UNIVERSITY OF TARTU
Institute of Computer Science
Computer Science Curriculum

Marianne Dengo

Blockchain Voting: A Systematic Literature Review

Bachelor's Thesis (9 ECTS)

Supervisor: Fredrik P. Milani, PhD

Tartu 2020

Blockchain Voting: A Systematic Literature Review

Abstract:

The aim of the thesis is to study blockchain-based voting and its methods. In doing so, it is determined how blockchain-based voting works, which types of voting blockchain technology can be used for, and what are the advantages and disadvantages of doing so. A systematic literature review is carried out to study and compare different solutions. The purpose of the systematic literature review is to identify relevant research papers and use them to find and analyze different voting methods that utilize the blockchain. As a result, a framework is compiled summarizing the advantages, disadvantages, components, and possible areas of use of different solutions.

Keywords:

Blockchain, electronic voting, e-voting

CERCS: T120 Systems engineering, computer technology

Hääletamine Plokiahelal: Süstemaatiline Kirjanduse Ülevaade

Lühikokkuvõte:

Lõputöö eesmärk on uurida plokiahelapõhist hääletamist ja selle meetodeid. Selle käigus tehakse kindlaks, kuidas toimib plokiahelapõhine hääletamine, millist tüüpi hääletuste puhul on plokiahela tehnoloogiat võimalik kasutada, ning mis on selle eelised ja puudused. Plokiahelapõhise hääletamise lahenduste uurimiseks ja võrdlemiseks viiakse läbi süstemaatiline kirjanduse ülevaade (ingl *systematic literature review*). Selle eesmärk on teemakohaste teadustööde identifitseerimine ning nende kasutamine plokiahelal põhinevate hääletusmeetodite tuvastamiseks ja analüüsimiseks. Töö kokkuvõttena valmib tabel erinevate lahenduste eelistest, puudustest, komponentidest ja võimalikest kasutusvaldkondadest.

Võtmesõnad:

Plokiahel, elektrooniline hääletamine, e-hääletamine

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

Contents

1. Introduction

Voting has always been an important part of expressing one's views in a democratic society. From counting raised hands and filling out paper ballots to casting votes electronically, mankind is actively finding ways to improve on a process that was once laborious, unreliable, and prone to errors. Implementing an electronic system for different types of voting events, such as elections and general meetings, is perhaps the most clear-cut way to eradicate or lessen the burden of counting votes manually and making mistakes in the process. The first country to adopt an electronic system for national elections was Estonia [1]. Switzerland and Norway were soon to follow, implementing electronic systems for state-wide [2] and council elections [3], respectively.

These electronic voting systems have come under close scrutiny by researchers and security experts. One of the primary critiques is the secrecy of crucial parts of the source code. For example, the transparency of the Estonian voting system is questionable as the script for posting votes has never been made public [4]. Leaked source code of the now discontinued Swiss voting system was, however, analyzed by international researchers, who found that it would have been entirely possible for someone to replace all the valid ballots with fraudulent ones through a cryptographic backdoor [5]. Another critical security risk of these implementations is their centralization. This means that they are controlled by a single main entity and have several security flaws, such as vulnerability to distributed denial-of-service (DDoS) attacks. A DDoS attack entails making the system inaccessible to the end user by overloading it with requests [6]. Moreover, given enough computing power, it might be possible to launch a state-level attack to analyze and alter the voting data in all of the aforementioned electronic voting systems.

As a possible solution to the drawbacks of traditional electronic voting, a system based on the blockchain technology has been proposed [7]. Blockchain is a distributed ledger managed by a peer-to-peer consensus network, which allows its stored data to be transparent, verifiable, and tamper-resistant by nature. The aforementioned benefits and a lack of central authority make it a potentially ideal platform for digital voting. [8]

Due to the growing popularity of blockchain technology, there are already multiple proposed methods and existing commercial solutions that promise secure voting on the blockchain. For example, among the organisations offering blockchain-based services are Kaspersky Lab with their election-oriented solution Polys [9], and Nasdaq [10], whose main focus is voting in general meetings. However, as of writing this paper, there is no overview of the different processes for electronic voting on the blockchain. In light of that, this paper aims to address the main research question of how blockchain technology can be used to enable electronic voting. In order to do so, a systematic literature review is carried out to study different solutions and to find out which types of voting blockchain technology can be used for, as well as the advantages and disadvantages of doing so. As a result of the literature review, a framework is created comparing the different solutions. The resulting overview of blockchain-based voting methods could be beneficial to analysts intending to design, develop and implement secure voting systems.

The rest of the paper is structured as follows. Chapter 2 provides a background for blockchain technology and other important terms related to the paper. The methodology of carrying out the literature review is detailed in chapter 3. Results of the review are described in chapter 4. Chapter 5 contains the discussion of results and a framework comparing different blockchain-based voting methods. Finally, the work is concluded and summarized in chapter 6.

2. Background

In order to fully understand the process of some of the voting solutions described in the following chapters, it is necessary to be familiar with some terms and methods related to blockchain voting. Smart contracts, SHA-256, and ring signatures are important components of specific blockchain-based voting methods described later. As such, a brief background and definitions of blockchain technology and the aforementioned terms are provided in the following segment.

2.1 Blockchain

The blockchain was invented by Satoshi Nakamoto in 2008 as a public ledger for a cryptocurrency called Bitcoin. It is an ever-growing distributed ledger that consists of records that are linked using cryptography. These records are called blocks. Each block contains a timestamp, a cryptographic hash of the previous block, and data of the transaction. [11] The basic structure of a blockchain is illustrated in figure 1.

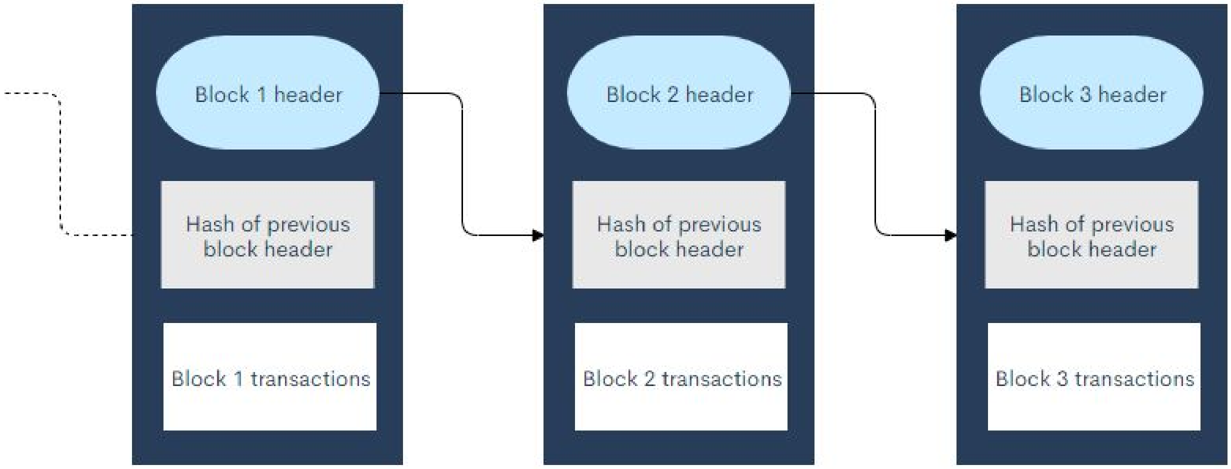


Figure 1. Blockchain structure.

As a characteristic of the blockchain, it is managed by multiple nodes in a peer-to-peer network, each of which verify the validity of a transaction before adding it to the blockchain. This kind of decentralization ensures that individuals cannot modify or add invalid blocks to the blockchain without reaching a majority consensus on the network. As such, a blockchain can be considered secure by design. [12]

Currently, there are three main types of blockchain: public blockchain, private blockchain, and consortium blockchain. These blockchain types are characterized as follows: [13]

Public blockchain has no access restrictions. This means that anyone can read it, write to it by performing transactions, and even become a validator as one of the nodes. This type of blockchain is also called a *permissionless blockchain*.

Private blockchain has restrictions as to who can read and write to the chain, as well as validate it. It is generally controlled by an organization that aims to limit the access to the blockchain internally. This type of blockchain can also be called a *permissioned blockchain.*

Consortium blockchain is another type of permissioned blockchain. However, instead of being restricted to use by a single organization, the ownership can be divided among several of them.

The blockchain networks used in some of the voting processes in this paper include Bitcoin, Ethereum, and Zcash.

2.2 Smart Contract

Due to its decentralization and each node operating on a consensus algorithm, the blockchain is considered an immutable, secure data structure. Ethereum makes use of this property by expanding its blockchain with smart contracts [14].

Smart contract is a blockchain-based application that processes incoming information. Essentially, it is a script deployed on the blockchain that executes automatically as its functions are called. As such, it cannot be illegally removed or manipulated once written. This means that it can work transparently and autonomously without any external assistance. Many applications that would normally require a web server to function can be run through a smart contract instead. [15]

2.3 SHA-256

SHA-256 is a secure hash algorithm that was designed by the National Security Agency (NSA) in 2001 and used to secure communications on the federal level. It takes the input of plaintext in any size and encrypts it to a fixed-size 256-bit binary value. It is strictly a one-way function and cannot be decrypted without guessing the input data and running it through the SHA-256 algorithm to see if the hashed value is a match. Figure 2 illustrates the basic function of the SHA-256 algorithm. [16]

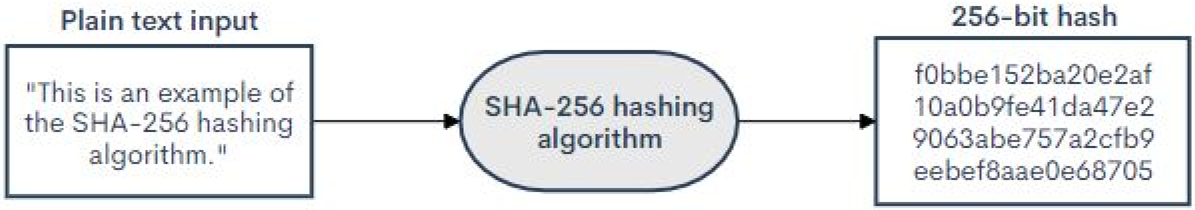


Figure 2. Basic function of SHA-256.

