Smart Voting keys to e-Democracy

Andrew Wolfe
School of Engineering & Technology
University of Washington
Tacoma, WA
awolfewa@uw.edu

Arnold J. Sze
School of Engineering & Technology
University of Washington
Tacoma, WA
szea@uw.edu

Yared Beyene
School of Engineering & Technology
University of Washington
Tacoma, WA
yared@uw.edu

***Abstract*—Voting systems and information technology are used ubiquitously in many countries around the world. It's only logical that the next step is to bring smart electronic voting systems into ubiquity. However, there are various security issues and public challenges right now that surround the implementation of smart electronic voting systems. The main challenges that have been identified here are voter identity and authorization, vote integrity, and voter perception when it comes to smart electronic voting systems. What will be explored will be controls, strategies, and recommendations on how smart electronic voting systems can be better secured and improved upon on. Then they can be introduced to voter populations and be perceived positively.**

Keywords—smart voting, evote, blockchain, biometrics, public perception

I. Introduction

A fundamental aspect of a proper democracy is the ability to hold free and fair government leadership elections for its constituents. It is so fundamental that if an election is not viewed as free and fair, the legitimacy in regard to the democracy of the government that held the election is put into question by the general public. Democratic voting systems have been used by different societies for over two millennia with its earliest known record originating from Athens, Greece during 510 BCE. Regardless of when or whom is holding the election, the ability to effectively and transparently collect votes is universally necessary to a properly functioning democracy. This paper will be explored how smart electronic voting technology can be used to improve and modernize the voting process in the age of smart devices while also considering the core requirements that will lead the public to perceive it as free and fair. Traditional electronic voting schemes are indeed utilized around the world today with mixed results and many concerns surrounding the security of such systems. These traditional electronic voting schemes often have problems that involve insufficient security to mitigate voter fraud, inefficient vote processing, and technological rigidity. Cutting-edge smart electronic voting schemes proposed by researchers utilize biometric authentication, blockchain technology, and central processing units to alleviate the issues that are common in traditional electronic voting schemes. In an effort to synthesize perspectives and recommendations that can be applied to modern democracies in general, findings from a variety of international scholarly journal articles from different countries have been cited. The research cited range from the world's largest democracies to some of the smallest in an effort to find principles that can be generally applied independent of the political entity's size. While there are many societal factors that can impact the nature of an election such as intimidation or disenfranchisement of the electorate by the government, the primary focus will be on the process of casting and collecting votes. What have been identified are three core areas that can impact the legitimacy of a vote; the ability to authenticate the voter, the integrity of the vote that is cast, and the perception of the system as being reliable while also being free and fair.

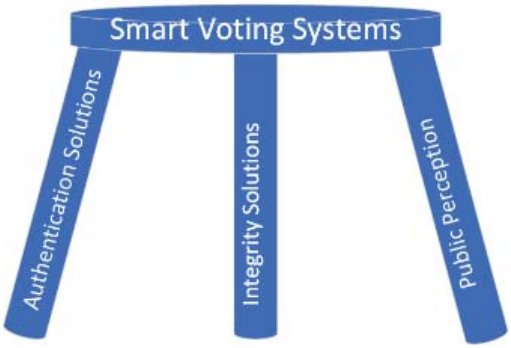

Figure 1 Support for smart voting systems

The metaphorical stool of smart voting systems is supported by the three legs that deal with the three core areas that can impact the legitimacy of the vote. These legs are the concepts of authentication solutions, integrity solutions, and public perception. In Section II of the study we will explore ways to improve the ability to authorize the voter as being a legitimate voter using technology to support the identity and authorization of the voter. In Section III we will study technical methods for maintaining the integrity of the vote data after the vote has been cast. Section IV is devoted to how the perceptions of the voting public and impact the legitimacy of the voting process. In Section V we will provide recommendations and areas for further study on what needs to be improved so that smart electronic voting systems can be effectively implemented into a democracy.

II. Identity and Authorization

The first core area that can impact vote legitimacy is voter authentication. Authentication of identity for authorization is necessary in ensuring beyond a reasonable doubt that a smart

electronic voting system is authentically being used by the registered voter in question. In contrast to the on-site nature of traditional in-person ballot voting, smart electronic voting systems run a higher risk of voter impersonation. Voter impersonation is when an individual assumes someone else's voter identity to either vote illegitimately or to vote multiple times than permitted. The remote nature of smart electronic voting systems comes with a host of unique circumstances and stages in the process where voter impersonation can occur. Therefore, sufficiently strong identity and authentication controls need to be present within smart electronic voting systems in order to deter voter impersonation. While voter impersonation is indeed a problem posed for implementing smart electronic voting systems, concerns of voter impersonation in recent years have been recognized and addressed in other readily used forms of voting such as mail-in ballots. For example, the United States started issuing controls such as voter ID laws that have been put in place since 2010 with the purpose of mitigating voter impersonation.

