JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 15, Issue 1
March 2022
ISSN: 1946-1836

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three to four issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is under 38%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP who perform the editorial and review processes for JISAR.

2022 ISCAP Board of Directors

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

2022 JISAR Editorial Board

Security Control Techniques: Cybersecurity & Medical Wearable Devices

Jeff Deal
Jeff@n6networks.com
N6Networks

Samuel Sambasivam
Samuel.Sambasivam@Woodbury.edu
Computer Science Data Analytics
Woodbury University
Burbank, CA 91504

Abstract

The Internet of things (IoT) has been a significant advancement in technology, advancing the modernization of repetitive tasks, streamlining data collection, and providing new ways to collect, interpret, and disseminate information. Numerous industries have benefited from advancements in IoT technology, including the healthcare industry. For example, medical IoT (MIoT) has deployed several devices, including internet-connected sleep apnea, blood pressure regulators, glucose monitoring, and mobile echocardiogram and heart rate monitors. The advancement in MoT devices has revolutionized medicine and the treatment of care. Both treatment facilities and patients perform a significant amount of care solutions from their homes, saving the patient time and money. However, the integration of technology to maintain potential life-sustaining functions within the patients comes with the challenge of ensuring that data integrity and patient safety are not compromised. This study leveraged a qualitative case study to understand the security controls and techniques cybersecurity professionals need to protect medical wearable devices. Participants were selected from a wide range of medical treatment facilities, including information system technicians, information system security officers, and chief information officers. The top three cybersecurity concerns identified by survey respondents are 1) IT professionals require a better understanding of how devices function – including criticality of health care task, authentication protocol, data transmission details, etc. 2) users/wearers lack a fundamental understanding of cybersecurity risks and available security functions/features 3) the cooperative role required by the device manufacturer, the medical treatment professional, IT professional, and users to properly secure MIoTs is not understood. Recommendations for cybersecurity professionals identify MIoT devices' standards based on identifying and prioritizing device function as a substantial factor for security risk assessments and ensuring devices deployed multi-factor authentication while maintaining a robust patching and security framework.

Keywords: Medical Wearable Devices, MIoT, IoT, Cybersecurity.

1. INTRODUCTION

Today's average citizen is more connected than ever (Pew Research Center, 2019). Technology is integrated into all aspects of our lives (Dutta, 2018). Data can now be requested from a simple voice query from smart home assistants such as Alexa, Contra, and Siri. The Internet of Things (IoT) area is evolving into multiple solutions from the corporate deployment to meet enterprise shortfalls to the integration into homes such as a doorbell, garage door openers, refrigerators, and camera systems. Martin (2019) reported that 69% of homes in the United States have at least one smart device. Gartner (2014) identified that a significant majority of mobile device vendors had deployed wearable devices, which is a substantial increase

from only two companies using wearable technology. The emerging threat towards healthcare and medical treatment facilities is on the rise. As IT systems become integrated into medical treatment solutions, the risk of data exposure, device compromise, and physical harm is significantly increased. The successful execution of malicious code is causing both a danger towards the integrated medical treatment facilities and the patient life-sustaining systems such as respirators, blood pressure, heart rate monitors, and insulin distributors.
Piwek et al. (2016) identified that one in six consumers utilizes a wearable device, including smartwatches, to collect health information.
Leveraging medical wearables or implantable devices, medical providers and treatment facilities can provide robust medical treatment options for patients worldwide (Li et al., 2017).

By interconnecting medical treatment facilities, information can be shared directly between the patient and provider, significantly reducing cost while maintaining high levels of care (McCaldin et al., 2016). In addition, specific devices such as insulin pumps, pacemakers, and defibrillators remotely monitored through an internet connection can provide patients with overall better quality of life (Mantas et al., 2016). The study aims to provide insight into how cybersecurity specialists implement different security controls to protect medical wearable devices. As the Internet provides numerous capabilities to organizations, healthcare is no stranger to advancing technology solutions. As a result, the term (IoT) has evolved and has created a sub-culture of devices identified as Medical IoT (MIoT). Devices that fall into the category of Medical IoT provide patients with remote monitoring of numerous services to include blood pressure, heart rate, echocardiogram (EKG), insulin deployment, and monitoring of oxygen levels. Medical IoT's benefits allow medical treatment facilities to deliver patient care remotely, reducing costs for patients. In addition, medical IoT devices can receive pre-programmed instruction sets to help patients in an emergency until they can be reached by a local healthcare professional.

2. RESEARCH PROBLEM

The problem addressed in this study was the security controls techniques cybersecurity specialists need to protect medical wearable devices have not been identified (McCaldin et al., 2016). The IoT industry has a $6.2 Trillion-dollar growth market, with a significant majority of devices identified as healthcare devices valued at 2.5 trillion (Brown, 2013). With numerous organizations entering the wearable technology area, one of the critical gap areas is device security and user privacy.

Lang (2018) identified that a considerable majority of healthcare treatment facilities could not manage the emerging threats related to enterprise IT solutions. Ransomware has become the weapon of choice when targeting healthcare organizations. Ragan (2016) noted that The Hollywood Presbyterian Medical Center (HPMC) targeted a ransomware attack that causes the organization to pay out $3.4 million in bitcoin to decrypt systems. With a significant number of healthcare organizations initially slowly integrating the cloud into the IT solution for healthcare operations, cloud service providers have seen a substantial increase in cloud utilization for healthcare services, including software deployment as a service (SaaS). Zhang and Ravishankar (2019) identified that organizations that leverage IaaS could increase productivity while reducing the on-premise footprint. While it was determined that the movement to cloud infrastructure was inevitable, there were several concerns regarding security (Zhou et al., 2010). Several challenges were discussed in the cloud on-demand model: security, performance, availability, and integration were rated the highest by survey participants. A significant number of MIoT devices leverage critical services such as patient monitoring of heart rate, oxygen levels, and echocardiogram data that have a necessary dependency on software that integrates with the patient and hardware devices. Proper monitoring of the patient's vitals can become compromised from the improper configuration of software, leading to the backdoor intrusion of devices (Miclăuș et al., 2019). Ransomware is a popular choice of cyber criminals against medical treatment facilities. Argaw et al. (2019) discussed that The Department of Justice identified over 4,000 ransomware attacks across medical treatment facilities across the United States. Identifying and discussing emerging threats towards medical treatment facilities and MIoT devices can help identify solutions that can bridge the gap in organization security posture and the overall cyber hygiene of medical treatment facilities. The "gap" can only be solved by increasing awareness as new challenges are presented daily. Increasing visibility in threats and implementing user best practices play a critical role in integrating the defense-in-depth approach, including addressing hardware,

software, procedures, and protocols to ensure patient safety.

3. POPULATION AND SAMPLE

This study's population included cybersecurity experts with roles and responsibilities for creating, implementing, enforcing, or improving the understanding of cybersecurity policies and related industry standards. In addition, the population included members from cybersecurity specialists from the International Information System Security Certification Consortium (ISC2), which provides for more than 150,000 certified members recognized globally for its advancement in the development of cyber and infrastructure security (ISC2, n.d.). The research study sample comprises 10 participants, identified as an appropriate sample by Creswell (1998). The target population is determined using several factors, including the scope of the research and the limitation of the researcher; however, Thomson (2010) discusses that the average sample size for qualitative research was 25 participants. Creswell (1998) identified a range of 20-30 participants. Morse and Field (1996) identified a range of 30-50 participants. The overall goal of leveraging recommended sample sizes is to ensure the researcher reaches saturation within the selected population.

Raw data were collected using the 13 interview questions:

1.What are the most significant cybersecurity threats to your medical treatment facility?
2.What is the most significant underlying issue with medical IoT devices?
3.What physical security measures do you implement to protect the current IT infrastructure?
4.What administrative security measures do you implement to protect the current IT infrastructure?
5.Who has the responsibility of securing medical wearable devices? Should the security role fall on the device manufacturer, the user, the medical treatment, the government, or a combination of all entities?
6.Do you think that Medical IoT devices should be identified in different priorities based on the function they serve?
7.With laws such as the General Data Protection Regulation in Europe, do you think there is a need for a legal framework to protect Medical IoT devices and the data generated?
8.In your opinion, does your organization place budget as a priority over security?
9.Do you subscribe to any security-related magazines, attend any trade shows, conferences, or are a part of any cybersecurity groups that discuss emerging threats?
10.If so, does it help you stay up to date on emerging threats and provide new methods of protection?
11. What direction should organizations take to protect medical wearable devices?
12. What are three items that should be a part of every cybersecurity specialist's playbook to protect medical wearable devices?
13. What can medical wearable device users protect themselves from potential data compromise or physical harm from a cybersecurity incident?

4. ANALYSIS OF DATA

In a study conducted by Williams and Woodward (2015), the researchers identified the increased connectivity and complexity medical wearable devices bring creates a complicated challenge. With the expansion and integration of technology and healthcare, the need to protect the information system from malicious attacks and the safety of both patients and data and physical harm. Moreover, the researchers discussed several areas of concern, including data storage and data transfer, which several participants also identified as a gap of security focus for medical device manufacturers.

Major Theme 1: Function

The theme regarding functions was a significant item of the discussion by all participants. Each participant identified that devices should be determined by the function they serve. The discussion primarily focused on identifying that cybersecurity specialists must identify how the devices function, including if the device supports life-sustaining functions such as heart rate, insulin control, blood pressure, and oxygen levels. Additionally, a function must also include how data is transmitted, received, and encrypted to and from the device, how the user authenticates with the device, and any additional operational safety functions or features. The implementation of system hardening is a common practice within the cybersecurity realm. Hardening systems allow security practitioners to remove non-essential services such as open ports, protocols, services, and programs, reducing the entry point for attack. Devices that manage life-sustaining functions should implement multi-factor authentication, logging, and auditing. Multi-factor authentication (MFA) required the use of two or more verification factors to perform actions on a resource (Ometov et al., 2018). Multi-factor authentication leverages several items including,

something you know (i.e., security questions, passwords, and one time passcodes (OTP)), something you have (i.e., Tokens, OTP's sent over cellular or email messaging), and something you are (i.e., fingerprints, facial recognition, voice, retina) (Choi et al., 2017). Other MFA examples include Behavioral analysis such as gait when walking, location-based authentication leveraging IP address location. Risk-based authentication is another MFA method that leverages authentication attempts with behavioral analytics (Wiefling et al., 2019).

Authentication access is based on when a user tried to gain access, the device type, location services, and historical attempts to authenticate. Logging of the device's authentication attempts and transmission of data ensures that all information sent to and from the device is authorized and requires the user to present multiple authentication methods before executing commands on a device. Logging can provide a wide variety of metrics, including performance, behavioral and environmental data vital in supporting device function. Integrated with ML/AI devices can provide data sets allowing cybersecurity specialists to recognize anomalous activity and provide audit trails for all actions on the device (Muggler et al., 2017).

Major Theme 2: Users

The theme regarding users was discussed by 90% of the participants, with a significant majority of discussion surrounding the user's knowledge base and responsibility while using medical wearable devices. The participants describe users in both the medical treatment facility who are intermediate or 3rd party users of the device maintain the CIA triad of confidentially, integrity, and availability. Participants discussed that users often lacked training on operating the device, unaware of the security functions or features, and are unaware of the risk that the user's mismanagement of devices brings the enterprise IT infrastructure. Users are a significant part of an organization's cybersecurity posture. Cain et al. (2018) discussed that end users are often identified as the weakest point as 95% of attacks are aimed at users. Kweon et al. (2019) further recognized a direct relation between leveraging cybersecurity training and reducing cybersecurity incidents.

Major Theme 3: All Entities

The theme regarding all entities was discussed by 9 out of 10 participants representing the need for a robust cybersecurity approach to protecting medical wearable devices. Participants stressed the need for multiple entities to be involved in the cybersecurity process. All entities include the inception of the device developer. The doctors/nurses present with the device are recommended as a treatment solution, cybersecurity specialists who managed MIoT devices on the network, and the end-users who leveraged the device as treatment solutions. The device manufacture should ensure not only ensure the physical security of the devices. It should also perform code validation of the software and firmware that the device will use to control or monitor the patient's bio-health systems. Doctors, nurses, and medical staff need to understand how the device supports the patient's health but must be aware of the potential side effects of cybersecurity vulnerabilities and the risks of threats related to MIoT.

Cybersecurity specialists that work within medical treatment facilities must also understand risk by correctly identifying which devices are on the network, the device classification/function, and the different threats each type of device presents to the infrastructure. Users must also understand the risk involved with device usage, data encryption, transport security, and the safety function to ensure the device operates at peak efficiency without compromising the device, user, or treatment facility. Potential hackers can compromise devices that do not implement robust security controls. Unencrypted medical data is a data-rich target for potential hackers. Security professionals have seen a spike in cyberattacks towards hospitals as security and encryption are often misconfigured or not implemented. The Catawba Valley Medical Center was a recent victim of a cyberattack exposing over 20,000 patient records compromised through a phishing attempt that compromised three employee's accounts. Hackers were able to access protected health information that, if encrypted, could potentially reduce the likelihood of exposed personal health data.

Major Theme 4: Legal Framework

All participants identified that some established frameworks help protect data in the medical Field, including HIPPA and PII laws, but the gap was in protecting MIoT devices. Users are more invested in understanding what data is being collected from the end devices and how the information is being used. The European Union has taken legal action to hold the organization accountable for the data collection process, transmission, collection, and usage of end-users data. Participants stressed that the United

States was behind in establishing a national legal framework regarding the use of user data. California has taken an individual step forward in implementing a legal framework in the establishment of SB 327, which required device manufacturers to ensure devices are equipped with reasonable security features, including the protection of the data collected, contained, or transmitted. While one state strives to protect data, device users may become unprotected if the user data is generated outside of California, as SB-327 only identifies protections for California residency (Eagan, 2020).

5. CONCLUSION

The study on the security control techniques cybersecurity experts needs to protect the medical wearable device identified the functional areas to address when integrating MIoT devices within a medical treatment facility. The literature review identified the massive integration of IoT devices across all platforms. The MIoT device adoption provides new methods for delivering medical care in remote and unique medical treatment scenarios. Cost savings, reduced visits, and prioritization of care treatment are all benefits of MIoT adoption. The integration of technology supporting life-sustaining functions presented several challenges to cyber professionals, including physical safety and the potential loss of life from a compromised device and information security for data transmitted to and from the device (Bonderud, 2019). Each case enforces the need to support a robust cybersecurity solution to enforce the protection of medical wearable devices and ensure both the safety from physical harm and privacy of patient data. As the adoption of wearable devices use increases cybersecurity professionals can leverage the four themes identified as security foundations for the establishment of a security program and framework when implementing MIoT devices within the organization. The identification of security shortfalls identified in this study can act as the launch point in the discussion of controls needed in the establishment of cyber hygiene and cyber posture. Stakeholders play a significant role in the deployment of organization security as funding and executive buy-in are often controlled by shareholders/stakeholders. Cyber professionals and senior leadership can leverage the information and security shortfalls understanding the risk associated with the importance of user awareness, and the role each entity plays with the implementation and maintenance of integrated MIoT devices.

6. FUTURE RESEARCH

The study was intended to determine the security control techniques cybersecurity specialists need to protect medical wearable devices that expand upon what is known within the current literature and identify opportunities from experienced participants. The participants for this study were IT professionals supporting the medical IT infrastructure. The insights and knowledge of IT professionals who participated in this research study provided clear details on the different strategies needed to protect medical wearable devices. The research study provided valuable information and data, which identified recommendations for further research.

Recommendation 1 is the need for data protection concerning big data generated through wearable devices. Medical wearable devices can generate vast amounts of data to find underlying solutions providing more robust healthcare solutions through data collection and processing. Data generated by medical wearable devices can become a gold mine for insurance companies. Olson (2014) discusses that a significant amount of insurance data is driven by behavior. Numerous insurers in multiple arenas use data points to shape rates based on behavior-driven data. Medical wearable devices could give insurance companies near-real-time data with reasonable latency tolerances to support their users' habitual actions. This research effort would benefit from identifying the best tactics for supporting privacy concerns related to wearable devices and further investigating the relationship between healthcare and insurance providers who collect and use the data to help the device users (Leedy & Ormrod, 2010).

Recommendation 2 is additional research is needed concerning medical wearable device type security. Medical wearable devices vary in different types based on different functions. Devices that are passive such as heart rate monitors and oxygen level monitors, may need more or fewer security functions than devices that support life-sustaining MIoT functions such as blood pressure monitors, echocardiograms, and pacemakers. More research is needed with the underlying framework or legislation on the proper deployment and management of Medical IoT devices. This research effort would benefit from the comparison approach of security between passive and active MIoT devices as there is a lack of knowledge of security vulnerabilities based on active and passive MIoT devices. (Leedy & Ormrod, 2010).

