applied sciences

MDPI

Article

Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain

Vehbi Neziri, Isak Shabani *, Ramadan Dervishi and Blerim Rexha

Faculty of Electrical and Computer Engineering, University of Prishtina, 10000 Pristina, Kosovo; vehbi.neziri@uni-pr.edu (V.N.); ramadan.dervishi@uni-pr.edu (R.D.); blerim.rexha@uni-pr.edu (B.R.)
* Correspondence: isak.shabani@uni-pr.edu

Abstract: Anonymity and privacy in the electoral process are mandatory features found in any democratic society, and many authors consider these fundamental civil liberties and rights. During the election process, every voter must be identified as eligible, but after casting a vote, the voter must stay anonymous, assuring voter and vote unlinkability. Voter anonymity and privacy are the most critical issues and challenges of almost all electronic voting systems. However, vote immutability must be assured as well, which is a problem in many new democracies, and Blockchain as a distributed technology meets this data immutability requirement. Our paper analyzes current solutions in Blockchain and proposes a new approach through the combination of two different Blockchains to achieve privacy and anonymity. The first Blockchain will be used for key management, while the second will store anonymous votes. The encrypted vote is salted with a nonce, hashed, and finally digitally signed with the voter's private key, and by mixing the timestamp of votes and shuffling the order of cast votes, the chances of linking the vote to the voter will be reduced. Adopting this approach with Blockchain technology will significantly transform the current voting process by guaranteeing anonymity and privacy.

Keywords: privacy; anonymity; electronic voting; Blockchain; vote; distributed technologies

Citation: Neziri, V.; Shabani, I.; Dervishi, R.; Rexha, B. Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain. *Appl. Sci.* **2022**, *12*, 5477. https://doi.org/10.3390/app12115477

Academic Editors: Nadejda Komendantova and Hossein Hassani

Received: 21 April 2022
Accepted: 27 May 2022
Published: 28 May 2022

1. Introduction

Many countries, companies, and institutions have thought about and developed a wide range of election systems that use the most up-to-date technologies to allow all citizens to vote quickly and accurately as a result of the rapid development of technology, the large movement of people, and the necessity for movement.

The use of technology in elections began a long time ago. However, these technologies have varied, including blackballing, punch cards, lever voting machines, ballot optical scanning, electronic voting cabins, direct-recording electronic voting, and other types of technologies combined with some manual parts [1]. When technology is used to organize elections, the success of elections depends not only on the successful implementation of technology but also on procedures related to privacy and auditing. Traditional voting or electronic voting systems are usually managed by a single authority. Therefore, election manipulation is possible because a single authority can change votes. Challenges such as manipulation, privacy, and anonymity can be solved by switching to systems based on distributed technologies that take security aspects into account.

Transactions in traditional electronic voting systems are stored in a centralized ledger or centralized database. In contrast, in distributed systems, there is not just one ledger (database), but all nodes have the same access to a shared ledger, which allows all participants to see the system of record (ledger). Various voting techniques are used, as mentioned in [2,3], ranging from raising hands, punch cards, lever voting machines, electronic voting machines, and online voting, but the idea is for voters to make their electoral choices anonymously. Technology is developing faster than most people can understand it, but the issues of privacy and personal data protection are becoming increasingly critical.

All efforts to implement technology aim to increase security, guarantee integrity, and ensure the reliability of the process, from voting to counting and the announcement of results. Regardless of the type of technology used in the electoral process, voters pay the most attention to the direct use of voting technology, privacy, and anonymity. Electronic voting, or e-voting, is one of the many government services that the implementation of Blockchain can positively affect. E-voting, on the other hand, is a service that may be utilized by a variety of companies and institutions to save time and money, to provide remote access, and to increase inclusiveness. Despite advancements in technology and in voting processes, transparency, anonymity, and privacy remain a concern. As a result, the adoption of new technologies should enable the promotion of system trust and dependability by allowing mechanisms to be audited, but they should also ensure privacy. Privacy is defined in different ways, but Alan Westin [4] defines privacy as "individuals have the right to determine how much personal information they want to disclose and to whom"; however, this does not apply to voting because the privacy of voters should not be dependent on them. The electoral process is very complex and comprehensive; it determines who will lead public life, and it functions as a kind of competition where we hire our representatives. The origin of the electoral process began long ago and has historically developed differently from one country to another [5]. In almost all democracies, the electoral process is highly reliant on the legal aspect, which defines the mechanisms for organizing, supervising, and conducting the electoral process accurately and without deception, but this is not always achieved in practice. There are initiatives for electronic voting in various countries and institutions, and many of them are moving towards more advanced electronic voting systems. The purpose of electoral reform varies from country to country. Some countries seek to increase voter turnout, others seek to reduce electoral fraud, and others reduce bureaucratic procedures and make it easier for voters [2]. Electronic voting can meet these numerous objectives to speed up, simplify, and reduce the cost of elections, and it encourages higher voter turnout, particularly among young voters, who are the most tech-savvy. To better fulfill the legal aspect and organize the best possible elections, many countries have started or are implementing some form of electronic voting. There are many definitions of electronic voting, but according to [6], it is a way to get responses from voters at a given time and make elections more efficient. According to [7], electronic voting is a system where registration, ballot casting, or counting are conducted using information and communication technologies. Therefore, electronic voting can be any voting method in which voter preferences can be expressed or collected through electronic resources. There are various ways to organize electronic voting. Some countries use different electronic devices at polling stations, while others use the Internet [8]. Regardless of the methods used, all efforts to implement new technologies aim to ensure the credibility of the voting process and of the election results. The electronic system faces various challenges but must guarantee the anonymity and privacy of voters to be reliable. Electronic voting systems must also consider transparency, verifiability, and other aspects. Various types of technology offer different possibilities for these features, but there are also difficulties in achieving these features. The use of technology in electoral processes must be safe and secure to the same extent that equivalent manual processes are safe and reliable.

