Systematic Review to Propose a Blockchain-Based Digital Forensic Ready Internet Voting System

Edmore Muyambo[1] and Stacey Omeleze Baror[2]
[1]Digital Forensic Research Group, Dept of Computer Science
[2]University of Pretoria, South Africa

Edmore.muyambo@tuks.co.za
Stacey.baror@cs.up.ac.za

Abstract: The ballot paper-based voting system has a high risk of data manipulation and vote tampering due to a lack of immutability, transparency and privacy. This systematic review is conducted with the intention of proposing a digital forensic-ready internet voting process to mitigate issues of vote rigging and vote fraud. The review focused on current and up-to-date literature. Publications that are out of this date range were ignored and considered stale or irrelevant. We extracted and reviewed publications with either or all the following keywords: "digital forensic", "internet voting", "e-voting" and "blockchain". A total of thirteen databases were consulted. These include ACM, IEEE, Web of Science, Science Direct, Academic Search Complete, Access Science, ProQuest, Oxford Academy, Ingenta, Cambridge Core and Clarivate. From the inclusion list of one hundred and five (105) studies that were looked at in detail, twenty of them (i.e.,19%) covered blockchain technology. Two percent (2%) of them were focused on digital forensics in internet voting. The results herein were synthesised and presented in a qualitative methodology. The review shows that a secure and reliable digital forensic system could effectively mitigate vote rigging and fraud. Therefore, we proposed a blockchain-based digital forensic-ready internet voting system. The proposed system is beneficial to the electorate, election observers, electoral candidates, electoral administration bodies as well as the national law enforcement agencies.

Keywords: Digital forensics, Blockchain, Internet voting, Online voting, Cyber security

1. Introduction

With the rapidly growing Internet of Things, smart technologies are emerging. The emergency of smart technologies brings about the need for smart infrastructure. This holistically integrates to form smart cities. In smart cities, smart devices are interconnected to render municipal essential services such as water billing, electricity billing, traffic management as well as municipal e-voting processes amongst many other things. Therefore, it becomes essential that we conduct a systematic review of digital transactions, privacy and security. This gives us a clear understanding of the currently existing knowledge in the research field thereof.

Research has shown that many countries are still experiencing electoral issues, pre-election, during and post-election season (Gomes, Moura,2017). Most of these issues are linked to alleged vote rigging and vote fraud. These cases are mostly recorded in countries that are still using the ballot paper-based voting system (Smith,2016). This is due to the fact that the ballot paper-based system has a high risk of data manipulation and vote tampering (Singh, Wable, Khrose, 2021). The process involves several manual procedures. This exposes electoral data to human errors and malicious vote tampering practices that can subsequently result in vote fraud and vote rigging. As a result, electoral disputes usually ensue due to lack of immutability, transparency, privacy and data security in the process. However, some sources still argue that the traditional process is still better than the electronic means. Given all the above details, we decided to conduct an extensive systematic literature review to ascertain how the integration of internet voting and digital forensics can be used to mitigate vote rigging and vote fraud issues. The use of digital security technologies such as the blockchain is still relatively new in the industry. Therefore, the available systematic reviews in this research field are still quite few. Hence our motivation to conduct a review.

With reference to some studies in the domain, Blockchain has been identified as one such technological process that can be used to preserve data security, integrity and privacy within a set of interconnected devices and systems (Hjalmarsson, Hreioarsson et al, 2018). The studies highlighted that Blockchain can achieve the above-mentioned security benefits in a transparent yet uncompromisable manner (Ayed, AB, 2017). An attack or alterations to the secured datasets or digital transactions can be easily detected and flagged by the blockchain technology. However, the transparency characteristic risks the exposure of personal data to the public.

1.1 Research Question and Objectives

The research question in this study is: can digital forensics mitigate issues of vote rigging and vote fraud in internet voting processes? The objective of the literature revision is to systematically analyse current studies on the use of digital forensics backed by blockchain technology in a voting process.

2. Method

This review was done on publications that were peer-reviewed and published by accredited academic publishers. We reviewed publications that centered their research on digital forensics in internet voting in integration with blockchain technology. At least three of the main search keywords must exist in the publication. These are “digital forensic”, “internet voting” and “blockchain”. Publications that had some alternative search keywords such as “online voting” instead of “internet voting” were also taken up into the inclusion list; provided at least three of the main keywords (highlighted above) existed. Publications that had all the required keywords but were published some ten years ago were not reviewed. We consulted studies that were not more than ten years old. We were mainly interested in studies that investigated ballot paper-based voting systems, electronic-based voting systems and the blockchain technology. Other key screening criteria for our inclusion list were language, credibility and authenticity. Publications were supposed to be in English, peer-reviewed and published by internationally accredited publishers. For verifiability and referencing purposes, we reviewed only publications that have been stored in internationally recognized academic libraries and databases. We made very little to no reference at all to grey literature.

Key players in this research were voters, election candidates and the election administration board. The main aim of having a secure vote administration system is to protect voters’ choices.

2.1 Information Sources

Our information base was gathered from a total of thirteen databases. We also made use of referral websites. These include Google Scholar and the University of Pretoria’s online library. We narrowed the search to articles and documents published between the first of January 2015 and the thirty-first of March 2023. A full list of consulted databases and dates thereof is shown in Table 1 below.

