Evaluating the Public Perception of a Blockchain-Based Election

Vincent Schiarelli
vds7@uw.edu
University of Washington
Bothell, Washington, USA

Marc Dupuis
marcjd@uw.edu
University of Washington
Bothell, Washington, USA

ABSTRACT

The concept of voter confidence was introduced into the political domain after the contentious recount of the 2000 United States presidential election results in Florida. Twenty years after this election, the concept of voter confidence has made headlines again as record low number of voters express confidence that votes will be accurately cast and counted nationwide. Even in the absence of specific security concerns regarding vote tabulation, the low voter confidence elicited by our existing voting infrastructure has impacts to our democratic institutions. As an alternative to existing voting infrastructure, some have proposed incorporating blockchain solutions into electoral systems. While blockchain could add additional transparency through mechanisms such as the public ledger and decentralized accounting, blockchain's impact to voter confidence may not be straightforward. This project seeks to evaluate the public's confidence in the ability of a blockchain-based voting system to fairly and accurately tabulate votes. To measure this confidence, the Technology Acceptance Model was leveraged so that we could quantify the relationships between individuals and their perception of blockchain technology. A between groups experiment was performed to measure these relationships.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; **Formal methods and theory of security**; **Human and societal aspects of security and privacy**; • **Applied computing** → **Command and control**; **Enterprise computing**; • **Information systems** → *Information systems applications.*

KEYWORDS

blockchain, voter confidence, elections, cybersecurity, information integrity

ACM Reference Format:
Vincent Schiarelli and Marc Dupuis. 2023. Evaluating the Public Perception of a Blockchain-Based Election. In *The 24th Annual Conference on Information Technology Education (SIGITE '23), October 11–14, 2023, Marietta, GA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3585059.3611439

SIGITE '23, October 11–14, 2023, Marietta, GA, USA

ACM ISBN 979-8-4007-0130-6/23/10.
https://doi.org/10.1145/3585059.3611439

1 INTRODUCTION

In the weeks prior to the 2020 United States general election, a Gallup poll found that 59% of Americans were either very or somewhat confident that votes would be accurately cast and counted throughout the country [15]. This figure is equal to the lowest voter confidence recorded by Gallup in 2008. In the weeks following the election, the Pew Research Center had a similar finding which identified that only 59% of voters felt that elections were run and administered well [7]. These surveys provide a general sense of voter confidence in the electoral process.

While the reasons for low voter confidence are varied, it is reasonable to consider the use of other secure vote counting mechanisms in an attempt to increase voter confidence. The use of blockchain in the election process is one mechanism being studied for this purpose [26]. Historically, electronically-based ballots instill less confidence than paper ballots [3]. One of the potential reasons for this lower confidence is that the traditional electronic systems appear to be a black-box to the voter. The more open nature of a public ledger that can be provided via blockchain may be able to counteract the lower voter confidence, and the decentralized nature of blockchain could assuage concerns of improper vote counting.

1.1 Blockchain

The concept of the blockchain can roughly be traced back to Haber and Stornetta, who proposed a concept for a chain of timestamps, which could be used to timestamp digital data [18]. However, the more recognizable modern blockchain was conceptualized by someone under the pseudonym of Satoshi Nakamoto, who developed the framework for the Bitcoin cryptocurrency [27]. This blockchain allows for secure peer-to-peer transactions to take place in a decentralized manner, obviating the need for a central authority to manage transactions.

While this system works well for financial transactions, a blockchain intended for vote tallying would have significant design modifications. As an example, Bitcoin mining nodes verify transactions because they are paid transaction fees to do so [27]. In a theoretical vote tabulating blockchain, there is no transaction to levy a fee against. Additionally, there is a perverse incentive for mining nodes to not include votes that are contrary to the node owner's voting preferences. A blockchain-based election system would need to address concerns such as these.

1.2 Voter Confidence

The modern concept of voter confidence was born in the aftermath of the 2000 United States presidential election, in which confidence in the administration of elections was thrown into question during a contentious recount in the state of Florida [38]. In future elections,

Gallup began to measure voters' confidence that votes will be accurately cast and counted in that year's election [15]. The concerns surrounding voter confidence evolved over the next twenty years, with the problem coming to a head in the period surrounding the 2020 presidential election. During this time, unsubstantiated claims of voter fraud by political leaders and their supporters ran rampant on social media and other media outlets, undermining voters' confidence in the election results [4].