2.4 Ring Signature

Ring signature is a type of digital cryptographic signature that is created by a member of a group in which each person has their own key. It is designed in a way that it would be computationally impractical to find out which of the group members' keys was used to create it. Ring signatures were originally proposed by Rivest et al. [17] in 2001 as a way to leak a secret. As per their example, they could be used by a high-ranking government official to provide an anonymous signature, without revealing which of the government officials signed the message. As the identity of an individual cannot be deduced from a ring signature alone, the anonymity it provides is a useful property for many appliances, including digital voting. [18] Basic function of the ring signature can be seen in figure 3.

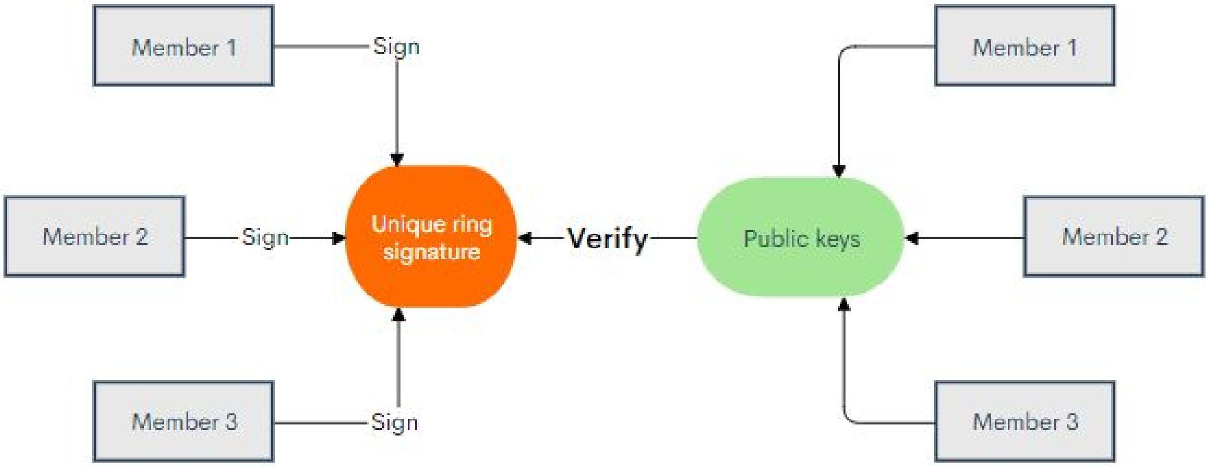


Figure 3. Ring signature function.

In a ring signature, there is a defined group of individuals, each of which have their own public/private key pairs of *(P_1, S_1), (P_2, S_2), …, (P_n, S_n)*. For a user *i* to sign a message *m*, they must use their own secret key S_i and the public keys of the other group members *$(m, S_i, P_1 \ldots P_n)$*. It is then possible to check the validity of the signature by knowing the public keys of the group, but not possible to determine exactly which member signed the message if the private keys of the group are not known. [19]

3. Systematic Literature Review

In order to find out how blockchain technology can be used to vote, a systematic literature review (SLR) is carried out. Its purpose is to identify relevant research papers and use them to find and compare different solutions for blockchain-based voting.

3.1 Planning the Review

The SLR follows the guidelines proposed by Kitchenham & Charters [20], who have defined three main phases in which to carry out the review: planning, conducting, and reporting. Describing the motivation for the review, defining research questions, and developing the review protocol are all parts of the first phase. The second phase includes identifying relevant papers, making a primary selection of studies, assessing their quality, as well as extracting and synthesizing the necessary data. The third phase consists of reporting the findings in a formatted and evaluated manner. This section details the first phase of the SLR.

3.1.1 Motivation for Review

The main objective of the SLR is to provide a systematic and scientific assessment of how blockchain technology can be used to vote. This can be done by identifying studies that describe voting on the principle of blockchain and using them to answer the research questions by identifying, analyzing and comparing relevant solutions.

3.1.2. Research Questions

The purpose for carrying out the review is to answer the main research objective:
How can blockchain technology be used to enable electronic voting?

In order to identify primary studies where blockchain voting has been applied, the above research objective is decomposed into a set of research questions (RQ):

RQ1: What are the components of a blockchain-based voting solution?

RQ2: What kinds of voting can blockchain technology be used for?

RQ3: What does blockchain-based voting look like?

RQ4: What are the advantages of blockchain voting over traditional voting?

RQ5: What are the limitations of blockchain voting?

3.2. Search Procedure

In order to find relevant scientific studies, it is necessary to devise a search strategy. To make sure no important papers are missed, it is recommended by several scientific guides [21-23] to use a strategy consisting of a primary screening and secondary screening. For the primary search, several electronic databases are scoured using search strings. A secondary search is then conducted by backward and forward tracing the citations of the papers found in the primary screening. List of papers found by scouring the databases are filtered for relevance by using selection criteria.

The first step of screening is to carry out a comprehensive search to identify an initial set of relevant studies. To do so in accordance with the guidelines proposed by Kitchenham & Charters [20], it is necessary to produce a search string pertaining to the subject matter and apply it to the chosen electronic sources.

3.2.1. Primary Search

The terms *blockchain* and *voting* are the main keywords derived from the scope of the study. Based on these search terms, the following search string can be formulated: “blockchain” AND “voting”. The following electronic databases are selected based on the coverage of scientific papers in the field of computer science: Scopus, Web of Science, and Google Scholar. The previously formulated search string *“blockchain” AND “voting”* is then applied to the sources while all the duplicate results are filtered out.

3.2.2. Selection Criteria

Not all the papers found by using the search string may be relevant to the literature review. The purpose of selection criteria is to identify applicable studies that provide sufficient information to address the research questions. It is necessary to develop criteria for both including and excluding specific research papers.

Following is a list of criteria developed in relation to the research questions. When looking through the research papers found during the search, a specific study is selected if a positive answer can be given to all the questions of the inclusion criteria. However, a study will be excluded if it's possible to provide a positive answer to at least one of the exclusion criteria.

Inclusion criteria (IC):
IC1: Is the paper within the domain of blockchain and voting?
IC2: Does the paper propose a voting solution based on blockchain?
IC3: Is the full text digitally accessible?
IC4: Is the paper written in English?

Exclusion criteria (EC):
EC1: Is the paper less than 5 pages long?
EC2: Is the paper a duplicate?

To be able to answer the previously defined research questions, it is crucial that the papers cover the topics of both blockchain technology and voting. The first inclusion criterion is derived from the aforementioned statement. However, a paper cannot be used to study and compare different voting solutions if it fails to present at least a conceptual blockchain-based method for voting. Thus, the second inclusion criterion is specified. The next two inclusion criteria are developed to assure the paper is both digitally accessible and comprehensible to the researcher. If the full paper is inaccessible or not written in English, studying it is not possible. For papers to be considered accessible, they must be freely available online or through the digital sources provided by the researcher’s university. The first exclusion criterion sorts out papers that are less than 5 pages long as they do not contain enough information for sufficient research. All duplicates of previously found studies are excluded with the final exclusion criterion.

3.2.3. Secondary Search

Following the primary search and selection process using the inclusion and exclusion criteria, a secondary search is performed. This is done by using techniques for backward and forward tracing on the confirmed list of relevant papers. During backward tracing, potential new studies are identified by going through the list of references in the existing relevant papers. In case of forward tracing, Google Scholar is used to find studies that have previously cited any of the existing papers. The inclusion and exclusion criteria defined earlier are once again used to filter the papers for relevance and quality. As per the recommendation of Webster & Watson [24], the search is concluded when no new relevant papers are discovered.

Figure 4 describes the process of including or excluding studies from the final body in detail. The number of papers marked in bold above a particular step signifies the total amount of remaining studies before the action below it is taken. The numbers on the lines represent numeric change in the amount of relevant studies as a result of the previous action. Following every step of the described search procedure resulted in 29 total papers relevant to the literature review (see **Appendix A** for the list of papers).

