IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 21, 2019, accepted January 22, 2019, date of publication February 25, 2019, date of current version March 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2895670

Trustworthy Electronic Voting Using Adjusted Blockchain Technology

BASIT SHAHZAD[1] **AND JON CROWCROFT**[2]
[1]Department of Engineering, National University of Modern Languages, Islamabad 44000, Pakistan
[2]Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, U.K.

Corresponding author: Basit Shahzad (basit.shahzad@gmail.com)

ABSTRACT The electronic voting has emerged over time as a replacement to the paper-based voting to reduce the redundancies and inconsistencies. The historical perspective presented in the last two decades suggests that it has not been so successful due to the security and privacy flaws observed over time. This paper suggests a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method. This paper claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process.

INDEX TERMS Electronic voting, blockchain voting, i-voting, e-voting, blockchain Pakistan, future voting.

I. INTRODUCTION

Will of the people is a well-respected phenomenon for representation of opinion in formation of electoral bodies. These electoral bodies vary from the college unions to the parliaments. Over the years, 'vote' has emerged as a tool for representing the will of the people when a selection is to be made among the available choices. The voting [1] tool has helped improving the trust of people over the selection they make by a vote of majority. This has certainly helped in democratization of the voting process and the value of voting system to elect the parliaments and governments. In 2018, there are 167 counties out of little over 200 who have some kind of democracy; full, flawed, or hybrid etc [2]. Since the trust of people is increasing in democracies it is important that they don't lose their trust on vote and voting system. By virtue of the emerging trust on the democratic institutions, the voting system emerged as a platform to help people to elect their representatives, who consequently form the governments [3]–[6]. The power of representation empowers the people with a trust that the government shall take care of the national security, national issues like health and education policies, international relations, and taxation for the benefit of the people.

In order to make the voting process more effective the institutions like 'Election Commission' came into existence in different parliamentary democracies. The institutions, along with setting up the process and legislation for conducting the elections, formed the voting districts, electoral process, and the balloting systems to help in conduct of transparent, free, and fair elections. The concept of secret voting was introduced since the beginning of the voting system. Since the trust on democratic systems is increasing it is important to uphold that the trust on voting should not decrease. In the recent past there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments. Such examples can be vastly found in countries like Nigeria, India, Brazil, Pakistan, and Bangladesh. The nature of the issues, causing this mistrust are multi-fold and some are listed in Table 1:

Since all these countries are among the emerging democracies, it is pretty likely that in next decades they will emerge as full democracies and the vote and the voting process will

The associate editor coordinating the review of this manuscript and approving it for publication was Jiajie Fan.

TABLE 1. Nature of issues causing mistrust.

S#	Reasons	Description
1	Pre-poll rigging	This includes but not limited to the (sometimes intentional) errors in the voting lists and formation of the voting districts to help one and hinder other parties. In some areas the polling stations are made too far that he voters prefer not to vote than going too far to vote.
2	Casting duplicate votes	Since there is no biometric authentication on the polling stations, it is easy to cast vote again for the ones who have not voted. Sometimes there are thousands of ballot papers found voted without the presence of the actual voters.
3	Use of power to influence polling staff	The use of power is not uncommon to influence the voters either by incentives or by threats.
4	Unsupervised vote counting	For the parties or independent condiments who do not have a strong representation in a region, it is likely that their votes can be miscounted.
5	Lack of audit and appeals	The process of hearing and deciding the appeals on such issues is so slow that they can hardly be finalized before the next elections. Therefore, the losing candidates and/or the losing parties start the street agitation instead of going to the constitutional bodies to get the conflicts resolved. This causes in unrest and political instability in the country.
6	Lack of interest by public at large	By observing the reasons mentioned in 1-5, there has been a feeling that the people are not fully convinced to vote and the mistrust on the voting system has taken over their right of participation. Such issues can be dealt with the trustworthy electronic voting platforms.

earn more respect and trust over time. The disadvantages of such mistrusts are multi-fold and they include but not limited to the following national problems:

- ✓ Political instability
- ✓ Compromised writ of the government
- ✓ Mistrust over the electoral process
- ✓ Compromised governance
- ✓ Disorder in the state institution
- ✓ Chain of command to run state affairs
- ✓ Economic instability

II. BACKGROUND RESEARCH

Mistrust in the voting is not an uncommon phenomenon even in the developed countries. In order to improve the trust, the least thing that can be done in this regard is the orientation of the electronic voting based on the biometric authentication. This may help is solving half of the problems being faced by many countries in the electoral process. The e-voting systems have been used by few countries in the past, e.g. Estonia, Ireland, and Norway, while some are not going to use it anymore to eliminate the audit problems.

Basin *et al.* [7] has presented an example from the canton of Valais Switzerland in March 2017, where the postal ballots were not received by the voters and when the ballots were re-issued, it was identified that the vote of the affected voters had already been voted. Although Switzerland, has an e-voting system but it still allows her voters to vote either electronically or by post or by physically going to the polling station. The e-voting system also needs more security, privacy, and transparency to become a completely reliable system of voting. Bevelander and Pendakur [8] has mentioned that there were controversies in the election of student's union elections held in Austria in 2009. The constitutional court of Austria considered this election invalid as the electoral committee was not regulated and the process of vote and voter verification was found to be beneath the security standards.

Volkamer *et al.* [3] has stated that the Irish government used evoting machines in 2002 general elections and it was being planned to use them in 2004 EU elections. These machine were bought at a cost of €55 million. During the audit it was discovered that the machines are not reliable and its outcome can't be trusted concretely as there were issues with the paper trail and the verification system. The Irish government therefore has opted to scrap the machines while this initiative has costed €55 million to the Irish taxpayers. For the similar reasons, Germany and the Netherlands, have also decided to permanently ban the voting machines at political votes.

Wolchok *et al.* [9] provide an insight about the use and vulnerabilities of the electronic voting machines (EVM's) both in terms of software, hardware and other related challenges. Parshad has discussed several incidences where the malfunctioning of either hardware or software was reported while in some cases it was also observed that the EVM's in use for the election day had modified hardware and/or software in anticipation. It was also reported that the few US

scientists belonging to University of Michigan (experimentally) could intervene into the Indian elections and could play with the numbers.

Rivest [10] has presented the concept of providing three ballots to the voter where voter will cast all the ballot papers after marking. Each ballot paper contains a unique identifier but the voter remains anonymous as the keys are decrypted. At the time of tabulation, the votes casted are linked and the choice found on two ballot papers is chosen while the choice with one ballot paper is rejected. The scheme may not be effectively used if there are only two contestants or if there are number of contestants. The scheme also has the disadvantage of being slow and the human error increase if the votes are not accurately poled in the respective boxes.

