Evolution of Bulletin Board & its application to E-Voting – A survey

Misni Harjo Suwito[1] and Yoshifumu Ueshige[2] and Kouichi Sakurai[3]

***Abstract*—The voting process is fundamental to any democratic system – be it a country or a company's boardroom. Nearly forty years ago, e-voting was theoretically perceived as a more efficient replacement of the widely existing paper-based traditional voting system. Several research works have been carried out to ensure more security and efficiency in different settings for e-voting schemes. One of the fundamental building blocks of e-voting systems is the public Bulletin Board through which several security properties are achieved. After introducing Blockchain technology, the bulletin board has found a new meaningful and concrete way of distributed way of implementation. Before Blockchain technology, either such a system was theoretically assumed or perceived as a public broadcast channel with memory. In this survey, we present a concise survey of bulletin boards' evolution with a typical application to the e-voting systems. We note that bulletin boards have other applications in other joint computation areas. Still, we are interested in evolving e-voting systems based on bulletin board and how several desired security properties are realized through bulletin boards.**

***Index Terms*—E-voting, Verifiability, Receipt Freeness, Bulletin Board, Blockchain.**

I. Introduction

EVoting system was invented to provide better service in terms of convenience, security, and efficiency to overcome traditional voting systems' shortcomings. However, with all the advantages that e-voting has, there are significant potential unresolved challenges such as privacy, transparency, verifiability, receipt-freeness, and coercion resistance. E-voting has been known as a very challenging cryptography theme because of the motivation of voter anonymity and to ensure voters' privacy [1]. Blockchain technology was first proposed to protect digital information from various threats and interference. Finally, this Blockchain technology has proven that, after a decade to become an agent of change revolutionary shift. Blockchain is a platform that can share data in a decentralized, eliminate third party, and transactional manner across large, untrusted networks. Blockchain can be applied in various fields such as supply chain, ownership management, protection of civil infrastructure, electronic wholly independent, and decentralized architecture in its operations without the possibility of influencing the process memory to help achieve global verification. Bulletin Board is a communication channel that can be used publicly, and anyone can read all the information received by the Bulletin Board. After everyone has received information and read it, an election council keeps it, which cannot be deleted or modified. The purpose of this paper is to provide those interested in building an electronic bulletin board system. This report will also explain how the bulletin board system can be implemented and the possible problems, and how the solution is.

[1]. Misni Harjo Suwito is with Department of Informatics, Kyushu University, Fukuoka, Japan & Faculty of Computer Science, Mercu Buana University, Jakarta, Indonesia. Email: misni.muhammad@mercubuana.ac.id

[2]. Yoshifumu Ueshige is with the Center for Info. and ComTech., Nagasaki University, Nagasaki, Japan. Email: yueshige@nagasaki-u.ac.jp

[3]. K. Sakurai is with Faculty of Information Science & Electrical Engg., Kyushu University, Fukuoka, Japan. Email: sakurai@inf.kyushu-u.ac.jp

A. Blockchain Technology

In this sub-section, provided a short description of Blockchain technology which was proposed to protect digital information from various threats and interference. Blockchain is a platform that has the potential to share data in a decentralized manner, can eliminate the role of a trusted third party, and transaction across large, untrusted networks, immutable, and transparency.

Blockchain works making blocks and arranged into links with specific identifiers. Distributing the current block with the previous block occurs by hashing. Each node in the network is synchronized with previous hashing by the same hash data across the network. Fig. 2 describes how Blockchain work and transaction procedures. Hash is a data structure to stored of the transaction records in the block. If changing hash in a block, automatically changes the hash value causing the Blockchain become invalid. [2].

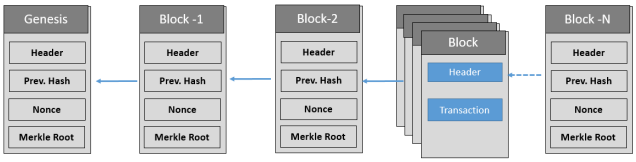

Fig. 1. Outline of a typical Blockchain - how it works

1) Smart Contracts: This term first was coined by Nick Szabo in 1994 as a digital transaction protocol that executes contract terms [3]. The basic concept of the Smart Contract is as an interpreter of contract clauses (collateral damage, bonds, etc.). Into a script (code), and embed it into properties (hardware or software) that can force it, to minimize the need for trusted intermediaries between parties who carry out transactions carried out in a decentralized environment (e.g. Blockchain). These contracts are written using the Solidity programming language, which is a combination of C ++ , Python, and JavaScript.

2) Ethereum: Ethereum is a platform for development a Blockchain network [4]. Ethereum provides a wider range of cases, with the power of smart contracts. For most applications

that use a web server, Ethereum can be operated or can be run through this smart contract.

B. The Bulletin Board

This section, first provided a short description of Bulletin Board. In Paris (Colonne Morris) and Berlin (Litfaßsäule) in the 19th century, the first commercial advertising "cork boards" were patented and approved by George Brooks [5] in 1924. It then continued to experience rapid development in the 20^{th} century, and similar inventions to "cork boards" were widely used as local communication.

The rapid development of electronic media has turned the attention to bulletin board system (BBS) to overshadow analog bulletin board (BBA). BBA as a model for bridging many-to-many communications as a pioneer for computer networking services. In 1978 [6] in Chicago, the First Dial-up Bulletin Board was created very similar in function and features to its predecessor analog bulletin board (BBA). Cohen & Fischer [7] in 1985, proposed a voting protocol using cryptography which involves a public repository where all interested parties post all data related to voting (cryptography keys, voters list, candidates, registration information, ballots, audit information etc.). This repository was called Bulletin Board (BB) and was defined as a broadcast or publication channel with memory.

1. Definition of Bulletin Board

Electronic Bulletin Board can be defined as a computer system service that offers senders or users to send and read electronic messages, transfer files, and other data that are of interest to the general public rather than indicated by certain circles. This digital/electronic information exchange system (bulletin board) is implemented on computers connected to the Internet network. Billions of bulletin boards are scattered and can be found all over the world (as mentioned earlier). The most bulletin boards are operated by companies and agents, and some are operated by individuals from their homes.

2. Utilization of Bulletin Board. Bulletin Board utilize as broadcasting channel with memory [8] consists of three entities – (1) readers, (2) writers, and the (3) Bulletin Board itself. The board allows writers who have been assigned to publish messages or information – messages cannot be changed or deleted in any way, if one tries to perform any sort of modification it is identified by the readers. The Bulletin Board itself is public, meaning that everyone can read the published messages. Bulletin boards function or are usually used for universal verification [9].

