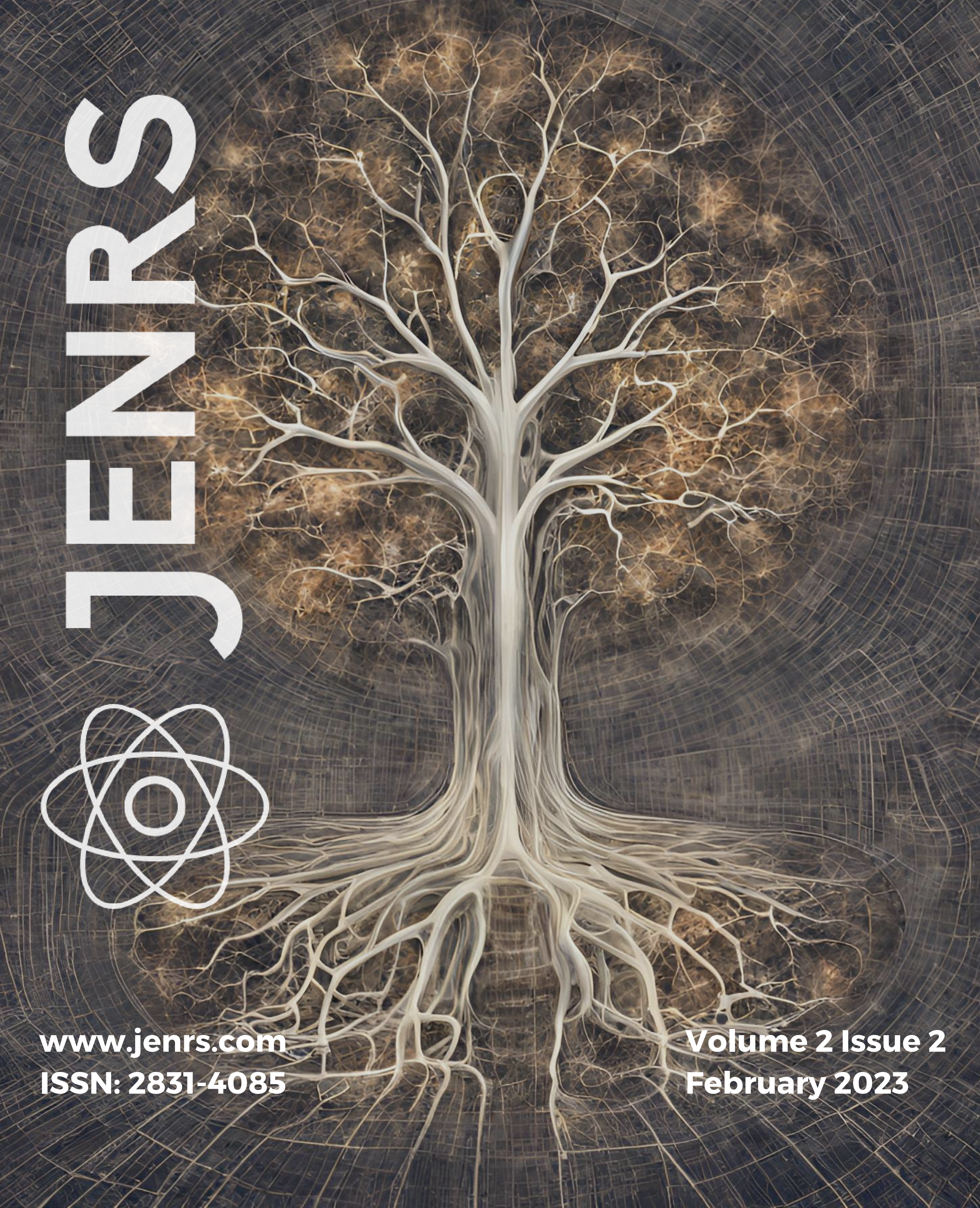
JOURNAL OF ENGINEERING RESEARCH & SCIENCES



JENRS

www.jenrs.com
ISSN: 2831-4085

Volume 2 Issue 2
February 2023

EDITORIAL BOARD

Editor-in-Chief

Prof. Paul Andrew
Universidade De São Paulo, Brazil

Editorial Board Members

Dr. Jianhang Shi
Department of Chemical and Biomolecular Engineering, The Ohio State University, USA

Dr. Sonal Agrawal
Rush Alzheimer’s Disease Center, Rush University Medical Center, USA

Dr. Unnati Sunikumar Shah
Rush Alzheimer’s Disease Center, Rush University Medical Center, USA

Prof. Anle Mu
School of Mechanical and Precision Instrument Engineering, Xi’an University of Technology, China

Dr. Jianhui Li
Molecular Biophysics and Biochemistry, Yale University, USA

Dr. Lixin Wang
Department of Computer Science, Columbus State University, USA

Dr. Prabhash Dadhich
Biomedical Research, CellfBio, USA

Dr. Żywiołek Justyna
Faculty of Management, Czestochowa University of Technology, Poland

Dr. Anna Formics
National Research Council, Istituto di Analisi dei Sistemi ed Informatica, Italy

Prof. Kamran Iqbal
Department of Systems Engineering, University of Arkansas Little Rock, USA

Dr. Ramcharan Singh Angom
Biochemistry and Molecular Biology, Mayo Clinic, USA

Dr. Qichun Zhang
Department of Computer Science, University of Bradford, UK

Dr. Mingsen Pan
University of Texas at Arlington, USA

Ms. Madhuri Inupakutika
Department of Biological Science, University of North Texas, USA

Editorial

In this edition of our journal, we present three exceptional research papers that address vital issues ranging from mental health during pandemics to the security of digital data and the transparency of agro-food certification. Each study offers innovative approaches and detailed analyses that contribute significantly to their respective fields.

The first paper examines the profound impact of pandemics on the mental well-being of medical students and their parents. With the ongoing emergence of new coronavirus variants, this study provides crucial insights into the psychological effects and highlights factors contributing to mental health deterioration. Through a cross-sectional study involving 438 participants and using the Warwick–Edinburgh Mental Wellbeing Scale (WEMWBS), the authors found that 35.2% of respondents showed signs of probable depression, while only 6.4% exhibited high mental well-being. The comparison between students and parents revealed that a significant proportion of students (44.7%) suffered from probable depression compared to their parents (43.8%), who mostly had average mental well-being. This research underscores the urgent need for targeted mental health interventions for both medical students and their families during such crises [1].

Digital multimedia assets are integral to modern communication, making their security paramount. The second paper explores the evolving field of steganography for secure information concealment within digital audio files. By employing advanced cryptographic techniques, the study offers a robust framework for secure communication that mitigates potential risks and vulnerabilities. The research emphasizes the importance of reliable steganographic methods in hiding significant amounts of secret data within digital images and audio files, thereby enhancing the confidentiality of sensitive information. This work contributes to the development of more secure digital communication systems, ensuring that crucial information remains protected against unauthorized access [2].

The third paper introduces an innovative framework for the certification of agro products using smart contracts and blockchain-based non-fungible tokens (NFTs). Utilizing the ERC-1155 Ethereum token standard, the authors developed a system that ensures the uniqueness and traceability of each harvest. By deploying and testing the framework on the Ethereum test net blockchain, the study demonstrates how consumers can access Third-party Certificates (TPC) via an Android app, promoting transparency and trust in the agro-food supply chain. The implementation of blockchain technology in this context reduces counterfeiting and greenwashing, fostering sustainable buying habits and enhancing food safety. This research highlights the potential of blockchain to revolutionize agro-food certification and supply chain transparency [3].

The three papers presented in this edition exemplify the innovative and impactful research that our journal strives to publish. From addressing mental health challenges during pandemics to enhancing digital data security and revolutionizing agro-food certification, these studies provide valuable contributions to their fields. We are honored to share these insights with our readers and anticipate that they will inspire further advancements and research.

References:

[1] M. Khan, M. Ibrahim, M.S. Shabbir, M.H. Tofique, M.N. Khalili, M. Asad, M. Ahmed, M. Haroon, S. Zainab, "COVID-19 Pandemic and Mental Well-Being: A Study Conducted on Medical Students and Their Parents in a Private Medical College in Pakistan," Journal of Engineering Research and Sciences, vol. 2, no. 2, pp. 1–7, 2023, doi:10.55708/js0202001.

[2] B.B. Oo, “Applied Salt Technique to Secure Steganographic Algorithm,” Journal of Engineering Research and Sciences, vol. 2, no. 2, pp. 8–14, 2023, doi:10.55708/js0202002.

[3] R.B. Dos Santos, R.P. Pantoni, N.M. Torrisi, “Blockchain Tokens for Agri-Food Supply Chain,” Journal of Engineering Research and Sciences, vol. 2, no. 2, pp. 15–23, 2023, doi:10.55708/js0202003.

Editor-in-chief

Prof. Paul Andrew

JOURNAL OF ENGINEERING RESEARCH AND SCIENCES

Volume 2 Issue 2 **February 2023**

CONTENTS

Received: 24 November, 2022, Revised: 21 January 2023, Accepted: 25 January 2023, Online: 22 February, 2023

DOI: https://doi.org/10.55708/js0202001

COVID-19 Pandemic and Mental Well-Being: A Study Conducted on Medical Students and Their Parents in a Private Medical College in Pakistan

Misha Khan *, **Mufliha Ibrahim**, **Muhammad Saad Shabbir**, **Muhammad Huzaifa Tofique, Muhammad Naheel Khalili, Muhammad Asad, Muhammad Ahmed, Muhammad Haroon, Saima Zainab**

Liaquat National Hospital and Medical College, Karachi, Pakistan
*Corresponding author: Misha Khan, mishashabbir39@gmail.com

ABSTRACT: Pandemics always have a significant effect on the physical, mental, and financial status of people in general. With new variants of coronavirus emerging now and then, it is difficult to process the sudden changes and new healthcare implementations for all individuals. In this situation, our objective was to assess the mental-wellbeing of medical students and their parents and highlight factors that could be associated with their mental-wellbeing deterioration. This is a cross-sectional study in which the non-probability consecutive sampling technique was used. Our sample size was 219 for each population (i.e., parents and medical students). Two questionnaires were designed, one for parents and another for students, each consisting of a personal information section (including personal data and COVID-related questions) and a mental well-being assessing section with the Warwick–Edinburgh Mental Wellbeing Scale (WEMWBS). Descriptive data analysis and all calculations are done using SPSS version 22. A total of 438 responses indicates that 35.2% (n = 154) of respondents have probable depression, 14.6% (n = 64) have possible depression, 43.8% (n = 192) have average mental well-being, and only 6.4% (n = 28) have high mental well-being. A comparison of scores for both groups show that the majority of students (44.7%) have probable depression, while most parents (43.8%) have average mental well-being. High mental well-being was found only in 3.2% medical students and 9.2% of their parents. Hence, the realization of the effects of different factors, including coronavirus, on both groups is essential.

KEYWORDS: Covid-19, pandemic, coronavirus, mental well-being, parents, medical students, MBBS students

1. Introduction

Pandemics always take a toll on people's physical health. They are also seen to have significant psychological impacts [1], and the COVID-19 pandemic is no different. Due to its highly contagious nature, it has been advised to limit as much social interaction as possible. Therefore, the lockdown was implemented in various countries, and it has proved quite effective in reducing the number of new COVID-19 cases [2].

The first case of coronavirus in Pakistan was reported from Karachi on February 26, 2020, which eventually led to the implementation of a lockdown in Pakistan on March 13, 2020, by closing borders and educational institutes in the initial phase that was followed by a complete lockdown in multiple cities, forcing the general population to confine themselves to their homes. Although the lockdown was supposed to be lifted in a month due to the degrading conditions, it kept on delaying. On August 9, 2021, the lockdown was eased, but still, there are many restrictions in the state, like fixed business hours, only vaccinated citizens being allowed in public places, 50% attendance of staff in offices, students in institutions, etc.

This pandemic has shaken the global health and economic systems to their core. Almost 800 million people have been pushed down the line of poverty, with nearly 3.3 billion people at risk of losing their livelihoods [3].

With people losing their jobs and children studying from home due to the lockdown, parents and students faced a dilemma. Although being in lockdown would naturally mean parents had more time with the kids, with no end to this situation in sight, the household environment got stressful. As was proved by a longitudinal, observational study conducted in the United States, parent stress increased substantially during COVID-19 and has not returned to its pre-COVID-19 level [4]. It was also recognized in a cross-sectional study done at the University of Wisconsin-Madison and the University of Southern California that 39.4% of parents reported moderate to severe anxiety and/or depression symptoms. Most of these parents testified that their current emotions or concerns interfered with their ability to parent. These effects were more profound in females and low-income families [5].

