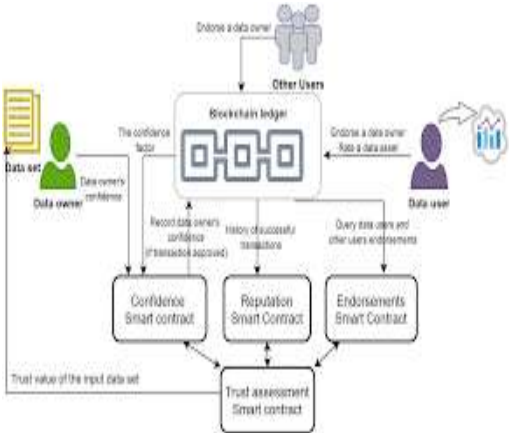

Fig: 2 Trust value for the input data sets

Terminology

The management and security of our distributed data trust architecture rely heavily on data sets. Consequently, these repositories of data are sometimes referred to as "data assets." In the context of data management, the "data owner" is the individual or entity that possesses complete ownership rights to a particular data asset. To access some data, you need a key, often called an identifier, which is a unique integer. To obtain the data asset, one must be the data owner. Data owners have the right to control who can see their data, when they can see it, and for what reasons. The data owner may easily keep track of all the rights that have been provided and taken away in an easily searchable database.

Reputation

The min-max normalization method takes into account the data owner's own successful transaction history in addition to the minimum and maximum values of all users' successful transactions in order to determine the data owner's trustworthiness.

Endorsement

Two primary endorsements are available to data holders. Someone who is well-versed in the system and has expertise working with the data owner may be able to recommend someone to join the first group. The second kind of endorsement is provided by those who have previously examined the dataset that the present data owner is making publicly available. Based on the user's evaluation of the data, a recommendation is made to the data owner. When calculating the data owner's endorsement score for a certain statistic,

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

the second kind of endorsement is more important.

Confidence

The data entry worker will indicate their level of confidence in the acquired data by assigning it a confidence rating between 0 and 1 (confidence [0, 1]). In order for the present data owner to determine the data asset's reliability, past investigations must be documented.

4. RELATED WORK

DATA TRUST

The multifaceted concept of trust has been studied by numerous disciplines, including economics, psychology, computer science, and information technology, among many more. Each of these fields delves into a unique aspect of trust and its applications. Morals, emotions, views, and facts from many walks of life are all entangled in the concept of trust, making it difficult to define and describe. When one party (the trustor) invests their faith in another party (the trustee) within predetermined boundaries, a dynamic relationship known as trust is formed.

The following definition of trust has been arrived at after much academic discussion: trust is the willingness of the trustor to have faith that the trustee will act responsibly to safeguard the trustor's interests in an uncertain circumstance. The trustor has come to this conclusion after considering the trustee's previous treatment of them.

The computational value established between a trustee and a beneficiary is a typical explanation of digital trust. Quantified according to trust qualities, it is evaluated using a standardized technique. Recognizing the interdependence of many pieces and individuals and working to establish a trusting culture are both crucial. O'Hara outlines eight characteristics that are essential for data trusts to thrive.

(1) Discovery
(2) Provenance
(3) Access Controls,
(4) Access
(5) Identity Management
(6) Auditing of Use
(7) Accountability
(8) Impact

- The person raised the possibility of Web Observatory as a technological solution to the major problem of data trust.
- Consumers initially gain knowledge about the nature and qualities of the data they will be accessing through the data discovery process.
- The "provenance" of data and the details around it are its historical context.
- Data owners can manage who has access to their information and make changes to those permissions through access control.
- Consumers of data are granted "access" to the data in order to view and make use of it.
- The term "identity management" refers to the process by which data proprietors verify the identities of individuals who wish to access their data.
- "Auditing of use" in this context refers to maintaining a thorough log of who

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

accessed what information.