7. REFERENCES

Argaw, S. T., Bempong, N.-E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Medical Informatics and Decision Making*, *19*(1). https://doi.org/10.1186/s12911-018-0724-5

Bonderud, D. (2019, June 19). IoT Security and the Enterprise: A Practical Primer. Security Intelligence; Security Intelligence. https://securityintelligence.com/articles/iot-security-and-the-enterprise-a-practical-primer/

Brown, A. (2013). *M2M Revenues by Industry Vertical*. Strategyanalytics.com. https://www.strategyanalytics.com/access-services/enterprise/iot/reports/report-detail/m2m-revenue-industry-vertical

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Choi, Y., Lee, Y., Moon, J., & Won, D. (2017). Security enhanced multi-factor biometric authentication scheme using bio-hash function. *PLOS ONE*, *12*(5), e0176250. https://doi.org/10.1371/journal.pone.0176250

Creswell, J. (1998). *Qualitative inquiry and research design: Choosing among five traditions* (p. 64). Sage.

Dutta, P. (2018). *How Technology Is Influencing Humanity In Daily Life*. Thriveglobal.com. https://thriveglobal.com/stories/how-technology-is-influencing-humanity-in-daily-life/

Eagan, C. (2020, January 9). *California's IoT cybersecurity bill: What it gets right and wrong*. Help Net Security. https://www.helpnetsecurity.com/2020/01/09/californias-iot-cybersecurity-bill/

Gartner. (2014). *Gartner Says Worldwide Smartwatch and Wristband Market Is Poised for Take Off*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2014-09-17-gartner-says-worldwide-smartwatch-and-wristband-market-is-poised-for-take-off

ISC2. (n.d.). *Why Join (ISC)² | Benefits of Membership*. Www.isc2.org. Retrieved January 26, 2021, from https://www.isc2.org/Benefits-of-Membership#

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09977-z

Lang, U. (2018). Securing Complex Cyber-Physical Medical Device Landscapes. *Information System Security Association*, *16*(4). https://objectsecurity.com/tmp/2018.04.ISSAJournal.UlrichLang.MedicalDeviceSecurity-article.pdf

Leedy, P. D., & Ormrod, J. E. (2010). Practical research.

Li, C.-T., Wu, T.-Y., Chen, C.-L., Lee, C.-C., & Chen, C.-M. (2017). An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System. *Sensors*, *17*(7), 1482. https://doi.org/10.3390/s17071482

Mantas, J., Hasman, A., Gallos, P., Kolokathi, A., & Househ, M. (2016). Unifying the applications and foundations of biomedical and health informatics. *Technology and Informatics*.

Martin, C. (2019). *Smart Home Technology Hits 69% Penetration in U.S.* Www.mediapost.com. https://www.mediapost.com/publications/article/341320/smart-home-technology-hits-69-penetration-in-us.html

McCaldin, D., Wang, K., Schreier, G., Lovell, N. H., Marschollek, M., Redmond, S. J., & Schukat, M. (2016). Unintended Consequences of Wearable Sensor Use in Healthcare. *Yearbook of Medical Informatics*, *25*(01), 73–86. https://doi.org/10.15265/iy-2016-025

Miclăuș, T., Valla, V., Koukoura, A., Nielsen, A., Dahlerup, B., Tsianos, G., & Vassiliadis, E.

(2019). Impact of Design on Medical Device Safety. *Therapeutic Innovation & Regulatory Science*. https://doi.org/10.1007/s43441-019-00022-4

Morse, J. M., & Field, P. A. (1996). An overview of qualitative methods. *Nursing Research*, 18–34. https://doi.org/10.1007/978-1-4899-4471-9_2

Muggler, M., Eshwarappa, R., & Cankaya, E. C. (2017). Cybersecurity Management Through Logging Analytics. *Advances in Intelligent Systems and Computing*, 3–15. https://doi.org/10.1007/978-3-319-60585-2_1

Olson, P. (2014). Wearable Tech Is Plugging Into Health Insurance. Forbes. http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#16d50cff5ba1.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Pew Research Center. (2019, October 28). *The Internet will continue to make life better*. Pew Research Center: Internet, Science & Tech; Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/10/28/4-the-internet-will-continue-to-make-life-better/

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The Rise of Consumer Health Wearables: Promises and Barriers. *PLOS Medicine*, *13*(2), e1001953. https://doi.org/10.1371/journal.pmed.1001953

Ragan, S. (2016, February 14). *Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers*. CSO Online. http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-

Thomson, S. (2010). Sample Size and Grounded Theory. *Journal of Administration and Governance*, *5*(1), 45–52.

Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2019). Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. *ICT Systems Security and Privacy Protection*, 134–148. https://doi.org/10.1007/978-3-030-22312-0_10

Williams, P., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305. https://doi.org/10.2147/mder.s50048

Zhang, G., & Ravishankar, M. (2019). Exploring vendor capabilities in the cloud environment: A case study of Alibaba Cloud Computing. *Information & Management*, *56*(3), 343–355. https://doi.org/10.1016/j.im.2018.07.008

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *Sixth International Conference on Semantics, Knowledge, and Grids*, *IEEE*(), 105–112. https://doi.org/10.1109/skg.

The Effect of Review Valence on Purchase of Time-Constrained and Discounted Goods

Prathamesh Muzumdar
pmmuzumdar@usf.edu
Muma College of Business
University of South Florida
Tampa Florida

Abstract

In the past decade, e-commerce industry has become a common source of electronic word of mouth (eWOM) for various products. Increasing online shoppers have generated enormous amount of data in form of reviews (text) and sales data. Aggregate reviews in form of rating (stars) have become noticeable indicators of product quality and vendor performance to prospective consumers at first sight. Consumers subjected to product discount deadlines search for ways in which they could evaluate product and vendor service using a comprehensible benchmark. Considering the effect of time pressure on consumers, aggregate reviews, known as review valence, become a viable indicator of product quality. This study investigates how purchase decisions for new products are affected by past customer aggregate ratings when a soon-to-expire discount is being offered. We examine the role that a consumer's attitude towards review valence (RV) plays as an antecedent to that consumer's reliance on RV in a purchase decision for time-discounted search goods. Considering review credibility, diagnosticity, and effectiveness as determinants of consumer attitude in a time-constrained search and purchase environment, we follow the approach-avoidance conflict theory to examine the role of review valence and perceived uncertainty in a time-constrained environment. The data was collected through an online survey and analyzed using structural equation modelling. This study provides significant implications for practitioners as they can better understand how review valence can influence a purchase decision. Empirical analysis includes two contributions: 1. It helps to understand how consumer attitude toward review valence, when positively influenced by the determinants, can lead to reliance on review valence, further influencing purchase decision; 2. Time constrained purchase-related perceived uncertainty negatively moderates the relationship between consumer attitude and reliance on review valence.

Keywords: Online Consumer Reviews, Review Valence, Perceived Uncertainty.

1. INTRODUCTION

In the last decade, online customer reviews (OCRs) have emerged as an important source of information for prospective buyers, substituting other forms of marketing promotions. OCRs act as electronic word-of-mouth (eWOM) for buyers (Q. B. Liu & Karahanna, 2017). OCRs are significant indicators of product quality, reliability, and performance (C. Liu & Forsythe, 2010). The advantage of OCRs is their accessibility compared to other forms of WOM and marketing promotions. Consumers can make their opinions easily accessible to other consumers through the Internet (Z. Zhang et al., 2020). The literature on eWOM has shown that the OCRs significantly influence customer purchase behavior (Q. B. Liu & Karahanna, 2017), further influencing product sales (Q. B. Liu & Karahanna, 2017; C. Liu & Forsythe, 2010).

Considering the influence of information available through various digital forms, it is important to understand the effects of time pressure and product promotions on consumers' incorporation of such information. In this study, we account for the significance of time pressure relating to a consumer purchase decision. Goods can be classified across a continuum of search,

experience, and credence claims. We will not consider credence goods in this paper (Z. Zhang et al., 2020). Experience goods can only be accurately evaluated after the product is purchased and then used (Z. Zhang et al., 2020). Search goods are both non-experience and non-credence goods that are evaluated prior to purchase using prior knowledge, direct product inspection, reasonable effort, and normal channels of information acquisition, such as Consumer Reports (Ford et al., 2021). Such goods have discounted prices during promotions, thereby being time-constrained for purchase. This generates a complex conflict for prospective consumers in making purchase decisions. Relying on few evaluation parameters, prospective consumers seek a shorter alternative to longer OCRs to make a decision.

Time-discounted search goods are non-experience goods which have discounted price for a specific time frame. This makes it deceptive for consumers to make an uncertain purchase decision for these products. Time constraints leave them with few options to evaluate the quality and performance unfamiliar product. Review valence plays a pivotal role in helping consumers unearth the insights in its quantified shorter evaluation form, e.g., product star rating plus number of reviews (Wang et al., 2020). Thus, consumers prefer to use aggregate reviews (review valence) as a measure to quickly judge product quality and performance to make the purchase decision (Allard et al., 2020). RV becomes a parameter to quickly judge a non-experience product and support the purchase decision; nevertheless, it still produces unforeseeable uncertainty among consumers. Most of the existing literature has focused on examining the influence of online consumer reviews on purchase decisions for experience goods (H. Zhang & Gong, 2020). In contrast, only a handful of studies have focused on search goods. Not much has been done to understand the role of OCRs on time-constrained price discounted search goods. To date, no study has examined the effects of review valence on purchase decisions for time-discounted search goods.

This study uses the approach-avoidance conflict theory to understand how time pressure influences consumers' evaluation parameters, affecting the purchase decision. Approach-avoidance conflict theory suggests that conflicts occur when a specific event or goal has appealing and unappealing characteristics (Penz & Hogg, 2011). Discounted search goods having purchase time pressure might lead to conflicts in the form of low price (appealing) or bad quality (unappealing). These outcomes are related to time pressure, which compels the consumer to make a quick decision based on a few easily comprehendible parameters like review valence (aggregate ratings). We, as researchers, try to address the following questions in this study:

1. Under time pressure, what impact does review credibility, diagnosticity, and effectiveness have on consumers' attitude towards review valence (RV) while using discounts on search goods?
2. Under time pressure, how does consumers' attitude toward review valence influence their reliance on review valence for making a purchase decision on search goods?
3. Under time pressure is perceived uncertainty, a significant moderator of the consumer's attitude in making a review valence less relevant?

The remainder of this paper is organized as follows: Section 2 discusses the theoretical background of the study, which includes five sub-sections. Section 3 takes into account the conceptual model and hypotheses. We have collected the data using online surveys and then analyzed them using structural equation modelling (SEM). Section 4 presents the methods and measurements used in this study. Section 5 outlines study results, and section 6 discusses research findings. The paper concludes with a summary of research findings and implications for future research and practice in Section 7.

2. THEORETICAL CONTEXT

WOM, in general, is defined as an informal advice or communication about products, services, and brands that can be communicated from one customer to another in person or through a distance communication medium (Mandal et al., 2021). eWOM is electronic word of mouth that is digitally communicated through the Internet (Beurer-Zuellig & Klaas, 2020). Online consumer reviews are the most exclusive eWOM omnipresent in different forms on online retail outlets. Because online consumer reviews are initiated by customers independent of the market, they are perceived to be more reliable and trustworthy than other communications (Mandal et al., 2021). Mandal et.al (2021) showed that OCRs are widely accepted as eWOM and are closely related to business success.
The growth of online retail and the reach of the internet has allowed consumers to share their experiences using OCRs; this provides the

consumers with an online channel to share their product evaluations. As a product of this process, online consumer reviews have emerged as a phenomenon influencing consumer purchase decisions (Tonietto & Barasch, 2020). Compared to traditional promotional marketing techniques and WOM, which are limited to a local physical social network (Lin & Xu, 2017), the impact of online consumer reviews is beyond local communities. It uses information technology and internet tools to reach people all over the world (Clemons et al., 2006). In their study, Wang et.al (2020) inferred that traditional WOM generally does not play the role of a direct decision variable for product sales. Recent research by Jensen et.al (Jensen et al., 2013) found a direct connection between online consumer reviews (eWOM) and product sales. For example, Kim et.al (Kim et al., 2011) studied the effect of online consumer reviews on hotel bookings.

Experience goods vs. time-discounted search goods

Consumers subjectively evaluate experience goods through sampling or purchase in order to evaluate their quality (Calderón Urbina et al., 2021). On the other hand, search goods are evaluated by feature properties, and consumers usually do not require interacting with the product for evaluation (H. Zhang & Gong, 2020). Examples of experience goods include music, books, and soda. Search goods include smartphones, cameras, and clothing (Mandal et al., 2021). With the rise in online retail, all search and experience goods features are searchable, and the traditional distinction between experience goods and search goods has been reduced (Calderón Urbina et al., 2021). However, the research by Zhang et.al (2020) found that the distinction is still valid due to the different ways in which product-related information is accessed and processed. Their study also shows that online consumer reviews help make purchase decisions for search goods (Calderón Urbina et al., 2021; H. Zhang & Gong, 2020).

Online consumer reviews and time-discounted search goods

OCRs about technology products are considered more relevant to customers than online marketing promotional information created by sellers (Mandal et al., 2021). Promotional information mostly includes the product's technical specifications. For experience goods, this information is important and helps consumers relate the technical features to their experience (Calderón Urbina et al., 2021; H. Zhang & Gong, 2020). In contrast, product details are important for consumers for search goods but are not enough to support their purchase decision (Tonietto & Barasch, 2020). Zhang et.al (2020) showed that consumers are also interested in knowing how other consumers feel about the product, technical specifications, and product conclusion. Online consumer reviews are provided by consumers who have used the product for a certain period and know the product's features.

Consumers who find it difficult to form an opinion on product purchases use online consumer reviews to help them comprehend the benefits of such products (Calderón Urbina et al., 2021). Non-experience buying relies heavily on consumers' ability to form an opinion from the information in the reviews. Consumers highly rely on online consumer reviews to support their purchase decision (H. Zhang & Gong, 2020) in case of search goods. In this study, we examine the role of OCRs in shaping consumers' attitudes toward review valence, especially when deciding on the purchase of search goods.

Approach-avoidance conflict theory

Intertemporal choices are defined as decisions that have consequences in multiple periods (Penz & Hogg, 2011). These choices require decision-makers to trade-off costs and benefits at different points in time (C. Liu & Forsythe, 2010). A decision about cashing a discount for goods is an intertemporal choice. Descriptive discounting models capture the phenomenon that most economic agents prefer current rewards to delayed rewards having similar magnitude (Penz & Hogg, 2011; C. Liu & Forsythe, 2010). Most current rewards in the form of smaller rewards are considered immediate discounts (D. Zhang et al., 2016). In this study, we examine the effects of immediate discounts on consumers' ability to make quick purchase decisions. Offers having a limited validity time for participation may increase discount redemption in a shorter period if consumers know the expiration date. Pressure to take action before the offer ends or time pressure and information about the offer are components of persuasion. Consumers seek to avoid losses associated with missed opportunities by making quick purchase decisions based on few selected product evaluation factors (Lee & Hong, 2021). This study proposes approach-avoidance conflict theory as a plausible theoretical mechanism to discuss the effects of time pressure and discounts on purchase decisions.

Approach-avoidance conflict theory shows the duality of event outcomes that occur when events are appealing and non-appealing simultaneously (Clemons et al., 2006). RV is a very comprehendible measure to evaluate a product in a shorter span of time and helps support consumers in making their purchase based on that one criterion. Though that makes the process less arduous for consumers to jump on the purchase decision, it also develops unsettling perceptions among consumers. These perceptions lead to uncertainty among consumers on their reliance on RVs. Do RVs give us complete insights on the product on display? Is this the question those consumers have in their minds? The use of RVs occurs due to the time pressure that promotions build during product sales, and perceived uncertainty comes out to be an unappealing outcome of such decisions. This study considers both time pressure and approach-avoidance conflict theory to examine how uncertainty influences consumers' reliance on easily comprehendible product criteria like RV.

Credibility and diagnosticity of OCRs

The credibility of OCRs in eWOM literature has been studied extensively for several years (Jha & Shah, 2021). Credibility in communications literature is defined as the extent to which a communication source is considered valid and perceivable to the reader (Jha & Shah, 2021; Cheung et al., 2012). Some have defined credibility as evaluation done by readers concerning the believability of a reviewer (Cheung et al., 2012). Diagnosticity is defined as the adequacy of a piece of conclusive information provided to the reader about the relevance of the information to the judgmental task (Weathers et al., 2015). A review is evaluated for its diagnosticity by the relevancy of the information it provides to the actual task, which the reader wants to complete (Cheung et al., 2012). Information usefulness for making a judgment over a decision is what makes the information very relevant. Relevancy of the information in reviews leads to diagnosticity (Jha & Shah, 2021). This study on OCRs heavily relies on consumers' evaluation of reviews to help them understand the product features and performance. Thus, these two variables play important roles in helping consumers evaluate reviews and develop an attitude toward reviews.

