

Research Article

A Manipulation Prevention Model for Blockchain-Based E-Voting Systems

Ruhi Taş^{1,2} and Ömer Özgür Tanrıöver¹

¹Department of Computer Engineering, Ankara University, Ankara 06830, Turkey

²Turkish Radio Television Corporation, IT Department, Ankara 06550, Turkey

Correspondence should be addressed to Ruhi Taş; ruhtas@yahoo.com

DWV[hW \$" 6 VWV TVM \$" \$" - DVM[eW \$%? SdZ \$" \$#- 3UWdFW ## 3bd[^\$" \$#- BgT [eZW \$* 3bd[^\$" \$#

Academic Editor: Vincenzo Conti

Copyright © 2021 Ruhi Taş and Ömer Özgür Tanrıöver. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security and trust are seen as the most important issues in electronic voting systems. Therefore, it is necessary to use cryptographic procedures to ensure anonymity, security, privacy, and reliability in these systems. In recent years, blockchain has become one of the most commonly used methods for securing data storage and transmission through decentralized applications. E-voting is one of these application areas. However, data manipulation is still seen as a major potential problem in e-voting systems. In the proposed model, administrators or miners are prevented from previewing election results which are normally accessible data due to the blockchain structure. A double-layer encryption model is proposed and tested to prevent manipulations that may occur with the election results. It is ensured that the election results can be counted after the participation of all stakeholders at the end. In this way, potential manipulations may be prevented during the election period. As a result of the model, the privacy of voters is ensured, no central authority is needed, and the recorded votes are kept in a distributed structure.

1. Introduction

A fair election is desirable by everyone. Frequently, there are doubts in the minds of voters related to the voting procedures, counting processes, and the announcement of results [1–3].

Election systems have evolved depending on the needs and developments of the time during which they were developed. Technological developments or possible innovations to every field; likewise, it is thought that digitalization mechanisms to be added to voting systems can minimize human errors [4]. But, unlike paper-based electoral systems, problems such as system failure, network security, and information security may arise with an electronic voting system.

One of the most important issues in e-voting systems is the security weaknesses made by people inside or outside who are authorized to access the system. A decentralized design and cryptographic data storage security approach may have the potential for solving these problems. Normally, cryptography is mainly used to encrypt information such as

voter data, votes, and voting results before data are stored on the server. Therefore, the system can ensure the authenticity and security of the voting information [5]. In this context, various additional features and solutions have been proposed to be integrated into election systems. Development work is still ongoing. Different types of improvements to e-voting have been done to provide easy election organization, easy participation, and low cost. Accordingly, various enabling technologies have been adapted ranging from biometric authentication to remote voting [6, 7] to kiosk systems [8] or to mobile voting systems [9]. Nowadays, the security and privacy of blockchain platforms have attracted great attention. Recently, blockchain-based voting systems have been proposed [10–13]. However, it is stated that such systems still have trust problems. Abuidris et al. [14] and Ghosh et al. [15] state the risks and vulnerabilities of blockchain applications. In e-voting systems, the guaranteeing the security of the votes is seen as one of the most important problems. An attacker can copy and decipher passwords if he has sufficient computational power or when

