Mutable and Privacy-aware Decentralized Ledger for Data Management in Wood Supply Chain Environments

Sidra Aslam [1,2], Michael Mrissa [1,2]

1. *InnoRenew CoE, Livade 6, 6310 Izola, Slovenia*
2. *University of Primorska, Faculty of Mathematics, Natural Sciences and Information Technology, Glagoljaška ulica 8, 6000 Koper, Slovenia*

Wood supply chain (WSC) actors need to store, update, and access data about wood products for traceability purposes. Besides, they need to protect data from unauthorized access and, sometimes, to preserve anonymity (Abeyratne and Monfared, 2016). Typical solutions rely on a centralized third party, which brings security issues such as single point of failure (SPOF). Distributed Ledger Technology (DLT) such as blockchain solves the SPOF problem with data replication on distributed nodes and ensures trust through cryptographic signatures (Toyoda, et al., 2017). However, blockchain relies on full disclosure of immutable data, thus making privacy management and data modification major concerns (Biryukov, et al., 2014).

In this work, we design a decentralized framework that provides data mutability and privacy management while avoiding the SPOF problem. We combine blockchain, Distributed Hash Table (DHT), role-based access control, and multiple encryption mechanisms to provide an end-to-end solution for decentralized data management for the wood supply chain. We designed and implemented a protocol that stores metadata and pointers on the blockchain whereas actual WSC data are encrypted and stored off-chain on a DHT.

Our framework relies on a set of components that apply necessary operations at runtime to protect data. The privacy component implements role-based access control and filters incoming requests. The encryption component decides when data is written, how it should be stored based on meta-information, and when data is read, how to encrypt it.

We implemented a Python prototype and are evaluating the performance of our solution. We expect the overall average time overhead to be reasonable when compared to a typical solution. Further work includes integrating key management solution into our framework as it is the main limitation with respect to fault tolerance and scalability.

Keywords: distributed ledger, wood supply chain, privacy, security

Acknowledgement

The authors gratefully acknowledge the European Commission for funding the InnoRenew CoE project (Grant Agreement #739574) under the Horizon2020 Widespread-2-Teaming program and the Republic of Slovenia (investment funding from the Republic of Slovenia and the European Regional Development Fund) and Slovenian Research Agency ARRS for funding project J2-2504.

References

Abeyratne, S.A. and Monfared, R.P., 2016. Blockchain ready manufacturing supply chain using distributed ledger. International Journal of Research in Engineering and Technology, 5(9), pp.1-10.

Toyoda, K., Mathiopoulos, P.T., Sasase, I. and Ohtsuki, T., 2017. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE access, 5, pp.17465-17477.

Biryukov, A., Khovratovich, D. and Pustogarov, I., 2014, November. De anonymisation of clients in Bitcoin P2P network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 15-29.