The COVID-19 outbreak also negatively affected the mental well-being of medical students. An observational study conducted in the Department of Physiology, College of Medicine, King Saud University shows that 56.2% of students suffered academically, 44.1% showed emotional detachment from family and friends, and 23.5% were disheartened [6]. Also, in an online survey in Jordan, about 58.4% of medical students seemed concerned about the inability to get clinical sessions and labs [7]. Likewise, the results of a survey in Australia show that the mental well-being of 68% of medical students declined during COVID-19 [8].

Parents and medical students living in Pakistan, a developing country, cannot be put in the same category as parents and students from other nations, as Pakistan's government couldn't support the families as much as governments in developed countries did. Moreover, the median household income for a family living in Pakistan is $508.977, compared to $9,733 [9,10] in the rest of the world. The average family size in Pakistan is 6.7, as compared to the rest of the world, which is 4.9 [11,12]. Also, extended family systems are very common in Pakistan.

A parent is the caretaker of a child. Their main role is to provide for and nurture their children in the best possible manner. The COVID-19 situation took its toll on this role, thus putting stress on parents. Research conducted in Italy showed that 17 percent of the sample collected experienced significant parenting-related exhaustion during the COVID-19 outbreak [13]. In 2017, a research paper highlighted the evidence of the association of stress with ineffective parenting and poor child adjustment [14]. In another study, over-reactive parents, who showed constant expressions of anger and arguing, led to children expressing similar personality traits as their parents [15]. Hence, the well-being of parents has a direct role in the proper upbringing and welfare of the children [16, 17]

Moreover, as shown in the results of the study conducted in US medical schools [18], more than 20 percent of the students are considering a shift in their field of specialization after the COVID-19 pandemic, mostly due to the shift in financial status and mental well-being in their household. Therefore, along with parents, it is important to find out the effects this pandemic has had on medical students as well.

The COVID-19 pandemic has caused significant damage to different aspects of society. Even though it affected everyone equally, the influence of this pandemic on parents and medical students has been mostly overlooked. The purpose of this research is to take into consideration parents' and medical students' mental well-being during the COVID-19 pandemic. So that positive steps can be taken to ensure a better quality of life for both parents and students.

2. Materials and methods

2.1. Study design, sampling technique, and participants:

This is a cross-sectional study in which a non-probability consecutive sampling technique was used. All medical students and their parents were included in this study, except students or parents who have any diagnosed psychological disorder, whether on medications or not. Prior consent was obtained from all participants. No harm or benefit was subjected to any participant. The anonymity of every participant and the confidentiality of their data was ensured.

2.2. Sample size:

The sample size was calculated for two independent population proportions using the online sample size calculator "clincal.com" [19]. Using the proportion of increased stress after children's return to school during COVID-19 among population 1 (parents) as 55% [4] and deterioration of mental well-being during COVID-19 among population 2 (medical students) as 68% [8], the margin of error is 5%, the confidence level is 95%, and the power is 80%. The final sample size calculated is at least 219 in each group.

2.3. Data collection procedure:

For 2 years, on and off, the lockdown was implemented, and data was physically collected between February 2022 and June 2022, during new waves of omicron and delta variants of coronavirus. In this survey, physical data were collected from 219 medical students (n1) and their parents (n2). A total of 470 (N) forms were received, 219 from students and 251 from their parents, of which 32 were excluded due to incomplete data or diagnosed psychological disorders. Before participation, consent forms were signed by all participants. Questionnaires were distributed among students from the first year to the final year of medical school, one for the students and two for their parents, which were then filled out individually by all participants and returned to us.

2.4. Instrument:

Our team designed a questionnaire consisting of a section containing demographic or personal information, in which COVID-related questions were also included, and a section assessing mental well-being with the Warwick–Edinburgh Mental Wellbeing Scale (WEMWBS), a 14-item scale. The scoring range for each item was from 1–5, and the total score is from 14–70. This provided a WEMWBS cut point of 40 or less for probable depression, 41–44 for possible depression, 45–59 for average mental well-being, and scores of 60 or more for high mental well-being.

2.5. Data analysis:

Descriptive data analysis and all calculations were done using SPSS version 22. The mean and standard deviation were calculated for continuous variables like age, family size, and WEMWBS scores. Frequency and percentage were calculated for categorical variables like gender, marital status, employment status, and monthly income. By applying Chi-square and Fischer exact tests, the association between qualitative variables was determined. An independent t-test was used to find the mean difference between the WEMWBS scores of both groups. A p-value of <0.05 will be considered significant.

3. Results

3.1. Report of parents' responses:

The results of the response show a contribution of 54.8% males and 45.2% females, with a mean age of 51.54 years. Most respondents belong to the nuclear family type (71.7%), and 13.2% of them are single parents. Variations were found in the answers to the question of employment status: 56.6% were employed, 36.1% were homemakers (mostly females), 1.4% chose the category of others, and 5.9% were unemployed. The majority of the participants were of high socioeconomic status (65.4%) and owned their homes (83.6 %). Parents usually had no (43.4%) or one (42.9%) comorbidity. Family COVID positivity was reported at 56.6%, whereas 32.4% of them tested positive for COVID. 28.8% of them lost their close ones to COVID. Their WEMWBS mean score was 47.21. In parents, the probable depression was 25.6%, the possible depression was 13.2%, the average mental well-being was 51.6%, and the high mental well-being was 9.6% in Table 1.

3.2. Report of Students' responses:

Students taking part in this survey were 68% females and 32% male with a mean age of 20.69 years. Responses comprise 38.8% from the third year of medical school, 33.2% from the second year, 12.8% from the fourth year, 7.8% from the first year, and 7.3% from the final year, with an average GPA of 3.08 (SD = 0.398) across all years. Hostilities were 21.5% while the rest of the participants were day scholars. Similar to their parents' results, the majority live in a nuclear family system (74%) and come from a high socioeconomic class (81.5%). About 64.8% of students reported a decrease in study hours, 16.9% reported an increase in their study hours, and 18.3% reported that their study hours remained unchanged. Across all five years, the mean WEMWBS score was 41.68. In students, probable depression was scrutinized at 44.7%, possible depression at 16.0%, average mental well-being at 36.1%, and high mental well-being at 3.2% (Table 1)

3.3. Comparison of Parents' and Students' Mental - well-being:

An independent t-test was applied to compare the means of parents' and students' WEMWBS scores, and the mean difference was found to be statistically significant (p<0.001). The mean difference can also be seen in Figure 1. A Pearson chi-square test was used to determine if there was a significant relationship between parents' and students' well-being, and the results were highly significant(0.001).

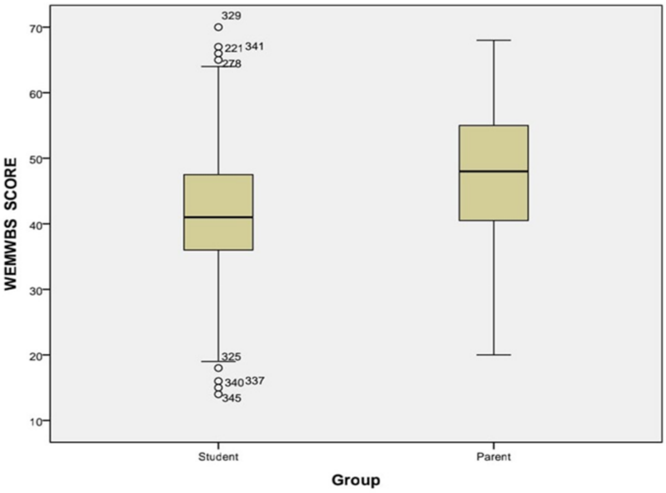


Figure 1: Box and whisker plots showing variation in the WEMWBS scores of students and parents.

Table 1: Responses of parents and students and their corresponding p-values

		Parents n (%)	Students n (%)	P-value
Gender	Male	120 (54.8)	70 (32)	<0.001
	Female	99(45.2)	149 (68)	
Age	Mean ±SD	51.54 ±6.766	20.69 ±1.228	<0.001
Family type	Nuclear	157(71.7)	162 (74)	0.591
	Extended	62(28.3)	57 (26)	
Household income	Under Rs. 25000	6 (3.4)	0 (0)	<0.001
	Between Rs.25,000 - Rs.50,000	7 (3.9)	4 (2.2)	
	Between Rs.50,000 - Rs.75,000	18 (10.1)	3 (1.7)	
	Between Rs.75,000- Rs.1,00,000	31 (17.3)	26 (14.6)	
	Rs.1,00,000 or over	117 (65.4)	145 (81.5)	
Family tested positive for covid	Yes	124 (56.6)	140 (63.9)	0.118
	No	95 (43.4)	79 (36.1)	
Deaths by covid	Yes	63 (28.8)	52 (23.7)	0.232
	No	156 (71.2)	167 (76.3)	
Tested positive for covid	Yes	71 (32.4)	61 (27.9)	0.289
	No	148 (67.6)	158 (72.1)	
WEMWBS score	Mean ±SD	47.21 ±9.839	41.68 ±9.684	<0.001
Mental Well-being	Probable depression	56 (25.6)	98 (44.7)	<0.001
	Possible depression	29 (13.2)	35(16)	
	Average mental well-being	113 (51.6)	79 (36.1)	
	High mental well-being	21 (9.6)	7 (3.2)	

4. Discussion

The COVID-19 pandemic was a time of intense uncertainty, fear, and stress, and its effects were seen in both groups' mental well-being, which was found to be on the lower end of the spectrum, more in students than in parents. Through an independent sample t-test, the mean difference between the WEMWBS scores of participants who had tested positive for COVID-19 during the pandemic and those who didn't were found to be significant (p=0.019) which points to the possibility that they might still be suffering from the after-effects of being quarantined or be on their path to recovery. Using the Pearson chi-square test, no significant relationship was found between participants' mental well-being status in nuclear and extended family systems (p = 0.845).

Results of this study show that students who are suffering from probable depression are 44.7%, which is alarmingly high; however, one thing that stood out in the results of this study was that the students of different years had different levels of mental well-being (Figure 2). Second and fourth-year students had the best mental health, which can be attributed in part to the fact that second-year students had already been exposed to the medical world in their first year, so they knew what steps to take to perform well. Similarly, fourth-year students also became familiar with their clinical rotation schedule, due to which they reported relatively higher mental well-being despite the pandemic. The study conducted on medical students in Australia [8] showed somewhat similar results: first-year students showed the highest level of distress, with 24% of first-year students scoring 'very high' The third year showed surprisingly lower rates of distress, with only 9% of students scoring in the 'very high' category, as compared to 44.7% of students showing probable depression in this study. These findings on student mental well-being are important to address, as poor mental health in medical students may make them less enthusiastic physicians in the future, which will ultimately affect the delivery of healthcare services in the country. Medical colleges should organize regular group sessions to keep their students' mental health in check. In a study done in Canada, it was found that participation in extracurricular activities or school sports was associated with better mental health outcomes in children and youth [20]. This emphasizes the importance of being proactive in hobbies where a student finds peace and thoroughly enjoys himself/herself while partaking in those activities, whether extracurriculars or book reading, for example. PMC should construct some sort of course in their curriculum where the students can easily relieve themselves from the intensely high-paced and competitive environment that medical colleges are known to have.

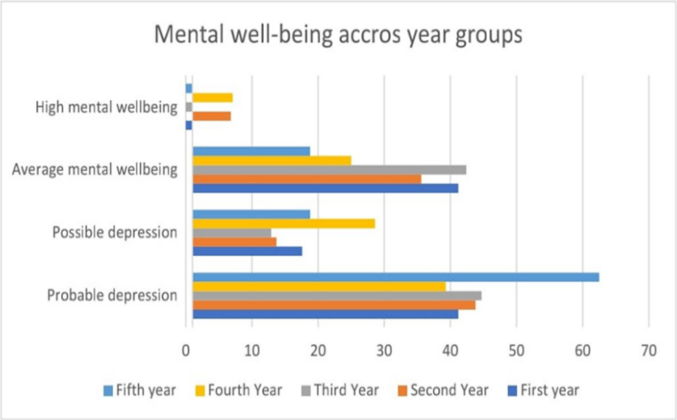


Figure 2: Graph comparing percentages of mental well-being across all year groups

Although the majority of the parents were found to have average mental well-being, a large proportion of parents had probable depression at 25.6% and high mental well-being was only seen in 9% of the parental population, which is worrying and calls for action. If we were to compare these results to the study done on parents in Richmond, US [4], we would find that only 22.4% of parents showed positive results for high stress; this had increased from 3.5%, which was reported before the pandemic. This can be because in Pakistan there are a greater number of people living in joint families as compared to America, where they have nuclear family systems, so added family members tend to increase stress levels. It was also noted that 46.9% of the single parents had probable depression and 18.8% had possible depression, as compared to the proportions of 21.9% and 12.3%, respectively, in non-single parents. The mean difference between the WEMWBS scores of single and non-single parents was also found to be significant (p = 0.002) when an independent sample t-test was applied. This finding can be supported by a study conducted on single parents, which proved that single parents have a higher prevalence of poor mental health compared to partnered parents [21]. Single parents were affected more than parents who were not single. This may be the case because single parents must have faced the socioeconomic burden alone without the financial and emotional support of a partner, thus making them more vulnerable to declining mental well-being. A significant mean difference was also found between the WEMWBS scores of parents with comorbidities and those who didn't (p<0.001). Moreover, in Pakistan, there is a lack of family security, political unrest, and a poor standard of living. All of these factors combine to cause a disproportionate amount of stress in a Pakistani parent.