Votem [11] presents a commercial solution that deal with a token based system build on the blockchain technology and thus ensure the anonymity and security of the voting system. The solution is more suitable for i-voting where the physical and biometric authentication of the voter is not utilized. The token based system, however, limits the applicability of the this voting platform to be used effectively in wide ranged, full fledge elections where the power of the solution looks compromised to address the challenges. The blockchain developed for the purpose of the electronic voting can either be kept public or private [12], [13]. In the public blockchain, however, the contents of the transactions remain visible to everybody in the blockchain. It is therefore important to encrypt the contents of the blocks by using some secure algorithms, e.g. AES to keep the contents of the block unreadable and encrypted [14], [15]. The AES keys however, have to be secured and applied effectively to recover the encrypted contents. This make the transaction bit slower and the power of electronic voting and blockchain is compromised. To overcome this challenge, the private blockchain is suggested. It can however be noted that many challenges may originate during the software development aspect [16]–[19] of the blockchain based e-voting solution while the mobile based solution have their own respective security and privacy challenges [20]–[23] while there are certain concerns, trends, and challenges to be considered for developing social media apps for such systems [24]–[27].

Zheng *et al.* [28] has shown some concerns for using the blockchain for the electronic voting. The e-voting system demands that a blockchain is responsive and scalable at all time to get efficient response to formulate the overall results. In this regard the block size has to be of adequate size. Currently, the bitcoin blockchain covers 100's of gigabytes of storage which makes the addition of blocks and information retrieval quite slow. Johnson *et al.* [29] is of the view that in blockchain based electronic voting systems the users make the transitions based on the addresses and not on their identity and in case if there is an information leakage, the users can generate several addresses. It is tough for the blockchain mechanism to ensure transactional privacy since the information of all transactions and public keys are visible to public. Barcelo [30] is of the view that a link between the users and the transactions made by the individual users can be identified. Biryukov *et al.* [31] has presented a method to link user's pseudonyms to the IP address of the user even when the users are behind a firewall or even behind the network address translation which can help in reaching to the origin of a transaction. Hjalmarsson *et al.* [42] has presented an e-voting framework that is yet in-progress and has not test against the claims that were made about increasing the security and reducing the cost of conducting elections. Panizo Alonso *et al.* [43] have argued about the e-voting initiatives are pretty common but the actual developed system are very few. The author has also mentioned that how the social and cultural limitations can affect the e-voting initiatives. Kshetri and Voas [44] have introduced a smartphone based electronic platform that is more of an example of i-voting rather than e-voting. Zhang *et al.* [45]–[47] in his work, has discussed different applications based on blockchain.

The private or the consortium blockchain which is maintained by an organization, e.g. election commission of the country, has its own issue that require a resolution strategy in place. In the private blockchain only the eligible nodes can see the details of the votes and transaction and the voting process does not remain visible to the voters. This makes the voting process less transparent as compared to paper based voting.

Another threat in the private blockchain being used for voting, is that the authority hosting the private blockchain may have access the data and it can be observed in anticipation about the results while the voters in general don't have significant knowledge of the proceedings. This causes a situation which compromises the level playing field for all the parties as some parties having anticipated knowledge may be in better decision making position. Although the electronic voting is anticipated to have a great future yet the past is not that glorious. In some countries e-voting is not an option while few are in a process to eliminate the security, verifiability, and anonymity concerns. There are issues that require immensely deep consideration by the legislatures, technologist, civil society, and the people.

III. RESEARCH QUESTIONS

The study will address the following objectives:

a. What are the activities formulating the electronic voting process?
b. How to ensure that the transactions and voters data are secure?

IV. METHODOLOGY

We will adopt a process to address the following activities.

A. MODELING OF ENTIRE E-VOTING PROCESS

The system modeling helps in drawing the entire system on paper to develop a ***deep*** understanding of the system and to identify errors and flaws that can be observed before the system can be implemented.

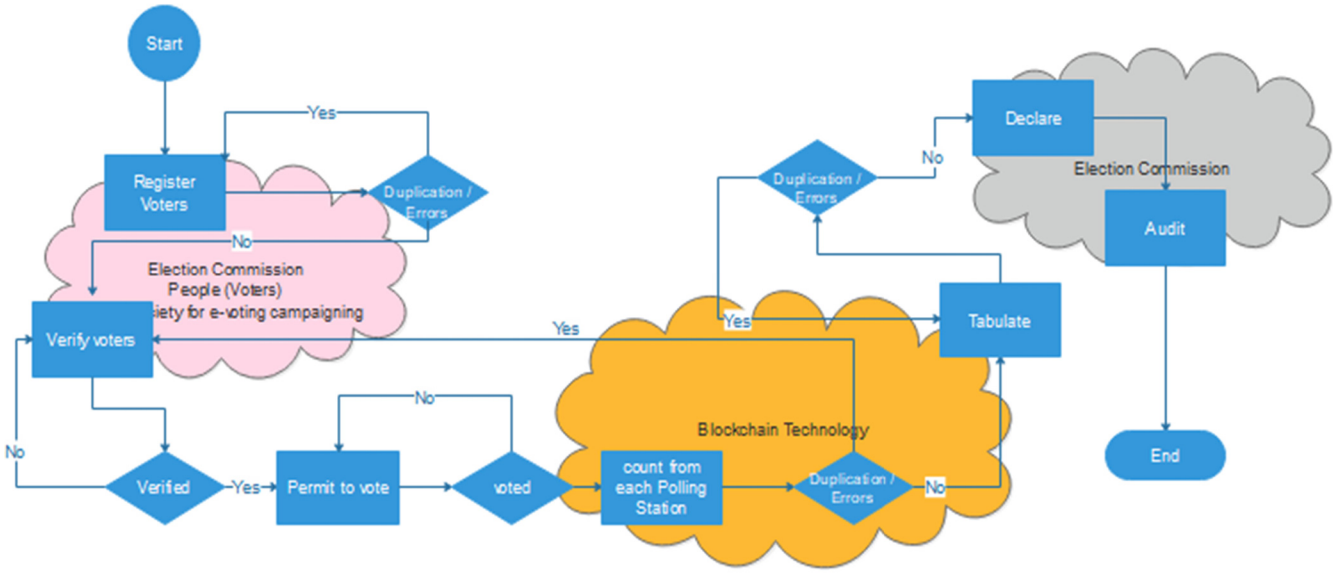

FIGURE 1. The electronic voting process with institutions involved.

B. DETERMINATION OF THE SUITABLE TECHNOLOGY PLATFORM TO ENSURE ANONYMITY, PRIVACY, AND SECURITY

The e-voting process requires the features like privacy, security, anonymity, and verifiability as the core function of this solution, it is important that the choice of the underlying technology is consistent to meet these challenges. It has been identified that the Blockchain technology sufficiently deals with all such challenges.