Understanding voter confidence is important since there is a strong relationship between voter confidence and future turnout decisions [3, 23]. Stated another way, individuals may choose not to participate in elections if they do not trust that their vote will be counted.

2 RELATED WORKS

The use of blockchain for elections has become a popular area of research. Many proposed implementations provide a solid foundation for developing a usable system. However, requirements for the administration of elections are meticulous, and meeting these requirements in a decentralized manner is challenging.

In evaluating the suitability of a particular system for public use, a subset of electronic system voting requirements were selected from a list developed by Johns Hopkins University [6]. The following requirements were chosen based on the impact that the use of blockchain has on the ability of the system to meet the requirement.

- Voter Authenticity – Ensure that the voter must identify themselves to be entitled to vote.
- Data Integrity – Ensure that each vote is recorded as intended and cannot be tampered with in any manner.
- Secrecy / Privacy – No one should be able to determine how any individual voted. This also includes securing the vote total through completion of the voting period.
- Non-coercibility – Voters should not be able to prove to others how they voted.
- Availability – Ensure that the system is protected against accidental and malicious denial of service attacks.
- System Disclosability – The core of the system shall be open-source to allow external inspection and auditing.
- Distribution of Authority – The administrative authority shall not rest with a single entity.
- Convenience – The system shall allow voters to cast their votes quickly and in one session.

2.1 Voting via Smart Contracts

Hjalmarsson et al. evaluated the use of blockchain as a service with voters executing smart contracts [20]. Smart contracts are programmable contracts that automatically execute when pre-defined conditions are met. In this case, voters execute the contract, which is preloaded by election administrators with all of the necessary information regarding each race in the election. Results can then be tallied on the fly as a part of contract execution.

One drawback of this design is the difficulty in securing the vote total until the casting of ballots has been completed. Even with a permissioned blockchain, significant distribution of the blockchain between district nodes creates a wide distribution of the in-process vote total. This could create an unfair advantage if candidates could see live vote totals and adjust electoral strategies accordingly. This system also explicitly allows voters to retrieve their voting transaction from the blockchain, potentially creating a concern that votes could be coerced. Based on these drawbacks, the system does not meet the secrecy and non-coercibility requirements.

2.2 Double Envelope

Adiputra et al. discuss a system that combines the idea of double envelope encryption and blockchain technology [2]. Voters secure their ballot by first encrypting the ballot with the public key provided by the election authority (the inner envelope). The voter then signs the encrypted ballot with the use of their personal private key (the outer envelope) before sending the ballot to be included on the blockchain. At the conclusion of voting, the election authority releases the private key used to encrypt the ballots, allowing for votes to be counted. This ensures that the vote total is secured until the conclusion of voting.

This design utilizes a public proof-of-work blockchain. The idea is proposed that the individual voters are also miners, creating the blocks that are appended to the blockchain. By the authors' own admission, there is limited incentive for voters to expend effort in mining blocks for this blockchain. Additionally, when the scale of the election is small, it may be feasible to gain 51% of the blockchain mining capability, enabling control of which votes are appended to the chain.

Based on the existence of the 51% problem and the fact that voters can vote more than once, the data integrity requirement is not met for this system. Additionally, the multi-vote paradigm used in this system does not obfuscate the number of revotes performed by the voter. Therefore, anyone could determine the final cast ballot of a particular voter. This means that the non coercibility requirement is not met.

2.3 Voter Anonymity

Dimitriou offers a robust system that bases security on the use of token randomizers, which are hardware devices that are tamper-resistant [10]. The actual use of blockchain in this system is somewhat abstract, however, a well-defined process for anonymizing a voter's identity is presented. This methodology protects against a voter being coerced, since a voter cannot prove that a particular ballot belongs to them.