Today, many countries have developed or are developing advanced voting systems using the latest technologies to enable all citizens to vote quickly and accurately regardless of their location [9,10]. However, some countries have stopped e-voting projects due to the unreliability of the technologies used [11], but distributed Blockchain technology can increase credibility and reliability. There is always controversy with any new technology, so continual research on all aspects of the process and technology is necessary.

Despite the many benefits of online or electronic balloting using different methods, digital vote casting needs to be significantly researched because it can also introduce new threats [12], such as modifying the voter list or adding illegitimate voters, accounting theft, or account interference.

Blockchain technology offers some attractive features, such as transparency, immutability, and distributed consensus, which are difficult to achieve using other technologies. These features make Blockchain an appealing technology for elections, as distributed consensus might boost voter confidence and guarantee correct outcomes. Blockchain technology has primarily been used in banking and finance, where anonymity is not required because it is necessary to know who is making the transaction; however, in electronic voting, anonymity is a required and indisputable feature. There have been several reviews and ideas about Blockchain technology, but Blockchain-based applications and electronic voting have generally received limited attention [13]. However, there are several different schemes and protocols that other authors have proposed, but privacy and anonymity are the main challenges that have not yet been adequately addressed.

Our paper analyzes how Blockchain technology might be used to alleviate these challenges. The main focus will be on assuring privacy and anonymity through the latest Blockchain technology, which offers new possibilities that previous technologies did not. In addition to analyzing and comparing existing electronic voting solutions in Blockchain, we also propose a schema by combining two different Blockchains.

The concept used in this scheme enables voter privacy and voting anonymity as two basic rights in the voting process. The first Blockchain, called "Distributed Key Management" generates and manages keys and key infrastructures. The second Blockchain, called "Encrypted Votes Blockchain" is separate from the first Blockchain and is used to store votes during the voting process.

2. Blockchain Description

Blockchain technology is a relatively new technology that has changed governments, institutions, and industries worldwide. Understanding distributed systems is essential to understanding Blockchain technology, as Blockchain is a distributed system at its core, which can be centralized or decentralized. In other words, Blockchain is a distributed technology used to record electronic data transactions, which are linked in blocks and stored in many places simultaneously (nodes). The node can be an individual player in a distributed system. Distributed and decentralized systems can easily be confused. The difference is that there is a central authority in a decentralized system that governs the whole system. In contrast, in a distributed system, the work is done by all nodes simultaneously to achieve this result.

The Blockchain era started with Bitcoin, a digital virtual currency or digital payment system without an organization to authorize transactions. Many people think that Blockchain is the same thing as Bitcoin or that Blockchain is a financial technology. Because people are starting to hear more about Blockchain right after the peak of Bitcoin's popularity, such an opinion may be considered valid because the essence of the Bitcoin system is Blockchain, through the computational process called mining; however, Blockchain is more than that. The rules of creating blocks and mining are explained in many types of research, including a study by Gobel [14]. Companies, organizations, and institutions are now researching Blockchain technology, and millions of dollars have been spent experimenting with it. Therefore, Blockchain is being implemented and used in many institutions [15], such as banks, finance, and governments, and in various processes of democracy, such as electoral processes. However, a large part of the global population still has no idea what Blockchain is or how it works. Blockchain applications may be categorized according to different fields, particularly the Internet of Things (IoT), so both industry and academia are paying attention to it, and many research studies are being conducted [16]. As the authors of [17,18] say, Blockchain is becoming a standard technology of the digital age. Blockchain functions as a kind of database or open and distributed register in which transactions between parties are recorded into blocks effectively, permanently, and verifiably. No one can modify the data in a Blockchain, so the Blockchain is an immutable ledger. "Block" refers to a collection of data or records, and "chain" refers to a database of these blocks, stored as a list that is public to all participants. These lists are chained cryptographically

in chronological order after meeting the preconditions for creating the block. In its most basic form, the Blockchain structure is presented in Figure 1, with each block containing a timestamp, transactions, block hash, and previous block hash created using cryptographic functions. The initial block, often known as the genesis block, does not contain the prior block's hash. The authors of [12] describe a similar approach to the Blockchain structure, noting that each block's hash is stored in the next block or that each block contains the previous block's hash.