C. DEVELOPMENT & TECHNOLOGY INTEGRATION WITH THE PERCEIVED E-VOTING MODEL

Based on the system model, the system will be developed and will be integrated with the baseline technology.

V. POLLING PROCESS

The electronic voting system is executed in a way that it deploys many individuals at different levels. In order to develop an effective block creation system, it is important to understand the actual execution on ground. In the conduct of the elections, the election commission and the NADRA (National Database and Registration Authority) have a big role to play. NADRA is the national registration authority in Pakistan and is responsible for the registration and issuance of identity documents to the citizens of Pakistan. The NADRA is responsible to ensure that each citizen of the country has its record available and the biometrics of each individual are also available [32]–[35]. The biometric authentication is used in the voter's authentication on the polling day. The election commission is responsible for making the electoral lists available which are verifiable from the base records. The authenticated voters can vote according to the provision provided to them and the usage of technology is made to get the vote recorded and tabulated accordingly. It is also the responsibility of the election commission to declare the results when polling station wise and constituency wise tabulation has been made. The figure 1 describes the flow of the activities along with the respective institution and dependent technology.

In this system, we consider Pakistan as a case study. In Pakistan, the national assembly has 272 direct national seats elections. For the purpose of polling, each constituency is divided into the number of polling stations that may vary based on the number of voters in the area (normally there is one polling station for 1,000 voters). Each polling station is administered by the presiding officer who is assisted by an assistant and some staff. The responsibilities are designated to each staff member for authentication of the voters and helping him to cast the vote without fear or influence.

This paper provides a solution that is based on the electronic voting machines and biometric authentication of the voter before he can cast the vote. The casting of vote is a procedural step that includes the following.

a) The voters name must exist in the voting list to enable himself to visit the polling station for the purpose of voting. It is the responsibility of the voter himself to ensure that once he attained the age of eighteen years, his name should be present in the voting list. This can be done by consulting the respective offices, e.g. National Database and Registration Authority (NADRA) in Pakistan. The voting lists are published few weeks earlier than the elections. The individual having his name in the voting list is eligible to vote and presents his original identity to the polling staff. Before casting the vote, the voter has to be authenticated by the biometric system. The record of the voter is checked with the help of NADRA's database.

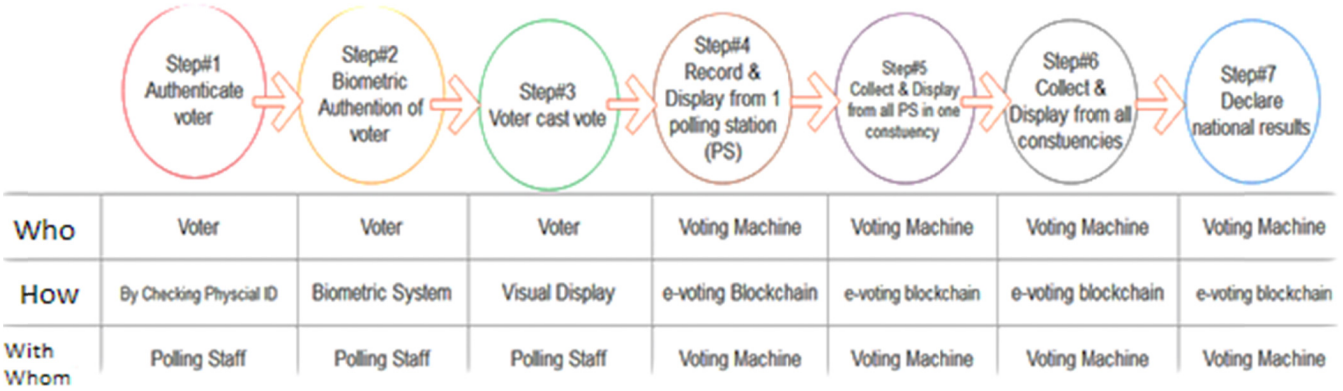

FIGURE 2. Electronic voting process and contributing entities.

b) Once the voter has passed the authentications check, he is brought to voting screen to vote. From the voting machine the names and respective party symbols of each candidate are displayed and the voter can vote according to his will. The confirmation screen seeks the confirmation of the voter and records the vote casted by the voter.
c) The voter can vote only once, and once the vote is casted is voting record is marked as ''voted'', which restricts the voters from voting again. The name of the voter can be blocked or eliminated from the list of eligible voters list for the current elections, once he has casted the vote. In his work on internet voting [41], he has presented a framework where the voters can vote multiple times, and every time they vote, the previous vote is cancelled. This does not appear to be a workable solution if the voting process is to be completed in one day and some 110 million voters have to vote, which is the case in Pakistan.
d) The polling process continues until the voting time ends or all the voters in the voting list have casted their votes.
e) The results of the polling station are declared and the votes attained by each candidate are listed. The process is repeated for all the polling stations in the constituency and the collective result of all the polling stations forms the result for that specific constituency. Likewise, the results for all the constituencies are collected to form the results of the national election. The process of voting and the result accumulation is demonstrated in the figure 2.

The figure 2, demonstrates the three layered working of the process. The Layer 1 (Who), describes the participants of the system who can interact with the polling process, including the voters, polling staff, and polling machine. The second layer (How) deals with identification of the underlying tools and technologies to ensure that the process can smoothly work. The second layer of technology along with its algorithmic variations is discussed in this paper. The third layer (with whom) deals with the supporting elements.

VI. HASHING, PROOFS, AND BLOCKCHAIN TYPES

The past events in the human life are timestamped and linked with each other. They can neither be reversed nor be duplicated. Also the correctness of these events is known by many individuals who can verify the information as and when needed. This provides the idea of the blockchain where the irreversible, distributed, public ledger is formed to hold blocks of data. The events can be represented as block of information which are linked to form an invisible blockchain of the events in our life. The idea of a computational blockchain is no more different. In the computational blockcahin past blockchain is an open and distributed ledger which can be seen by anybody and can be updated by anybody depending on the conditions of the blockchain. The concept revolves around making the trust oriented system where the records can't be altered and the exclusion is not unilateral.

A. TYPE OF BLOCKCHAIN

Blockchain has three different types, i.e. public blockchain, private blockchain, and consortium blockchain [36]. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will [37]. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively [38]. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country.

Block is the primary component of the blockchain. A block consists of the header and the body, the body of the block contains the transactions being written to the system [39]. The header of the block contains the information about the block

that includes previous hash, nonce value and difficulty, and the time stamp of the block and the transactions. The length of the block is variable and deemed to have been among1 to 8 MB of size. The header of the block uniquely identifies the block to be placed.

B. HASHING

Hashing is the process of changing the arbitrary and variable size input to a fixed size output. There are different functions that perform hashing of different level. The comparison of the hash function is provided in the Table 2.

