ISSN No:-2456-2165

How Blockchain can be used for Digitization of Human Consciousness

Alastair Smith
MS in Artificial Intelligence, Northwestern University
New York, United States

Abstract:- This article presents empirical evidence collected from experts and professionals in the field of digitization of minds and virtual reality about the potential role that blockchain technology could play in the digitization of human consciousness. The results of the survey and secondary research indicate that blockchain technology can be used to enhance the security and privacy of digitized minds. The study shows evidence with supported arguments to the role that blockchain technology could play in terms of prevention of attacks, data integrity, availability, confidentiality, operational security and privacy.

Keywords:- *Digitization of human consciousness,Blockchain technology; Security; Privacy;*

I. INTRODUCTION

The search for eternal life has obsessed the Man of every age and culture: if for some immortality was conceived as a "damnation" (think of the curse that strikes the wandering Jew), for others it was to be understood as an " award "to be achieved after a long process of magical, spiritual and initiatory research. Modernity embraces the millennial dreams of the alchemists, emptying them and making the frame of the progress of the technique. The instinct of modern man is to "technologically" improve one's own potentialities, to finally succeed in substituting the completed natural evolution, to continue one's own course according to autonomous purposes. The new technologies have gained such power of suggestion and conditioning that are intended to modify the social and political relations in the future towards the establishment of a pyramidal society and oligarchic.

In order to gain immortality, modern society has put its hopes in technology instead of magical elixirs. In the recent past, technology has been used by various companies to use the latest technologies to replicate the human brain in hopes to transfer it to a virtual being of humans. One of the processes used by a company called Nectome is hibernation of a human brain.

A. *Brain Hibernation*

Although the brain hibernation techniques are not fully developed yet, people in hope that they will soon become reality, have already resorted to cryonics practice in order to preserve their body from the dead in hibernation. In order to preserve the structures of the brain that retain information about the personality and the self of the deceased. In this way it is hoped that in a more or less distant future it will be possible to "wake up" the frozen patients, giving them the so-called cybernetic immortality, reawakening them from the "sleep" of death, or bringing the bodies back to life and then transferring them the memory downloaded. Recently the news has been spread that the American start-up Nectome has started a project of cryopreservation to the mind, waiting for the scientists to develop a system to digitize the thoughts and recreate them on the computer. But in order for the metamorphosis to succeed, the process must begin when the brain is still alive, or at most a few minutes after death. Around 25 people have already booked for the procedure [1].

B. *Mind uploading, the biological brain mapped and copied*

The transfer of the mind or brain emulation is the project that involves the hypothetical process of transferring or copying a conscious mind from a brain to a non-biological substrate. The process involves the scanning and detailed mapping of the biological brain and the copy of its state in a computer system or other computing device. The computer would perform a simulation of the model so reflective to the original that the simulated mind would behave, in essence, in the same way as the original brain, or for all practical purposes, in an indistinguishable manner. Information within a brain may be partially or entirely copied or transferred to one or more other substrates (such as digital storage or another brain), reducing or eliminating the risk of mortality. On the other hand, one would have the possibility of obtaining several mirrored copies of a single human mind and hence the creation of clones with identical memory [2].

C. *The creation of Avatar by 2045*

This type of research tries to explain and simulate the functioning of the brain and the relationship with perception, mind and personality, omitting, however, any metaphysical vision on the conscience and above all on the soul. Connectomics and mind uploading are based on a mechanistic view of the mind that denies the vitalist vision of human life and consciousness. As early as 1950, one of the founding fathers of cybernetics, Norbert Wiener, predicted that one day a mind could be transferred through the wires of a telegraph, while twelve years ago the scientist and futurist Ian Pearson said he was convinced that by the year 2050 the entire content of human brain can be completely "downloaded" onto a super-computer [3]. Human thoughts can be stored like files, memories in the form of bits, emotions and portions of mind can be zipped and then they can be made available for download as if they came from the hard drive of a computer instead of the brain. The young Russian media magnate Dmitry Itskov is convinced that by 2045 he will be able to transfer his mind into an avatar, a hologram that will allow him to do without the body and live forever. In reality, "surviving" will be the recording/copying/transfer of brain information [4].

ISSN No:-2456-2165

D. *Research Rationale*

The discussion so far shows that they wish to gain immortality is a longing that has prevailed in the humankind for a very long time and in the modern world of technology, people today have put in their hopes in technologies instead of alchemy and magic. After the rise of the internet followed by the Big Data revolution, the latest technological advancement that has increased the hopes of people such as Dmitry Itskov are artificial intelligence and blockchain technologies. This study is focused on exploring the role blockchain technology in digitization of human brain and consciousness.

II. LITERATURE REVIEW

A. *From Artificial Intelligence to Digitization of Human Consciousness*

In recent years we have witnessed a more and more in-depth research, supported by technological and IT development, in the field of Artificial Intelligence and efforts have been multiplied in trying to create increasingly sophisticated systems of robots able to "think" or at the very least to show intelligent skills in specific areas. Since the early developments in computer science, scientists have been fascinated and attracted by the possibility of building intelligent machines that could compete with human capabilities. According to Hofstadter himself, "it could be said that the AI was born when mechanical devices replaced men in some of the tasks previously performed only by the human mind" [5]. From the birth of the expression "Artificial Intelligence" (which took place in 1956 by the American mathematician and computer scientist John McCarthy) to date, the branch of computer science that performs this kind of studies has made giant steps despite not yet being able to create a thinking machine in the true sense of the word. As Ray Kurzweil states, however, "turn this stupid myth that the AI has failed, but the AI is everywhere around you every second of the day" [6].

In the subsequent developments of the theories linked to the Artificial Intelligence a distinction was made between "Strong Artificial Intelligence", which consists in creating machines really able to think thanks only to the instruments of its artificial neural network, and a "Weak Artificial Intelligence", which consists in the creation and use of programs that can be used in certain situations to solve everyday problems, often outside human capacities (see the case of a computer, Deep Blue, which is 1997 beat, in a game chess, world champion Garry Kasparov). In the case of "Weak Artificial Intelligence", however, it is questionable whether it is possible to consider these machines really "intelligent" because they do not really demonstrate the ability to think but, more simply, apply an algorithm, more or less complex, to solve specific problems [7].