While secure, this system creates procedural issues in its practical implementation. For example, some voters may not understand that there are actions required before and after voting so that a valid ballot is created. Additionally, if a voter loses their token randomizer after creating the commitment, they cannot create a valid ballot under this system. For these reasons, this system does not meet the convenience requirement.

2.4 Requirements Summary

In order to best meet all of the presented requirements, portions of each of the designs discussed above were codified into a model system. This model system forms the basis of a survey that is used to evaluate the public's confidence in a blockchain-based election system. The authors note that other blockchain-based voting systems were reviewed as a part of the survey preparation. However,

the systems presented above were found to be best suited for illustrating the concepts that would be included in the model system presented to survey participants.

3 METHODS

To determine users' trust level in blockchain applications, Völter et al. evaluated the effectiveness of trust signals addressing familiarity, information, and reliability in combination with social effects [37]. Participants were briefed on a scenario and given basic information about blockchain technology. They were presented one of four interfaces and asked to interact with the interface by adding four transactions to the ledger. This type of experiment allowed for measurement of the difference in trust between the four different interfaces. At the end, participants filled out a questionnaire to capture their level of trust in the given interface. Trustworthiness was measured via questions on a 7-point Likert scale (1 = Not at all, 7 = Extremely). This methodology of performing a between-groups experiment followed by a questionnaire will be utilized for this project.

3.1 Proposed Blockchain System

In order to perform a between-groups experiment, a model blockchain-based election system must be developed in order to brief participants. Due to the limited time that participants have, briefs will be presented at a high level in order to best communicate the relevant concepts. Therefore, the technical implementation details will not be determined herein. However, the overall system design must be scrutinized to ensure that requirements are met.

3.1.1 Voter Participation Mechanisms. Many blockchain-based voting systems focus on creating a viable remote voting platform, such as the application developed by Voatz for the 2018 federal election in West Virginia [34]. However, this project seeks to view the use of blockchain through a different lens. Blockchain can be thought of as an accounting system that tracks transactions on an immutable public ledger. In the context of elections, the use of traditional polling places and paper ballots could still be maintained while utilizing a blockchain-based tabulation methodology.

Therefore, for this experiment, one can assume that the mechanisms with which voters traditionally interact (e.g. voting machines, paper ballots, etc.) to submit ballots remain unchanged. The difference here is that the tabulation will involve the use of a public ledger, which makes the election process more transparent.

3.1.2 Consensus Mechanism. Two popular consensus mechanisms used in cryptocurrencies are proof-of-work and proof-of-stake. As discussed previously, proof-of-work is not feasible due to the lack of incentive for miners and the possibility of an adversary gaining 51% of the computing power in the mining network. Proof-of-stake typically requires users to stake some sort of collateral on their ability to validate new blocks on the blockchain. The staker is then compensated for successfully validating the new transactions. As with proof-of-work, the election model does not offer incentive for the staker to act honestly.

Therefore, a permissioned blockchain using proof-of-authority is a more reasonable approach in the election case. A number of trusted institutions could be given the authority to operate validation nodes which validate and append legitimate ballots to the blockchain. This architecture would allow public visibility of the blockchain without the need to trust unknown entities. This design also accounts for a number of validation nodes to be compromised or unavailable, as long as at least half of the nodes remain secure and available. While this mechanism still requires voters to trust specific entities, the trust is decentralized and an improvement over having a single authority responsible for tabulation.

3.1.3 Securing Ballots Through Voting Period. To secure the vote total until the voting period is over, each voter must encrypt their ballot with a key that is not revealed until the conclusion of voting. While there are many processes that could achieve this, there are two straightforward methods: a voter-provided key and an election authority-provided key.

The use of asymmetric encryption does create concern of lengthy decryption times. However, this concern is minimal in practice. A desktop computer with an Intel i7 processor has been shown to perform a 1 kB file decryption with a 256-bit elliptic curve key in 17.27 ms [17], resulting in more than 200,000 decryptions per hour. Considering that there were just over 4 million ballots cast in the 2020 United States presidential election in Washington state [29], all Washington state ballots could likely be decrypted by 20 average computers in one hour.

