**INTRODUCTION**

Data sharing has become a big concern regarding privacy and confidential issues, abusing data, and legal and ethical violations. The lack of a transparent and trustworthy framework for data trust hinders many data owners from sharing their data, which could be vital for many research purposes. Data sharing is not merely a big concern for data owners, but also data users are concerned about the trustworthiness and reliability of the provided data at the origin. Hence, trust is a two-way problem for both data owners and data users. Data trust is a fairly new concept that aims to facilitate data sharing by forcing data users to be transparent about the process of sharing and reusing data. Data trust entails legal, ethical, governance and organizational structure as well as technical requirements for enabling data sharing. Previous studies have suggested the potential of web observatory [1] and institutional repositories [2] for implementing data trust. Block chain technology has salient potential to effectively present the essential properties for creating a practical data . trust framework by transforming current auditing practices and automatic enforcement of smart contracts logic, without relying on intermediaries to establish trust. Many other studies have investigated block chain potential for data sharing, establishing trust and access control. However, those are mostly scattered studies that have focused on a particular step or specific aspect in data sharing or have taken one side of the parties in data sharing by addressing only data owners' concerns. Block chain can be used as a data trust interface between data controllers and data users. The distributed, secure and reliable nature of the block chain can reinforce the trustworthiness of the data trust framework. O'Hara [1] introduces eight properties that should be considered for data trust architecture, including (1) discovery, (2) provenance, (3) access controls, (4) access, (5) identity management, (6) auditing of use, (7) accountability,(8) impact. Some of these properties, such as provenance, auditing of use, and accountability, already exist in the block chain. Because block chain provides a secure, immutable record of transactions, and all blocks are linked together through their hash values. Some other properties, such as discovery, access control, access, and impact, could be implemented through smart contracts and be executed on permissioned block chain. Identity management can be addressed by membership service in permissioned block chains. Ultimately, accountability can reach because multiple peers validate transactions through consensus mechanisms, and the immutable ledger is maintained precisely through cryptographic methods. Besides, every peer has a copy of the ledger, and the network can easily recognize any inconsistency. Figure 1 illustrates how each element in a permissioned block chain can be mapped to the required properties for data trust architecture stated by [1]. In this study, we propose an end-to-end framework for data trust based on block chain, which ensures the trustworthiness and quality of the data at origin for data users and ethical and secure usage of data for data owners. First, we introduce a trust model to assess input data sets' trustworthiness using three parameters: data owner endorsement and reputation, data asset endorsement and data owner confidence level in the provided data set. All these parameters are recorded on the ledger, and they will be updated with every new transaction. We also apply adaptive transaction validation using Hyper ledger Fabric state-based endorsement based on datasets trust value. Finally, we conduct a comprehensive performance analysis to demonstrate our system's efficacy in handling large sets of transactions and scaling across multiple organizations. We state that our system presents all the properties required for data trust. At the same time, it benefits from transparency, immutability, security offered by block chain technology, and smart contracts' automation capabilities [3]. The rest of the paper is structured as follows. Section II introduces the concept of data trust, followed by a block chain-based data trust framework. Section III discusses related studies. The architecture of the proposed framework is outlined in section IV. In section V, we present a trust model to formulate the trust value for the input data sets. Sharing data and access management are presented in section VI. VII presents the experimental results and evaluation of the system. In section VIII, we evaluate our system based on O'Hara's [1] data trust properties. And, Section X concludes the paper.