DOI: 10.24996/ijs.2022.63.3.38

ISSN: 0067-2904

A Review on E-Voting Based on Blockchain Models

Saba Abdul-Baqi Salman[*1],Sufyan Al-Janabi[2], Ali Makki Sagheer[3]

[1]*Department of Computer Science, Al-Iraqia, University, Baghdad, Iraq*
[2]*College of Computer Science and IT, University of Anbar, Ramadi, Iraq*
[3]*Al-Qalam University College ,Kirkuk, Iraq and affiliated to University of Anbar, Ramadi, Iraq*

Received: 19/6/2021 Accepted: 20/10/2021

Abstract

Developing a solid e-voting system that offers fairness and privacy for users is a challenging objective. This paper is trying to address whether blockchain can be used to build an efficient e-voting system, also, this research has specified four blockchain technologies with their features and limitations. Many papers have been reviewed in a study covered ten years from 2011 to 2020. As a result of the study, the blockchain platform can be a successful public ledger to implement an e-voting system. Four blockchain technologies have been noticed from this study. These are blockchain using smart contracts, blockchain relying on Zcash platform, blockchain programmed from scratch, and blockchain depending on digital signature. Each blockchain model has details about its features and limitations. Finally, this study suggests developing a blockchain platform that can avoid limitations of currently used blockchain platforms by ensuring authentication, privacy, security for remote e-voting processes.

Keywords: Blockchain, cryptography, e-voting, information security

مراجعة في التصويت الالكتروني المعتمد على نماذج سلاسل الكتل

صبا عبد الباقي سلمان*[1] سفيان الجنابي[2] علي مكي صغير[3]

[1]قسم علوم الحاسوب ، الجامعة العراقية ، بغداد ، العراق
[2]كلية علوم الحاسوب وتكنلوجيا المعلومات ، جامعة الأنبار ، الرمادي ، العراق
[3]كلية القلم الجامعة ، كركوك ، العراق وانتمائه إلى جامعة الأنبار ، الرمادي ، العراق

الخلاصة

ان تطوير نظام الكتروني يضمن العدالة و الخصوصية يعد مهمة لها تحديات تتعلق بالحماية و الخصوصية. هذ البحث يحاول تحديد فيما اذا كانت تقنية سلاسل الكتل مفيدة في مجال انظمة التصويت الالكتروني. وفي هذا الصدد حدد البحث اربعة انواع من التقنيات المستخدمة لبناء سلاسل الكتل مع مميزات ومحددات كل منها. تم دراسة العديد من الاوراق البحثية للفترة بين عامي 2011 و 2020 . وقد استخلصت هذه الدراسة الى ان تقنية سلاسل الكتل تقنية ناجحة كوسيلة خزن عامة الملكية لتنفيذ انظمة التصويت الالكتروني. وقد تم ملاحظة اربعه تقنيات وهي (سلاسل الكتب بالعقود الالكترونية، سلاسل الكتل باستخدام منصة Zcash ، سلاسل الكتل المطورة بشكل مستقل عن اي منصة جاهزة، سلاسل الكتل المعتمدة على التوقيع الالكتروني) مع تحديد مميزات و ثغرات كل تقنية. اخيرا ، توصي هذه الدراسه بتطوير نظام تصويت

*Email: Sabasalman2019@gmail.com

الكتروني بسلاسل الكتل يتجاوز الثغرات المذكورة في الانظمة الاربعة لضمان الامان ، الخصوصية و
الموثوقية للتصويت عن بعد.

1. Introduction

Voting usually an essential part of expressing one’s views in a democratic society. From counting raised hands and filling out paper ballots to casting votes electronically. Adopting electronic systems in voting events 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. Switzerland and Norway were soon to follow, implementing electronic systems for state-wide and council elections, respectively [1] . E-voting system security is a crucial issue in those systems. Many studies addressed the following issues that are related to security like data integrity, reliability, the privacy of the ballot, consequences of breakdown, uneducated voters, specialized IT skills, storage of equipment, security, effects of fraud, and cost [2] In recent years, blockchain-based voting has become a more important option for overcoming many of the security issues that may arise with e-voting. Blockchain-enabled voting systems have been suggested as the next generation of modern electronic voting systems due to the blockchain's immutable function. Blockchain technology enables governments to deploy intelligent, low-cost voting systems that incorporate sustainability information to ensure that all members have accurate information about ongoing properties. Even though blockchain is increasingly beginning to be used in improving the protection of electronic voting systems, several issues remain [3]. By building a systematic mapping to review documents about types of blockchain and how each type can be used to implement e-voting events, this paper can answer two questions. The first question is: whether the blockchain is suitable to implement e-voting applications?. Secondly, what are the blockchain types? What are their advantages and limitations in the domain of e-voting for both public and private blockchains? The purpose of this is to find the weak points in each of the blockchain technologies to put a future design.

2. Literature review

Early works that were depending on bitcoin schema like O.Spycher et al. (2012) who has proposed a model where the authorities can check if there is any fake ballot. Checking fake ballots can be satisfied further by exploiting the blockchain schema of digital currency. This system is custom programmed from scratch and is not relying on smart contracts or bitcoin. So, this solution was to prevent attacking the chain if it was small [4].

Also in 2015, Czepluch discussed the applications of the blockchain and pointed to a possibility to use the blockchain for e-voting systems. Czepluch used a smart contract that may cause slowness and difficulty to update ledgers [5]. Z. Zhao et al. (2015) proposed a design for voting depends on bitcoin that preserves privacy, verifiability, and irrevocability. Zhao proposed schema was similar to z-cash that ensures vote validity but may be attacked from the end-user device, accordingly, Zhao improve bitcoin e-voting by using third-party vote commitment to check the voter authenticity [6].

In 2016 a system suggested by Takabatake Y. depends on Ziroin to ensure anonymity for an e-voting system. bitcoin is a money transfer system and can be attacked from user devices, so, this work used Zircon as a cover for the bitcoin ledger to increase privacy [7].