Over the years, scientists have repeatedly wondered what could be a method for understanding and defining with certainty, whether a machine can be considered as truly thinking (like a man) or not. In this regard, Alan Turing, a British mathematician, considered one of the fathers of computer science, has proposed what he defined at the time "the game of imitation", today known as the Turng Test. Summing up the functioning of your test to the maximum, you can say that there are three entities involved: two men and one computer. A man (the interrogator) stands alone in a room and asks questions, via computer, to the other two entities (the computer and the other man) who answer in turn by telematic means. At the end of the test, on the basis of the answers received, the questioner must determine which of the two entities is more human-like, and which, instead, is the machine [8].

From 1950 to today no machine has exceeded the Turing Test in a minimally satisfactory way, thus demonstrating the inability of its artificial neural networks to be identifiable with those of man. Faced with the joint commitment of science and information technology in creating machines that can help man in a more and more evident and consistent way, developing what could be defined as forms of "Weak Artificial Intelligence", are actually the builders of entertainment systems that are dramatically increasing their efforts to create machines that can interact with human beings (this is mostly in the context of video games, those that can stimulate growth processes in their characters, just as happens in humans) [9].

From the successes achieved with artificial intelligence and the limitations that robots present in terms of acting as humans, the concept of turning a human into a machine arose. This concept implies that human brain and consciousness can be transferred into a machine, a virtual world, in which a person can continue to exist with a virtual body while still having the same mindset and thoughts, attitude and behavior. This concept completely eliminates all kinds of difficulties that researchers have been facing in ‘humanizing' the robots. Now digitization of brain is a goal that indicates how modern society may achieve immortality, though it is in a virtual world. This is different from artificial intelligence or improving robots to become as human as possible [10].

Dmitry Itskov predicts that by the year 2045, humans will be able to make copies of themselves to the cloud. He believes that you will be able to create a digital version of your human consciousness, stored in a synthetic brain and an artificial host. Itskov's overall project to do just that is summarized in four phases. He has spent millions on the plan, called the Avatar Project, which operates under the umbrella of Initiative 2045 [4]. The development of a robot that is controlled by a human brain is Avatar A, the first of the four phases. Avatar B consists of transplanting a human brain into a synthetic body. The content of a biological brain will be loaded into a synthetic one in Avatar C. The final piece of the Avatar Project, Avatar D, is based on emulation: replacing the biological body and the brain with a hologram or other avatar, which houses a digital camera version of our human conscience [3].

B. *The human brain and its Conectoma*

The Human Genome Project set out to identify all human genes and human DNA sequence. The Human Microbiome Project was created to identify and sequence all the microbes that colonize the human intestine. And another similar project, scientific research is the identification,

ISSN No:-2456-2165

mapping and deciphering something else that defines our humanity: the nerve pathways of the brain [10, 13]. This is the Human Connectome Project. The connectome, it is believed, is responsible for the things that make you who you are. The human brain contains an estimated 100 billion individual neurons, each connected and firing messages to a maximum of 10 thousand other neurons [11].

This signaling, which may be neurons firing simultaneously or in a sequence, is how it encodes and processes information, how associations are formed and how the brain performs tasks. It is, possibly, also the very essence of the human being, including his personal memories, his talents and all the extravagant things that make up his individual personality. That is all contained in the connectome [11, 13]. The concept of human consciousness is often compared to the keys of a car- your car is an incredible machine, but without the ignition key there is no spark, there are no signs of life. Consciousness is what we know and experience both in ourselves and the world that surrounds us, and is created from the exchange of information that occurs in the neural network of the brain [11]. There are some main theories, or starting points, at least as to what constitutes human consciousness. Integrated information theorists, for example, calculate the amount of information embedded in a neural network, a quantity called phi. The more links within the network, the more information exchange, and vice versa. Another theory suggests human consciousness works as computer memory [12].

The theory of the global workspace suggests that the brain collects information and the art of dispersion through the neural network is, perhaps, consciousness. While the brain of the nematode is not as complex as that of a human being, which translates into digital code is no small thing. Emulation of the whole brain, Minds-independent substrate and a Lego robot worm [12], perhaps surprisingly, part of this futuristic vision of human consciousness digitization is actually already possible, at least in very early stages. Take, for example, the Lego worm robot. In the development field of all brain emulation research, scientists have successfully traced the neural networks of the earthworm Caenorhabditis, including 302 neurons of its nervous system and the 7,000 neural connections of each-think of this as a wiring diagram of the Brain [14, 15].

Following the model of the neural network and connections in the brain of the worm, a code is written and inserted into, in this case, a Lego robot 'customized with a sonar-sensing nose and the motor neurons to replicate the wiring biological neuron of the worm. In theory, it could be done with the human brain at a much larger scale - the human brain has 100 billion neurons and 100 billion connections between them [14]. Mapping the precise, street-like city grid and deciphering the rules of the neural network of the human brain could lead to advances in our understanding of the roots of human neurological, neurobehavioral and neuropsychiatric disorders. It could also contribute significantly to innovations in the prevention, treatment and cure of conditions associated with problems related to brain wiring [15]. It could also lead to a deeper understanding of our way of thinking and reasoning, our sense of self, and the ways in which we could emulate the human mind. Mind-charging, or the creation of minds-independent substrate, involves transferring the contents of your human brain to a new synthetic brain - a digital copy of not only your memories but the details of your personality and your own consciousness [13, 14].

Although research is still in the early stages, in the long term, scientists plan to develop a synthetic, a hologram created to host the worm's digital connectome. And then there's the Avatar Project, under the Defense Advanced Research Projects Agency (DARPA). The Pentagon project combines advances in both remote control and telepresence - in simpler terms, this means that the Department of Defense is working on the development of surrogate soldiers, controlled by real soldiers from a safe distance. Also funded by DARPA, a study at Johns Hopkins University in Baltimore succeeded amputees to move their artificial limbs with mind control and the help of brain implants. Similarly, amputees in a study in Iceland were able to control their orthopedic legs through 5 millimeters long by 3 millimeter sensors throughout myoelectric implanted (IMES) sensors developed to stimulate and control the muscles of the remaining part of the leg [15].

An interesting comparison between the human brain and modern supercomputer technology is presented by XXXX who argues that developing an artificial intelligence is not as simple as the concept and perception is. Nature has provided humans with a perfectly optimized genetic apparatus. A human brain would possess the computing capacity of 36.8 petaflops and a memory capacity of 3.2 petabytes. One gram of DNA can theoretically store 455 million terabytes. For comparison, the world's first supercomputer has a computing power of 93 petaflops and a memory amount of 1.31 petabytes. However, the supercomputer requires an area of 1000m² and an electrical power of 15 MW, while the human brain does not need more than 1400cm³, and 20 W effective power [16].