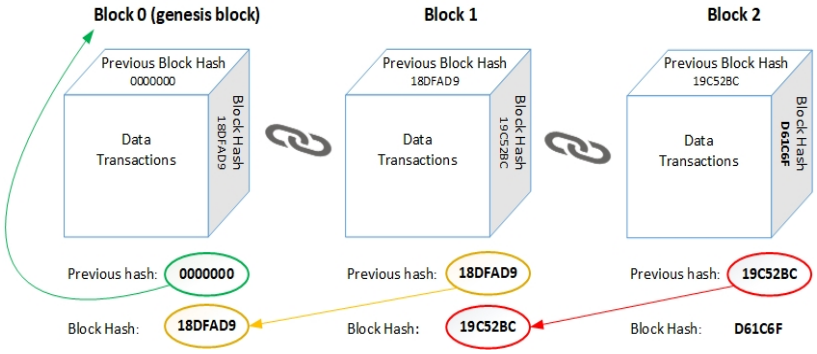

Figure 1. Blockchain data model.

A hash is a value generated by a string using a mathematical function and functions in a one-way manner by converting entries of different lengths into an encoded output with a fixed size. Each block contains a set of transactions that are chronologically linked to previous transaction blocks and precede the transactions of future blocks.

Blockchain may be the future of many businesses and governments. However, as the authors in [19] put it, a transformation of business and government is still far away, but the adoption process will be gradual. Blockchain is a technology that can lay new foundations for our government systems and beyond by providing shared, standardized, and secure data while maintaining privacy and anonymity. One of the government systems is electronic voting, which is a potential use for Blockchain technology. However, for a system or process to be successful, it is essential to choose a suitable Blockchain. The Blockchain system can be public, private, or mixed, but the Blockchain for government services is usually private with known identities, and only they can add transactions [20].

3. Related Works

The requirements of any voting system can be numerous and wide-ranging; however, in general, electronic voting systems should first meet the legal and regulatory framework of the country while also meeting the security requirements, which are mandatory and indisputable. Even new blockchain technology can have certain challenges and drawbacks [21]: unlike other distributed solutions, blockchain is challenging to scale, and node growth affects performance. Therefore, the issue of performance is resolved in private networks by implementing different mechanisms, as presented in [22,23].

The electronic voting system must meet security requirements in order to achieve security that is the same as or greater than traditional paper voting. These requirements can be grouped into four main principles: authentication, integrity, privacy, and verifiability. Authentication guarantees that each voter is uniquely and unmistakably identified, which means that only authorized voters should be able to vote. Integrity ensures that each vote is signed and cannot be changed by anyone other than the voter himself. Privacy is about the confidentiality of the vote and the anonymity of the voters, such that the ballot is secret and its content is not disclosed. Voter privacy enhances voter autonomy and aids in preventing voter pressure and vote-buying. Verifiability is a control principle that ensures accuracy. Various aspects of these principles are listed in the papers [12,24], such as accessibility, availability, transparency, fairness, voter verifiability, privacy, anonymity, auditability, and accuracy, which are very important for a reliable system of voting. Every security require-

ment is very important, but anonymity, privacy, and transparency are the cornerstones of electronic voting [25]. The general security of the voting system, but especially privacy and anonymity, is essential in electronic voting and needs further exploration, especially in Blockchain technology. In traditional systems, privacy is maintained through various cryptographic algorithms, but in Blockchain, this is a challenge because Blockchain is a distributed technology and can even be public.

Recent initiatives to study applications of Blockchain have mainly been in banking and finance, but there have been fewer efforts to study the use of Blockchain for electronic voting. A Blockchain approach to electronic voting using Multichain, which highlights Blockchain's effectiveness in terms of basic electronic voting requirements, is proposed in the paper [26]. This technique allows a solid cryptographic hash-based to be generated totally based on voter-specific records in such a way that allows the voters' anonymity, privacy, and integrity to be protected. There have been various efforts and initiatives to implement Blockchain technology within the election process [27]. Table 1 presents the various electronic voting solutions and applications using Blockchain technology. These applications are for use in elections in corporations, communities, cities, or even nations.

Table 1. Blockchain-based electronic voting applications.

Company/Country	Context/Remarks
Voatz/United States	From 2018 to 2020, Blockchain-based elections were held in West Virginia, Utah, and Colorado. The company used a voting application using biometrics, Blockchain, and hardware-based cryptography by generating paper and chain voting, but the authors in [28] have expressed concerns about its vulnerability to third-party attacks.
Agora/Sierra Leone	In 2018, Sierra Leone deployed a Blockchain-based network for a presidential election to count votes in addition to the official count [29]. The network was an independent vote count, and as a result, privacy and anonymity were very evident because anonymous votes are placed on the Blockchain.
LVH Group/Nasdaq/Estonia	Estonia's cyber security is derived from its keyless signature (KSI) infrastructure, which verifies every electronic activity mathematically using the Blockchain. This system issues each shareholder's voting assets and symbolic voting assets [30].
I.T. Department of Moscow Government/Russia	In December 2017, the Moscow City Active Citizen Program began using a Blockchain for voting and to make voting results publicly auditable [31]. Voting using Blockchain technology was held in Moscow and other regions in 2020, but Ethereum was unable to handle the load, and also there were challenges in securing the ballot [32].
LayerX/Japan	Tsukuba City in 2018 introduced a Blockchain voting system but had problems mainly due to forgotten passwords [33].
Switzerland	In June 2018, Switzerland held elections in the city of Zug based on Blockchain, but it was an experiment and the result was not binding [33].