Several papers repeatedly emphasized the consistency and need for Bulletin Board in e-voting. Benaloh [10] assumes Bulletin Board for auditing, and also affirms that "implementing Bulletin Board may be a problem for itself". It is important for all engaging parties to develop and implement a reliable Bulletin Board to use in e-voting. In literature, proposals regarding construction of secure and efficient Bulletin Board are described in [11] [12] [13] [8] [14]. The most realistic examples which include a Bulletin Board that is applied to the e-voting system is vVote [15] [16], and then, from the D-DEMOS system known as *internet*-voting (i-voting) [17]. In almost all cases of this voting system, the Bulletin Board is introduced and is an integral part of the electoral system or specifically e-voting [12], [17], [11], [13], [14], [19],and [20].

C. E-voting System

This section, provided a short description of security properties, entities in e-voting system and election process.

The security properties of an ideal voting scheme are as follow

1) **Eligibility:** Eligible voters, without any exception, who satisfy eligibility criteria can vote and participate in the voting process. In most of the existing systems, a voter is eligible to cast one vote.
2) **Privacy:** Vote of any voter must be kept private and should not be exposed to anyone.
3) **Integrity:** The voting system as a whole must be integrated. Also, the accuracy and consistency of votes must be maintained and the final counting process guaranteed.
4) **Fairness:** The results of the provisional voting must not be leaked until the vote is declared complete. This is to ensure that fair decisions can achieve for all.
5) **Robustness:** It is desirable that the scheme is able to tolerate misbehaviour from certain number of entities in the system who have malicious intent.
6) **Verifiability:** In general, two categories of verifiability notions exist:
   - **Individual Verifiability:** Each and every voter must be able to check whether their vote is included into the system and counted correctly during tallying process. Individual verifiability then subdivided into: *poor verifiability* and *robust verifiability*. The poor version is to guarantee that a voter is able to verify if his vote has reached the appropriate place and being counted during tallying phase. In the robust notion of verifiability voter can also verify his vote which may include his choice of candidate.
   - **Universal Verifiability:** Any auditing agency (may or may not be part of the system) is able to verify that the published results equal with the number of total votes.
7) **Receipt-freeness:** Receipt-freeness of a voting scheme is to ensure that no voter can get hold of evidence (i.e. receipt) so that the voter cannot convince the other party that he has chosen, for example (voted a particular candidate).
8) **Vote-selling Resistance:** Misbehaving voters for various reasons wanting to sell their votes to the buyer and will follow orders from the buyer to select a particular candidate. This vote-selling can be done in two different ways: selling the credentials and entire identity directly to the buyer or providing the buyer with proof that he is following his guidance. Resisting this types of vote-selling process is an important requirement.
9) **Coercion resistance:** An important property that is desirable for any e-voting scheme is to empower an *honest* voter to cast according to his choice. Nothing can influence or dictate his choices against his original intention. However, specifically, this property has attracted

a lot of attention from researchers. It is very difficult to formalize appropriately and is very challenging to implement.

D. Entities in Voting System

The briefly of review entities an e-voting system, which have been common to most of the works existing in the literature [21]–[24] viz. voters (V_i), candidates (C_i), registration authority (RA), election authority (EA), tallying authorities (TA).

- **Election Authority (EA)** EA has the authority to regulate all voting preparations for example; initialization, starting, and ending the casting process, maintaining all election parameters, validating voters, candidates, and other important tasks such as designing and *constructing* ballots in collaboration with the tallying authority (TA).
- **Registration Authority (RA)** This authority plays an important role to organize voting and is responsible for authenticating voters during the registration phase. Here, the voter should sign up to the e-voting system. The voters obtain their public keys (PK_i) and secret keys (SK_i).
- **Tallying Authorities (TA):** In general, the counting process can use an external account(s) owned. Modeling the tallying authorities can be done in a different manner which is suitable for the electoral system – for example, only a centralized authority or there may be multiple authorities. In addition, TA has the authority to make ballots with EA, collect all encrypted ballots, count valid ballots and issue them for voters/auditors to verify the accuracy of the final counting process.
- **Candidate (C_i)** Candidate is a person who has been declared by an electoral commission valid, and has been registered by the administrator as the candidate to be . For the candidate can be defined to vote as C_i to make it suitable for vote tallying.
- **Voter (V_i)** Voter are people who have the right to vote and generally are included in a list. Each valid and eligible voter has been awarded and created an account by the **EA**. authorities. They need to register with the voting system before they cast their votes. Each voter (V_i) has a key pair, private key, and public key. A valid public key must be added to the voter list after authentication. By using an authentication system, all electoral systems must provide voter information that qualifies and who does not. Only eligible voters (V_i) can vote, others are rejected.

In line with the entities mentioned earlier, there are several other important components that are particularly relevant for implementing large-scale elections.

- **Voter ID card:** Voters who have met the eligible, register at the registrar's authority, and then are given a Voter's ID. ID Cards usually contain all voter identity data and include voter Biometric data [25]–[27], public keys, and private key pairs. Election authority signs the voter's ID card with a digital signature with a Biometric template to bind the voter's identity. This is the same as the process of digitally signing ID cards which makes the voting process resilient to *(simulated attacks)*.
- **Polling Officials:** This officer is responsible for checking all eligibility of voter ID cards (to verify requirements), on election day, when voters start voting, and determining the place of voters according to voter ID cards and sending voters who register electronically and cancel a registration after the election is declared complete (only once).
- **Public Bulletin Board (BB):** Public Bulletin Board is a channel for publication with memory [13] enabling the parties involved in the protocol to publish messages, and while providing assurance that the message cannot be deleted and modified. Public Bulletin Board means that all published information can be seen publicly (everyone can view the content but cannot write on it). In another scheme Public Bulletin Board that means a part of memory that is universally accessible.

E. Contribution of this paper

We concentrate on performing a comprehensive survey on implementing an e-voting based on Blockchain. In particular, the main contributions of our survey can be summarized as follows:

- We review of existing Bulletin Board suited for constructing e-voting. In literature review, we describe how a Bulletin Board is implemented or at least perceived before the advent of blockchain technology.
- We sum up of challenges that Bulletin Board might face. Then we propose a thorough list of requirements as uniform criteria that can serve as a measure to evaluate the performance of Bulletin Board as a building block e-voting system.

The remainder of the paper is organized as below. We provide the Bulletin Board in Blockchain e-voting in Section II. In Section III, overview of Bulletin Board includes functionality of bulletin board and review of an existing bulletin board system. In section IV, security issues and analysis of bulletin board including operational and organisational issues are discussed. Implementation of bulletin board including basis functionality and properties are discussed in Section V. Related Work in section VI. Finally, conclusion and future work are provided in the last section.

II. Bulletin Board in Blockchain e-voting

This section, introduced protocol and entities when the Bulletin Board is used through Blockchain based e-voting. Assuming that all information published on the Bulletin Board can be read by anyone, after the bulletin receives information. Some of the entities involved in the voting process are as follows:

- **Election Authority (EA):** Determines the electoral context (initializing, running and stopping, authenticating valid voters, and working with the counting authority (TA).
- **Node (Polling Station):** When the Election Authority makes an election, each voter, smart contract ballot,

represented to all nodes in the network, is distributed to the Blockchain.

