Chapter 71
Secure Digital Voting System Based on Blockchain Technology

Kashif Mehboob Khan
NED University of Engineering and Technology, Karachi, Pakistan

Junaid Arshad
The University of West London, London, UK

Muhammad Mubashir Khan
NED University of Engineering and Technology, Karachi, Pakistan

ABSTRACT

Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as increased efficiency and reduced errors. However, challenges remain to the achieving of wide spread adoption of such systems, especially with respect to improving their resilience against potential faults. Blockchain is a disruptive technology of the current era and promises to improve the overall resilience of e-voting systems. This article presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The article presents details of the proposed e-voting scheme along with its implementation using Multichain platform. The article also presents an in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme.

1. INTRODUCTION

Elections are fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever-evolving domain. This evolution is primarily driven by the efforts to make the system secure,

DOI: 10.4018/978-1-7998-5351-0.ch071

verifiable and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in 1960's, e-voting systems have achieved remarkable progress with its adaption using the internet technologies (Gobel et al., 2015). However, e-voting systems must adhere to specific benchmark parameters so as to facilitate its widespread adoption. These parameters include anonymity of the voter, integrity of the vote and non-repudiation among others.

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks (Rosenfeld, 2017; Kadam et al., 2015; Nakamoto, 2009). Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains (Nakamoto, 2009; Kraft, 2015; Narayanan et al., 2015).

Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity. In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to-verification. We believe e-voting can leverage from fundamental blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result.

The focus of our research is to investigate the key issues such as voter anonymity, vote confidentiality and end-to-end verification. These challenges form the foundation of an efficient voting system preserving the integrity of the voting process. In this paper, we present our efforts to explore the use of the blockchain technology to seek solutions to these challenges. In particular, our system is based on the Prêt à Voter approach (Ryan, 2008) and uses an open source blockchain platform, Multichain (Multichain, 2017) as the underlying technology to develop our system. In order to protect the anonymity and integrity of a vote, the system generates strong cryptographic hash for each vote transaction based on information specific to a voter. This hash is also communicated to the voter using encrypted channels to facilitate verification. The system therefore conforms with the fundamental requirements of an e-voting system as identified by (Rura et al., 2016). More discussion around this is presented in section 2.

The rest of the paper is organized as follows: the next section presents the requirements for an e-voting system as identified by (Rura et al., 2016) and explains how our proposed system fulfils them. Section 3 presents the state-of-the-art with respect to e-voting and how we contribute to it followed by a detailed description of the system design in section 4. Section 5 presents the implementation of our proposed system with Multichain and user interface along with evaluation of the system highlighting