This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Paavolainen, Santeri; Antonino, Antonio

Demo: Secure marketplace for access to ubiquitous goods

Published in:

Proceedings of IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021

DOI:

[10.1109/ICBC51069.2021.9461097](https://doi.org/10.1109/ICBC51069.2021.9461097)

Published: 24/06/2021

Document Version

Peer reviewed version

Please cite the original version:

Paavolainen, S., & Antonino, A. (2021). Demo: Secure marketplace for access to ubiquitous goods. In *Proceedings of IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021* IEEE. <https://doi.org/10.1109/ICBC51069.2021.9461097>

© 2021 IEEE. This is the author's version of an article that has been published by IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Demo: Secure Marketplace for Access to Ubiquitous Goods

Santeri Paavolainen*[†] and Antonio Antonino[†]

*Department of Communications and Networking, School of Electrical Engineering, Aalto University, Finland

Email: santeri.paavolainen@aalto.fi

[†]Ericsson, Finland

Email: santeri.paavolainen@ericsson.com, contact@antonioantonino.me

Abstract—Smart contracts in decentralized blockchains can be used to implement neutral exchanges of goods, i.e. decentralized marketplaces. The marketplace actors can audit and trust the correctness and neutrality of the smart contract to act as a neutral third party. While many such marketplaces have been demonstrated, they are constrained to operate in a single blockchain. We present a decentralized marketplace spread over two blockchains, allowing separation of concerns between different blockchains and simultaneously increasing overall performance. The presented marketplace shows how *smart lockers* are rented on the platform, and how access tokens to the rented lockers are communicated securely in a manner that facilitates off-grid physical access.

Index Terms—Blockchain, Interledger

I. INTRODUCTION

Blockchain technologies are frequently seen as a potential benefit to many use cases across multiple fully or partially distrusting parties. For example, decentralized marketplace applications have been found to bring several benefits, especially in terms of reduced degree of control by the marketplace owner and increased privacy guarantees for the marketplace users [1], [2]. Existing demonstrators are often, however, limited to operating in a single blockchain. The use of multiple blockchains offers the possibility of bridging organizational boundaries, increasing performance, separating trust domains [3], and enabling integration of low-power IoT devices [4]. Furthermore, a multi-blockchain infrastructure could greatly benefit systems that enable cyber-physical interactions between users and IoT devices, which otherwise must generally define trade-offs between scalability, security, and availability [5].

SMAUG, or Secure Marketplace for Access to Ubiquitous Goods, is a decentralized marketplace that allows owners of smart lockers to use the marketplace to rent out the lockers in exchange for payment. Potential renters can query available smart lockers and submit rental offers for the time interval of their choosing. The rules of the marketplace are enforced in the smart contract and hence the security of the operations is guaranteed by the Ethereum network consensus and not on the security or trustability of a centrally managed server.

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779984.

Fig. 1. Overall SMAUG architecture, showing the primary active actors (locker owner, locker renter), resources (smart locker), and services (smart contracts, web services).

In this demonstration, we present the marketplace across two separately operated blockchains, the different roles locker owner and marketplace owner assume, and how the mobile application is used to rent and access a smart locker.

II. DESIGN AND IMPLEMENTATION

The marketplace system is structured into different components as shown in Figure 1: a) Marketplace, split further into the Management Backend and the Smart Contract, b) Authorization Service, c) Interledger Service, d) Mobile Application, and e) Smart Lockers. There are two different Ethereum blockchains, one for the Marketplace Smart Contract and another for the Authorization Service. This allows for separation of concerns, as the authorization service can be operated by a different entity or entities, as well as faster turn-around as the authorization blockchain can be run as a consortia blockchain utilizing an energy-efficient Proof-of-Authority consensus with immediate sealing. The two blockchains are bridged by the Interledger Service, implementing a transparent and auditable protocol¹.