- **Bulletin Board Authority (BBA):** Officers who are authorized to manage and manage the Public Bulletin Board and all network infrastructure, nodes (pooling stations), and servers.
- **Voter** (V_i)**:** A person who has the right to vote during the election day which has been determined by the electoral authority (EA).

The brief description of the voting protocol as following assumed that each voter (V_i) can only write into the designated area on the Public Bulletin Board. Here we distinguish four main phases (Initialization, Casting, Tally, and Verify) in sequence as explained in the following protocol:

- **Vote Initialization:**
  1) All election parameters are generating by the electoral authorities and published on the Public Bulletin Board.
  2) The Election Authority has the authority to determines when voting begins and ends, which adjusted to the time zone and constituency.
  3) The Administration Authority has elected to publish a valid voter list on the Public Bulletin Board.
  4) EA anonymizes valid voter lists.
  5) Each anonymized voter determined by the polling area Bulletin Board Authority.
  6) The Election Authority issues a published public key encryption on the Public bulletin board.
- **Vote casting:**
  1) EA provides a message throughout the node (PS) to begin the voting process and establish vote conditions (possibly, and establish cooperation with TAs)
  2) Every voter (V_i) encrypts its votes and issues ballots through the appropriate Blockchain in the designated area on the public bulletin board. Each voter receives confirmation that his ballot has been published.
  3) Every voter (V_i) has finished has given his vote. It is possible for a voter to vote multiple times, only the last vote counted.
- **Vote Tallying:**
  1) Every valid ballot encrypted votes distributed through the Blockchain is then published to the Public Bulletin Board.
  2) Election Authority anonymizes and encrypts each valid vote, and decrypts, then distributes it through the Blockchain. Subsequently published in the Public Bulletin Board.
  3) Tally Authority (TA) completes the vote count in accordance with the time determined by the EA.
- **Vote Verification:**
  1) Each voter (V_i) has or receives an ID card from RA (registration authority) to verify his vote.

III. Overview of Bulletin Board

In this section, the review of Bulletin Board. Ubiquitous Bulletin Board, wherever you are, both in small cities, in the city center, and even in modern cities, it is very full of various types of bulletin boards can be found overall in the world (digital big screen or billboards, big poster, ect).

A. Ubiquitous Bulletin Board

The Bulletin Board can be found in offices, both private and government, and modern offices, for example, bulletin boards through large screens, individual PCs, posters, leaflets attached to boards, in the form of printed paper, newspapers, books, journals, magazines, etc. Besides, there is a bulletin board on each person, which can be called an online bulletin board (OBB) e.g, smartphone, tablet, gadget, etc.

The Bulletin Board is a very sophisticated in the century of revolution industries 4.0 which can be called an electronic bulletin board (EBB). These means, most of people activities use electronic media for example, conference, meeting, work from home (WFH), school from home (SFH), using (zoom, google classroom, Webex, Microsoft Team, Google Meet, Jitsi, Big Blue Bottom, What App, and Skype) and Facebook, Twitter, Instagram, Youtube, Goole Drive, Dropbox, ect, developed into digital bulletin board (DBB) [28]. Towards the industrial revolution 5.0 which means that humans are very important as satisfying public services supported (Smartphone, Tablet, and Gadget), all messages posted to the public bulletin board and visible (everyone can see it) after it was published, it cannot be deleted and tampered with [28].

B. The functionality of Bulletin Board

The Bulletin Board System plays an important role in various fields. For example in the voting case, posting all data related to voting (cryptography keys, voters, candidates, registration information, ballots, audit information, etc.). This repository is called the Bulletin Board and is defined as a broadcast or publication channel with memory.

The following are some of the functionalities provided by the Bulletin Board:

1) The Bulletin Board System assigns service requests to certain servers. Bulletin Board System places request data in a valid server request queue.
2) The Bulletin Board System maintains dynamic, how large/many requests are waiting for a particular server queue, and how large/many requests have been processed.
3) The Bulletin Board System provides server location transparency and allows applications to be developed independently of use. The development and deployment costs must be considered minimized.
4) The Bulletin Board System supports service name aliases, multiple names to be assigned to the same service and very useful for building translations, such as getaway.

C. Bulletin Boards before the advent of blockchain

This section, a short description of history of Bulletin Board before an architecture of blockchain was introduced. We note that during this time, bulletin board was assumed

to exist without concrete specification of implementing them. The various e-voting protocols without focusing how the functionality of BB's were used and implemented them in reality. Several schemes existing Bulletin Boards can be seen in Table I.

Chaum [31] pointed out the importance of security – confidentiality and integrity are two very important properties needed to hold throughout protocol conversation. Blind Signature much-needed to anonymize voters and ballots in elections. Chaum [32] proposed that during a voting process, high transparency ensuring confidentiality of votes with careful auditing the counting and recording process are the fundamental properties. Security, privacy and verification guarantees are not only applicable to the consumer side but as a whole to a voting scheme. Each voters verify that their votes are accurately included in the tallying process, election verification must put confidence on the correct behavior of vote-counting [34].

Juels et al. [44] each legitimate voter will get credentials from the Register Authority. Each voter encrypts their credentials and the chosen candidate is encrypted by using the public key tallies. Ballots will not be counted, without valid evidence and will be removed at the counting stage. This protocol requires untappable channels in the registration phase which means the credentials cannot be disclosed to anyone. The scheme proposed by Smith et. al [50] is an efficient scheme based on [44] but according to [49], the system is not proven.

Civitas [45] proposed e-voting scheme could achieve coercion-resistance and improved and upgraded the scheme by [44]. Each voter gets personal credentials and compatible public credentials published on the Bulletin board ensuring the integrity of the voting scheme. Personal credentials are derived from registering authority and is distributed using Needham-Schroeder-Lowe (NSL) protocol [52]. The main goal of Civitas is same as [44] – to defend itself from coercive attacks. To address scalability issue, each voter is grouped into blocks to help Civitas reduce computation time with respect to [44] which did not consider time efficiency.

Meng et. al [48], proposed an e-voting scheme that uses a commitment ([53] called a BCP commitment scheme) to generate keys that used to validate voter identity interactively. Then voter will choose a candidate and then encrypt using BCP or commitment. In tallying phase, this scheme uses a collision-find algorithm (CFA) to verify and validate ballots. There is great potential that voters can generate fake credentials in deniable encryption schemes and can deceive coercers. One positive aspect of the scheme is that no secure communication channel is needed for communication.

Araujo et al. [49] developed AFT which can achieve universal-verifiability and receipt-freeness based on the ideas of [44] to defend against voter coercion. There is an improvement to this scheme which is to reduce the time complexity from quadratic to linear. Juels et al. [44] claimed that this scheme is resistant to three attacks of coercion which the authors have also demonstrated.