According to UNICEF, the good mental well-being of caregivers, whether they're parents or anyone else, is key to thriving families [22]. and thus, they must have high mental well-being. Promotion of family counseling through mass media should be done to improve family resilience both before and during any crisis such as this pandemic. Moreover, institutions should regularly invite parents to seminars and make them aware of the importance of mental well-being through the statistical data provided in this study.

Limitations include the cross-sectional study design, self-reported questionnaires by students on behalf of parents, and higher female students' participation. Also, there was a slight difference in the reporting of socioeconomic status by parents and their children, which we assume means that their children do not know about their monthly household income or that many people went into financial losses during COVID that their children do not know about.

5. Conclusions

In a nutshell, this study shows highly significant results. Students' well-being was seen to be most affected by the coronavirus, whereas parents' mental well-being was average. As these groups are highly vulnerable to depression, creating awareness about their mental health is crucial, especially during this time. We hope that the sensitivity of this issue will be understood and that together we will bring about a positive change.

List of Abbreviations

COVID-19 (coronavirus disease of 2019), MBBS (Bachelor of Medicine, Bachelor of Surgery), WEMWBS (Warwick-Edinburgh Mental Well-being Scale).

Conflict of Interest

The authors declare no conflict of interest.

Funding Source:

The authors received no financial support for the research, authorship, and publication of this article.

References

[1] D. Cuadra-Martínez, P.J. Castro-Carrasco, J. Sandoval-Díaz, D. Pérez-Zapata, D. Mora Dabancens, "COVID-19 y comportamiento psicológico: revisión sistemática de los efectos psicológicos de las pandemias del siglo XXI [COVID-19 and psychological behavior: a systematic review of the psychological effects of 21st century pandemics]," *Revista Médica de Chile*, vol. 148, no. 8, pp. 1139–1154, 2020, doi:10.4067/S0034-98872020000801139.

[2] V. Alfano, S. Ercolano, "The Efficacy of Lockdown Against COVID-19: A Cross-Country Panel Analysis," *Applied Health Economics and Health Policy*, vol. 18, no. 4, pp. 509–517, 2020, doi:10.1007/s40258-020-00596-3.

[3] World Health Organization, Impact of COVID-19 on people's livelihoods, their health and our food systems, https://www.who.int/news/item/13-10-2020-impact-of-covid-19-on-people's-livelihoods-their-health-and-our-food-systems, 2020.

[4] E.L. Adams, D. Smith, L.J. Caccavale, M.K. Bean, "Parents Are Stressed! Patterns of Parent Stress Across COVID-19," *Frontiers in Psychiatry*, vol. 12, , 2021, doi:10.3389/fpsyt.2021.626456.

[5] M.L. Kerr, H.F. Rasmussen, K.A. Fanning, S.M. Braaten, "Parenting During <scp>COVID</scp> -19: A Study of Parents' Experiences Across Gender and Income Levels," *Family Relations*, vol. 70, no. 5, pp. 1327–1342, 2021, doi:10.1111/fare.12571.

[6] S.A. Meo, D.A.A. Abukhalaf, A.A. Alomar, K. Sattar, D.C. Klonoff, "COVID-19 Pandemic: Impact of Quarantine on Medical Students' Mental Wellbeing and Learning Behaviors," *Pakistan Journal of Medical Sciences*, vol. 36, no. COVID19-S4, 2020, doi:10.12669/pjms.36.COVID19-S4.2809.

[7] K. Seetan, M. Al-Zubi, Y. Rubbai, M. Athamneh, A. Khamees, T. Radaideh, "Impact of COVID-19 on medical students' mental wellbeing in Jordan," *PLOS ONE*, vol. 16, no. 6, pp. e0253295, 2021, doi:10.1371/journal.pone.0253295.

[8] Z. Lyons, H. Wilcox, L. Leung, O. Dearsley, "COVID-19 and the mental well-being of Australian medical students: impact, concerns and coping strategies used," *Australasian Psychiatry*, vol. 28, no. 6, pp. 649–652, 2020, doi:10.1177/1039856220947945.

[9] CEIC, Pakistan Household Income per Capita 2005-2019, https://www.ceicdata.com/en/indicator/pakistan/annual-household-income-per-capita, 2019.

[10] G. Phelps, S. Crabtree, Worldwide, Median Household Income About $10,000, 2013.

[11] National Institute of Population Studies-NIPS, Pakistan Maternal Mortality Survey, Islamabad/Pakistan, 2020.

[12] S. Kramer, With billions confined to their homes worldwide, which living arrangements are most common? https://www.pewresearch.org/fact-tank/2020/03/31/with-billions-confined-to-their-homes-worldwide-which-living-arrangements-are-most-common/, 2020.

[13] M. Spinelli, F. Lionetti, M. Pastore, M. Fasolo, "Parents' Stress and Children's Psychological Problems in Families Facing the COVID-19 Outbreak in Italy," *Frontiers in Psychology*, vol. 11, 2020, doi:10.3389/fpsyg.2020.01713.

[14] M.E. McQuillan, J.E. Bates, Parental Stress and Child Temperament, Springer International Publishing, Cham: 75–106, 2017, doi:10.1007/978-3-319-55376-4_4.

[15] P. Prinzie, C.M. van der Sluis, A.D. de Haan, M. Deković, "The Mediational Role of Parenting on the Longitudinal Relation Between Child Personality and Externalizing Behavior," *Journal of Personality*, pp. no-no, 2010, doi:10.1111/j.1467-6494.2010.00651.x.

[16] S.B. Wolicki, R.H. Bitsko, R.A. Cree, M.L. Danielson, J.Y. Ko, L. Warner, L.R. Robinson, "Mental Health of Parents and Primary Caregivers by Sex and Associated Child Health Indicators," *Adversity and Resilience Science*, vol. 2, no. 2, pp. 125–139, 2021, doi:10.1007/s42844-021-00037-7.

[17] Centers for Disease Control and Prevention (CDC), Mental health of children and parents —a strong connection, https://www.cdc.gov/childrensmentalhealth/features/mental-health-children-and-parents.html#:~:text=The%20mental%20health%20of%20children, support%20their%20children's%20mental%20health, 2021.

[18] Y.M. Byrnes, A.M. Civantos, B.C. Go, T.L. McWilliams, K. Rajasekaran, "Effect of the COVID-19 pandemic on medical student career perceptions: a national survey study," *Medical Education Online*, vol. 25, no. 1, 2020, doi:10.1080/10872981.2020.1798088.

[19] Clincal.com, Sample Size Calculator (online), https://clincalc.com/Stats/SampleSize.aspx, Nov. 2021.

[20] K. LaForge-MacKenzie, K. Tombeau Cost, K.C. Tsujimoto, J. Crosbie, A. Charach, E. Anagnostou, C.S. Birken, S. Monga, E. Kelley, C.L. Burton, R. Nicolson, S. Georgiades, D.J. Korczak, "Participating in extracurricular activities and school sports during the COVID-19 pandemic: Associations with child and youth mental health," *Frontiers in Sports and Active Living*, vol. 4, 2022, doi:10.3389/fspor.2022.936041.

[21] K.A. Kong, H.Y. Choi, S.I. Kim, "Mental health among single and partnered parents in South Korea," *PLOS ONE*, vol. 12, no. 8, pp. e0182943, 2017, doi:10.1371/journal.pone.0182943.

[22] S. Friedlander, B. Perks, Caregiver mental health and well-being: The key to thriving families, https://www.unicef.org/blog/caregiver-mental-health-well-being-key-thriving-families, 2022.

Copyright: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (https://creativecommons.org/licenses/by-sa/4.0/).

Received: 30 December, 2022, Revised: 06 February 2023, Accepted: 07 February, 2023, Online: 22 February, 2023

DOI: https://doi.org/10.55708/js0202002

Applied Salt Technique to Secure Steganographic Algorithm

Bo Bo Oo*

Edinburgh Napier University, School of Computing, Edinburgh, EH10 5DT, UK

*Corresponding author: Bo Bo Oo, +44 77 7863 0269, bobooo.1249@gmail.com

ABSTRACT: Digital multimedia assets, including photographs, movies, and audio files, have become a staple of contemporary life. Steganography is a method for undetectable information concealment in these files. One can communicate messages to another by modifying multimedia signals so that a human would be unable to tell the difference between the original signal and the altered one. The widespread use of digital data in practical applications has prompted the development of new and efficient methods for ensuring its security. Steganographic techniques can be used to, at least in part, achieve efficient secrecy. There have been suggested new and adaptable audio steganographic techniques. By using cryptography, readable language is converted to unintelligible data. In order to send and receive text, multimedia, or other important digital files safely, this paper discusses secure communication media. To have secure communication tools, the tools must lessen potential risks and weaknesses. Therefore, the primary factor to take into account for creating a solid communication system is transferred media. The objective of steganographic systems is to find a secure and reliable method to hide a significant amount of secret data. This research focuses on digital image audio steganography, which has become a popular method for data concealment.

KEYWORDS: Steganography & Cryptography, Secure communication media, Salt Encryption, AES, Steganography with SHA-256

1. Introduction

In order to share information across many geographies through digital communication, a number of new technologies are constantly developing. Information can sometimes include user privacy, confidential data, and other sensitive material that needs to be segregated. Secure communication media should be used to communicate this information. Even if a crucial piece of information is given to a person who is acting strangely, unforeseen events that could result in dangerous situations could still happen. Therefore, this information is shielded from corruption or breach by a malevolent hacker using the data concealing approach. The majority of data concealment techniques use steganography, cryptography, and digital watermarking.

The message should first be encrypted using a secure cryptographic procedure before being encoded using the steganography algorithm. In that case, not even steganographic algorithms can simply decode the message. The message will be converted into ciphertext, rendering it unintelligible to attackers. The algorithms used in cryptography methods are numerous. In essence, key management infrastructure is used. To improve the encryption algorithm, symmetric and asymmetric cryptographic key management approaches are used. To confirm that the sender and receiver are the authorised users, the symmetric key is originally provided with both parties. Steganography doesn't really make message authentication better. To protect messages for visual detection from sender and receiver, numerous encryption techniques are used.

The mechanism through which steganography and cryptography will interact to create secure media is being developed in this secure communication medium. Additionally, steganalysis will be used to find stego-objects in developed material using a variety of analysis tools and evaluation results from various hashing techniques. Python programming will be used to carry out the implementation. This study will outline an improvement strategy for using secure media to transmit private information.

2. Related work

2.1. Steganography

Frequency domain and spatial domain are the two main domains that can be utilised to identify data embedding in image processing that uses pixels, according to an analysis of steganography techniques. The measurement of image quality and quantity distinguishes the two domains most proposed in [1]. Quantity is determined by using image sensitivity. Based on the results of the peak signal to noise ratio (PSNR) or the structural similarity index metric, the quality measure is examined (SSIM). Based on the results of bits per pixel, the quantity measurement is examined. In addition to these two, imperceptibility and robustness are important considerations. Robustness is the ability to clearly degraded modified image from partial attacks to lose data integrity. The human eye can detect significant changes that point to the existence of embedded data. The study of this perceptible is referred to as imperceptibility. Using bit numbers, the spatial domain integrated the simple text into the cover image.

In LSB methods, bit numbers of the message are substituted for the image's least significant bits. There will be 3 bytes for red, green, blue, and alpha when decomposing the pixel (RGBA). There are 8 bits in each byte, and one byte is used to represent each colour. The least significant bit (LSB) for each byte is the one on the right, while the most significant bit (MSB) is the one on the left (MSB). An image with an RGB value of 800x600 pixels can hold up to 180,000 bytes for embedding explained in [1].