3.1.4 Coercion-Resistance. Unfortunately, this is the most difficult voting requirement to fulfill, as it nearly contradicts the goal of ensuring that an individual's ballot is properly counted. Coercion resistance generally means that voters cannot prove to someone else (potentially a coercer) how they voted. This, in turn, makes it difficult to prove to the voter that their vote was fairly counted.

There are typically two types of coercion-resistant electronic voting systems; revoting and fake credentials [24]. Revoting systems allow voters to vote multiple times, allowing them to recast a ballot that may have been coerced. On its face, this type of system violates the data integrity requirement by allowing voters to vote more than once. With fake credentials, a voter could cast a fake ballot with fake credentials if coerced, following up later by casting the true ballot with their true credentials.

Each voter could be provided with two ballots, one marked as the true ballot and one marked as the test ballot on a perforated section of the paper. If the voter chooses to utilize the test ballot, then both ballots are filled out and the perforation removed. The ballots now appear identical with the exception of a QR code which encodes the identifier (or lack thereof) in the ballot. Both ballots are then mailed in and processed.

3.2 Technology Acceptance Model

To evaluate participants' overall impression of the proposed system, a model for evaluating their acceptance of blockchain technology must be used. The Technology Acceptance Model (TAM) is a commonly employed theory for describing an individual's acceptance of information systems, and questionnaire-based field studies of information systems often utilize the TAM [22]. This model was developed by Davis and assumes that a users' attitude toward using an Information System is determined by measuring Perceived

Usefulness and Perceived Ease of Use [9]. Other considerations will always exist, such as past experiences and risk tolerance [11], but the two primary constructs of TAM provide a logical starting point for this research.

In order to facilitate the widespread adoption of blockchain technology, use of the TAM is justified so that we can better understand the public's attitude toward the technology. Kern sought to quantitatively analyze the public perception and state of knowledge about Blockchain technology as a whole [21]. In doing so, a modified TAM was used, which also included Perceived Risk and Level of Knowledge variables.

The Perceived Risk variable was derived from previous analysis of e-commerce applications, which is due to the distant and impersonal nature of the systems [31]. In the blockchain context, the Level of Knowledge was hypothesized, and confirmed to be, negatively related to the Perceived Risk. This led to development of the Blockchain Acceptance Model. Based on these observations, we propose the following hypothesis: **H1: Level of Knowledge positively correlates with Change in Voter Confidence**

3.3 Experiment

A survey was developed on the Qualtrics platform for the between-groups experiment. A survey was chosen as the research method due to the ability to sample a large, geographically diverse population with low cost. Additionally, anonymity was relied on as a mitigating factor against bias in the survey data. While interviews and focus groups can often provide richer data, maintaining anonymity in these settings is more difficult. Since this project seeks the participation of human subjects, institutional review board approval was sought and obtained. This study qualified for exempt status from a full board review.

Distribution of the survey to participants was accomplished with the use of Prolific. Prolific is a crowdsourcing platform that matches survey participants to relevant research. Studies have generally indicated that Prolific can provide high quality data from survey participants (e.g., [30]), similar to other crowdsourcing platforms (e.g., Amazon's Mechanical Turk) [12]. Nonetheless, it is important that quality control measures are implemented due to the propensity for abuse [13].

3.4 Survey Construction

The purpose of this experiment is twofold. The first objective is to determine if the hypothesis H1 is correct by attempting to disprove the null hypothesis H0. The second objective is to determine the overall positive or negative attitude toward a blockchain-based election.

To accomplish this, a framework similar to Völter et al. [37] was used. Three prompts were developed to create three distinct messaging strategies. Each prompt began with the same general description of blockchain and how the election application would generally function. Then the participants would be shown one of the following:

(1) A contrast between the functionality of popular cryptocurrencies and the functionality of an election implementation,
(2) A simplified system diagram of the election implementation, or
(3) A discussion of pertinent features that a blockchain-based system could or could not provide.

During development of the survey, a pretest was performed to ensure that the survey had logical flow and was coherent to a non-technical audience. Three independent individuals with backgrounds outside of computer science completed the survey and provided feedback. In addition to minor comments, each individual identified that the language was overly technical and should be revised to better communicate with a broad audience. For this reason, the prompts are focused at a high level and do not contain many technical details.