Selection [51] is an e-voting scheme with protocols that achieve verifiability on internet voting. This scheme requires each voter to register at a private booth in person and get a password from voting system which is a panic password [54]. The votes are encrypted using homomorphic encryption and then published in a public register.

D. Reviewing existing Bulletin Boards Systems

This section, a reviews six of the main existing Bulletin Board systems and how they are implemented in the context of e-voting system. More concretely, we study Peters' bulletin board [13], [19], [14], STAR-Vote bulletin board, D-DEMOS bulletin board and e-voting Services of Dini.

1. Peters' Bulletin Board. Peters [13] has studied more than one protocols for secure broadcast channels. Then he compared the communication and computation complexities, type of threats to the system and chose to implement various proposed protocol variations [29] over group membership protocol [30]. The aim of the study was for the implementation.

Peters replaces digital signatures with threshold signatures, which aim to increase the complexity of communication and computing. However, it eliminates the need of trusted third parties – it emphasizes that to obtain a fully distributed bulletin board there is no need for reliable arrangements. In the setup phase, Bulletin Board completely distributed and, therefore, using the threshold signature scheme only tolerates $t_c < \frac{N_c}{2}$ faulty members and by definition $t_c + 1$, signature shares are needed to produce a valid threshold signature. The scheme of [35] is considered to be the most suitable by Peter's in his work. Beuchat [37] in his thesis, implemented BB based on the work of [13] using the threshold signature scheme of [36] which required a trusted third party to generalize keys. A detail description and set-up of the protocol is at Peter's work.

2. Heather & Lundin's Bulletin Board. The authors [19] were motivated by the e-voting system security properties. For example, irreversible history is an analog of immutability (no items can be removed from Bulletin Board after being published); certified publishing is an analog of stability (only items that have been approved for publishing can appear on the Bulletin Board) and accuracy of publication captures that every item posted must be published in the end. A system containing one partner (proposed by the authors) can prove that the system has fulfilled the requirements mentioned above. This system uses locking and hashing techniques. They briefly discussed what approach might be, but ignored the substantial system and security analysis for future work.

3. Krummenacher's Bulletin Board. Krummenacher [14] was inspired by the proposal that was introduced by [19] concerning the distributed BB system related to the e-voting system. The aim was to improve and approach proposed by Heather–Lundin. In other words, it aims at achieving error-tolerance and distributed nature of BB by using light threshold signatures. But Krummenacher makes stronger assumptions, for example by assuming that there is adequate public key infrastructure and that the system was distributed using RSA threshold signatures [36], which requires highly trusted dealers.

There are two versions of the protocol, one in the synchronous model and another in the asynchronous model. The synchronous version is not compatible with e-voting systems, because it may not tolerate a large number of requests due to locking. Asynchronous protocol in other versions, users post messages independently to I from their N_c counterparts. In this case, it is not guaranteed that all peers in I also publish messages because the threshold signing is not used.

4. STAR-Vote Bulletin Board. STAR-Vote [38], [39] is a kiosk-based e-voting system designed to tolerate faulty colleagues, has a function to collect votes and then publish at the end of the election period. The arrangement is different from remote e-voting system. In STAR-Vote, the voting terminals is important plays role as the Bulletin Board. Consequently, the collection of votes left untreated and only the counted votes tracking problem is considered. This is claimed to be solved using the approach of [40]. The concept is based on the existence of voting terminal (a polling station) where maintenance of the voting log uses a hash chain where the votes are only hashed into the chain and log for immutability. This scheme cannot be implemented on a remote voting setting when the system must scale and handle multiple users posting items. The web bulletin board (WBB) through the voting terminal(s). But it does not solve the problem of the inconsistency of the polling terminal itself.

5. D-DEMOS Bulletin Board. Chrondors et al. [17] proposed a distributed voting system for the Bulletin Board known as D-DEMOS, [18]. This scheme depends on the electoral authority, but the function of the bulletin board is divided into two distributed sub-systems. First one is a vote-collection (a.k.a IC sub-system) and the second is a sub-bulletin board (a.k.a sub-system web bulletin board or simply, WBB sub-system). The IC sub-system is responsible for gathering votes and running two protocols: the voting protocol and the vote-set consensus protocol. Both are explained and analyzed explicitly. This protocol can tolerate less than $< \frac{N_c}{3}$ corrupted IC peers and less than $< \frac{N_c}{2}$ corrupted WBB peers. The concept is that the user sends votes to only one IC member who is responsible for sending the receipt back to the user.

The main different of this scheme with [20], being that the collection of vote is completely not synchronous. It is believed that the cause is due to the complexity of the vote-set consensus protocol because for each vote, the Bracha binary protocol [41] is implemented. But in this scheme, the vote can only be validated at the end of the voting period. The author [17] suggests that a voter receives a receipt, so with a high probability, it is certain that the vote will be published to WBB members using synchronous communication model.

6. E-voting Services of Dini. Dini [12] proposed a distributed voting system service following the approach of [42]. Dini's approach is based on replication and can tolerate arbitrary failures. Dini does not focus on the Bulletin Board system, but rather on the general voting service. The scheme focus to achieve *eligibility, uniqueness, privacy, and availability*. There are some disadvantages to this approach: anonymous channels are required for senders and voters are required to run their validation protocols. On the other hand, we formalize the general voting requirement whereby it is assumed that voters have the credentials to authenticate themselves on a vote taking place with a ballot collection system, therefore, no anonymous channel requirements are required. Then Dini assumes the existence of a reliable channel in its security model.

IV. Security Issues and Analysis of Bulletin Board

The following subsections, we discuss possible issues arising related to the implementation of Bulletin Board System in general. Operational issues are also touched upon. In each case, we provide several possible suggestions for the solution; and the general objectives of the basic functionality and properties of the Bulletin Board. And also we provide a list of properties that are very critical for use of the Bulletin Board in the cryptographic voting protocol. Also discuss several operational and properties in the voting protocol can be made with the Bulletin Board.

A. *Operational Issues*

- ***Conflicting Messages:*** The designing a secure cryptography voting system, it may be necessary to prevent the involved parties from sending messages continuously, likely unequal, and opposite messages contents. This case can be solved simply that the first message must be stated differently in type and origin which is taken into consideration. In this case, the board may reject all subsequent messages from the same party. In this case, all the same, messages will be rejected by the board. The Bulletin Board will count the final messages and must memorize the order of message publication and arrival with a time stamp.
- ***Malformed Messages:*** Every message sent to Bulletin Board has a certain structure and content. If there are messages sent from parties that do not meet the terms and conditions and/or are not complete, whether intentional or unintentional, the board needs a strategy to deal with them. One simple strategy is that all messages received which do not meet the terms and conditions of the system, they are rejected and considered flawed and not published. Bulletin Board can quickly detect them.
- ***Replayed Messages:*** There is a need to anticipate and prevent copying from other people on behalf of another party. If the renewal of votes is permitted in the electoral system, it can be exploited for the cancellation of renewed votes by only sending the first vote for the second time.
- ***Early and Late Messages:*** In designing a secure cryptography voting system, of course, the administrator or election authority has specified the start time and end of the election period. Acceptable ballots that are posted during a specified period are counted at the final tally and then published. Whereas for votes or messages that arrive too early and too late are rejected and not published or counted. One of the simplest solutions to this case is to let the Bulletin Board reject all messages that do not reach within the limit of the set voting period. The message

can be published together with timestamps to avoid any discrepancy.