Biometric authentication is a promising potential option when it comes to access controls for identity authorization within smart electronic voting systems. Biometric authentication relies on the input of the supplicant's physical attributes. These range from body characteristics such as facial features and physical behaviors such as walking gait. Simply put, the biometric authentication system process starts with the initial enrollment scan which is done by the biometric reader in order to obtain scan data from the true party who is creating the identity profile. Next, the mass of enrollment scan data is extracted by the reader for a few key features which will be used during user identification and verification from that point forward. Finally, the reader realizes the biometric template when it sends the key feature data to the database for storage. Due to the nature of biometric key features not being exact matches to the template and the possibility of multiple templates being present from different enrollment scans, major issues with biometric authentication largely stem from access false positives. This is due to the biometric readers often having a match index with flexibility in the decision criteria when scanning for supplicant input to reduce access false negatives. This is due to the fact that replicating the exact conditions present during the enrollment scan such as lighting and positioning is next to impossible. While biometric authorization is in no way foolproof to voter impersonation, biometric data is harder to obtain for authorization in comparison to obtaining Personal Identification Numbers or passwords. Additionally, since biometrics is a physical access control, it to at least some degree counteracts the more remote nature of electronic voting systems and can bolster existing authorization controls to form a multi-factor approach to authorization. In recent years, biometric scanners have become common features in the form of fingerprint scanners on smartphones and face recognition software on laptop computers.

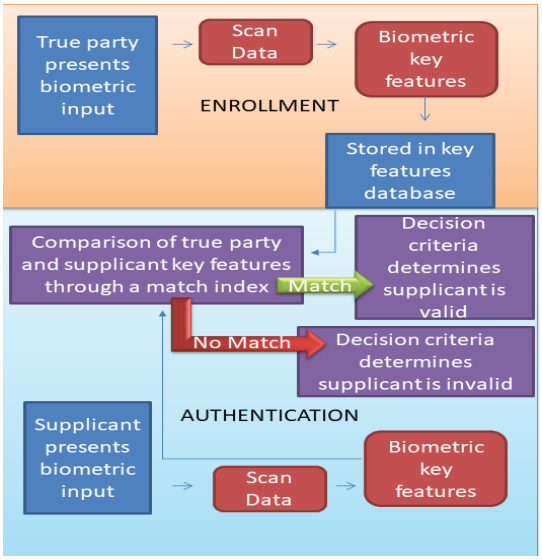

Figure 2 Biometric Authentication Flowchart.

Democratic elections are a significant feature and have a major sway to the minds of the people of India. Furthermore, India's election commission does utilize traditional electronic voting machines. However, these voting machines have been highlighted as having notable issues and are in need of improvements. Specifically, they require too many workers to run, they are known to be time-consuming, and have issues when it comes to being trusted [1]. Researchers throughout India's academic institutions have researched and proposed multiple smart electronic voting systems and strategies that seek to solve the issues they face with the traditional electonic voting machines. In a brief snapshot of techniques, researchers from the Rashtreeya Vidyalaya College of Engineering have proposed a smart electronic voting system that utilizes the Aadhar identification number card, fingerprint scanners, and iris scanners [2]. Researchers from India's D.Y. Patil College of Engineering have also proposed a strategy for a smart electronic voting system with controls in place to prevent electoral fraud in the form of Aadhar based biometric authentication and one-time passwords which will be received on their registered Aadhar linked mobile phone number [3]. Researchers from the V.R. Siddhartha Engg. College have also proposed a secured electronic voting machine that uses the Aadhar identification numbers for authorization and implements fingerprint biometric identification as an additional security layer [4]. Researchers from the Rajalaksmhi Institute of Technology Science have proposed a mobile application electronic voting system that is geared toward efficiency and security. The proposed system brings together cloud storage, biometric verification, and security in an effort to establish trustworthy voting. Access of the cloud storage database and the processing of that data is proposed to be done on the Arduino boards [5]. Now for a more in-depth technique analysis, the Jeppiaar Maamallan Engineering College has researchers that have proposed four different smart electronic voting system concepts that can replace the voting systems currently utilized by India's election commision. These

proposed systems include a fingerprint-based algorithm voting system, a wireless authentication voting system using Zigbee, a radio-frequency identification (RFID) based biometric voting system, and a hybrid system. The fingerprint-based algorithm system and by extension the other systems utilizing fingerprint biometrics are based on the same framework. Which is leveraging biometric identification in the form of fingerprint scanners that utilize templates collected by the government in a stored database. This proposed system is comprised of a 32-bit processor connected to a fingerprint module, a LCD display, a GSM modem, an indicator alarm, a printer, a touch screen, and a personal computer interface hooked up to a personal computer. The hybrid system, the last proposed system, uses a technique that involves generating a hash code from the fingerprints of both hands for stronger security. Vote counting in this voting system is automatically done through Internet of Things (IOT) technology, networks, and devices. This application of IOT technology allows for vote counting and collecting to be done faster and simultaneously. The proposed system is comprised of a PIC16F877A microcontroller connected to a power supply, a display, an IOT processing device, a buzzer, a crystal oscillator circuit, a keypad, and a fingerprint module. This also uses the Global System for Mobile communciations standard [1].