3.5 Survey Variables

For measuring voter confidence, questions with responses on a four-point, unipolar Likert scale were used, in addition to a non-responsive "Don't Know" option. This methodology matches the MIT module to the 2020 Cooperative Congressional Election Study [1]. Question wording was also adapted from this study to allow for future comparison. The voter confidence questions were asked at the beginning of the survey in relation to previous elections, and the questions were then later asked in relation to the theoretical blockchain-based system. The difference between these values represents the Change in Voter Confidence.

The remaining variables (Level of Knowledge, Perceived Ease of Use, and Perceived Usefulness) were measured on a five-point Likert scale in a similar manner as that performed by Kern [21]. Level of Knowledge and Perceived Usefulness were measured on a unipolar scale, while Perceived Ease of Use was measured on a bipolar scale. This was done to better align the questions grammatically for a more straightforward presentation to participants.

3.6 Quality Control Measures

The Prolific platform has strict criteria that must be used in evaluating whether a response can be rejected. Within these limitations, two instructional manipulation checks (IMCs) and nonsensical items were employed with each consisting of five choices. Additionally, two comprehension checks were utilized for each prompt to evaluate the participant's understanding of the content presented. Since the application of blockchain is generally a technical topic that some individuals may have difficulty understanding in a short period of time, this study did not penalize participants for failing to understand the prompts presented. The data will instead be used to validate the survey results. Finally, we utilized the the Qualtrics bot detection feature. Using reCAPTCHA, each response is rated on a probability that the respondent was a bot. Any response scoring below the Qualtrics-recommended threshold of 0.5 was filtered out.

4 RESULTS

There were a total of 405 participants. Sixteen responses were withdrawn by the participant. Since consent for this data was also inherently revoked, this data was deleted from the final results. Two results timed-out and were incomplete. These partial results were deleted from the final results. One response failed both attention checks and was not withdrawn by the participant. This response

was rejected. Each participant's survey duration was analyzed to determine if the duration is feasible to provide a fair response.

The distribution of survey response durations is non-normal. The skewness was calculated as 4.1, indicating a heavy positive skew, and kurtosis was calculated as 26.8, indicating a large number of outliers. Due to the skew and outliers, only one response was less than one standard deviation below the mean. This response had a duration of seventy-three seconds. Per the Prolific guidelines, this response could not be rejected. However, qualitative analysis shows that completion of the survey in seventy-three seconds is unlikely to be done thoughtfully. Therefore, this response was not used. The remaining 385 responses were responsive, passed both attention checks, and were unlikely to be sourced by bots. Therefore, the data from these responses were used for analysis.

4.1 Data Analysis

Change in Voter Confidence was measured on a four-point Likert scale. Participants were asked to measure confidence that "your vote" and "all votes" were counted as intended in both the current and blockchain-based system. Non-voters were only prompted to answer in regard to "all votes". Scores for the questions were averaged to give equal weight to voters and non-voters. A response of "Don't Know" to any of the confidence questions was treated as non-responsive and was excluded from the Change in Voter Confidence calculation. Twenty-four responses were excluded in this way, leaving 361 responses for analysis.

The average of the responses resulted in Change in Voter Confidence of -0.35 on the four-point Likert scale, meaning that average confidence in the blockchain system was 0.35 points (11.7%) lower than the current system when measured on a scale from one (Not At All Confident) to four (Very Confident). The percentage calculation represents the percentage of the available scale that the variable quantity represents. The percentage is calculated as follows: ((Change in Voter Confidence)/(Scale Max-Scale Min)) × 100%= ((-.35)/(4-1))× 100% = -11.7%

The average baseline confidence in existing voting systems was measured at 3.20, which places the average between Somewhat Confident (3) and Very Confident (4). Therefore, the average confidence in the blockchain-based voting systems was measured at 2.85, which places the average between Not Too Confident (2) and Somewhat Confident (3).

The correlation between Level of Knowledge and Change in Voter Confidence was assessed by having the values projected onto a scatter plot with Level of Knowledge on the x-axis and Change in Voter Confidence on the y-axis. A linear trendline was then calculated to determine the overall effect on Change in Voter Confidence in relation to Level of Knowledge. A scatter plot with superimposed linear trendline with positive slope of 0.19 was produced. Note that since the x and y values are discreet, the data points overlap on the graph. Jitter to the data points was added to better illustrate the density.