Another approach was taken by [34], which proposed using ZeroCoin to give Bitcoin anonymity. ZeroCoin's proposal fixes voting groups and makes it difficult for the administrator to vote fraudulently. The authors of the paper [35] proposed the implementation of smart contracts in Ethereum, and they addressed voter security, voters' privacy, and non-repudiation of votes. To gain privacy, the authors of paper [36] used a blind signature as proposed by the authors of paper [37], which mathematically prevents every other person from linking a blinded message to the only one who signed it. The proposal uses Blockchain technology and smart contracts to build a reliable and efficient scheme without using certificates. The various online platforms, their consensus, and the technology used for systems development are given in [12], but problems with scalability are highlighted. Developing a transparent online voting protocol using Ethereum through the open voting network is presented in [38], but this proposal fails to prevent system corruption. The authors of [39] suggested using a distributed, anonymous, and transparent system with minimum trust between the parties, but even their proposal fails to be secured from attacks. A Blockchain-based anti-quantum electronic voting protocol making changes to the Niederreiter cryptosystem algorithm is proposed by [40], but according to [41], security and efficiency decrease as the number of voters increases.

The authors of the paper [12] compare many electronic voting proposals using Blockchains, such as a comparison of schemes, systems, and scalability analyses. These comparisons define the framework, cryptographic algorithm, consensus protocol, audit, anonymity, verifiability, mining difficulty, block, scalability, integrity, accuracy, and other aspects. According to [12] and the comparison of BSJC, Anti-Quantum, OVN, DATE, BES, and BEA, no scheme offers solutions for any security requirements, such as anonymity, security, integrity, variability by voter, scalability, privacy, and auditing. Basit Shahzad & Jon Crowcroft's (BSJC) scheme does not meet the requirements of accuracy, scalability, and variability by voters while the counting method is from a third party [42]. The anti-quantum scheme, similar to the BSJC scheme, does not meet the requirements for accuracy, scalability, or voter variability, but the counting mechanism is self-tallying [40]. Although the open vote network (OVN) [38] does not meet the auditing, accuracy, scalability, or integrity requirements, the counting mechanism is self-tally. The other scheme, DATE, does not meet the auditing, accuracy, or integrity requirements, but it does meet voter scalability and variability [39]. BES, unlike BEA, achieves accuracy, integrity, and scalability, but not anonymity and voter variability [43], which BEA does [44].

Agora, a company based in Lausanne, Switzerland [45], has analyzed and developed a token electoral process mechanism based on Blockchain technology. They point out that current systems do not meet key voting features such as transparency, privacy, and integrity that can be achieved with new technologies. The Australian company, based in Brisbane, Horizon State [46] presents a voting application of Blockchain technology and addresses issues that need to be resolved, such as transparency, anonymity, and voter trust. The American company Voatz, in Boston, MA, USA, has created a Blockchain-based voting system that was approved in the U.S. presidential election. In their technical report [47], this company highlighted the challenges of identity, auditing, and protection against DoS attacks. Zcash is a decentralized payment scheme [25] that aims to provide anonymity, and unlike Bitcoin, proof-of-work in Zcash relies on an optimized form of zero-knowledge proofs called zk-SNARK. Double voting is a concern in Zcash since the same granted vote token is used to vote for several candidates [48]. A zero-knowledge proof refers to a cryptographic approach by which a party, referred to as "the prover", can prove to another party, referred to as "the verifier", that particular statements are true without giving any other information. Because a malicious user could gain unauthorized access to the Blockchain due to its open nature, the zero-knowledge proof can be used to validate if the prover has sufficient transactions in the Blockchain environment without exposing any data [49]. One of the simplest and most often-used proofs of knowledge is the Schnorr algorithm, also known as the proof of knowledge of a discrete logarithm [50].

Different analyses and approaches have been made based on research and evaluation of related work on blockchain-based electronic voting systems, but there are still gaps in the implementation of security requirements. Security requirements for voting schemes, with an emphasis on anonymity and privacy, need to be addressed in future studies.

4. Proposed Approach to Assure Anonymity and Privacy in E-Voting Using Blockchain Technology

Privacy and anonymity are two crucial features related to voter privacy and vote anonymity, so they are closely related to each other in the voting process. Privacy in the case of voting is when no one can know for whom and how the voter is voting, although the voter's identity is potentially known. Anonymity in the case of voting is when no one knows for whom and how the voter voted, but it is potentially known what the voter is doing. No one should be able to detect, identify, or link the vote to a voter during and after the poll. However, in different electoral systems, the voter can verify that their vote is counted correctly.

Since anonymity and privacy are critical features of any electoral system, the data flow diagram, as presented in Figure 2, aims to preserve these two features through two separate Blockchains: Distributed Key Blockchain (DKB) and Encrypted Votes Blockchain (EVB).