Ahmed ben-ayad (2017) has proposed an e-voting system formed by manipulating custom programmed blockchain. The system is also open-source, reliable, and anonymous design. Unfortunately, this system can be attacked by hackers as its small blockchain systems. But it can be improved by adding a new tier of encryption not like the bitcoin e-voting system that can be attacked from end-user software [8]. Moura et al. (2017) have explored the possibility of using a blockchain framework to ensure transparency, confidentiality for a nationwide scale election. Moura also discussed societal issues and analyze them [9].

In addition, Bartolucci et al. (2017) introduced secrete sharing voting based on a blockchain environment. This mode makes use of Shamir's secret sharing to send the vote submission and determine the winner. To de-link voters from their submissions, the model used a circle, shuffle technology, which is similar to ring encryption. delinking ledgers from voters is a solution to the weakness of anonymity in the bitcoin schema [10].

Koc et al. (2017) implemented an e-voting system based on smart contracts of Ethereum framework wallets. Voters would cast their ballots using their Ethereum wallets. The consensus of all Ethereum nodes is used to encrypt these transactions. This consensus security relies on the well-known ring signature and proof-of-work mechanisms used in mining may improve the security but still smart contracts schema suffering from slowness and authentication that have to be ensured by biometric features [11]. Also, Casado-vard et al. (2018) introduced a model in which a distributed ledger is used to broadcast a vote to a poll station through a Smart Contract. After that, the polling station sends a smart contract to each voter and registers the vote in a chain. Smart contracts are used to prevent malicious activities. The poll station also applied a multi-signature to each vote[12]. Y. Wu (2017) introduced an e-voting system based on ring signature and a bitcoin blockchain mechanism. For securing the voting process, a voter has to gain a public key from all other voters. These keys will be used to create a signature that consists of the voter's private key and the previous voter's public key. Voting authorities collect all transactions and verify their signatures. This mechanism may secure user identity when cracking end-user devices [13].

Friorik et al. (2018) suggested a blockchain e-voting system that uses voter credentials like user name and ID card to verify the voter from government identification service and establish a smart contract with a voter to verify the vote. The model uses a district node to secure the contracts from unauthorized users. This division of the system makes it faster than the traditional smart contract e-voting systems [14]. Furthermore, M. Al-Rawy et al. (2018) introduced a blockchain e-voting system that is relied on bitcoin ledgers. RSA public-private key is used to secure the information for each block or ballot. Mohammed's authentication schema relying on the usage of electronic card identification without biometric identification during the remote voting process [15]

Wang et al. (2018) proposed e-voting based on Ethereum smart contracts. This system is secured by using El-Gamal cryptography and ring signature. The one-time ring signature ensures the anonymity of a voter in the distributed ledger. This model improved the public key establishing by deriving it from the recipient address, so it is not like a bitcoin address, this address is used for each transaction [16]. Additionally, Akbari et al. (2018) used lived biometric of a person to ensure authentication and high reliability. The issue of scalability was tackled using parallel processing of multiple blockchains. Multichain systems enhance Ethereum speed and scalability. This system used fingerprints to ensure voter authentication [17]. Mubashir et al. (2018) proposed an e-voting schema with a multi-chain platform. The system achieved security using Ethereum blockchain wallets [18].

Latif et al. (2019) introduced a blockchain-based decentralized electronic voting system for elections on a large scale. This work focused on consensus and proof of work by choosing a suitable hash for a block; the proposed system uses a homomorphic stream cipher to encrypt the ballot in addition to the hash encryption. The homomorphic encryption targeted both increasing security and reducing the amount of data to be sent to the server. This system increases the speed of mining by selecting powerful nodes, this solution increases the speed of smart contract interaction also [19].

Tso et al. (2019) introduced an e-voting system and bidding system that are based on blockchain and smart contracts. Oblivious transfer and homomorphic cryptographic techniques are used to improve privacy protection. The smart contract is interactive with the system, allowing voters to check and count their ballots during the billing stage. This system uses Shamir's secrete sharing system to improve smart contracts and bitcoin schema [20].

Now, the work of Li et al (2019) that proposed a decentralized internet of things IOT points by dividing the systems into sub-blockchains to be managed and secured efficiently. This system is programmed from scratch not depending on other applications like smart contracts and it's used for mobile phone voting. The proposed model used El-Gamal encryption to encrypt the ballots with Diffie-Helman to distribute the keys. The system used a simple registration form to gain the keys from the voter [21].

In 2019, Yi et al. proposed techniques for leveraging the blockchain in a peer-to-peer network to enhance e-voting security. This work enhances the custom-programmed blockchain systems in three ways. First, to prevent vote forgery, the first step was to create a synchronized model of voting records based on distributed ledger technology (DLT). Second, to provide authentication and non-repudiation, a user credential model based on elliptic curve cryptography (ECC) was developed. Third, create a withdrawal model that allows voters to change their minds about their vote before a deadline[22].

In 2020, Kaspersky company introduced a white paper for a voting system from Kaspersky company focused on security features like reliability and ease of use, transparent, secure, anonymous voting, and flexible to use both in desktop and mobile. This system consists of two stages, the voting stage that encrypts ballots using a public key elliptic curve and the counting stage that is used to verify the counting of ballots [23].

It is noticed that some researchers like Bartolucci and others try to speed up the interactions, scalability of the smart contract e-voting blockchain by techniques like De-linking, multichain, and regional blockchains. Others researchers like Li et al (2019) and Yi et al (2019) used blockchain from scratch to control its privacy using a public key and key exchange mechanisms. But, these schemas are weak if the blockchain is small. Tabatake Y. used Zircon as a layer above the bitcoin environment to increase the anonymity of the blockchain user from his vote. For the blockchain that relies on the digital signature Y. Wu (2017) improved the signature to prevent anyone from claiming the signature ownership. As result, this literature review addresses four blockchain types (blockchain using smart contracts, blockchain relying on Zcash platform, blockchain programmed from scratch, and blockchain depending on digital signature) and their issues.