- Enforcing access controls and use audits is critical for holding individuals accountable.
- "Impact" in the context of data trust records refers to determining the data's worth, utility, and profitability.

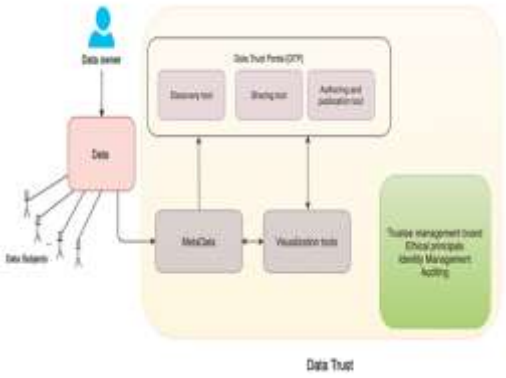

Fig: 3 Data Trust

DATA TRUST PORTAL ARCHITECTURE (DTP)

The Data Trust Portal (DTP) was designed by O'Hara using principles from web observatories, as shown in this picture. To put it simply, DTP does not store any information. The onus is instead on the data owners to ensure the data's security and to select and configure an appropriate interface mechanism for its accessibility. Establishing a safe method of data sharing and retrieval is a breeze with the DTP platform. Metadata describing the origins and attributes of the data are utilized by this protocol.

Data efficiency is a challenge that Stalla-Bourdillon et al. address in their work by releasing a single approach. In this paradigm, the authors emphasize the significance of having clear data governance duties and processes. There are three primary levels to the image that illustrate the concept of data trust.

(1) The data layer
(2) The access layer
(3) The process layer

Fig: 4 Data Trust Portal Architecture

O'Hara drew inspiration for his Data Trust Portal (DTP) from web observatories, as seen in the image. To put it simply, DTP does not store any information. The onus is instead on the data owners to ensure the data's security and to select and configure an appropriate interface mechanism for its accessibility. Establishing a safe method of data sharing and retrieval is a breeze with the DTP platform. Metadata describing the origins and attributes of the data are utilized by this protocol.

Data efficiency is a challenge that Stalla-Bourdillon et al. address in their work by releasing a single approach. Data governance duties and processes should be clearly defined in this framework, according to the authors. There are three primary levels to the image that illustrate the concept of data trus

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

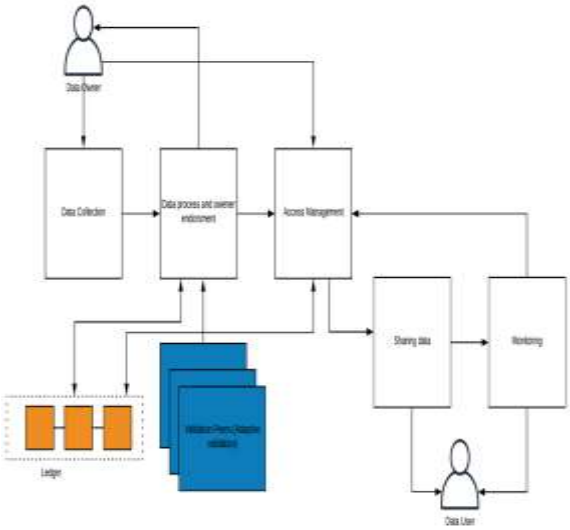

Fig: 5 End to end data trust architecture with adaptive validation

ACCESS MANAGEMENT AND SHARING DATA ASSETS

O'Hara's Data Trust Portal (DTP) was designed with the use of concepts derived from web observatories, as represented by the picture. To put it simply, DTP does not store any information. The onus is instead on the data owners to ensure the data's security and to select and configure an appropriate interface mechanism for its accessibility.

The DTP platform simplifies the process of establishing a secure method of data sharing and retrieval. In order to identify the characteristics and origins of the data, this protocol makes use of metadata.

