engineering proceedings

MDPI

Proceeding Paper

E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts †

Javier Díaz-Santiso [1] and Paula Fraga-Lamas [1,2,*]

[1] Department of Computer Engineering, Faculty of Computer Science, Universidade da Coruña, 15071 A Coruña, Spain; javier.diazs@udc.es
[2] Centro de Investigación CITIC, Universidade da Coruña, 15071 A Coruña, Spain
* Correspondence: paula.fraga@udc.es; Tel.: +34-981167000 (ext. 6051)
† Presented at the 4th XoveTIC Conference, A Coruña, Spain, 7–8 October 2021.

Abstract: The emergence of the current pandemic has led to a new reality in which bureaucratic formalities have been affected in terms of health security, procedures, resource management, among others. Specifically, in the electoral processes, where the difficulty of fulfilling the social distance and the mobility restrictions reopen the debate on the implementation of other more advanced and modern alternatives, such as electronic voting (e-voting). This article presents the design and implementation of a decentralized e-voting system that has the potential to provide a higher level of transparency, security, and cost-efficiency. Hyperledger Fabric blockchain and smart contracts are used to cast votes, which are then recorded in an immutable way, giving voters anonymity and trust in the fairness of the election process. In addition, promising results of the performance of the e-voting system in terms of latency and transaction load are presented.

Keywords: blockchain; e-voting; Hyperledger Fabric; Hyperledger Caliper; decentralized systems

Citation: Díaz-Santiso, J.; Fraga-Lamas, P. E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. *Eng. Proc.* **2021**, 7, 11. https://doi.org/10.3390/engproc2021007011

Academic Editors: Joaquim de Moura, Marco A. González, Javier Pereira and Manuel G. Penedo

Published: 30 September 2021

1. Introduction

The inexorable advance of the Internet and technology is changing our habits and the way we interact with each other. Despite the countless technological innovations in today's society, there are still processes that employ obsolete and inefficient mechanisms, as is the case of voting, which is mostly done through paper ballots. This article arises from this problem, with the aim of creating an electronic voting (e-voting) application that guarantees immutability and improves the current electoral systems in terms of performance and reliability. To meet this premise, an e-voting system based on blockchain technology is implemented. Specifically, the Hyperledger Fabric platform [1] is used since it allows for the implementation of permissioned networks and is widely accepted in business environments. Thus, this technology is used to develop a decentralized and scalable e-voting system for both public institutions and private business consortiums.

2. Design and Implementation

The proposed e-voting system makes use of a blockchain network implemented through the Hyperledger Fabric platform. Nodes are stored in replicated ledgers on CouchDBs. Data inside the different blocks are secured by cryptographic hashing using the SHA-256 algorithm and are also chained using hash to guarantee the immutability of votes. In addition, the blockchain implemented through Fabric ensures the integrity of transactions through TLS 1.2 certificates for communication between nodes and PKI-based X.509 certificates for node and user authorization.

Figure 1 shows the proposed architecture. This network consists of three organizations, each with a peer node (the one in charge of hosting a copy of the ledger and updating it) and an associated certificate authority. To manage the network communication and to

build and distribute the transaction blocks, a cluster of orderers was implemented, with a certification authority independent of the organizations associated to this cluster.

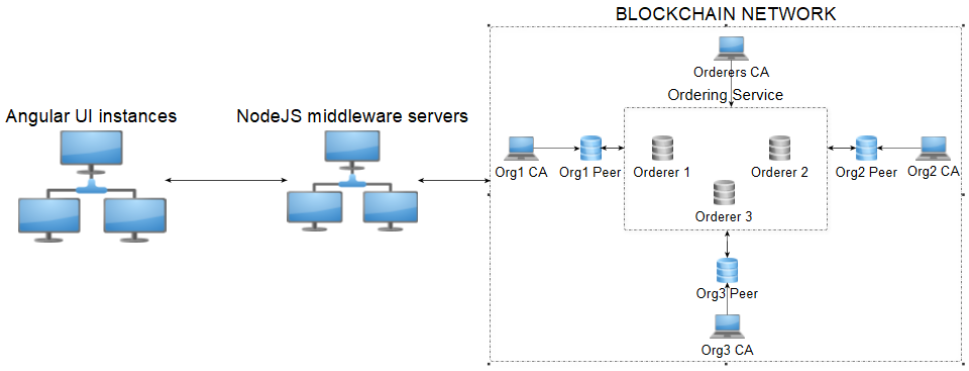

Figure 1. Architecture of the proposed e-voting system.