In the developing country of Bangladesh, the traditional voting system is a ballot paper based system. Furthermore, it has been reported that this voting system is rather time-consuming and at times is unfair. Due to this, there is always a problematic amount of unsafe risk that the incorrect candidate is elected through this system. While Banagladesh has very recently introduced electronic voting machines, they lack the necessary security controls to mitigate voter fraud. While a neighbor to India, Bangladesh is considered a low-to-middle income country. This means they lack the resources to implement smart electronic voting systems at the scale that India is capable of. However, smart electronic voting system technology can still produce secure voting solutions that are feasible for Bangladesh. Researchers from the American International University-Bangladesh have proposed a system that utilizes secure digital technology. This is a response to the problems that surround the traditional paper-based ballot voting system and the electronic voting machines currently used in Bangladesh. These researchers propose a system that is based on the electronic voting machine but with the additional feature of biometric security using voter fingerprints as inputs. Through this way, the system can identify each voter, keep track of votes, and stave off illegitimate votes through the use of the electronics platform Arduino and fingerprint scanners. This system intends to mitigate unregistered voters from casting votes and registered voters from casting additional votes. The voting system is intended to easily authenticate and verify identity but also have high accuracy and reliablity rates. Additonal considerations from the research team included creating a unique system that is cost-effective and time-efficient. The research team had also looked at a seperate internet-connected Aadhar card-based voting system from Indian researchers. Through looking at this advanced voting system, they decided that the system they create should not appear complicated to the user and should not be connected to the internet due to the risks associated with online systems. The user-friendly interface will include an LCD display and analog buttons. This proposed system will receive the fingerprint input of the supplicant through a scanner module. Subsequently, it will then attempt to match the input with a pre-existing template within the fingerprint database of registered voters. The system will then utilize its 32-bit CPU to determine if the fingerprint input falls within the match index of a registered voter that has not yet voted. An input that successfully meets match index criteria will result in the authorization of the supplicant to vote. This proposed system is also designed to allow users to change their vote one-time in the event of a mistake and only during the confirmation step of the initial vote. As standard to electronic voting machines, this system can count up votes for each candidate. After a priorly specified period of time, this system can then display the result when the voting period is over on its LCD display [6].

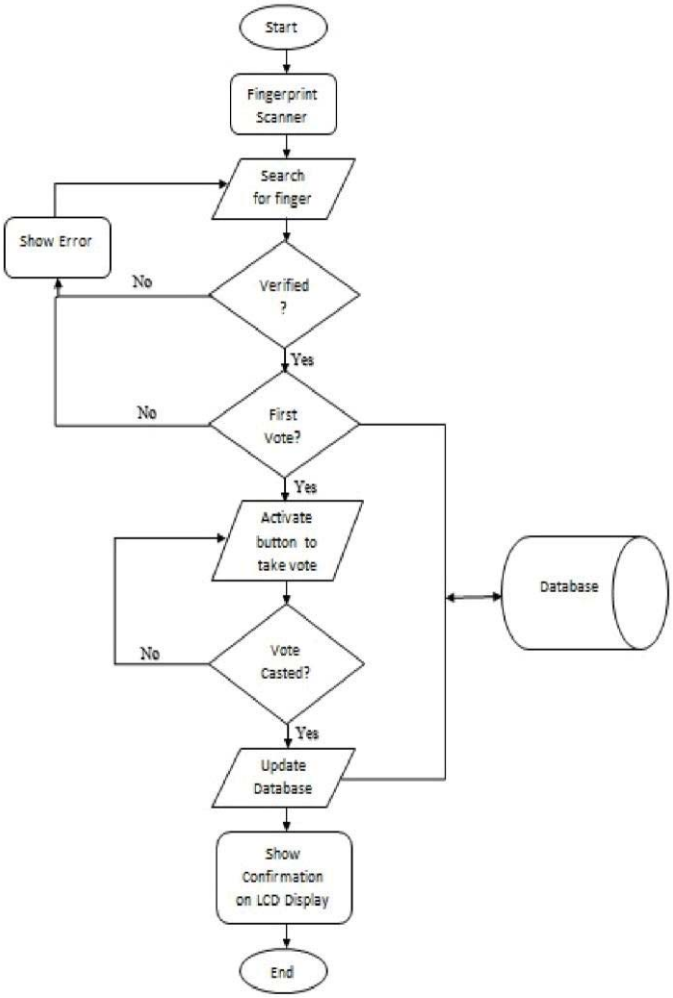

Figure 3 American International University-Bangladesh Research Team Proposed System Flowchart [6].