Table 1: Consulted Databases

DATABASE	DATE SEARCHED
ACM	1 March 2023
IEE	1 March 2023
WEB OF SCIENCE	4 March 2023
SCIENCE DIRECT	4 March 2023
ACADEMIC SEARCH COMPLETE	4 March 2023
ACCESS SCIENCE	7 March 2023
PROQUEST	7 March 2023
OXFORD ACADEMY	9 March 2023
INGENTA	9 March 2023
OPEN GLOBAL TRUSTED	9 March 2023
CLARIVATE	9 March 2023
CAMBRIDGE CORE	11 March 2023
BRILL	11 March 2023

2.2 Search Technique

Several keywords were used to search for relevant literature. Only publications that contained the required keywords were considered for review. The main keywords used in the search console are Digital forensics, internet voting, blockchain, online voting and e-voting. A combination of keywords strategy was also used to retrieve relevant publications. A list of search keyword combinations is listed below.

- Digital forensic
- Digital forensic + internet voting

- Digital forensic + internet voting + blockchain
- Digital forensic + internet voting + blockchain + online voting
- Digital forensic + internet voting + blockchain + online voting + e-voting
- Digital forensic + internet voting + blockchain + online voting + e-voting + published date between 2015/01/01 and 2023/03/31

On the first search, "Digital forensic" keyword was used. This presented us with thousands of search results in return. This was quite a large number to reference and read through. We then made various search combinations to try and narrow the search results as well as to get more relevant studies for review. Different search permutations were used as shown above and the number of hits was recorded. After all keyword combination search was done, we applied a date filter to get newer publications. Newer publications are essential as they contain recent research knowledge and findings. Older publications introduce a risk of bias in a review as they were done based on old or now-irrelevant technologies.

After applying the date filter, the number of publications became even smaller. We then went on to manually read through titles and abstracts in order to extract more relevant publications for review. Figure 1 below shows the search strategy used.

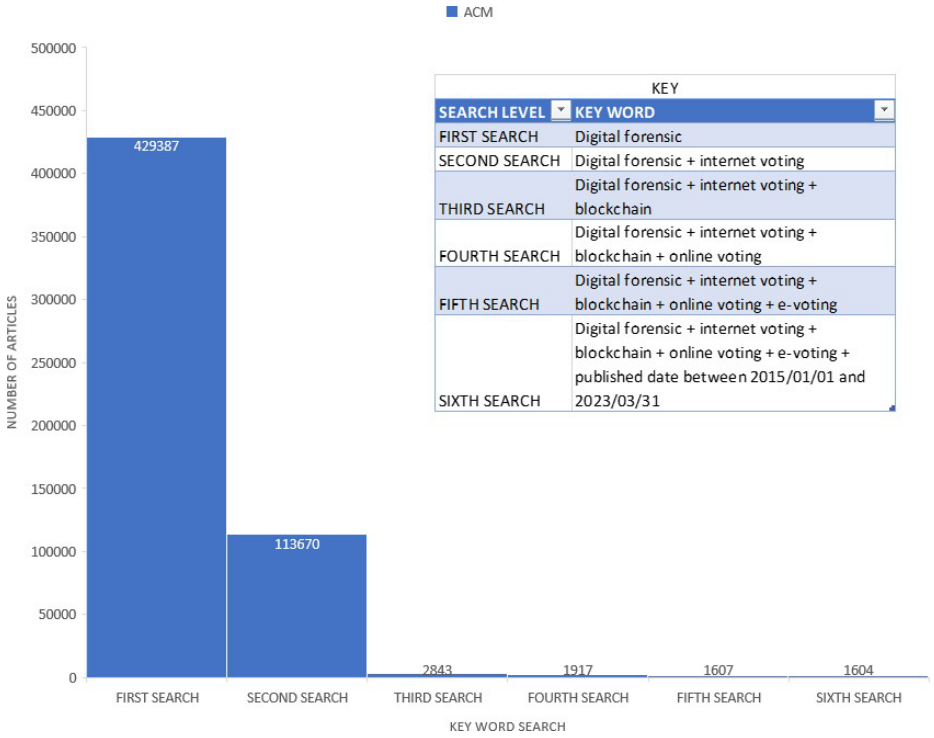

Figure 1: ACM Database Search Strategy

2.3 Selection Process

After applying the search strategy, publications that made it into the preliminary inclusion list were taken up for further screening. As a means of screening studies, we briefly read through titles, abstracts, introductions and the entire document. From this screening phase, we selected studies that would make it into the next phase of screening. The final screening was conducted by means of thoroughly studying the entire document. We believe that when the means of communication is not clear enough, it becomes difficult to understand the message being passed. Therefore, we also went on to exclude studies that we found linguistically unprofessional. The selection process was not done by groups or software but by a single reviewer.

2.4 Data Collection Process

Data collection was not done by means of some automated process or group collection but by a single reviewer. This was done through the means of manually reading published studies as well as studying reports, images, tables, graphs and numbers.

2.5 Data Items

The outcome domains in this review were:

- Inefficiency of the ballot paper-based voting system.
- Vulnerability of the ballot paper-based voting system to vote rigging.
- Efficiency of an online voting system based on blockchain technology.
- Importance of Blockchain technology in preserving data and digital transactions
- Importance of digital forensics in online voting processes

All the above outcomes are significant in the sought results. Results and conclusive findings for each outcome were accessed and considered. Proposed models and suggestive findings were also included in the inclusion list.