Review effectiveness

The effectiveness of online communication is well studied in IS literature. Online reviews are a type of user-generated content (UGC); their effectiveness plays an important role in influencing the readers' decision. Review effectiveness is defined as the degree to which a review can help consumers comprehend information and understand the judgmental task (Beurer-Zuellig & Klaas, 2020). Review effectiveness is multi-dimensional, and its three dimensions are popularity, helpfulness, and persuasiveness (Lin & Xu, 2017; Wu, 2017). Likes on reviews denote the helpfulness of the review (Hu et al., 2008); they indicate the richness of the information contained in the review. Hu et.al (2008) showed that highly liked reviews represent the predisposition of a review in helping consumers evaluate the information contained in the review. Review popularity represents the proneness of a review in attracting consumer attention (Zou et al., 2011) and is responsible for building awareness among consumers (Lin & Xu, 2017). Review persuasiveness is the final determinant of effectiveness; it convinces consumers to persuade and committing to making purchases (Kuan et al., 2015). In this study, we examine the role of effectiveness in influencing consumers' attitudes toward RV.

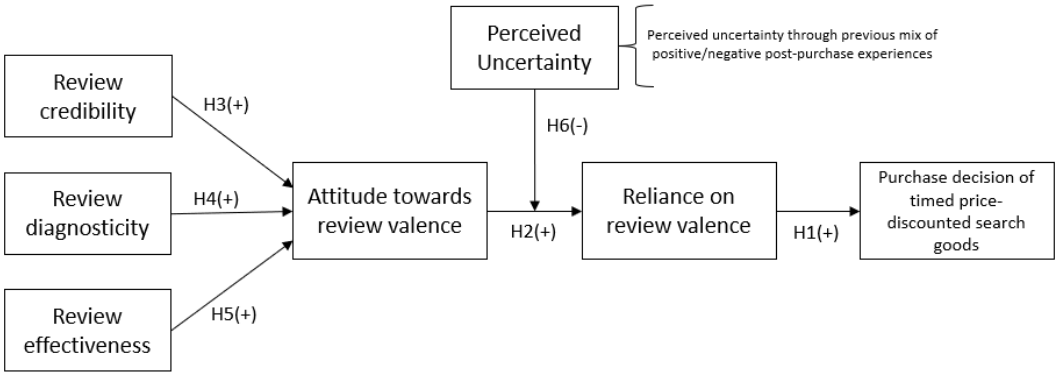

Figure 1. Conceptual model for purchase decision of timed price-discounted search goods

3. CONCEPTUAL MODEL AND HYPOTHESIS

The proposed conceptual model for the study is shown in Figure 1. Purchase decision is posited to be driven by consumers' reliance on OCRs driven by their attitudes towards reviews, which in turn are posited to be driven by review trustworthiness (credibility & diagnosticity) and effectiveness.

Reliance on review valence and purchase decision

In this study, reliance on review valence is viewed as the extent to which consumers depend on aggregate ratings to make their purchase decision. Reliance addresses the extent to which a consumer feels a need to use OCRs before making purchase decisions. At the same time, consumers worry about the decision quality if they do not adhere to extraneous advice through OCRs. Aggregate rating in the form of review valence becomes an easy way to assess product quality in a shorter time frame, helping consumers to decide for the purchase of timed price-discounted search goods. In the case of experience goods, previous experience with products makes it easy for the consumer to come up with the purchase. However, when it comes to timed price discounted search goods, it becomes important to purchase within the specified time frame to avail discount. For such consumers, it becomes important to rely on the aggregate ratings in the form of review valence. Consumer expertise can be expressed in the form of an online review (eWOM), helping new consumers get an insight into what the product has to offer consumers. However, more importantly, those insights in the form of ratings can help new consumers quickly conclude their decision. This conceptualization of online aggregated ratings (review valence) draws on the conclusion that reliance on online review valence is a more complex construct than simply following eWOM and traditional WOM; the amount of time spent with the medium and more belief in aggregated rating determines the severity of the influence on the consumer (Allard et al., 2020; Tonietto & Barasch, 2020; East et al., 2007). Therefore, we hypothesize that:

H1: Consumers' purchase decision of timed price-discounted search goods is positively influenced by their reliance on review valence.

Attitude toward review valence

In this study, attitude is defined as a tendency to evaluate an opinion with some degree of favor or disfavor, usually expressed in cognitive and behavioral responses (Tonietto & Barasch, 2020). Attitude toward online review valence speaks about consumers' feelings about online consumer reviews (Allard et al., 2020). A general tendency to view OCRs in either a positive or negative light gets reflected in their attitude. Consumers comprehend review valence better than online consumer reviews. Since it is an aggregated rating value, it helps consumers conclude in lesser time (East et al., 2007). This quickly leads to developing a positive or negative attitude toward review valence. This attitude further influences the consumers' reliance on review valence. Therefore, we hypothesize that

H2: Consumers' reliance on review valence is positively influenced by consumers' attitudes toward review valence.

Credibility and diagnosticity of online consumer reviews

In this study on OCRs, credibility is the extent to which consumers trust OCRs to deliver truthful and accurate product information. Diagnosticity signifies review relevancy towards the task at hand. Past studies have shown that credibility judgments and diagnosticity influence consumers' attitudes in various contexts (Jensen et al., 2013). In the case of OCRs, Zhang et.al (2016) found that along with time spent on a retailer website and product specifications, OCR credibility is an important determinant of attitude toward the OCR. Kaun et.al (2015) showed that consumers rely heavily on diagnosticity to believe in the facts presented in the information, and somewhere this affects their attitude toward the review. As time plays a crucial role in time-discounted search goods purchase decision, it is very important to examine how consumers perceive review valence (aggregate rating) as an accurate indicator of product evaluation. Shorter time makes it taxing and tenuous for consumers to read and appraise all reviews. Review valence becomes a strong indicator of product performance and quality at first glance, followed by reading selective reviews to support their thoughts on review valence. This study is determined to explore the role of review credibility and diagnosticity in the context of time-discounted search goods, wherein the shorter time frame to cash in the discount makes it difficult for the consumer to spend more time reading reviews. Therefore, we hypothesize that:

H3: Consumers' attitude towards review valence is positively influenced by the perceived review credibility of OCRs.

Review diagnosticity is defined as the degree to which a consumer can rely on reviews to make purchase decision (Chua & Banerjee, 2014). In this research, review diagnosticity is associated with review depth and review readability.

H4: Consumers' attitude toward review valence is positively influenced by the perceived review diagnosticity of OCRs.

Review effectiveness

Previous research on effectiveness has heavily focused on understanding its determinants and its effects on purchase intention. In their study, Lin et.al (2017) showed that review effectiveness is a determining factor of consumers' persuasion of a product. It influences the consumers' attitude toward OCRs by trusting the information in the review (Wu, 2017). Review persuasiveness is considered one of the determinants of effectiveness, influencing the consumers' overall attitude toward review information (Hu et al., 2008). Review helpfulness exhibits the richness of the information and its relevancy toward product features (Wu, 2017). Review popularity attracts consumers toward reviews and makes them more prone to believing in the information in the review (Cheung et al., 2012). Time pressure and price promotions make it tedious for consumers to read every review posted in support or against the product. It is important to understand the role of effectiveness on time-constrained evaluation criteria like review valence. Therefore, we hypothesize that

H5: Consumers' attitude toward review valence is positively influenced by the perceived review effectiveness of OCRs.

Perceived uncertainty

Product uncertainty refers to a situation where consumers realize at the post-purchase stage that the product, they bought is different from what they perceived it to be at the shopping stage. Such experiences lead to uncertain decisions during search and purchase periods. Perceived uncertainty is defined as emotional costs associated with unexpected losses that could occur after purchasing the product, caused by information asymmetry (Lee & Hong, 2021). The goal of the consumer is to evaluate the intrinsic quality of a product based on the information available in the reviews and then purchase the product with the lowest uncertainty. Search goods are non-experience goods; most consumers may or may not have previously used the product or conducted business with the online vendors. In such cases, there are financial and psychological uncertainties associated with the product and online vendors (Hong et al., 2017).

According to approach-avoidance conflict theory, events can have appealing and non-appealing outcomes. In such cases, perceived uncertainty can generate the fear of unexpected losses due to non-appealing outcomes. To understand the effects of perceived uncertainty on consumers' purchase decisions, we examine its moderating effects on consumers' attitudes and reliance on RV. As time pressure plays a crucial part in cashing discounts, we hypothesize that

H6: Perceived uncertainty negatively moderates the relationship between attitude toward review valence and reliance on review valence.

4. METHODS

The data to test the hypothesis was collected through a self-administered structured online survey using respondents drawn from Survey Monkey's panel of US consumers. Responses were collected only from respondents who had read or used an OCR within the past six months for searching for goods which they never experienced or used before. It was made sure through screening section that respondents were looking for price discounted goods with time deadline. A sample of 320 responses was purchased, and the sample size was established based on the guidelines in the SEM literature. The sample sizes are recommended to be between 100 and 400 respondents for the simple SEM model used in this study. It helps avoid unstable solutions at low sample sizes and sensitivity issues at large sample sizes (>500), often resulting in poor model fitting.

Measures and measure validation

All items for reliance on review valence and attitude towards review valence were adapted from Zou et.al (Zou et al., 2011) except items 3 and 4 from the variable attitude toward review valence. Items for reliance on RV reflect different dimensions of reliance as captured in dictionary definitions. In contrast, items for attitude toward RV reflect the degree of positivity or negativity that a consumer has toward RV in general. All items for review credibility and diagnosticity were adapted from Ghazisaeedi et.al (2012) and Hennig-Thurau and Walsh (2003), with adaptations made to reflect consumers' perceptions of the credibility and diagnosticity of OCRs. The items for review effectiveness and review uncertainty of OCRs were adapted from Kim et.al (Kim et al., 2011),

which reflect the consumers' perception of the effectiveness of the information presented in the review. Items for perceived uncertainty reflect the unpredictability consumers feel when comprehending information from the reviews. Consumer's purchase decision was measured using a single question, it is also the dependent variable in the conceptual model. All the items were measured using a Likert-type scale to which respondents expressed agreement/ disagreement on a seven-point scale (1 = strongly disagree; 7 = strongly agree).

Following Anderson and Gerbing (1988), before conducting structural analysis for hypothesized relationships, the construct measures were validated through confirmatory factor analysis (CFA) using LISREL for Windows. Table 1 summarizes standardized factor loadings, composite reliability, average variance extracted, and Cronbach's alpha. All the items were retained as standardized factor loadings were above the recommended level of 0.5 (Anderson & Gerbing, 1988). Construct reliability was measured via composite reliability and Cronbach's alpha to estimate the consistency of the construct. The values for both the constructs in Table 1 exceeded the minimum threshold value of 0.70, signifying the high reliability of the constructs. Convergent validity was verified through average variance extracted (AVE); it measured the overall variance in the indicators as truly representative of the latent construct. The AVE values ranging from 0.660 to 0.872 implied that convergent validity was achieved because all items in the measurement model were statistically significant.

The overall model fit statistics (Table 1) show an acceptable fit of the measurement model to the data [x 2(288 df) = 308 ($p < 0.001$); Comparative Fit Index (CFI) = 0.98; Root Mean Square Error of Approximation (RMSEA) = 0.058; Goodness-of-Fit Index (GFI) = 0.90; Adjusted Goodness-of-Fit Index (AGFI) = 0.84]. RMSEA is just slightly higher than the recommended minimum value of 0.05, GFI is 0.94 (above 0.9 is preferable), and AGFI is slightly below 0.9 at 0.89. Table 2 shows discriminant validity; it was checked by comparing the shared variance among variables with the square root of AVE by each construct. The shared variances among factors are lower than the square root of AVE. We conclude that the discriminant validity was achieved.

Common Method Bias

To address common method bias we analyzed the data through Harman's single factor analysis using principal axis factoring (Jordan & Troth). For results we extract 30.8% of variance which is less than 50%. We conclude that no common method bias exists in our measurement.

5. ANALYSIS AND RESULTS

Descriptive Statistics

Table 3 shows the means and standard deviations for all the constructs. Means for all the constructs are above the scale mid-point of 4. One sample t-tests were conducted to test if one can conclude that scores of the constructs are above the scale mid-point in the larger population based on the sample means. The results show that all the t-values are statistically significant at the 1 percent level. Thus, we conclude that, in general, the study population finds OCRs to be both valuable and credible; they have positive attitudes towards review valence and generally rely on these aggregate ratings in product purchase decisions.

Hypotheses Tests

The hypothesized relationships (H1 to H4) were tested using structural equation modeling (SEM) (table 4) by adding structural parameters to the measurement model in Table 1. For this test, the structural model was run on the entire sample. The coefficient for the reliance on review valence and purchase decision relationship is positive and statistically significant ($b = 0.42$; $p < 0.01$). In general, consumers' reliance on review valence positively influences their purchase decision for timed discounted search goods, supporting H1. Aggregate reviews can be a strong determinant of purchase decisions. From table 4, the coefficient for the attitude toward review valence and reliance on review valence relationship is positive and statistically significant ($b = 0.68$; $p < 0.01$). It implies that a positive attitude towards review valence can lead to more reliance on review valence, supporting H2. The coefficients for review credibility ($b = 0.76$; $p < 0.01$), review diagnosticity ($b = 0.48$; $p < 0.01$), and review effectiveness ($b = 0.52$; $p < 0.01$) are positive and statistically significant, supporting hypotheses H3, H4, and H5, respectively. Thus, both factors are significant drivers of consumers' attitudes toward review valence. In relative terms, however, perceived credibility has a greater impact than perceived diagnosticity.

Moderator effects

A moderator analysis was performed in SEM to test the two moderators in table 5. The moderating effect of review effectiveness on the relationship between attitude toward review valence and reliance on review valence and

perceived uncertainty on the relationship between reliance on review valence and purchase decision. A moderating effect is identified when the chi-square significantly increases after the paths are constrained. Table 5 shows the results of the moderating test for the overall model and each path. The chi-square change of the overall model is significant ($p<0.001$), showing a possible moderating effect and supporting H5 and H6. Thus, both aspects are determined to be significant drivers of consumers' attitudes toward review valence. In relative terms, however, review credibility has a more significant impact than review diagnosticity.

6. DISCUSSIONS AND IMPLICATIONS

This study examined the role of review credibility and review diagnosticity (OCRs) on consumers' attitudes toward review valence and how such attitudes impact the extent to which consumers rely on review valence in purchase decisions of non-experience goods when the decision is time-constrained. Results show that review credibility and review diagnosticity are strong positive drivers of attitudes toward review valence, with review credibility having a relatively higher impact. In turn, attitudes strongly predict the tendency to rely on review valence. Additional analyses show a significant moderating effect of review effectiveness and perceived uncertainty. It is also noteworthy that respondents found review valence (aggregate ratings) credible, relevant, and effective, as evidenced by the high mean scores. Respondents likewise had positive attitudes toward review valence and generally relied on the aggregate ratings for product purchase decisions. The results have theoretical and managerial implications.

Theoretical Implications

From a theoretical point of view, this research adds to the OCR literature in two important ways. First, it introduces two constructs that can add to our understanding of how consumers relate to review valence (aggregate rating) when it comes to time-discounted search goods and how they rely on the aggregate rating of the review valence to support their purchase decision. The construct of reliance on review valence adequately captures a growing phenomenon that has been observed in many recent consumer surveys about time-constrained discounted goods, i.e., consumers reporting an increasing tendency to rely on review valence for many purchase decisions of time-constrained discounted goods, while overlooking most reviews in the process. Attitude toward review valence is a relevant construct in the digital economy and retail. There is a growing realization by consumers that OCRs are subjective regarding the credibility and diagnosticity of the reviews. The study calls attention to these two new constructs and provides initial conceptualizations and empirical analysis.

Second, this study contributes to the limited literature on the possibility of perceived uncertainty as a moderator, regulating the relationship between consumers' attitudes and reliance on review valence. While perceived uncertainty has been explored in different capacities in other studies (Clemons et al., 2006), this study considers the uncertainty developed under time-constrained circumstances while purchasing a time-discounted search goods. The present study found a significant impact of perceived uncertainty as a moderating variable. Furthermore, it was successful in providing theoretical and empirical grounds for expecting the existence of approach-avoidance conflict theory in OCRs. Further research is needed, possibly in different contexts, to understand the role of perceived uncertainty in moderating the main effects of OCRs.

Industrial Implications

From an industrial point of view, this study's findings are helpful for marketing managers to the extent that they demonstrate the power that review valence (aggregate reviews), a very common noticeable value in OCRs, exert on consumer purchase decisions. The findings also suggest that managers also need to recognize the importance of perceived uncertainty in moderating the relationship between attitude and reliance. Furthermore, the study signifies the importance of review credibility in driving the attitude and further reliance. Thus, the online review system needs to employ techniques that help reduce uncertainty and generate review credibility in time-constrained environments, e.g., by finding ways to communicate the expertise (knowledge) and trustworthiness (unbiased motives) of reviewers (Weathers et al., 2015).