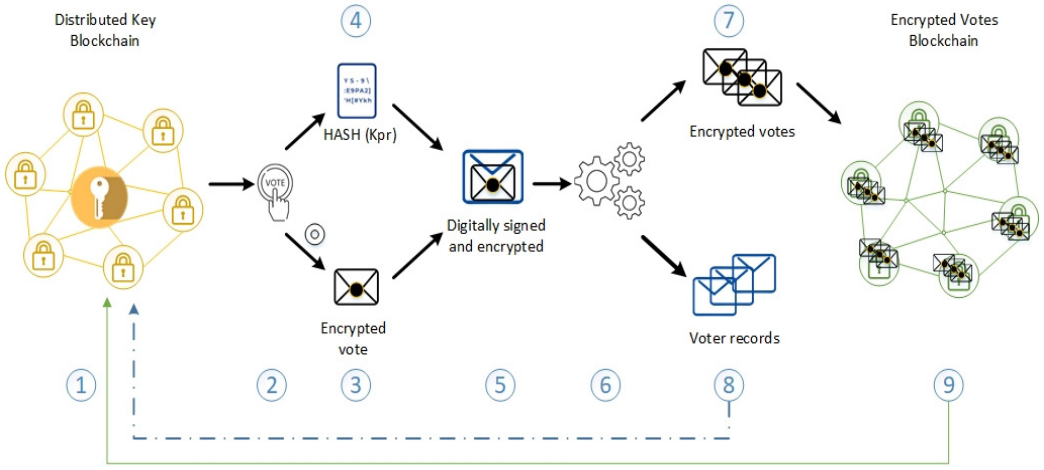

Figure 2. Proposed scheme.

A Distributed Key Blockchain or Distributed Key Management is a cryptographic process in which multiple parties compute a standard set of public and private keys by applying specific protocols and consensus algorithms. This way of generating distributed keys prevents single parties from accessing a private key. The Distributed Key Blockchain can include various authorities dealing with elections, including civil society or other stakeholder institutions. The Encrypted Votes Blockchain (EVB), which is separate from the Distributed Key Blockchain, stores encrypted votes throughout the voting process. Before adding transactions (votes) to the EVB, they are validated and confirmed as legitimate transactions through various consensus algorithms and Smart Contracts. The following steps describe how the scheme works:

- Step 1. The Distributed Key Blockchain generates public keys that eligible voters will use to encrypt votes. In addition to generating and managing keys, this blockchain must verify in advance whether the voter has the right to vote and has not voted before.
- Step 2. At the voter's request and after reaching consensus with the algorithm used for consensus, as described in [51], the DKB generates the pair of keys that the voter will use to encrypt the vote. The preliminary DKG confirms that the voter has the right to vote and has not already voted. There may be some form of interface or application in this part of the scheme that allows voters to vote.

- Step 3. As presented in Figure 3, the voter encrypts the ballot using the public key generated by DKB. The voter generates a cryptographic nonce and adds it to the vote before encrypting it with the public key. A nonce is an abbreviation for "number used only once", which is added to the vote and can be used by the voter to verify that the vote has been counted accurately after it has been counted. Nonce-generation and encryption occurs during the voting process within the interface or application that the voter uses to vote. This relationship, as presented in Figure 3, hash and encrypted vote with nonce, assures the voter that their vote has been counted and, furthermore, their vote is counted correctly.

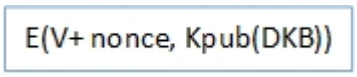

Figure 3. Encrypted vote + nonce.

- Step 4. As presented in Figure 4, the voter generates a hash of their private key within the interface or application and ties it to the encrypted vote + nonce. Using the hash of their private key, the voter may verify that their vote is valid and has not been tampered with during the voting process.

Figure 4. Hash and encrypted vote + nonce.

- Step 5. The encrypted vote + nonce and hash are digitally signed with the voter's private key, as presented in Figure 5. The voter is ready to cast his ballot, which will be sent to the EVB; however, there will be a mechanism in place to separate the voter data from the vote data.

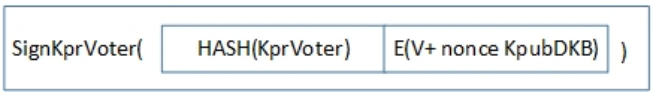

Figure 5. Signature of hash and encrypted vote + nonce.

- Step 6. A form of anonymizer is used in this step, mixing timestamps of votes and shuffling them in order to reduce the risk of voter or vote identification. In addition to timestamp mixing, this approach guarantees that voter data is separated from the vote. This is an analogy of envelopes, where the inner envelope carries the ballot but no information about the voter, whereas the outer envelope contains voter data but no ballot data.
- Step 7. After the operation in step 6, the encrypted votes will be stored in the EVB. Because the so-called outer wrapper, which was the voter's signature, is removed in this step, only the encrypted votes remain as presented in Figure 4. According to the envelope analogy, in this case, it is only the inner envelopes that do not contain any information about the outer envelope (voter data).
- Step 8. The voter's signature is removed from the encrypted ballot, assuring that the vote is not linked to the voter. According to the envelope analogy in this case it is only the outer envelopes, that do not contain any information about the inner envelope (vote data). The DKB stores voter signatures as well as other voter information. Both voters and authorities can verify that a voter has voted by storing the voter's signature and other voter data in the DKB.
- Step 9. The Encrypted Votes Blockchain stores the encrypted votes and the hash of the voter's private key throughout the voting session.