We collected information based on the year of publication, keyword match and literature relevance. The information collected was not country-specific, nor was it individual-specific. Any publication which met the screening criteria would make it into the inclusion list. Thus, our target publications were those that focused on voting, data encryption and digital forensics.

2.6 Study Risk of Bias Assessment

In this research, the risk of bias was conducted by assessing what is known thus far and comparing it with other studies' findings. If the comparison looked somewhat deviating from the known knowledge that has scientific proof, then a risk of bias would be flagged. We expect quantified findings to have a valid point of reference. Therefore, if there is a numerical representation in a study but there is no valid source of reference to it, we flagged this as a potential introduction of risk of bias in the review. This assessment was done by a single reviewer.

2.7 Effect Measures

From the one hundred and five (105) studied publications, ninety (90) of them i.e., 85.7% of them expressed clearly the vulnerability of ballot paper-based voting systems to vote rigging. They possess a high risk of undetectable vote tampering and untraceable vote manipulation activities. Of the ninety

(90) studies, eighty-five (85) of them i.e.,94.4% clearly stated how blockchain technology can be of great importance in the mitigation of vote rigging and vote fraud in online voting processes. Of these eighty-five publications that highlighted the importance of blockchain technology, only twenty (20) of them i.e., 23.5% referred to the importance of digital forensics in preserving data integrity in online transactions. There is still very limited knowledge, research and literature about digital forensics in online voting. The percentage of articles that spoke about digital forensics in online voting was 2%. Of the twenty (20) studies in our inclusion list that focused on blockchain technology, only 2% of these were focused on digital forensics in online voting.

2.8 Synthesis Methods

The coding used to determine the suitability of each study considered for synthesis in this research was:

- Online voting/Internet voting process
- Ballot paper-based voting process
- Blockchain technology
- Digital forensics
- Vote rigging

These codes of synthesis basically aimed to extract and understand information about the traditional voting system, its flaws and its strengths. The codes also aimed to extract information about online voting systems. It is essential that a study be conducted on the two identified voting systems. This would then give a clear indication of the strengths and weaknesses of each. Due to the high vote rigging allegations in a traditional voting system, this review targeted studies that highlight how the online-based voting system can be fortified and strengthened in order to mitigate such vote rigging. Blockchain technology was identified as one of the most reliable mechanisms that can be used to preserve online transactional data integrity, privacy and security. Hence the need to have blockchain studies in the inclusion list. The implementation of blockchain technology is just a technical process. This process gives a platform for the digital forensic process to take place. Hence all studies that met the digital forensic inclusion criteria were considered for synthesis.

We used a graphical representation (histogram) for our digital search findings. The graphical representations are per search level and keyword used in each library or database. An example is shown in Fig 1 above.

2.9 Reporting Bias Assessment

Online voting is still in the infancy stages. Likewise, the onboarding of the blockchain technology in the process thereof. Therefore, research studies in the implementation of blockchain technology to mitigate vote rigging and vote fraud are still quite limited due to lack of literature and research in the faculty. Search results from the keyword "blockchain" were compared with the search results from the "ballot paper voting process". There was quite a huge difference in the number of articles returned. The former had quite a few results whilst the latter had a huge number of studies returned. This shows that there is a gap of bias due to the lack of sufficient reference literature in the past. This assessment was evident and therefore did not require any collaboration or group effort. Hence, only a single reviewer contacted the assessment.

2.10 Certainty Assessment

From the search conducted, we derived a degree of certainty and confidence in the search results after assessing their consistency. The physical analysis was used to identify and separate isolated results from the popular ones. This assessment was carried out by only one reviewer.