In their research, Stalla-Bourdillon et al. provide a consistent way to address the challenge of data efficiency. In this paradigm, the authors emphasize the significance of having clear data governance duties and processes. The graphic illustrates the concept of data trust on three primary levels.

5. SYSTEM ANALYSIS

Discovery

Authorized users of the data can access metadata describing the data sets and other information about the accessible data assets through the system interface. Our proposed solution informs data consumers about the quality of the data assets through the trust value it provides.

Provenance

Data owners are obligated to furnish metadata pertaining to the data's provenance, including the data's origin, collection date, and collection method, once their data sets have been added to the system as data assets. This information can be used by data consumers and transaction verifiers to determine the quality of the data. Modifying a data collection also triggers a transaction that updates the data asset's properties on the ledger. By decoupling the actions performed on the data sets, we can monitor the evolution of the data and trace its origins.

Access Control

Owners of digital assets have complete authority over them. With the use of smart contracts, they can easily regulate who has access to their data. You can verify the submitted transactions' validity in further detail with smart contracts as well.

Access

Data sets containing personally identifiable information must be de-identified or anonymized prior to sharing in order to safeguard individuals' interests when allowing others access to their data. If data owners are concerned about other users being able to view sensitive information, Hyperledger Fabric's private data and private communication features could be a

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

good fit. They can make details about their data assets available to anybody interested using this functionality. You can restrict access to the data source and modify the rules of a smart contract at the same time. For instance, data consumers can inquire about the data's origins with the data's owners.

Identity Management

A digital identity backed by an X.509 certificate is required for every user wishing to use the Hyperledger Fabric permissioned blockchain. This identification is crucial in a blockchain network for determining the data and resources that each user has access to. To prove ownership of a digital identity, you can add additional identifiers to it. With these capabilities, data owners can identify those attempting to access their data.

Auditing

Data auditing is a primary motivation for implementing blockchain technology. We can verify every system link and process with blockchain technology. When it comes to exchanging data, blockchain technology creates an unchangeable record of all actions, including changes, requests, grants, and revocations.

The owners of data can see who has accessed their data and when their permissions were changed by looking up previous inquiries. Data consumers have access to a wealth of information, including the history of revisions, sources, and data sets themselves. The ability to automatically create audit trails and keep track of any efforts to breach data makes it easier to detect risks when an immutable log of all data transactions is maintained.

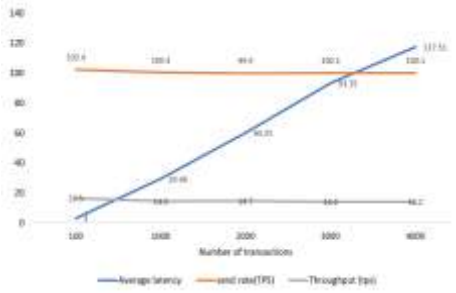

Fig: 6 Send rate, throughput and average latency for Create Data transaction

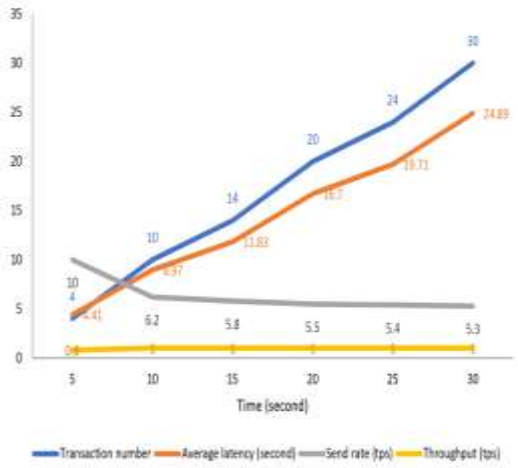

Fig: 7. Calculate and record the minimum and maximum number of data assets belong to a single user (MinMax)