- ***Board Flooding:*** It is possible the parties involved may allow posting messages arbitrarily. How to resist malicious behavior committed by individuals sending messages arbitrarily to flood the Bulletin Board is a challenging problem. "Flooding" attack is possible to be used by another user who wants to disturb or make the voting time fail just by sending a large number of messages trash with useless content. The board can be flooded with messages until its capacity is covered. If the Public Bulletin Board received messages from outside the protocol the problem got worse. However, the ideal bulletin board has a very large and unlimited memory capacity.
- ***Secure Authentication:*** An administrator of the Bulletin Board has the authority to create designated electoral areas where voters can publish their messages/ballot. Each author and message posted can be authenticated by Bulletin Board and rejected if it is from an unauthorized party. Bulletin Board functionality must be compatible with the infrastructure that provides secure cryptography authentication during implementation.
- ***Undeniable Receipt:*** When the user or voter is publishing a message/vote, Bulletin Board needed protocol to respond with a confirmation. The aim is that evidence has been provided to voters that their message has been posted. Therefore, receipts must be able to be generated by an undeniable Public Bulletin Board (these receipts cannot be used to track voters). In the voting protocol, each voter then keeps a secret duplicate, their votes can be verified and counted correctly using a receipt.
- ***Consistent Views:*** Voting protocols must be able to show consistency from the verifiers to the results of election verification, all data must be taken from the public Bulletin Board. It is clear, that verifier(s) will only come to consistent conclusions if all get the same point of view from the board. Bulletin Boards can provide a consistent view by description, but a fraudulent BB can easily reply to different operations with disparate message sets. The way to anticipate malicious behavior needs to be set out on the Bulletin Board carefully.

B. *Organisational Issues*

- ***Extending the Voting Period:*** Election protocols explicitly do not include procedures for dealing with unexpected or extraordinary circumstances, such as sudden power outages, network, or server errors. To cope with these problems it may need to re-adjust the voting period. As a solution, the administrator announces to give additional time or extension to the Bulletin Board. This means that strategy provided for splitting with late messages must be adjusted and needs to be time-stamped.
- ***Multiple Voting:*** The existence of a Bulletin Board in every election sounds very impractical. Therefore, the board must design in detail to support multiple elections, for instance prepare designated zone for different elections, which are separated strictly.
- ***Simultaneous Voting:*** The Bulletin Board is an important element in the voting system to support simultaneous elections – most likely with possibly different administrators, trusted authorizations, or voters.
- ***Termination of voting process:*** The Bulletin Board must provide a mechanism to close the voting by lock the whole result of the election and by making its visible publishing to the general community.
- ***Archiving the votes:*** Preserving election result data from all previous elections may not be necessary or meaningful. Therefore the Public Bulletin Board must make it possible to delete all election data quickly the people verifies and accepts the final voting results and the winner is declared.

V. Implementation of Bulletin Board

To addresses the issues mentioned above, it is necessary to formally and flexibly define what is BB and how it works. In general, the Bulletin Board has prime purpose, namely to save a set of messages received published and each user can retrieve them. Additional properties may require some type of metadata to be added to each message, for example, $p = (m, \alpha, \beta)$ is stored as a repository for message $m \in M$ and its metadata. Moreover, to distinguish the metadata included in the post is based on its origin as it can be added either by the message writer (user) or by the board and uses different symbols $\alpha \in A$ and $\beta \in B$, respectively. α and β can be modeled as a list of features known as user features and board features respectively. For a set of index I, α_I and β_I denote the appropriate feature sub-list from A and B respectively.

The widely model [43] the goal of BB is to store a set of posting, not a set of messages. Let Q_t denote this set of posts at some time t. This set represents the internal state of the board. There are two ways to define this order over properties rather than data structures. First, it allows easy integration of various solutions (see History of BB of Content). The second solution, when taking the subset $R \subset Q$ allows a solution that provides for each $q \in R$ an absolute position in the Q. Which aims so that no message can be deleted or modified which can be expressed in the above notation by $Q_t \subseteq Q_{t'}$ for all $t' \geq t$.

*1) **Basic Operations.**:* The principle, Bulletin Board provides a public interface (for posting and fetching) and support many operations such as update and delete but this is contrary to the principle of append-only property. When Bulletin Board publishes a message $m \in M$, we can say that user will also give some user attributes $\alpha \in A$.

After Bulletin Board receives the message (m, α), it performs "checks" to validate post. If check fails then an error message $\perp$ is returned. On the other hand, if the check passes then some Board attributes $(\beta \in B)$ are generated and post $p = (m, \alpha, \beta) \in M \times A \times B$ is formed. Observe that by accepting β in response to the post (m, α), the user successfully completes the procedure of post $P : \beta \vee \perp \leftarrow \mathsf{post}(m, \alpha)$.

Users always get posts that are on P where P can grow into a large pool of posts. The user defines the query $Q \subseteq M \times A \times B$, which is applied as a filter to the P element. The result of the query is set $R = P \cap Q$. Observe that an

unconstrained query $Q = M \times A \times B$ yields the return of the full set P as above. The metadata $y \in C$ is modeled as a list $y = (y_1, \ldots, y_w)$ of the attributes $y_i \in C_i$ without specifying any further sets of C_i which can be referred to as result attributes: R,$y \leftarrow (Q)$

For better readability, it can be written for the resulting subset of posts R= $P \cap Q$, to limit only the user attribute to a single value $\alpha_i \in A_i$ or to a subset of values $A_i \subseteq A$.

*2) **Content Structuring of Board**:* The Bulletin Board based on content structure, there are at least three characteristics which make it possible to reduce communication costs [43].

- **Feature-1 (Sectioned).** The main target of sectioned BB is to share content. Messages (content) are divided into unrelated logically independent units.In order for the right section post to be active, the author must provide section $s \in S$ as user attributes. If the post in the right section $s \notin S$ contains different attributes, it is rejected. In the implementation of a voting system, it is natural to define individual parts for each voter's data. Therefore, this feature can overcome the problem of utilizing Bulletin Board for possibly simultaneous multiple elections (see Operation Issues).
- **Feature-2 (Group).** One of the functionality Bulletin Board for classifying messages or content. When posting a message or content, the writer must identify an available group $g \in G$ that acts as a user attribute for the message. If there is an invalid message $g \notin G$, then it will be rejected by the board.
- **Feature-3 (Typed).** The messages or content of group in Bulletin Board called typed, if each $g \in G$ defines $M_g \subseteq M$ a subset of itself valid messages. M_g called g. Typed board, messages incoming m of group g are received if $m \in Mg$, while all other messages $m \notin Mg$ are rejected. For example, in Figure 2 it can be shown that the message type on the keyboard is different for each group, for example, M_Group1=(0,...,9)^5, M_Group2=(A,...Z], M_Group3=(0,...,9)^8. To be addressed the Public Bulletin Board on voting to solve problems with malformed messages (see Operation Issues).