3. Results

3.1 Study Selection

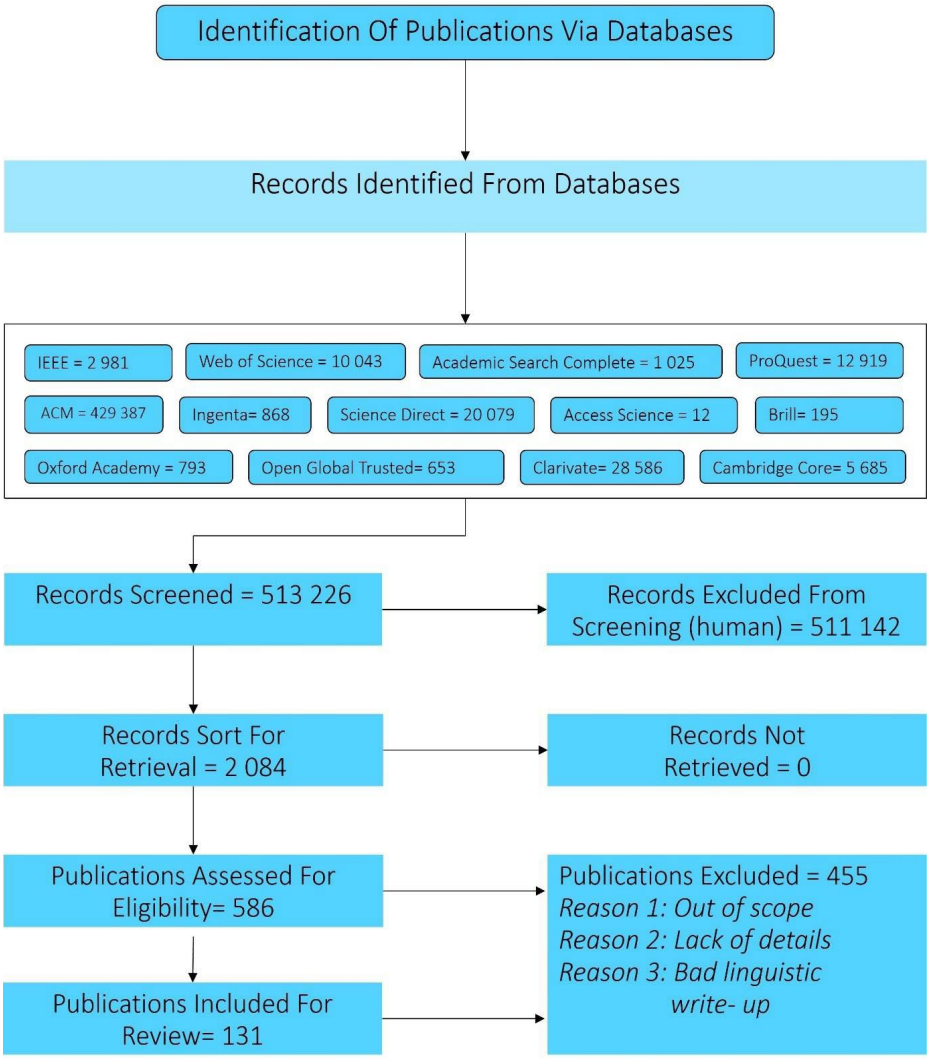

Figure 2: Search Results-Selection Criteria

As depicted in Fig 2 above, our initial search criteria gave us 513,226 records. These were then screened against our inclusion list criteria. The next screening phase excluded 511,142 records. This was done through the application of search filters such as keywords and year of publication. Of the 2 084 publications that survived the previous screening phase, 586 of them made it to the next round of screening. These were then manually assessed by physically reading through titles, abstracts and introductions. After this exercise, only 131 records made it to the next stage.

Of the 131 records from the previous screening stage, 17 were excluded. To prevent our paper from spanning too many pages, we only listed five of the seventeen excluded studies. These are shown in Table 2 below. In a nutshell, most of them were technically irrelevant to our review field, some lacked scientific detail and relevance, and some were just not properly written up grammatically. It was difficult to understand the concept and knowledge shared due to poor grammar or a lack of standard scientific writing.

Table 2: The Exclusion List

Author	Year	Tittle	Exclusion Reason
Neloy, Mohammad Nabiluzzaman; Wahab, Md. Abdul; Wasif, Sheikh; All Noman, Abdulla	2023	A remote and cost- optimized voting system using blockchain and smart contract	Does not cover digital forensic scope
Chaabane, Faten; Ktari, Jalel; Frikha, Tarek; Hamam, Habib	2022	Low Power Blockchained E-Vote Platform for University Environment	Limited scope
Vatsa, Avimanyou	2021	BCT-Voting : A Blockchain Technology Based Voting System BCT-Voting : A Blockchain Technology Based Voting System	Does not cover digital forensic scope
Dimitri, Nicola	2022	Quadratic Voting in Blockchain Governance	Too technical and lacks clear linguistic literature
Desai, Shreya; Desai, Shreya; Desai, Shreya; Li, Zhigang; He, Jing; Xu, Xiaohua	2019	Untampered electronic voting in entertainment industry: A blockchain-based implementation	Outside the required scope

3.2 Study Characteristics

Table 3: Included Study Citation

Author	Year	Tittle	Study Area
Li, Meng; Lal, Chhagan; Conti, Mauro; Conti, Mauro	2021	LEChain: A blockchain- based lawful evidence management scheme for digital forensics	Blockchain and Digital Forensic
Ryu, Jung Hyun; Sharma, Pradip Kumar; Jo, Jeong Hoon; Jo, Jeong Hoon	2019	A blockchain-based decentralized efficient investigation framework for IoT digital forensics	Blockchain and Digital Forensic
Koç, Ali Kaan; Yavuz, Emre; Çabuk, Umut Can; Çabuk, Umut Can	2018	Towards secure e-voting using ethereum blockchain	E-voting and Blockchain
Englbrecht, Ludwig	2020	A privacy-aware digital forensics investigation in enterprises	Digital Forensics
McCorry, Patrick; Mehrnezhad, Maryam; Toreini, Ehsan; Shahandashti, Siamak F; Hao, Feng	2021	On Secure E-Voting over Blockchain	E-voting and Blockchain