To determine if Level of Knowledge correlates with Change in Voter Confidence, Pearson's correlation coefficient (r) was calculated to be 0.17 for this data. Values of $|r| < 0.35$ represent a weak correlation [35]. Therefore, this experiment has demonstrated a weak positive correlation between Level of Knowledge and Change in Voter Confidence.

4.2 Results Discussion

Support for our hypothesis is considered weak due to the low correlation coefficient (r = 0.17). As discussed previously, Kern performed a similar experiment which evaluated the correlation between Level of Knowledge and Intention to Use in a more generic blockchain context and found a moderate positive correlation (r = 0.43) between these variables [21]. The significantly lower correlation observed in this experiment leads to the likely conclusion that an individual's familiarity with blockchain is not a strong factor in determining their overall confidence in a blockchain-based election. A future experiment would be required to determine a new independent variable that was more correlative with Voter Confidence. Some examples worthy of consideration may include political ideology, frequency of computer usage, or other demographic factors. Additionally, the development of such a system involves a multitude of inter-related factors, from design, software development, security, and implementation. It is important that the development of such components are not done is isolation from one another [28].

The between-groups experiment produced noteworthy results. Prompts one and three indicated significant drops in confidence, while prompt two generally precipitated a neutral response, with a drop in confidence within the margin of error discussed in earlier. The causality of this relationship warrants further exploration. Prompt two provided a simplified system diagram on the blockchain-based election system, while the other two prompts provided text-based discussion. One possible explanation for the neutral response to prompt two is that people process images significantly faster than they process text [36]. Given that the median survey duration was 4 minutes and 54 seconds, participants had very little time to understand the system that was being presented to them, especially if they were not already familiar with the concept of blockchain. The visual representation may have provided the best tool for understanding the system in a short amount of time.

4.3 Limitations

Due to the use of a survey involving a single data collection source, this project inherently suffers from common method bias [32]. To help mitigate the effects of this bias, several mitigating factors were employed (e.g., anonymity provided on crowdsourcing platforms)

One available method for testing for common method bias is to use Harman's single factor test [25]. To perform this analysis, the survey results were loaded into IBM SPSS Statistics software. The software evaluated the total variance extracted by one factor as 41.5%, which does fall below the recommended threshold of 50%. This leads to a reasonable assumption that common method bias did not greatly impact the results, but a larger margin between the measured variance and the 50% threshold would have provided a more solid basis for this assumption.

This survey is also largely susceptible to acquiescence bias, where the participant responds in the way that they believe the researcher wants them to respond. Acquiescence bias has been shown to inflate the estimated incidence of conspiratorial beliefs and political misperceptions by up to 50% [19]. Since this survey deals with topics

that have prominently surfaced in various conspiracy theories and political misperceptions, the impact of acquiescence bias cannot be ignored.

5 CONCLUSION

Societal acceptance of technology does not happen overnight. Personal computer use took 24 years to go from 21% of US households in 1992 to 89% in 2016 [33]. Other technologies (e.g., voice authentication) may show promise, but also face many challenges with respect to their effective implementation and acceptance [8]. The use of blockchain is still a relatively new concept, and acceptance will likely grow as time goes on. The possibilities for the use of blockchain are extensive, with potential applications in areas as wide-ranging as solid waste management [14], food traceability [16], and public health [5]. However, when working with critical infrastructure such as voting systems, it is important to ensure that the underlying technology is mature and well-accepted.

Based on the results herein, a transition to blockchain-based elections is not advisable in the near term. Even if an implementation of a blockchain-based election system could be modeled to demonstrate high security, the technology does not appear to have enough widespread acceptance to elicit confidence among the public at this time. As earlier argued, a blockchain-based election system must demonstrate both strong security and high confidence among the public. The between-groups nature of the experiment did demonstrate that proper messaging could play an important role in acceptance of blockchain. While the exact nature of the messaging is unclear based on the results, the experiment did demonstrate that the nature of the messaging plays an important role. Future work could lay the foundation for a messaging strategy of a blockchain-based election system.