The challenge of Artificial Intelligence is to make up for this backlog of hundreds of millions of years in a few decades, so that the Artificial Intelligence will one day succeed, for example, in detecting the subtlety of sarcasm in a statement. The impasse is not in the hardware limitations because supercomputers seem to have today the computing power and memory needed, but in the software [13,15]. How could we write software equivalent to hundreds of millions of years of evolution? One of the possibilities envisaged would be to reproduce the concept of genetic selection with algorithms (genetic algorithms). The most efficient algorithms would phagocyte the computing power of those who fail [12]. The second approach would be to create a computer that carries out research and development around the field of artificial intelligence while being able to integrate its discoveries into updates [15].

C. *Blockchain Technology and Digitization of Human Brain*

The Internet gives us the opportunity to have direct access to information. Platforms for connecting individuals such as Facebook, Twitter, Uber, etc. act as intermediation agents. They embody an alienation from the original

philosophy of the Internet. This is why Blockchain technology has emerged as the vector for disintermediation of all human and digital activities [18].

The Blockchain is a Peer-to-Peer technology that securely distributes a database across all nodes of its network. In the same way that robotization has replaced jobs with repetitive manual tasks, by eliminating any intermediary, Blockchain technology will cause the disappearance of trades acting as a trusted third party, that is to say, reliable human transactions (manager, notary, banker, Human Resources, real estate agency, public institution). Two models of algorithmic governance based on the Blockchain will then oppose [17].

- The regulation of the behavior of the citizens will be carried out by the algorithms (Regulation by Law), and thus by those who control them, in order to preserve the relations of existing domination [19]
- An ethical regulation of behaviors (Governance by design) by affixing a social layer Blockchain technology would allow humanity to maintain the ascendancy of the decision-making delegated algorithms [20].

The Ethereum smart contract is a computer protocol that automates the execution of the terms of a contract between different parties (human or not). By extension, you can scan a company whose operation is governed by algorithms and secured via the Blockchain. Hiring, job distribution, compensation would become computerized activities [17, 18]. Moreover, this algorithmic company could be owned collectively or not. The Blockchain is a tool considered by libertarians and transhumanists as liberators because it allows doing without any intermediary and thus to upset the existing relations of domination. But will they disappear? Behind all these algorithms is the question of capture. The Blockchain will undoubtedly be massively used to lock the domination relationships in place. This is a unique opportunity to systematically regulate the behavior of the citizens with a hitherto unequalled efficiency, but also to reduce massively the costs and thus aggravate the inequalities greatly, or even to circumvent the legislative framework of our "democracies" [21]. But, it will also be a chance to realize a social project around communities sharing common interests, and consequently to create an alternative digital society to the first. By breaking free of borders and discriminating characters [22].

D. *Virternity Project, Blockchain, and Digitized Human Consciousness*

Virternity conjectures the idea that neural networks combined with blockchain will allow them to conduct a precise multivariate analysis of possible courses of events. Thus, intimating that reliable forecasts and foresight will be introduced into everyday life [17]. This could be a possible way of looking into the future with better certainty in their opinion. They also submit that the system will be able to track in the real-time mode the state of a person's health and even offer advice and future options [23].

The blockchain is a system which indelibly writes transactions that link information together and cannot afterwards be erased. Initially focused on financial virtual currencies, the blockchain technique has wider applications that can encompass many types of transactions. Imagine the scenario where even though a person might have deleted posts or comments from their social media these are still available in the system [17]. The implication is that this type of information and opinion can be used for forecasting trends or possible future events. The concept of personal future forecasting implies an expert system that may present outcomes based on an individual's current courses of actions, beliefs or opinions, among other things. The mining of health information implies a connection with a tracking device that provides this information and consults a health, expert system, which can give advice based on its database and algorithms [23].

E. *Current Applications of Blockchain in Digitization of Human Consciousness*

In recent years more and more startups have emerged with the intention of connecting our brains to digital platforms. The goals are to monitor our thoughts and moods or to download activity data. As you can imagine, such technologies are inevitably raising a number of problems regarding data security, privacy and even transparency. Customers obviously want their brain data to be protected and treated in accordance with the terms and conditions. To this end, it is very likely that these companies take a look at blockchain technology to ensure that data remains truly secure. Some neurotechnology startups have already outlined plans to put brain data on the blockchain. Let's see some of them.

One of the first companies to confirm that they will use blockchain technology is Neurogress. Registered in Geneva and established in 2017, the company focuses on building neural control systems, allowing users to control robotic arms, drones, smart appliances and AR / VR devices (augmented reality / virtual reality) with their own thinking. The Neurogress control system is based on the use of automatic learning to improve the accuracy of the brain reading. All this requires the maintenance of 90% of the brain data to train the artificial intelligence (AI) used by the system. In other words, "large user neural activity data" is required. The same whitepaper of the company cites the need for " exabyte (1 exabyte = 1 billion gigabytes) of memory " of the Human Brain Project as an example of the type of storage capacity required [24, 25].

It is not surprising that Neurogress intends to use blockchain, which he believes effectively solves the problem of data storage security and privacy. By recording user data on a decentralized blockchain, they become "resistant to hacking attacks" and therefore more private. The candidate blockchain is those of Ethereum, IOTA and EOS [25,26]. At the same time, the use of blockchain technology makes the Neurogress system open and transparent to potential users of the Neurogress platform services. Since any anomalous activity would be easily traceable, the system will guarantee the security and confidentiality of personal data [25].

There are great ambitions, but these are more than compensated by the other startups operating in the neurotechnology space. Perhaps the most ambitious of all is Nectome, a California-based company that aims to preserve the human brain through an embalming process known among professionals as cryopreservation stabilized with the aldehyde [24, 25]. Not only does Nectome aim to preserve the human brain, but its website states the aspiration to digitize your preserved brain and use that information to recreate your mind. The digitization of an entire human brain obviously requires a means to store it, and this is where the blockchain technology peeps out again. In fact, there is also the opening of Nectome to the possibility of using a blockchain [26].

One of the Co-founder Michael McCanna, a graduate of MIT (Massachusetts Institute of Technology) claims that they are trying to abstain from speculation on specifics relating to neurotechnology not yet invented [25]. But they assume that there is a possibility that blockchain technology, including smart contracts, may one day play a role in managing the aspects of any neurotechnology service offered in the future [26]. However, at the moment, it has no specific plans to incorporate blockchain technology, if only because the uploading part of its operations is still extremely early [27].

