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.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

2022 JISAR Editorial Board

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

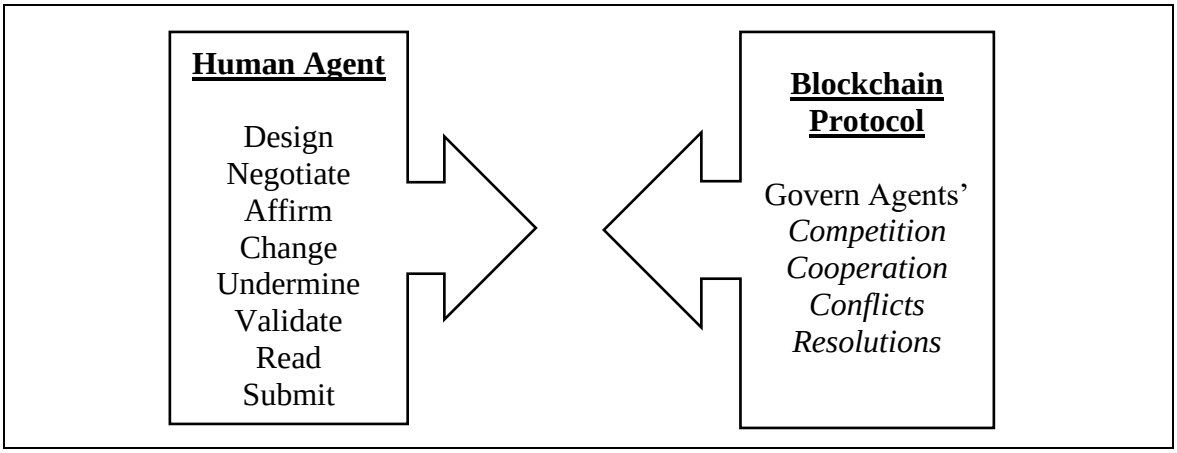

Fig. 1. Blockchain Protocol Level

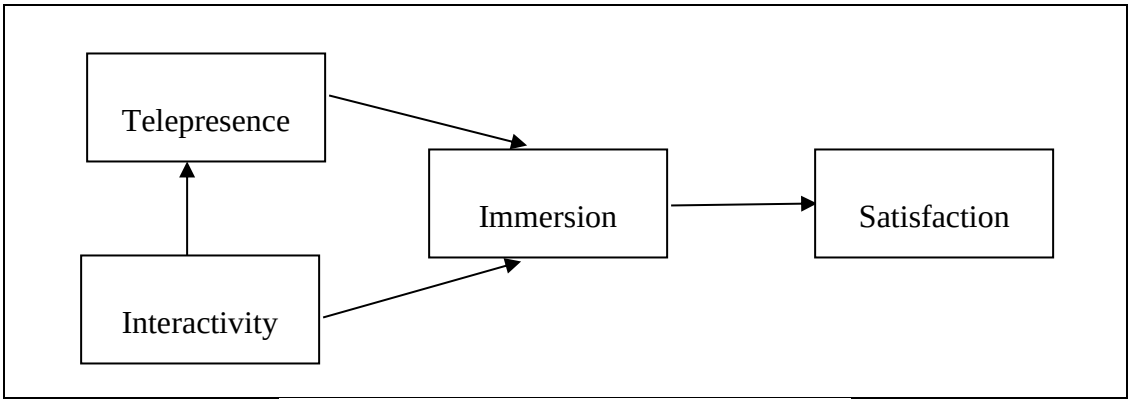

Fig. 2. Three Features of Virtual Reality (Mutterlein, 2018)

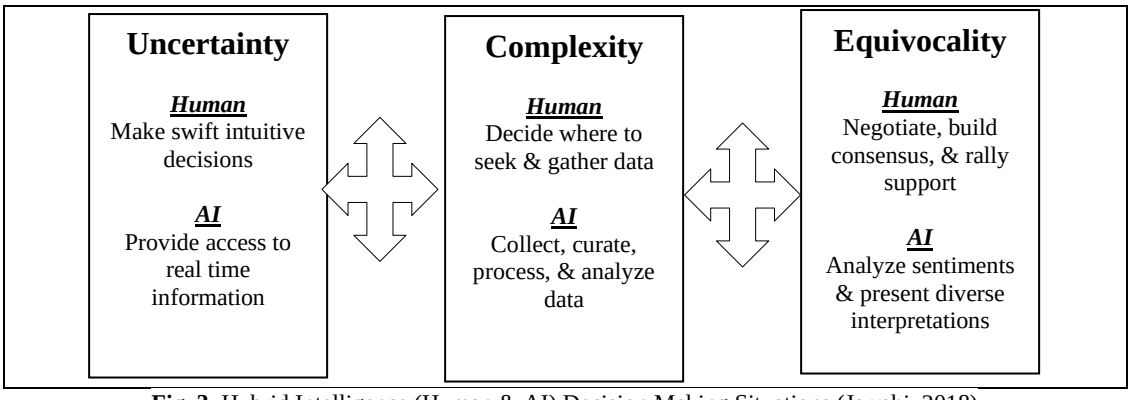

Fig. 3. Hybrid Intelligence (Human & AI) Decision Making Situations (Jarrahi, 2018)