The system has four main interaction points visible to locker owner and customers: 1) Smart Locker availability registration

¹<https://github.com/SOFIE-project/Interledger>

and rental request acceptance, performed by the locker owner, 2) Discovery of lockers (via NFC, Bluetooth, or REST API) 3) Rental of a Smart Locker, with escrowed payment on the public blockchain, 4) Granting access to the locker, with direct communication between the locker and the customer's phone running the marketplace application. For a locker to be rented, the locker owner registers the locker on the Marketplace and specifies the constraints for its rental (e.g. price, availability, minimum and maximum rental times) as well as the rental policy, i.e. the locker owner can decide whether to allow the marketplace itself automatically authorize non-conflicting rental requests as they come in, or to manage decisions themselves enabling more complex decision logic. The details of locker owner's operation, including the configuration of the locker is out of the domain of the marketplace itself, but we presume this would normally be done by an IoT device management system. In our case, the locker software parameters are set manually to match the registration.

The complete flow from making the locker available for rental to the issuance of the access token across the two ledgers is achieved with bridging activity of the Interledger service. The cross-ledger data transfer is triggered with the generation of a specific type of event on either blockchain, depending on the direction of the data transfer, and forwarded to the destination blockchain with the invocation of a specific function on the receiving smart contract. The receiving smart contract can then accept or discard the payload depending on the business rules. These events and functions are part of the generic Interledger SOFIE interface. Since all cross-ledger operations are initiated based on activity on either ledger, the behaviour of the Interledger service is completely transparent and can be independently verified.

To enable interacting with the marketplace we have implemented two mechanisms to perform locker rental: a flexible and configurable command-line tool and an Android application running on a mobile. The application implements also the Bluetooth discovery protocol and an NFC protocol allowing direct bi-directional communication between the locker and the phone (these are similarly implemented in the Raspberry Pi-based locker software). The application lacks some of the features implemented in the command line tool, nonetheless allows us to consider the usability of the overall system from a customer's point of view.

A smart locker has been physically realized with a Smart Locker implemented using a Raspberry Pi single-board computer, interfacing with a PN532 NFC reader and a relay-controlled magnetic lock. The locker is shown in Figure 2 along with an example of the application and the locker communicating over NFC to authenticate the renter, allowing him or her to open the locker.

III. APPLICATION AND CONCLUSIONS

We demonstrate a decentralized marketplace, SMAUG, that enables cyber-physical interactions in a secure way without forgoing scalability or availability. While providing a decentralized infrastructure for marketplace interactions, SMAUG

Fig. 2. Smart locker showing NFC interaction with the mobile phone application.

also guarantees a high level of security without requiring the smart lockers to even have Internet connectivity, widening the spectrum of use cases that the marketplace supports, e.g. in places with poor coverage such as basements or remote areas. The throughput of the system is inherently limited by the blockchain used for payment escrow (about 15 transactions per second for Ethereum), as all other portions of the system are either out of this critical path, or can be chosen for the required performance characteristics. We expect that using another blockchain such as Tendermint or Ethereum 2.0 would mitigate the experienced bottleneck on payment escrow transactions.

The SMAUG marketplace is part of the SOFIE EU H2020 Research & Innovation Action project, and has been used as an instrument to validate the integration of the SOFIE framework components developed within the project. We are also looking for ways to extend this work towards other types of marketplaces, for example towards 5G spectrum leasing.

The entirety of the system described here is open source and is available from the SOFIE project's GitHub repository², and can be deployed easily for local testing using Docker containers.

REFERENCES

- [1] H. Subramanian, "Decentralized Blockchain-based Electronic Marketplaces," *Commun. ACM*, vol. 61, no. 1, pp. 78–84, 2017-12, ISSN: 0001-0782. DOI: 10.1145/3158333.
- [2] C. Serban, Y. Chen, W. Zhang, and N. Minsky, "The concept of decentralized and secure electronic marketplace," *Electronic Commerce Research*, vol. 8, no. 1, pp. 79–101, 2008-06-01, ISSN: 1572-9362. DOI: 10.1007/s10660-008-9014-0.
- [3] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger Approaches," *IEEE Access*, vol. 7, pp. 89 948–89 966, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2926880.
- [4] P. Nikander, J. Autiosalo, and S. Paavolainen, "Interledger for the Industrial Internet of Things," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1, 2019-07, pp. 908–915. DOI: 10.1109/INDIN41052.2019.8972167.
- [5] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," *IEEE Access*, vol. 4, pp. 959–979, 2016, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2521727.

²<https://github.com/SOFIE-project/SMAUG-Deployment>