Neurotechnology remains in a very experimental phase and only a few selected startups have managed to confirm a role for blockchain technology. In addition to Neurogress and perhaps Nectome, there is also Basis Neuro. A company registered in the Cayman Islands that wants to use blockchain for its neuro-control platform to effectively systematize data on brain activity under conditions of anonymity [24, 26]. However, the potential exists, just as in the field of artificial intelligence, which overlaps with neurotechnology and is finding a role for blockchain in a growing number of companies. The question remains, however, on how the personal data of the brain remains 100% safe on a blockchain [27]. The decentralized and transparent nature of blockchain would certainly prevent data from being altered or stolen, but many of the general concerns surrounding large-scale data collection still apply. The sensitive data may end up being sold to third parties for marketing purposes questionable [25]. Furthermore, users could still be indirectly identifiable (as they are with Bitcoin) through pseudonymous data identifiers or schemas [26].

Blockchain and GDPR allow realizing "security by design" solutions guaranteeing pseudonymisation (decoupling of data from individual identity) and minimization of data (sharing only the absolutely necessary data points). Recall that in the Blockchain data protection is ensured by a public key of the sender of the transaction [24, 27]; from a public key of the recipient of the transaction; from a cryptographic hash of the contents of the transaction; from the date and time of the transaction [25, 26]. With this setting, it is impossible to reconstruct the contents of a transaction from the unidirectional cryptographic hash. And unless one of the parties to the transaction decides to link a public key to a known identity, it is not possible to map and link transactions to individuals or organizations [26]. This means that even if the Blockchain is "public" (where anyone can see all transactions on it), no personal information is made public [27].

III. METHODOLOGY

This section explains the methodological structure adopted for the research process. This section justifies each and every decision related to research design. The discussion includes explanations for research design, data collection method, sampling techniques, and other research-related issues.

A. *Research Design*

This study has been based on quantitative design. Since the aim of this study is to explore the role of blockchain technologies in digitization of human consciousness, therefore the researcher assumed that the empirical evidence to be collected be based on objective and verifiable data, free of personal bias [28]. The quantitative design has the potential to address these concerns and the knowledge thus gained is considered to be reliable and valid as well as acceptable in the research community [34].

Furthermore, there are several components of research design. Research design includes data collection strategy, data collection instrument, sampling process, and data analysis techniques [29, 30]. Following discussion explains each of these choices briefly yet comprehensively.

B. *Data Collection Strategy*

Social researchers have a wide variety of data collection strategy which includes experiments, ethnographic study, survey strategy, etc. This study adopted a survey as data collection strategy [30, 31]. The main benefit of survey strategy is that is widely used in the research community and it enables researchers to gather a large amount of data with a high level of time efficiency. As compared to experiments and ethnographic studies surveys collect data in less time [33]. Furthermore, surveys are also considered to be cost efficient because internet and telecommunication technologies have overcome geographical and physical barriers, that previously, increase time and cost of surveys [37].

In this study, the researcher focused on digitization and virtual reality experts who are working in multinational companies around the world [31, 35]. The researcher sent invitations to potential participants through emails attaching research background, questionnaire, and consent forms. The survey was completed successfully through collaboration via emails [32].

C. *Data Collection Instrument*

This study adopted a self-administered questionnaire as data collection instrument. The questionnaire designed for the study was divided into three sections [32]. The first section of the questionnaire collected demographic characteristics of the research participants. The second section of the questionnaire was focused on gathering data about the role of blockchain technologies in the security aspects of digitization of human consciousness [34, 35]. The third section in the questionnaire focused on the role of blockchain technologies to enhance the

privacy of the digitization of human mind. All questions in the questionnaire were structured as the closed-ended question, having a Likert five-point scale to quantify the opinions of experts in the study [36].

D. *Sampling Strategy*

Sampling refers to the method or technique that is used by researchers to identify a sample from the target population. The sample is assumed to be a reliable representative of the entire population [29, 33]. The researchers then conduct research process using the sample and assume that the results so gathered are applicable to the entire population [30, 31].
The target population in this study is experts and professionals working in digitization and virtual reality industries. This study adopted a random sampling technique. The researcher searched professional profiles of digitization and virtual reality experts on the LinkedIn platform which is one of the most prominent social networks for professionals around the world. The researcher then collected contact information from professional profiles and sect invitation to potential participants. The researcher sent around 100 emails and in response only 76 professionals showed interest in the study and responded back with a filled questionnaire.

E. *Data Analysis Techniques*

Quantitative studies apply statistical techniques to analyze the data. Statistical techniques are considered to be highly reliable and valid [34]. Furthermore, there is statistical software dedicated to conducting statistical analysis with accuracy and ease which otherwise would be complex and time-consuming [35]. This study used SPSS to analyze data. This study used frequency analysis to analyze the trends and opinions of digitization and virtual reality experts about the role of blockchain technology in enhancing the security and privacy of the digitization of human consciousness.

F. *Ethical Considerations*

In order to main integrity with the research community and research participants, social researchers are required to observe a variety of ethical values and principles [36]. In this study, the highest priority was given to plagiarism. The researcher provides proper credit to the works of all authors used in the study as per publication standards [37]. Furthermore, the researcher obtained prior consent from all participants before data collection process [30]. Furthermore, the researcher maintained the confidentiality of all participants [28]. In addition, the researcher ensured that the privacy of all participants is protected and the data and information provided by them were not used for any commercial purposes [33].

IV. RESULTS

This section presents the results of the survey. The results are presented using graphs and interpretations of the graphs. The study also analyses the results within the context of general literature in order to assess consistency. The results begin with results regarding how blockchain technology can contribute towards the security of data and information for digitized brain and human consciousness and then continues to present results regarding privacy concerns. The results are presented using tables and a detailed discussion of results by comparing them with other researchers.

A. Security of Data and Information

Although humans have an abundant capability to reproduce, yet there is no technology that can be used to replicate a human. However, if and when the digitization of human brain is achieved, the concept to replicate the entire brain is not impossible anymore. Thus, there is a need to ensure that data and information recorded from the brain of a person for the purpose of digitization and to create a virtual person is absolutely secure. The security of the physical brain or biological brain is somewhat easier as compared to the security of a digital brain or virtual brain. This is because the virtual brain or digitized brain is, in fact, nothing but data that is vulnerable to security breaches. With the rise in digital crimes, particularly credit crime crimes through the internet indicate that there is a need to proactively address security issues of digitized brains. Within this context, the study asked participants to opine whether blockchain technology offers a potentially effective solution for the security of digitized human consciousness. The results show that majority of the respondents agreed that blockchain is considered to be a technological advancement that provides a high level of security.