TABLE 2. Hashing algorithms.

Hash Function	Hash Length	Secure
Md5	128 bit (32 symbols)	No
Ripemd 1	160 bit (40 symbols)	Yes
SHA1	160 bit (40 symbols)	No
SHA256	256 bit (64 symbols)	Yes
SHA3	256 bit (64 symbols)	No
Keccak-256	256 bit (64 symbols)	Yes

MD5 algorithm is widely used for hashing purposes and it provides a 128 nit or 32 symbols long hash value. MD5 is the latest algorithm in the series while before that Md2, Md3, and Md4 also existed [40]. The algorithm was designed to be used as a cryptographic hashing algorithm but it faces some problems that reduce the production of unique hash value and hence it faces some vulnerabilities. Race Integrity Primitive Evaluation Message Digest(RIPEMD) is a family of hash function developed by Hans Dobbertin in 1996. This algorithm was designed to replace the MD5 as a more secure alternative. It has few variations that have emerged over time including RIPEMD-128, RIPEMD-160, RIPEMD256, and RIPEMD-320.

SHA (Secure Hashing Algorithm) is another cryptographic hash function that yields 160 bit hash value consisting of 40 hexadecimal characters. The algorithm could not resist the collusion attacks against it and its usage has declined after 2005. In this time several new algorithms have also been proposed, including SHA 3, and SHA 256. The SHA 2 set of algorithms is designed by the US's Nation Security Agency. SHA 256 and SHA 512 are new hash functions that do not have collusion problems and deemed secure otherwise, at least as yet. Keccak is a family of algorithms designed by designed by Guido Bertoni, Joan Daemen, MichaëlPeeters. The flexibility of the algorithm, in contrast to its other counterparts, is that it accepts any length of input and yields an arbitrary length of output, while all other algorithms produce a fixed length output.

C. PROOFS

a) *Proof of Work:* The concept of the proof of work deals with the mining / creation of the blocks in such a way that it can be proved that a significant effort has been made for the resolution of the mathematical problem introduced for the creation of a block in the blockchain [41]. The mathematical complexity is increased on the creation of every new block so make the creation of the block complex and a rewarding scenario. The increasing complexity is introduced with the help of the hash functions, marckle trees, and the nonce value.

b) *Proof of Stake:* The concept of the proof of stake revolves around the identification of the stakes in the blockchain [42]. The holders of assets are subject to have more priority in the creation of the blocks. The likelihood of that only few creators of the blocks may control the entire blockchain by virtue of the assets that they have, can't be ignored. This concept is applicable in the consortium blockchain or the private blockchain where the holding companies may need an administrative access to the blockchain.

c) *Proof of Burn:* The proof of burn deals with the burning of the coins that are gained over a period of time [43]. This burning process works as a fuel for the creation of new blocks. This proof of burn concept ensures that the individuals don't become powerful enough by increasing their stakes in the network. The burn process is recorded by sending the coins / proof of work to an arbitrary address, that may be designated by the network itself.

The above mentioned proofs exist well in the literature and they are being practiced well in the bitcoin mining. The application of blockchain, however, differs in its application in other areas and the proofs that we mentioned in this section may not be applicable in actual but an adjustment may be sought in implementation based on the nature of the application itself. How much change? The answer of the question is governed by the nature of the application area where the blockchain method is to be applied.

In this paper, we are addressing the application of the blockchain in trustworthy electronic voting, and it is identified that the existing blockchain may need some adjustments because of the following reasons.

a) *Creation of Block:* The block creation in the electoral process is a basic entity and the voters can't record their vote if the block is not created. It is therefore vital that the blocks are created without solving the mathematical puzzles to form the proof of work. Since it will be a consortium blockchain, the proof of stake will not be relevant and likewise the proof of burn is not applicable as created block will be held by one individual.

b) *Sealing of Blocks:* The voters can vote and the transactions are recorded in the blocks, by the time the polling time ends, the blocks are required to be sealed by the hash functions and using the Merkle tree and nonce function. The sealing concept is not present in the existing concepts.

c) *Polling Time:* Since the voting process continues for 8-10 hours, it is vital that the blocks can be created, sealed, and secured in this time. As the proof of work,

proof of stake, and proof of burn can only be applied after a very lengthy process, their application on the trustworthy electronic voting is not that suitable.

d) *Result Delay:* Once the polling process is complete and the results have been announced, there will be no further need for continuing the mining or block creation activity. Since the proof of work and proof of stake algorithm keep on repeating themselves recursively, use (waste) a lot of computational power over time. The proposed system does not use that much resources and hence remains cost, time, and power effective.

Considering the limitations of the existing algorithms, it is vital that an algorithm is developed that can deal with the identified issue and overcomes the limitations of the existing algorithms when they are applied to the area of trustworthy electronic voting.

VII. BSJC PROOF OF COMPLETENESS

The (Basit Shahzad & Jon Crowcroft's) proof of completeness algorithm deals with the creation of blocks, sealing of blocks, data management, and building the blockchain specifically for the electronic voting platform. The concepts are described here.

A. CREATION OF BLOCK

Unlike the bitcon's blockchain, where a significant proof of work is required it is not the case for the voting system. It is vital that the nodes / block are created before the transaction can take place in the respective blocks. The creation of the blocks on the blockchain is a sensitive matter and requires sufficient security before a block can be created. The creation of the block takes place when following have been met.

a) The presiding officer (PO)verifies his unique identity number and his biometric authentication.

b) The biometric are verified and the permission is granted.

c) The system shall generate a random number by using the SHA-256 hashing algorithm, system will generate a hash and send the result to the presiding officer to generate a block. Along with the other information of the block the hash value is also saved in the block header which is visible to others as well.

d) The next block to be generated will be requested by the next presiding officer. Based on the hash value of the first block, the presiding officer will submit his unique identity for the creation of the next block. The next block is generated by the generating a new random number, associating that with the hash of the previous block and applying the SHA-256 algorithm., i.e (RN describe random number).

$$Block\ 1 = hash\,(Uid + RN\ (length = 3)) \quad (1)$$

$$\text{Block 2..n} = \text{hash(Uid} + \text{Block(n} - 1) + \text{RN(length} = \text{n} + 2)) \quad (2)$$

B. DIFFICULTY AND NONCE VALUE

The first block will be generated based on the unique id of the PO and the system will add a three-digit random number and will apply SHA-256 algorithm to develop the hash and the first block will be generated. For every proceeding block, the hash of the previous block hash code, unique id of the PO and the random number generated will be derived. The length of the random number used to generate the hash will increase with the number of the block being generated, e.g. the length of random number for block number 20 will be 20 and for the 100^{th} block it will be 100. Since this is a private blockchain, the creation of the blocks will be restricted to the holders of the unique id's provided to the PO's.