Voter impersonation in the form of unregistered voters casting votes and registered voters casting additional votes is also a concern surrounding the implementation of electronic voting systems in the United Kingdom. Numerous electronic voting schemes handle vote casting and tallying by trusting polling station officials to properly authenticate voters. This method assumes a trustworthy environment and as a result has the risk of being abused for voter fraud by voters and polling station officials that act improperly. In generally benign environments, the assumption of trust is reasonable. However in untrustworthy and highly-coercive environments, greater authentication security is necessary to mitigate voter impersantion along with electroral fraud such as vote buying and selling. At the Royal Holloway University of London, researchers propose utilizing biometrics and digital signatures for ballot authentication in voting environments that have the potential to be untrustworthy. In their project, untrustworthy voting environments are defined as environments where complete trust cannot be placed on polling officials and voting terminals. This is due to the possibility that the voting system has been compromised due to factors such as unitentional operation lapses or intentional usage of malware. The team has also observed voting schemes where protocol weaknesses allow for the exploitation of casting votes under the identity of abstaining voters due to cast votes not being signed by voters. Additional security threats mentioned involve the illegal distribution and manipulation of voting channels such as smartcards and tokens. In response to these threats, the research team at the Royal Holloway University of London has highlighted three primary security requirements for countermeasures. The first security requirement is eligibility verificability, where only voters who are elligible are authorized to vote and cannot vote multiple times. Next, the second security requirement is receipt freeness, where the voter cannot obtain information that can indicate to a coercer how the voter voted. Finally, the third security requirement is privacy, where voters should not be linked to votes in a way that can indicate to anybody how a voter casted their vote. The Royal Holloway University of London research team proposes a biometrics-based mutual entity authentication protocol that ensures proper vote eligibility. The checking done by the biometrics component mimimizes the trust placed on polling equipment and officials. Furthermore, the system utilizes a tamper-proof voting smart card that holds the biometric template of the true party and can carry out cryptographic functions such as digital signatures. The protocol in an overview is comprised of initialization, card terminal authentication, voter verification, and lastly card and issuing authority authentication. Firstly, the initialization process involves a message exchange handshake to start authentication. Secondly, card terminal authentication involves the mutual authentication of the voter smart card and voting terminal using cryptographic functions. Thirdly, voter verification provides assurance that the voter smart card and supplicant is legitimate by match indexing the biometric input on the smart card and asking for a personal identification number from the supplicant. Lastly, the card and issuing authority authentication phase has the voter smartcard and issuing authority share a symmetric key which is utilized to create a media access control over a set of data that the two both verify. In this phase, the voter smartcard also signs messages using digital signature to prevent entities from exploiting the identity of abstaining voters and voting using those identities. An existing re-encryption mix-net scheme incorporated into the voting system contributes to a layered approach that ensures voter anonymity. This is done through the mix-net taking a set of encrypted ballots, re-encrypting them, and creating a set of encrypted ballots that are incapable of being linked to the original input value. The researchers at Royal Holloway University of London have shared that they have not formally verified the mix-net voting scheme and suggest that anonymity, universal verifiability, privacy, and robustness should be further looked upon in this area for future research [7].

As democracy is very much a defining feature of the United States government, it comes to no surprise that researchers from the University of Pittsburgh have proposed a vision to modernize the United States voting processes. This is illustrated through the vision of creating a secure, privacy-preserving, resilient and transparent national electronic voting framework that utilizes policies, standards, federal entities, and technological infrastructure. Strategic processes are also in place to enhance voter trust by taking advantage of the observed link between democracy confidence and election infrastructure trust. The researchers at the University of Pittsburgh believe that the biggest threat to democratic institutions around the world is the creation of disinformantion, distrust, and social discord by capable threat agents. The researchers have also cited the use of insecure and unreliable electronic voting machines across the United States resulting in missed voter tally calculations and security vulnerabilities. Moreover, each state purchases their own voting machines and establishes their own voting rules. As a result, old hardware and software along with a lack of adequate funding are issues of varying severity across the country. The University of Pittsburgh researchers have proposed a National E-Voting framework that will include country-wide policies, technological infrastructures, along with standards and processes to remediate the aformentioned problems. National policy funding and equipment standardization is proposed as an approach to easing state and local government financial burden and standardizing equipment nationwide. Additionally, integrated circuit chips in state ID cards capable of digital signatures and hash functions will be standard through this funding. The issue of supply chains from outside of the United States producing key voting machine components with malicious spyware software and hardware is also brought up. The proposed solution for this is to mandate that key voting machine compenents are developed within the United States. The platform design incorporates biometric scanners that take fingerprint, retina, or face characteristics as input to authenticate every user for transparency and accountability. The initial enrollment scan will happen through a proposed Congress mandated policy of biometric civil registry for American citizens starting at 15 years of age. What is intriguing and concerning about this proposition, is that the