- *Prevention of Attacks*

Security benefits are widely reported in general literature also. For example, Zyskind and Oz [38] concluded that the review of commonly cited advantages attributed to the blockchain against classic solutions, from the point of view of the security management. The biggest achievement of the blockchain is the abandonment of the need for authority. This abandonment does not seem an advantage in itself [38]. From the point of view of safety, to know if it is better to put the eggs in many baskets or in one basket (and to monitor that basket well), guardians would need to know the safety of each basket. The blockchain supports its security in that the model of cooperation between nodes is inviolable against malicious nodes unless they are many [39]. The PoW model guarantees, in effect, that the massive creation of malicious nodes does not provide an advantage, making the so-called "sybil attack" impossible. In a corporate blockchain, the security would lie in the supposed difficulty of several of the participating entities to reach an agreement and in the design of the consensus model and associated software [40].

However, Biswas, Kamanashis, and Vallipuram [41] contradicts and criticizes by arguing that it is not clear that managing the security of each team in each entity is easier or cheaper than managing the security of the only team that manages our classic solution. In the case of unified equipment, it will be necessary to establish internal controls. It is possible that creating this team is, from an operational point of view of the entities, more difficult than having each entity create and manage its own team. But the security model researchers know best is the management of security in a team managed under an authority [41]. The security model of the blockchain, on the other hand, requires an almost absolute confidence that the technological solution does not allow a malicious node to take advantage of others. But the reality is that, to this day,

consensus models that are not based on PoW do not provide that security [42]. Even if such a model existed, we would need a mechanism to arbitrate a conflict of consistency. In theory, no such conflict should occur, but in practice assume such a thing is equivalent to also deposit full confidence that the software that automates the model has no flaws [43].

- I*ntegrity*

Another important aspect of the security of a digitized human consciousness is the integrity of data and information stored. The survey asked specialists regarding the integrity of data and the role of blockchain technology and the results indicate that majority of the specialists are confident that blockchain technology helps to ensure data integrity [44]. Therefore, it is safe to assume that blockchain will provide the same level of integrity for digitized human consciousness as it provides for economic transactions through bitcoins.

Comparing these results with general literature, this study refers to Shrier, Weige, and Pentland [45] who compared blockchain with the traditional system. The author refers to the degree of confidence in the people who manage the service, be it blockchain or classic and then evaluates the degree to which an external attacker could subvert the system. A well-known paradigm of the blockchain in the guarantee of the immutability of the "ledger", in case digitized brain a chain of documents. In models with PoW, this guarantee is based on the physical impossibility of recalculating a coherent chain of hashes, due to the enormous computational capacity required [45]. On the contrary, both the corporate blockchain and the classic solution must ensure the integrity of the information with the usual digital signatures. In the classic solution, key management would be done as a classic control authority does. In the case of the corporate blockchain, if a classic control authority is not adopted, security personnel should build a "web of trust" in the PGP style. Both models have in common the need to guard the keys [46]. If an attacker were made with the appropriate keys he could build a valid string of documents (from the cryptographic point of view), he would not need an impossible computing power for it. Confidence in the integrity of the corporate blockchain should, therefore, be based on the same premises as in the classical solution, and the challenges of sharing keys between entities are those known in a PKI. It does not seem that here using a corporate blockchain is more or less sure, a priori, than using a classic solution [47].

- *Availability*

Furthermore, another important aspect of the security of data is Availability. The survey asked experts to opine whether blockchain ensures a high level of availability of data. The results show that the majority of the experts agreed that blockchain provides full availability of data [48].

Tse, et al. [49] argued that as compared to classic security solutions the problem of availability has been delegated to the use of cloud technologies. Obviously, the clouds have their percentage (low) of unavailability. But in the same way, the management of computation and storage distributed between nodes can only guarantee the availability of service with a certain probability, if one is to impose the condition of consistency. It does not seem therefore that the blockchain technology or the use of the cloud in the classic solution present many differences in this regard [49].

- *Confidentiality*

One of the most important aspects of digitized human consciousness is confidentiality. The survey results show that the majority of the experts show a high level of confidence regarding confidentiality provided by blockchain technology.

Within this context, this study refers to Samavi, Thomas, and Thodoros [50] who concluded that a priori the ability to manage confidentiality should be based on data encryption, which brings back the problem of responsibility in the custody of keys when there is no authority. From the point of view of privacy, encryption seems, of course, the only answer in the case of the use of blockchain technology. Although it is not technically equivalent to destroy a key to erase the data, one can reduce the risks as necessary by guaranteeing the destruction of keys. However, it seems difficult to quantify this guarantee without a centralized custody of keys [50]. From the point of view of regulation, what is certain is that GDPR has not been conceived with blockchain technology in mind. The question of who is responsible for a data located in a "ledger" distributed and modified by consensus can only have an answer over time, depending on the interpretations of the regulator. It is clear at least that the use of a classical solution, in this case, has many fewer uncertainties than the use of blockchain [51].

- *Operational Security*

Finally, another important aspect of security is operational security. The survey among experts shows that only a few experts show confidence in terms of operational security provided by blockchain technology. In order to identify reasons for lack of confidence, this study consulted general literature and found that Puthal, et al. [52] argued that without a doubt, the key aspect here is the lack of maturity of the blockchain technology. This is a problem associated with all new technologies, which as usual will be resolved with time, experience and patches. The problem of software vulnerabilities, in the case of a blockchain, seems to be a complicated solution. The entities responsible for the nodes must coordinate with each other the production of new versions or patches. This always seems more difficult than when the software is centralized, as in the classic solution [52].

B. Privacy

Privacy is also one of the main issues faced by modern society. With the development of new digital technologies, it has been increasingly easier for people to share personal information. Social media, for example, invites people to share not only personal information but also personal photos, and other information [53]. On one hand, these technologies offer opportunities for better communication and leisure while on the other hand, the same technologies are vulnerable to invasion of personal privacy. In order to improve privacy, digital platforms and businesses have developed a number of techniques to allow users to protect their privacy from unwanted people. One of the most basic technique is

ISSN No:-2456-2165

authentication protocols [54]. Authentication features allow people to restrict access to personal information and data [55, 54].