Once the block has been created the polling process can start as demonstrated in Figure 2. Each casted vote will serve as a new transaction. The blocks will keep on recording the transaction unless the voting process is completed as shown in Figure 3.

C. SEALING OF THE BLOCKS

The polling process shall continue until either the polling time finishes or the number of registered voters has completed. Once the polling is complete, the next step is to seal the blocks to ensure that the block come even more secure and adding security is included. Therefore, in order to seal a block following items are considered.

a. It is to be ensured that either the polling time has elapsed or all the registered voters have casted their votes.

b. The completion of the polling process is to be confirmed by the PO of that polling station.

c. The data of the block (i.e. the entire result) will be hashed using the SHA-256 algorithm. This is done by concatenating the results inside the block and hashing them in pairs the block is hashed based on the hashed contents of the block. Another system generated random number can be added in the hashing to make it more secure.

d. Every proceeding block that confirms the completion of the transactions will have used the hash of previous block, a new random number, and hash of the block to generate the hash value that will be used by the proceeding blocks.

e. The sealing of the block means that the block has now been sealed with a hash function and the contents of the block can't be changed by ensuring the application of the mathematical puzzles that are NP hard to solve. The sealing process is use the hashing algorithm called SHA-256 and following equations introduce the mathematical complexity.

$$\begin{aligned} &Sealed\ Block1 \\ &= hash(hash(pairs\ of\ transactions) \\ &\quad + RN(length\ n+2) + hash\ of\ block\ 1) \end{aligned} \quad (3)$$

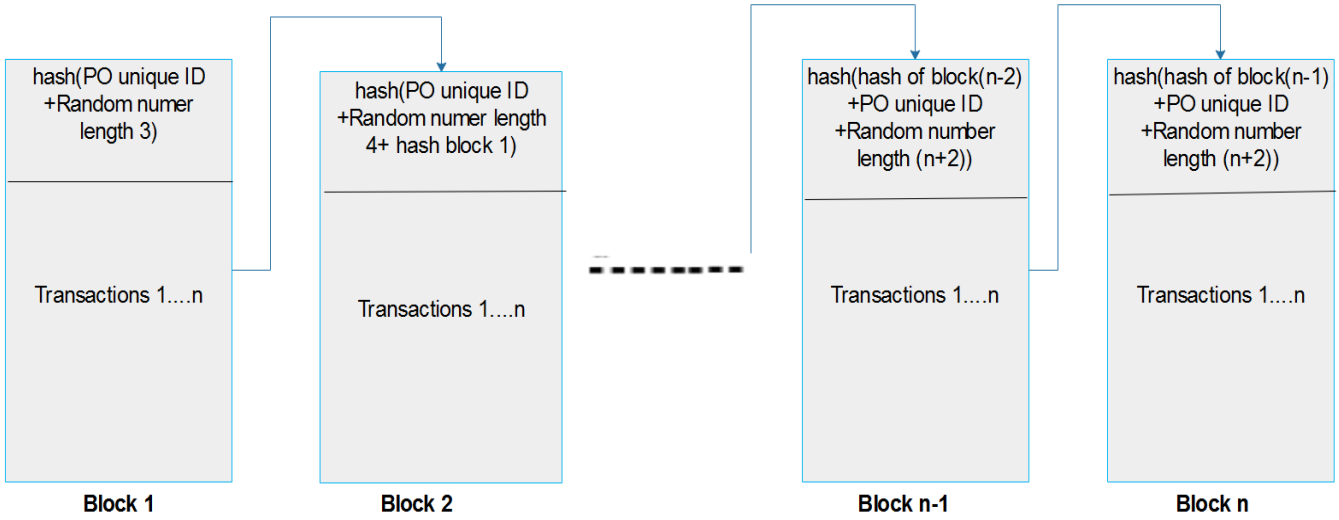

FIGURE 3. Creation of blocks in blockchain.

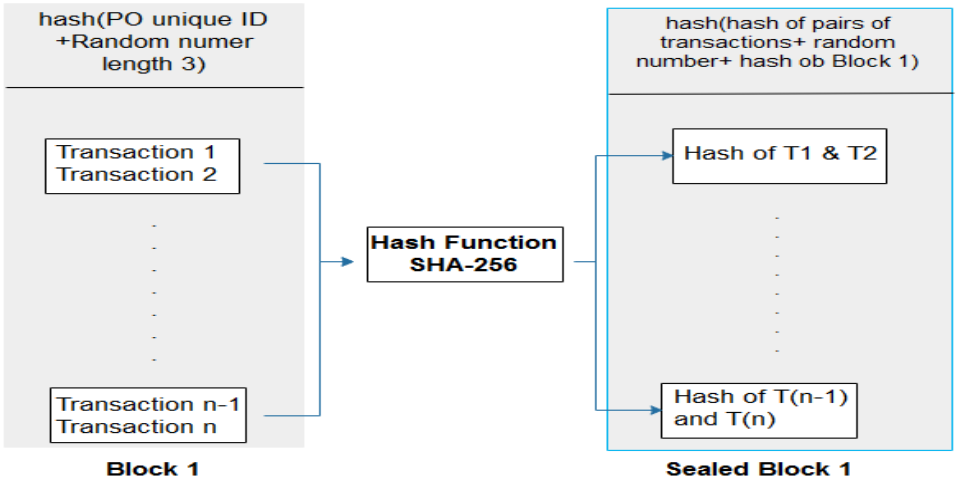

FIGURE 4. Block sealing process.

$$Block\ 2 \ldots n = hash(hash(pairs\ of\ transactions) + Random\ Number(length\ n+2) + hash(Block\ (n-1))) \quad (4)$$

The sealing process of the blocks is demonstrated in Figure 4. After the block has been sealed, the sealed block represents the actual block.

The representation of the sealed blocks is such that the blocks are integrated among themselves by using the chained hash key and the key of one block is used by its proceeding block to generate the next hash and this chain continues unless the blocks finish.

During the process of applying the hash function on the transactions a pair of transactions (sequential) are selected and the hash is applied on them. This sequential hashing process runs on all pairs of transactions and a hash is generated based on all the hashed data by applying the SHA-256 algorithm. Once the hash of a block has been generated it is integrated with the hash of the previous block and a new random number and the outcome is hashed again to ensure that the hash outcome function is not solvable without the capability of the solving NP hard problems. The purpose of the blockchain based electronic voting is to introduce secure voting process that can gain trust of the stakeholders, including, voters, political parties, and state institutions. The security of the casted vote is ensure by the block creation, block sealing, and content hashing. While the created block is secured by the (1) and (2) and uses the SHA-256 algorithm which is known to be sufficiently secure to secure the e-voting process, the blocks is sealed with the unique hashes produced by the SHA-256 algorithm based on the unique input values, mentioned in (1), (2), (3), and (4).