privacy of the true party is sacrificed for the assurance of identity that comes with the registry. What is also incorporated is a Zero Trust framework. This is an approach that leverages existing technologies to reduce the need to rely on entities that are too unsafe and unacceptably suseptible to corruption or error. This also means the burden of responsibliltiy of addressing national electronic voting security should not rest solely on local and state government who lack technical expertise to effectively understand and address the cybersecurity threats. This framework incorporates the use of emerging blockchain technologies to provide depth to the electronic voting infrastructure and to assist in fostering voter trust in the same infrasturcture. Due to blockchain being an emerging technology, the research team has shared that the creation of a national level blockchain infrastructure and its governance is an issue that needs to be addressed within their proposed framework [8]. Blockchain technology will further be explained and expanded on in the following section.

III. Vote Integrity and Blockchain

The second core area that impact vote legitimacy is the integrity of the vote being cast. Fraud protection is needed to ensure vote data integrity. Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as increased efficiency and reduced errors [9]. The traditional E-Voting system improved the way votes are cast and counted. However, it lacks the mechanism to secure vote data integrity. The main issue of the current conventional voting system is the possibility of fraud in the electoral system itself [10]. In the existing e-voting solutions client-side and server-side compromises are the main concerns in e-voting system that result in voter's data manipulations. Voters need to make sure the integrity of their casted vote, its accessibility, and anonymity.

Blockchain-based e-voting systems has a potential to solve problems related to voting integrity, accessibility, and anonymity. The basic characteristics of blockchain technology are empowering the user, no third-party risk, transparency, and Authenticity. These characteristics are critical in conducting the fair and free election in a democratic system. Traditional Smart voting or e-voting system improved the manual voting process. However, there are still challenges to resolve contrasting yet vital components in voting systems such as privacy vs. transparency, flexibility vs. integrity, and fairness (openness) vs. security. Voters perception, which will be discussed in detail below, and trust are critical in voting systems. Blockchain offers the security and transparency requirements that so far lacked in the electronic voting systems adopted in various countries [11].

The intention of this paper is not to explain Blockchain technology; however, it will attempt to sets the stage by explaining the fundamentals of the technology. A blockchain is a transaction ledger containing a series of blocks chained together linearly. To understand the purpose of blockchain it is important to understand the problem it is designed to solve. Transaction, trust, and social institution are the core of blockchain technology, especially the loss of faith in social institution. The technology is designed to complete transaction securely between two parties without the interference of a third party. Blockchain application is based around the concept of decentralization. Regulation, decision making, and relationship are managed individually instead of centrally. Blockchain, at its core, is a linked list. However, instead of a using pointer function, blockchain uses a hash function. Blockchain uses layers of cryptography to protect user data. There are different types of blockchains, public, federated, and private. Most preferred blockchain type for the e-voting system is private blockchain.

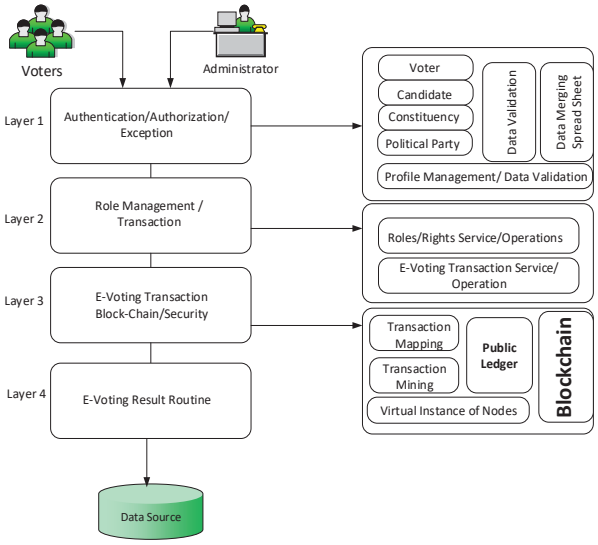

Figure 4 Architecture for proposed e-voting system with blockchain [9].