3. BLOCKCHAIN CONCEPTS

Blockchain Technology is so-called because it is a chain of blocks. These blocks are interconnected such that each one has a copy of the distributed ledger that saves the history of all transactions in that blockchain. After a process known as mining, which involves granting a new block, data is added to the blockchain. For additional integrity, each block contains the hash of the previous block, forming a chain of blocks. The genesis block is the first block in the chain. As a result, it takes the form of a linked list. Data can only be appended, not removed, or tampered with, since the blockchain uses several ledgers to store data. As a result, the blockchain is unchangeable. The blockchain system can be either public or private. Public blockchain implying that everyone can read or write data to it (granted). While in the private one, only a few select individuals have access to read or write data.,. This is depicted in Figure (1).

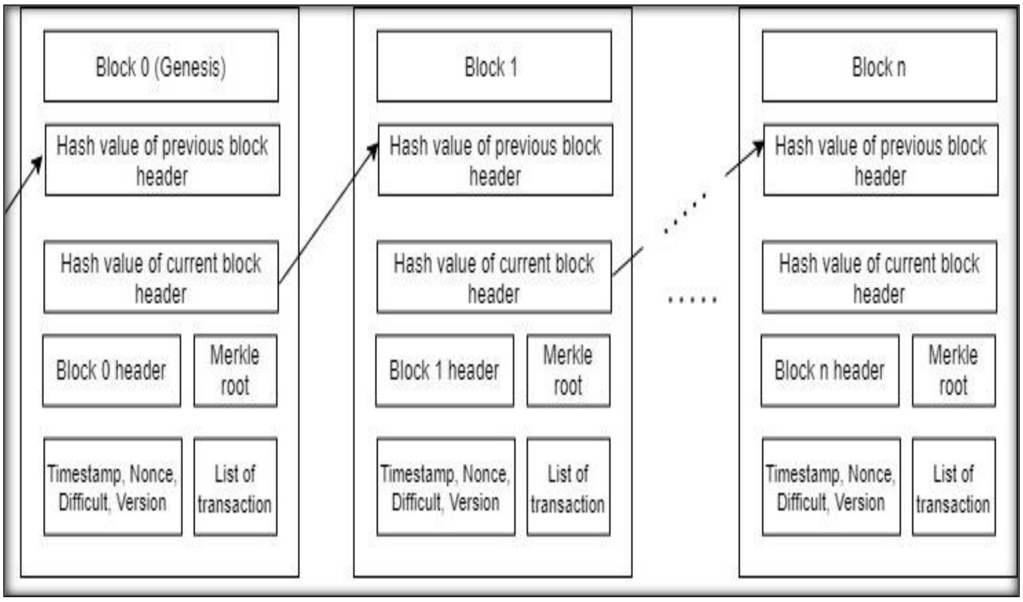
Block 0 (Genesis)
Hash value of previous block header
Hash value of current block header
Block 0 header
Merkle root
Timestamp, Nonce, Difficult, Version
List of transaction
Block 1
Hash value of previous block header
Hash value of current block header
Block 1 header
Merkle root
Timestamp, Nonce, Difficult, Version
List of transaction
Block n
Hash value of previous block header
Hash value of current block header
Block n header
Merkle root
Timestamp, Nonce, Difficult, Version
List of transaction

Figure 1-General Framework of Blockchain.

A digital signature is used to prevent non-repudiation and ensure a node's activity in a blockchain. Once the transaction is validated, the hash function is operated to add a block to the blockchain in a tamper-proof way. A hash is a mathematical feature that can be used to transform a numerical input value into another value that can be used to verify data integrity later[23].

4. E-VOTING SYSTEMS

Electronic voting is a modern type of online voting system that uses cryptography. Voters may cast their ballots from the comfort of their own homes using computers or mobile devices. The final voting results can be secretly counted by the central server automatically[24]. These systems bind the entire voting process, greatly improving the efficiency of arranging, gathering ballots, counting the results of ballots, and maintaining the fairness and transparency of the voting process as compared to conventional voting. In general, a secure e-electronic voting scheme should fulfill several conditions, including Voter privacy, which requires that the voter's choices remain hidden; no one can divulge the voter's choices within the ballot. Second, personal verifiability requires voters to be able to verify that their votes were correctly counted. Third, qualification ensures that only eligible voters are allowed to vote in the election. Fourth, the Judiciary: Nothing can impact a vote's outcome. It is prohibited to reveal the voting results or to increase the number of voters participating in the voting process. Otherwise, it would have a negative impact on voting outcomes [25]. Sixth, Individuality: Each elector is only allowed one vote. There are many strong aspects in e-voting systems like their cost cheaper than paper traditional voting systems, and enable elastic elections in specific duration and conditions. While the weakness in e-voting systems is its implementation may be high in cost. Many people may be don’t accept the thought as there is a low perception of confidence. And, the internal procedure may be bot understandable because it should be straightforward. Other technical drawbacks like the scalability of the database may be an issue. Unfortunately, some unsuccessful attempts give a negative opinion about those systems [26].

5. BLOCKCHAIN-BASED E-VOTING

The e-voting systems take the benefits of blockchain in saving ballots, secure the ballots, and ensure voters' privacy and anonymity. These systems are relying on hashed blocks that can save the ballots with security. Each block has the hash of the previous block. If an attacker tries to change the block, then he has to change the previous block's hash till reaching the first block in the chain; this job may require powerful processing machines and may be impossible in many cases. Another benefit of blockchain systems is using mining to search for a suitable hash code number that is accepted for a blockchain in a particular region[26].