Saving the votes in the EVB without the voter's signature guarantees anonymity and privacy, whereas saving the voter's signature at the DKB prevents double voting. With

an Encrypted Votes Blockchain, the vote cannot be associated with the voter, but even the Distributed Key Blockchain can never associate the signature (voter) with the vote, thus meeting the two main preconditions of voting. Smart Contracts can manage voting time in both DKB and EVB. When the voting time is over, the generation of keys will not be allowed, and consequently, neither will the voting. Next, the counting begins, and if the Distributed Key Blockchain and Encrypted Votes Blockchain have agreed to this, the Encrypted Votes Blockchain signs the dataset of all encrypted votes with its private key and sends this dataset to the Distributed Key Blockchain, as presented in Figure 6. The dataset, in this sense, represents a ballot, a list of votes without voter information, thus assuring voter anonymity and privacy.

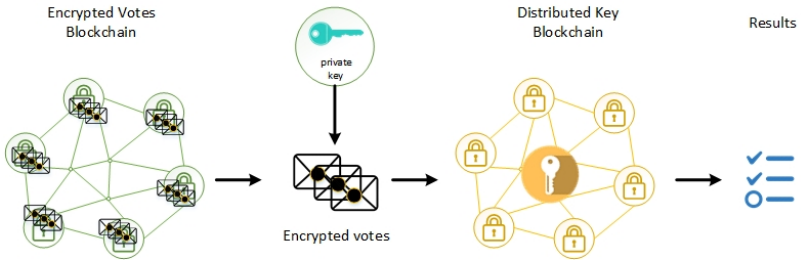

Figure 6. Vote transfer, decryption, and results.

The Distributed Key Blockchain validates the signing of encrypted ballot data sent by the Encrypted Votes Blockchain using EVB's public key; if it is valid, it decrypts the encrypted votes. The private key of the Distributed Key Blockchain is used to decrypt the votes. The Distributed Key Blockchain verifies that the number of voter signatures equals the number of votes received by the Blockchain Encrypted Votes prior to decryption, proving that there are no more votes than voters or vice versa. After decrypting the votes, the Distributed Key Blockchain calculates the votes and announces the results based on the legally defined criteria.

4.1. Evaluation of Storage and Energy Consumption

Various data, such as voter data, electoral zone data, and other comparable data, are processed and stored during the voting process. Depending on the number of voters, the storage size may increase. Data are redundant because the Blockchain is distributed. The redundant data depend on the number of nodes used to mine in the Blockchain. The storage calculation to store the voting records is based on the Blockchain's structure. The organization of data in the block depends on the number of transactions and the platform used. Since, in the current Blockchain, the size of the block is almost 1 MB (megabyte), calculations are based on 1024 bytes (1 kilobyte). According to I BM calculations [52], a 1 MB block must be able to store 1000 votes. Based on the assumptions above, the formula to calculate the needed storage for the voting system is:

$$storage\_size = (number\_of\_voters/1000) * 1\ \text{MB}$$

In the case of 10 million voters, the minimum storage size of one node must be about 10,000 MB or approximately 10 GB (gigabytes). The redundant data are calculated by multiplying the storage_size by the number of nodes performing the mining. Energy consumption should be considered regardless of whether of the two most popular platforms are used, whether the Ethereum platform as a public network or the Hyperledger platform as a limited access or allowed blockchain network. The amount of energy consumed by the blockchain is determined by the block's difficulty and the number of hashes generated per second (called the hash rate) [53]. The total energy consumption is also determined by the total number of nodes, which can range from a few tens to several hundreds depending on the type of election and actors involved, such as ministries, municipalities, civil society,

universities, and other important institutions. The assumption of the overall cost of all systems (energy consumption only for transaction mining) was calculated as follows:

$$energy\_cost\_per\_day = (no\_of\_nodes * node\_power\_consumption) * prices\_per\_kWh * 24\ h$$

A similar approach of calculation is given in [54], which defines the average energy for storing a data unit for one year. However, because electronic voting only takes a few days or weeks, disk size and energy usage may be less relevant.

4.2. Discussions

Current schemes and protocols do not meet the reliability criteria since they do not adequately meet the security, privacy, and anonymity characteristics. The BSJC and Anti-Quantum systems, for example, fail to meet voter expectations for accuracy, correctness, scalability, and variability. The OVN, DATE, BES, and BEA schemes, on the other hand, do not meet the requirements for correctness, integrity, and scalability. Our scheme manages to balance the qualities of privacy and anonymity by using two Blockchains (DKB and EVB). Integrity, precision, and correctness are also obtained, in addition to anonymity and privacy. This is accomplished by using a cryptographic nonce and a hash of the voter's private key, which allows the voter to verify their vote and ensure that their vote is correctly counted. Future researchers should consider the component of the vote separation from the voter and the part of anonymization that occurs in step six of the scheme, as presented in Figure 2.

5. Conclusions

Electronic voting systems have recently begun to find more applications in the real world due to their numerous advantages. The application of Blockchain technology can be more reliable than traditional ones because traditional or electronic voting systems are usually managed by a single authority that also has the risk of manipulation. Because Blockchain is distributed, not managed by a single authority and uses different consensus methods between parties, it can improve electronic voting systems. The immutability of Blockchain ensures data integrity through auditing, but privacy and anonymity are still among the main concerns. The proposed approach addresses these concerns with electronic voting, employing two independent Blockchains.

