

ASSURANCE OF LEGAL COMPLIANCE IN INFORMATION SHARING USING BLOCKCHAIN

Darshana Siriwardana

A dissertation submitted in partial fulfilment of the requirement for
Master of Science degree in Cyber Security and Forensics

**School of Computing
Informatics Institute of Technology, Sri Lanka
in collaboration with
University of Westminster, UK**

2023

ABSTRACT

Online data privacy and ownership has been two of the most debated and regulated topics in the past decade. Some of the service providers that offer online data storage and sharing have acted in bad faith towards end-users and their data. To answer the problems faced by users, governments, regional governing bodies, and regulatory authorities have introduced multiple regulations that protect their citizen's privacy and data. Compliance with these regulations have also been made mandatory. Whilst there are many centralized solutions that provide online data storage and sharing, there aren't many that provide decentralized, regulatory framework-compliant services to users.

In this research, we propose a framework that combines multiple decentralized concepts like Blockchain, Smart Contracts, IPFS, and other novel concepts such as Decentralized Identifiers, and Blockchain Oracles to provide users with maximum privacy and ownership of data while providing compliance with regulatory frameworks. Unlike in traditional software, there are no centralized elements or authorities utilized in this framework. Instead, we leverage the immutable properties of Blockchain, Smart Contracts, and IPFS to achieve legal compliance, data privacy and ownership.

This research was successful in producing a framework which assures legal compliance in information sharing using Blockchain, in a legal framework-agnostic manner. As evidence to this, a comparison of two legal frameworks and compliance achieved has been presented as a part of this research.

Keywords: Blockchain, Data Privacy, Data Ownership, IPFS, Smart Contracts, Decentralized Identifiers, Blockchain Oracles

Subject Descriptors

- Computer systems organization → Architectures → Distributed architectures → Peer-to-peer architectures
- Information systems → Information storage systems → Storage architectures → Distributed storage
- Security and privacy → Security services → Privacy-preserving protocols