Two smart contracts were deployed on the Fabric network: one to perform voter validation and another that function as a ballot box, in order to guarantee secrecy and voter anonymity. Additionally, to ensure the authenticity of the network participants, X.509 certificates were used through the Fabric Membership Service Provider component [2]. Such a component is used to abstract the mechanisms and protocols required for the management of these certificates. The generation and validation of the cryptographic material was performed by simulating certificate authorities through the Fabric framework.

In order to support the functionalities of the smart contracts, multiple servers were used in Node.js, with the purpose of guaranteeing the decentralized philosophy of blockchain, specifically on Express. These operations are exposed through an API REST, following the procedure shown in rfc2616. This layer of the application is responsible for managing the authorization within the platform, through the integration of JSON Web Tokens, an open source standard for the generation of access tokens proposed by the IETF in rfc5719. The environment proposed to allow consuming this API consists of a user interface implemented on Angular. It should be noted that this layer of the system has navigation and functionalities restricted according to the role of the user, being the administrators the ones in charge of integrating new data into the system and its monitoring, and the voters are the ones enabled to participate in electoral processes and visualize the results.

Finally, as a complement to the described system, two tools provided by the Hyperledger platform, Explorer and Caliper, were integrated. Regarding the former, it was the entry point for the graphical visualization of the operation of the network blockchain, both in terms of the blocks indexed to the blockchain and the transactions they contain, and in terms of the network participants. Regarding the latter, it is a benchmark tool that allows for analyzing the tolerance of the blockchain network in terms of latency and supported congestion, allowing to verify that the system supports a high load of concurrent transactions without penalizing performance.

3. Results

Analyzing the performance metrics shown in Figure 2, it is worth noting the low latency of the blockchain read operations and the high transaction load supported by the vote casting and total vote listing operations.

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
Create ballot	997	0	50.1	9.86	2.10	6.75	34.9
List all ballots	1000	0	50.1	0.13	0.01	0.03	50.0
List all voters	1000	0	50.1	0.09	0.01	0.02	50.0
Find voter by dni	1000	0	50.1	0.05	0.01	0.01	50.0
List ballot voters	1000	0	50.1	0.09	0.01	0.02	50.0
Get ballot result	1000	0	50.1	0.13	0.01	0.03	50.0
Get ballot by id	2500	0	298.4	8.37	0.16	3.94	284.3
Vote	2500	0	298.5	7.90	0.14	3.75	283.3

Figure 2. Performance of the e-voting blockchain platform developed.

This high transaction load is linked to a high latency, so a study on the number of transactions, shown in Figure 3, was carried out to obtain an optimal performance in terms of latency. As a result, the inflection point from which the e-voting system starts to deteriorate its performance was obtained.

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
Get ballot result	2500	0	100.0	0.06	0.01	0.01	100.0
Get ballot by id	2500	0	150.1	0.10	0.01	0.01	150.0
Vote	2500	0	200.1	0.28	0.01	0.01	200.0

Figure 3. Transactions for optimal performance of the e-voting blockchain platform.

4. Discussion

Regarding the implementation of blockchain solutions, Hyperledger presents problems with concurrency management due to its Multiversion Concurrency Control (MVCC) system, by means of which an entity cannot be modified in concurrent transactions, making it necessary to store composite keys for concurrent changes.

Additionally, although Fabric nodes support 2500 concurrent transactions, the Hyperledger Caliper platform only allows 500 simultaneous transactions, preventing the analysis of the maximum performance of the Hyperledger blockchain.

5. Conclusions

The proposed e-voting system was designed and tested with the aim of studying the feasibility of a decentralized solution capable of supporting the most demanding requirements of both public environments and private business consortiums. In view of the preliminary results, it is clear that blockchain fulfilled requirements for e-voting schemes like transparency, consistency, and resiliency. In addition, it is undeniable the breakthrough that blockchain technology provides in terms of automating processes in an immutable and secure way.

Hyperledger's platform is a relatively new framework that has certain improvable aspects such as concurrency management on the same entity or the early stage of development of complementary frameworks to the blockchain network.

In order to deploy this system in a real-world environment, additional performance tests and audits need to be performed to ensure scalability and robustness in large-scale elections.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. The Linux Foundation, Hyperledger Fabric. Available online: https://www.hyperledger.org/use/fabric (accessed on 3 August 2021).
2. Membership Service Provider. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/msp.html (accessed on 3 August 2021).