The usage of two different Blockchains recommended in our study, i.e., the Encrypted Votes Blockchain and the Distributed Key Blockchain, takes voter privacy and vote anonymity into account and provides solutions. Voter privacy and vote anonymity are achieved by storing votes and voter data in a separate Blockchain and using cryptographic methods and protocols. The nonce and hash of the voter's private key, as well as a comparison of the number of votes with the number of signatures of voters, ensure the integrity of the data. In addition, this approach makes it possible to verify if the vote has been counted correctly. The Distributed Key Blockchain also guarantees that no fraudulent voter has voted more than once, as this is verified before the voter casts their vote.

Author Contributions: Methodology, V.N., B.R., R.D. and I.S.; formal analyses, V.N, B.R., R.D. and I.S.; writing—original draft preparation, V.N.; writing—review and editing, B.R., R.D. and I.S.; visualization, V.N.; supervision, B.R. and I.S. project administration, B.R.; funding acquisition, B.R. and I.S. All authors have read and agreed to the published version of the manuscript.

Funding: Ministry of Education, Science, Technology and Innovation, Government of Kosovo with Decision no. 2-814 dt. 15.06.2021 has funded this research.

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

References

1. Solutions, I. Software that Powers Democracy Should Be Free. Available online: http://inno.vote/whitepaper/Inno.vote%20%E2%80%94%20Bringing%20Democracy%20to%20Elections.pdf (accessed on 28 January 2022).
2. Neziri, V. E-Voting: System Architecture—Kosovo Case. Master's Thesis, Faculty of Electrical and Computer Engineering, University of Prishtina, Prishtinë, Kosovo, September 2011.
3. Dhillon, A.; Kotsialou, G.; McBurney, P.; Riley, L. Introduction to Voting and the Blockchain: Some open questions for economists. EconPapers. In *CAGE Online Working Paper Series 416, Competitive Advantage in the Global Economy*; Örebro University: Örebro, Sweden, 2019.
4. Westin, A. Privacy And Freedom. *Wash. Lee Law Rev.* **1968**, *25*, 166.
5. Webb, P.D.; Eulau, H.; Gibbins, R. Election Political Science. Available online: https://www.britannica.com/topic/election-political-science (accessed on 7 September 2021).
6. Enguehard, C. Ethics and Electronic Voting. In Proceedings of the ETHICOMP—Liberty and Security in an Age of ICTs, Paris, France, 25–27 June 2014.
7. Wolf, P.; Nackerdien, R.; Tuccinardi, D. *Introducing Electronic Voting: Essential Considerations*; International Institute for Democracy and Electoral Assistance (International IDEA): Stockholm, Sweden, 2011.
8. e-Estonia. i-Voting—the Future of Elections? Available online: https://e-estonia.com/i-voting-the-future-of-elections/ (accessed on 28 January 2022).
9. International Institute for Democracy and Electora. If e-Voting is Currently Being Used, What Type(s) of Technology Used? Available online: https://www.idea.int/data-tools/question-view/743 (accessed on 17 May 2022).
10. Microsoft Corporate Blogs. Electronic Voting: What Europe Can Learn from Estonia. Available online: https://blogs.microsoft.com/eupolicy/2019/05/10/electronic-voting-estonia/ (accessed on 17 May 2022).
11. Gibson, P.; Krimmer, R.; Teague, V.; Pomares, J. A review of E-voting: The past, present and future. *Ann. Telecommun.* **2016**, *71*, 279–286. [CrossRef]
12. Jafar, U.; Ab Aziz, M.J.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors* **2021**, *21*, 5874. [CrossRef] [PubMed]
13. Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.-H. A critical review of blockchain and its current applications. In Proceedings of the International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113. [CrossRef]
14. Göbel, J.; Keeler, H.; Krzesinski, A.; Taylor, P. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Perform. Eval.* **2016**, *104*, 23–41. [CrossRef]
15. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–376. [CrossRef]
16. Wu, M.; Wang, K.; Cai, X.; Guo, S.; Guo, M.; Rong, C. A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. *IEEE Internet Things J.* **2019**, *6*, 8114–8154. [CrossRef]
17. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
18. Akram, S.V.; Malik, P.K.; Singh, R.; Anita, G.; Tanwar, S. Adoption of blockchain technology in various realms: Opportunities and challenges. *Secur. Priv.* **2020**, *3*, e109. [CrossRef]
19. Iansiti, M.; Lakhani, K. The Truth about Blockchain. Hardward Business Review. Available online: https://hbr.org/2017/01/the-truth-about-blockchain (accessed on 19 December 2021).
20. Anh Dinh, T.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.-L. BLOCKBENCH: A Framework for Analyzing Private Blockchains. In Proceedings of the ACM International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; pp. 1085–1100. [CrossRef]
21. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2019**, *105*, 475–491. [CrossRef]
22. Oliveira, M.; Carrara, G.; Fernandes, N.; Albuquerque, C.; Carrano, R.; Medeiros, D.; Mattos, D. Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload. In Proceedings of the 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 19–21 February 2019; pp. 180–187. [CrossRef]
23. Hussain, H.A.; Mansor, Z.; Shukur, Z. Comprehensive Survey and Research Directions on Blockchain IoT Access Control. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 239–244. [CrossRef]
24. Augoye, V.; Tomlinson, A. *Analysis of Electronic Voting Schemes in the Real World*; UK Academy for Information Systems: Oxford, UK, 2018.
25. Tarasov, P.; Tewari, H. The Future of E-Voting. *IADIS Int. J. Comput. Sci. Inf. Syst.* **2017**, *12*, 148–165.
26. Khan, K.; Arshad, J.; Khan, M. Secure Digital Voting System Based on Blockchain Technology. *Int. J. Electron. Gov. Res.* **2018**, *14*, 53–62. [CrossRef]
27. Neziri, V.; Dervishi, R.; Rexha, B. Survey on Using Blockchain Technologies in Electronic Voting Systems. In Proceedings of the 25th International Conference on Circuits, Systems, Communications and Computers (CSCC), Crete Island, Greece, 19–22 July 2021; pp. 61–65. [CrossRef]