Author	Year	Tittle	Study Area
Gomes, Alexandre	2017	Blockchain Voting and its effects on Election Transparency and Voter Confidence	Blockchain
Huang, Jun; He, Debiao; Obaidat, Mohammad S.; Vijayakumar, Pandi; Luo, Min; Choo, Kim Kwang Raymond	2021	The Application of the Blockchain Technology in Voting Systems	Blockchain and Voting
Rabia, Fatih; Sara, Arezki; Sara, Arezki	2021	A survey on e-voting based on blockchain	Blockchain and E-Voting
Vladucu, Maria Victoria; Dong, Ziqian; Medina, Jorge; Rojas-Cessa, Roberto	2023	E-voting Meets Blockchain: A Survey	Blockchain and E- Voting
Shah, Akhil; Sodhia, Nishita; Saha, Shruti; Banerjee, Soumi; Chavan, Madhuri	2020	Blockchain Enabled Online-Voting System	Blockchain and Online Voting
Anitha, V; Marquez Caro, Orlando Juan; Sudharsan, R.; Yoganandan, S.; Vimal, M.	2023	Transparent voting system using blockchain	Blockchain
Mizzi, Jerome; Inguanez, Frankie	2018	Blockchain based E-Voting System	Blockchain and E-Voting
K., Edison; B., Venansius	2022	Blockchain Based Electronic Voting Protocol	Blockchain
Holmes, C	2022	How Blockchain Technology could support Democracy and E-Voting	Blockchain and E- Voting
Fatrah, Aicha; Kafhali, Said El; Haqiq, Abdelkrim; Salah, Khaled	2019	Proof of concept blockchain-based voting system	Blockchain
Hossain, Syeda Sumbul; Arani, Samen Anjum; Tanvir Rahman, Md; Bhuiyan, Touhid; Alam, Delwar; Zaman, Moniruz	2019	E-voting system using Blockchain technology	Blockchain and E- Voting
Abuidris, Yousif; Kumar, Rajesh; Wenyong, Wang	2019	A survey of blockchain based on e-voting systems	Blockchain and E- Voting
González, Camilo Denis; Mena, Daniel Frias; Muñoz, Alexi Massó; Rojas, Omar; Sosa-Gómez, Guillermo	2022	Electronic Voting System Using an Enterprise Blockchain	Blockchain and E- Voting
Lahane, Anita A.; Patel, Junaid; Pathan, Talif; Potdar, Prathmesh	2020	Blockchain technology based e-voting system	Blockchain and E- Voting
Leune, Kees; Punjwani, Jai	2021	Enhancing electronic voting with a dual-blockchain architecture	Blockchain and E- Voting

Author	Year	Tittle	Study Area
Bartolucci, Silvia; Bernat, Pauline; Joseph, Daniel	2018	SHARVOT: Secret SHARe-based VOTing on the blockchain	Blockchain
Alshehri, Ali; Baza, Mohamed; Srivastava, Gautam; Rajeh, Wahid; Alrowaily, Majed; Almusali, Majed	2023	Privacy-Preserving E- Voting System Supporting Score Voting Using Blockchain	Blockchain and E- Voting
Neloy, Mohammad Nabiluzzaman; Wahab, Md. Abdul; Wasif, Sheikh; All Noman, Abdulla; Rahaman, Mustafizur; Pranto, Tahmid Hasan; Haque, A. K. M. Bahalul; Rahman, Rashedur M.	2023	A remote and cost- optimized voting system using blockchain and smart contract	Blockchain and Smart Contract
Wahab, Yousif Mohammed; Ghazi, Alaan; Al-Dawoodi, Aras; Alisawi, Muthana; Abdullah, Sirwan Saber; Hammood, Layth; Nawaf, Asmaa Yaseen	2022	A Framework for Blockchain Based E- Voting System for Iraq	Blockchain and E- Voting

Table 3 above details a citation list of some of the included studies in this systematic review. The table details author(s), year of publication, publication title as well as the reviewed literature. In this research, the four main study areas of focus were Digital Forensics, Blockchain, Internet Voting and to some extent Cyber Security details.

3.3 Risk Of Bias in Studies

The risk of bias in this study was conducted by studying publications' context. In some cases, only the abstract was read in order to determine the risk of bias whilst in other cases both the abstract and introduction were read. However, in most cases the abstract, introduction and the entire publication's content were read through in order to get the logical flow of the study and its intentions.

3.4 Reporting Biases

Since electronic voting is still not widely adopted, literature relating to digital forensics in electronic voting is likewise very limited. From our research list, the main identified studies that specifically relate to blockchain-based digital forensics in internet voting are *LEChain: A blockchain-based lawful evidence management scheme for digital forensics*, *Using Blockchain Technology to Create a Secure Digital Voting System*, *Survey on Digital E-Voting System by using Blockchain Technology, Towards secure e-voting using Ethereum blockchain, On Secure E-Voting over Blockchain* and *Blockchain Voting and its effects on Election Transparency and Voter Confidence*. This is a very small number. Consequently, the knowledge acquired also spans a limited coverage. Hence a risk of results bias cannot be entirely ruled out.

3.5 Certainty of Evidence

To a greater extent, an internet-based voting system that is integrated into blockchain technology for digital forensics has shown to be more resistant to vote rigging than the ballot paper-based voting system. Of the total consulted studies, 95% of them concur that the ballot paper-based voting system is prone to human errors and electoral data manipulation which can subsequently lead to vote rigging and vote fraud.

From the research and information that we have gathered thus far, we can conclude that apparently there is no known system yet which can be used to effectively address issues of vote rigging and vote fraud in online voting. The currently available processes lack transparency, privacy, integrity, confidentiality and auditability. Therefore, there is a need to have a voting system that is non-comprised and protected. In case of any data tampering attempts, the activities must be swiftly and automatically detected for further investigations. As of now (at the writing of this paper), such a system does not exist.