The following sections are discussing the four main types of blockchains that have been used to implement e-voting systems in previous researches [27] The discussion of these four types will obtain their advantages and limits :

5.1 Voting Based on Smart Contracts

The general process of smart contract e-voting is outlined in Figure (2). The users must obtain an official Ethereum wallet and use the settings menu to change the test network's connection. The process is described as follows:

1. Smart contract is implemented on the Ethereum blockchain, saving the owner of the contract as "chairman". Then define the structures of voters and candidates and the functions for voting, giving the right to vote and counting votes.
2. Chairman establishes the election event and gives the grant for voting to individuals by using 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 checking if the voters have been voted, and if not, distributes a vote to their favoured candidate. The 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, this type should only be used for small-scale polls and elections that are not critical [10][27][28].

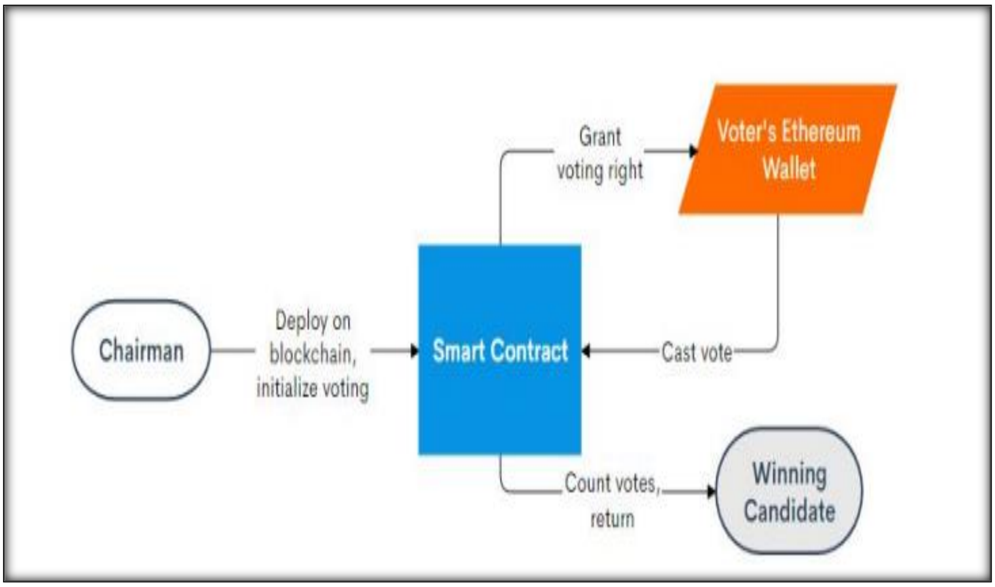

Figure 2-Smart Contract E-Voting System Chart[27].

5.2 Voting Based on the Zcash Platform

Zcash is a cryptocurrency based on the Zerocoin protocol. This currency was designed to hide the transactions on the Bitcoin blockchain. Takabatake et al. 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.

Another type of system is based on Zcash, which uses quadratic voting, making the voters pay 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 (3) and described as follows [29].

1. The Users have to register by using the registration page provided by the election authority. When a user is approved and recorded, an email with a unique link is sent to the voter. The link in question provides the user with a unique election ballot. 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 getting a ZEC token, chooses a specific candidate and goes through a legal agreement before the transaction begins. 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 voting token.

3. Once voting is concluded, the candidates save all their ZEC vote tokens received during the voting process to a wallet owned by the voting system. The system wallet tracks its number of tokens before and after each transaction to calculate the candidates' number of votes. 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.

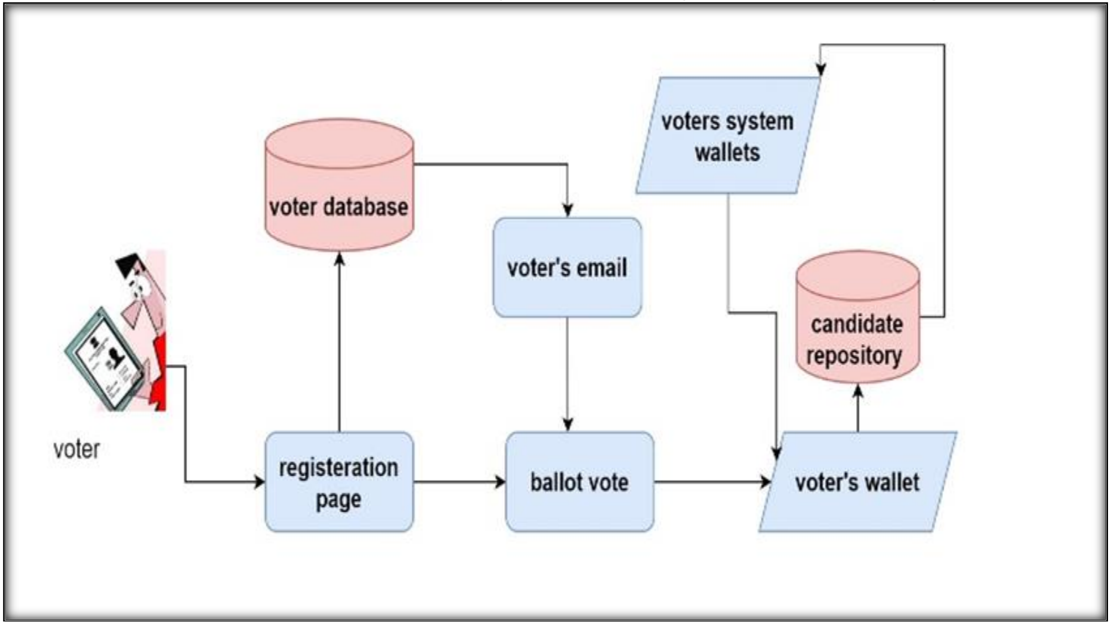

Figure 3-Zcach E-Voting System Chart.

5.3 Voting with a Custom Blockchain

Building a blockchain from scratch is also possible. Ayed has proposed a blockchain for each candidate. The voters who are voted a specific candidate are saved in a particular 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 (4). Simplified process of voting with a custom blockchain [8] [30],

1. User logs in to the voting system using their credentials. Before that, the user must be registered in the databases of the authorities and got a confirmation about his registration validity. If the system can match the provided credentials with a valid voter, it grants the user a right to vote.