The Merkle trees are formed as each block is associated with the next and previous block (except the first and the last block) in terms of accepting and providing the hash value that is used for stitching the block with the chain.

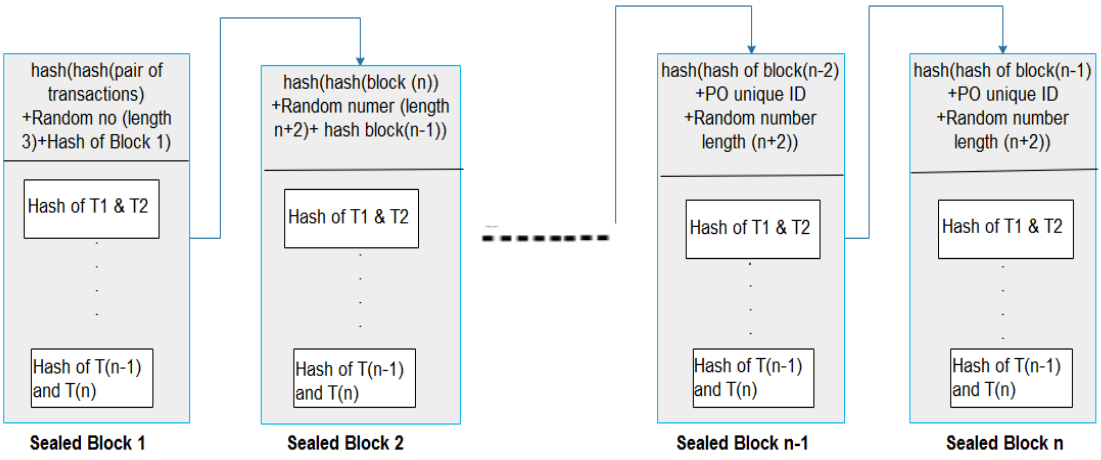

FIGURE 5. Conversion of blocks to sealed blocks.

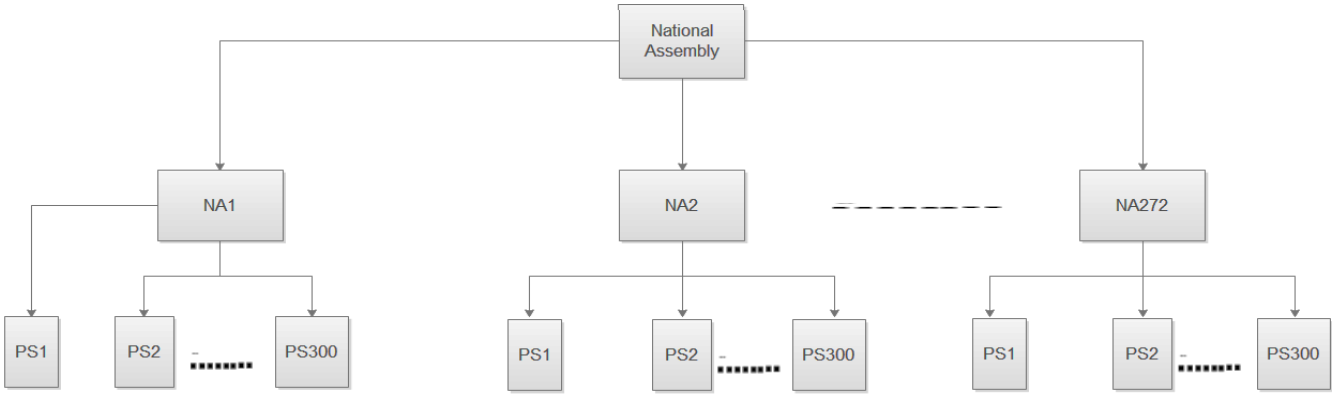

FIGURE 6. Distributed block structure.

The representation of the sealed blocks is demonstrated in the Figure 5, that shows the connection of the block after they are sealed.

VIII. COLLECTION OF VOTING RESULTS

The collection of the results is done from the stored data on the blocks through the significant organization of the nodes in the blockchain. The chain of blocks works at the lower end and works to accumulate the data in the containers (block) that are chained together through and algorithm serially.

However, a Merkle tree is maintained that records the distribution of the block and the degree of their decomposition. Figure 6 demonstrates the logical division of the national assembly seats and the polling stations in each national assembly seat.

In Figure 7, the Merkle tree representation of the system is demonstrated and it can be observed that the record of each transaction taking place is stored at the top level, i.e. level 0. At level 1, the layer describes the national seats while at level 2, the layer demonstrates the polling stations in any constancy. Thus, any transaction, in any block, can directly be located and recorded by keeping them distributed and open for transaction but securing the contents with the BSJC algorithm of proof of completeness. In order to improve and maintain trust among the voters it is vital that the voter knows about the count of his vote. In order to make the process transparent, a trail of the voters who casted their votes is generated at the end of the polling process.

IX. DISCUSSION

The paper presents a perspective in the electronic voting process. That includes but not limited to identifying the polling process, the selection of the suitable hash algorithm, the selection of adjustments in the blockchain, the process of voting data management, and the security and authentication of the voting process in particular are discussed.

The polling process discussed in this paper is inspired from the actual voting process used on the polling day, which includes the physical and logical verification of the voter and the voter's data but only by using the voters lists etc. The electronic voting process ensure that the voters is verifiable by its physical record, e.g. the national identity card and also verifiable by using the biometric authentication. The availability of the verification system on the polling time

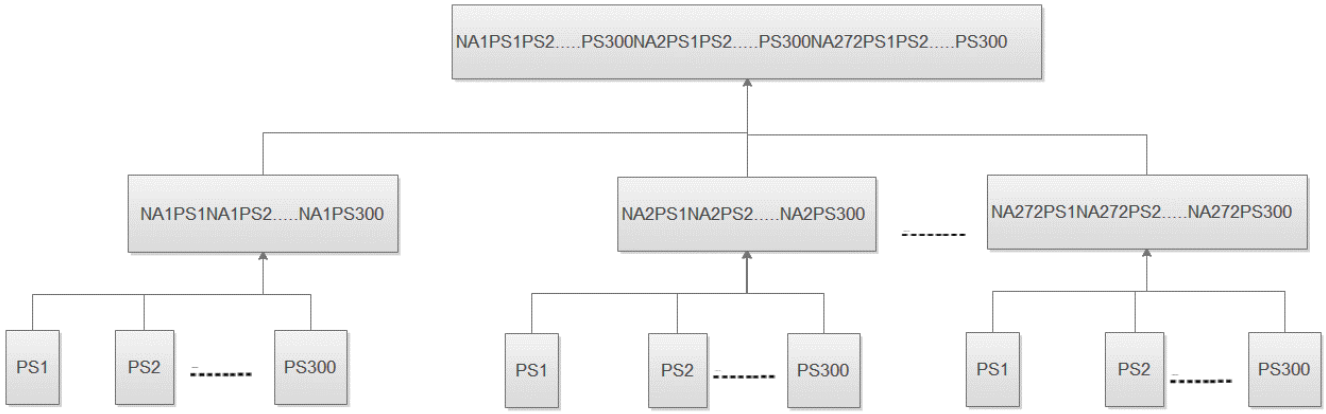

FIGURE 7. Merkle tree formation of the blocks.