Countries such as Estonia have implemented and shifted into the online voting poll for their elections [12]. The country established e- Identity cards that allow a citizen to access government service. Such a platform creates a conducive stage for a blockchain e-Voting system to be secure and functional. However, in their 2013 elections, some number of potential security risks was highlighted, where the risks are some possible malware in the clients and servers that allows change of votes [13]. Estonia's e-voting system is based on the traditional client-server model that has a client-side and server-side vulnerability. To resolve this the country proposed the implementation of the blockchain technology in the voting system [13].

Blockchains have been the subject of mainstream research of the past decade because of its decentralized, peer to peer transactions, distributed consensus, and anonymity. It is these characteristics that provide a strong fit for the e-voting purpose [14]. While blockchain has a strong fit for the e-voting purposes it is not a complete solution due to technical issues around how the chain can be manipulated. A solution for the short comings of blockchain is to couple blockchain with smart contracts. Researchers at the University of Reykjavik identifying three parts to define smart contracts (1) identifying the roles that are

involved in the agreement (the election agreement in our case), (2) the agreement process (i.e., election process), and (3) the transactions (i.e., voting transaction) used in the smart contract [15]. Like we stated earlier the preferred blockchain types is private using a proof of stake. Based on these researchers at the university of Reykjavik University identified using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second [15].

The ability combining smart contracts and blockchain is able to solve some of the problem in contract signing, problem of fairness in a multiparty protocol, which are impossible without a blockchain structure. Some of the thing that are mathematically impossible now become possible with at least the idea of blockchain. Goldwasser stated that it is known that there are differences between theory and practice, but that doesn't mean that we should stop pursuing developing these technologies. Cryptocurrencies remains the most distinguished application of blockchain however researchers at NED University of Engineering and Technology and University of West London are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits as non-repudiation, integrity and anonymity [9].

IV. Voter Perception

The third core area that can impact vote legitimacy is the perception of the system as being reliable while also being free and fair. Currently today the gold standard in vote perception on a secure and reliable vote system is a paper ballet that is marked by the voter and placed in a locked box by the voter. While this has a great perception in the voting public there are many technical challenges with this type of vote being both easy to process and secure from tampering. In addition to the technical merits of any e-voting solution both in the authentication and in the integrity of the solution the perception will be critical to the adoption of the solution by the general population. The perception of the electorate can be measured in voter trust in the integrity and validity of the solution regardless of the technical merits of a solution. If there is not a strong measurable acceptance of the results of the vote this reflects a lack of trust in solution and it will fail to be an effective e-voting solution. The perception of the election system is an important factor in the mandate of any person elected by it and an attack on the perception of the system could be as damaging as an attack on the system itself [16]. For this reason not only the technical merits of a given solution must be considered but the perceptions of the voters of the system must be managed as well.

There is a strong interest in the expansion of e-voting as a way to use technology to assist in greater participation by the electorate in choosing their leaders [17]. When looking at the ability of a government to move to an e-voting system there are two broad categories of areas that will increase the voters trust of the e-vote system. There are many societal factors that will increase the acceptance of the system; trust in the internet, trust in the government, attitudes towards technology, beliefs and general skills with technologies [17]. In Estonia the launch of e-vote was very successful which was attributed to the level of internet penetration and e-readiness among the citizens. Estonia also already has some technical solutions in place to support the trust in the systems including a digital identification system for citizens, and government IT programs [13]. Beyond these general societal climate factors for the acceptance of an e-vote there are technical issues that must be addressed; there must be a perceived usefulness of e-voting and a perceived ease of use of the e-voting system [17]. For the implementation of an e-voting system to have success all of these elements must be present and if not would be considered precursor education and infrastructure efforts before a technical solution can be introduced to the voting process. This can be seen in the successful e-voting carried out in Nigeria where five critical elements were identified that the system must have availability, privacy, ease of use, and reliability for the population to feel trust in the outcome of the election [18]. An additional area that can be seen to improve the populations confidence in an e-vote can be seen in the Argentina use of e-voting is the perceived competence of the poll works. When there are issues in voting the voter's confidence of the vote outcome is decreased so where a highly qualified poll work that can quickly solve issues for the voter is critical to the perception of the legitimacy of the vote [19].