2. The user is taken to the ballot page 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 initialized, the system creates a new block 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. A correct blockchain is chosen depending on 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 the following figure:

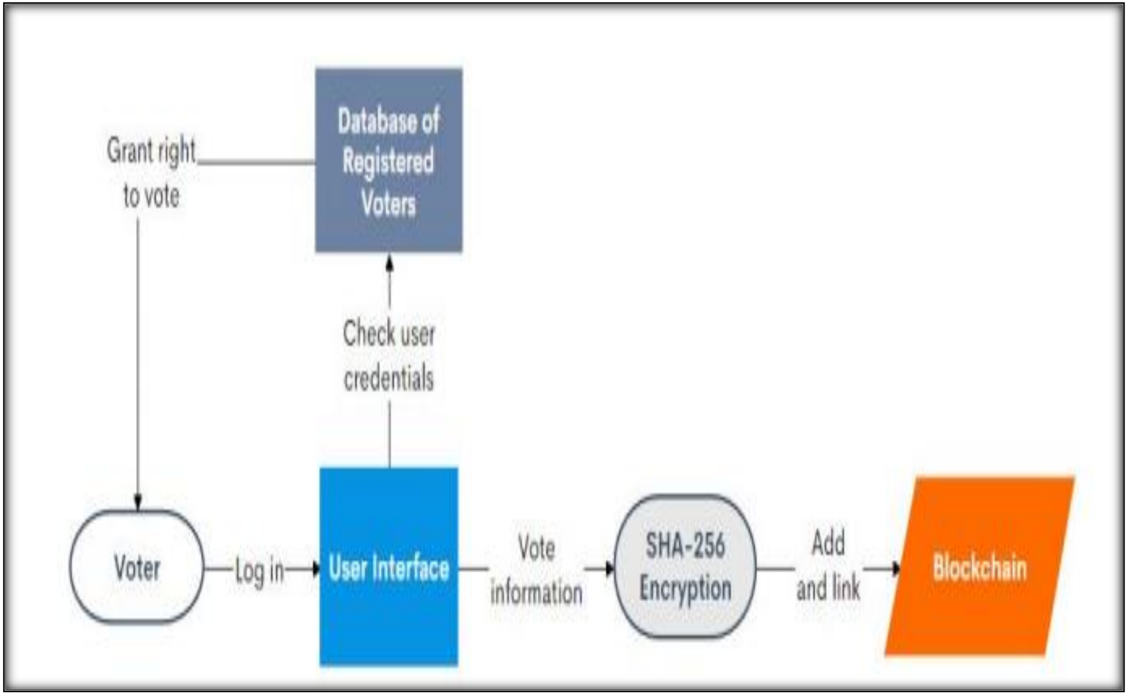

Figure 4-Standard Blockchain E-Voting System Chart **Error! Reference source not found.**.

5.4 Voting Using a Cryptographic Signature

To provide anonymity similarly to a voter, it's far feasible to comprise cryptographic signatures, together with ring signatures or blind signatures, inside the balloting scheme. Wu proposes this unique voting machine primarily based on the Bitcoin community and ring signatures. It consists of three essential entities: a registration authority (RA), election authority (EA), and a Bitcoin cope with a pool that includes randomly generated Bitcoin addresses. [31], [32] and [33]. [33]

1. For the preparation step duration, the election authority (EA) sets up the mission and saves its Bitcoin wallet address into the device. Candidates authenticate themselves to the registration authority (RA) and are each given a unique identity. Addresses for applicants also are initialized the usage of the Bitcoin address pool.

2. Polling stations run by using the RA are located in residential areas. Customers are registered to vote when they've authenticated themselves to the RA with a passport or different identification approach. Once registered, a public/private key pair is generated for the voter. The voter needs to then proportion the general public key with the device and preserve it onto the private key. Registration is closed at the set closing date and the listing of the electorate's public keys is saved to the machine.

3. All through the balloting phase, the machine sends all customers the listing of public keys and candidate IDs and a fixed quantity of Bitcoin for vote casting. Voters use their key, selected candidate's identity, and the public keys of all voters as additives to generate a unique ring signature. This ring signature is hashed using SHA-256, which is then brought to the blockchain by sending the fixed amount of Bitcoin, hashed signature, and candidate identification to EA's Bitcoin pockets cope with. Each hashed and not hashed version of the ring signature is also saved to the machine. The system of generating ring signatures is defined in Figure (5).

4. Inside the tallying step, the system returns all sets of hashed and not hashed ring signatures generated through the users. Each transaction's ring signature validity is verified through the system. Each candidate's vote count number is increased with the aid of one for every established transaction that includes their identity. If a couple of transactions are made from the identical cope with, most effective the first one is counted.

5. As EA's pockets transactions and the list of all public keys are publicly readable, every voter can confirm their vote using the candidate identification, list of public keys, and the hoop signature.