28. Specter, M.; Koppel, J.; Weitzner, D. The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in U.S. federal elections. *USENIX Secur. Symp.* **2020**, *87*, 1535–1552.
29. Zambrano, R.; Young, A.; Verhulst, S. Seeking Ways to Prevent Electoral Fraud using Blockchain in Sierra Leone. Available online: https://blockchan.ge/blockchange-election-monitoring.pdf (accessed on 7 February 2022).
30. Buldas, A.; Kroonmaa, A.; Laanoja, R. Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. In *Secure IT Systems*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8208, pp. 313–320. [CrossRef]
31. Kshetri, N.; Voas, J. Blockchain-Enabled E-Voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
32. Polyakov, K. How Moscow Organized Voting on Blockchain in 202. (ICT Moscow). Available online: https://ict.moscow/en/news/how-moscow-organized-voting-on-blockchain-in-2020/ (accessed on 9 January 2022).
33. Huang, J.; He, D.; Obaidat, M.; Vijayakumar, P.; Luo, M.; Raymond Choo, K.-K. The Application of the Blockchain Technology in Voting Systems: A Review. *Assoc. Comput. Mach.* **2021**, *54*. [CrossRef]
34. Yu, T.; Yasuo, O. An anonymous distributed electronic voting system using Zerocoin. In Proceedings of the International Conference on Information Networking, Jeju Island, Korea, 13–16 January 2021; pp. 163–168. [CrossRef]
35. Yadav, A.S.; Urade, Y.V.; Thombare, A.U.; Patil, A.A. E-Voting using Blockchain Technology. *Int. J. Eng. Res. Technol.* **2020**, *9*, 375–380.
36. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices. *IEEE Trans. Ind. Inform.* **2021**. [CrossRef]
37. Atsushi, F.; Tatsuaki, O.; Kazuo, O. A practical secret voting scheme for large scale elections. In Proceedings of the International Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; Volume 718.
38. McCorry, P.; Shahandashti, S.; Hao, F. A smart contract for boardroom voting with maximum voter privacy. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017.
39. Wei-Jr, L.; Yung-chen, H.; Chih-Wen, H.; Ja-Ling, W. Date: A Decentralized, Anonymous, and Transparent E-voting System. In Proceedings of the IEEE International Conference on Hot Information-Centric Networking, Shenzhen, China, 15–17 August 2018; pp. 24–29. [CrossRef]
40. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* **2019**, *7*, 115304–115316. [CrossRef]
41. Fernández-Caramès, T.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
42. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
43. Yi, H. Securing e-voting based on blockchain in P2P network. *J Wirel. Com Netw.* **2019**, 137. [CrossRef]
44. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Future Gener. Comput. Syst.* **2020**, *105*, 13–26. [CrossRef]
45. Agora. Bringing Our Voting Systems into the 1st Century. Available online: https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf (accessed on 29 January 2022).
46. Horizon State. Available online: https://cryptorating.eu/whitepapers/Horizon-State/horizon_state_white_paper.pdf (accessed on 30 January 2022).
47. Voatz Inc. Voatz Mobile Voting Platform—An Overview. Available online: https://new.voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf (accessed on 3 February 2022).
48. Tarasov, P.; Tewari, H. Internet Voting Using Zcash. *IACR Cryptol. ePrint Arch.* **2017**, 585.
49. Xiaoqiang, S.; Richard, Y.F.; Peng, Z.; Zhiwei, S.; Weixin, X.; Xiang, P. A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network.* **2021**, *35*, 198–205. [CrossRef]
50. Schnorr, C. Efficient identification and signatures for smart cards. In *Advances in Cryptology—CRYPTO' 89, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, 10–13 April 1989*; Springer: Berlin/Heidelberg, Germany, 1990; pp. 239–252.
51. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In Proceedings of the IEEE International Conference on Systems, Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. [CrossRef]
52. IBM. IBM Storage: Storage Needs for Blockchain Technology. 2018. Available online: https://www.ibm.com/downloads/cas/LA8XBQGR#:~{}:text=So%20even%20at%20a%20modest,storage%20per%20year%20is%20required (accessed on 6 February 2022).
53. Saingre, D. *Understanding the Energy Consumption of Blockchain Technologies: A Focus on Smart*; Ecole nationale supérieure MinesTélécom Atlantique: Nantes, France, 2021.
54. Coroamă, V. *Blockchain Energy Consumption: An Exploratory Study*; Swiss Federal Office of Energy SFOE: Bern, Switzerland, 2021.