Although modern technologies have not advanced so much so that they can access private thoughts and ideas in the physical human brain and gain access to the thoughts and therefore there is no need for a person to implement authentication protocol to save data, information, ideas, etc. from unwanted people. However, the same cannot be true for a digitized mind. As mentioned earlier, a digitized mind is nothing but data and information, a record of actual mind and consciousness, or just a virtual replica [53, 56]. This implies that it is vulnerable to virtual attacks. Within this context, the survey asked participants to share their opinion about the privacy of digitized minds and how blockchain technology can play an effective role in terms of protecting the privacy of users. The survey questions were mainly focused on authentication techniques in blockchain technology [54, 57].

➢ *REMME*

The first question regarding authentication techniques in blockchain technologies was related to Token Remme, and Authentication without passwords through decentralized Public Key Infrastructure (PKI) [58]. The survey asked whether Token Remme enhances privacy protection. The results indicate that majority of the experts opined that Token Remme has significant potential to block cyber-attacks and prevent invasion of privacy [59].

Similar results have been provided by Mosakheil [58] who concluded that the main objective of this token is to get a user to authenticate without the need to use passwords, avoiding the problems derived from its use [58]. REMME proposes as a solution for the implementation of a decentralized PKI (Public Key Infrastructure) within blockchain. This blockchain will store the information of the certificates that REMME will generate for each device that wants to authenticate itself. This solution has the purpose of eliminating all the problems associated with the use of passwords (loss, theft, brute force attacks, etc.), centralization of certificates and existing rates in the current PKI systems, pretending to be more economical and secure [58,59]. Supports certificates of type X.509 both self-signed and signed by an external organization. At the technical level, REMME is an ERC20 Token that works on the Ethereum network using a side chain. For their development, they have used Hyperledger Sawtooth, a platform for the creation and deployment of blockchains. This framework is designed to be modular since each of its parts can be replaced by its own code [58, 59].

➢ *VeriME*

The survey also explored the opinions of experts regarding other authentication techniques. Participants were asked whether Token Verime, Verification as a service (VaaS) is an effective technique for protection of privacy of users of blockchain. The majority agreed that this technique can also be considered as an effective tool to ensure privacy and protect data and information.

According to Shah [60] VeriME is a new cryptocurrency focused on digital identity and facilitating authentication mechanisms. Its objective is to offer Verification-as-a-service (VaaS) on blockchain and mobile applications. The idea is to use biometrics and machine learning to identify and authenticate the client during the purchase of goods and services, allowing the client to verify who is with any service provider that is a VeriME partner in just a few seconds [60]. VeriME uses the Token ERC20 working directly on the blockchain of Ethereum, that is, on the nodes existing in the blockchain of Ethereum [61]. However, it is important to note if a person wants to access digitized brain after his/her demise than biometric access would not be feasible, however, the users may identify another person to provide biometric and ensure protection and privacy [60, 61].

A number of researchers have reported various benefits of this authentication technique that can be used for the privacy of digitized minds [62]. For example, Song, et al. [63] reported that one of the solutions that VeriME.

- *D-KYC*

This technique is based on the notion of "Know Your Customer" and its objective is to allow companies to verify and validate the identity of the clients. D-KYC obtains data from users (ID, driving license, credit cards, etc.) digitally and remotely. Once obtained, the client must take a photograph [61,62]. Through the use of biometrics and machine learning, VeriME checks that the documents provided are correct. This data is stored in the user's mobile device to guarantee privacy and reduce the risk of leakage. This mechanism aims to prevent customers from going in person to the service provider so that they can validate their identity [64].

- *D-SECURE*

Nikouei, et al. [65], reported another important feature of VeriME which is D-SECURE. It is a decentralized authentication mechanism that can be used once the user has been identified by D-KYC. The user can authenticate himself by scanning a QR code or by biometrics. Additional checks are also made such as IP / GEO, device fingerprinting, etc., using machine learning tools for the prevention of fraud [65].

➢ *VerifyUnion*

Furthermore, the survey also explored the opinions of experts regarding effectiveness and role of Token VerifyUnion, a Decentralized authentication with blockchain and public key cryptography, in terms of protection of privacy of blockchain users for the privacy of digitized minds. Majority of the experts indicate that blockchain has a variety of effective authentication technique, one of which is VerifyUnion [61,63].

General literature shows that similar results have been obtained by other researchers. Wu, et al., [64] for example, reported that VerifyUnion is a decentralized digital platform whose objective is to obtain the authentication of the users or, what is the same, in this scenario, verify their identity. As a differentiation to other platforms, they add the social concept trust as a service and use a social scoring score for which they use data from social networks and public documents. The user

can improve his score by adding data to his profile [64]. The user's data is stored locally to maintain privacy. It uses the ERC20 token working directly on the Ethereum blockchain, which simplifies the coin creation process since it is not necessary to define protocols or own architecture elements because they use the existing ones in the Ethereum chain. Thus, in this way, the private information cannot be accessed by users who have low scores or otherwise inadequate credentials [63, 65].

Furthermore, according to Shah [60], VerifyUnion proposes a solution for the verification of the identity of people through a decentralized methodology. Using the blockchain technology for the authentication process they try to eliminate the possibility of someone altering the information, since every time a transaction is made, or what is the same, information is added to the chain, most of the network You must verify its validity. VerifyUnion aims to combine blockchain with public key cryptography. Once the data is stored in the chain, through public key cryptography a user can send their credentials securely. The recipient can verify the validity of the credentials against a block in the given chain [60]. For this to be possible it is necessary that each block of the chain has an identifier. This ID is a set of data of the string that can be verified. By adding an ID to the block, a pair of keys is created and the private key is transferred to the user, this means that the user and only the user is able to create a signature that can be verified with the public key that is stored in the chain [65]. This mechanism will then serve as decentralized authentication. In order to authenticate a user, an application only has to request a digital signature and the ID of the user's block that wants to authenticate. Once this information is received, the application can verify the signature with the public key stored in the block of the chain whose ID matches the ID that the user has sent to it. Considering this whole scenario, it can be fairly opined that VerifyUnion can be used to secure data and information of digitized minds [63].

V. DISCUSSION & CONCLUSIONS

This study concludes that the security of digitized human brains and consciousness is based in the notion that humans are able to ensure the security of their thoughts and information in their brains, however, digitized minds are nothing but digital data and information. Therefore, digitized minds are vulnerable to hackers. For this matter, this study explored the role of blockchain technology and found that experts in the study survey, as well as researchers in general, see significant potential in solutions provided by blockchain technology. One of the main solutions discussed in this study is that blockchain technology eliminates the need for a central authority. Although in itself, lack of authority does not seem an advantage, however, from the point of view of safety and security, blockchain technology allows to store and retrieve data from a large number of nodes instead of storing it in a single place or storage unit. Therefore, for a hacker to access complete information has to deal with numerous nodes and storage points instead of accessing a single storage unit. The algorithms used in blockchain technology are considered too complex to be hacked. The blockchain supports its security in that the model of cooperation between nodes is inviolable against malicious nodes unless they are many. From this, it can also be fairly assumed the loss of data and information is also minimized even if a hacker(s) is able to access some nodes and fails to access others.