3.6 Proposed System-Digital Forensic Readiness Model for Internet Voting

In their study, (Muyambo, Omeleze Baror, 2023) proposed a blockchain-based system that could be used to mitigate vote rigging in Internet voting systems. To mitigate issues of vote rigging and vote fraud, this study

introduces the Digital Forensic Readiness Model for Internet Voting (DFRMIV). The model consists of four main layers described below, namely, the vote casting layer, digital forensic data store, electoral board data store and the vote reconciliation layer. The main components of the DFRMIV's model are the voting process, electoral board vote processing, digital forensic vote processing and the vote reconciliation process as shown in Figure 4 below. When a vote is cast, it goes through the Blockchain encryption technology. This technology makes sure that the vote is secure, safe and auditable. After the encryption process, votes are simultaneously stored in the Electoral Board's data repository and the Digital Forensic data repository. The Digital Forensic Readiness process would then merge the two datasets and perform a vote reconciliation process. If there are vote irregularities or vote rigging attempts, the vote reconciliation process would flag this.

Figure 3 below shows a diagrammatic view of DFRMIV's technical details. The first block encloses the voting process, the second block encloses the data repository mechanism and the 3rd block encloses the vote reconciliation process.

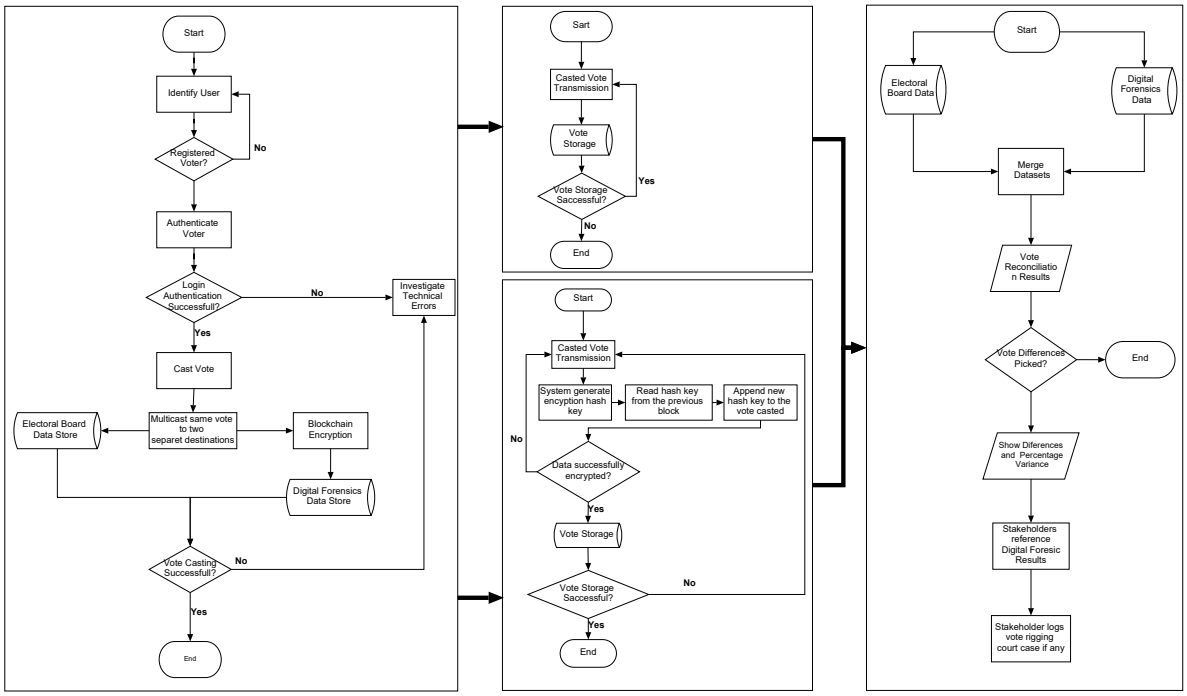

Figure 3: Proposed Blockchain-Based Digital Forensic Model Readiness Model for Internet Voting

3.6.1 Four main layers of the proposed system

- Vote Casting

This is the starting point of the election process. Before vote casting, every voter is required to register to vote. On the Election Day system users would log into the voting system for the vote casting process to begin. Once the user has been successfully verified against the voter's roll and authenticated, they can proceed to the vote-casting phase. The user chooses a candidate of their choice and submits the selection. When the submission process is completed successfully, the user will be automatically logged out. They will be presented with a confirmation of success and a reference number.

- Digital Forensics Data Store

When votes are cast, they are simultaneously distributed into two data repositories which are, the Digital Forensic Data Store and the Electoral Board Data Store. The Digital Forensic Data Store keeps raw data of votes cast. This dataset is used for digital forensic investigations i.e., vote rigging detection. This layer is not government-owned, it is owned by independent service providers.

- Electoral Board Data Store

Electronic votes cast are simultaneously captured into the digital forensic data store and the electoral board data store. This means by default the two data stores should contain exactly the same number of votes. If at any point there is a discrepancy in the number of votes between the digital forensics data store and the

electoral board data store, a possible vote-rigging activity could have occurred. The electoral board data store is used by the Electoral Board for vote counting, auditing and results presentation.