is extremely essential and the process can't be completed without the completely available system. The threats to the verification process can be extremely high if either the system is not available or the system is not in a state to be used effectively for the purpose of the voter's verification. It is the responsibility of the election commission and allied institutions to ensure that the equipment, tools, and technologies are available to make / keep the proceedings on track. The process can only be successfully completed if all the stakeholders perform their duties with extreme coherency and consistency.

Conceptually, the blockchain is implemented by the effective use of the hashing algorithms that govern the core of the blockchain itself. The quality of the hash algorithm being used govern the quality of the blockchain. It has been noted that continuous improvements are taking place in this domain. Many algorithms that were proposed in last decade have proven to have flaws while the struggle for the identification of flawless algorithm remains continuous. This research uses the SHA-256 algorithm, that is supposed to be the best of the available in ensuring the security and irreversibility of the blockchain.

The blockchain concept used in the electronic voting is a private or a consortium blockchain where the transactions and the block creation and sealing are done in a supervised environment and the entries and block creation can only be done by the authorized members of the users. Generally, the proof of work is a mathematically expensive task which requires massively large computation to solve the problem before the block can be created. In the polling scheme, the delay for the creation of the block can't be that huge which may delay the polling process itself. Also the sealing of the block has been introduced without compromising the strength of the blockchain.

The blocks are responsible for containing all the transactions that are made during the polling day. This contains the voter's information and the vote that he might have casted. Although the information about the vote and voters are saved yet they are not linkable by the unauthorized access. The record is maintained to ensure that every vote is verifiable at every given time.

In contrast to different e-voting systems e.g. in [42]–[44] it has been identified that many systems developed until now have their limitations, with respect to the model of their development, while some systems have flaws as well. Few systems are more suitable for i-voting instead of e-voting. The paper has suggested a flawless result accumulation method from the blocks to declare the results from the polling stations, constituencies, and the national result but this research has also its limitations which are presented in section X.

X. ASSUMPTIONS & LIMITATION

There are some assumptions that are considered in this research.

a) The voter is well educated and aware of his fundamental rights and the polling process. It is vital that each voter can vote in the stipulated time.
b) The data of all the voters is available and up for the purpose of verification. The data is to be provided by the national agency that maintains the data. It is also assumed that the connectivity is available all the time and no delay in communication delay is faced and no interruption because of unavailability of internet is envisioned.
c) It is also assumed that the polling staff is aware of the technology and they can guide the voters to effectively complete the process.

XI. CONCLUSION

Mistrust in the voting is not an uncommon phenomenon even in the developed countries. The electronic voting, however, has emerged as an alternative but still not being practiced at a large scale. The electronic voting is anticipated to have a great future yet the past is not that glorious. In some countries e-voting is not an option while few are in a process to eliminate the security, verifiability, and anonymity concerns. There are issues that require immensely deep consideration by the legislatures, technologist, civil society, and

the people. This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

REFERENCES

[1] *EIU Democracy Index 2017*. Accessed: Aug. 3, 2018. [Online]. Available: https://infographics.economist.com/2018/DemocracyIndex/

[2] ScienceDirect. *Democracy Online: An Assessment of New Zealand Government Web Sites*. Accessed: Aug. 1, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X00000332

[3] M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in Internet voting," in *Proc. 5th Int. Conf. Theory Pract. Electron. Governance*, 2011, pp. 1–6.

[4] É. Bélanger and R. Nadeau, "Political trust and the vote in multiparty elections: The Canadian case," *Eur. J. Political Res.*, vol. 44, no. 1, pp. 121–146, 2005.

[5] T. Kunioka and G. M. Woller, "In (a) democracy we trust: Social and economic determinants of support for democratic procedures in Central and Eastern Europe," *J. Socio-Econ.*, vol. 28, no. 5, pp. 577–596, 1999.

[6] T. van der Meer, "In what we trust? A multi-level study into trust in parliament as an evaluation of state characteristics," *Int. Rev. Administ. Sci.*, vol. 76, no. 3, pp. 517–536, 2010.

[7] D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, "Election security and economics: It's all about eve," in *Proc. Int. Joint Conf. Electron. Voting*, 2017, pp. 1–28.

[8] P. Bevelander and R. Pendakur, "Electoral participation as a measure of social inclusion for natives, immigrants and descendants in Sweden," Tech. Rep., 2008, p. 33.

[9] S. Wolchok *et al.*, "Security analysis of India's electronic voting machines," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 1–14.

[10] R. L. Rivest, "The threeballot voting system," Tech. Rep., 2006, p. 15.

[11] J. Stern. *Votem—Voting for a Mobile World*. Accessed: Jul. 31, 2018. [Online]. Available: https://votem.com/

[12] M. Pilkington, "11 Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. 2016, p. 225.

[13] G. Gabison, "Policy considerations for the blockchain technology public and private applications," *SMU Sci. Tech. Rev.*, vol. 19, p. 327, Sep. 2016.

[14] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Cryptographic Hardware and Embedded Systems*. 2004, pp. 357–370.

[15] Y. Stein and H. Primo, "Programmable data encryption engine for advanced encryption standard algorithm," U.S. Patent 7 508 937 B2, 2009. Accessed: Aug. 1, 2018. [Online]. Available: https://patents.google.com/patent/US7508937B2/en

[16] B. Shehzad, K. M. Awan, M. I.-U. Lali, and W. Aslam, "Identification of patterns in failure of software projects," *J. Inf. Sci. Eng.*, vol. 33, no. 6, pp. 1465–1480, 2017.

[17] A. M. Abdullatif, B. Shahzad, and A. Hussain, "Evolution of social media in scientific research: A case of technology and healthcare professionals in Saudi Universities," *J. Med. Imag. Health Inform.*, vol. 7, no. 6, pp. 1461–1468, 2017.

[18] B. Shahzad, "Identification of risk factors in large scale software projects: A quantitative study," *Int. J. Knowl. Soc. Res.*, vol. 5, no. 1, pp. 1–11, 2014.