7. LIMITATIONS AND SUGGESTIONS FOR FUTURE WORK

This study has limitations that future studies could address. First, it focused on the effects of review valence on time-discounted search goods. However, given the widely held notion that higher review volume could suffice the

genuineness of OCRs, it is essential to study the effect of the volume for such goods. Does volume moderate the relationship between attitude and reliance? At lower volumes, do consumers rely on higher aggregate ratings? If yes, what are the determinants of such phenomena?

Second, the moderating effects of perceived uncertainty exist when we consider the approach-avoidance conflict theory. It would be interesting to explore which other variables and theories can exhibit their influence on purchase decision of discounted search goods under time pressure. Third, our measures of reliance of review valence had excellent psychometric properties; they did not address the issues surrounding the construct and items scales. Researchers can pursue the development of measures to better represent the constructs.

8. REFERENCES

Allard, T., Dunn, L. H., & White, K. (2020). Negative Reviews, Positive Impact: Consumer Empathetic Responding to Unfair Word of Mouth. *Journal of Marketing*, *84*(4), 86–108. https://doi.org/10.1177/0022242920924389

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411

Beurer-Zuellig, B., & Klaas, M. (2020). The Social Side of Brick and Mortar: The Impact of Brand-Related User-Generated Content on Different Consumer Typologies in Food Retailing. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. Published. https://doi.org/10.24251/hicss.2020.314

Cheung, C., Sia, C. L., & Kuan, K. (2012). Is This Review Believable? A Study of Factors Affecting the Credibility of Online Consumer Reviews from an ELM Perspective. *Journal of the Association for Information Systems*, *13*(8), 618–635. https://doi.org/10.17705/1jais.00305

Chua, A. & Banerjee, S. (2014). Developing a Theory of Diagnosticity for Online Reviews. Proceedings of the International Multi Conference of Engineers and Computer Scientists 2014, Vol I, IMECS 2014, March 12 - 14, 2014, Hong Kong

Clemons, E. K., Gao, G. G., & Hitt, L. M. (2006). When Online Reviews Meet Hyperdifferentiation: A Study of the Craft Beer Industry. *Journal of Management Information Systems*, *23*(2), 149–171. https://doi.org/10.2753/mis0742-1222230207

East, R., Hammond, K., & Wright, M. (2007). The relative incidence of positive and negative word of mouth: A multi-category study. *International Journal of Research in Marketing*, *24*(2), 175–184. https://doi.org/10.1016/j.ijresmar.2006.12.004

Ford, G., Smith, D., & Swasy, J. (1988),"An Empirical Test of the Search, Experience and Credence Attributes Framework", in NA - Advances in Consumer Research Volume 15, eds. Micheal J. Houston, Provo, UT: *Association for Consumer Research*, Pages: 239-244.

Hennig-Thurau, T., Walsh, G., & Walsh, G. (2003). Electronic Word-of-Mouth: Motives for and Consequences of Reading Customer Articulations on the Internet. *International Journal of Electronic Commerce*, *8*(2), 51–74. https://doi.org/10.1080/10864415.2003.11044293

Hong, H., Xu, D., Wang, G. A., & Fan, W. (2017). Understanding the determinants of online review helpfulness: A meta-analytic investigation. *Decision Support Systems*, *102*, 1–11. https://doi.org/10.1016/j.dss.2017.06.007

Hu, N., Liu, L., & Zhang, J. (2008). Do Online Reviews Affect Product Sales? The Role of Reviewer Characteristics and Temporal Effects. *SSRN Electronic Journal*. Published. https://doi.org/10.2139/ssrn.1324190

Jensen, M. L., Averbeck, J. M., Zhang, Z., & Wright, K. B. (2013). Credibility of Anonymous Online Product Reviews: A Language Expectancy Perspective. *Journal of Management Information Systems*, *30*(1), 293–324. https://doi.org/10.2753/mis0742-1222300109

Jha, A. K., & Shah, S. (2021). Disconfirmation effect on online review credibility: An experimental analysis. *Decision Support Systems*, *145*, 113519. https://doi.org/10.1016/j.dss.2021.113519

Jordan, P., & Troth, T. (2020). Common method bias in applied settings: The dilemma of researching in organizations. *Australian Journal of Management*. 45(1):3-14. doi:10.1177/0312896219871976

Kim, E. E. K., Mattila, A. S., & Baloglu, S. (2011). Effects of Gender and Expertise on Consumers' Motivation to Read Online Hotel Reviews. *Cornell Hospitality Quarterly*, *52*(4), 399–406. https://doi.org/10.1177/1938965510394357

Kuan, K., Hui, K. L., Prasarnphanich, P., & Lai, H. Y. (2015). What Makes a Review Voted? An Empirical Investigation of Review Voting in Online Review Systems. *Journal of the Association for Information Systems*, *16*(1), 48–71. https://doi.org/10.17705/1jais.00386

Lee, J., & Hong, I. B. (2021). The Influence of Situational Constraints on Consumers' Evaluation and Use of Online Reviews: A Heuristic-Systematic Model Perspective. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1517–1536. https://doi.org/10.3390/jtaer16050085

Lin, C. A., & Xu, X. (2017). Effectiveness of online consumer reviews. *Internet Research*, *27*(2), 362–380. https://doi.org/10.1108/intr-01-2016-0017

Liu, C., & Forsythe, S. (2010). Sustaining Online Shopping: Moderating Role of Online Shopping Motives. *Journal of Internet Commerce*, *9*(2), 83–103. https://doi.org/10.1080/15332861.2010.503848

Liu, Q. B., & Karahanna, E. (2017). The Dark Side of Reviews: The Swaying Effects of Online Product Reviews on Attribute Preference Construction. *MIS Quarterly*, *41*(2), 427–448. https://doi.org/10.25300/misq/2017/41.2.05

Mandal, S., Sahay, A., Terron, A., & Mahto, K. (2021). How implicit self-theories and dual-brand personalities enhance word-of-mouth. *European Journal of Marketing*, *55*(5), 1489–1515. https://doi.org/10.1108/ejm-07-2019-0591

Mehdi Ghazisaeedi,. (2012). Trustworthiness of product review blogs: A source trustworthiness scale validation. *African Journal of Business Management*, *6*(25). https://doi.org/10.5897/ajbm12.079

Penz, E., & Hogg, M. K. (2011). The role of mixed emotions in consumer behaviour. *European Journal of Marketing*, *45*(1/2), 104–132. https://doi.org/10.1108/03090561111095612

Tonietto, G. N., & Barasch, A. (2020). Generating Content Increases Enjoyment by Immersing Consumers and Accelerating Perceived Time. *Journal of Marketing*, 002224292094438. https://doi.org/10.1177/0022242920944388

Wang, L., Gunasti, K., Shankar, R., Pancras, J., & Gopal, R. (2020). Impact of Gamification on Perceptions of Word-of-Mouth Contributors and Actions of Word-of-Mouth Consumers. *MIS Quarterly*, *44*(4), 1987–2011. https://doi.org/10.25300/misq/2020/13726

Weathers, D., Swain, S. D., & Grover, V. (2015). Can online product reviews be more helpful? Examining characteristics of information content by product type. *Decision Support Systems*, *79*, 12–23. https://doi.org/10.1016/j.dss.2015.07.009

Wu, J. (2017). Review popularity and review helpfulness: A model for user review effectiveness. *Decision Support Systems*, *97*, 92–103. https://doi.org/10.1016/j.dss.2017.03.008

Zhang, D., Zhou, L., Kehoe, J. L., & Kilic, I. Y. (2016). What Online Reviewer Behaviors Really Matter? Effects of Verbal and Nonverbal Behaviors on Detection of Fake Online Reviews. *Journal of Management Information Systems*, *33*(2), 456–481. https://doi.org/10.1080/07421222.2016.1205907

Zhang, H., & Gong, X. (2020). Consumer susceptibility to social influence in new product diffusion networks: how does network location matter? *European Journal of Marketing*, *55*(5), 1469–1488. https://doi.org/10.1108/ejm-06-2019-0491

Zhang, Z., Zhang, Z., & Chen, P. Y. (2020). Early Bird Versus Late Owl: An Empirical Investigation of Individual Shopping Time Habits and its Effects. *MIS Quarterly*, *45*(1), 117–162. https://doi.org/10.25300/misq/2021/14312

Zou, P., Yu, B., & Hao, Y. (2011). Does the Valence of Online Consumer Reviews matter for Consumer Decision Making? The Moderating Role of Consumer Expertise. *Journal of Computers*, *6*(3). https://doi.org/10.4304/jcp.6.3.484-488

Editor's Note:

This paper was selected for inclusion in the journal as the CONISAR 2021 Best Paper The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2021.

9. APPENDIX

Items	Std. loadings	Composite reliability	Average variance extracted	Cronbach's alpha
Reliance on review valence		0.88	0.68	0.86
If I do not consider aggregate rating before buying a product, I worry about my decision	0.86			
Aggregate ratings are more valuable to me than the opinion of my friends	0.92			
I trust aggregate ratings more than the opinion of those around me	0.72			
Attitude toward review valence		0.86	0.66	0.88
Online aggregate ratings are helpful for my decision-making	0.88			
Online aggregate ratings make me confident in purchasing a product	0.67			
I find online aggregate ratings to be informative	0.58			
Online aggregate ratings are a great way to discover good things about products and services	0.78			
Online aggregate ratings are a great way to discover bad things about products and services	0.66			
Review credibility		0.88	0.72	0.87
Not dependable . . . Dependable	0.61			
Not trustworthy . . . Trustworthy	0.84			
Not credible . . . Credible	0.72			
Not believable . . . Believable	0.91			
Not reputable . . . Reputable	0.82			
Review diagnosticity		0.84	0.70	0.86
I find individual review ratings to be informative	0.68			
I find in-depth and detailed reviews to be informative	0.72			
I find information in the reviews to be understandable and readable	0.58			
I find reviewers' profile to be authentic	0.88			
Review effectiveness		0.83	0.78	0.88
I find the review helpful in making the purchase	0.86			
The information in the review motivates me to purchase the product	0.72			
I find the popular reviews to be very relevant with product information	0.86			
Perceived uncertainty		0.84	0.72	0.86
I feel uncertain about the information in the review	0.88			
I feel uncertain about reviewers' experience with the product	0.62			
I feel uncertain about the authenticity of the aggregate ratings	0.78			
Purchase decision I would like to purchase the product	Dependent variable			

Table 1. Measurement model analysis

	1	2	3	4	5	6
1. Reliance on review valence	**0.811**					
2. Attitude toward review valence	0.218	**0.834**				
3. Review credibility	0.446	0.328	**0.868**			
4. Review diagnosticity	0.403	0.160	0.172	**0.824**		
5. Review effectiveness	0.268	0.327	0.228	0.162	**0.812**	
6. Perceived uncertainty	0.116	0.186	0.366	0.432	0.436	**0.812**

Notes: Diagonals represent the square root of the AVE

Table 2. Results of tests for discriminant validity of study constructs

	Descriptive statistics		One sample t-test	
Constructs	**Mean**	**SD**	***t* (df)**	***p***
Reliance on review valence	4.32	1.20	4.48 (282)	0.008
Attitude towards review valence	5.27	1.51	3 (282)	0.000
Review credibility	5.67	1.78	1.65 (298)	0.000
Review diagnosticity	4.82	1.13	4.66 (271)	0.001
Review effectiveness	5.69	1.61	1.94 (271)	0.000
Perceived uncertainty	4.89	1.16	13 (288)	0.000
Purchase decision	5.74	1.32	9.41 (282)	0.000

Table 3. Descriptive statistics

Hypotheses			Estimate	S.E.	C.R	P value	Results
H1	Reliance on Review valence	→ Purchase decision	0.42	0.112	2.842	0.000*	Supported
H2	Attitude towards Review valence	→ Reliance on Review valence	0.68	0.162	1.432	0.000*	Supported
H3	Review credibility	→ Attitude towards Review valence	0.76	0.132	2.682	0.000*	Supported
H4	Review diagnosticity	→ Attitude towards Review valence	0.48	0.174	1.786	0.004*	Supported
H5	Review effectiveness	→ Attitude towards Review valence	0.52	0.156	2.016	0.000*	Supported

*p-value<0.01

Table 4. Result of hypothesized structural model

Hypothesis	Constrained model	Unconstrain-ed model	Chi-square difference	Result on moderati-on	Result on hypothesis
H6 Perceived uncertainty moderation effect	388.486 (df = 282)	369.320 (df = 278)	20.368	Significant	Supported

Table 5. Result of the effects of moderating variables

Harvesting Intrinsically Verifiable Trust: Building a Honey Traceability System for Sustainable Development

Max A.S. Rünzel
maxruenzel@gmail.com
Center for Analytics Research and Education

Edgar Hassler
hassleree@appstate.edu
Department of Computer Information Systems

Brandy Hadley
hadleybe@appstate.edu
Department of Finance, Banking and Insurance

Aaron Ratcliffe
ratcliffeah@appstate.edu
Department of Marketing and Supply Chain Management

James T. Wilkes
wilkesjt@appstate.edu
Computer Science Department

Joseph A. Cazier
cazierja@appstate.edu
Center for Analytics Research and Education

Appalachian State University
Boone, NC 28608-2049

Abstract

Creating and building trust between consumers and producers is an important and challenging problem for the global economy, in particular for agricultural markets that rely on smallholder producers in mostly rural areas. We propose that Distributed Ledger Technology (DLT) can support a new, more scalable, and robust form of trust creation built on value congruence and *intrinsically verifiable trust*. A permissioned blockchain, in combination with a data-backed record-keeping system and IoT sensor data, allows producers and consumers to verify product characteristics such as provenance, production conditions, and environmental, social, and economic impacts. We study the application of DLT and our model for trust creation in the context of honey supply networks. Honey is

one of the most adulterated food products globally and honey production offers high potential for rural development, livelihood fortification, and food security through crop pollination. We demonstrate how the implementation of DLT may help mitigate the deteriorating trust in honey product integrity while, at the same time, grant smallholder beekeepers greater access to markets and leverage for product differentiation.

Keywords: Economic Development, Sustainability, Blockchain, Trust, Value Congruence

1. INTRODUCTION

Research shows that consumers would be willing to pay more for a product if they knew it was in line with their values (Cazier et al., 2006 and Cazier et al., 2017). More specifically, Loreiro and Lotade (2005) show that consumers are willing to pay higher price premiums for fair trade labeled coffee over organic offerings. To underscore food labelling's importance, Tonkin et al. (2015) describe the labelling as "a channel for communication between the food system and consumers" (p.319).

Providing the consumer with choices that are specific, safe, nutritious, ecologically-viable, and profitable for the producers helps to grow markets and unlock the development potential of smallholder producers and rural areas through product differentiation. Research shows that Distributed Ledger Technology (DLT) has the potential to further enhance traceability and accountability throughout the production and transport process (Min, 2019). In addition, DLT can create an infrastructure that enables consumers to connect with producers and the origin of their produce through technology while reducing the cost of product differentiation.

To show the potential of DLT to strengthen supply networks for different groups of stakeholders, we will use honey production as a use case for the beneficial extension of trust based on three principal reasons as summarized in Table 1. First, beekeeping has been described as an ideal, accessible, and empowering opportunity for rural entrepreneurs in economically-challenged areas (Mburu et al., 2015). Start-up costs are low, the infrastructure required is minimal, and, as a non-perishable good, honey can be stored and sold throughout the year. Hence, development actors, governments, and farmers have embraced beekeeping as a means for livelihood diversification in rural and semi-urban areas contributing to the United Nations Sustainable Development Goals (see Table 1) (Mujuni et al., 2012; Ogaba, M., and Akongo, T., 2001). Second, beekeeping offers positive externalities by providing ecosystem services in the form of pollination, stabilizing yields, biodiversity, and ecologically-intensifying farming practices (Klein et al., 2007). Third, bottled honey is also among the most adulterated food products in the world, currently ranking among the highest three, creating a strong incentive for more transparent honey supply networks globally (García, 2018).

This paper studies the promise and implementation challenges of applying DLT to the beekeeping sector to enable product integrity and encourage sustainable development. The objective is to illustrate how such a system can support supply network stakeholders from beekeepers to aggregators to vendors and consumers in adopting and supporting sustainable production processes.

Beekeeping-related impact	United Nations Sustainable Development Goal
Livelihood diversification (Mujuni et al., 2012; Ogaba, M., and Akongo, T., 2001)	Goal 1 - No Poverty Goal 2 - Zero Hunger Goal 8 - Decent Work and Economic Growth
Pollination ecosystem services to farmers, stabilizing yields and biodiversity (Klein et al., 2007)	Goal 11 - Sustainable Cities and Communities Goal 13 - Climate Action
More accountable honey production (García, 2018).	Goal 12 - Responsible Consumption and Production

Table 1: Beekeeping-related impacts and their contribution to the Sustainable Development Goals.