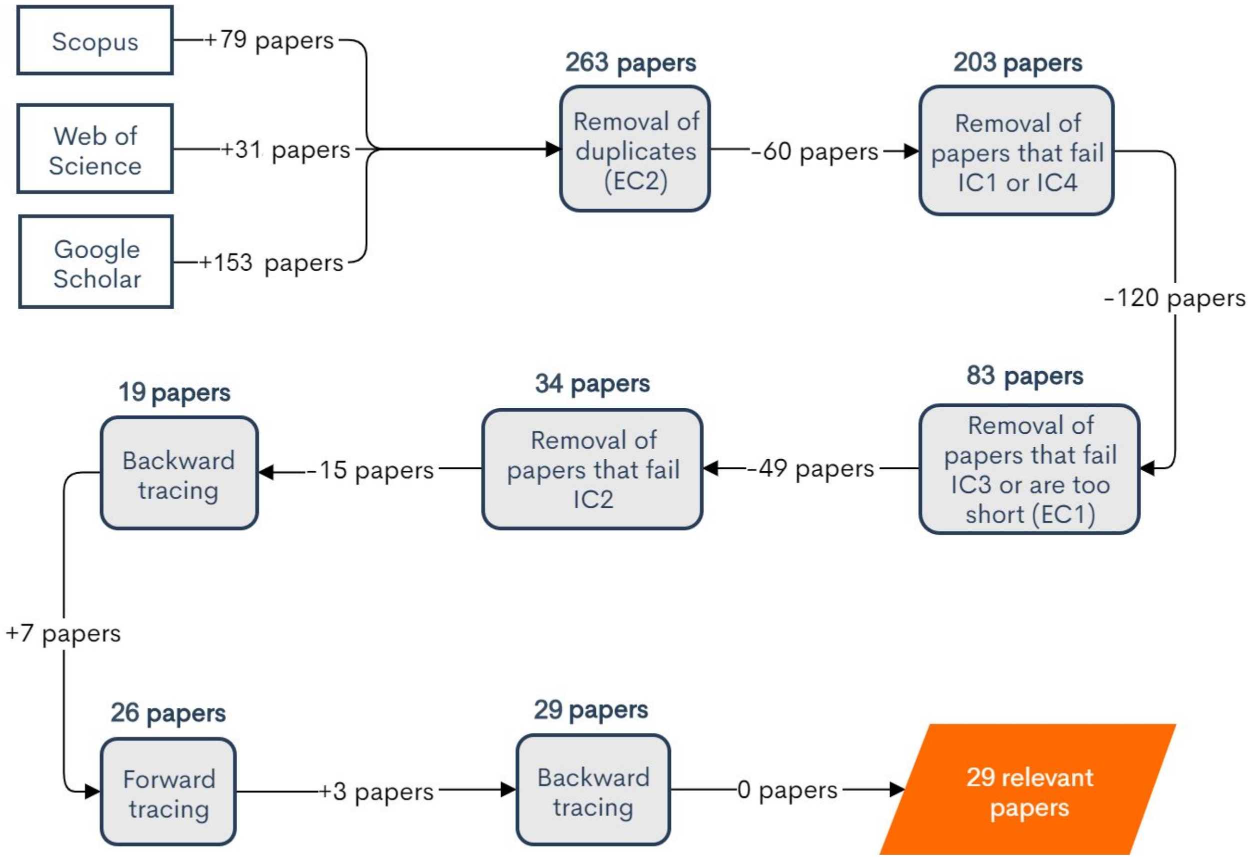


Figure 4. Process of selecting relevant studies.

3.3. Data Extraction Procedure

In order to carry out the review, data must be extracted from the relevant papers. To make sure it is done in an unbiased manner, it is recommended [25] to develop an extraction form to base the procedure on. As seen in table 1, two types of data are extracted for each study: Firstly the metadata of the paper, and then the data related to the context of blockchain voting and the research questions proposed earlier. Data is then extracted based on the developed form.

Metadata of the Paper	**Description**
Identifier	Unique identification number
Title	Title of the paper
Authors	Authors of the paper
Year	Year of publication
Type	Type of publication
Citations	Number of citations
Data about the Context of the Study	
Implementation	Status of implementation (concept, proof of work, commercial solution)
Voting Type	Type of voting the proposed solution can be used for
Blockchain Type	Type of blockchain used in the voting solution (public, consortium, private)
Components	Components of the proposed voting solution
Advantages	Advantages of the proposed voting solution over traditional voting
Limitations	Limitations of the proposed voting solution
Process	Process of the proposed voting solution

Table 1. Form developed for data extraction.

3.4. Statistics

Of the 29 papers relevant to the literature review, the number of papers published each year is shown in figure 5. From a single study in 2015 to seven studies related to voting on the blockchain published in 2017 and 2018 each, it is evident that the idea of applying blockchain technology to digital voting has gained significant traction in a relatively short amount of time.

Furthermore, 12 additional relevant papers published in 2019 display how the topic of blockchain voting continues to grow in popularity to this day.

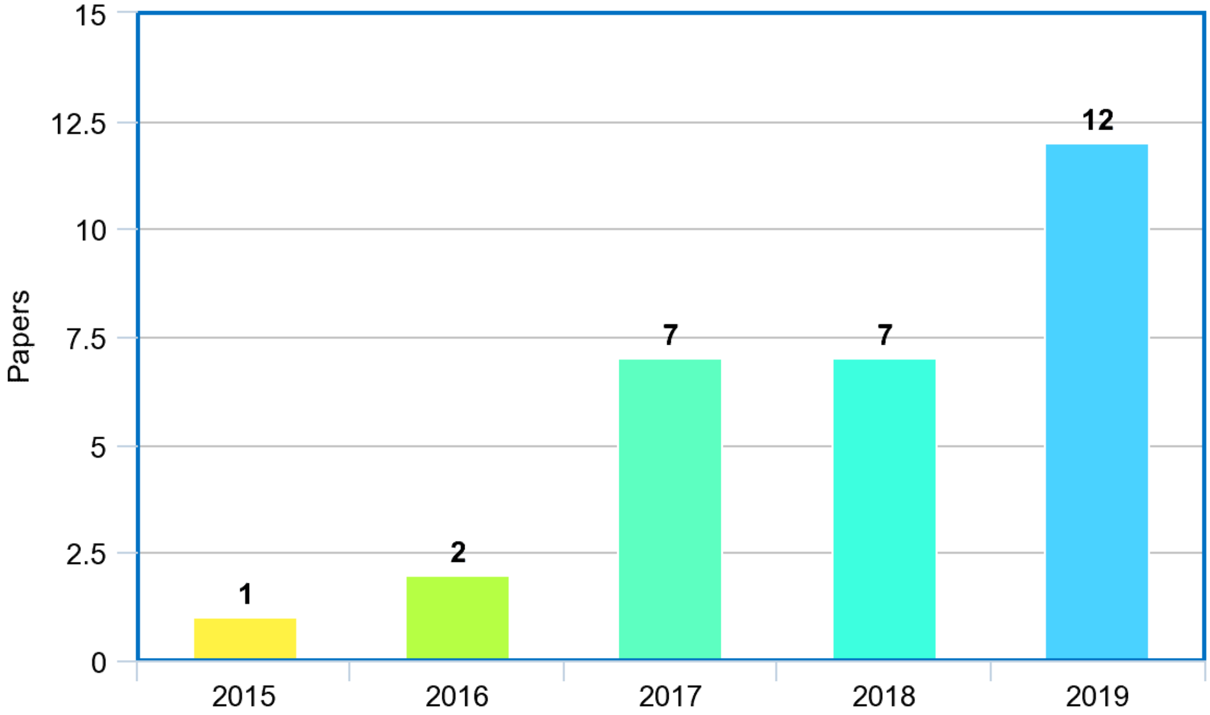


Figure 5. Number of relevant papers by year.

4. Results of the Review

Data extracted from the relevant papers found during the search procedure can be used to answer the main research objective of the review: “How can blockchain technology be used to enable electronic voting?” This is done by answering the further research questions proposed during the planning stage:

RQ1: What are the components of a blockchain-based voting solution?
RQ2: What kinds of voting can blockchain technology be used for?
RQ3: What does blockchain-based voting look like?
RQ4: What are the advantages of blockchain voting over traditional voting?
RQ5: What are the limitations of blockchain voting?

As such, this section aims to provide an overview of the components, possible voting types, process, advantages, and limitations of a blockchain-based voting solution.

4.1. Components of Blockchain-Based Voting Solutions

According to the taxonomy of electronic voting schemes by Sampigethaya & Poovendran [26], digital voting has 4 main phases: preparation phase, registration phase, voting phase, and tallying phase. This is illustrated in figure 6. While the components of blockchain-based voting can vary with the specific method, they often share some common characteristics and can be categorized into these four phases. Following is a discussion of the components typically used in each stage of blockchain voting.

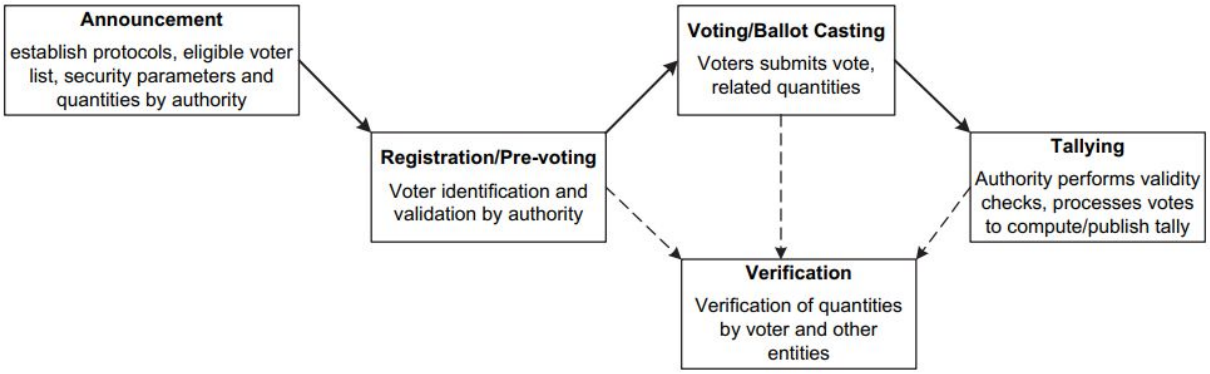

Announcement
establish protocols, eligible voter list, security parameters and quantities by authority
Registration/Pre-voting
Voter identification and validation by authority
Voting/Ballot Casting
Voters submits vote, related quantities
Tallying
Authority performs validity checks, processes votes to compute/publish tally
Verification
Verification of quantities by voter and other entities

Figure 6. Stages of an electronic voting scheme. [26]

1. Preparation phase: A decision is made regarding the type of **blockchain** to be used. This can either be a private blockchain set up for the election or a public blockchain, in which case an existing network, such as Bitcoin or Ethereum is typically used. Whether or not **smart contracts** are used depends largely on this decision [27]. In case of a private blockchain, **polling stations** can be used as nodes [28, 29]. Additionally, some methods include creating a **user interface** for ease of access to the end user [28]. Another component required in this stage would be an **administrator** who sets up and initializes the voting process [27, 30].
2. Registration phase: A **registration authority** allows users to register to vote and/or verify their identity. This phase often includes generating a public/private key pair for the user by utilizing a **cryptographic algorithm**, such as RSA (Rivest-Shamir-Adleman). [31, 32]
3. Voting phase: Different **cryptographic algorithms** can also be used to anonymize the votes. For example, this can be done using the previously discussed SHA-256 or ring signatures. [31]
4. Tallying phase: The components used in this phase are generally set up in the previous stages. As an example, tallying can be done by using **smart contracts**. [27]

4.2. Types of Voting on the Blockchain

Majority of the reviewed papers propose solutions for elections between several candidates. For example, Ayed [28] has designed a blockchain-based voting method with official elections in mind. As mentioned, incorporating blockchain technology to vote is not only possible for elections, but also for broader use cases, such as polls or boardroom meetings. One such solution is provided by Nasdaq [10]. Koç et al. [27] have also designed a voting system for small-scale polls and elections within the university, such as department chairs, student council elections or choosing a rector. To summarize, blockchain technology can be implemented in voting solutions for elections and polls of different varieties. These can further be classified by the scale of the voting system to small-scale and large-scale use cases.