SECTION 1		
Group-1	Group-2	Group-3
123456	KHHG	01010101
665544	ADFGH	11110011
223344	HH	10101010

SECTION 2		
Group-1	Group-2	Group-3
	GGH	10101010
432211	KKHGGF	00001100
	UUHRD	11110011

SECTION 3		
Group-1	Group-2	Group-3
542322	bbggrgf	11111101
	Llkjhjhg	00000001
	hagfads	11001100

Fig. 2. Example of a structured content Bulletin Board with three types, three groups, the appropriate type, and multiple messages

*3) **Authentication and Integrity.**:* This section, two features are discussed to help ensuring the authentication and integrity of messages on the Bulletin Board.

- ***Feature-1 Access-control:*** Bulletin Board realizes the access control that serves to authenticate user and reject the message if user or voter is not authorized. The Bulletin Board can activate a checking protocol which can be realized by (public-key) signatures K, for authorized users and is known to the board at any time. There are static sets or dynamic sets. In the case of static sets, K is publicly known. It cannot be changed, whereas, in the case of dynamic sets, $K = K(P_t, \alpha, \beta)$ is implicitly defined by functions known to public K, which depend on the current board state P_t and attributes included in the postal entry $K = (m, \alpha, \beta)$. User's public key pk and signature $S = Sign(m, \alpha)$ must be entered as a user attribute in α. We use $\alpha 1$ to denote list of user attributes that are different from pk and S. BB conducts an examination whether $pk \in K$ and verify with $(pk, m, \alpha 1, S)$ to decide if p comes from authorized users or not. In voting systems, dynamic sets K are more flexible and can serve various purposes. For example, we can define a function K that allows election administration or trusted authority to post exactly one message. Therefore, K must depend on P_t (to check whether same author has previously posted messages with same characteristics) and on α (which contains the public key of the author's). This mechanism is a solution to conflicting messages and message flooding attacks. In chronological Bulletin Board, each post contains a timestamp in board attribute list, which implies that in this case, K must depend on P.
- ***Feature-2 Publishing Certified:*** The Bulletin Board offers publishing certified [19] user returned digital signature can provide evidence of board response. In the interlinked Bulletin Board, signature S_{post} is not only a receipt for publication of messages but also a commitment to current board's content. Likewise, each signature S_{get} is board's commitment to content at time t. By issuing that commitment every post received, and for each request, board guarantees its historical consistency and, therefore, integrity of data stored. In voting systems, it is a prerequisite for offering a consistent view of election data to each verifier (see Operational Issues).

We consider Bulletin Board to satisfy all properties and features described above. To post a message $m \in M_g$ to Bulletin Board, users must provide a list of user attributes $\alpha = [s, g, pk, S]$ which contain a part $s \in S$, a group element $g \in G$, user's public key $pk \in K$, and a signature $S = Sign(m, [s, g])$ using user's secret key sk. If a post is accepted, board responds with a list of board attributes $\beta = [i, t, H_i, S_{\text{post}}]$ containing sequence numbers $i \in N$, a timestamp $t \in T$, hash value $H = H_{i_p}$ and signature $S_{\text{post}} = Sign(m, \alpha, [I, t, H_i])$.

VI. Related work

This Section we focus on the recent work because almost no researchers paid attention to Bulletin Board in e-voting earlier. In Table I, we summarize some important existing e-voting schemes, which use BB as a core technology. The last column indicates if the implementation is done using Blockchain. Almost protocols cryptography voting system use a bulletin board as a central communication channel with the parties involved, to ensure that verification procedure is public.

Shahzad et al. [65], has proposed a reliable e-voting system that is compatible with block creation and block sealing (helping to make the Blockchain adaptable to meet the needs

TABLE I
COMPARISON OF BULLETIN BOARD BASED ON E-VOTING SCHEMES

E-voting System	Verifiability	Receipt Freeness	Polling Station	Bulletin Board	Used Blockchain
D.Chaum [31] [32] [33]	UniVer	Yes	Yes	Yes	No
A.Juels et al. [44]	UniVer	Yes	Yes	Yes	No
Civitas [45]	UniVer	Yes	Yes	Yes	No
Helios [46]	UniVer-WIVer	No	Yes	Yes	No
Helios.2 [47]	UniVer-WIVer	No	Yes	Yes	No
Bo Meng [48]	UniVer	Yes	Yes	Yes	No
AFT [49]	UniVer	Yes	Yes	Yes	No
Selection [51]	UniVer-WIVer	Yes	Yes	Yes	No
Caveat Coercitor [55]	UniVer-WIVer	Yes	Yes	Yes	No
PGD [56]	UniVer-WIVer	No	Yes	Yes	No
Philip et al. [57]	UniVer	Yes	Yes	Yes	No
ZeroCoin [58]	UniVer	Yes	Yes	Yes	Yes
BitCongress [70]	UniVer	Yes	Yes	Yes	Yes
Vote Watcher [59]	UniVer	Yes	Yes	Yes	Yes
Votebook [60]	UniVer	Yes	Yes	Yes	Yes
Open Vote Network [69]	UniVer	Yes	Yes	Yes	Yes
TIVI [69]	UniVer	Yes	Yes	Yes	Yes
Follow My Vote [71]	UniVer	Yes	Yes	Yes	Yes
Verify-Your-Vote [62]	UniVer	Yes	Yes	Yes	Yes
Proof of Vote [64]	UniVer	Yes	Yes	Yes	Yes
Agora [63]	UniVer	Yes	Yes	Yes	Yes

UniVer = Universal Verifiability | WIVer= Weak Individual Verifiability | Yes= Used core technology | No= Not used core technology

of the polling process) by changing the hash function on the Blockchain to achieve credibility and fairness. Lai et al. [66] presented Blockchain based e-voting schemes with fairness where privacy protection for voters is achieved by using ring signatures. Wu [67] proposed a Blockchain based e-voting system and used ring signature to achieve transparency and privacy. Then [68] suggested that an anonymous e-voting scheme with efficient decentralization could be realized with Ethernet and Ring Signature to ensure transparency and privacy. Furthermore, McCorry et al. [69] proposed a blockchain based e-voting scheme with smart contracts for the selection of board members. Also, the commercial E-voting schemes for instance, Netvote [4], Follow My Vote [71], TIVI [69], ZeroCoin [58], Vote Watcher [59], Votebook [60], AGORA [63] and BitCongress [70], E-Vote-ID 2020 [73], FC20.ifca-2020 [72]. One important issue is coercion resistance (impossible to achieve CR with BB) – Teague [74] has BB some particular type of Coercion resistance, but it does not require complex voter verification.(whether the voter was present or they prefer, that they have not attended and uses BB). The authors [75] Verifiable E-voting with Resistance against Physical Force Abstention Attack for Blockchain schemes using polling booth and suggested a solution using Bockchain.