2. RELATED WORK

Value Congruence and Purchasing Decisions A value is understood as a set of principles or standards guiding an individual's conduct. Moreover, values serve as a normative

guide when choosing between various behavioral patterns (Elizur and Sagie, 1999). While consumer values are based on personal beliefs and backgrounds, a company projects a variety of values. In his work on the links between product attributes and values, Gutman (1982) finds that values significantly influence purchasing behaviors.

Value congruence defines the state when specific values held by consumers are congruent with the values projected by a company (Cazier et al., 2006 and Cazier et al., 2017). Cazier et al. (2007) and Zhao et al. (2012) show that value congruence increases trust and impacts the disclosure of personal information both directly and indirectly (through trust). In making value-based purchasing decisions as reflected in the choice of ethically or ecologically labeled items, value congruence takes a prominent role (Cazier et al., 2017). Namely, the congruence of values between organizations and consumers, upon which purchasing decisions rely, is facilitated through trust (Cazier et al., 2006).

Trust

Trust is defined as, "The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer, Davis and Schoorman, 1995, p. 712). Furthermore, trust is the willingness to take a risk and not the level of risk per se. In their model, Mayer, Davis, and Schoorman define the propensity to trust as a trait that "leads to a generalized expectation about the trustworthiness of others" or "the general willingness to trust others" (p. 715). While the natural propensity to trust varies among people, it can be influenced by the three primary forces of trust creation outlined below. These forces change the person's perceptions on one or more of the three dimensions of trustworthiness.

The Dimensions of Trustworthiness

Following Mayer et al.'s (1995) work, trust is commonly theorized to be built upon three dimensions: *ability*, *benevolence*, and *integrity*. Ability is the group of skills, competencies, and characteristics that enable a party to influence a specific domain. While the ability factor includes domain level expertise, it is not limited to that element. Other elements such as quality, innovativeness, and prestige can influence the perception of ability, which may disguise the true ability. Benevolence is the extent to which a trustee is believed to want to do good for the one trusting them, aside from their own self-centered motive. Integrity is the trustor's perception that the trustee will adhere to a set of principles that the person trusting them finds acceptable.

The Three Primary Forces of Trust Creation

Trust is a complex multidimensional construct that can be affected in different ways by different trust production methods (Zucker, 1986). Namely, three main forces lead to the creation of trust by producing information on and influencing perceptions of the dimensions of trustworthiness: *process-*, *characteristic-* and *institution-based* trust creation (See Figure 1) (Zucker, 1986, Cazier, 2007). *Process-based trust production* captures how information from past experiences and interactions influence perceptions of trustworthiness for future exchanges. *Characteristic-based trust production* influences perceptions of the dimensions of trustworthiness through a sense of shared commonality with the other party that may include shared values, a common background, culture, or ethnicity.

Trust is increased by having something in common with the other party or by possessing a characteristic the trustor finds desirable. Trust based on characteristics corresponds to the factor of benevolence and integrity (Cazier, 2007). *Institution-based trust* influences perceptions of the dimensions of trustworthiness through the use of a third party, which can be a government agency, a bank, or some other central organization that, in its role as facilitator or intermediary, assures the trustworthiness of the target organization. Such a transference of trust to intermediaries, then allows an entity to benefit from that trust. The concept is illustrated in Figure 1. below.

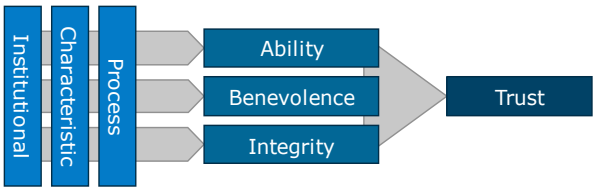

Figure 1. The Primary Forces of Trust Creation - Traditional Model For Trust Creation adapted from Cazier (2007).

Not all primary forces of trust production affect trust in the same way, and trust is not binary, it goes beyond simply trusting or not trusting (Zucker, 1986). Different types of trust creation can affect the factors of trustworthiness in various ways, prompting different behaviors in the trustors.

The three types of trust creation defined above have several weaknesses. Any recently established company faces the challenge of convincing the consumer of the integrity of its products, as both process-based and characteristic-based trust are limited in the early stages of a business endeavor where prior exchanges are absent or constrained. Furthermore, characteristic-based trust does not bridge well across cultures as regional or national borders confine shared commonalities. This has become a more prominent limitation of trust building in our context due to globalization of agricultural supply chains as it relates to fair trade products and to smallholder farmers specifically.
These limitations in scalability to new (process-based trust) or foreign (characteristic-based trust) markets have left institutional-based trust as the primary source for trust creation for international commerce. However, institution-based trust is also limited in its ability to promote rural economic growth. Indeed, institution-based trust, which in the development sector has manifested itself in labels and certificates, has been a significant barrier to entry for many smallholder farmers in rural areas due to significant requirements regarding infrastructure or production capacity and quality (Barrett et al., 2001). Therefore, institution-based trust often only scales at a high cost. At the same time, institutions may lack genuine trust, especially across borders, as they have shown to be prone to corruptibility.

Distributed Ledger Technology
Distributed Ledger Technology (DLT) enables the secure functioning of a decentralized digital database through a defined protocol. The distributed architecture of the network eliminates the need for a central authority to guard against manipulation (Swan, 2015).

DLT utilizes cryptography to store all the information in a secure and accurate manner. Once stored, the information becomes an immutable database and is governed by the rules of the network. Stored data can be accessed via keys and cryptographic signatures (Olnes et.al, 2017).

The nature of a decentralized ledger makes it immune to a cyber-attack, as all the copies stored across the network must be attacked at the same time to be successful. Additionally, the peer-to-peer sharing and updating of records make the whole process more effective, faster and cheaper (Nakamoto, 2008).

For additional information, the reader is referred to Olnes et.al. (2017).

3. THEORY DEVELOPMENT

In light of the limitations of traditional forces for trust creation outlined above, nascent DLT may help pave the way for a new force for trust creation. We model intrinsically verifiable trust as a force of trust creation, similar to institution-based trust creation, that influences a stakeholder's perceptions of the dimensions of trustworthiness. Driven by its underlying consensus mechanism, explained in more detail below, DLT's decentralized, immutable and secure nature, allows anyone, anywhere - in theory - to verify trust beyond processes, institutions, and characteristics. We define this new force for trust creation as follows.

Intrinsically Verifiable Trust describes the characteristic of being verifiable by itself in an independent way. Notably, intrinsically verifiable trust influences perceptions on the dimensions of trust through an underlying automated cryptographic and algorithmic mechanism that allows any user to verify the existence and veracity of the provided information independently.

The intrinsically verifiable nature of DLT, among many other applications, allows consumers to gain confidence through verifiable and potentially real-time traceability of marketed goods along a digitized supply network. Since trust has been proven to increase price premiums (Cazier et al., 2017), DLT-enabled intrinsically verifiable trust should also positively impact prices vendors can charge for agricultural and other products. Figure 2. Illustrates this additional force for trust creation.

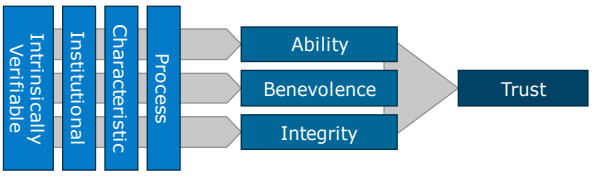

Figure 2. Updated Model for Trust Creation adapted from Cazier (2007).

The distributed ledger allows those in the value chain with limited influence, time, resources, or technical abilities to see the actions of other organizations with more power. For consumers, intrinsically verifiable trust helps to unveil the actors at stages further up the supply chain toward the producer. The consumer may not have the time, resources, or technical

capabilities to evaluate all of the information on the blockchain, but knowing it exists could still influence perceptions of dimensions of trustworthiness in other players across stages of the supply chain.

Intrinsically verifiable trust allows the producers to see further down the supply chain toward the consumer and trust that their product has not been adulterated along the way and that they are receiving a fair price for the product. Throughout the network, intrinsically verifiable trust helps to enable greater information sharing and more accurate forecasting as upstream players have a clearer picture of end consumer demand, which helps to support supply chain coordination and address issues with the bullwhip effect.

Intrinsically verifiable trust will likely play a more prominent role as the supply chain becomes longer, more complex, and increasingly globalized. Let's consider some simple examples in our context of honey supply chains to illustrate this point.

- Case #1: Suppose the consumer purchases the honey from a favorite small local producer who sells it at the local farmer's market or a roadside produce stand. In this case, a blockchain or IoT sensors may help the seller to build trust by verifying where certain actions were taken in production; but given the proximity, the consumer would likely rely more on process-based and characteristic-based forces of trust creation. For example, the consumer drives by the producer's farm on the way to work, the consumer has purchased honey with that producer in the past, or the consumer and the seller attend the same faith community or drive the same model of car.

- Case #2. Suppose the consumer purchases the honey from a favorite small local bakery that procured the honey directly from a small producer within the same region. In this case, blockchain technology could help to verify the producer's actions as in Case #1 and now also the seller's actions, e.g., the product was not altered, damaged, or stored incorrectly. However, process- and characteristic- based trust still play prominent roles. Perceived shared characteristics due to local sourcing could promote trust between the consumer and the producer. Past experiences and shared characteristics with the bakery could promote trust between the consumer and the seller, e.g., the consumer also buys bread and jam from this bakery and has had favorable past experiences.

- Case #3. Suppose the consumer purchases honey from a local franchise of a large grocery store chain that stocks honey produced by a small producer of similar size to Cases #1 and #2 in a country on a different continent. The product must pass through multiple hands including an aggregator, exporter, and distributor before reaching the grocery store. The product is labeled "organic fair trade certified", but the consumer recently read a news article discussing corruption in fair trade certification. In this case, the intrinsically verifiable trust will play a greater role by allowing the consumer to see further up the supply chain across a wider scope of activities and by addressing the gaps in process-, characteristic-, and institution-based forces of trust creation due to globalization and the complexity for this scenario.

Intrinsically verifiable trust may play a crucial role in the development sector. Enabling smallholder producers backed by DLT to access both local and the global supply networks can allow them to sell agricultural produce based on verifiable provenance and characteristics to markets of value congruent consumers. As Barrett et al. (2001) show, currently, smallholder producers often rely on prohibitively expensive third-party assessment to prove the integrity of their products.

Distributed ledger-based systems, however, allow for a low entry-barrier implementation, as access to the internet is the driving requirement to start recording time-stamped and immutable activities throughout the production process. Consumers, then, being able to verify the integrity of the product, would be more willing to pay price premiums, which eventually help smallholder farmers in rural areas strengthen their livelihoods. Thus, the factors of trust creation mentioned above, upon which value congruence has a positive effect through a more generous perception, heavily influence the way trust is created, mostly through the Characteristic Based Trust-creating mechanism. Furthermore, trust is facilitated through the congruence of values of consumers and organizations (Cazier et al., 2006).

Blockchain

The value of DLT, such as the blockchain, is the underlying process that validates blocks and

records them on the public ledger (Swan, 2015). Through a mechanism of consensus, each DLT and its supporting network use a protocol to make the inclusion of a new block intrinsically verifiable. In the case of the Proof-Of-Work (PoW) mechanism, solving a cryptographic puzzle requiring critical amounts of computer processing power grants a miner the right to add the next block to the chain (Nakamoto, 2008).

The public ledger is valuable for its transparency and integrity of transactions in the form of data stored within each block. On a public or permissionless ledger, all non-identifiable information related to a transaction within a block is viewable to any entity at any time. Moreover, information stored within a block is immutable as cryptographic hashes, integral components of the blockchain, and included within each transaction, providing blocks with an identity (Nakamoto, 2008).

As new blocks must include the prior blocks' cryptographic hash (e.g., a hash point), the blockchain can quickly identify ostensibly altered blocks. Since the nodes recognize a new block using the verifiability provided via the ledger-inherent consensus mechanism outlined above, any alteration disrupts the chain and disallows access. The consensus mechanism illustrates the value in being distributed as the community of nodes (e.g., miners in the PoW case) that are responsible for the blockchain's network as this community of nodes contributes to the verification of transactions within a block on the blockchain. Thus, to take control of the blockchain, a majority of nodes would be needed (i.e., 51 percent attack). By default, the decentralized architecture of the blockchain has enormous value as it manifests intrinsically verifiable information.

Indeed, the unique features of DLTs in general and the consensus mechanism-backed blockchain, in particular, may open a new era in the age of data analytics. First, the combination of cryptographic features, the consensus mechanism, and their decentralized nature ensures the integrity of data once they are stored on the blockchain, thus generating trust through intrinsically verifiable information. Second, data stored on the blockchain enables data analytics as data is available in a standardized manner. Third, data is easily tracked and shared across peers to facilitate analytics. Fourth, timestamps on each data entry on the blockchain allow the accurate visualization of the data history and near real-time analysis (Brooke, 2019). Rünzel et al. (2021) show how a blockchain traceability system could be built and the type of data that would be needed to be effective.

Data-Driven Beekeeping for Development

Beekeeping has been described as an ideal, accessible, and empowering opportunity for both men and women who are rural entrepreneurs in economically challenged areas (Mburu et al., 2015). Hence, development actors, governments, and farmers have embraced beekeeping as an alternative for livelihood diversification, particularly in rural areas (Mujuni et al., 2012; Ogaba and Akongo, 2001). Comparatively low labor requirements and start-up costs in combination with minimal land use are just some of beekeeping's competitive advantages for on-farm integration (Ogaba, 2002; Ndyomugyenyi et al., 2015; Gupta et al., 2014). Beyond stable year-round financial contributions that strengthen smallholder livelihoods, bee pollination benefits not only the beekeepers but also helps the farmers by increasing their yields. Providing more plentiful food in the region reduces hunger and helps alleviate poverty by reducing food costs in rural areas (Sacco et al., 2014).

The need for technological intervention has been recently summarized by Lietaer (2019): "Despite the favorable natural environment existing in almost all developing countries and the potential for building sustainable livelihoods in rural areas, beekeeping often lacks the necessary financial, extension, and technological support required to fully exploit its great potential in conserving forests and natural ecosystems and in reducing poverty." A significant development in unlocking this potential could be realized by sustainably-increasing honey production through technological, data-enabled solutions that improve beekeeping practices and bee health.

Honey Traceability

In line with coffee, chocolate, and wine, among others, honey is one of the most adulterated higher-value foods (Everstine et al., 2013). Methods of EMA - commonly referred to as food fraud - in the honey sector include diluting and extending honey, and transshipping (e.g., adulterating the origin of imports to avoid the payment of tariffs or even testing) (Strayer et al., 2014).

In the U.S. particularly, several aspects render the control of honey adulteration difficult. First, given its international market status, 75% of the honey supply is imported (Mathews et al., 2019). Second, as of today, there is no identity

standard for honey on the U.S. federal level, which slows down regulatory efforts that could verify honey safety and quality. Third, trade policies, such as free trade areas, lead to shared responsibilities weakening the control process. Fourth, indeed, analytical methods that may detect honey adulteration are - still - insufficient or too cost-intensive to be performed on a regular and scalable basis (Strayer et al., 2014).

Trust & Honey Traceability for Development

Having identified traceability as a critical solution to the problem of economically-motivated honey adulteration, verifiable traceability can help beekeepers as it tackles one of the emerging problems underpinning the honey business. Namely, honey adulteration and fraud are outpacing methods of detection and verification, further eroding consumer confidence. At the same time, this drives the growth of the emerging varietal and local honey markets. Smallholder producers - equipped with the right means to prove the origin and veracity of honey verifiably - may benefit significantly, both in the Global South and Global North.

Blockchain technology, product differentiation, and price premiums in the global honey market

While it is challenging to produce accurate data on the amounts of adulterated honey available, industry statistics help illustrate the size of the phenomenon. Notably, since 2007, honey exports have increased by 61 percent, while the number of beehives has increased by only approximately 8 percent (FAO, 2018).

One of the implications of this honey supply surge is deteriorating prices for international bulk import prices. As García (2018) states, honey purity is not guaranteed by a higher price. Low-priced honey, however, has a higher likelihood of being subject to adulteration. Hence, import prices serve as an indicator of the quality of honey and the need to perform further tests for quality, origin, and purity (García, 2016).

The European Union, the second-largest producer of honey worldwide and an important importer of honey, found in a recent study that 14 percent of the honey analyzed across all member states, including Norway and Switzerland, had been adulterated (Aries et al., 2016). The Canadian Food Inspection Agency even reported that 21.7 percent of the jars of honey tested showed the presence of added sugar (Canadian Food Inspection Agency, 2019). Moreover, lower prices and production costs, as well as illegal practices, affect beekeepers' income and are stated as a threat to European producers' market shares (Rossi, 2017).