4.3. Process of Blockchain-Based Voting

While the specific process of blockchain-based voting is dependent on the solution, it largely follows the same phases as outlined for digital voting in figure 6. However, not all of the phases take place within the blockchain as registration generally requires an external system. Among the proposed solutions found for voting on the blockchain, there are four that provide a unique method of doing so. Remaining papers follow largely the same process with slight to moderate modifications. As such, this section focuses on four distinct methods: voting using smart contracts [27], using Zcash [33], using cryptographic signatures [31], and finally, a method for voting with a custom blockchain system [28], which contains a solution with a different blockchain for each candidate. Following is a high-level overview of each of the aforementioned methods.

4.3.1. Voting With Smart Contracts

Koç et al. [27] propose a voting system based on smart contracts on the Ethereum blockchain. Since deploying smart contracts on the official blockchain is costly, the voting process in question is carried out on Rinkeby, an Ethereum test network. The general process is outlined in figure 7. To use a test network, users must obtain an official Ethereum wallet and use the settings menu to change the connection to the test network. Rest of the process is described as follows:

1. Smart contract is deployed on the Ethereum blockchain, saving the owner of the contract as "chairman" and defining structures for voters and candidates, as well as the functions for voting, giving the right to vote, and counting votes. The code blocks for each of these can be seen in figures 7.1, 7.2, 7.3, and 7.4.

2. Chairman initializes the voting process and gives out voting rights to individuals based on their Ethereum wallet codes.

3. Voters contact the smart contract through a transaction in the Ethereum wallet to vote for their candidate. The smart contract checks if they've already voted, and if not, distributes a vote to their favored candidate. Current winning candidate is returned after each vote. The function for the winning candidate can also be called once the election is over.

This solution does not provide anonymity as a vote from one wallet to another can be seen by anyone. As such, it should only be used for small-scale polls and elections that are not critical.

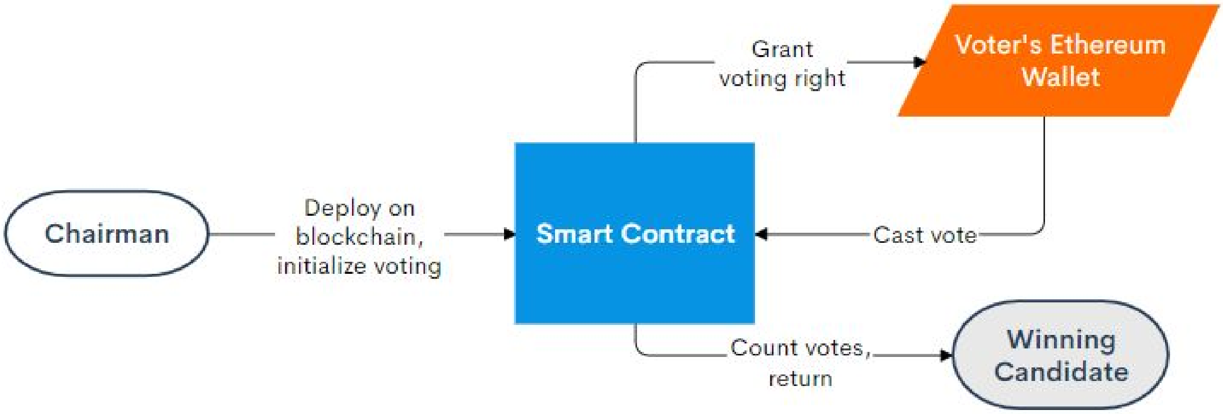
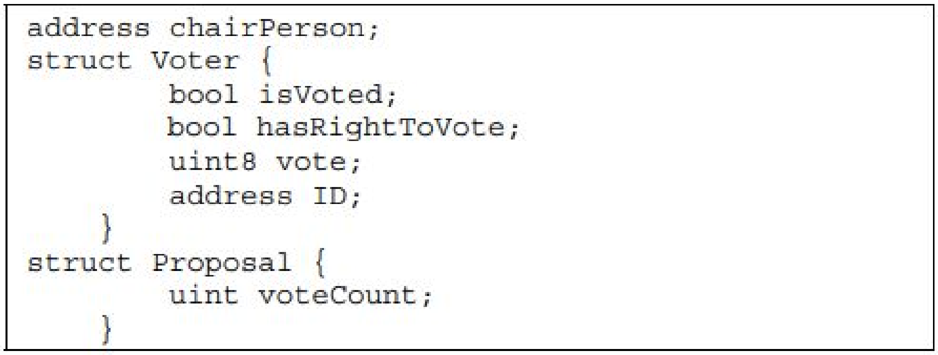
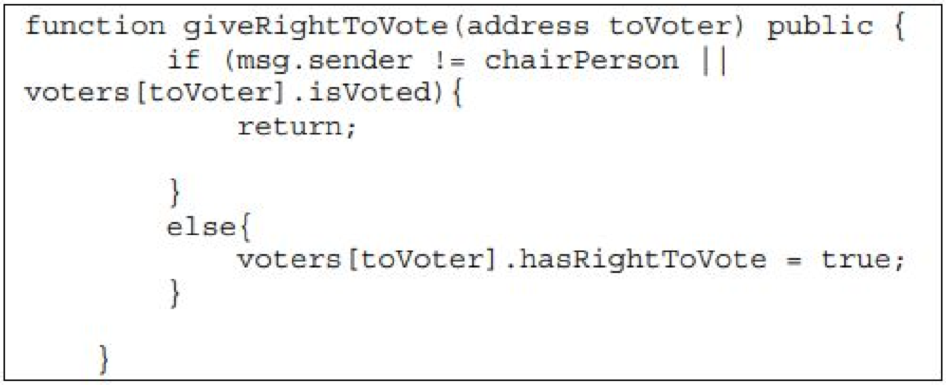


Figure 7. Process of voting with a smart contract.



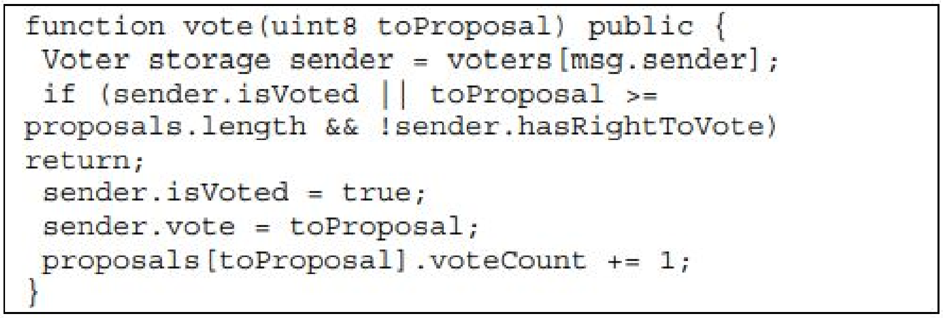
```
address chairPerson;
struct Voter {
        bool isVoted;
        bool hasRightToVote;
        uint8 vote;
        address ID;
    }
struct Proposal {
        uint voteCount;
    }
```

Figure 7.1. Code block defining structures and variables. [27]



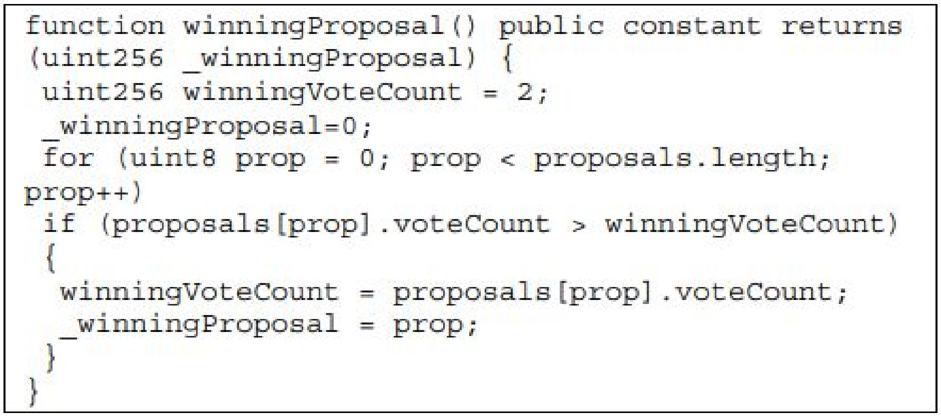
```
function giveRightToVote(address toVoter) public {
        if (msg.sender != chairPerson ||
voters[toVoter].isVoted){
            return;

        }
        else{
            voters[toVoter].hasRightToVote = true;
        }

    }
```