- Vote Reconciliation

This is a Digital Forensic Readiness component. Datasets from both data stores are merged and compared against each other. A difference between the datasets would mean a possible vote-rigging activity has occurred. The digital forensic readiness model for internet voting would automatically detect this and flag all the numeric deviations in detail.

3.6.2 Current state of work

In their study, Vatsa A and Raikar D highlighted the need to have a reliable blockchain-based online voting process to mitigate vote manipulation in an election process (Vatsa, 2021). The authors proposed a five-layer Blockchain Technology based Voting system (BCT-Voting) intending to mitigate vote fraud and data tampering. However, as we studied the author's proposal we found out that this system has several shortcomings. Amongst them is the ability to allow voters to alter their votes after casting. We believe this opens a room for vote tampering as well as vote manipulation. Voters must be able to cast their vote only once, without room to amend the vote thereafter. We also learned that BCT-Voting allows system administrators direct access to plain personal details in the database. Based on the principles of data privacy and cyber security, we hereby argue that this proposed system does not adequately meet the data privacy and voter secrecy checkpoints. Hence our motivation to propose a DFRMFIV system that cushions the shortcomings of the current proposals in the faculty.

3.6.3 DFRMIV evaluation

DFRMIV evaluation points

- Data accessibility – how safe and secure is the data access process? Is access safely granted and maintained?
- Data integrity – the integrity of the dataset in an end-to-end process. The dataset should be the same throughout the process and across systems. It should not be easily altered or manipulated without detection or trace.
- Data verifiability – data and digital transactions must be verifiable at any point in the process. Source and destination datasets should always be aligned. Misalignments should be accounted for (either in audit reports or any other data reconciliation processes).
- Data auditability – the ability to detect and reflect data changes in the process should be met. All transactions must be clearly recorded and the audit records must be easily accessible anytime by stakeholders.
- Digital forensics – datasets and all associated transactions must be securely handled through some robust technologies such as the blockchain in order to provide accurate digital forensics.

4. Discussion

Since the study of digital forensics in internet voting is still relatively new, we were faced with an issue of limited literature for review. Some of the studies lack explicit details such as quantification and source referencing. Some studies based their facts on general knowledge and empirical assumptions. However, according to (Adiputra, CK et al, 2018), it is quite evident that our research findings are well aligned with the little-known knowledge thus far about blockchain-based digital forensics in internet voting. (Kshetri, Vosa, 2018) highlighted that the current ballot box voting system is highly associated with vote rigging and data fraud. (German, Serdult, 2017) highlighted that it is arguable that internet voting increases voter turnout. This we could not attest to as our findings were quite limited to this fact-finding aspect.

This review was not conducted by a team or group but by a single reviewer. This exposes the review process to a risk of bias and inconsistency due to a lack of peer review and discussion. However, even though this review was conducted by a single reviewer, source references were clearly highlighted and the content referenced was understandably explained. Due to a lack of sufficient studies in the research field, not so many studies of relevance were found in the searched databases. In order to enhance clear communication, we only referenced English written studies. In avoidance of outdated information, we only referenced studies that were published not more than ten years ago from the writing of this publication.

From this review, implications for practice and policy are that ballot paper-based voting systems are quite vulnerable to vote rigging and vote fraud.

5. Other Information

This review was conducted as a Masters research student project. The paper was presented at the European Conference on Cyber Security (ECCWS) on the 24th of June 2023 in Greece, Athens. The full paper: https://papers.academic-conferences.org/index.php/eccws/article/view/1186/1216 . The paper has since been published to the world of academics for referencing. The research was self- funded (student). No external financial institutes or donor contributions. Therefore, this review was not registered under any organization. The author does not have any interests to declare.

References

Abuidris, Y., Kumar, R. and Wenyong, W., 2019, December. A survey of blockchain based on e-voting systems. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications* (pp. 99-104).

Abuidris, Y., Kumar, R. and Wenyong, W., 2019, December. A survey of blockchain based on e-voting systems. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications* (pp. 99-104).

Adiputra, C.K., Hjort, R. and Sato, H., 2018, October. A proposal of blockchain-based electronic voting system. In *2018 second world conference on smart trends in systems, security and sustainability (WorldS4)* (pp. 22-27). IEEE.

Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M. and Almusali, M., 2023. Privacy- Preserving E-Voting System Supporting Score Voting Using Blockchain. *Applied Sciences*, *13*(2), p.1096.

Anitha, V., Caro, O.J.M., Sudharsan, R., Yoganandan, S. and Vimal, M., 2023. Transparent voting system using blockchain. *Measurement: Sensors*, *25*, p.100620.

Ayed, A.B., 2017. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *9*(3), pp.01-09.

Bartolucci, S., Bernat, P. and Joseph, D., 2018, May. SHARVOT: secret SHARe-based VOTing on the blockchain. In *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain* (pp. 30-34).

Chaabane, F., Ktari, J., Frikha, T. and Hamam, H., 2022. Low power blockchained e-vote platform for university environment. *Future Internet*, *14*(9), p.269.

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G., 2022. Electronic voting system using an enterprise blockchain. *Applied Sciences*, *12*(2), p.531.