To combat these problems, beekeepers across the European Union currently aim to evoke trust in their honey through 46 labels of Protected Designation of Origin (PDO) or Protected marketing advantages (Walley et al., 1999). Also, regional labels increase the Willingness To Pay (WTP) and attract consumers with higher incomes (Van Ittersum et al., 1999). Vecchio

Geographical Indication (PGI) (European Commission, 2019). Research shows that these labels add value to the product, including and Anunziata (2011) even show that these labels may be the primary purchasing motivation for people with a thorough knowledge of the labeling system.

Likewise, consumers pay price premiums for varietal types of honey. Data from Spain shows that honeydew honey's retail prices are, on average 27 percent higher than multifloral honey (European Commission, 2017).

	Impact of Fair Trade (ie. coffee)	Impact of Organic (bulk honey)	Impact of Varietals (ie. honeydew honey)	Impact of Geographical Labeling (ie. effect of PDOs adjusted for product specificity)
Price Premiums	10%-27%	7%	27%	21%

Sources: (De Pelsmacker et al., 2005; National Honey Board, 2019; European Commission, 2017; Deselnicu et al., 2013, from left to right)

Table 2. Potential Economic Value Added Through Price Premiums

Similarly, in the international market for wholesale bulk honey, a price premium of 7 percent is charged for organic honey (National Honey Board, 2019). Given an estimated global organic honey market size of $500 million in 2017, and assuming this increase in pricing is passed along to retail consumers, verifiable organic honey results in economic value creation of upwards of $35 million. The market for organic honey is projected to increase to $910 million by 2023, driving the economic impact even larger and creating opportunities for new players to benefit (Statista, 2017).

Research on price premiums related to fair trade coffee shows that consumers are willing to pay a 10 percent price premium on average, while supporters of the fair-trade program are willing to pay up to 27 percent more (De Pelsmacker et al., 2005). Moreover, Arnot et al. (2006) find that purchasers of fair trade-labeled coffee are less price-sensitive compared to their peers. The authors use a choice model to confirm earlier WTP studies' findings that consumers are willing to pay price premiums outside of stated preference studies' hypothetical settings.

Hence, consumers who can verify the integrity, quality, and origin of the honey they buy are willing to pay price premiums. Moreover, value congruence will further increase the price premium paid, as value congruent consumers may confirm overlapping values through origin and ethical production checks. The range of price premiums cited for the impact of fair-trade coffee illustrates the market potential for products driven by value congruent consumers. Potential price premiums for blockchain-enabled verifiable characteristics are provided in Table 2.

DLT-backed and data-driven beekeeping will allow smallholder beekeepers access to markets and price premiums from both standard and value congruent consumers. At the same time, intrinsically verifiable trust in the honey will alleviate pressure from adulterated honey and protect beekeepers' livelihoods. If the price premiums observed for fair trade coffee are similar for honey with verifiable integrity and quality from developing countries, price premiums between 10 percent to 27 percent would result in economic value creation of $91 to $246 million for the African smallholder honey economy alone, which amounts to 13% of the $7 billion global honey production market (Châtel, 2017; Statista, 2018). Beyond price premiums, however, DLT can allow new forms of product differentiation and has the potential to significantly decrease the transaction costs of assessing and certifying product characteristics, unlocking the potential to profoundly disrupt and transform how value can be created in the Global South.

4. CONCLUSION

Beekeeping has been acknowledged as a sustainable and low-investment strategy to alleviate poverty, providing rural populations with a stable income. The affordability and flexibility of beekeeping lowers the threshold to enter the beekeeping business even in remote areas. We contend that distributed ledger technology may prove to be the right technology to solve two pressing problems of emerging and established beekeeping industries, mitigating the deteriorating trust in honey product integrity and, at the same time, granting smallholder beekeepers access to markets.

Value congruence has the potential to radically alter our ability to influence others in sustainable ways through our purchase behaviors. However, this can only be realized through a system that includes data, analytics, and intrinsically verifiable trust, enabled through records on a distributed ledger. Taken together, this collection of technologies can build a precise traceability and authenticity system that shows the entire history and origin for each product. This can have a profound impact by setting up proper economic incentives to align with the values of consumers and decision makers, and drive product differentiation. Nascent distributed ledger technology is disrupting the way we perceive trust. Blockchain technology extends the boundaries of the traditional model of trust creation, paving the way for new forms of data analytics.

The nature of distributed ledger technologies, such as blockchain, allows for improved data integrity, as well as complete and open data in a secure and decentralized system. Within the use case of beekeeping, we have shown the potential for improved descriptive, diagnostic, predictive, and prescriptive analytics for hive management, helping beekeepers across the globe become more productive and resource-efficient. Enabling smallholder beekeepers backed by DLT-enabled data analytics and traceability to enhance their beekeeping operations and take part in the honey value chain would unlock the development potential of rural areas while strengthening the biodiversity and food supply, and contributing to several of the Sustainable Development Goals of the United Nations.

Future research could focus on the technical and operational side of implementing and testing a DLT-backed traceability system that supports beekeepers in rural areas, proving that development can be both economically viable and environmentally sustainable. Eventually, other value chains could follow to ensure smallholder producers have a stake in the value chain and access to value congruent consumers so that sustainable development reaches even the most rural areas.

While blockchain cannot guarantee that a product is not adulterated, it can decrease the likelihood. By tracing honey production in an unalterable way and connecting it with a labeling system, adulteration due to dilution, extension, and transshipment is reduced as the source and amount of honey produced are verified along the supply chain.

4. ACKNOWLEDGEMENTS

This work was funded in part by a Chancellor's Innovation Grant from Appalachian State University and a Flash Grant (#2019-FLG-3863) from the North Carolina Biotechnology Center.

5. REFERENCES

Aries, E., Burton, J., Carrasco, L., De Rudder, O. and Maquet, A. (2016). Scientific support to the implementation of a Coordinated Control Plan with a view to establishing the prevalence of fraudulent practices in the marketing of honey - Results of honey authenticity testing by liquid chromatography-isotope ratio mass spectrometry. *JRC Technical Reports*, European Commission.

Arnot, C., Boxall, P.C. and Cash, S.B., (2006). Do Ethical Consumers Care About Price? A Revealed Preference Analysis of Fair Trade Coffee Purchases. *Canadian Journal of Agricultural Economics*, 54:4, 555-565.

Barrett, H. R., Browne, A. W., Harris, P. J. C., and Cadoret, K. (2001). Smallholder farmers and organic certification: accessing the EU market from the developing world. *Biological Agriculture and Horticulture*. 19, 183-189.

Brooke, Sophia. (2019). How Will Blockchain Make Predictive Analytics Accessible? *Towards Data Science*. https://towardsdatascience.com/how-will-blockchain-make-predictive-analytics-accessible-d256d543081d. Accessed 2019-11-15.

Canadian Food Inspection Agency. (2019). Report: Enhanced honey authenticity surveillance (2018 to 2019). Retrieved Nov 15, 2019 from https://inspection.gc.ca/about-the-cfia/science/our-research-and-publications/report/eng/1557531883418/1557531883647.

Cazier, J.A., Shao, B.B.M., and St. Louis, R.D. (2006). E-Business differentiation through value-based trust. *Information and Management Science*. 43:6, 718-727.

Cazier, J. A. (2007). "A Framework and Guide for Understanding the Creation of Consumer Trust". *Journal of International Technology and Information Management*, 16(2), 45-56.

Cazier, J.A., Shao, B.B.M., and St. Louis, R.D. (2007). Sharing information and building trust through value congruence. *Information Systems Frontiers*. 9:5, 515–529.

Cazier, J.A., Shao, B.B.M., and St. Louis, R.D. (2017). Value Congruence, Trust, and Their Effects on Purchase Intention and Reservation Price. *ACM Transactions on Management Information Systems*. 8:4, 13.

Châtel, B. (2017). Honey Exports Take Off in Africa. *The Technical Centre for Agricultural and Rural Cooperation*. Retrieved Nov 5 from https://spore.cta.int/en/marketing/all/article/honey-exports-take-off-in-africa-sid077abaf13-7588-4cd3-9ae3-13c52b88ca57.

De Pelsmacker, P., Driesen, L. and Rayp, G. (2005). Do Consumers Care about Ethics? Willingness to Pay for Fair-Trade Coffee. *The Journal of Consumers Affairs*. 39:2, 363–86.

Deselnicu, O.C., Costanigro, M., Souza-Monteiro, D., and Thilmany, D. (2013). A Meta-Analysis of Geographical Indication Food Valuation Studies: What Drives the Premium for Origin-Based Labels? *Journal of Agricultural and Resource Economics*. 38:2, 204-21.

Elizur, D. and Sagie, A. (1999). Facets of personal values: A structural analysis of life and work values. *Applied Psychology*. 48:1, pp. 73-87.

European Commission. (2019). Agricultural Rural Development, DOOR. Retrieved Nov 15, 2019 from http://ec.europa.eu/agriculture/quality/door/list.html?&recordStart=0&filter.dossierNumber=&filter.comboName=&filterMin.milestone__mask=&filterMin.milestone=&filterMax.milestone__mask=&filterMax.milestone=&filter.country=&filter.category=PDOPGI_CLASS_14&filter.type=&filter.status=REGISTERED&locale=en&recordPerPage=50.

European Commision. (2017). EU Honeymarket Presentation. Retrieved Nov 15, 2019 from https://ec.europa.eu/agriculture/sites/agriculture/files/honey/market-presentation-honey_en.pdf.

Everstine, K., Spink, J., and Kennedy, S. (2013). Economically Motivated Adulteration (EMA) of Food: Common Characteristics of EMA Incidents. *Journal of Food Protection*. 76:4, 723-735.

Food and Agriculture Organization (FAO). (2018). Faostat. Retrieved Mar 13, 2019 from http://www.fao.org/faostat/en/#search/beehives.

García, N. (2016). A Study of the Causes of Falling Honey Prices in The International Honey Market. *Alberta Beekeepers Annual Meeting*.

García, N. (2018). The Current Situation on the International Honey Market. *Bee World*. 95:3. https://doi.org/10.1080/0005772x.2018.1483814.

Gutman, J. (1982). A means-end chain model based on consumer categorization process. *Journal of Marketing*. 46, 60-72.

Gupta, R.K., Reybroeck, W., van Veen, J.W., and Gupta, A. (2014). Beekeeping for poverty alleviation and livelihood security. New York: Springer.

Klein, A.-M., B.E. Vaissiere, J.H. Cane, I., and Steffan-Dewenter. (2007). Importance of pollinators in changing landscapes for world crops. *Proceedings of the Royal Society* B. 274, 303-313.

Lietaer, Charlotte. (2019). Impact of beekeeping on forest conservation, preservation of forest ecosystems and poverty reduction. Retrieved Nov 15, 2019 from https://www.researchgate.net/publication/238732690_Impact_of_beekeeping_on_forest_conservation_preservation_of_forest_ecosystems_and_poverty_reduction.

Mann, C. L. (2004). Information technologies and international development: Conceptual clarity in the search for commonality and diversity. *Information Technologies & International Development*. 1:2, 67–79.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review (AMR)*. 30:3, 709-734.

Mburu, P., Affognon, H., Irungu, P. Mburu, J., and Raina, S. (2015). Beekeeping for Women Empowerment: Case of Commercial Insect Programme in Kitui County, Kenya. Retrieved Mar 12, 2019 from https://doi.org/10.13140/RG.2.1.1452.4245.

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*. 62:1, 35-45. https://doi.org/10.1016/j.bushor.2018.08.012.

Mujuni, A., Natukunda, K., and Kugonza, D. (2012). Factors affecting the adoption of beekeeping and associated technologies in Bushenyi district, Western Uganda. *Livestock Research for Rural Development*. 24:08.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved Nov 15, 2019 from https://bitcoin.org/bitcoin.pdf.

National Honey Board. (2019). Retrieved Nov 15, 2019 from https://www.honey.com/honey-industry/statistics/international-bulk-prices.

Ndyomugyenyi, E., Odel, I., and Okeng, B. (2015). Assessing honey production value chain in Lira sub-county, Lira district, Northern Uganda. *Livestock Research for Rural Development*. 27:1.

Ogaba, M. R., and Akongo, T. (2001). Gender issues in Beekeeping - the Uganda case. *Apimondia Congress No. 37*. Durban, South Africa.

Ogaba, M. R. (2002). Household poverty reduction through beekeeping amongst Uganda rural women. Standing commission of beekeeping for rural development, Monmouth. *71st Honey show and exhibition*, Kensington, London.

Olnes, S., Ubacht, J., Janssen M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly.* 32:3.

Rossi, R. (2017). At a glance - The EU's beekeeping sector. *European Parliamentary Research Service (EPRS), Members' Research Service.*

Rünzel, M. A., Hassler, E. E., Rogers, R., Formato, G. and Cazier, J. A (2021). "Designing a Smart Honey Supply Chain for Sustainable Development," *IEEE Consumer Electronics Magazine*, doi: 10.1109/MCE.2021.3059955.

Sacco, S., Jones, A, and Sacco, R. (2014). Incorporating global sustainability in the business language curriculum. *Global Business Languages*. 19:1, 3.

Statista. (2018). Honey Market Worldwide and in the US. Retrieved Nov 15, 2019 from https://www.statista.com/topics/5090/honey-market-worldwide/.

Statista. (2017). Global Organic Honey Market Value. Retrieved Nov 15, 2019 from https://www.statista.com/statistics/933490/global-organic-honey-market-value/.

Strayer, S., Everstine, K., and Kennedy, S. (2014). Economically motivated adulteration of honey: Quality control vulnerabilities in the international Honey Market. *Food Protection Trends*. 34:1, 8-14.

Swan, M. 2015. Blockchain: Blueprint for a new economy.O'Reilly Media, Inc.

United Nations Development Programme. (2012). Sustainable Development Goals - Background. Retrieved Nov 15, 2019 from https://www.undp.org/content/undp/en/home/sustainable-development-goals/background.html.

Van Ittersum, K., Candel, M. and Torelli, F. (1999). The Socio-Economics of Origin Labelled Products: Spatial, Institutional and Co-Ordination Aspects. *The Socio-Economics of Origin Labelled Products: Spatial, Institutional and Co-Ordination Aspects*, edited by B. Sylvander, D. Barjolle, and F. Arfini, 210–21. Le Mans, France.

Vecchio, R., and Annunziata, A. (2011). The Role of PDO/PGI Labelling in Italian Consumers' Food Choices. *Agricultural Economics Review*. 12:2, 80–98.

Vermeir, I., and Verbeke, W. (2006). Sustainable Food Consumption: Exploring the Consumer "Attitude - Behavioral Intention" Gap. *Agric Environ Ethics*. 19-169. https://doi.org/10.1007/s10806-005-5485-3

Walley, K. Parsons, S. and Bland, M. (1999). Quality Assurance and the Consumer: A Conjoint Study. *British Food Journal*. 101:2, 148-161.

Zhao, Y., Zhao, D., and Liu, M. (2012). Research on online consumer building trust and sharing information through value congruence. *International Journal of Networking & Virtual Organizations*. 11:3/4, 277-289.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure 1840-1920. *Research in Organizational Behavior (ROB)*. 8, 53-111

Combating Private Blockchain Fraud: A Virtual Reality & Artificial Intelligence Model

Ehi E. Aimiuwu
eeaimiuwu@campbellsville.edu
Information Technology Management
Campbellsville University,

Abstract

One of the problems hindering the adoption of blockchain today is that managers are insecure about financial security. Business secrets being stolen by competitors in both public blockchain and private blockchain discourages public participation and data transparency, which managers control, and can lead to fraud if management manipulates transaction data for individual gain (Wang & Kogan, 2018). The aim of this literature review is to propose a Virtual Reality (VR) and Artificial Intelligence (AI) model, which can be used to combat private blockchain fraud without compromising confidentiality and transparency. Research shows that VR platforms that use blockchain technology have been instrumental in the music, gaming, hotel, copyright, and property industries. Also, AI is helpful in analyzing huge data in real time and using Machine Learning (ML) logic from expert systems to prevent fraud through clustering, classification, nearest-neighborhood, and statistical methods. Data mining techniques, like class imbalance, the Bayes Network, and forest tree are also useful for upgrading private blockchain technology with AI protocols within the protocol level in order to capture the digital location of the fraudsters in real time for VR verification later. This should discourage private blockchain managers from fraud and enable private blockchain to become more trustworthy for the general public, because confidentiality is compromised by VR only to identify fraudulent private blockchain managers.