Figure 7.2. Code block defining the function of giving voting rights. [27]



```
function vote(uint8 toProposal) public {
 Voter storage sender = voters[msg.sender];
 if (sender.isVoted || toProposal >=
proposals.length && !sender.hasRightToVote)
return;
 sender.isVoted = true;
 sender.vote = toProposal;
 proposals[toProposal].voteCount += 1;
}
```

Figure 7.3. Code block defining the voting function. [27]



```
function winningProposal() public constant returns
(uint256 _winningProposal) {
 uint256 winningVoteCount = 2;
 _winningProposal=0;
 for (uint8 prop = 0; prop < proposals.length;
prop++)
 if (proposals[prop].voteCount > winningVoteCount)
 {
  winningVoteCount = proposals[prop].voteCount;
  _winningProposal = prop;
 }
}
```

Figure 7.4. Code block defining the function to return voting results. [27]

4.3.2. Voting With Zcash

The voting protocol proposed by Tarasov [33] utilizes basic functions offered by the Zcash blockchain to create a platform to cast votes. Zcash is chosen as it allows to anonymize the users who participate in an election with its option to pass both private and transparent values during a transaction. Zcash is a cryptocurrency born from the Zerocoin protocol, which was designed to obscure the trail of transactions on the Bitcoin blockchain. Takabatake et al. [30] have designed a voting process using the Bitcoin blockchain and Zerocoin protocol. However, as the Bitcoin community refused the proposal to integrate it into the Bitcoin network, Zerocoin is currently incompatible with Bitcoin. [34] Another proposed solution based on Zcash [35] employs quadratic voting, which allows for voters to pay in order to cast additional votes for a desired candidate or idea. This means that the resulting outcome is aligned with the intensity of voter preferences, rather than simply conforming to the majority vote. The general process of voting using Zcash is shown in figure 8 and described as follows.

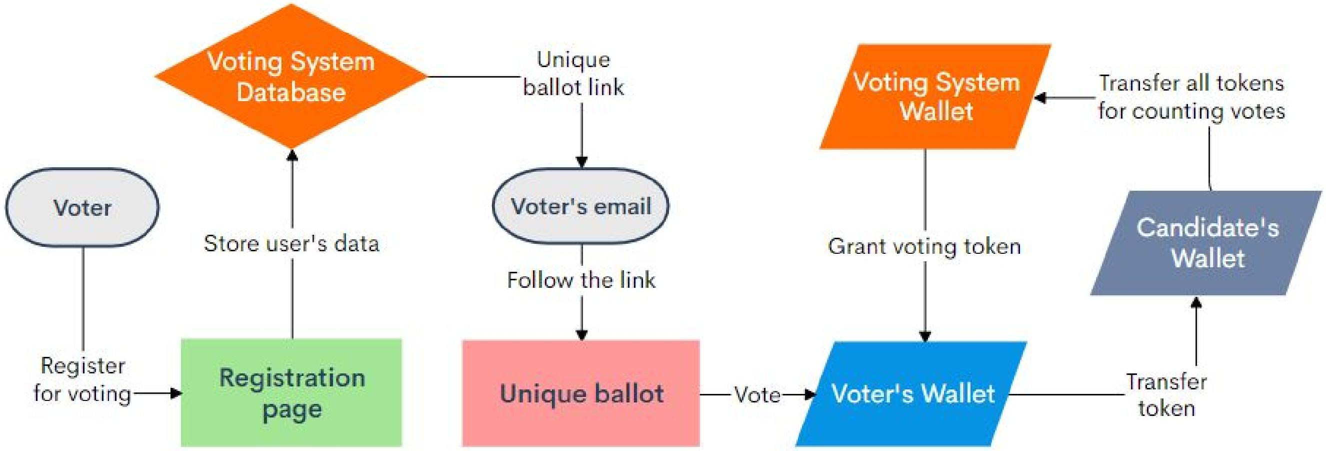


Figure 8. Voting process using Zcash. Based on [33].

1. User registers for the poll using the registration page provided by the authority. Once the user is verified and registered, an email with a unique link is sent to the voter. The link in question brings the user to a unique election ballot. Given that the voter has provided a valid address of their Zcash wallet, the system sends them a zero coin (ZEC) token to cast their vote.
2. The voter, after receiving a ZEC token, chooses a preferred candidate and proceeds through a legal agreement before the transaction takes place. The system then increments its counters that, among others, represent the total number of voters, and sends a ZEC token from the voter to the candidate's wallet. This serves the purpose of a vote token.
3. Once voting is concluded, the candidates forward all their ZEC vote tokens received during the voting phase to a wallet owned by the voting system. The system wallet tracks its number of tokens before and after each transaction to calculate the number of votes received by the candidates. Since the total number of votes cast by the voters is also recorded, the candidates cannot be dishonest in the amount of ZEC tokens they send to the system without being discovered.

4.3.3. Voting With a Custom Blockchain

Creating a blockchain for the voting system is also a possibility. Ayed [28] has proposed a voting solution that employs a separate blockchain for each candidate. The votes to specific candidates are added to the corresponding blockchain. As the voting method is designed with official elections in mind, there is a node in each voting district. The simplified process is illustrated in figure 9.

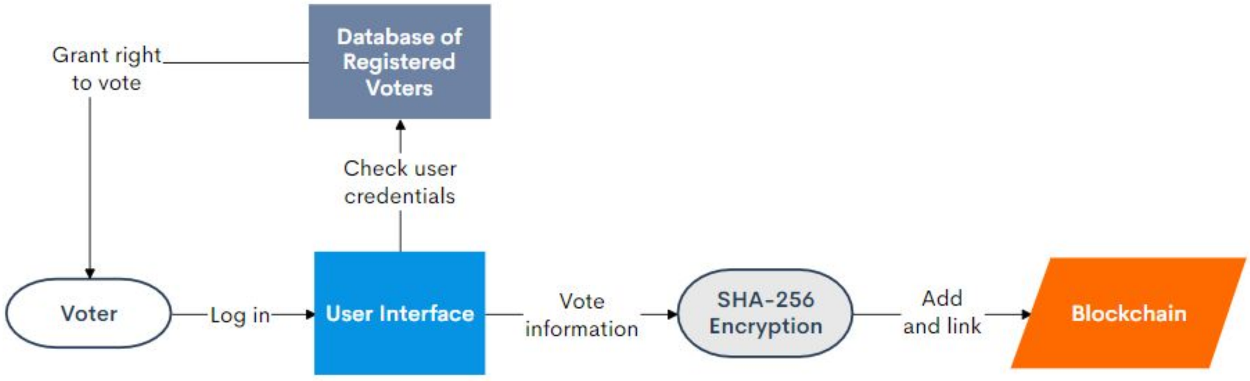


Figure 9. Simplified process of voting with a custom blockchain. Based on [28].

1. User logs in to the voting system using their credentials. In this case, it is assumed the voter is already registered and their identity has been confirmed by the authorities. If the system is able to match the provided credentials with a valid voter, it grants the user a right to vote.
2. The user is guided to the ballot through a friendly interface, where they must choose a candidate to vote for or leave the ballot empty to cast a protest vote.
3. Once the vote is casted, the system generates an input consisting of the voter's identification number, full name, and the hash of the previous vote to make sure each input is unique. This information is then encrypted using a one-way hash function, SHA-256. Without knowing the input data, it is impossible to reverse engineer it and retrieve the voters' information.
4. Once the correct blockchain is chosen according to the selected candidate, the hashed information from the previous stage is sent to a node that adds it to the blockchain and links it to the previously cast vote. A simple representation of the blockchain structure can be seen in figure 9.1.

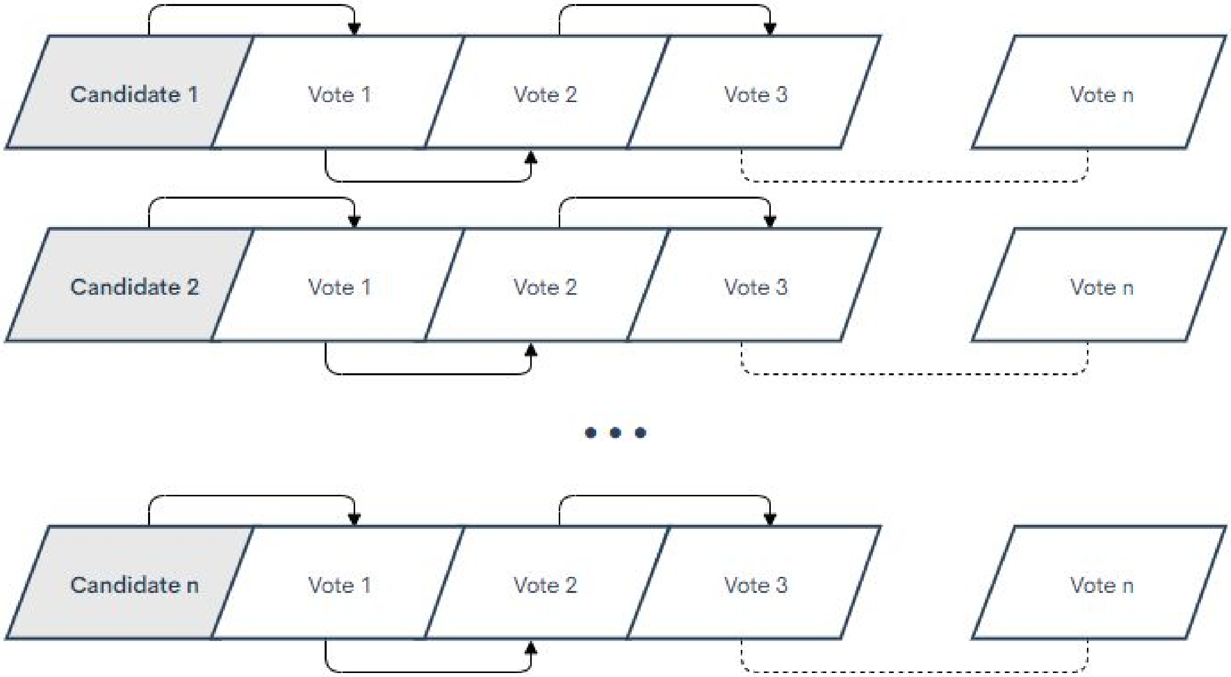


Figure 9.1. Blockchain structure for each candidate. Based on [28].