Furthermore, this study also concludes that another important aspect of the security of a digitized human consciousness is the integrity of data and information stored. The research shows that the majority of study participants agreed that it is an important issue and that blockchain technology has potential solutions to enhance the integrity of data and information. The blockchain technology is based on the degree of confidence in the people who manage the service and it evaluates the extent to which an external attacker is able to subvert the system. In this regard, researchers argue that confidence in the integrity of the blockchain is essentially based in the same premises as it is in the classical security solutions. Therefore, based on the opinions of survey participants and other researchers, it is concluded that blockchain technology in this regard is almost a priori when compared to classical solutions to data integrity.

Furthermore, this study concludes that availability is an important aspect of the security of data and information for digitized minds. The study participants showed that it is unlikely that blockchain technology could make a significant difference in this regard. As per other researchers when blockchain solutions for availability are compared to classic solutions, the problems in latter are credited to the use of cloud technologies. The cloud technology has its limitations in terms of availability and accessibility. The blockchain technology, in the same way, is based on the management of computation and storage distributed in a large number of nodes which can only guarantee the availability to a certain extent provided that there is excellent consistency in all nodes in terms of hardware and software. Therefore, overall based on results the study concludes that the blockchain technology in terms of availability does not provide a much better solution instead the solutions based on blockchain are almost the same as compared to classic solutions.

Furthermore, this study also focused on the confidentiality aspect to evaluate whether blockchain technology could enhance confidentiality for digitized minds. The majority of study participants involved in this study opined that classical solutions are likely to be better than blockchain technology to enhance security in terms of confidentiality. When compared to classical solutions, other researchers are found to have arrived at similar conclusions. This report concludes that as a general rule the confidentiality of data and information is achieved through data encryption techniques. In blockchain technology, the main problem in this regard is the lack of a central authority. From the point of view of privacy, encryption, of course, seems the only answer in the case of the use of blockchain technology. The risks of confidentiality breach can be reduced by destroying the keys which, although not technically, is equivalent to destroying the data to keep confidentiality. But when there is no central authority there is no sure way to quantify this guarantee. Concerns have also been raised regarding accountability and

responsibility due to lack of central authority. The blockchain cannot determine the responsible persons for data located in a "ledger" which distributed and modified by consensus. Therefore, based on the discussion this study concludes that there is much lower uncertainty in using a classical solution for confidentiality of data and information as compared to using blockchain technology. However, it is hoped that with the passage of time and new developments the blockchain technology may offer new and better solutions to enhance the confidentiality of digitized minds.

Furthermore, the study concludes that privacy is a significant issue in modern society as the advancements in digital technologies has made it increasingly easier for people to share personal information with other people and thus there are opportunities for hackers to breach privacy and misuse data and information on the internet. The research indicates that the information shared by people on social media platforms is one of the critical issues that reflect the security concerns for digitized minds. Since the entire mind, memories, and consciousness is to be stored in the digital format, therefore this study explored how blockchain technology could be used to enhance privacy. This study thus focused on the authentication techniques in that could be used to enhance privacy. The experts involved in the study agreed that there are various techniques that can be used to achieve this task. For example, REMME is an authentication technique that is beneficial to prevent unwanted access. VeriME and VerifyIUnion authentication techniques were also found to be more effective for protection of privacy of digitized minds. Overall this study concludes that blockchain technology is likely to play a significant role in the development and operations of digitized minds in the future and in the development of a virtual eternity in this world.

REFERENCES

1. Regalado, Antonio. “A startup is pitching a mind-uploading service that is 100 percent fatal”. The technology review. 2018 https://www.technologyreview.com/s/610456/a-startup-is-pitching-a-mind-uploading-service-that-is-100-percent-fatal/ accessed 30th August, 2018
2. BBC. “The immortalist: Uploading the mind to a computer”. British Broadcast Network. 2016. https://www.bbc.com/news/magazine-35786771
3. McCray, Patrick. “You, Me, and Your Avatar Makes Three”. 2016 http://www.patrickmccray.com/2013/06/05/you-me-and-your-avatar-makes-three/
4. Bolton, Doug. “Russian billionaire Dmitry Itskov seeks 'immortality' by uploading his brain to a computer”. The Independent UK. 2016. https://www.independent.co.uk/news/science/dmitry-itskov-2045-initiative-immortality-brain-uploading-a6930416.html
5. Loebbecke, Claudia, and Arnold Picot. "Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda." The Journal of Strategic Information Systems 24.3 (2015): 149-157.
6. Karwowski, Waldemar, and Tareq Ahram, eds. Intelligent Human Systems Integration: Proceedings of the 1st International Conference on Intelligent Human Systems Integration (IHSI 2018): Integrating People and Intelligent Systems, January 7-9, 2018, Dubai, United Arab Emirates. Vol. 722. Springer, 2017.
7. Bond, Alan H., and Les Gasser, eds. Readings in distributed artificial intelligence. Morgan Kaufmann, 2014.
8. Warwick, Kevin, and Huma Shah. "Can machines think? A report on Turing test experiments at the Royal Society." Journal of experimental & Theoretical artificial Intelligence28.6 (2016): 989-1007.
9. Bostrom, Nick, and Eliezer Yudkowsky. "The ethics of artificial intelligence." The Cambridge handbook of artificial intelligence316 (2014): 334.
10. Garnham, Alan. Artificial intelligence: An introduction. Routledge, 2017.
11. Mizutani, Haruo, et al. "Whole brain connectomic architecture to develop general artificial intelligence." Procedia Computer Science 123 (2018): 308-313.
12. Liao, Xuhong, Athanasios V. Vasilakos, and Yong He. "Small-world human brain networks: perspectives and challenges." Neuroscience & Biobehavioral Reviews 77 (2017): 286-300.
13. Vogelstein, Joshua T., et al. "To the cloud! A grassroots proposal to accelerate brain science discovery." Neuron 92.3 (2016): 622-627.
14. Lawrence, Neil D. "Living together: Mind and machine intelligence." arXiv preprint arXiv:1705.07996 (2017).
15. Norman, Robert A., and Sharad P. Paul. "The Last Natural Brain." The Last Natural Man. Springer, Cham, 2017. 51-64.
16. Barfield, Woodrow. "The Law of Artificially Intelligent Brains." Cyber-Humans. Copernicus, Cham, 2015. 71-99.
17. Smith, Alastair. “To Identify the Challenges and Opportunities Associated with Virtual Currency”. International Journal of Innovative Science and Research Technology. 3(7). 2018. 538-551
18. Buchanan, Bill, and Naseem Naqvi. "Building the Future of EU: Moving forward with International Collaboration on Blockchain." The JBBA 1.1 (2018): 3579.
19. Pilkington, Marc. "11 Blockchain technology: principles and applications." Research handbook on digital transformations(2016): 225.
20. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2 (2016): 6-10.
21. Till, Brian M., et al. "From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage?." BMJ global health 2.4 (2017): e000570.
22. Underwood, Sarah. "Blockchain beyond bitcoin." Communications of the ACM 59.11 (2016): 15-17.
23. Bailey, David Evans. "Virternity." (2017).
24. Chandler, Simon. “Your Brain on a Blockchain – Literally”. 2018. https://cryptonews.com/exclusives/your-brain-on-a-blockchain-literally-1673.htm