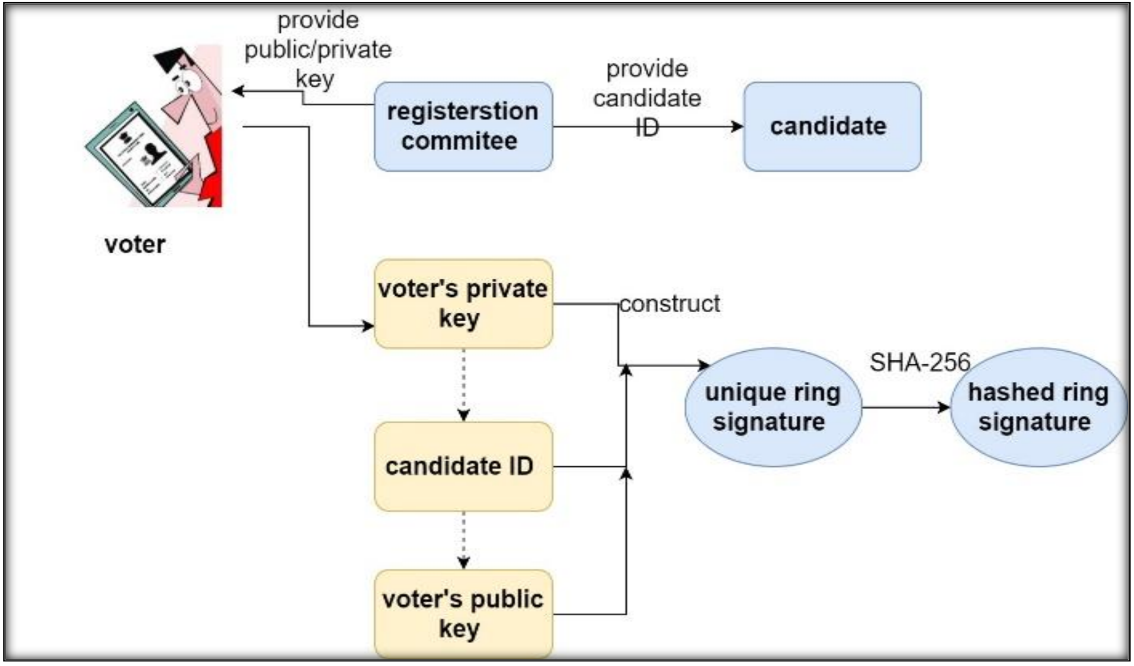

Figure 5-Cryptographic Signature E-voting Chart [27].

6. RESULTS AND DISCUSSION

Let's now begin to review and discuss each type of blockchain technology, its advantages, and disadvantages, in both public and private blockchains and for both small and large elections and as shown in Table (2), and try to select the best option as follows:

Smart Contracts are computer programs that can retain state, interact with bitcoin in a decentralized manner, and receive user input and are operated through blockchain transactions. Solidity is a programming language that combines C++ and JavaScript. Smart Contracts are developed in this language. Smart Contracts are monitored by Ethereum peers at regular intervals, and they must be approved by at least two separate clients to be launched. Contract functions can then be carried out, and contracts can be distributed to various applicants. . It's difficult to amend an Ethereum smart contract once it's been built. The execution is a little sluggish. Accessing the data necessitates the use of external programs.[27] [34],[35].

Zcash Platform is a decentralized blockchain payment system that attempts to keep transactions anonymous. The proof-of-work method, in which Zcash relies on zero-knowledge proofs, is one of the most significant differences between Zcash and Bitcoin. Zcash features two sorts of addresses, unlike Bitcoin, which only has one. This allows it to handle both anonymous and transparent transactions. These addresses are z-address and t-address, where z-address maintains anonymity in transactions while t-address is structured similarly to Bitcoin addresses and enables transparent transactions. The conversion of transparent value into a shielded value and vice versa is ensured by transactions between separate addresses. The public is unable to **see** the specifics of protected values. The drawback of using z-cash is the possibility to attach the user's wallet to the end-user device itself [36].

A Cryptographic Signature process used to authenticate the quality and integrity of digital data is known as a digital signature. The method essentially entails hashing a message with the private key of the signer. The recipient of the message can then use the signer's public key to verify that the signature is valid. A digital signature certificate is an electronic identifying document that enables a person, company, computer, or organization to securely transmit information over the internet utilizing the Public Key Infrastructure (PKI). A Certificate Authority issues a digital certificate, often known as a Public Key certificate. It requires the same documentation as a passport or driver's license. A digital certificate includes the holder's name, a serial number, a certificate expiration date, and a copy of the holder's public key. If a digital certificate is signed by a trustworthy Certificate Authority's root certificate, it is only genuine and valid. The weakness of digital certificates is that it is possible to claim that votes have been tampered with if the authority is corrupted. This attack can be done using generating an extra signature [37].

The Custom-Programmed Blockchain Technology employed is similar to the Bitcoin system's blockchain technology in that it focuses on database recording. The nodes engaged in the Blockchain that is used by Bitcoin are completely random and are not counted. However, blockchain permission is used in this e-voting system for nodes to be made the opposite of the Bitcoin system, and the Node in question is a place of a general election because the place of general election must be registered before the start of implementation, and the amount and identity must be clear. This strategy seeks to safeguard data integrity from alterations and manipulations that should not occur in the first place during the election process. The disadvantage of this type is that if the blockchain is small, the custom blockchain can be simply attacked and tampered with because it is made up of little blocks[21][38]. These observations can be summarized in Table No. (1) below:

Table 1- E-voting System Blockchain Methods Advantage and Restrictions

Method	Blockchain type	Voting scale	Advantages	Restrictions	Papers
Custom-programmed blockchain	Private and public	Small to large elections	Block can be created easily and fast. This type can use for small and large elections as it can be set up easily.	Private small custom blockchain can be attacked and tampered with easily because it consists of small blocks.	[8],[20],[29],[39]
Smart contract	Public	Small scale	Smart contracts are saved permanently, no one can remove, manipulate them. Ethereum also has the ability to self-tallying. In the Ethereum system, all transactions can be executed in an asynchronous manner.	Difficult to update Ethereum smart contract after it's established. There is slowness in execution. Accessing the data require executing an external code.	[10],[27],[33],[40]
	Private	Small and large elections	In private networks the difficulty of establishing a block is reduced, the block can be created in less time.	Difficult to be set up because the network has to include a private Ethereum testing network.	[24], [40]

Zcash	Just public	Small elections	Zcash provides hiding the voter's identities. Zcash protocol ensures vote validity and no one can vote twice.	The voting machine may be attacked because the targeting cash platform is the end-user device.	[28],[29]
		Large elections	This paradigm uses quadratic voting that grants voters to pay to cast additional votes for their desired candidates. So, the result is tuned to the intensity of voters preferences.		[36]
Cryptographic Signature	Public and private	Small to large elections and polls	It is difficult for the voter to voter to show how he voted, so it has a good privacy.	It is possible to claim that votes have been tampered with if the authority is corrupted. This attack can be done using generating an extra signature.	[30],[31],[32],[37],[41],[42],[43]

The previous works were standardized concerning security standards: Security, Privacy, Authentication and finally Speed, and the conclusion was that the programmed type Custom Blockchain is the best because it can be programmed and is open source, and authentication can be added to it and its structure is improved by adding other layers of encryption.