[19] A. B. Shahzad and A. Said, "Application of quantitative research methods in identifying software project factors," *Int. J. Inf. Technol. Elect. Eng.*, vol. 1, no. 1, pp. 30–33, 2012.

[20] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, "Human-oriented design of secure machine-to-machine communication system for e-healthcare society," *Comput. Hum. Behav.*, vol. 51, pp. 977–985, Oct. 2015.

[21] K. Saleem, A. Derhab, J. Al-Muhtadi, B. Shahzad, and M. A. Orgun, "Secure transfer of environmental data to enhance human decision accuracy," *Comput. Hum. Behav.*, vol. 51, pp. 632–639, Oct. 2015.

[22] J. Al-Muhtadi, B. Shahzad, K. Saleem, W. Jameel, and M. A. Orgun, "Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment," *Health Informat. J.*, Apr. 2017

[23] M. I. U. Lali, R. U. Mustafa, K. Saleem, M. S. Nawaz, T. Zia, and B. Shahzad, "Finding healthcare issues with search engine queries and social network data," *Int. J. Semantic Web Inf. Syst.*, vol. 13, no. 1, pp. 48–62, 2017.

[24] B. Shahzad, E. Alwagait, S. Alim, and I. Resaercher, "Investigating the relationship between social media usage and students grades in Saudi Arabia: A mixed method approach," in *Proc. Recent Adv. Elect. Eng. Educ. Technol.*, 2015, pp. 211–214.

[25] R. A. Abbasi *et al.*, "Saving lives using social media: Analysis of the role of Twitter for personal blood donation requests and dissemination," *Telematics Inform.*, vol. 35, no. 4, pp. 892–912, 2018.

[26] E. Alwagait, B. Shahzad, and S. Alim, "Impact of social media usage on students academic performance in Saudi Arabia," *Comput. Hum. Behav.*, vol. 51, pp. 1092–1097, Oct. 2015.

[27] B. Shahzad and E. Alwagait, "Does a change in weekend days have an impact on social networking activity?" *J. UCS*, vol. 20, no. 15, pp. 2068–2079, 2014.

[28] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[29] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[30] J. Barcelo, "User privacy in the public bitcoin blockchain," *J. Latex Class Files*, vol. 6, no. 1, p. 4, 2007.

[31] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin P2P network," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2014, pp. 15–29.

[32] A. Rasul and S. D. McDowell, "Consolidation in the name of regulation: The Pakistan Electronic Media Regulatory Authority (PEMRA) and the concentration of media ownership in Pakistan," *Global Media J.*, vol. 11, no. 21, pp. 110–121, 2012.

[33] S. K. Mohmand, "Patrons, brothers and landlords: Competing for the vote in Rural Pakistan," Ph.D. dissertation, Univ. Sussex, Brighton, U.K., 2011.

[34] S. Baig, U. Ishtiaq, A. Kanwal, U. Ishtiaq, and M. H. Javed, "Electronic voting system using fingerprint matching with Gabor filter," in *Proc. Int. Bhurban Conf. Appl. Sci. Echnol. Islamabad, Pakistan*, 2011, pp. 130–135.

[35] N. Yaser, N. Mahsud, and I. A. Chaudhry, "Effects of exposure to electronic media political content on voters' voting behavior," *Berkeley J. Soc. Sci.*, vol. 1, no. 4, pp. 1–22, 2011.

[36] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.

[37] ScienceDirect. *Datestamping the Bitcoin and Ethereum Bubbles*. Accessed: Aug. 2, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1544612317307419

[38] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[39] D. Bradbury, "In blocks [security bitcoin]," *Eng. Technol.*, vol. 10, no. 2, pp. 68–71, Mar. 2015.

[40] SpringerLink. *Security Analysis of SHA-256 and Sisters*. Accessed: Aug. 2, 2018. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-24654-1_13

[41] R. Silhavy, P. Silhavy, and Z. Prokopová, "Architecture of COOPTO remote voting solution," in *Advanced Techniques in Computing Sciences and Software Engineering*. Dordrecht, The Netherlands: Springer, 2010, pp. 477–479.

[42] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-based e-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, San Francisco, CA, USA, Jul. 2018, pp. 983–986.

[43] L. P. Alonso, M. Gasco, D. Y. M. del Blanco, J. A. H. Alonso, J. Barrat, and H. A. Moreton, "E-voting system evaluation based on the council of Europe recommendations: Helios voting," *IEEE Trans. Emerg. Topics Comput.*, Nov. 2018. doi: 10.1109/TETC.2018.2881891.

[44] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.

[45] Y. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, "TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain," *IEEE Access*, vol. 6, pp. 31077–31087, 2018.
[46] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, Sep. 2018.
[47] Y. Zhang, R. Deng, X. Liu, and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing," *IEEE Trans. Services Comput.*, to be published.
[48] B. Shahzad, "Quantification of productivity of the brands on social media with respect to their responsiveness," *IEEE Access*, vol. 7, no. 1, pp 9531–9539, Jan. 2019.

BASIT SHAHZAD received the M.Sc. degree from the National University of Science and Technology, Islamabad, Pakistan, and the Ph.D. degree from University Technology Petronas, Malaysia. He was a Postdoctoral Researcher with the Computer Laboratory, University of Cambridge, U.K. He was an Assistant Professor with King Saud University, Riyadh, and the COMSATS Institute of Information Technology, Islamabad. He is currently a Visiting Scientist with the University of Cambridge and a Visiting Fellow with Macquarie University, Australia. He is also a Collaborating Researcher with the Hagenberg Centre for Software Competence, Austria. He is also with the National University of Modern Languages, Islamabad. He has numerous publications in journals and at conferences of international repute and has a very active research profile. He has an editorial role in several conferences and journals of high repute and has edited a number of special issues in significant journals in the areas of software engineering, social networks, and mobile healthcare. His research and teaching career spans over 16 years. He is a good Reader and a very good Listener. He is also a Reader of history, poetry, science, and human behavior. He is a Reviewer for several high impact journals. He serves on the Program Committee for several distinguished conferences.

JON CROWCROFT has made pivotal contributions throughout the course of the Internet's development as a means of mass communication. He founded opportunistic networking: how network nodes can use real-time information about their connections to choose how to route data packets toward their destination. He is a pioneer in network technology, having developed the theory and practice of routing data across interconnecting computers. His work on satellite interconnection is helping to bridge the digital divide, enabling remote communities—rich or poor—to have broadband Internet access. He is at the forefront of developing algorithms that can facilitate effective large-scale peer-to-peer networks. His work also extends to investigating social networking sites. He is a former member of the Internet Architecture Board of the Internet Society, which works to promote the development of the Internet for the benefit of all people. In 2009, he received the SIGCOMM Award for lifetime contribution to the field of communication networks.