2.1.1. Image Steganography

The use of a picture as a cover to conceal a message is known as image steganography. The image can be used with a variety of image formats, including Portable Network Graphics (PNG), Bitmap (BMP), and Joint Photographic Experts Group (JPEG) (PNG). The JPEG image format compression is a popular format for lowering the size of the image described in [2]. Using an image as compression enables you to maintain aesthetic characteristics that are still evident. Since the human naked eye cannot breakdown the veiled information contained within the cover image, this information is difficult for humans to see.

2.1.2. Audio Steganography

A steganographic method called Audio Steganography involves encoding data using an audio-based file structure. Waveform Audio (WAV), Audio (AU), and MPEG Audio Layer III are all acceptable audio file formats (MP3). It is extremely difficult to embed the message in audio, however many different methods have been tried. An enhanced least significant bit modification technique for audio steganography shows large amounts of data can be compressed using audio, and it is difficult to hack in [3]. However, maintaining an audio signal becomes more challenging as more data are encoded. It primarily serves to safeguard digital copyright.

2.2. Cryptography

Encryption and decryption are the two main operations involved in cryptography. private information is transformed into bizarre, cryptic text with a variety of odd marks in order to prevent unauthorised access. It's called encryption. The output of encryption is referred to as ciphertext, which is difficult to decipher visually. Decryption is the process of converting this ciphertext back to plaintext (the original text). It is not possible to restore the ciphertext to plaintext using some cryptographic methods. The cryptography technique is carried out in these two operations using the key exchange infrastructure. The plaintext is converted to a cypher using a pseudorandom key or user-defined key, which is then utilised again during the decryption process. These three techniques are hash functions, symmetric cryptography (public-key cryptography), and asymmetric cryptography (secret-key cryptography). These three techniques are frequently used to send messages more securely in [4].

2.2.1. Asymmetric cryptography

Asymmetric cryptography, also known as public-key cryptography, uses two different kinds of keys: public and private. Public key infrastructure, digital signature, channel security, and tamper detection are the main applications for public key. A digital signature is used to confirm the message's validity and provide proof that it originated with the sender. Additionally, it has the capacity to confirm the non-repudiation and data integrity. The signature enables the sender to notify the recipient if the encrypted communication is changed or expanded upon described in [5]. Plaintext, ciphertext, an encryption method, a decryption algorithm, a private key, and a public key are the different parts of a public key infrastructure.

2.2.2. Symmetric cryptography

Symmetric cryptography, also referred to as secret-key cryptography, encrypts and decrypts data transformations using a single common key that is passed into a mathematical formula. Secret-key cryptography is used specifically to improve the privacy and confidentiality of data.

AES is a symmetric encryption method since it employs the same key for both both encryption and decryption. Additionally, it employs numerous rounds of the SPN (substitution permutation network) method to encrypt data. The impenetrability of AES is a result of these encryption rounds, which are impossible to break through due to their sheer number in [6]. The United States National Institute of Standards and Technology (NIST) developed the Advanced Encryption Standard (AES) as a specification for the encryption of electronic data in 2001. Despite being more difficult to build, AES is still commonly used because it is substantially stronger than DES and triple DES. Three key lengths—128 bits, 192 bits, and 256 bits—are used in the AES encryption and decryption process. For, a fixed block length of 128 bits is used. For 128-bits, 192-bits, and 256-bits, AES uses 10, 12, and 14 rounds, respectively.

2.2.3. *Hash Function*

One of the cryptographic methods that enables the complete transformation of the plaintext to the given varied fixed number is the hash functions. Digesting is the term for this transformation process. The hash functions do not need keys. Fundamentally, hash functions are used in digital signatures, password security enhancement, random number creation, and message authentication. The one way is another name for it explained in [4]. For instance, the message "Hello" is encrypted using the MD5 cryptographic hash function technique. "Hello" will result in a digest message of 128 bits rather than 16 bytes. The result will be 128 bits when another plaintext "World" message is similarly encrypted in that manner (16bytes).

Table 1: MD5 Hash Table

Plaintext	Hash value (MD5)	Output size
Hello	8b1a9953c4611296a827abf8c47804d7	128 bits (16bytes)
World	f5a7924e621e84c9280a9a27e1bcb7f6	128 bits (16bytes)
Hello World	b10a8db164e0754105b7a99be72e3fe5	128 bits (16bytes)

There are hundreds of different hashing algorithms available, and each one is tailored for a certain sort of data, speed, security, etc. Secure Hashing Algorithm, or SHA. There are two variants of the algorithm: SHA-1 and SHA-2. They differ in the bit-length of the signature as well as in creation (how the resultant hash is made from the original data). The National Institute of Standard of Technology released SHA (NIST). The hash value produced by FIPS 180-4 SHA can be MD. It generates a higher hash value than MD, is faster, and is more secure than MD. The output of SHA is a hash value of 160 bits (20 bytes) with 20 rounds.

As a hashing algorithm response to developing BCrypt assaults, SCrypt was developed. SCrypt is used in many software programmes to implement the protection against password cracking. For the purpose of generating the peak time for password processing, SCrypt uses a specific amount of their hardware resources in their farm. However, employing a specific amount of memory allows you to restrict an attacker's capacity to find passwords using high-tech gear. SCrypt is used to strengthen the encryption algorithm based on the findings.

2.3. *StegAnalysis*

The method known as steganalysis aims to counter steganography by locating the concealed data and extracting or erasing it. For law enforcement organisations, it becomes essential to decipher the communication or at the very least render it useless to the recipient, as is the case with nearly all such approaches. Through steganalysis, the primary attribute of a stego-object is analysed based on its robustness, capability, and imperceptibility. The steganalysis is carried out in the steganography studio to look at the detection of images that show the presence or absence of steganographic information using various algorithms and various image format types in [7]. In order to identify the cover image, stegananalysis is performed using server tools like Openpuff and Steganography Studio. Visual analysis (examining with human visual abilities to perceive the existence of information) and statistical analysis (examining of modification in statistical properties to the images). To improve security assessments, steganalysis can be researched on cutting-edge technologies like artificial intelligence, neural networks, fuzzy logic, and genetic logic by extracting data more thoroughly through statistical qualities as a progressive digital forensic.

3. Proposed System

In steganography, there are three main cover file formats that are utilised. They are steganography for audio, steganography for video, and steganography for images. Data steganography in audio and video is a very dedicated approach because even little changes can cause significant noise affects. This had a negative impact on the original quality and greatly affected the capacity of the human visual system (HAS) and human auditory systems (HVS). HAS is more sensitive than HVS when compared to each other. In order to see the variations in noise in an image file, you must look at it in great detail for a few seconds. The development of communication medium is more adaptable and trustworthy when using image and audio steganography. The effectiveness of audio steganographic techniques is influenced by a number of factors. Each feature's significance and effect vary depending on the application and the transmission environment. The durability to noise, compression, and signal manipulation, as well as security and the ability to hide concealed data, are among the most crucial characteristics shown in [8]. The robustness criteria is the most difficult to meet in a steganographic system when paired with data hiding-capacity because it is closely related to the application.

The most practical approach based on the spatial domain is called least significant bit (LSB). The image is broken up into a large number of pixels as part of the spatial domain process. A pixel has 24 bits in total. Red, blue, and green are represented by each 8-bit colour. The least significant bit of these three values is used in the LSB algorithm's processing. The first step of the method is to read the image and transform it into image pixels. The message is then transformed into a bit as well. The LSB of the picture is used to replace the message bits to create the stego-image. The image is not lost when the LSB is changed, and great perceptual transparency is supported. As a result, these changes are not easily visible to humans. In order to hide data, several image steganography programs alter bits using the least significant bit (LSB) technique. In low resolution pictures with 8-bit colour, changing the LSB could cause a noticeable shift in the colour palette, making it simple to spot hidden material. Another sign that there is hidden information present in an image is padding or cropping. The Hide-and-Seek tool can only be used to create fixed-size graphics.

4. Methodology

By using data hiding techniques on the communication carrier, the process can be divided into two primary parts: encryption and decryption. There will be two actors while employing a communication carrier: a sender and a receiver. Before sending the carrier, the sender must complete the encryption process. The system needs three user inputs for the encryption method: a cover image, a message, and a secret key. Stego-object as well as a shared secret key are needed for decryption. the symmetric communication mechanism that uses encryption. The sender must enter the secret and message into the system in order for symmetric communication to flow.

Utilizing the LSB approach, steganography and cryptography are combined in this system. The entered file is chosen as an audio file in this system. After that, the communication is encrypted using just one secret key. The Image Steganography and cryptography are also combined as different mechanism for encryption and decryption. Both systems are suggested and employ the LSB algorithm to conceal the message in communication media. Utilizing various essential communication networks has its benefits. Depending on the user's decision during encryption, the stego-object can be either an image or an audio file.

The AES algorithm first converts the secret key into a hash digest value. The salt will be generated prior to hashing the AES in order to combine the secret key. This procedure is only used in one-way operation. The hash value cannot be converted back to its original form and cannot be used to determine the secret key's value.

The hash value and encrypted message are base64 encoded into unintelligible ciphertext. The cover object is additionally mixed with the ciphertext using the LSB steganography algorithm. The ciphertext of the encrypted communication is converted to binary format. First, an RGBA format conversion is performed on the cover image. These binary-formatted data are also converted to hexadecimal form. By using a delimiter, the modified binary value of the message is inserted into the hexadecimal format value of the cover image. The system will return the cover image as the stego-image to deliver the message over communication media to the recipient once all of the transform values have been fully included into the cover image.

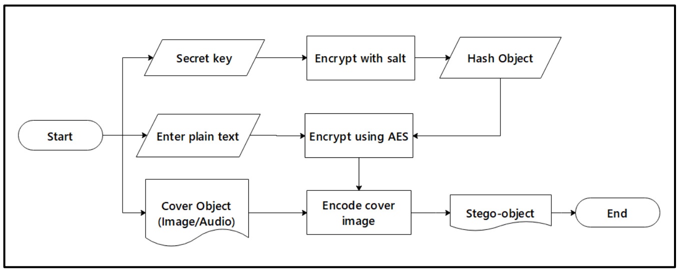


Figure 1: Encryption Algorithm

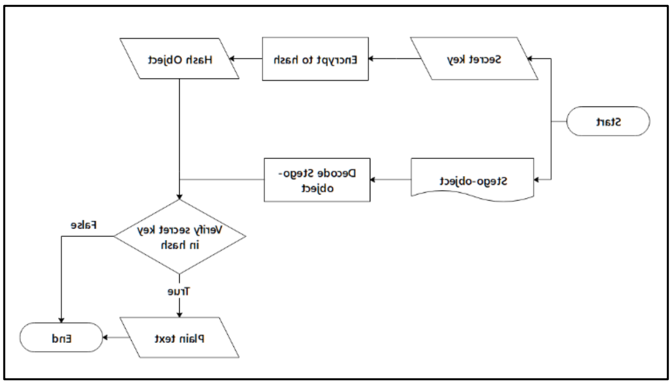
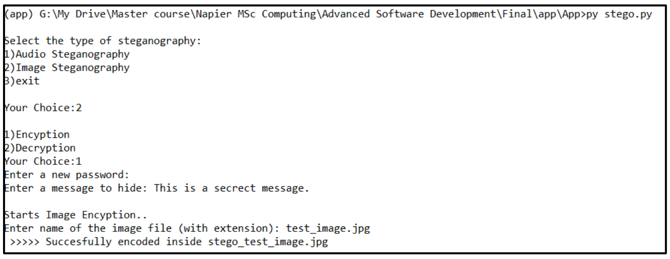


Figure 2: Decryption Algorithm

On the other side, High data embedding capacities are possible with the LSB method, which is also reasonably simple to use alone or in combination with other hiding methods. This method's limited resistance to noise addition, which makes it susceptible to even straightforward attacks, lowers its security performance. The data will probably be lost if the stego-audio is filtered, amplified, has noise added to it, or is compressed using lossy techniques. Without impacting the perceived transparency of the stego audio signal, it has extended the depth of the embedding layer from the fourth to the sixth and eighth LSB layers to improve the robustness of the LSB approach against distortion and noise addition. The other bits can be switched to create a new sample that is more similar to the original in order to reduce embedding error.