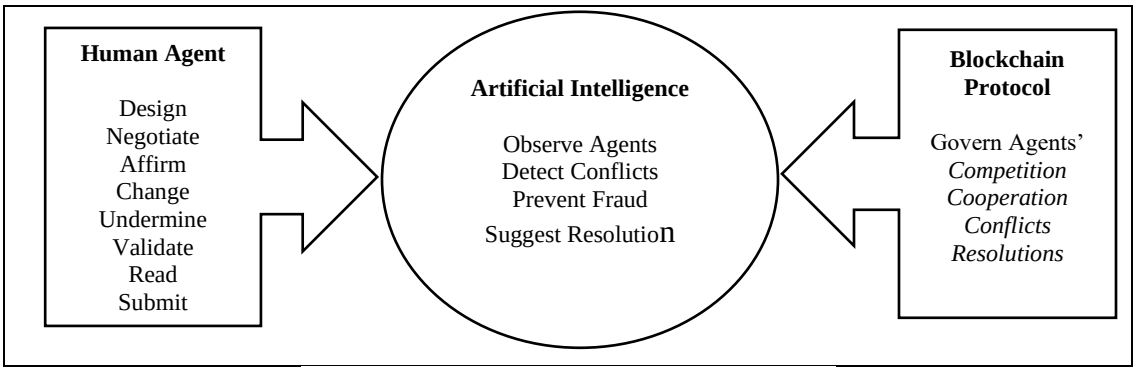

Fig. 4. AI within the Private Blockchain Protocol Level

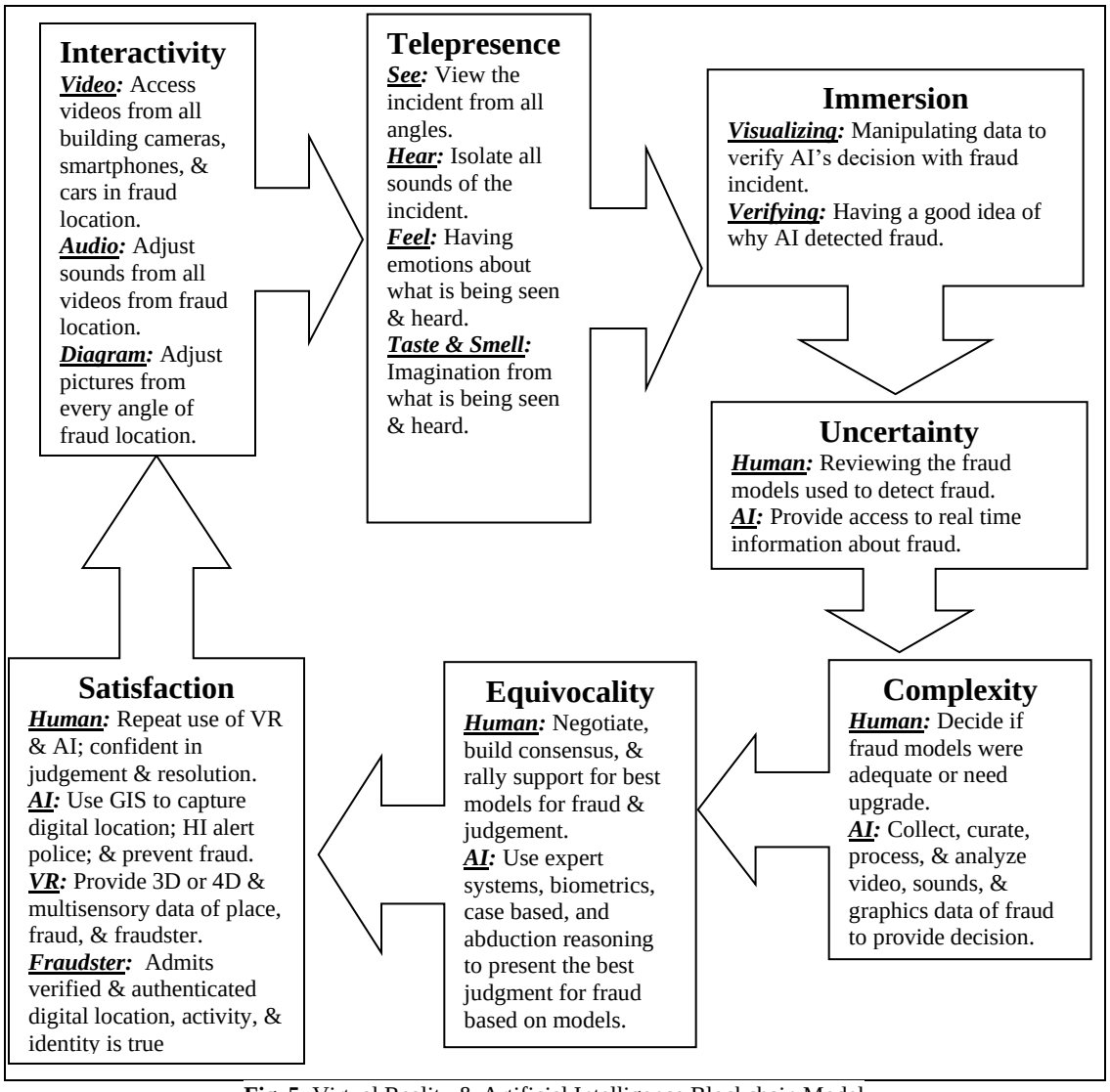

Fig. 5. Virtual Reality & Artificial Intelligence Blockchain Model