Keywords: Artificial intelligence, Blockchain, Fraud, Hybrid Intelligence, Security, Virtual Reality

1. INTRODUCTION

Many Fortune 500 firms are moving towards the use of blockchain for their business transactions to ensure audit security and to increase their revenue (Mofokeng & Matima, 2018). The three types of blockchain are: public blockchains, which are open for anybody to use and develop (Bitcoin and Ethereum); private blockchains, which are developed and controlled by approved entities (Ripple and Hyperledger); and consortium blockchains, which are owned and used by partner firms (R3 Bank and EWF Energy) (French, Risius, & Shim, 2020). The purpose of blockchain is to reduce the cost of protecting information integrity, data confidentiality, and verifiability of financial transactions in order to build trust (Wang & Kogan, 2018; Beck et al., 2017). One of the big issues in business ecosystems today is the issue of cooperation versus competition when it comes to information sharing and data communication to improve the efficiency of trading, because, while information transparency increases, it will also lead to an increase in compromising both business secrets and data confidentiality (Wang & Kogan, 2018; Beck et al., 2017). For business to operate efficiently, there must be public availability of data to allow cooperation, but at the same time, confidentiality to keep transactions private and prevent competitors from taking advantage of patents or sensitive strategic information.

Blockchain is an open and public shared system that records transactions and prevents data tampering, and the transactions are usually irreversible or immutable, so a marketplace is attained to allow peer-to-peer transfer of assets without central control or central authority in financial sectors, as well as in many industries, and may change how goods are paid for in the real world (Rossi et al., 2019; Wang & Kogan, 2018; Beck et al., 2017; Nofer et al., 2017). For blockchain to achieve the sort of trust and credibility expected by these industries, it needs to have protocols that govern how transactions are carried out within the consensus mechanism of each peer-to-peer network. Blockchain protocols are rules that guide human agents' rights to validate, read, and submit transactions, but human agents govern the protocol and the protocol governs how they interact (Rossi et al., 2019), as shown in Figure 1 in the appendix.

Each block in a blockchain has a time stamp, hash (value of the previous block), and nonce (to verify the hash), which helps prevent fraud. Whenever the hash value changes in a block sequence, it is because blocks are only added to the sequence after the block meets the validity of the consensus mechanism within the network (Nofer et al., 2017). This means that if a fraudster tries to change the time stamp or hash on a blockchain transaction, the nonce will become incompatible within the sequence. So the blockchain needs to have the time stamp, hash, and nonce on each block protected to prevent contamination or fraud within the chain.

Zero-knowledge proof (ZKP), which is a cryptographic method for protecting blockchain data confidentiality, can allow a valid transaction after proof is verified, without providing any sensitive information such as name or transaction amount, and homomorphic encryption, which uses mathematical algorithms to ensure that sensitive data is encrypted, with the goal of preventing fraud, monitoring transactions, providing real time accounting, and protecting confidentiality (Wang & Kogan, 2018). Encryption is an excellent way to prevent fraud or data tampering, but unfortunately, some private data are still being understood by the public or competitors. Bitcoin blockchain uses cryptography, but it is vulnerable to private attacks because it contains personal information and transactional information that can be deciphered, while Ethereum blockchain uses smart contracts cryptography that allows predefined agreements in real time in a decentralized network (Rossi et al., 2019; Wang & Kogan, 2018; Nofer et al., 2017), and smart contracts are treated as first-class citizens, as well as being used to control ownership of property, such as houses, cars, shares, and access rights (Nofer et al., 2017). In the United States, it was possible to track and identify the fraudsters involved, as well as recover the majority of the 4.4 million of the Bitcoin Blockchain or cryptocurrency ransom that was paid for the Costal Pipeline shutdown in May 2021. Blockchain will not just replace how we pay for goods or conduct transactions, but will also be used to control the ownership of both tangible and intangible assets that may be passed down to the next generation as inheritance.

Despite some research on blockchain and VR, as well as blockchain and AI, there has been little research done to include AI protocols within the blockchain protocol level in order to identify the digital location of a fraudster for further VR investigation. This literature review will show that private blockchain fraud by managers can be prevented and identified with the use of AI within the blockchain protocol level for further verification through the VR platform. In the rest of the paper, a literature review of both VR and AI will be presented. The relationship model, methodology, results, as well as a discussion, will follow. Finally, the limitations of the study as well as the conclusion and future research will be discussed.

2. LITERATURE REVIEW

Virtual Reality

VR is a hardware and software system that has the unique ability to make the user have telepresence while being immersed and interacting in a different environment (Mutterlein, 2018). The purpose of VR is to use the available technology of integrated devices through the user's five natural senses to give the user a multisensory experience of being close to a different and realistic reality, which allows the user to modify their perception of the world, and facilitate the capacity to transmit, store, and share information in a timely fashion (Pinto et al., 2019; Carlson & Caporuso, 2018). If AI is incorporated into a private blockchain protocol level, it can detect and register the digital location of a fraud as soon as the AI detects any attempted illegality in any blockchain transaction. This illegal blockchain transaction could be a modification of a time stamp, hash, or nonce on a block, or an unusual attempt by private blockchain managers to decipher a competitor's personal or transactional

information. Only when a fraudster tries to breach the confidentiality of the private blockchain does his or her confidentiality become exposed by VR through digital cameras located near the fraud scene.

Three-dimensional (3D) GIS is a VR that allows interaction, visualization, navigation, and accurate analysis of urban and underground infrastructure to enable timely decision making on geospatial and spatial data for direct integrating of 3D graphics into web pages in the fields of telecom, transportation, the urban, environment, and agriculture (Jurado et al., 2017). The 3D GIS seems to be more realistic because of its in-depth representation and adequate visualization, which leads to the creation of 3D scenarios with overlapping spatial datasets, such as measurements beside trees, hills, and buildings (Jurado et al., 2017; Carlson & Caporuso, 2018). VR is used by many United States agencies, such as the Centre for Disease Control and Prevention, the Department of Homeland Security, and police departments, to assist emergency responses and multi-agency collaboration because of its advancements in motion capture technology, as well as zero-latency cameras that enable physically immersed virtual reality (Carlson & Caporuso, 2018). Regardless of where the fraudster is located, VR can capture all of the activity from any digital video, audio, and image of the exact location of the fraudster.

The three main features in VR are telepresence, immersion, and interactivity, where telepresence is a subjective experience at a location, but is physically in another location with the aid of a medium; immersion is a psychological state of mind or an optimal experience where the user is totally absorbed in an activity in the medium; interactivity is the psychological state of mind or the degree to which a user is able to manipulate the content of the medium; and satisfaction is the user's feeling about an experience with a product or service (Mutterlein, 2018). Interactivity strongly impacts both telepresence and immersion, telepresence strongly affects immersion, while immersion directly influences satisfaction (Mutterlein, 2018), as shown in Figure 2 in the appendix. Past research showed that a user felt more telepresence and satisfaction when VR was used for learning than just using audio because they felt more spatial presence and involvement, and experienced realism (Pinto et al., 2019). VR will be a great tool to apprehend and discourage fraudsters in private blockchain transactions because his or her fraudulent activities will clearly be documented in real time, as this will be done on digital cameras, and the fraudster will have to face the consequences, based on the negotiated and affirmed penalty by the consensus mechanism within the blockchain network. Private Blockchain should have very strict penalties for blockchain managers who try to commit fraud. Blockchain managers should be trained in the efficiency of VR platforms in revealing their identity.

There are many VR platforms that already use blockchain ledgers for financial and business transactions. Decentraland is used to manage property rights, VibeHub and Cappasity provide online events and 3D content with copyright protection, Matryx provides 3D problems for problem solvers to win a bounty, and many other VR platforms are helping developers to create industry standards that use blockchain for storage of digital assets (French, Risius, & Shim, 2020). CEEK is a firm that allows users to attend concerts that are sold out, Marriott Hotels use a "4D VR" campaign to give customers future resort experiences, while CryptoCars is a gaming multimedia platform that allows a car racing experience on a racetrack using blockchain technology (Mofokeng & Matima, 2018). Any of these VR platforms can be used to verify fraud after the fraud has being recorded by digital cameras located around the fraud scene.

Artificial Intelligence

AI involves systems of techniques, tools, and algorithms that have the capability to think and learn, as well as improve work quality, which includes natural language processing (analyzing human language), machine learning (algorithms for learning), and machine vision (algorithms for image analysis) (Jarrahi, 2018). AI is able to learn from past experiences and data in order to develop intelligent solutions, can learn to enhance itself for knowledge-based tasks, and is able to make analytical decisions, while humans are excellent for intuitive decision making (Jarrahi, 2018). As long as AI is incorporated within the design of the private blockchain protocol level, AI has the learned logic and analytical ability to detect fraud proactively and in a predictive manner. AI can also instruct the transaction of the fraudster to fail, be terminated, or end as an incomplete transaction, but make the fraudster believe it was successful, so the fraudster is not alarmed and escapes too quickly.

The analytical approach of AI requires analysis of knowledge based on both conscious reasoning

and logical deliberation, but it is lacking in understanding common-sense and unpredictable situations, while the human intuitive approach is based on gut feeling, past experiences, and business instinct, but has the edge of creativity and imagination in decision making (Jarrahi, 2018). It is usually better to merge the potential of AI to analyze huge amounts of data in real time with the higher human intuition and insight for judgement, which is also known as hybrid intelligence (HI) (Jarrahi, 2018; Dellermann et al., 2019), as shown in Figure 3 in the appendix.

AI helps to enhance human decisions by providing predictions, while humans assist AI in learning updated machine learning models, so HI enables humans to benefit from the predictive ability of AI, and humans then use their intuition, creativity, and imagination to make decisions based on AI's prediction without bias (Dellermann et al., 2019). Human agents should use experiences and intuition to provide possible fraud models and fraud logic for AI, so that AI can learn and understand how to detect fraud proactively. AI can also recommend judgment for the fraudster based on the consensus mechanism of the peer-to-peer network, while terminating the fraudster's activity without alerting the fraudster of any wrongdoing, and HI may even contact the nearest police station or fraud prevention agency (FPA) in real time.

An expert system is a form of AI or a computerized HI that needs to imitate human expert behavior by acquiring and utilizing human expertise as both data and production rules in a computer program that can be used to resolve very complex problems (Nissan, 2017; Campbell 2020). Expert systems of people who have solved financial blockchain frauds in the past can also be used in AI to predict and analyze fraud before it takes place. Expert systems can also decide to terminate a transaction without warning, but HI should alert the nearest FPA in real time.

AI is used regularly around the world because it has tools for visualizing incidents, case-based reasoning, abductive reasoning for objective judgement, as well as biometrics to identify individuals based on their physiology or behavior, and can verify or authenticate an identity (Nissan, 2017). Case-based or data-reliant reasoning uses past cases, abductive reasoning or rules-based reasoning uses logic and theory to solve problems (Nissan, 2017; Campbell, 2020), and biometrics identifies individuals based on their physiological or behavioral qualities, which can verify an identity or authenticate the identity in question (Nissan, 2017). AI can use old blockchain fraud strategies to predict new fraud strategies, and it can use rules and logic to detect new blockchain fraud strategies, as well as biometrics to verify and authenticate fraudsters with the help of VR.

AI has been used to detect blockchain fraud through machine learning (ML) nomenclature with methods such as classification, which differentiates objects in normal classes from anomalous classes; clustering, which labels classes based on similarities; nearest-neighborhood, which has normal instances in crowded neighborhoods and anomalies in sparse areas; and statistical, which focuses on outliers within the normal instances or classes (Monamo, Marivate, & Twala, 2016; Sabry, Labda, Erbad, & Malluhi, 2020). Other methods, such as kd-trees and k-means, are used in clustering and nearest-neighborhood to further investigate the likelihood of fraud through the Random Forest method to find the maximum top 1% situations (Monamo, Marivate, & Twala, 2016). The two most common types of fraud activities in blockchain are record hacking, due to slowness in the peer-to-peer network, and double spending, which is making many transactions with the same coin due to the delay in payment notification within the network (Rahouti, Xiong, & Ghani, 2018; Sabry, Labda, Erbad, & Malluhi, 2020). These methods of using tested AI models for fraud detection are valuable for preventing fraud, and, with the aid of the VR platform, can be a worthwhile HI strategy for identifying a fraudster for arrest.

AI also has a data mining approach to preventing blockchain fraud. Datasets are used to experiment with many ML models with regards to their efficiency, through both validation protocol and performance metrics to detect class imbalance, where the anomalous class is extremely rare compared to other classes. Classifier issues, such as RIPPER, rely on sequential logic to extract classification rules; the Bayes Network is a probability model in a graph form based on set conditions; Random Forest uses various decision trees from many variants of the same data; and other performance issues are addressed in regards to accuracy, specificity, and sensitivity (Bartoletti, Pes, & Serusi, 2018). There are many ways that AI within the blockchain protocol level can help to prevent the success of any fraud and use VR to identify the fraudster.

3. RELATIONSHIP MODEL

Despite the concerns of privacy with VR and bias with some historical data in AI, this literature review shows how both VR and AI are effective tools against blockchain fraud by private blockchain managers. The model in Figure 4 in the appendix shows AI incorporated in the private blockchain protocol level design between the human agents and the blockchain protocol interaction. Aside from the human agents deciding how the private blockchain protocol will govern their blockchain transactions, they also have to decide how AI will be used to maintain and enforce the blockchain protocol in order to resolve issues of conflicts and fraud among human agents.

AI within the private blockchain protocol could be used to observe any human agent whenever AI detects fraudulent activity; detect and prevent conflicts whenever the time stamp, hash, or nonce of a block is being tampered with; detect and terminate fraud as soon as activity matches past strategies or new logical fraud models; and suggest a resolution for the activity, which includes calling the police and providing the FPA with the digital coordinates of the fraudster.

4. METHODOLOGY

This study was based solely on a literature review. Google Scholar was used to search for related articles, and keywords such as "Artificial Intelligence Bitcoin Fraud," "Artificial Intelligence Blockchain Fraud," "Artificial Intelligence Fraud," "Virtual Reality Bitcoin Fraud," "Virtual Reality Blockchain Fraud," and "Virtual Reality Fraud" were used. In the study, 26 articles that addressed the issues of blockchain, VR, and AI were selected, but only 17 of the articles were useful for the study. There were four articles on blockchain which helped to understand what blockchain was all about and to find issues with blockchain that needed to be resolved. One of the issues was preventing private blockchain managers from manipulating blockchain transactional data for personal gain. Six VR articles were reviewed and one of them was about how VR is used in law enforcement. Seven articles about AI were reviewed and three of the articles were about how law enforcement uses AI.

The goal of this study is to propose a VR and AI model to show how VR and AI can be used to combat private blockchain fraud, especially by blockchain managers. In future, AI applications should be included in private blockchain protocols, so that AI can detect any fraudulent activity, and digital cameras within the vicinity of the attempted fraud can be manipulated by VR for verification. AI can abort the transaction and recommend HI to alert law enforcement. This should discourage both private blockchain employees and customers from fraud because their own digital devices may be a witness against them in court.

5. RESULTS

In this literature review, we discovered that many Fortune 500 firms, such as IBM, MasterCard, and Amazon, are now using blockchain technology to conduct their business, and see it as an avenue to reach a new or different customer base to increase their profits. Many businesses have developed various 3D and 4D VR platforms to reach unique customers to try their business experience through a different medium and to keep their finances private through blockchain.

VR is able to give users a customer experience that makes them feel they are actually in a certain location and achieving the same or similar experience as if they were actually there. Users can see objects, hear the sounds, and sense the smells or taste in real time while in a different location entirely. AI models that many businesses already use to detect fraud can use clustering, classification, nearest-neighborhood, and statistical methods to detect attempted fraud in order to stop it or prevent it from happening. Data mining techniques such as class imbalance, the Bayes Network, and forest tree are also very efficient.

This means that strategically including AI within the blockchain protocol level and using VR platforms can help blockchain firms and law enforcement to identify any fraudster once the AI methods have detected the fraud. The fraud will not only be terminated or be unsuccessful, but fraudsters can be made to believe that it was successful, so that there is no panic to escape quickly. Private Blockchain managers will have no other choice than to make honesty and integrity a must in their career. VR and AI together will be an effective blockchain fraud prevention in the future.

6. DISCUSSION

The results of this literature review suggest that future blockchain ecosystems would benefit from the integration of AI at the protocol level in

order to prevent fraud and to enhance both the transparency and confidentiality of blockchain transaction data, which is presented in Figure 5 in the appendix, as follows:

Stage 1 is Satisfaction: Blockchain managers and FPA are satisfied that the VR in the blockchain protocol provided all the videos, audios, and pictures required to make an accurate judgement of the incident, and that the AI in the private blockchain protocol accurately analyzed the incident; the best and most consistent decision to terminate the transaction was made; HI notified the FPA about the current identity and location of the fraud; and a complete resolution or judgement for the fraudster was recommended.

Stage 2 is Interactivity: Blockchain managers and FPA can use VR to retrieve all digital videos, audios, and graphics from building, street, car and mobile cameras; audios from digital speakers and microphones (Google Assistant, Apple's Siri, and Amazon's Alexa), as well as pictures about the location of fraud from all angles and directions.

Stage 3 is Telepresence: Blockchain managers and FPA can use VR to be present at the fraud scene, despite not being present in the physical world, or when they were present, but need verification as to what was observed and heard in order to avoid any form of bias.