As can be seen in Table 1 There are only two very strongly correlated factors that can drive an increase in the confidence of the voters in the vote being recorded correctly and in their vote being private. The voter having a positive view of the use and impact of technology in the voter's daily life has a strong positive correlation on the voter's confidence in the voting system and outcome. This is useful information but is difficult for the government to directly impact so while important to understand it is not an area that can be addressed in the planning for the roll out of a e-voting system. The second area that has a very strong positive impact on the voter's confidence is the competence of the poll works at the voting site. If the poll workers are seen as competent and understand the system, then voters feel that the system is also effective. In this area the government can most positively impact the roll out of an e-voting system by making sure that there is the correct level of training for all poll works in the e-voting system operation, so they are confident in supporting voter questions and ability to vote using the system. As again seen in Table 1 even if the voter has a problem or needs help this does not strongly impact their view of the voting process as long as the poll workers that are supporting them are seen as competent in helping with the issue at hand. It is also important to note that in the study run in Argentina many factors that may seem important in impacting the voter confidence did not seem to have a strong indicator either positive or negative on the perception of the vote. Areas like previous experience with e-voting, experience with technology, or even having higher levels of education all did

not show a consistent impact on the perceptions. This would strongly suggest that many environmental factors do not need to be addressed but the training of the poll workers can make or break a roll out of an e-voting system. This lack of problems and in general ease of use was again seen in the use of e-voting in Greece where there was a clear relationship in exit surveys between the perceived ease of use and the confidence in the quality of the e-vote process, though this was a weaker relation than in other examples [20].

	Confident Vote Recorded			Confident Vote Private		
	Effect	95% C.I.		Effect	95% C.I.	
Problem Voting	-6.9	-14.8	0.2	-11.0	-20.0	-2.0
Poll Worker Competent	**16.6**	**10.6**	**22.6**	**23.3**	**15.7**	**19.9**
Previous e-voter	-0.1	-6.1	5.7	2.9	-4.0	9.4
Positive view of technology	**8.0**	**4.6**	**10.9**	**12.4**	**8.0**	**17.0**
Use of technology	-0.7	-6.6	4.6	-3.6	-10.8	3.6
Needed help to vote	-3.0	-12.2	5.3	-1.5	-12.2	9.5
Education	-2.7	-6.9	1.8	0.3	-5.1	5.4

Table 1 Confidence Factors from Reference [20] showing positive and negative impacts of different factors present in an e-voting system

V. Recommendations and Areas for Further Study

An area that we feel has not been adequately covered in the study of e-voting systems is how the three areas of this study interact and support each other in a holistic approach to the problem. Much of the study of the area of e-voting has revolved around a single technical area with on occasion a brief nod to the social considerations. It is the strong contention of the authors that only by viewing the issues that surround e-voting in a full system approach we will not achieve a complete solution. The base for any additional work that we recommend should be viewed as being suggested in the context of how that area for research would be influenced by all three legs of the E-voting stool of authentication, integrity, and public perception.

It has been demonstrated that electronic voting is a key area for governments to increase voter participation in the democratic process. Exploration into biometric technologies as a means to authenticate voters has been addressed. While biometrics are a well-developed technology there are issues with the public willingness to enroll in the system. While it is generally believed that the validity of the person voting is required the voters will need to give up some level of privacy to the government to ensure more accurate identification for voter authorization. The willingness of the population to provide needed biometric data for voter authorization will be an area for further study as well as ways to insure the data is protected for voter privacy. Recommended technologies such as blockchain for vote data integrity. However, the technology needs more development and further study before the deployment of national voting infrastructures that can support smart electronic voting. Blockchain-based voting systems are still in an experimental stage and need more research and exploration. The technology is instrumental in implementing end-to-end verifiable transaction which is critical to an online voting system. In its role as a trusted service application, blockchain technology comprises end-to-end functionality by facilitating highly specialized applications for any purpose imaginable [21]. Further studies will be needed to help augment blockchain based e-voting systems to be a more constant, dependable, and scalable platform for e-democracy. Establishing trustworthy provenance for e-voting systems will be crucial to achieving an end-to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional province layer to aid the existing blockchain infrastructure [9].

Three core areas have been identified that can impact the legitimacy of a vote. The first core area being the ability to authenticate the voter, which smart voting schemes have proposed to solve through various biometric authentication methods. Then the second core area being the integrity of the vote that is cast, which smart voting schemes address through leveraging the decentralized nature of blockchain. Finally, the third and last core area being the perception of the system as being reliable while also being free and fair. It is a core requirement that the government that is looking to introduce an e-voting system plan carefully the training of the poll workers that will be the most visible indication of the system being effective. It is critical that the poll workers are competent for the voters to have confidence in the system. The voter's confidence in the system is also by the ease-of-use that smart devices afford to the user. If the smart device that is used in the e-voting system is seen as easy to use, then the voters have a greater confidence level that the system is working correctly. Both factors can impact the perceived security along with impartiality that smart voting systems provide to the general public. There are not enough studies for public perception drivers though and the studies that have been cited need to be repeated and expanded both in scope and geographic diversity to continue to build a strong understanding of how to best drive the public perception of the e-voting system independent of the technical merits of the system.

VI. Acknowledgment

This research was conducted as a part of the Masters of Cybersecurity and Leadership (MCL) program at the University of Washington Tacoma. The authors also wish to thank Dr. Yan Bai for her insights and guidance as we developed our research.