While other types of e-voting systems that bases on the Zcash Platform. Privacy is threatened in the event of hacking the voter's device and knowing the person of this voter. Because the end device contains the wallet of the voter, so this may cause them to reveal his personality.

As for Smart Contracts, it suffers from some slowness, and it is possible to know the identity of the voter in case the wallet is hacked. The Cryptographic Signature relies on electronic certificates from a third source. If this source is hacked or damaged, the system will be threatened in terms of privacy. All previous systems have achieved security. After all, they provide a good degree of encryption during the transmission of voting data, because all of the mentioned paradigms depend on the hash system and private key signatures, so all of the models acceptably provide security and encryption.

None of the systems directly achieved authentication like biometric features on the electronic voting process such as fingerprint, eye, and face. Some of the proposed systems have adopted the electronic identification cards by using mobile SIM Cart, so the programmed Custom Blockchain system is the best in terms of the possibility of adding biometric features, adding a proof of work, and improving the encryption structure in it, so it will be the best choice for conducting the study later. These observations can be summarized in Table No. (2) below:

Table-2 Comparison between E-voting Blockchain Paradigms in Terms of Security

	Security	**Privacy**	**Authentication**	**Speed**
Smart Contract	Yes	No	No	No
Zcash Platform	Yes	No	No	No
Cryptographic Signature	Yes	No	No	Yes
Custom Blockchain	Yes	Yes	Yes	Yes

Finally, studying all papers yield an opinion to answer the first question that was mentioned in the introduction section of whether blockchain is suitable to implement e-voting systems? and the answer is blockchain is a useful public ledger that can be used successfully in developing e-voting systems and save voting ballots in it. the second question of blockchain techniques and their advantages, limitations are answered and discussed within the previous discussion.

7. CONCLUSION

In democratic countries the voting process playing a crucial role in specifying population choices. E-voting systems improving elections by casting votes electronically to ensure honest elections. E-voting systems are rich in issues that relate to privacy and security in general. Nowadays, blockchain voting systems have become a good choice to fulfill an e-voting event. Four types of blockchain systems have been noticed during doing the review. First, the e-voting system by the smart contract. This type is implemented using etherum wallets. This wallet is used to identify the voter. Smart contact save the information of each voter permanently, but it is difficult to update and slow in interaction with the voting system and scalability. Second, e-voting system using Zcash platform. Zcash cryptocurrency platform is used as a layer to hide transactions of bitcoin. zcash system can be attacked by installing malicious software on the end-user device. Third, implementing e-voting using custom blockchain. These e-voting systems depending on build blockchain from scratch without using any pre-built platform. This is a good choice and the developer can control design and authentication, security tools. Fourth, an e-voting system using a cryptographic signature. This type of blockchain system uses bitcoin wallets' addresses and ring signatures. This system hashed a key generated from the voter's private key, candidate ID, the public key of all voters. But, in this type, it is possible to exploit a signature. As a result, there are many blockchain paradigms to implement e-voting with security and authentication issues. Finally, this research suggests building a new platform that can tackle issues of security, privacy mentioned in the obvious four platforms.

REFERENCES

[1] Ü. Madise and T. Martens, “E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world,” 2006.

[2] J. Gerlach and U. Gasser, “Three Case Studies from Switzerland: E-Voting,” p. 17.

[3] K. M. Khan, J. Arshad, and M. M. Khan, “Investigating performance constraints for blockchain based secure e-voting system,” *Future Generation Computer Systems*, vol. 105, pp. 13–26, 2020.

[4] O. Spycher, R. Koenig, R. Haenni, and M. Schläpfer, “A new approach towards coercion-resistant remote e-voting in linear time,” in *International Conference on Financial Cryptography and Data Security*, 2011, pp. 182–189.

[5] J. S. Czepluch, N. Z. Lollike, and S. O. Malone, “The use of block chain technology in different application domains,” *The IT University of Copenhagen, Copenhagen*, 2015.

[6] Z. Zhao and T.-H. H. Chan, “How to vote privately using bitcoin,” in *International Conference on Information and Communications Security*, 2015, pp. 82–96.

[7] Y. Takabatake, D. Kotani, and Y. Okabe, “An anonymous distributed electronic voting system using Zerocoin,” *IEICE Technical Report*, vol. 116, no. 282, pp. 127–131, 2016.

[8] A. B. Ayed, “A conceptual secure blockchain-based electronic voting system,” *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.

[9] T. Moura and A. Gomes, “Blockchain voting and its effects on election transparency and voter confidence,” in *Proceedings of the 18th annual international conference on digital government research*, 2017, pp. 574–575.

[10] S. Bartolucci, P. Bernat, and D. Joseph, “SHARVOT: secret SHARe-based VOTing on the blockchain,” in *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain*, 2018, pp. 30–34.

[11] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, “Towards secure e-voting using ethereum blockchain,” in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, pp. 1–7.

[12] R. Casado-Vara and J. C. Rodríguez, “Blockchain for democratic voting: How blockchain could cast of voter fraud,” *Oriental journal of computer science and technology*, vol. 11, no. 03, p. 2019, 2018.

[13] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson, “Blockchain-based e-voting system,” in *2018 IEEE 11th international conference on cloud computing (CLOUD)*, 2018, pp. 983–986.

[14] M. Al-Rawy and A. Elci, “A design for blockchain-based digital voting system,” in *The 2018 International Conference on Digital Science*, 2018, pp. 397–407.