Stage 4 is Immersion: Blockchain managers and FPA are completely absorbed in the combined effect of both interactivity and telepresence, which gives them the perfect opportunity to match their VR experience with what was detected, analyzed, and implemented by AI, in order to come to a credible conclusion as to whether a fraud occurred or not. The how, where, when, and what happened is clearly understood, as well as why AI detected or concluded that fraud was taking place.

Stage 5 is Uncertainty: This is where blockchain managers are in full control of the AI aspect of the protocol. They have to ensure that AI has the current fraud models, expert systems, rules, and theories needed to analyze various fraud situations and arrive at acceptable decisions or judgments in real time.

Stage 6 is Complexity: This is where blockchain managers have to test and decide if the current fraud models, expert systems, rules, and theories needed by AI to analyze various fraud situations and arrive at the acceptable decisions or judgments in real time are adequate.

Stage 7 is Equivocality: This is where AI uses biometrics to verify or authenticate the fraudster. Then, a case-based or data reliant reasoning is used to find exact or similar frauds in the past and recommend the best decision. If a past or similar fraud is not found, abductive or rules-based reasoning is used to include theory and rules based on expert systems that rely on the best decision or behavioral pattern of FPA.

7. LIMITATIONS

This study could have been a qualitative study with the use of expert interviews to validate the ideas in this paper, but instead, a literature review was used to generate ideas for future research. From the literature review, it was clear that maintaining data confidentiality and transparency was a requirement for private blockchain to be trusted by the public as an acceptable form of currency, so this paper attempts to address those issues with the aid of both VR and AI.

Triangulation could have been done to see if private blockchain managers already have AI in their blockchain protocol levels and the policies that govern them, but there is very little research on them in regards to blockchain, especially on AI and VR being used together. Also, the possibility and levels of integrating AI into the private blockchain protocol level was not investigated in this study, but it is believed to be possible to incorporate programs or codes within a protocol to achieve this technologically.

Lastly, the fraudster may commit a fraud in either a secluded or a public place and may even be using a stolen device that cannot be traced, so VR and AI using exact Global Positioning System (GPS) coordinates of fraud location in real time maybe a much preferred method to prevent fraud, rather than relying on a fraudster's mobile information or address.

8. CONCLUSION & FUTURE RESEARCH

The combined use of VR and AI to enhance confidentiality and transparency in private blockchain transaction data is possible if AI is integrated into the protocol level. Confidentiality of all human agents will be maintained at all times in private blockchain unless a potential fraud is detected proactively by AI, which then records the digital coordinates, and VR is used to capture the actual identity of the fraudster.

While the VR captures the identity of the fraudster during the fraud activity (from pre-recorded digital cameras), the AI eventually terminates the transaction, and the HI notifies the FPA immediately in real time about the GPS location coordinates, the fraud activity, and the identity of the fraudster. Also, AI can use expert systems or the computerized HI of human fraud prevention and detection experts as learning models to detect, predict, and analyze if a fraud is about to take place and what type of fraud is occurring.

HI is a form of AI that allows both humans and AI to work together. Private blockchain managers can always update the fraud learning models for the AI based on their experience and business acumen, and AI, in return, provides private blockchain managers and human agents analytical and predictive services in order to detect and prevent fraud.

For future research, we need to know the best way to incorporate AI into the blockchain protocol and how well AI models can help to prevent fraud by terminating fraudulent transactions in real time. Also, we need to know if AI within the blockchain protocol can target the exact GPS coordinates of fraudsters and help to notify both law enforcement and FPA in real time.

We also need to investigate the possibilities of using AI within the blockchain protocol to interact with VR platforms that are based on blockchain technology that could also be linked to digital cameras in cars, buildings, and smartphones. This will allow VR platforms to display fraudsters in any location directly from any digital camera as soon as AI detects any fraud in progress; so we do not need to wait for VR verification later.

9. REFERENCES

Abu-Nasser, B. (2017). Medical expert systems Survey. *International Journal of Engineering and Information Systems (IJEAIS*), *1*(7), 218-224.

Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting bitcoin ponzi schemes. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE. 75-84.

Beck, R., Avital, M., Rossi, M., & Thatcher, J.B. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering*, *59*(6), 381-384.

Campbell, R.W. (2020). Artificial Intelligence in the Courtroom: The Delivery of Justice in the Age of Machine Learning. Colo. Tech. LJ, (18), 323-350.

Carlson, G., & Caporusso, N. (2018). A physically immersive platform for training emergency responders and law enforcement officers. *International Conference on Applied Human Factors and Ergonomics*, Springer, Cham, 108-116.

Dellermann, D., Ebel, P., Söllner, M., & Leimeister, J.M. (2019). Hybrid intelligence. *Business & Information Systems Engineering, 61*(5), 637-643.

French, A. M., Risius, M., & Shim, J. P. (2020). The interaction of virtual reality, blockchain, and 5G new radio: disrupting business and society. *Communications of the Association for Information Systems*, *46*(25), 603-618.

Jarrahi, M.H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577-586.

Jurado, J.M., Graciano, A., Ortega, L., & Feito, F.R. (2017). Web-based GIS application for real-time interaction of underground infrastructure through virtual reality. *Proceedings of the 25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 1-4.

Mofokeng, N. E. M., & Matima, T. K. (2018). Future tourism trends: Virtual reality based tourism utilizing distributed ledger technologies. African *Journal of Hospitality, Tourism and Leisure*, *7*(3), 1-14.

Monamo, P. M., Marivate, V., & Twala, B. (2016). A multifaceted approach to Bitcoin fraud detection: Global and local outliers. In *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)* IEEE. 188-194.

Mütterlein, J. (2018). The three pillars of virtual

reality? Investigating the roles of immersion, presence, and interactivity. *Proceedings of the 51st Hawaii international conference on system sciences*.

Nissan, E. (2017). Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement. *Ai & Society*, *32*(3), 441-464.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.

Pinto, D., Peixoto, B., Krassmann, A., Melo, M., Cabral, L., & Bessa, M. (2019). Virtual reality in education: Learning a foreign language. *World Conference on Information Systems and Technologies*, Springer, Cham, 589-597

Rahouti, M., Xiong, K., & Ghani, N. (2018). Bitcoin concepts, threats, and machine-learning security solutions. IEEE Access, (6), 67189-67205.

Rossi, M., Mueller-Bloch, C., Thatcher, J.B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, *20*(9), 1-13.

Sabry, F., Labda, W., Erbad, A., & Malluhi, Q. (2020). Cryptocurrencies and Artificial Intelligence: Challenges and Opportunities. *IEEE Access*, (8), 175840-175858.

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, (30), 1-18.

APPENDIX

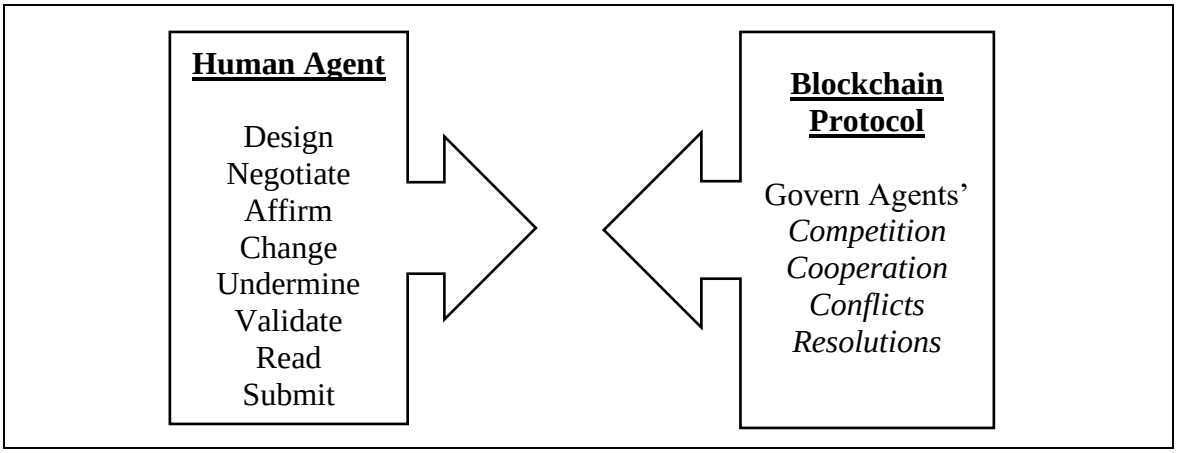

Fig. 1. Blockchain Protocol Level

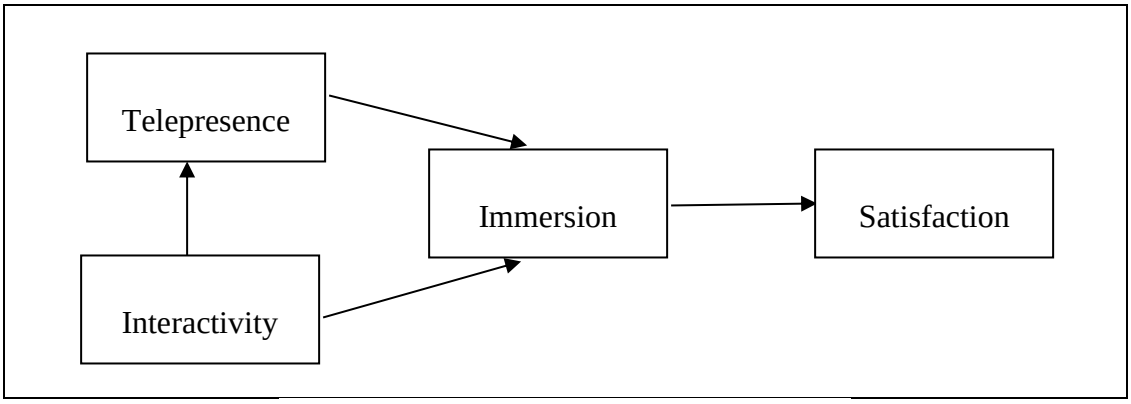

Fig. 2. Three Features of Virtual Reality (Mutterlein, 2018)

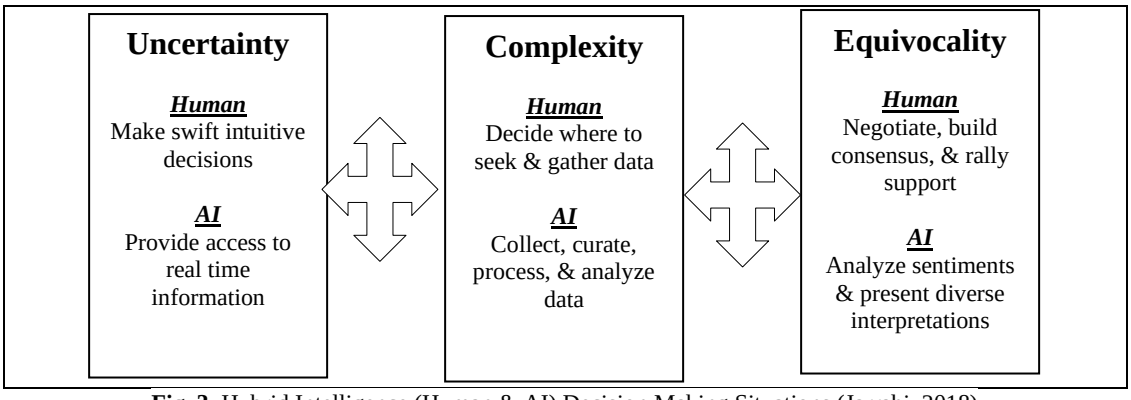

Fig. 3. Hybrid Intelligence (Human & AI) Decision Making Situations (Jarrahi, 2018)

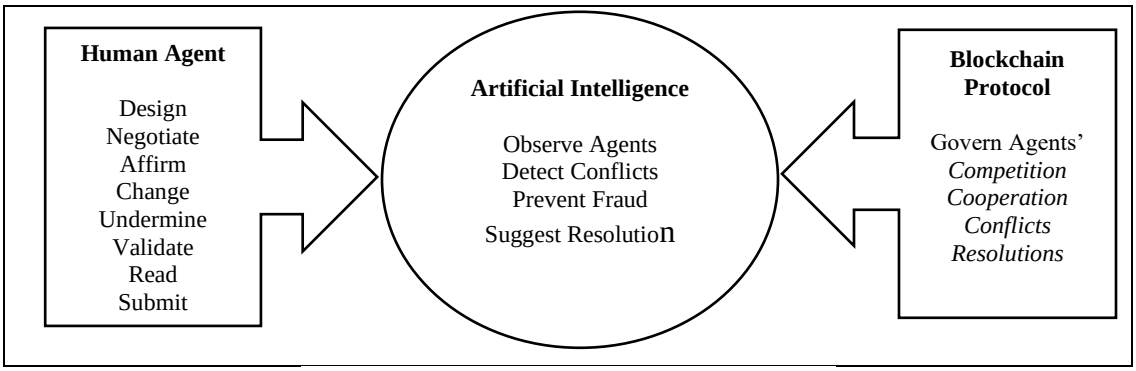

Fig. 4. AI within the Private Blockchain Protocol Level

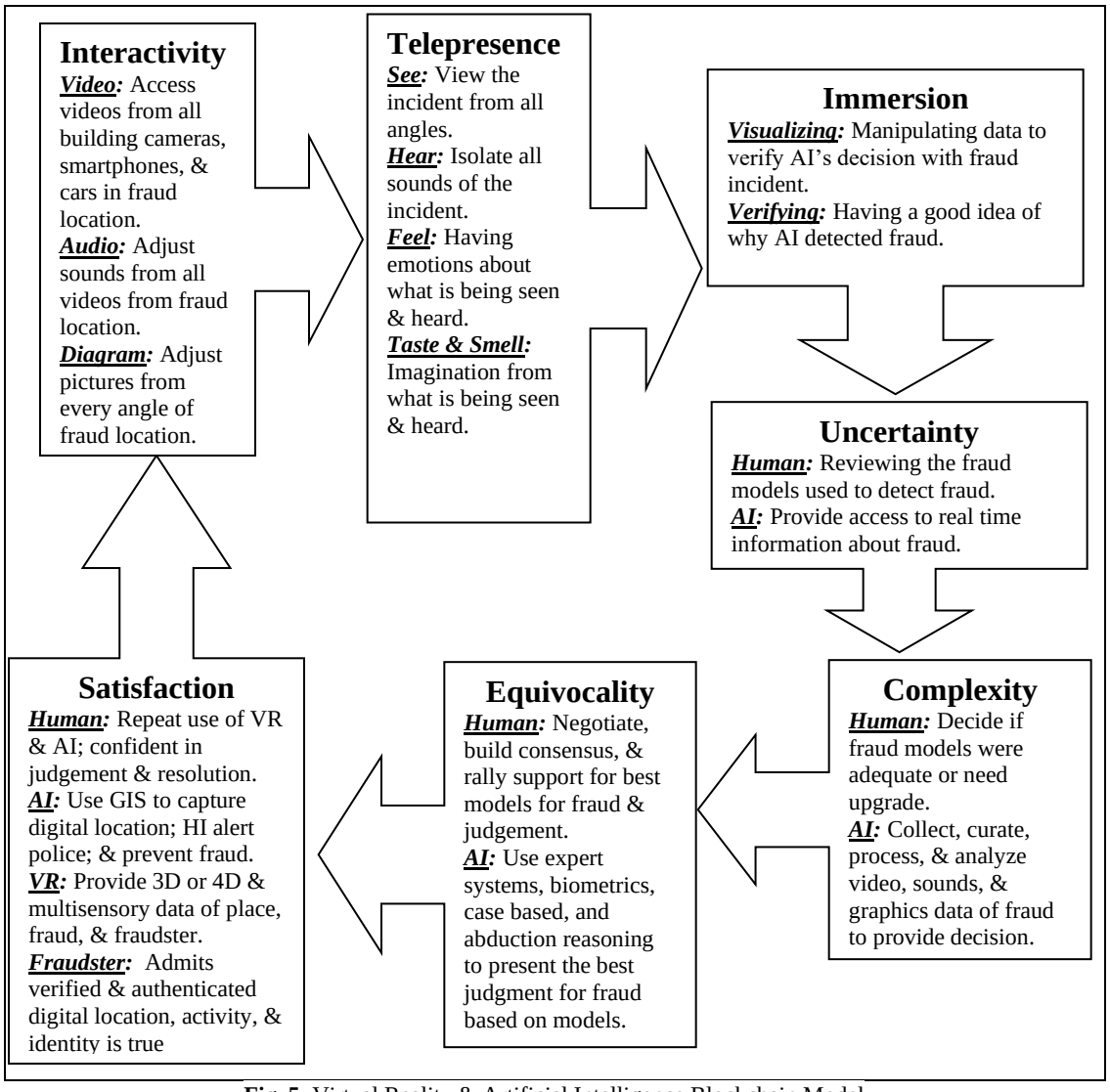

Fig. 5. Virtual Reality & Artificial Intelligence Blockchain Model