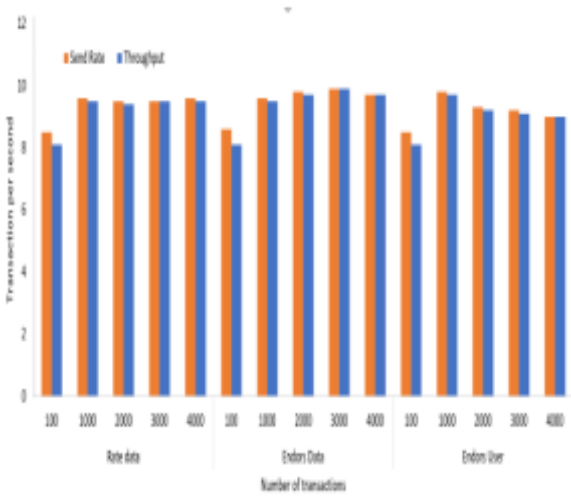

Fig: 8 Send rate and throughput for Rate Data, Endors Data, and Endors User transactions

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

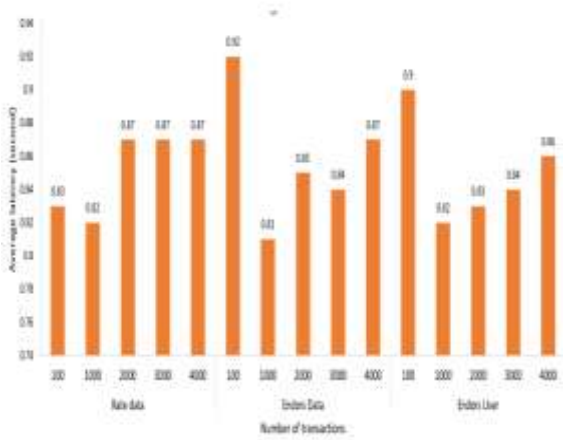

Fig: 9 Average latency for Rate Data, Endors Data, and Endors User transactions

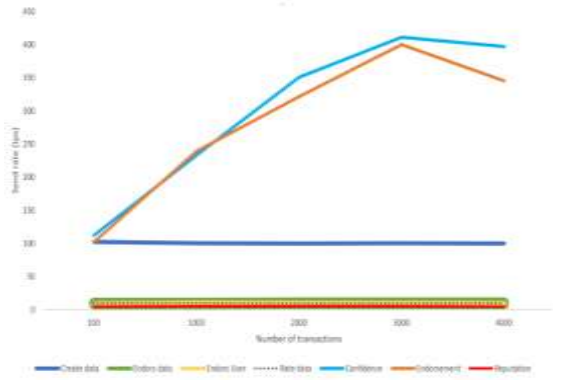

Fig: 10 Send rate for all transaction

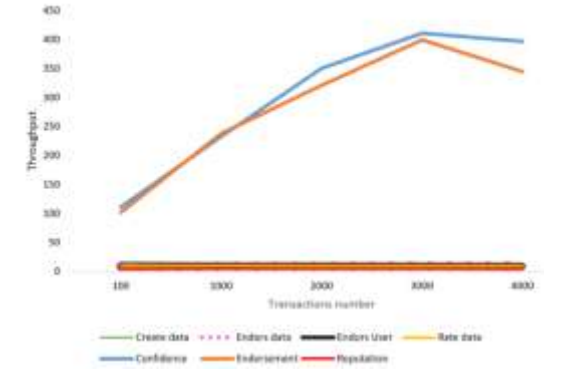

Fig: 11 Throughput for all transaction

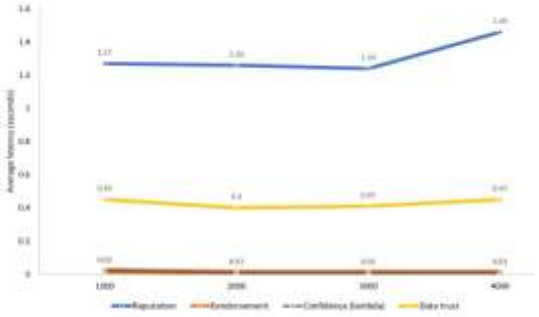

Fig: 12 Average latency for DataTrust, Reputation, Endorsement and Confidence transactions