References

[1] J. Deepika, S. Kalaiselvi, S. Mahalakshmi and S. Shifani, "Smart Electronic Voting System BasedOn Biometric Identification-Survey," in *Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, 2017.

[2] S. Kavitha, K. Shahila and P. Kumar, "Biometrics Secured Voting System with Finger Print, Face and Iris Verification," *2018 Second International Conference on Computing Methodologies and Communication (ICCMC),* pp. 743-746, 2018.

[3] S. Patil, A. Bansal, U. Raina, V. Pujari and R. Kumar, "E-Smart Voting System with Secure Data Identification Using Cryptography," *2018 3rd International Conference for Convergence in Technology (I2CT),* pp. 1-4, 2018.

[4] J. Lakshmi and S. Kalpana, "Secured and Transparent Voting System Using Biometric," *2018 2nd International Conference on Inventive Systems and Control (ICISC),* pp. 343-350, 2018.

[5] T. Illakiya, S. Karthikeyan, M. U. Velayutham and R. N. T. Devan, "E-Voting System Using Biometric Testament and Cloud Storage," *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM),* pp. 336-341, 2017.

[6] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and A. Rahman, "Biometrically Secured Electronic Voting Machine," *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) ,* pp. 510-512, 2017.

[7] V. Augoye and A. Tomlinson, "Mutual Authentication in Electronic Voting Schemes," *2018 16th Annual Conference on Privacy, Security and Trust (PST),* pp. 1-2, 2018.

[8] L. Carr, A. J. Newtson and J. Joshi, "Towards Modernizing the Future of American Voting," *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC),* pp. 130-135, 2018.

[9] K. M. Khan, J. Arshad and M. M. Khan, "Secure Digital Voting System Based on Blockchain Technology," *International Journal of Electronic Government Research,* vol. 14, no. 1, pp. 53-62, 2018.

[10] F. H. K. Z. A. I. M. Y. N. M. T. Nur Sakinah Burhanuddin, "Blockchain in Voting System Application," *International Journal of Engineering & Technology ,* vol. 4.11, no. 7, pp. 156-162 , 2018.

[11] F. Fusco, M. I. Lunesu, F. E. Pani and A. Pinna, "Crypto-voting, a Blockchain based e-Voting System," in *Proceedings of the 10th International Joint Conference on Knowledge Discovery,*, Cagliari, Italy, 2018.

[12] N. K. a. J. Voas, "Blockchain-Enabled E-Voting," *IEEE Software,* vol. 35, no. 04, pp. pp. 95-99, 2018.

[13] N. Mpekoa and D. Van Greunen, "E-voting Experiences: A Case of Namibia and Estonia," in *IST-Africa* , Windhoek, Namibia , 2017.

[14] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use cases in Blockchain Technology," in *9th ICCCNT 2018* , Bengaluru, India, 2018.

[15] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," in *IEEE 11th International Conference on Cloud Computing*, Reykjavik University, Iceland, 2018.

[16] Q. Yao, M. Zhao, Y. Li and Z.-M. Gao, "A Trust and Risk Based Dispute Settlement Mechanism in E-Voting," in *Proceedings of the Eighth International Conference on Machone Learning and Cybernetics*, Baoding , 2009.

[17] M. K. Alomari, "Towards E-democracy in the Middle East: E-voting Adoption," in *9th International Conference for Internet Technology and Secured Transactions*, 2014.

[18] O. Osho, V. L. Yisa and O. J. Jebutu, "E-Voting in Nigeria: A Survey of Voters' Perception of Security and Other Trust Factors," in *2015 International Conference on Cyberspace Governance* , Abuja , 2015.

[19] J. Pomares, I. Levin, R. M. Alvarez, G. L. Mirau and T. Ovejero, "From Piloting to Roll-out: Voting Experience and Trust in the First Full e-election in Argentina," in *2014 International Conference on Electronic Voting* , Lochau/Bregenz, Austria , 2014.

[20] A. Delis, K. Gavatha, A. Kiayias, C. Koutalakis, E. Nikolakopoulos, L. Paschos, M. Rousopoulou, G. Sotirellis, P. Stathopoulos, P. Vasilopoulos, T. Zacharias and B. Zhang, "Pressing the Button for European Elections Verifiable e-voting and Public Attitudes Toward Internet Voting in Greece," in *2014 International Conference on Electronic Voting*, Lochau/Bregenz, Austria, 2014.

[21] K. Sultan, U. Ruhi and R. Lakhani, "CONCEPTUALIZING BLOCKCHAINS: CHARACTERISTICS & APPLICATIONS," in *11th IADIS International Conference Information Systems*, Ottawa,Canada, 2018.