CONCLUSION

This article we survey evolution of public bulletin board before and after the introduction of Blockchain technology, particularly in the context of e-voting. Although bulletin board has other applications, we focus on its applicability which ensures several security properties of an e-voting scheme.

REFERENCES

[1] OO Okediran, EO Omidiora. A Comparative Study Of Generic Cryptographic Models For Secure Electronic Voting. In British Journal of Science, ISSN 2047-3745, Vol. 1 (2), 2011.

[2] Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic, Jordan Mohler, "BroncoVote: Secure Voting System using Ethereum's Blockchain" , ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy, 2018.

[3] Szabo, N.: Smart Contracts (1994)

[4] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014

[5] Brooks GW. Bulletin board and the like [Internet]. US1494583A (1923). $https://patents.google.com/patent/US1494583A/en$

[6] Gilbertson S. Feb. 16, 1978: Bulletin Board Goes Electronic. In: WIRED [Internet]. 16 Feb 2010 [cited 2 May 2018]. $https://www.wired.com/2010/02/0216cbbs-first-bbs-bulletin-board/$

[7] Cohen, J. D., and Fischer, M. J. (1985). A robust and verifiable cryptographically secure election scheme (Extended Abstract). In FOCS (pp. 372-382).

[8] Heather, J., Lundin, D.: The Append-Only Web Bulletin Board. In: FAST 2008, pp. 242-256.

[9] Cramer, R., Gennaro, R., Schoenmakers, B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. EUROCRYPT 1997, 103-118 (1997).

[10] Benaloh, J. : Verifiable secret-ballot Elections. PhD thesis, Yale University (1987)

[11] Reiter, M.K.: The Rampart Toolkit for Building High-integrity Services. In: TPDS 1995, pp. 99–110.

[12] Dini, G.: A secure and available electronic voting service for a large-scale distributed system. Future Generation Computer Systems 19(1) (2003) pp. 69–85.

[13] Peters, R. A. 2005. "A Secure Bulletin Board." Master's thesis, Department of Mathematics; Computing Science, Technische Universiteit Eindhoven, The Netherlands.

[14] Krummenacher, R.: Implementation of a Web Bulletin Board for E-Voting Applications. MSE Seminar on E-Voting. Institute for Internet Technologies and Applications (2010).

[15] Culnane, C., Ryan, P.Y.A., Schneider, S.A., Teague, V.: vVote: A verifiable voting system. ACM Trans. Inf. Syst. Secur. 18(1), pp. $3:1-3:30$ (2015).

[16] Burton, C., Culnane, C., Schneider, S., vVote: Verifiable Electronic Voting in Practice. IEEE Security & Privacy 14(4), pp. 64-73 (2016).

[17] Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., Delis, A., Kiayias, A., Roussopoulos, M.: D-DEMOS: A Distributed, End-to-End Verifiable, Internet Voting System. In: ICDCS 2016, pp. 711-720.

[18] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. End-to-End Verifiable Elections in the Standard Model, pages 468–498. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[19] Heather, J., and D. Lundin. 2008. "The Append-Only Web Bulletin Board." In FAST'08, 5th International Workshop on Formal Aspects in Security and Trust, edited by P. Degano, J. Guttman, and F. Martinelli, 242–256. LNCS 5491. Malaga, Spain.

[20] Chris Culnane and Steve A. Schneider. A Peered Bulletin Board for Robust Use in Verifiable Voting Systems. In CSF 2014, pages 169–183, Vienna, Austria, July 19–22, 2014. IEEE Computer Society.

[21] R. Anane, R. Freeland, and G. Theodoropoulos, E-voting requirements and implementation," IEEE International Conference on E-Commerce Technology and IEEE International Conference on Enter-prise Computing, E-Commerce and E-Services, pp. 382-392, 2007.

[22] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli, "Seas, a secure e-voting protocol: design and implementation", Computers & Security, vol. 24(8), pp. 642-652, 2005.

[23] L. F. Cranor and R. K. Cytron, Sensus: A security-conscious electronic polling system for the internet," The Hawaii International Conference on System Sciences, vol. 3, pp. 561570, 1997.

[24] R. Joaquim, A. Zuquete, and P. Ferreira, REVS a robust electronic voting system," IADIS International Journal of WWW/Internet, vol. 1(2), pp. 47-63, 2003.

[25] Jain, A.K., Feng, J., Nandakumar, K., "Fingerprint matching", Computer 2010 (43), 36-44 (2010).

[26] Yang, W.; Wang, S.; Zheng, G.; Chaudhry, J.; Valli, C. ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures. J. Supercomput. 2018, 74, 4893–4909.

[27] Doroz, R., Wrobel, K., Porwik, P., "An accurate fingerprint reference point determination method based on curvature estimation of separated ridges", Int. J. Appl. Math. Comput. Sci. 2018 (28), 209–225 (2018).

[28] Adida, B.: Advances in Cryptographic Voting Systems (2006) $http://groups.csail.mit.edu/cis/theses/adida-phd.pdf$.

[29] Michael K. Reiter. Secure Agreement Protocols: Reliable and Atomic Group Multicast in Rampart. In Proceedings of the 2Nd ACM Conference on Computer and Communications Security, CCS '94, pages 68–80, New York, NY, USA, 1994. ACM.

[30] Michael K. Reiter. A Secure Group Membership Protocol. IEEE Trans. Softw. Eng., 22(1):31–42, January 1996.

[31] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commun. ACM 24(2): 84-88 (1981)

[32] David Chaum: Blind Signatures for Untraceable Payments. CRYPTO 1982: 199-203

[33] David Chaum, Amos Fiat, Moni Naor: Untraceable Electronic Cash. CRYPTO 1988: 319-327

[34] David Chaum, Peter Y. A. Ryan, Steve A. Schneider: A Practical Voter-Verifiable Election Scheme. ESORICS 2005: 118-139

[35] Alexandra Boldyreva. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In Yvo Desmedt, editor, PKC 2003, volume 2567 of LNCS, pages 31–46, Miami, Florida, USA, January 6–8, 2003. Springer, Heidelberg.

[36] Victor Shoup. Practical Threshold Signatures. In Bart Preneel, editor, EUROCRYPT 2000, volume 1807 of LNCS, pages 207–220, Bruges, Belgium, May 14–18, 2000. Springer, Heidelberg.