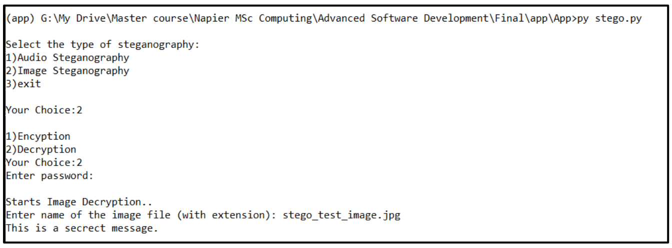
The communication carrier (stego-object) is extracted on the recipient side using a shared key. The stego-object is initially broken down into an acceptable format by identifying a delimiter to recreate the binary data. By converting to binary, these hexadecimal values are retrieved back into plaintext. The system begins ciphertext decryption once the ciphertext has been successfully obtained. There is a password verification function that must be passed through in order to acquire the original message prior to the decryption of the ciphertext. The system extracts the salt from the ciphertext before encrypting the newly entered password from the receiver and converting it to a hash value. The system then compares the newly created hash value to the other hash value that was derived from the stego-object. The generated hash must be verified in order to ensure that the password is valid. The system unpads the result and sends the message to the recipient after the ciphertext has been decrypted.

The suggested steganography system's encryption and decryption procedures are shown in the diagram below. The encryption procedure for both audio and image steganography requires the cover file, password, and secret message in order to produce a new stego-image. The application simply needs a password and stego-object to decrypt data.



```
(app) G:\My Drive\Master course\Napier MSc Computing\Advanced Software Development\Final\app\App>py stego.py

Select the type of steganography:
1)Audio Steganography
2)Image Steganography
3)exit

Your Choice:2

1)Encyption
2)Decryption
Your Choice:1
Enter a new password:
Enter a message to hide: This is a secrect message.

Starts Image Encyption..
Enter name of the image file (with extension): test_image.jpg
 >>>>> Succesfully encoded inside stego_test_image.jpg
```

Figure 3: Encryption Process



```
(app) G:\My Drive\Master course\Napier MSc Computing\Advanced Software Development\Final\app\App>py stego.py

Select the type of steganography:
1)Audio Steganography
2)Image Steganography
3)exit

Your Choice:2

1)Encyption
2)Decryption
Your Choice:2
Enter password:

Starts Image Decryption..
Enter name of the image file (with extension): stego_test_image.jpg
This is a secrect message.
```

Figure 4: Decryption Process

5. Experimental Results

The two techniques from the data hiding techniques will be used to produce the secure stego-object. The evaluation of each method will be done separately from this implementation of data concealing strategies. For the steganography, the evaluation will be performed on the changes of stego-object and original cover object.

The system's performance is controlled by the local host machine: Storage: 1TB HDD with read/write speeds of 100 MB/s, CPU Processor: Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz, 2901 Mhz, 2 Core(s), and Operating System: Windows 10 Pro 64 bit As a result, utilising this local machine, the results of both encryption and detection with cryptography are acquired.

As a result of the changes in their pixel construction and attributes, the difference between the original cover image and stego-object is compared. These outcomes were acquired using the output characteristics of https://www.textcompare.org/image/. Size in bytes, dimension, bit depth, horizontal resolution, and vertical resolution are all aspects of an image's attributes. Bit depth is the term used to describe the colour information stored in an image. The image can store more colour values due to the huge number of bit depth values. The measurement of pixel density, known as horizontal and vertical resolution, is typically expressed in dots per inch (dpi). A 1-inch square has a grid of pixels that is 72 pixels wide by 72 pixels high when a picture has a resolution of 72 dpi. Changes in size, bit depth, and horizontal and vertical resolution can be seen in these findings. Comparing the stego-picture to the cover image, the size has risen. Then the bit depth increased by roughly 8 and both stego-object resolutions were displayed at 96 dpi.

The bytes that will be embedded in the cover picture will be located initially from the above and stored until the final hiding with the pink areas, based on the results of the difference in images. The only way to see these allocations is by employing a tool for comparing and contrasting.

The steganalysis is performed to investigate the presence of the encrypted message. In this steganalysis, the stego-object are used to detect with several steganography. The detection process is performed with decoding the stego-image into text information.

Table 2: Steg-analysis Tools Table

No.	Steg-analysis Tools	Detection Results
1.	Stegdetect	Failed
2.	Mcafee Steganography Defense Initiative	Failed
3.	Steghide	Failed
4.	Steganography Online	Failed
5.	VSL	Failed

The difference between the cover image and the stego image is being compared in this experiment's results. The test is carried out using Guiffy Image Diff (11.11). The highlighted portion of the stego-object showed a small discrepancy between the stego-image and the original image. The secret data is totally encrypted after starting at the beginning of the image and being put in that highlighted bit.

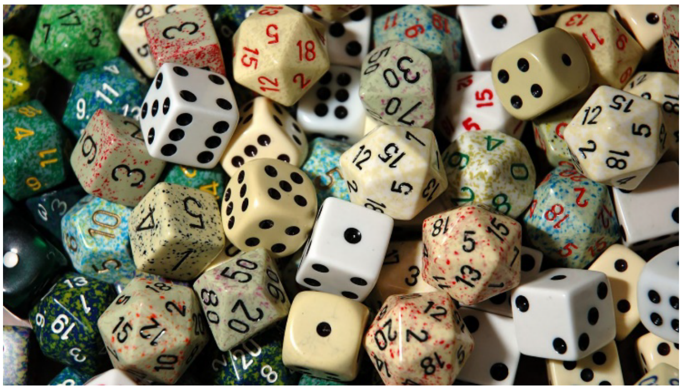


Figure 5: Original Image

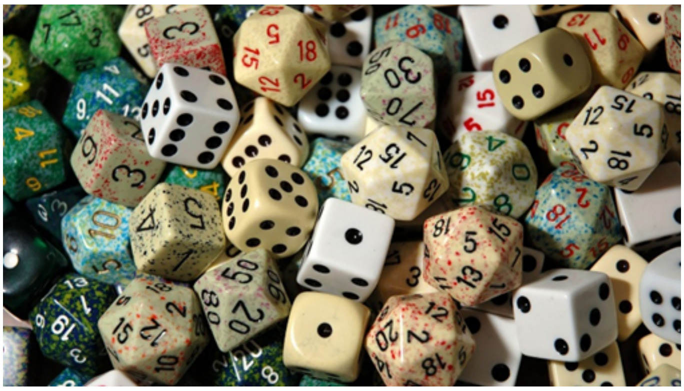


Figure 6: Stego-Image

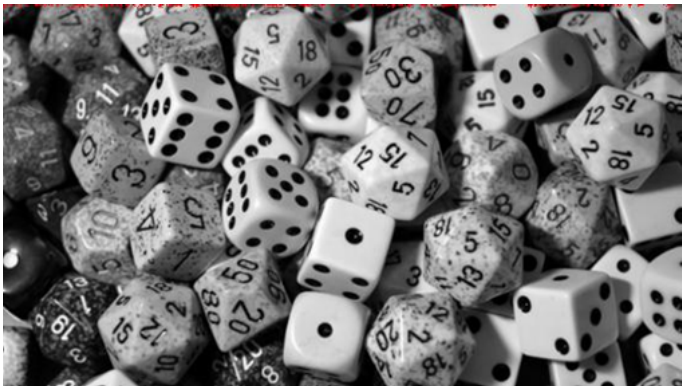


Figure 7: Image Difference between Original Image and Stego-image

Audio steganography is used on fixed LSBs to determine the point at which the difference between the host message and stego message may be heard. Every sample of the host message's fixed bits is replaced with bits from the secret message without employing the randomness suggested in Bit Selection and Sample Selection. In this following, it is simpler to conceal the existence of noise or secret data. A frequency study of the same data, however, makes it clear that there is foreign data in the media. The main goal of the suggested approach was to keep noise levels low by minimising the disparity between original audio and stego audio. There is no discernible difference between the stego signal and the original signal, even after stegano-manipulation.

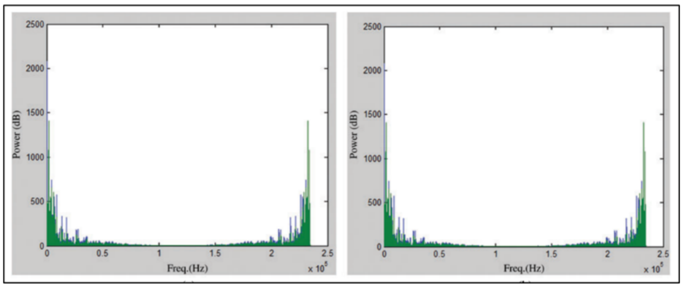


Figure 8: Comparison between Original Audio and Stego-audio

6. Conclusion

The system that was put into place had benefits for protecting communication medium thanks to data-hiding algorithms. With base 64 encoding and the SHA-256 hashing technique, the message and secret key can be compressed thanks to the robust security of AES encryption. Utilizing the most recent hashing algorithm development raises the security level of password authentication. Controlling the resilience and lowering the level of suspicion in a visual attack on a carrier using LSB. The techniques based on audio steganography primarily work with audio and spoken signals for a protective communication. While evaluating these techniques, the key steganographic characteristics of capacity, security, and resilience are taken into account. The difference image in the performance section shows the modifications and differences between the original and the stego-image. Because of the LSB approach and base64 encoding, the final output size does not vary even when a significant quantity of data is inserted into the cover image.

Acknowledgment

I would like to thank my Supervisors at Edinburgh Napier University, for her kind support throughout this research process.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] P. Rajkumar, R. Kar, A. K. Bhattacharjee, H. Dharmasa, "*A Comparative Analysis of Steganographic Data Hiding within Digital Images*," International Journal of Computer Applications, vol. 53, no. 1, pp. 1–6, 2012, doi:10.5120/8382-1981.

[2] V. Lokeswara Reddy, Dr.A. Subramanyam, Dr.P. Chenna Reddy, "*Stegnography Rajarao Kaviliga Related papers Implementation of LSB Steganography and its Evaluation for Various File Formats*," J. Advanced Networking and Applications, vol. 868, , pp. 868–872, 2011.

[3] M. Asad, J. Gilani, A. Khalid, "*An enhanced least significant bit modification technique for audio steganography*," Proceedings - International Conference on Computer Networks and Information Technology, pp. 143–147, 2011, doi:10.1109/ICCNIT.2011.6020921.

[4] G. Kessler, "*An Overview of Cryptography (Updated Version 24 January 2019)*," Publications, 2019.

[5] D.S.Abdul. Elminaam, H.M.A. Kader, M.M. Hadhoud, "*Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices*," Undefined, pp. 343–351, 2009, doi:10.7763/IJCTE.2009.V1.54.

[6] Rūta Rimkienė, *What is AES Encryption and How Does It Work? |* Cybernews, https://cybernews.com/resources/what-is-aes-encryption/, 2022.

[7] Y. JinaChanu, Kh. Manglem Singh, T. Tuithung, "*Image Steganography and Steganalysis: A Survey*," International Journal of Computer Applications, vol. 52, no. 2, pp. 1–11, 2012, doi:10.5120/8171-1484.

[8] F. Djebbar, B. Ayad, K.A. Meraim, H. Hamam, "*Comparative study of digital audio steganography techniques*," Eurasip Journal on Audio, Speech, and Music Processing, vol. 2012, no. 1, pp. 1–16, 2012, doi:10.1186/1687-4722-2012-25/FIGURES/12.

Copyright: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (https://creativecommons.org/licenses/by-sa/4.0/).

Bo received his BSc in Hons Computing from Edinburgh Napier University and is currently pursuing his MSc in Computing from the same university. Additionally, he is attending Contemporary Technology University for an MSc in Computer Science (Data Science and Applied Artificial Intelligence). His research interests include Data Analytics and Wrangling, Scripting for Cybersecurity and Networks, Software Security and cryptography.

Received: 01 December 2022, Revised: 01 February 2023, Accepted: 07 February 2023, Online: 22 February 2023
DOI: https://dx.doi.org/10.55708/js0202003

Blockchain Tokens for Agri-Food Supply Chain

Ricardo Borges Dos Santos[*,1], **Rodrigo Palucci Pantoni** [2], **Nunzio Marco Torrisi**[1]

[1]UFABC, Center of Mathematics, Computing and Cognition, Federal University of ABC, Campus São Bernardo do Campo, São Paulo 09606-070, Brazil

[2] Department of Eletrical Engineering and Computer Science, Federal Institute of São Paulo, Campus Sertãozinho, São Paulo 14169-263, Brazil

[*]Corresponding author: Nunzio Torrisi, nunzio.torrisi@ufabc.edu.br

ABSTRACT: The aim of this research is to suggest and analyze a framework to give universal publicity to food properties certificates from any certification authorities. The focus is the certification of agro product instances, i.e. unique for every single harvest, using smart contracts and blockchain non fungible tokens minted by third-party authorities. The development and testing of a set of smart contracts used the newly established ERC-1155 Ethereum token standard to implement Non-Fungible Tokens (NFT)s. The ERC-1155 tokens allow for representing both the uniqueness, thus non-fungibility, between different harvests as well as the quantitative elements within a specific harvest, e.g. mass fractions of product from the same harvest, which can be interchanged, thus fungible. The framework was developed, deployed, and tested on the Ethereum test net blockchain and submitted to extensive testing. The blockchain data is accessible through general-purpose block scanners and can be read through an Android App used by regular consumers during a supermarket visit. The goal is to give consumers easy access to the Third-party Certificates (TPC) URLs available at the public Ethereum blockchain. The benefit for food safety of widespread TPC visibility through web applications can not be underestimated, since the use of blockchain tokens controlled by smart contracts injects trust in the traceability of the merchandise, reducing counterfeiting and green-washing. The broadcasting of the TPCs with the corresponding discipline of tokens transfer and smart contact restriction to possible abuses increases agro-food supply chain transparency. Trust and transparency foster sustainable buying habits by many consumers and transparency in the complete production and distribution links.