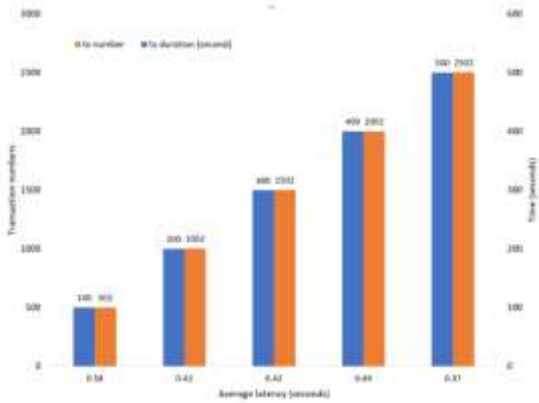

Fig: 13 Average latency for DataTrust based on time

6. CONCLUSION

The inability of present approaches to offer a clear and useful means to transfer data is due to a lack of confidence between parties. An end-to-end data trust system built on permissioned blockchain was demonstrated in this article. To determine the quality of the input data, our method employs a novel trust model that considers the data owner's credibility, suggestions, and faith in the data. This is why data consumers routinely verify and update the public data set to ensure its integrity.

Secure, transparent, and automatically managed access based on smart contracts is something data owners can reap the benefits of as well. Being the sole user in

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

the system gives them complete authority over their data assets and gives them the option to independently govern who has access to what.

The auditability and provenance of blockchain technology allows data owners to view the history of changes made to their data assets, including access limitations. You can gain valuable insights from the ledger, which provides a transparent picture of the system, reveals questionable requests, and highlights rule violations to help you spot potential risks. An abundance of transactions, including writing, editing, and inquiring about trust parameter values, can be handled by the system, according to the evaluation results.

REFERENCES

1. W. Yang, and M. Guizani, "An incentive mechanism for data sharing based on blockchain with smart contracts," Computers & Electrical Engineering, vol. 83, p. 106587, 2020.
2. K. Shrestha and J. Vassileva, "User data sharing frameworks: A blockchain-based incentive solution," in 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2019, pp. 0360–0366.
3. M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1229–1241, 2020.
4. L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM). IEEE, 2017, pp. 117–121.
5. Brandão, H. São Mamede, and R. Gonçalves, "Systematic review of the literature, research on blockchain technology as support to the trust model proposed applied to smart places," in World Conference on Information Systems and Technologies. Springer, 2018, pp. 1163–1174.
6. J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660– 4670, 2018.
7. Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495–1505, 2018.
8. S. Stalla-Bourdillon, G. Thuermer, J. Walker, L. Carmichael, and E. Simperl, "Data protection by design: building the foundations of trustworthy data sharing," Data & Policy, vol. 2, 2020.
9. L. Hang, I. Ullah, and D.-H. Kim, "A secure fish farm platform based on blockchain for agriculture data integrity," Computers and Electronics in Agriculture, vol. 170, p. 105251, 2020.
10. A. Kushida, D. A. Nichols, R.

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com

JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/16
DOI: https://doi.org/10.5281/zenodo.19087709

Jadrnicek, R. Miller, J. K. Walsh, and K. Griffin, "Strategies for deidentification and anonymization of electronic health record data for use in multicenter research studies," Medical care, vol. 50, no. Suppl, p. S82, 2012.

11. S. Rouhani and R. Deters, "Blockchain based access control systems: State of the art and challenges," in IEEE/WIC/ACM International Conference on Web Intelligence, 2019, pp. 423–428.
12. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 1–15.

© 2026 Journal of Digital Engineering and Business Management | www.jdebm.com