[37] Jose Beuchat. Realization of a Secure Distributed Bulletin Board, Master's Thesis. Bern University of Applied Sciences, 2012.

[38] Josh Benaloh, Mike Byrne, Philip T. Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, and Dan S. Wallach. STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. CoRR, abs/1211.1904, 2012.

[39] Susan Bell, Josh Benaloh, Michael D. Byrne, Dana Debeauvoir, Bryce Eakin, Philip Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, Dan S. Wallach, Gail Fisher, Julian Montoya, Michelle Parker, and Michael Winn. STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. In 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13), Washington, D.C., 2013. USENIX Association.

[40] Daniel Sandler, Kyle Derr, and Dan S. Wallach. VoteBox: A TamperEvident, Verifiable Electronic Voting System. In Paul C. van Oorschot, editor, USENIX Security Symposium, pages 349–364. USENIX Association, 2008.

[41] Gabriel Bracha. Asynchronous Byzantine Agreement Protocols. Inf. Comput., 75(2):130–143, November 1987.

[42] Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: AUSCRYPT 1992, pp. 244–251.

[43] Hauser, S. and R. Haenni "A generic interface for the public bulletin board used in UniVote" In CeDEM'16, 6th International Conference for E-Democracy and Open Government, edited by P. Parycek, N. Edelmann 49-56. Krems, Austria

[44] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES '05, pages 61–70, New York, NY, USA, 2005. ACM.

[45] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a secure voting system. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, SP '08, pages 354–368, Washington, DC, USA, 2008. IEEE Computer Society

[46] Ben Adida, "Helios: Web-based open-audit voting", In USENIX Security Symposium, volume 17, 335-348, 2008.

[47] Ben Adida, Olivier De Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a university president using openaudit voting: analysis of real-world use of helios. In Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections, pages 10–10. USENIX Association, 2009.

[48] Bo Meng, Zimao Li, and Jun Qin. A receiptfree coercion-resistant remote internet voting protocol without physical assumptions through deniable encryption and trapdoor commitment scheme. Journal of Software, 5(9), 2010.

[49] Roberto Araujo, Sebastien Foulle and Jacques Traore, "A practical and secure coercion-resistant scheme for internet voting", In Towards Trustworthy Elections, pages 330-342. Springer, 2010.

[50] Warren D Smith. New cryptographic election protocol with best-known theoretical properties. In Proc. of Workshop on Frontiers in Electronic Elections, 2005.

[51] Jeremy Clark and Urs Hengartner. Selections: Internet voting with over-the-shoulder coercion-resistance. In George Danezis, editor, Financial Cryptography and Data Security, volume 7035 of Lecture Notes in Computer Science, pages 47–61. Springer Berlin Heidelberg, 2012.

[52] Gavin Lowe. An attack on the needhamschroeder public-key authentication protocol. Information processing letters, 56(3):131–133, 1995.

[53] Emmanuel Bresson, Dario Catalano, and David Pointcheval. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In Chi-Sung Laih, editor, Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 37–54. Springer Berlin Heidelberg, 2003.

[54] Jeremy Clark and Urs Hengartner. Panic passwords: Authenticating under duress. HotSec, 8:8, 2008

[55] G.S. Grewal, M.D. Ryan, S. Bursuc, and P.Y.A. Ryan. Caveat coercitor: Coercion-evidence in electronic voting. In Security and Privacy (SP), 2013 IEEE Symposium on, pages 367– 381, May 2013.

[56] Peter YA Ryan and Vanessa Teague, "Pretty good democracy", In Security Protocols XVII, 111-130. Springer, 2013.

[57] A. A. Philip, S. A. Simon and A. Oluremi, "A receipt-free multi authority e-voting system", International Journal of Computer Applications, 30(6): 15-23, 2011.

[58] Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributede-cash from bitcoin. In: IEEE Symposium on Security and Privacy (2013)

[59] VoteWatcher - The World's Most Transparent Voting Machine." Vote Watcher. Accessed December 14, 28, 2016. http://votewatcher.com/.

[60] Kirby, Kevin, Anthony Masi, and Fernando Maymi. Votebook: A Proposal for a Blockchain-based 16Electronic Voting System. The Economist. Accessed December 14, 2016. http://www.economist.com/sites/default/files/nyu.pdf

[61] McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security, Springer (2017)

[62] Marwa Chaieb, Souheib Yousfi, Pascal Lafourcade and Riadh Robbana, "Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol", EMCIS 2018: 16-30 (2018).

[63] Gailly, N., Jovanovic, P., Ford, B., Lukasiewicz, J., Gammar, L.: Agora: Bringing our voting systems into the 21st century. https://agora.vote/Agora Whitepaper v0.1.pdf (2018) [Accessed 27-Mar-2018].

[64] "Proof of Vote White Paper". In: (2018).

[65] B. Shahzad, J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," IEEE ACCESS., 2019, 7: 24477-24488.

[66] W.J. Laietal., "DATE: A Decentralized, Anonymous, and Transparent Evoting System,"in 1st IEEE International Conference on Hot Information Centric Networking., (HotICN). IEEE, 2018: 24-29.

[67] Y.Wu,"An-voting system based on blockchain and ring signature,"M.S. thesis, Dept. Computer Science., University of Birmingham., 2017.

[68] L. Wei-Jr, W. Ja-Ling, "An efficient and effective Decentralized Anonymous Voting System," arXiv preprint., arXiv:1804.06674, 2018

[69] McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security, Springer (2017)

[70] BitCongress. Control the world from your phone. [Online]. Available: $http://www.bitcongress.org/BitCongressWhitepaper.pdf$

[71] Follow my vote: Followmyvote. $https://followmyvote.com/(2012)[Accessed15-Dec2017]$.

[72] FC20.ifca-2020, Colin Boyd, Thomas Haines, and Peter Roenne. '' Vote Selling Resistance Voting '', Shangri-La Tanjung Aru R, sort Spa Kota Kinabalu, Sabah, Malaysia, February 14, 2020

[73] E-Vote-ID 2020, Ehsan Estaji, Thomas Haines, Kristian Gjosteen, Peter Roenne, P. Y. A. Ryan and Najmeh Soroush,5th Joint International Conference on Electronic Voting , Revisiting Practical and Usable Coercion-Resistant Remote E-Voting.

[74] Nicholas Akinyokun and Vanessa Teague. 2019. Receipt-Free, Universally and Individually Verifiable Poll Attendance. InProceedings ofthe Australasian Computer Science Week Multiconference (ACSW '19),January 29–31, 2019, Sydney, NSW, Australia.ACM, New York, NY,USA, 10 pages. https://doi.org/10.1145/3290688.3290696.

[75] Misni Harjo Suwito and Sabyasachi Dutta, Verifiable E-voting with Resistance against Physical Force Abstention Attack, International Workshop on Big Data and Information Security (IWBIS). October 2019. DOI: 10.1109/IWBIS.2019.8935763