[15] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, “Large-scale election based on blockchain,” *Procedia Computer Science*, vol. 129, pp. 234–237, 2018.

[16] E. Akbari, Q. Wu, W. Zhao, H. R. Arabnia, and M. Q. Yang, “From blockchain to internet-based voting,” in *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2017, pp. 218–221.

[17] K. M. Khan, J. Arshad, and M. M. Khan, “Secure digital voting system based on blockchain technology,” *International Journal of Electronic Government Research (IJEGR)*, vol. 14, no. 1, pp. 53–62, 2018.

[18] S. Latif and T. Anees, “Blockchain based Decentralized Electronic Voting System: A Step towards Transparent Elections,” *IJCSNS*, vol. 19, no. 12, p. 165, 2019.

[19] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, “Distributed E-voting and E-bidding systems based on smart contract,” *Electronics*, vol. 8, no. 4, p. 422, 2019.

[20] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, and M. Guizani, “A blockchain-based self-tallying voting scheme in decentralized IoT,” *arXiv preprint arXiv:1902.03710*, 2019.

[21] H. Yi, “Securing e-voting based on blockchain in P2P network,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–9, 2019.

[22] A. Korunov, A. Sazonov, and P. Murzin, “Polys Online Voting System: Lessons Learned from Utilizing Blockchain Technology,” *E-Vote-ID 2021*, p. 393, 2021.

[23] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, “Peace engineering: The contribution of blockchain systems to the e-voting process,” *Technological Forecasting and Social Change*, vol. 162, p. 120397, 2021.

[24] M. Dengo and F. P. Milani, “Blockchain Voting : A Systematic Literature Review | Semantic Scholar,” Bachelor’s Thesis, UNIVERSITY OF TARTU, Estonia, 2020. Accessed: Mar. 25, 2022. [Online]. Available: https://www.semanticscholar.org/paper/Blockchain-Voting-%3A-A-Systematic-Literature-Review-Dengo-Milani/8732933cbbe5db165a0de9ee3f97b7fd377c5d16

[25] U. C. Çabuk, E. Adiguzel, and E. Karaarslan, “A survey on feasibility and suitability of blockchain techniques for the e-voting systems,” *arXiv preprint arXiv:2002.07175*, 2020.

[26] “Blockchain Voting : A Systematic Literature Review | Semantic Scholar.” https://www.semanticscholar.org/paper/Blockchain-Voting-%3A-A-Systematic-Literature-Review-Dengo-Milani/8732933cbbe5db165a0de9ee3f97b7fd377c5d16 (accessed Mar. 24, 2022).

[27] X. Yang, X. Yi, S. Nepal, and F. Han, “Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain,” in *International Conference on Web Information Systems Engineering*, 2018, pp. 18–35.

[28] P. Tarasov and H. Tewari, “Internet voting using zcash,” *Cryptology ePrint Archive*, 2017.

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

[30] T. P. Abayomi-Zannu, I. A. Odun-Ayo, and T. F. Barka, “A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication,” in *Journal of Physics: Conference Series*, 2019, vol. 1378, no. 3, p. 032104.

[31] Y. Wu, “An e-voting system based on blockchain and ring signature,” *Master. University of Birmingham*, 2017.

[32] S. H. Shaheen, M. Yousaf, and M. Jalil, “Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain,” in *2017 13th International Conference on Emerging Technologies (ICET)*, 2017, pp. 1–6.

[33] N. Goel, C. van Schreven, A. Filos-Ratsikas, and B. Faltings, “Infochain: A Decentralized, Trustless and Transparent Oracle on Blockchain,” *arXiv:1908.10258 [cs]*, Jul. 2020, Accessed: Mar. 25, 2022. [Online]. Available: http://arxiv.org/abs/1908.10258

[34] F. Meeser, “[PDF] Decentralized , Transparent , Trustless Voting on the Ethereum Blockchain Fernando | Semantic Scholar,” 2017, Accessed: Mar. 25, 2022. [Online]. Available: https://www.semanticscholar.org/paper/Decentralized-%2C-Transparent-%2C-Trustless-Voting-on-Meeser/d667a4f6e63aa385e6c6be769c97951fdad71fe8

[35] J. Lopes, J. L. Pereira, and J. Varajão, *Blockchain based e-voting system: A proposal*. Association for Information Systems (AIS), 2019.

[36] C. C. Z. Wei and C. C. Wen, “Blockchain-based electronic voting protocol,” *JOIV: International Journal on Informatics Visualization*, vol. 2, no. 4–2, pp. 336–341, 2018.

[37] M. K. K. Sharma, M. Patole, and V. M. Lomte, “Securing Voting System using Blockchain and Fingerprint Verification,” 2019.

[38] S. Park and R. L. Rivest, “Towards secure quadratic voting,” *Public Choice*, vol. 172, no. 1–2, pp. 151–175, Jul. 2017, doi: 10.1007/s11127-017-0407-2.

[39] S. Park and R. L. Rivest, “Towards secure quadratic voting,” *Public Choice*, vol. 172, no. 1, pp. 151–175, 2017.

[40] J. Lopes, J. L. Pereira, and J. Varajão, “Blockchain based E-voting system: A proposal,” 2019. . Available: http://repositorium.sdum.uminho.pt/

[41] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, “An anti-quantum e-voting protocol in blockchain with audit function,” *IEEE Access*, vol. 7, pp. 115304–115316, 2019.

[42] K. E. Abdullah and N. H. M. Ali, “A Secure Enhancement for Encoding/Decoding data using Elliptic Curve Cryptography,” *Iraqi Journal of Science*, pp. 189–198, 2018.

[43] H. Abdulsalam and A. A. Fahad, “Evaluation of Two Thresholds Two Divisor Chunking Algorithm Using Rabin Finger print, Adler, and SHA1 Hashing Algorithms,” *Iraqi Journal of Science*, pp. 2438–2446, 2017.