**CHAPTER-2**

**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. Blockchain 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 blockchain 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. Blockchain can be used as a data trust interface between data controllers and data users. The distributed, secure and reliable nature of the blockchain 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 blockchain. Because blockchain 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 blockchain. Identity management can be addressed by membership service in permissioned blockchains. 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 blockchain can be mapped to the required properties for data trust architecture stated by [1].

**2.1 LITERATURE SURVEY**

# 1. Title: Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship

**Author:** O'hara, Kieron

**ABSTRACT:** In their report on the development of the UK AI industry, Wendy Hall and Jérôme Pesenti recommend the establishment of data trusts, “proven and trusted frameworks and agreements” that will “ensure exchanges [of data] are secure and mutually beneficial” by promoting trust in the use of data for AI. This paper defends the following thesis: A data trust works within the law to provide ethical, architectural and governance support for trustworthy data processing. Data trusts are therefore both constraining and liberating. They constrain: they respect current law, so they cannot render currently illegal actions legal. They are intended to increase trust, and so they will typically act as further constraints on data processors, adding the constraints of trustworthiness

# 2.Title: Trust Modeling and Management: From Social Trust to Digital Trust

# Author: Zheng Yan

**ABSTRACT:** This chapter introduces trust modeling and trust management as a means of managing trust in digital systems. Transforming from a social concept of trust to a digital concept, trust modeling and management help in designing and implementing a trustworthy digital system, especially in emerging distributed systems. Furthermore, the authors hope that understanding the current challenges, solutions and their limitations of trust modeling and management will not only inform researchers of a better design for establishing a trustworthy system, but also assist in the understanding of the intricate concept of trust.in a digital environment.

# 3.Title:An incentive mechanism for data sharing based on blockchain with smart contracts

**Author:** Shichang Xuan ,Li Zheng

**ABSTRACT:** Data sharing techniques have progressively drawn increasing attention as a means of significantly reducing repetitive work. However, in the process of data sharing, the challenges regarding formation of mutual-trust relationships and increasing the level of user participation are yet to be solved. The existing solution is to use a third party as a trust organization for data sharing, but there is no dynamic incentive mechanism for data sharing with a large number of users. [Blockchain](https://www.sciencedirect.com/topics/computer-science/blockchain" \o "Learn more about Blockchain from ScienceDirect's AI-generated Topic Pages) 2.0 with [smart contract](https://www.sciencedirect.com/topics/computer-science/smart-contract) has the natural advantage of being able to enable trust and automated transactions between a large number of users. This paper proposes a data sharing incentive model based on evolutionary game theory using blockchain with smart contract. The smart contract mechanism can dynamically control the excitation parameters and continuously encourages users to participate in data sharing.

# 4.Title: Blockchain-Based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds

# Author: [Meng Shen](https://ieeexplore.ieee.org/author/37085393066); [Junxian Duan](https://ieeexplore.ieee.org/author/37088408058)

# ABSTRACT: The prosperity of cloud computing has driven an increasing number of enterprises and organizations to store their data on private or public cloud platforms. Due to the limitation of individual data owners in terms of data volume and diversity, data sharing over different cloud platforms would enable third parties to take advantage of big data analysis techniques to provide value-added services, such as providing healthcare services for customers by gathering medical data from multiple hospitals. However, it remains a challenging task to design effective incentives that encourage secure and collaborative data sharing in multiple clouds. In this paper, we propose a reliable collaboration model consisting of three types of participants, which include data owners, miners, and third parties, where the data is shared via blockchain and recorded by a smart contract. In general, these participants may acquire and store the sharing of data using their private or public clouds. We analyze the topological relationships between the participants and develop some Shapley value models from simple to complicate in the process of revenue distribution. We also discuss the incentive effect of sharing security data and rationality of the designed solution through analysis towards distribution rules.

# 5.Title: Hyperledger fabric: a distributed operating system for permissioned blockchains

**Author:**  [Konstantinos Christidis ,](javascript:void(0);" \o "Konstantinos Christidis) [Yacov Manevich](javascript:void(0);" \o "Yacov Manevich)

**ABSTRACT:**

Fabric is a modular and extensible open-source system for deploying and operating permissioned blockchains and one of the Hyperledger projects hosted by the Linux Foundation (www.hyperledger.org).

Fabric is the first truly extensible blockchain system for running distributed applications. It supports modular consensus protocols, which allows the system to be tailored to particular use cases and trust models. Fabric is also the first blockchain system that runs distributed applications written in standard, general-purpose programming languages, without systemic dependency on a native cryptocurrency. This stands in sharp contrast to existing block-chain platforms that require "smart-contracts" to be written in domain-specific languages or rely on a cryptocurrency. Fabric realizes the permissioned model using a portable notion of membership, which may be integrated with industry-standard identity management. To support such flexibility, Fabric introduces an entirely novel blockchain design and revamps the way blockchains cope with non-determinism, resource exhaustion, and performance attacks.

This paper describes Fabric, its architecture, the rationale behind various design decisions, its most prominent implementation aspects, as well as its distributed application programming model. We further evaluate Fabric by implementing and benchmarking a Bitcoin-inspired digital currency. We show that Fabric achieves end-to-end throughput of more than 3500 transactions per second in certain popular deployment configurations, with sub-second latency, scaling well to over 100 peers.