4.3.4. Voting With Cryptographic Signatures

To provide further anonymity to a voter, it is possible to incorporate cryptographic signatures, such as ring signatures or blind signatures [36], in the voting scheme. This particular voting system based on the Bitcoin network and ring signatures is proposed by Wu [31]. It contains three main entities: a registration authority (RA), election authority (EA), and a Bitcoin address pool that consists of randomly generated Bitcoin addresses.

1. During the preparation phase, the election authority (EA) sets up the project and saves its Bitcoin wallet address into the system. Candidates authenticate themselves to the registration authority (RA) and are each given a unique ID. Addresses for candidates are also initialized using the Bitcoin address pool.

2. Polling stations run by the RA are located in residential areas. Users are registered to vote after they've authenticated themselves to the RA with a passport or other means of identification. Once registered, a public/private key pair is generated for the voter. The voter must then share

the public key with the system and hold onto the private key. Registration is closed on the set deadline and the list of voters' public keys is saved to the system.

3. During the voting phase, the system sends all users the list of public keys and candidate IDs, as well as a set amount of Bitcoin for voting. Voters use their private key, chosen candidate's ID, and the public keys of all voters as components to generate a unique ring signature. This ring signature is hashed using SHA-256, which is then added to the blockchain by sending the fixed amount of Bitcoin, hashed signature, and candidate ID to EA's Bitcoin wallet address. Both hashed and unhashed versions of the ring signature are also saved to the system. The process of generating ring signatures is described in figure 10.

4. In the tallying phase, the system returns all sets of hashed and unhashed ring signatures generated by the users. Each transaction's ring signature validity is verified by the system, and each candidate's vote count is increased by one for every verified transaction that includes their ID. If more than one transaction is made from the same address, only the first one is counted. Figure 10.1 depicts the process of voting, validation, and tallying in a voting system with ring signatures.

5. As EA's wallet transactions and the list of all public keys are publicly readable, every voter can verify their vote using the candidate ID, list of public keys, and the ring signature.

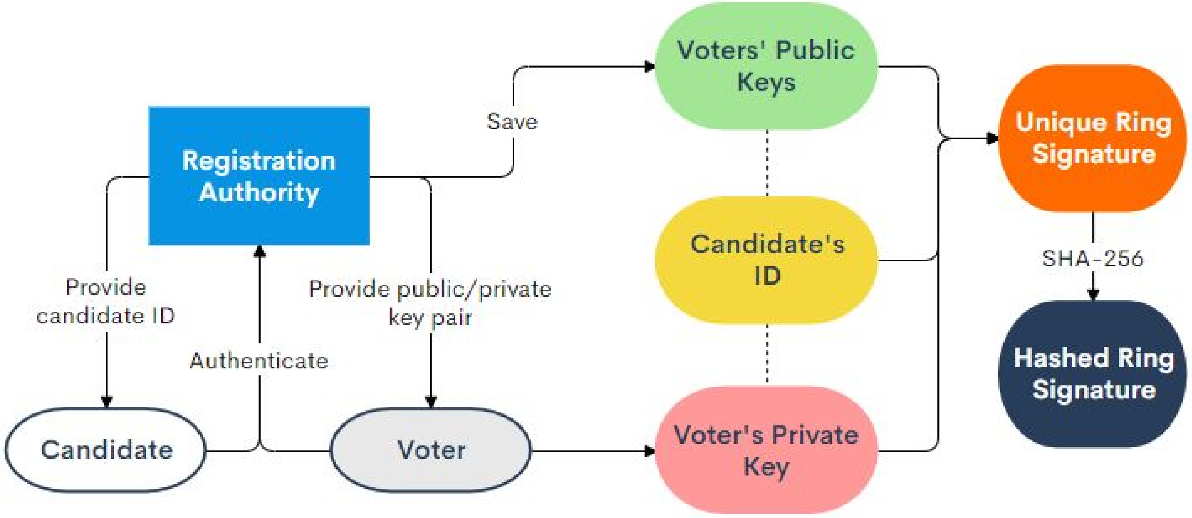


Figure 10. Process of generating ring signatures.

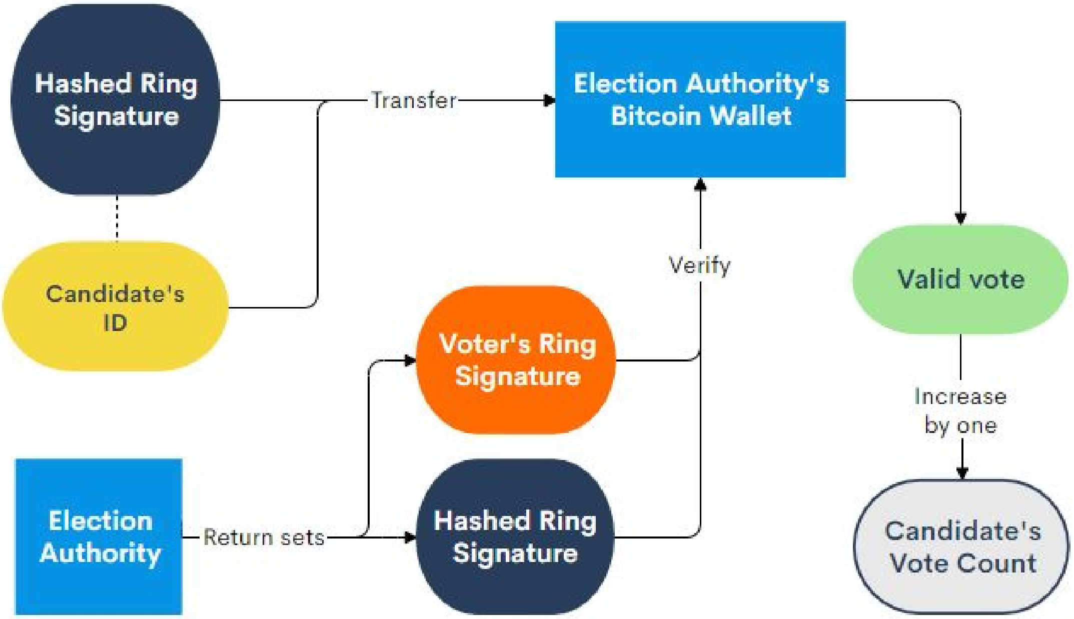


Figure 10.1. Casting, validating, and tallying votes in a solution with ring signatures.

Table 2 provides a quick overview of the voting methods described in this chapter. In summary, the general voting process of these methods is as follows. First, the voting system is set up on the blockchain. The users are then authenticated and given voting rights. This is followed by the user making a selection of a proposal or candidate and casting a vote. How exactly the vote is cast depends on the particular solution: this might be done by adding the encrypted vote to the custom blockchain [28], transferring a cryptographic signature to the election authority [31], transferring a vote token to the candidate [33], or calling the voting function of a smart contract [27]. In all cases, this stage incorporates blockchain technology. The votes are then validated, counted by the system, and may be verified by anyone who wishes to do so by acquiring a copy of the blockchain.

Name	Description	Reference
Voting With Smart Contracts	Smart contract is deployed on the Ethereum blockchain with functions for voting, giving voting rights, and counting votes. Voting rights are given based on Ethereum wallet codes. Voters contact the smart contract through a transaction on the Ethereum wallet to cast votes. Smart contract counts votes and returns the winning candidate.	[27, 37-45]
Voting With Zcash	Voters are led to a unique voting ballot after registering and providing a Zcash wallet address. Voting system sends a vote token (ZEC) to the valid users, which they can then use to vote by transferring it to a candidate's Zcash wallet. Once voting is concluded, candidates send all their Zcash tokens to the voting system's wallet, which counts the number of votes received by each candidate.	[30, 33, 35, 46]
Voting With a Custom Blockchain	In the example, a separate blockchain is initialized for each candidate. Voters log into the voting system and valid users are granted a right to vote. Voters are then guided to a ballot where they choose a candidate and cast their vote. Voter's identification number, full name, and the hash of the previous vote are encrypted and added to the blockchain of the desired candidate. The hashed vote is linked to the previously cast vote on the blockchain.	[28, 29, 47-51]
Voting With Cryptographic Signatures	Voters authenticate themselves to the registration authority and are provided a public/private key pair while all the voters' public keys are saved to the system. Voters use information related to their identity and the chosen candidate to generate a unique cryptographic signature. The signature is transferred to the voting system's Bitcoin wallet address along with the candidate's ID to cast a vote. All transfers are verified by the system and each candidate's vote count is increased by one for every valid vote cast for them.	[31, 36, 52-57]

Table 2. Overview of the blockchain-based voting solutions.