KEYWORDS Third Party Certification, Smart Contracts, Non-Fungible Tokens, Food Certification, Blockchain

1. Introduction

In 1990, the Organic Foods Production Act (OFPA) established standards for agricultural producers of commodities that claimed to use organic methods. The methods, practices and substances used in agricultural practice, including sowing; growing; and harvesting; as well as handling crops and processed agricultural products, restrict the wording on the product labels and marketing. Since OFPA, the US consumer has been continuously increasing demand for certified organic foods brands that claim to use organic production processes. Nevertheless, these organic farm certification methodologies have shown limitations and criticism: the authors of [1] conclude that the "current regulatory framework is not only inadequate to the task of regulating domestic organics, but also incapable of ensuring the integrity of imported organics. Thus, the USDA Organic seal misleads consumers.".

1.1. Justification

Several studies have recently claimed that the certification of products holds great beneficial potential, such that [2]: "Product certification is one of the most promising and developed instruments to reward the socially and environmentally friendly practices of market producers".

Third-party certification (TPC) differs from first and second-party certification mainly because the third-party authority that issues the certificate has no interest in the transaction. A TPC involves an "independent Organisation with expertise to provide an assessment and verification of the company's compliance with standards or legal requirements" [3].

TPC can be very useful to ascertain product physical, chemical, or organoleptic properties and is allowing bolder certification of social, environmental, and sustainability properties. According to the work in [4]: "TPC also offers opportunities to create alternative practices that are more socially and environmentally sustainable".

Although the farming procedures may be certified according to criteria such as quality, sustainability, or social fairness, there is no form of ensuring that certification of the typical farming methods, such as USDA Organic certification methodology, avoids specific harvests being stained by malpractices such as agrochemical exposure or used hidden child labor.

Each harvest of a specific crop is unique. The difference may lie in the seeds used for that particular season or in the total hours of sunshine in that specific location during the crop's growth.

One good example is the wine industry, where consumers know that the time and the different weather conditions between harvests of different years even from the same farm will influence the wine quality. Organoleptic tests of wine produced from grapes of different years and locations evidence these differences. The wine counterfeit problem can be summarized as avoiding that larger quantities of more valuable wine from grapes harvested on better years or regions reach retail than the volume actually produced. This fraud is academically known as the mass balance [5] or the double spending problem [6] and has a negative impact on the luxury goods business as it can hurt the reputation of premium brands. This fraud also hurts products that are geographically traceable to a specific region, i.e., reserved by local laws under the protected designation of origin (PDO) concept.

1.2. *Related Work*

The work in [7] provides a comprehensive overview on the application of blockchain technology to agri-food value chains. These are in line with the work in [8] which concludes that the use of blockchain technology can improve sustainability from social, environmental, and market perspectives. Recent literature [9] presents a blockchain-enabled supply chain architecture to ensure the availability of a tamper-proof audit trail for foods free of COVID-19 contamination Further [10] conducts an extensive literature review on the integration of blockchain into traceability systems. Discussion on a blockchain strategy to trace organic food products is presented in [11]–[12] . Attempts to use less costly distributed data structures such as the interplanetary File System (IPFS) for food traceability are discussed in [13]. These and other articles are convergent in stating that blockchain tools are possibly the most appropriate technologies to meet the various requirements the rapidly expanding food value chains such as traceability, auditability, fault tolerance, and flexibility [14]–[15]. Research on certification using blockchain [16]–citecreydt2019blockchain has also evolved with many interesting sustainability findings and efforts.

Nevertheless, no research has been found where harvests are recognized as being unique, thus their yield not interchangeable between different harvests. This approach, where the produce or yield of the different harvests are not interchangeable except within the same harvest, leads this research to use Non-Fungible Tokens (NFT) of the type ERC-1155.

1.3. *Proposed Solution*

It is proposed to use Ethereum-based tokens and smart contracts pointing to TPC certificates for keeping track of certificates for individual harvests of each farm. In this manner, we show that it is possible to track the exact origin and quantity of each harvest from farm to consumer, offering the benefits of TPC available to the last links of the chain. Practical economic incentives to the chain participants are described allowing for effective productive usage. The focus is on information availability, reliability, synchronization to the physical flow of goods, and, above all, ensuring good publicity of the certificate at the consumer level.

This research paper is structured as follows. Section 2 presents relevant concepts and literature of traceability, blockchain, smart contracts, and distributed ledger technology (DLT) and the Ethereum-based non-fungible token (NFT). Section 3 discusses the requirements and implementation of a token passing TPC framework using the ERC-1155 token smart contracts and analyses the results obtained. Section 5 presents the conclusions pinpointing the research's main contributions and limitations.

2. Blockchain Key concepts applied to Certification

A chain of transactions, organized into cryptographically linked blocks, could, for the first time, reach a consensus, even within a (limited) number of unreliable (traitor) nodes. For a more detailed description of the data structures involved see in [17, 18]. Albeit the eventually synchronized nature of the protocol and possible temporary partitions in the network, the linear block of data is re-established after a partition and regains consistency and availability.

Consistency of distributed data within a predetermined time frame is achieved, avoiding the double spending [6] of the digital asset.

The technology behind blockchain successfully implements consistency and access discipline for collaborative data in a diffuse globally distributed accessible trustless environment. The consistency achieved by the underlying data structures and control mechanisms with validation through the consensus of third party validators or miners shows that this technology is an important step towards supply chain transparency and traceability data [19]–[20].

A blockchain is a cryptographically auditable, append-only, tamper-resistant, distributed and replicated data structure, accessible to anyone employing a web browser.

Blockchain can store proof of structured data as well as methods or programs to process this data according to deterministic program steps known as smart contracts. Blockchains require no central trust mechanism, thus there exists no central point of failure. The main strengths of Blockchain Technology (BCT) are listed below.

- Tamper resistance, i.e., cryptographic hashes to previous block, in practice, make it impossible to change data that has been recorded;
- Pseudo-anonymity, i.e., data are available publicly but encoded through hashed keys that allow for trust on the existence and on the authorship;
- Distributed presence, i.e., the data structures are replicated maintaining several copies with no single point of failure and keeping integrity between data sets;
- Software-driven, i.e., the Blockchain mechanism does not require human privileged operators to maintain the transactions, thus the system is not prone to bribery;

- Allows for certification of the tamper-proof storage of off-chain data by means of side blockchain. These are hierarchically hash-certified sub-database that can store larger volumes of data, including multimedia, and provide evidence and tools for more detailed analysis.

Ethereum [21] expanded the concept of the blockchain to distributed ledger technology by including tokens and programs called smart contracts that are executed independently of human intervention. These are open-source, human-readable high-level programs that are stored on the blockchain and run inevitably, without any human intervention, strictly as implemented thus avoiding any risk of downtime, censorship, or fraud [22]. The Ethereum Virtual Machine implements "unstoppable" and "unavoidable" Turing-complete computer processes. Smart contracts use open-source code and are developed to establish standard behavior between blockchain stakeholders and other contracts. They allow for extensive development and precise control, ensuring transparency of each data manipulation and thus trust. Digital blockchain tokens are capable of representing object properties, assets, or rights that have strict transactional behavior and ownership. The execution of smart contracts is immune to any human interference and therefore allows for transparent systematic transactions. Tokens can be used to represent supply chains, intellectual properties, voting, or identity management systems, among other objects. The associated smart contracts assure discipline to the corresponding state transitions of token balances and thus generate trust to the parties without a trusted third party thus no single point of failure. This assures transparency and prevents possible "double-spending" frauds in the certification system.

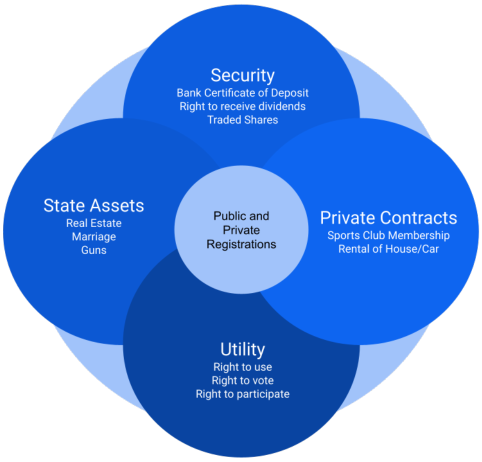


Figure 1: Families of assets and rights according to registration requirements.

2.1. *Digital Tokens*

Tokens are digital objects that represent specific rights or assets. They should be understood as assets that can be negotiated or used as guarantees. Note that the necessary and sufficient condition for full ownership of the balance of the token on a public address is the knowledge of its private key. Figure 1 shows a diagram for most common assets and rights, grouped into families along with their corresponding registration requirements.

The registration of the rights and property of assets, if required by law or regulation, will usually be centralized at a government-trusted centralized database. Because these data are maintained in centralized databases they are prone to corruption, fraud, censorship, downtime, or misuse. On the other hand, distributed registration schemes based on replicated databases, such as distributed ledgers, provide very high availability, are fraud-resistant, are fault-tolerant, and typically cannot be censored. Security and utility assets can reliably be represented, registered, and easily traded as cryptographic tokens. Automated processes through smart contracts allow high availability, low costs of the transaction, full traceability, non-repudiation, and pseudo-anonymity.

In order to be useful, tokens should not be copyable (i.e., should not be prone to double spending attacks) or suffer arbitrary changes. Thus, they need to follow strict discipline at each change of state to usefully represent real-world objects.

The development of digital objects to simulate real-world objects requires that the object's properties and behaviour are modeled through common data structures and coded procedures. Smart contracts manipulating tokens must respect some standard to allow for multiple users and contracts to share functionalities among different applications. Application independence and fungibility of digital objects could be achieved with a minimum set of functionalities. The ERC-20 token fungible objects standards are key to the success of many cryptocurrencies and many Ethereum decentralized applications. Because the ERC-20 token metadata structure holds all relevant property data within the blockchain, they can be freely transferred from one blockchain to another, allowing these to be exchanged for other ERC-20 assets.

It is important to note that like a real estate property record, which entitles the bearer to have full use and ownership of a real estate asset, the possession of a private key of a token on one blockchain entitles that person or smart contract to unrestricted use of that token for payment, exchange, deposit as warrant or collateral, lending or selling this assets at his discretion.

Further, it is important to recognize that objects can be categorized in fungible objects and non-fungible objects. Fungible objects are those that need not be distinguished from one another. The important question here is "How many of these objects?". Non-fungible objects, on the other hand, are those that are distinguishable from similar objects. The decisive question here is "Which of these similar, although unique, objects?"

The distinctive property between fungible and non-fungible tokens is that the former are fully exchangeable and thus can be added, e.g., coins of the same face type and value can be added or subtracted at will. The latter, not being exchangeable, can only be transacted as unique identifiable objects.

A non-fungible token (NFT) is a unique blockchain-based digital entity which can represent a non-fungible object. If this token follows a protocol such as the ERC-1155 or ERC-721, it can be traded as an asset between various stakeholders in possibly multiple applications.

The methods defined in the ERC-1155 standard assure consistent behavior, transparency, no double spending, and a verifiable auditable trail to families of similar, yet unique, objects. An ERC-1155 compliant NFT has one identifier that points to a specific URL, in which typically all properties and details are described. Additionally, an overview of these main differences is outlined in Table 1 and a numerical characteristic of the ERC-1155 object is also available (https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1155.md accessed on 26 November 2022).

Table 1: Comparison between ERC-721 and ERC-1155 tokens

	ERC-721	ERC-1155
Fungible	N	Y(within same family)
Non Fungible	Y	Y
Smart Contract	One instance	Multiple instances

2.2. Harvest TPC Algorithm

For decades, important crops have been traded as commodities. Commodities are intrinsically fungible. Once the product is classified in a certain grade, according to purity, size, or maximum cross-contamination levels, then, the lot is handled as a commodity. Global trading standards and procedures require that a certain measure of a commodity, say, a bushel of a certain grade of wheat, is fully fungible with the same measure of this same commodity, i.e. another bushel of the same wheat grade. However, a specific harvest should be regarded as a unique object. No other harvest possesses the exact same physical, chemical or organoleptic properties, therefore harvests should be handled as non-fungible physical objects. To track this object appropriately, it is necessary to record all relevant data which will individualize and keep the history of that specific harvest product.