Desai, S., Han, M., Li, L., Li, Z., He, J. and Xu, X., 2019, September. Untampered Electronic Voting in Entertainment Industry: A Blockchain-based Implementation. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (pp. 166-166).

Dimitri, N., 2022. Quadratic voting in blockchain governance. *Information*, *13*(6), p.305.

Djanali, S., Nugraha, D.P., Studiawan, H. and Pratomo, B.A., 2018. Vote identification and integrity of ballot in paper-based e-voting system. *Electronic Government, an International Journal*, *14*(3), pp.240- 254.

Englbrecht, L. and Pernul, G., 2020, August. A privacy-aware digital forensics investigation in enterprises. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

Fatrah, A., El Kafhali, S., Haqiq, A. and Salah, K., 2019, October. Proof of concept blockchain-based voting system. In *Proceedings of the 4th International Conference on Big Data and Internet of Things* (pp. 1-5).

Germann, M. and Serdült, U., 2017. Internet voting and turnout: Evidence from Switzerland. *Electoral studies*, *47*, pp.1-12.

Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. and Hjálmtýsson, G., 2018, July. Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983- 986). IEEE.

Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. and Hjálmtýsson, G., 2018, July. Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983- 986). IEEE.

Holmes, C., 2022. How Blockchain Technology could support Democracy and E-Voting. *The Journal of The British Blockchain Association*.

Hossain, S.S., Arani, S.A., Rahman, M.T., Bhuiyan, T., Alam, D. and Zaman, M., 2019, December. E- voting system using blockchain technology. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications* (pp. 113-117).

Huang, J., He, D., Obaidat, M.S., Vijayakumar, P., Luo, M. and Choo, K.K.R., 2021. The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR)*, *54*(3), pp.1- 28.

Kshetri, N. and Voas, J., 2018. Blockchain-enabled e-voting. *Ieee Software*, *35*(4), pp.95-99.

Lahane, A.A., Patel, J., Pathan, T. and Potdar, P., 2020. Blockchain technology based e-voting system. In *ITM Web of Conferences* (Vol. 32, p. 03001). EDP Sciences.

Leune, K. and Punjwani, J., 2021. Enhancing Electronic Voting With A Dual-Blockchain Architecture. *Ledger*, *6*.

Li, M., Lal, C., Conti, M. and Hu, D., 2021. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, *115*, pp.406-420.

McCorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S.F. and Hao, F., 2021. On secure e-voting over blockchain. *Digital Threats: Research and Practice (DTRAP)*, *2*(4), pp.1-13.

Moura, T. and Gomes, A., 2017, June. Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th annual international conference on digital government research* (pp. 574-575).

Moura, T. and Gomes, A., 2017, June. Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th annual international conference on digital government research* (pp. 574-575).

Muyambo, E. and Baror, S.O., 2023, June. Digital Forensic Readiness Model for Internet Voting. In *European Conference on Cyber Warfare and Security* (Vol. 22, No. 1, pp. 657-667).

Neloy, M.N., Wahab, M.A., Wasif, S., All Noman, A., Rahaman, M., Pranto, T.H., Haque, A.B. and Rahman, R.M., 2023. A remote and cost-optimized voting system using blockchain and smart contract. *IET Blockchain*, *3*(1), pp.1-17.

Neloy, M.N., Wahab, M.A., Wasif, S., All Noman, A., Rahaman, M., Pranto, T.H., Haque, A.B. and Rahman, R.M., 2023. A remote and cost-optimized voting system using blockchain and smart contract. *IET Blockchain*, *3*(1), pp.1-17.

Raikar, D. and Vatsa, A., 2021. BCT-Voting: A Blockchain Technology Based Voting System. In *The 27 th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21), July* (pp. 26-29).

Raikar, D. and Vatsa, A., 2021. BCT-Voting: A Blockchain Technology Based Voting System. In *The 27 th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21), July* (pp. 26-29).

Ryu, J.H., Sharma, P.K., Jo, J.H. and Park, J.H., 2019. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The Journal of Supercomputing*, *75*, pp.4372-4387.

Shah, A., Sodhia, N., Saha, S., Banerjee, S. and Chavan, M., 2020. Blockchain enabled online-voting system. In *ITM Web of Conferences* (Vol. 32, p. 03018). EDP Sciences.

Singh, S., Wable, S. and Kharose, P., 2021. A review of e-Voting system based on blockchain technology. *International Journal of New Practices in Management and Engineering*, *10*(04), pp.09-13.

Smith, R., 2016. Confidence in paper-based and electronic voting channels: evidence from Australia. *Australian Journal of Political Science*, *51*(1), pp.68-85.

Wahab, Y., Ghazi, A., Al-Dawoodi, A., Alisawi, M., Abdullah, S., Hammood, L. and Nawaf, A., 2022. A Framework for Blockchain Based E-Voting System for Iraq. *International Journal of Interactive Mobile Technologies*, *16*(10).

Wei, C.C.Z. and Wen, C.C., 2018. Blockchain-based electronic voting protocol. *JOIV: International Journal on Informatics Visualization*, *2*(4-2), pp.336-341.

Yavuz, E., Koç, A.K., Çabuk, U.C. and Dalkılıç, G., 2018, March. Towards secure e-voting using ethereum blockchain. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-7). IEEE.