4.4. Advantages and Limitations of Blockchain Voting

Since blockchain operates on a peer-to-peer network without being controlled by a central authority, it is considered transparent and secure to attacks that target the central point of a system. Additionally, this means there is no need to trust a single authority to verify that the transactions are correct. These characteristics of a decentralized network allow introducing further democratic processes to electronic voting. [32]

In addition to being reliable and efficient for avoiding manual errors when checking forms, storing votes on the blockchain prevents existing data from being tampered with. [29] This also means that in case a blockchain-based voting solution uses components such as smart contracts, they cannot be illegally removed or manipulated once written. Hence, they can work properly, autonomously and transparently without any external assistance. [15]

Furthermore, results of voting can be verified by external auditors by obtaining a copy of the blockchain and checking that the votes in it are legitimate and that there are no duplicates. It is then possible to count the verified votes and compare the results with the official tally. [32]

Even though the blockchain technology offers many advantages for a digital voting system, there are some properties that cannot be addressed solely by using the blockchain. For example, authentication of voters on a personal level requires the integration of an external system or additional mechanisms, such as implementing biometric factors [58].

As an administrator is required for setting up and initializing the voting process on the blockchain, problems may arise when said administrator is untrustworthy. In some cases, it might be possible to falsify votes by creating new blockchain addresses if the administrator makes sure the added number of ballots doesn’t overflow the total number of possible votes. To discourage this, a fee per vote could be introduced to make the attack less cost-effective. [53]

There is also an issue with scalability for the major known blockchain networks. Each transaction on Bitcoin supports storing up to 80 bytes of arbitrary data, with a maximum of 7 transactions allowed to be made per second. Moreover, Ethereum measures its operations and storage using a metric called “gas”, and the gas that can be consumed by the users is limited. As such, these blockchains may not be able to support deploying voting systems for elections on the national scale. [59]

5. Discussion

This chapter provides an overview of the proposed voting solutions without making any modifications to their design. The results of the literature review are concluded in a framework that allows for interested parties to quickly find research papers relevant to their chosen voting method. For example, the framework could be used by analysts to find research material to assist them in designing, developing and implementing secure voting systems. General contents of the table, as well as the process of using the framework to find relevant studies are also explained.

5.1. Framework for Blockchain Based Voting

Framework providing an overview of all the proposed voting methods can be seen in table 3. To make it as simple as possible to select a blockchain-based voting solution while covering all the necessary bases, the papers are categorized by their voting types, blockchain types, methods, advantages, limitations, and references. Columns chosen to describe the solutions are explained as follows. Voting type allows the reader to find relevant papers based on the scale and type of use case they wish to implement a voting method for. These include polls and elections classified into small and large-scale voting cases, depending on which types of voting the particular solution supports. Blockchain type used in the implementations is either public or private. The method column denotes one of the four main methods that provide an overview for the general process of a blockchain voting solution. These are described in the previous chapter and include voting with smart contracts, Zcash, custom blockchain, and cryptographic signature. In addition to the general properties of blockchain voting, the advantages and limitations of particular voting methods are also included in the framework. Finally, the reference column provides reference numbers for studies conforming to the aforementioned properties. This makes it simple to identify papers relevant to specific voting methods correctly and efficiently.

Voting Type	Blockchain Type	Method	Advantages	Limitations	Reference
Small-scale polls and elections	Public	Smart Contract	Smart contracts cannot be (illegally) removed nor manipulated once written. Ethereum network is able to provide self-tallying. All transactions can be run asynchronously.	Difficult to make updates once the smart contracts are deployed. Code executes slower in smart contracts than in servers. Accessing external data requires external code.	[27, 39, 40, 42, 43]
Small to large-scale polls and elections	Private		On a private test network the initial block difficulty can be adjusted so that blocks can be produced in less time.	More difficult to set up as it includes building a private Ethereum test network.	[37, 38, 41, 44, 45]
Small-scale elections	Public	Zcash	ZCash allows for anonymization of the identities of the voters. The underlying ZCash protocol inherently ensures that every vote is valid and no same vote can be cast twice.	Zcash might be more vulnerable to attacks than Bitcoin or Ethereum. Since the target platform of the protocol would be user's end devices, there's a possibility of the voting machine being compromised.	[30, 33, 46]
Small-scale polls and elections			This method employs quadratic voting, which allows for voters to pay in order to cast additional votes for a desired candidate or idea. Thus, the resulting outcome is aligned with the intensity of voter preferences.		[35]
Small to large-scale elections	Private	Custom Blockchain	New blocks can be created in a custom blockchain almost momentaneously. More realistic for large-scale elections as it can be set up specifically to accommodate them.	With fewer nodes than in public networks, it might be easier to attack the entire blockchain.	[28, 29, 47-51]
Small-scale polls and elections	Public	Cryptographic Signature	In case of using digital signatures, it is difficult for the voter to prove how they voted. As such, a potential coercer cannot cooperate with the voter.	If voting authority is corrupt, it might be possible to falsify votes by generating extra signatures.	[31, 52, 54-57]
Small to large-scale polls and elections	Private				[36, 53]

Table 3. Framework of voting solutions based on blockchain technology.

Figure 11 illustrates the process of finding relevant papers by using the framework. First, the reader should have a voting type in mind that they wish to implement a voting system for. As such, it is efficient to start from the first column and identify which rows are relevant to that particular use case. The next useful step for the reader is to take a look at the advantages and limitations pertaining to these rows in order to decide which important properties their voting solution is going to include. They can then follow the chosen rows to find out the suitable voting methods and, if applicable, decide whether to implement a public or private blockchain for the solution. The general process of possible voting methods can be seen in chapter 4.3 of the thesis and references to the full papers can be located in the references column of the framework.

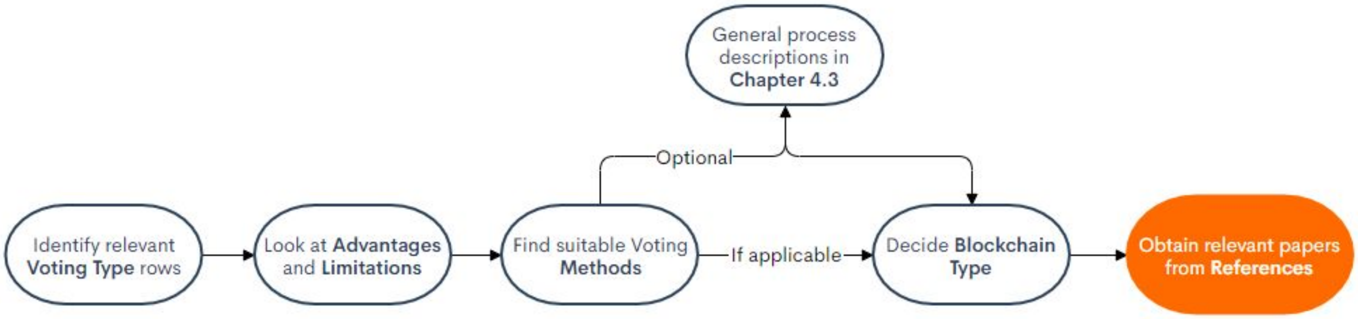

General process descriptions in Chapter 4.3
Optional
Identify relevant Voting Type rows
Look at Advantages and Limitations
Find suitable Voting Methods
If applicable
Decide Blockchain Type
Obtain relevant papers from References

Figure 11. Process of using the framework to find relevant papers.

6. Conclusion

The aim of the thesis was to address the main research question of how blockchain technology can be used to enable secure electronic voting. This was done by carrying out a systematic literature review. By doing so, it was found that blockchain voting can be used for both polls and elections of various scales. Four main methods were identified to provide a general overview of a blockchain-based voting process, including voting with smart contracts, Zcash, custom blockchain, and cryptographic signatures. The advantages and limitations of blockchain voting were also determined. As a result of the literature review, a framework was created providing an overview along with references for different blockchain-based solutions. The resulting framework could be beneficial to someone intending to design, develop and implement secure voting systems as it provides a way of finding relevant studies quickly and efficiently.

Future work can be done by identifying additional papers that provide recent solutions for using blockchain technology in a voting system. The data from these additional papers can then be extracted, analyzed, and used to improve the existing framework. In this way, the framework can always stay functional and up to date for as long as it is maintained.

References

[1] Madise Ü. Martens T. E-voting in Estonia 2005. The first Practice of Country-wide binding Internet Voting in the World. 2006.

[2] Gerlach J., Grasser U. Three Case Studies from Switzerland: E-voting. Berkman Center Research Publication. 2009.

[3] Stenerud. I. S. G., Bull C. When reality comes knocking: Norwegian experiences with verifiable electronic voting. *5th International Conference on Electronic Voting 2012 (EVOTE2012)*, 2012, vol. 205, p. 21-33.

[4] Springall D., Finkenauer T., Durumeric Z., Kitcat J., Hursti H., MacAlpine M., Halderman A. Security Analysis of the Estonian Internet Voting System. *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, p. 703-715.

[5] Lewis S. J., Pereira O., Teague V. Ceci n'est pas une preuve: The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system, 2019. https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf (13.01.19)

[6] CISA. Understanding Denial-of-Service Attacks, 2009. US-CERT. https://us-cert.cisa.gov/ncas/tips/ST04-015 (13.01.19)

[7] Osgood R. The Future of Democracy: Blockchain Voti1978ng. COMP116: Information Security 2016.

[8] What Is Blockchain Technology? A Step-by-Step Guide For Beginners. Blockgeeks. 2018. http://blockgeeks.com/guides/what-is-blockchain-technology-a-step-by-step-guidethan-anyone-can-understand/ (19.01.19)

[9] Polys Online Voting System. https://polys.me/ (05.08.20)

[10] Nasdaq eVoting Technology. https://www.nasdaq.com/solutions/evoting-technology (05.08.20)

[11] Economist. 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (18.01.19)

[12] Raval S. What Is a Decentralized Application? O'Reilly Media, Inc. Sebastopol, California. 2016.

[13] Ansper A., Buldas A., Willemson J. Krüptograafiliste algoritmide elutsükli uuring 2017. 2018. https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf (20.01.19)

[14] Buterin V. Ethereum white paper. 2013. https://ethereum.org/en/whitepaper/ (11.02.19)

[15] Clack C. D., Bakshi V. A., Braine L. Smart contract templates: foundations, design landscape and research directions. 2017. arXiv preprint arXiv:1608.00771.