Each harvest of a specific crop is unique. The difference may lie in the seeds used during that particular season or in the total number of hours of sunshine in that specific location during the crop's growth.

In several agricultural sectors, especially in the wine trade, expert consumers recognize the crop timing and the different characteristics between harvests of different years even from the same farm. The analysis of the organoleptic properties of the wine produced recognizes differences in the year and location of the harvest of grapes. In the wine sector, the wine counterfeit problem can be summarized as avoiding that larger quantities of more valuable wine from grapes harvested on better years or regions reach retail than the volume actually produced. This fraud is also known as the mass balance problem [5] or double spending [6] and is very deleterious to the business as it can stain the reputation of premium producers. Products that are geographically traceable to a specific region, i.e., reserved by local laws under the protected designation of origin (PDO) concept are also frequently affected by this type of fraud. A harvest TPC mechanism with tamper-resistant certificates which are easily available to any stakeholder via internet devices is very helpful to avoid double spending and can significantly boost trust along the supply chain stakeholders.

Thus, we researched the following main research questions (MQ1) and subsidiary research questions (SQ2, SQ3):

MQ1: "Is it possible to establish a harvest TPC mechanism with tamper resistant certificates easily available to anyone, even previously unknown food supply chain stakeholder via public blockchain access?"

SQ2: "If a TPC mechanism is possible, who will carry the data input and maintenance costs? In other words, how will each stakeholder be incentivized to use this mechanism?"

SQ3: "If a TPC mechanism is possible, what will a typical time of response for a certification query be, in other words what quality of service can be expected by the end consumer?"

To answer the Research Questions MQ1 and the subsequent research questions SQ2 and SQ3 a systematic method was used which involves designing all smart contracts needed, deploying and subjecting them to testing. The test evaluated compliance to functional and non functional design requirements. The procedure is depicted in the Algorithm 1 which shows a step-by-step description of the methodology for harvest TPC validation using a set of 7 smart contracts as a Proof-Of-Concept (PoC).

Algorithm 1: Methodology Systematic

```
Result: Write here the result
User Requirements;
while Register Request do
    SmartContract(ProofOfConcept);
    if TPC Authority exist then
        Token Transfer;
        Consumer Tracking Access;
    else
        Evaluate(ProofOfConcept);
    end
end
```

In summary, the algorithm develops a systematic methodology by means of the following steps:

- 1—Elicit and define user requirements (both Functional and Non-Functional).
- 2—Harvest Traceability - Define and Identify Traceable Units - Discipline data collection, i.e., when and what needs to be collected.
- 3—Design and implement proof-of-concept (PoC)—Deploy smart contracts.
- 4a—Analyze if third-party certification authority is capable of issuing tokens easily and transferring them along the Supply Chain Participants.
- 4b—Analyze if a token transfer allows the URL information to be made accessible to the token buyer along the Supply Chain Participants.
- 5—Analyze if consumers can access URL for TPC with internet applications easily, reliably, and fast (MQ1).

- 6—Evaluate PROOF OF CONCEPT and respective results and improve implementation.

Besides the blockchain immutability permit to trace of all the test runs and deployments of the smart contracts. This allows the research methodology and procedures to be easily reproducible and traceable (Examples of blockchain scanners are https://www.etherchain.org/, https: //www.EthPlorer.io or https://www.Etherscan.io accessed on 29 August 2022). In other words, both the smart contract source code as well as all the test runs of all tests performed to the PoC can be followed in detail on any browser.

2.3. Requirement Analysis

The desired functionalities of the system, i.e., the functional requirements are listed below.

- to allow for farmers to request any third person authority to inspect and certify properties that a specific harvest may have;
- to allow the inspection authority to issue a certificate on any website including quantitative data about the desired property of the yield;
- to allow the authority to create (“mint”) tokens, i.e., digital objects representing the harvest and carrying the URL linked to the certificate, representing information about the mass of product inspected (yield);
- to allow these tokens to be “passed on” along the chain of buyers of the product (yield);
- to allow the buyer that applies the package, wrapper, or label to the food product to write the URL to an easily and freely accessible reliable database and
- to destroy (“burn”) , after a predetermined time, these tokens once the food product is consumed, to avoid garbage accumulation or misuse.

As for the nonfunctional requirements, it is important to ascertain that the system satisfies the following:

(a) Universal access: allowing any supply chain participant, even previously unknown, to use the tool without previous registration;

(b) Tamper free auditabilty: enforcing tamper-free, auditable transactions between any parties;

(c) Robustness to faults: allowing the writing to a common persistent information layer in a robust manner;

(d) No double spending fraud: avoiding that token balances are used more than once;

(e) Universal read access: allowing any potential consumer to freely read the certificate by means of an internet device

(f) Interoperability: allowing usage with different systems and devices and

(g) Cost effectiveness: allowing information to be recorded in an inexpensive manner;

(h) Usability: allowing for comfortable user experience.

(i) Quality of Service: guaranteeing that response to a consumer query returns to the requesting device within a short time period;

(j) Scalability: allowing for a much larger number of transactions running within the acceptable quality of service i.e performance.

2.4. Persistence Layer Design: Do we need a Blockchain?

If harvests are to be certified for the benefit of the entire chain of potential stakeholders in the food industry, which type of data structure would be required to keep this information useful and trustworthy? Is it necessary to use a blockchain to record and make all relevant information consistently available to all stakeholders?

Figure 2, derived from [23] summarizes a structured approach to optimize the data structure architecture to be used for a specific application. In this case, the particular requirements for the TPC of Harvest in the Food Supply Chain recommend the use of a public permissionless blockchain as the best architecture. The sequence of questions we would ask is:

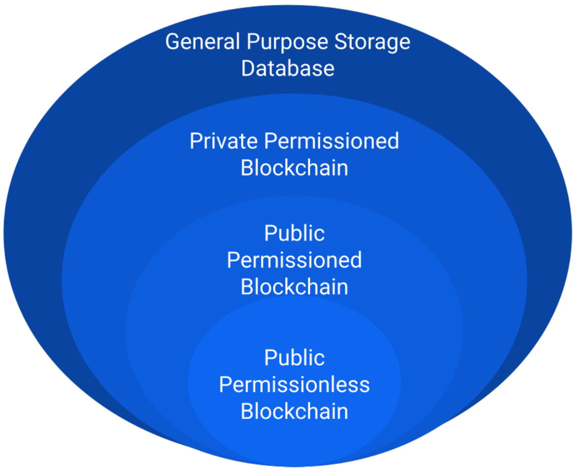

General Purpose Storage Database
Private Permissioned Blockchain
Public Permissioned Blockchain
Public Permissionless Blockchain

Figure 2: Scale of Requirements to define the type of data persistence layer (database or blockchain)

- Is it necessary to store current State (Current Custodian on Supply Chain)? YES;
- Is a Trusted Third Party available online? NO;
- Is WRITE access needed outside your organization? YES; (because of the possibly many unknown chain participants).
- Are all Writers known? NO.

Thus, the recommended architecture is Public Permissionless Blockchain. Because it is desired that the system maintains allows for new participants to join the supply chain such as new farmers, known farmers with new crops, new mills, new re-sellers, new comminglers or new retailers, the choice of a permissioned blockchain such as Corda or Hyperledger was discarded[24, 23].

Because Ethereum tokens meet the non-functional requirements (a–i) listed above, the public Ethereum environment with the non-fungible token ERC-1155 standard protocol was chosen. Ethereum also meets all of the non-functional requirements today including (j): scalability.

3. Smart Contract Implementation

The smart contract code used for ingredient certification in [25] was modified to implement the non-fungible token (NFT) discipline that better represents each instance of a crop with the use of the ERC-1155 (https://github.com/enjin/erc-1155 accessed on 29 August 2022) objects and methods.

The fully documented source code for all the smart contracts in the Solidity programming language was published in the Ethereum main net where all variables and algorithms are fully commented on and documented. The code was developed, tested, deployed, and made available at https://rinkeby.etherscan.io/address/0x841c5c79d9ae35db8fb4f216a478cd184fdae634#code (accessed on 4 august 2021). The source code shown in the link is the full smart contract code and is divided as follows: The ERC-1155 standard code and the standard libraries used are shown up to line 772. The specific smart contract code responsible for the application is shown as of line 772 and comprises the following methods:

- *farmerRequestCertificate*- This routine allows for the sale of ingredients along with the respective IGR token transfer

- *certAuthIssuesCerticate*- This routine is used to allow for certification authorities to confirm that ingredients are trustworthy as well as quantity, URL where published, product, details of IGR value property, location, date of harvest).

- *sellsIngrWithoutDepletion* - This routine allows for the simple sale of ingredients along with the respective IGR token transfer (with URL).

- *sellsIntermediateGoodWithDepletion* - This routine allows for the sale of intermediate products made from certified ingredients along with the respective IGR token transfer (with URL) i.e.: allows only the pro-rata quantity of semi-processed InGRedient tokens to be transferred.

- *genAddressFromGTIN13date* - This is an auxiliary function to generate an ethereum address for the specific food item visible numbers GTIN-13 + date of validity in format YYMMDD. This is used by the method comminglerSellsProductSKUWithProRataIngred to allow anyone such as e.g. by a consumer with an App or block-scanner to query the exact blockchain address where the certificate URL is stored(Figure 4).

- *transferAndWriteUrl* - This is also an auxiliary routine to transfer the balance from the token owner's account to the 'to' account. Note that the owner's account must have sufficient balance to transfer, that zero value transfers are allowed.

- *comminglerSellsProductSKUWithProRataIngred* - This code allows for the sale of the final-consumer product with resp SKU and Lot identification with corresponding IGR transfer with URL. In other words, it warrants that only the pro-rata quantity of semi-processed InGRedient tokens be transferred to the consumer-level package(SKU)

The smart contract code described can be viewed also as a class UML diagram. Generation of UML class diagrams from published Solidity programming language source code on the Ethereum blockchain can be obtained by an automated functionality of the Etherscan blockchain scanner, as shown in (https://rinkeby.etherscan.io/viewsvg?t=1&a=0x841c5c79d9ae35db8fb4f216a478cd184fdae634.

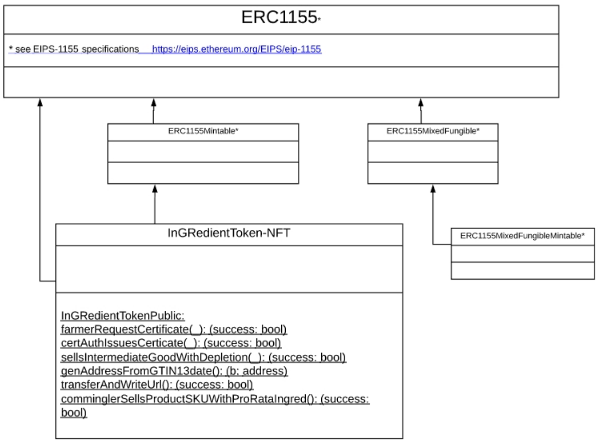

ERC1155*
* see EIPS-1155 specifications https://eips.ethereum.org/EIPS/eip-1155
ERC1155Mintable*
ERC1155MixedFungible*
InGRedientToken-NFT
ERC1155MixedFungibleMintable*
InGRedientTokenPublic:
farmerRequestCertificate( ): (success: bool)
certAuthIssuesCerticate( ): (success: bool)
sellsIntermediateGoodWithDepletion( ): (success: bool)
genAddressFromGTIN13date(): (b: address)
transferAndWriteUrl(): (success: bool)
comminglerSellsProductSKUWithProRataIngred(): (success: bool)

Figure 3: IGR Token class as a dependent class of the ERC 1155 class. (simplified by author from auto-generated UML class diagram from Etherscan).

4. Results and Discussion

A set of public blockchain smart contracts govern the token synchronization framework to positively identify each harvest along the food supply chain to the end consumer.

At each transactional change to the product such as change of custody, mixing, usage, or depletion of the product, tokens are exchanged.

Using a modification of the IGR token set of smart contracts rewritten for ERC1155, in Figure 3, the farmer responsible for the harvest can freely choose the properties to be certified between:

- functional - e.g. minimum size of fruit or grade.

- organoleptic - e.g. color or aroma.

- social - e.g. free of child labor cultures.