REFERENCES

[1] [n. d.]. https://electionlab.mit.edu/research/voter-confidence

[2] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato. 2018. A Proposal of Blockchain-Based Electronic Voting System. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, London, 22–27. https://doi.org/10.1109/WorldS4.2018.8611593

[3] R. Michael Alvarez, Thad E. Hall, and Morgan H. Llewellyn. 2008. Are Americans Confident Their Ballots Are Counted? *The Journal of Politics* 70, 3 (Jul 2008), 754–766. https://doi.org/10.1017/S0022381608080730

[4] Nicolas Berlinski, Margaret Doyle, Andrew M. Guess, Gabrielle Levy, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, and Jason Reifler. 2021. The Effects of Unsubstantiated Claims of Voter Fraud on Confidence in Elections. *Journal of Experimental Political Science* (Jun 2021), 1–16. https://doi.org/10.1017/XPS.2021.18

[5] Sudip Bhattacharya, Amarjeet Singh, and Mahbub Hossain. 2019. Strengthening public health surveillance through blockchain technology. *AIMS Public Health* 6, 3 (2019), 326–333. https://doi.org/10.3934/publichealth.2019.3.326

[6] Prashanth P Bungale and Swaroop Sridhar. 2013. Requirements of an Electronic Voting System. *Unpublished Thesis, Department of Computer Science, The Johns Hopkins University* (2013).

[7] Pew Research Center. 2020. Sharp Divisions on Vote Counts, as Biden Gets High Marks for His Post-Election Conduct. https://www.pewresearch.org/politics/2020/11/20/sharp-divisions-on-vote-counts-as-biden-gets-high-marks-for-his-post-election-conduct/

[8] Yun-Tai Chang and Marc Dupuis. 2019. My Voiceprint Is My Authenticator: A Two-layer Authentication Approach Using Voiceprint for Voice Assistants. In *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*. IEEE, Leicester, England, 1318–1325. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00243

[9] Fred D Davis. 1986. *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. PhD Thesis. Massachusetts Institute of Technology.

[10] Tassos Dimitriou. 2020. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting. *Computer Networks* 174 (Jun 2020), 107234. https://doi.org/10.1016/j.comnet.2020.107234

[11] Marc Dupuis, Robert Crossler, and Barbara Endicott-Popovsky. 2012. The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information. In *The Dewald Roode Information Security Workshop*. Provo, Utah.

[12] Marc Dupuis, Barbara Endicott-Popovsky, and Robert Crossler. 2013. An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud. In *International Conference on Cloud Security Management*. Seattle, Washington.

[13] Marc Dupuis, Karen Renaud, and Rosalind Searle. 2022. Crowdsourcing Quality Concerns: An Examination of Amazon's Mechanical Turk. In *The 23rd Annual Conference on Information Technology Education*. ACM, Chicago IL USA, 127–129. https://doi.org/10.1145/3537674.3555783

[14] A.S.L. França, J. Amato Neto, R.F. Gonçalves, and C.M.V.B. Almeida. 2020. Proposing the use of blockchain to improve the solid waste management in small municipalities. *Journal of Cleaner Production* 244 (Jan 2020), 118529. https://doi.org/10.1016/j.jclepro.2019.118529

[15] Gallup. 2020. Confidence in Accuracy of U.S. Election Matches Record Low. https://news.gallup.com/poll/321665/confidence-accuracy-election-matches-record-low.aspx

[16] Juan F. Galvez, J.C. Mejuto, and J. Simal-Gandara. 2018. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in Analytical Chemistry* 107 (Oct 2018), 222–232. https://doi.org/10.1016/j.trac.2018.08.011

[17] Víctor Gayoso Martínez, Luis Hernandez Encinas, and Araceli Queiruga-Dios. 2015. Security and Practical Considerations When Implementing the Elliptic Curve Integrated Encryption Scheme. *Cryptologia* 39 (May 2015), 1–26. https://doi.org/10.1080/01611194.2014.988363