[16] Raval S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc. Sebastopol, California. 2016.

[17] Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978, p. 120–126.

[18] Fujisaki E., Suzuki K. Traceable Ring Signature. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*. 2007, p. 181-200.

[19] Debnath, A., Singaravelu P., Verma S. Efficient spatial privacy preserving scheme for sensor network. *Central European Journal of Engineering.* 2012.

[20] Kitchenham B., Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering. Engineering. 2, 1051. 2007.

[21] Fink A. Conducting research literature reviews: from the Internet to paper. 2010.

[22] Levy Y., Ellis T. J. A systems approach to conduct an effective literature review in support of information systems research. *Informing Sci. 9*, 2006, p. 181–211.

[23] Okoli C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inf. Syst.* 37, 2015, p. 879–910.

[24] Webster J., Watson R. T. Analyzing the past to prepare the future. *MIS Q.* 26, xiii–xxiii. 2002.

[25] Randolph J. J. A Guide to Writing the Dissertation Literature Review. *Pract. Assessment, Res. Eval.* 14, 2009, p. 1–13.

[26] Sampigethaya K., Poovendran, R. A framework and taxonomy for comparison of electronic voting schemes. *Comput. Secur.,* 25(2), 2006, p. 137–153.

[27] Yavuz E., Koç A. K., Çabuk U. C., Dalkılıç G. Towards Secure E-Voting Using Ethereum Blockchain. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, 2018, p. 1-7.

[28] Ayed A. B. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9, 2017, p. 1-9.

[29] Hanifatunnisa R., Rahardjo Budi. Blockchain based e-voting recording system design. *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, p. 1-6.

[30] Takabatake Y., Kotani D., Okabe Y. An anonymous distributed electronic voting system using Zerocoin. 2016.

[31] Wu, Y. An E-voting System based on Blockchain and Ring Signature. School of Computer Science, University of Birmingham. 2017.

[32] Lee K., James J. I., Ejeta T., Kim H. Electronic Voting Service Using Block-Chain. *Journal of Digital Forensics, Security and Law*, 2016, vol. 11. p. 123-136.

[33] Tarasov P., Tewari H. Internet voting using Zcash. *IACR Cryptology ePrint Archive*, 2017, p. 585.

[34] Wells C. Hopkins researchers are creating an alternative to Bitcoin. *The Baltimore Sun.* 2014. http://www.baltimoresun.com/news/maryland/bs-md-hopkins-bitcoin-20140201-story.html (15.03.19)

[35] Park S., Rivest R. L. Towards secure quadratic voting. *Public Choice 172*, 2017, p. 151–175.

[36] Cruz J. P., Kaji Y. E-voting System Based on the Bitcoin Protocol and Blind Signatures. 2017.

[37] Khoury D., Kfoury E. F., Kassem A., Harb H. Decentralized Voting Platform Based on Ethereum Blockchain. *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, Beirut, 2018, p. 1-6.

[38] Triantafyllidis N. P. Developing an Ethereum Blockchain Application. University of Amsterdam. 2016.

[39] Meeser F. L. Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain. 2017.

[40] Yang X., Yi X., Nepal S., Han F. Decentralized voting: a self-tallying voting system using a smart contract on the Ethereum blockchain. *Web Information Systems Engineering – WISE 2018. Lecture Notes in Computer Science*, vol 11233. Springer, Cham, 2018.

[41] Latif S., Anees T. Blockchain based decentralized electronic voting system: A step towards transparent elections. 2019.

[42] Lopes J., Pereira J. L., Varajão J. Blockchain based e-voting system: A proposal. *AMCIS*, 2019.

[43] Pawlak, M., Poniszewska-Maranda A. Blockchain e-voting system with the use of intelligent agent approach. *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, 2019, p. 145-154.

[44] Tso R., Liu Z.-Y., Hsiao J.-H. Distributed E-Voting and E-Bidding Systems Based on Smart Contract. *Electronics*, vol. 8, 2019, p. 422.

[45] Sravani C., Murali G. Secure electronic voting using blockchain and homomorphic encryption. *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, 2019, p. 1002-1007.

[46] Tian H., Fu L., He J. A simpler Bitcoin voting protocol. 2018.

[47] Abayomi-Zannu T. P., Odun-Ayo I. A., Barka T. F. A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. 2019.

[48] Bulut R., Kantarcı A., Keskin S, Bahtiyar Ş. Blockchain-based electronic voting system for elections in Turkey. 2019.

[49] Shahzad B., Crowcroft, J. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, vol. 7, 2019, p. 24477-24488.

[50] Sharma K. K., Raghatwan J., Patole M., Lomte V. M. Voting system using multichain blockchain and fingerprint verification. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, 2019, p. 3588-3597.

[51] Li Y., Susilo W., Yang G., Yu Y., Liu D., Guizani M. A blockchain-based self-tallying voting scheme in decentralized IoT. 2019.

[52] Noizat P. Blockchain Electronic Vote. *Handbook of Digital Currency*, 2015, p. 453-461.

[53] Sheer Hardwick F., Akram R. N., Markantonakis K. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* 2018, p. 1561-1567.

[54] Shaheen S. H., Yousaf M., Jalil M. Tamper proof data distribution for universal verifiability and accuracy in electoral process using blockchain. *13th International Conference on Emerging Technologies (ICET)*, Islamabad, 2017, p. 1-6.

[55] Wei C. C. Z., Wen C. C. Blockchain-Based Electronic Voting Protocol. *JOIV: International Journal on Informatics Visualization*, vol. 2, 2018.

[56] Gao S., Zheng D., Guo R., Jing C., Hu C. An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. *IEEE Access*, vol. 7, 2019, p. 115304-115316.

[57] Yi H. Securing e-voting based on blockchain in P2P network. *J Wireless Com Network 2019*, no. 137, 2019.

[58] Çabuk U., Şenocak T., Demir E., Çavdar A. A Proposal on Initial Remote User Enrollment for IVR-based Voice Authentication Systems. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 2017, vol. 6, p. 118-123.

[59] Croman K., Decker C., Eyal I., Gencer A. E., Juels A., Kosba A., Miller A., Saxena P., Shi E., Sirer E., Song D., Wattenhofer R. On Scaling Decentralized Blockchains. *Financial Cryptography Workshops*. 2016.

Appendix A. List of relevant papers used in the literature review

Year	Title	Authors
2015	Blockchain electronic vote	P. Noizat
2016	Developing an Ethereum blockchain application	N. P. Triantafyllidis
2016	An anonymous distributed electronic voting system using Zerocoin	Y. Takabatake, D. Kotani, Y. Okabe
2017	Internet voting using Zcash	P. Tarasov, H. Tewari
2017	Decentralized, transparent, trustless voting on the Ethereum blockchain	F. L. Meeser
2017	Towards secure quadratic voting	S. Park, R. L. Rivest
2017	A conceptual secure blockchain-based electronic voting system	A. B. Ayed
2017	A simpler Bitcoin voting protocol	H. Tian, L. Fu, J. He
2017	E-voting based on bitcoin and blind signatures	J. P. Cruz, Y. Kaji
2017	An e-voting system based on blockchain and ring signature	Y. Wu
2018	Towards secure e-voting using Ethereum blockchain	A.K. Koç, E. Yavuz, U.C. Çabuk, G. Dalkiliç
2018	Tamper proof data distribution for universal verifiability and accuracy in electoral process using blockchain	S.H. Shaheen, M. Yousaf, M. Jalil
2018	Blockchain based e-voting recording system design	R. Hanifatunnisa, B. Rahardjo
2018	Decentralized voting platform based on Ethereum blockchain	D. Khoury, E. F. Kfoury, A. Kassem, H. Harb
2018	E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy	F. Sheer Hardwick, R. N. Akram, K. Markantonakis
2018	Blockchain-based electronic voting protocol	C. C. Z. Wei, C. C. Wen
2018	Decentralized voting: a self-tallying voting system using a smart contract on the Ethereum blockchain	X. Yang, X. Yi, S. Nepal, F. Han
2019	A blockchain-based self-tallying voting scheme in decentralized IoT	Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, and M. Guizani
2019	A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication	T. P. Abayomi-Zannu, I. A. Odun-Ayo, T. F. Barka
2019	An anti-quantum e-voting protocol in blockchain with audit function	S. Gao, D. Zheng, R. Guo, C. Jing, C. Hu
2019	Blockchain based decentralized electronic voting system: A step towards transparent elections	S. Latif, T. Anees
2019	Blockchain based e-voting system: A proposal	J. Lopes, J. L. Pereira, J. Varajão
2019	Blockchain e-voting system with the use of intelligent agent approach	M. Pawlak, A. Poniszewska-Marańda

2019	Blockchain-based electronic voting system for elections in Turkey	R. Bulut, A. Kantarcı, S. Keskin, Ș. Bahtiyar
2019	Distributed e-voting and e-bidding systems based on smart contract	R. Tso, Z.-Y. Liu, J.-H. Hsiao
2019	Secure electronic voting using blockchain and homomorphic encryption	C. Sravani, G. Murali
2019	Securing e-voting based on blockchain in P2P network	H. Yi
2019	Trustworthy electronic voting using adjusted blockchain technology	B. Shahzad, J. Crowcroft
2019	Voting system using multichain blockchain and fingerprint verification	K. K. Sharma, J. Raghatwan, M. Patole, V. M. Lomte

Appendix B. License

Non-exclusive licence to reproduce thesis and make thesis public.

I, Marianne Dengo,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, **Blockchain Voting: A Systematic Literature Review**, supervised by Fredrik P. Milani.
2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.
3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.
4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Marianne Dengo

10.08.2020