- environmental - e.g. "grown in certified no forest devastation areas"or "organic—no xyz herbicide", or non Genetic Modified seeds only.

as well as the appropriate authority that will audit and issue the corresponding certificate for each harvest.

The authority is then invited to audit the farm at harvest time. After the appropriate auditing procedures, including inspection of the farm and qualitative and quantitative evaluation of crop yield, the authority formalizes the audit results by publishing the certificate as a web page at the authority's domain web server.

The link to this certificate, in the form of the URL is part of the minting process. Further, this smart contract will issue the exact number of tokens to match the numerical mass yield of that specific harvest in grams.

Thus the ERC-1155 unified resource identifiers (URL) descriptor will point to the web page containing the full technical details of the certified "consumer-valued properties", including the original mass of goods in grams. The number of IGR tokens issued will represent this specific mass of ingredients.

By using the delegated transfer "setApprovalForAll()" and "safeBatchTransferFrom()" primitive in the smart contracts, it is not possible for the farmer to issue or make first-person claims on the certificate. Only the Authority has this capability, thus enforcing strict true third-person certification (TPC).

Comparing the current approach to the previously published certification using the ERC-20 IGR Ethereum token, the main improvement was to avoid tokens obtained from different harvests, thus with different characteristics, being mixed. The ERC-1155 discipline allows for the farmer to sell part of the harvested product whilst avoiding possible attempts to mix tokens from distinct harvests.

Further, as in blockchain distributed ledgers, "double spending" frauds are not possible.

The necessary information in order to evidence to a final consumer that a specific harvest or food ingredient raw material was effectively inspected and certified by a third party to hold some "consumer value property" is handed over from one chain participant to the next, all the way to the recipe final processor.

The farmer, can freely define any property that may be useful or cherished by his consumers and the certifying authority by using the smart contract *farmerRequestCertificate()*. After an inspection of the farm, the certification authority will confirm the quality, quantity, and date of the lot harvested. He will then include all relevant information in the certificate web page at the authorityś web domain. *certAuthIssuesCert()* The smart contract mints for this specific lot of crop an equivalent quantity of IGR tokens such that one IGR token corresponds to one gram of that certified ingredient. The authority issues IGR tokens through the smart contract including nature, quantity, location, and time of the harvest. The token will hold the URL to the web page of the full TPC. Note that only the certification authority has permission to mint or not mint the tokens or determine the correct quantities. This assures a truly independent third-party certification and avoids potential conflicts of interest.

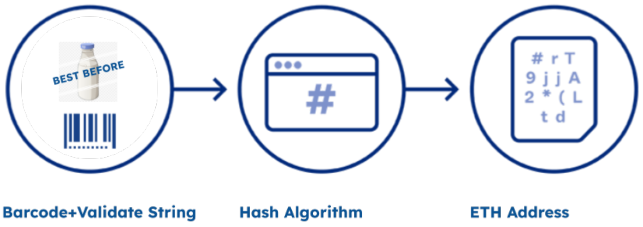


Figure 4: ETH Address generation from *genAddressFromGTIN13date*

The final processor, sometimes also known as commingler or packer, uses information printed on the product retail label to generate a public key which is linked to the certificate URL. The barcode (GTIN-13 SKU identifier) appended to the validity "best before" date on the wrapper are hashed to provide a unique public key in the Ethereum blockchain. Thus, the hash of the "GTIN-13 + Date" string is the public key on the Ethereum blockchain. Querying the blockchain at this address returns the URL link to the certificate.

This new ERC-1155 smart contract code retains the original functionalities while extending the framework to allow for non-fungible objects such as harvests of food products to be certified as unique objects. It has a major new focus on the conception, validation, and usability of smart contracts for TPC of non-fungible objects.

4.1. Answers to Research Questions

The research questions **MQ1** and subsidiary research question **SQ2** and **MQ3** can be answered as follows:

MQ1: Yes, the IGR token smart contracts after being modified to ERC-1155 are capable of truly evidencing harvest TPC with tamper-free certificates and are available to anyone, including new entrants to the food supply chain through simple internet devices, as shown by the PoC running on a test net as described.

SQ2: Yes, price incentive mechanisms are established for each stakeholder. The premium to the price that the final consumer is willing to pay for access to the TPC certification of products will be shared with the supply chain participants. The sum of the incentives along the links of the supply chain is approximately as large as the premium the consumer actually pays.

SQ3: The typical time for the response for an end consumer to a certificate query using the HTTP protocol is linear because it uses only one direct hashed access to the blockchain (linear data structure) plus one direct URL web access to the certificate, both of which are accessible in linear time. This is due to the fact that, at each change of custody, the URL to the certificate is "handed over" to the next in the chain all the way to the commingler or packer. The public key information (GTIN-13 + lot date) to the certificate URL saved on the blockchain can be scanned directly from the product label. This can be achieved conveniently using an Android App `https://play.google.com/store/apps/details?id=com.igrtoken&hl=en&gl=US&pli=1`

In summary, the modified IGR-token smart contracts suite using the ERC-1155 tokens allows for the synchronization of the transfer of custody of the crop with the corresponding IGR token representing each gram of the yield instantiated for each different harvest. The modifications to the IGR-token code to use the ERC-1155 have kept all original functionalities adding the necessary non-fungible discipline. The main enforcement is that yields from different harvests now may not be added.

The framework can not detect if a physical counterfeit of packaging, within a short period, i.e., re-utilization of original packaging material with counterfeit content, whilst the spent tokens are still "live".

5. Conclusions and Future Work

Farmers are systematically urged towards more sustainable farming methodologies whilst becoming more competitive. Some producers use the information on labels to induce customers to believe that their ingredients are harvested in environmentally and socially friendly manners without proper evidence. Third-party certification along with better availability of this information to the general public and supply chain actors can help fight this green-washing and promote consumer trust. Reliable publicity of the certificates with fast and easy access is paramount. A possible practical solution is the use of distributed ledger technology using tokens carrying the URL pointing to the certificate at the authority's website. This information is transferred at each change of custody from harvest along the chain.

This research shows that a TPC, via the certificate URL at the authority's website, can easily and publicly be made available through internet Apps. To allow for credibility among the target consumers, the certification authority can be freely chosen by the farmer. The authority is free to decide and has full control on whether or not to certify or deny certification. The architecture has a practical appeal because it allows economic incentives to be shared by stakeholders along the agro-supply chain links.

The major contribution of this research is to show a method for public access to URLs with TPC of harvests as unique objects, as opposed to a more generic certification of a farm.

Conflict of Interest The authors declare no conflict of interest.

References

[1] C. Liu, "Is usda organic a seal of deceit: The pitfalls of usda certified organics produced in the united states, china and beyond", *Stan. J. Int'l L.*, vol. 47, p. 333, 2011.

[2] F. DeClerk, J. F. Le Coq, B. Rapidel, J. Beer, *Ecosystem services from agriculture and agroforestry: measurement and payment*, Routledge, 2012.

[3] B. Tanner, "Independent assessment by third-party certification bodies", *Food control*, vol. 11, no. 5, pp. 415–417, 2000.

[4] M. Hatanaka, L. Busch, "Third-party certification in the global agrifood system: an objective or socially mediated governance mechanism?", *Sociologia ruralis*, vol. 48, no. 1, pp. 73–91, 2008.

[5] T. Hirbli, "Palm oil traceability: Blockchain meets supply chain", Ph.D. thesis, Massachusetts Institute of Technology, 2018.

[6] U. W. Chohan, "The double spending problem and cryptocurrencies", *Available at SSRN 3090174*, 2021.

[7] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions", *Computers in industry*, vol. 109, pp. 83–99, 2019.

[8] J. Kasten, "Blockchain on the farm: A systematic literature review", *Journal of Strategic Innovation and Sustainability*, vol. 15, no. 2, pp. 129–153, 2020.

[9] A. Iftekhar, X. Cui, "Blockchain-based traceability system that ensures food safety measures to protect consumer safety and covid-19 free supply chains", *Foods*, vol. 10, no. 6, p. 1289, 2021.

[10] K. Demestichas, N. Peppes, T. Alexakis, E. Adamopoulou, "Blockchain in agriculture traceability systems: A review", *Applied Sciences*, vol. 10, no. 12, p. 4113, 2020.

[11] X. Lin, S.-C. Chang, T.-H. Chou, S.-C. Chen, A. Ruangkanjanases, "Consumers' intention to adopt blockchain food traceability technology towards organic food products", *International Journal of Environmental Research and Public Health*, vol. 18, no. 3, p. 912, 2021.

[12] G. d. S. R. Rocha, L. de Oliveira, E. Talamini, "Blockchain applications in agribusiness: a systematic review", *Future Internet*, vol. 13, no. 4, p. 95, 2021.

[13] D. Prashar, N. Jha, S. Jha, Y. Lee, G. P. Joshi, "Blockchain-based traceability and visibility for agricultural products: A decentralized way of ensuring food safety in india", *Sustainability*, vol. 12, no. 8, p. 3497, 2020.

[14] A. Upadhyay, S. Mukhuty, V. Kumar, Y. Kazancoglu, "Blockchain technology and the circular economy: Implications for sustainability and social responsibility", *Journal of Cleaner Production*, vol. 293, p. 126130, 2021.

[15] J. F. Galvez, J. C. Mejuto, J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis", *TrAC Trends in Analytical Chemistry*, vol. 107, pp. 222–232, 2018.

[16] F. Zhao, X. Guo, W. K. Chan, "Individual green certificates on blockchain: A simulation approach", *Sustainability*, vol. 12, no. 9, p. 3942, 2020.

[17] J. Zhang, S. Zhong, T. Wang, H.-C. Chao, J. Wang, "Blockchain-based systems and applications: a survey", *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.

[18] M. Choi, S. R. Kiran, S.-C. Oh, O.-Y. Kwon, "Blockchain-based badge award with existence proof", *Applied Sciences*, vol. 9, no. 12, p. 2473, 2019.

[19] A. Rejeb, J. G. Keogh, S. Zailani, H. Treiblmaier, K. Rejeb, "Blockchain technology in the food industry: A review of potentials, challenges and future research directions", *Logistics*, vol. 4, no. 4, p. 27, 2020.

[20] R. Cole, M. Stevenson, J. Aitken, "Blockchain technology: implications for operations and supply chain management", *Supply Chain Management: An International Journal*, 2019.

[21] E. Wood, "A secure decentralised generalised transaction ledger, ethereum proj", *Yellow Pap*, , no. 151, p. 1.

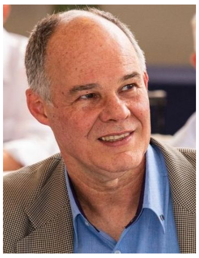
[22] W. Ethereum, "Ethereum whitepaper", *Ethereum. URL: https://ethereum. org [accessed 2023-01-01]*, 2014.

[23] L. Wu, "Blockchain smart contracts in megacity logistics", 2018.

[24] K. Wüst, A. Gervais, "Do you need a blockchain?", "2018 Crypto Valley Conference on Blockchain Technology (CVCBT)", pp. 45–54, IEEE, 2018.

[25] R. B. dos Santos, N. M. Torrisi, E. R. K. Yamada, R. P. Pantoni, "Igr token-raw material and ingredient certification of recipe based foods using smart contracts", "Informatics", vol. 6, p. 11, MDPI, 2019.

Copyright: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (https://creativecommons.org/licenses/by-sa/4.0/).



Ricardo Borges dos Santos has completed his Bachelor in Mechanical Engineering degree from PUC-RJ University in 1984 with honors. He has obtained a Computer Engineer Degree from UNIVESP, Sao Paulo in 2020 as well as a MS degree in Mechanical Engineering at Penn State University in 1989. He has earned his PhD degree in Computer Science from the Center of Mathematics, Computation e Cognition of the Universidade Federal do ABC in 2019.

His research activities are mainly related to Distributed Systems, Cryptography, Blockchain and Energy. He has over 20 articles on Food Traceability, Distributed Systems, Energy Efficiency and Supply Chain Management.

Rodrigo Palucci Pantoni He received the Computer Science degree in 2000 and subsequently received the M.S. in 2006 and PhD in 2012 at the University of São Paulo (USP).

He now teaches “Industrial Informatics” at the Department of Electrical Engineering and Computer Science of Federal Institute of São Paulo. His research activities are mainly in the area of Industrial Informatics with focus on development activities including Internet of Things and Industry 4.0.

Nunzio Marco Torrisi He received the Master degree and the PhD in Computer Engineering from the University of Catania, Italy, in 2002 and 2006, respectively.

He registered a Brazilian patent, published his work in international journals and magazine and since 2009, he has been an associate professor at the Federal University of ABC in São Paulo (UFABC).