[18] Stuart Haber and W. Scott Stornetta. 1991. *How to Time-Stamp a Digital Document*. Lecture Notes in Computer Science, Vol. 537. Springer Berlin Heidelberg, Berlin, Heidelberg, 437–455. https://doi.org/10.1007/3-540-38424-3_32

[19] Seth J. Hill and Margaret E. Roberts. 2023. Acquiescence Bias Inflates Estimates of Conspiratorial Beliefs and Political Misperceptions. *Political Analysis* (Jan 2023), 1–16. https://doi.org/10.1017/pan.2022.28

[20] Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa, and Gisli Hjalmtysson. 2018. Blockchain-Based E-Voting System. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, San Francisco, CA, USA, 983–986. https://doi.org/10.1109/CLOUD.2018.00151

[21] Alexander Günter Kern. 2018. *Blockchain technology: a technology acceptance model (TAM) analysis*. PhD Thesis.

[22] Younghwa Lee, Kenneth A Kozar, and Kai RT Larsen. 2003. The technology acceptance model: Past, present, and future. *Communications of the Association for information systems* 12, 1 (2003), 50.

[23] Inés Levin and R Michael Alvarez. 2009. Measuring the effects of voter confidence on political participation: An application to the 2006 Mexican election. (2009).

[24] Wouter Lueks, Iñigo Querejeta-Azurmendi, and Carmela Troncoso. 2020. VoteAgain: A scalable coercion-resistant voting system. In *29th USENIX Security Symposium (USENIX Security 20)*. 1553–1570.

[25] Naresh K Malhotra, Sung S Kim, and Ashutosh Patil. 2006. Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management science* 52, 12 (2006), 1865–1883.

[26] Teogenes Moura and Alexandre Gomes. 2017. Blockchain Voting and its effects on Election Transparency and Voter Confidence. In *Proceedings of the 18th Annual International Conference on Digital Government Research*. ACM, Staten Island NY USA, 574–575. https://doi.org/10.1145/3085228.3085263

[27] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.

[28] Jessica Nguyen and Marc Dupuis. 2019. Closing the Feedback Loop Between UX Design, Software Development, Security Engineering, and Operations. In *Proceedings of The 20th Annual Conference on Information Technology Education (SIGITE '19)*. ACM, Tacoma, WA, USA, 93–98. https://doi.org/10.1145/3349266.3351420

[29] WA Secretary of State. [n. d.]. November 3, 2020 General Election Results. https://results.vote.wa.gov/results/20201103/federal-all.html

[30] Stefan Palan and Christian Schitter. 2018. Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (Mar 2018), 22–27. https://doi.org/10.1016/j.jbef.2017.12.004

[31] Paul Pavlou. 2003. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce* 7, 3 (Apr 2003), 101–134. https://doi.org/10.1080/10864415.2003.11044275

[32] Philip M Podsakoff, Scott B MacKenzie, Jeong-Yeon Lee, and Nathan P Podsakoff. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology* 88, 5 (2003), 879.

[33] Hannah Ritchie and Max Roser. 2017. Technology Adoption. *Our World in Data* (2017).

[34] Michael A. Specter, James Koppel, and Daniel Weitzner. 2020. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 1535–1553. https://www.usenix.org/conference/usenixsecurity20/presentation/specter

[35] Richard Taylor. 1990. Interpretation of the Correlation Coefficient: A Basic Review. *Journal of Diagnostic Medical Sonography* 6, 1 (Jan 1990), 35–39. https://doi.org/10.1177/875647939000600106

[36] Douglas Rudy Vogel, Gary W Dickson, John A Lehman, et al. 1986. Persuasion and the role of visual presentation support: The UM/3M study. (1986).

[37] Fabiane Völter, Nils Urbach, and Julian Padget. 2021. Trusting the trust machine: Evaluating trust signals of blockchain applications. *International Journal of Information Management* (Oct 2021), 102429. https://doi.org/10.1016/j.ijinfomgt.2021.102429

[38] Charles R. Wise. 2001. Election Administration in Crisis: An Early Look at Lessons from Bush versus Gore. *Public Administration Review* 61, 2 (Mar 2001), 131–139. https://doi.org/10.1111/0033-3352.00014