25. Furqan, Muhammad. “Recreation Of Human Brains Using Blockchain Technology”. https://coinpick.today/recreation-of-human-brains-using-blockchain-technology/
26. Miller, Rob. “Your brain on a blockchain—Literally”. https://medium.com/@RobMillerMoney/your-brain-on-a-blockchain-literally-af0ce7cac29a
27. Wise, Rico. “Human brain data – blockchain strikes once more”. https://base.info/news/human-brain-data-blockchain-strikes-once-more
28. Brannen, Julia. Mixing methods: Qualitative and quantitative research. Routledge, 2017.
29. Choy, Looi Theam. "The strengths and weaknesses of research methodology: Comparison and complimentary between qualitative and quantitative approaches." IOSR Journal of Humanities and Social Science 19.4 (2014): 99-104.
30. McCusker, Kevin, and Sau Gunaydin. "Research using qualitative, quantitative or mixed methods and choice based on the research." Perfusion 30.7 (2015): 537-542.
31. Flick, Uwe. Introducing research methodology: A beginner's guide to doing a research project. Sage, 2015.
32. Creswell, John W., and J. David Creswell. Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications, 2017.
33. Walliman, Nicholas. Research methods: The basics. Routledge, 2017.
34. Dang, Giang, and Low Sui Pheng. "Research methodology." Infrastructure Investments in Developing Economies. Springer, Singapore, 2015. 135-155.
35. Mertens, Donna M. Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods. Sage publications, 2014.
36. Hartas, Dimitra, ed. Educational research and inquiry: Qualitative and quantitative approaches. Bloomsbury Publishing, 2015.
37. Barnham, Chris. "Quantitative and qualitative research: Perceptual foundations." International Journal of Market Research 57.6 (2015): 837-854.
38. Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015.
39. Linn, Laure A., and Martha B. Koo. "Blockchain for health data and its potential use in health it and health care related research." ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. 2016.
40. Liu, Hong, Yan Zhang, and Tao Yang. "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing." IEEE Network 32.3 (2018): 78-83.
41. Biswas, Kamanashis, and Vallipuram Muthukkumarasamy. "Securing smart cities using blockchain technology." High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE, 2016.
42. Underwood, Sarah. "Blockchain beyond bitcoin." Communications of the ACM 59.11 (2016): 15-17.
43. Yli-Huumo, Jesse, et al. "Where is current research on blockchain technology?—a systematic review." PloS one11.10 (2016): e0163477.
44. Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." Open and Big Data (OBD), International Conference on. IEEE, 2016.
45. Shrier, David, Weige Wu, and Alex Pentland. "Blockchain & infrastructure (identity, data security)." Massachusetts Institute of Technology (2016).
46. Esposito, Christian, et al. "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?." IEEE Cloud Computing 5.1 (2018): 31-37.
47. Yue, Xiao, et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40.10 (2016): 218.
48. Liang, Gaoqi, et al. "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks." IEEE Transactions on Smart Grid (2018).
49. Tse, Daniel, et al. "Blockchain application in food supply information security." Industrial Engineering and Engineering Management (IEEM), 2017 IEEE International Conference on. IEEE, 2017.
50. Samavi, Reza, Thomas E. Doyle, and Thodoros Topologlou. "The first workshop on blockchain & eHealth: towards provable privacy & security in data intensive health research." Proceedings of the 27th Annual International Conference on Computer Science and Software Engineering. IBM Corp., 2017.
51. Li, Jiaxing, et al. "Blockchain-Based Security Architecture for Distributed Cloud Storage." Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on. IEEE, 2017.
52. Puthal, Deepak, et al. "The blockchain as a decentralized security framework." IEEE Consum. Electron. Mag. 7.2 (2018): 18-21.
53. Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015.
54. Rahulamathavan, Yogachandran, et al. "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption." 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2017.
55. Ikeda, Kazuki. "Security and Privacy of Blockchain and Quantum Computation." (2018).
56. Wang, Yunsen, and Alexander Kogan. "Designing Privacy-Preserving Blockchain Based Accounting Information Systems." (2017).
57. Wirth, Christian, and Michael Kolain. "Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data." Proceedings of 1st ERCIM Blockchain Workshop

2018. European Society for Socially Embedded Technologies (EUSSET), 2018.
58. Mosakheil, Jamal Hayat. "Security Threats Classification in Blockchains." (2018).
59. Ahire, Jayesh. Blockchain: the future?. Lulu. com, 2018.
60. Shah, Shahid N. "Digital blockchain authentication." U.S. Patent Application No. 15/427,806.
61. Moinet, Axel, Benoît Darties, and Jean-Luc Baril. "Blockchain based trust & authentication for decentralized sensor networks." arXiv preprint arXiv:1706.01730 (2017).
62. Lin, Chao, et al. "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0." Journal of Network and Computer Applications116 (2018): 42-52.
63. Song, Joo Han, Jay Wu Hong, and Joon Sun Uhr. "Method for issuing authentication information and blockchain-based server using the same." U.S. Patent Application No. 15/487,530.
64. Wu, Longfei, et al. "An out-of-band authentication scheme for internet of things using blockchain technology." 2018 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018.
65. Nikouei, Seyed Yahya, et al. "Real-Time Index Authentication for Event-Oriented Surveillance Video Query using Blockchain." arXiv preprint arXiv:1807.06179 (2018).