International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Pedagogy of Blockchain: Training College Students on the Basics of Blockchain

Dr. Karen C. Benson
Georgia Gwinnett College
Lawrenceville, GA 30043, USA

Dr. Binh Tran
Georgia Gwinnett College
Lawrenceville, GA 30043, USA

Ms. Lorraine Jonassen
Georgia Gwinnett College
Lawrenceville, GA 30043, USA

***Abstract* - In whom do you trust? The Internet boom of the 90s promised instant world-wide connectivity, ubiquitous information of all things knowledgeable, and a new level of comprehension beyond what the universe had ever conceived. However, the resultant collateral damage and fall-out of the word-wide-web (WWW) is trust. With the advent of global economies, persistent data collection, and omnipresent cameras, the privacy factor of all-things-data has come-up lacking. The answer to the distrust, doubt, and uncertainty variables found in the Internet equation is Blockchain. Visualized as a pervasive ledger replicated throughout the ether-world, Blockchain is postured to be the harbinger of the way we do business, secure our creative talents, and promote trust in our transactions. Occupants of the college desks of today are the purveyors of tomorrow's technology. As such, how does the instructor impart the concepts of Blockchain to the social media mind-set of today's students? The authors of this paper chose to use the classroom of a medium sized college in the United States to perform the active learning and gamification principles leading to the education of Blockchain. The classroom learning method used was the asynchronous learning method, in which the concepts were categorically divided into blocks. These elementary principles built upon each other, which led to the synergistic knowledge and definition of Blockchain for the student. The instructor performed these exercises in the introductory Information Technology (IT) courses, as well as, upper level Ethics and Professionalism classes, in an effort to discern different levels of cognizance concerning the subject of Blockchain.**

Keywords - Blockchain, college curriculum, informational awareness, cyber-security training, gamification, active learning

I. INTRODUCTION

In whom do you trust? The ubiquity of the Internet and the informational resources it provides has become a part of our daily existence. We depend on the Internet's data from our banking to simple communication with family members. In a world where hackers have become expert voyeurs, how do we maintain the integrity of our data and confidentiality of our lives? The answer is Blockchain: the latest evolution in Internet Technology (IT) which is postured to revolutionize the way we do business, secure our creative talents, and promote trust in our transactions [43]. In the ethernet-society of today where fraud, copyright infringement, and scams are as commonplace as an *HTTP* address, Blockchain was created to bolster confidence and trust in Internet transactions [46]. As such, Blockchain is a redundant, decentralized journal, one which cannot be removed or altered, and is verifiable by other journals in the Cloud. Increasingly important is the necessity to instruct college students as to the pivotal economic change initiated by Blockchain and prepare the graduate for entrance into the workforce [4]. Blockchain promises to be the 1994 equivalent to the Internet boom and the harbinger of digital security and trust [24]. However, will the college students in the classroom today understand the basics underpinning this new technology revolution? And, by which lens should we instruct in the pedagogy of Blockchain?

II. MOTIVATION AND PURPOSE

There is new and emerging technology related to the internet. This disruptive, paradigm shift is one that will eliminate the middlemen, move markets from a centralized to a decentralized standard, and create a bond of trust between parties who will never meet beyond the abstract of the Internet [42]. Rising above the economics and intrinsic problems of ethernet-trust lies the solution of Blockchain, which is prepared to move the Web into the next trajectory. A plethora of issues exists in the world of record keeping, intellectual property, intangibles, and finance which the adoption of Blockchain would alleviated [28]. A trustworthy record available for the public to see, but not delete or alter, is accomplished by the instrument of Blockchain [38]. Because of the many data breaches witnessed recently, the lack-of-trust is logical from a consumer perspective. Consider the following evolution of cyber-attacks which have contributed to the skepticism of consumers and Internet users.

Denial-of-Service Attack (DDoS)

One of the most employed attacks by a hacktivist is an anonymous campaign against a Web server using

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

random *pings* [41]. In an effort to fully consume the network capability of a web server, the hacktivist sends a continual *ping*, making the service unavailable to legitimate users of the Internet server. The pings are not sent from one single malfeasant; however, a conglomerate of computers called *bots* issue the pings. These bot-machines are virtually unaware they are sending the ping activity, as the malware placed on the client contributing to the DDoS is unbeknownst to the computer user. The first DDoS attack was created by a Cornell University student Robert Tappan Morris who was experimenting with a cyber *worm* creation. The experiment resulted in damages estimated to 100 million dollars [13]. This first DDoS attack by Morris heightened the awareness of the vulnerabilities involved with transactions on the Internet.

International Computer Terrorism

In 2014, North Korea hacked Sony servers which stored private employee information, company top-secret documents, and high-level emails [39]. The attack was in retaliation for the spoofed comedy, *The Interview*, which featured a comical plot to kill Kim Jung-un. The malware infiltrated the Sony network and destroyed half of Sony's global network, erasing 3,262 servers and 6,797 personal computers [15]. This type of breach heightens the lack-of-trust in our society when a rogue country can hold our nation hostage because of a personal vendetta. In reality, attempts to prevent cyber-attacks are retroactive as opposed to proactive in the global arena of cyber warfare [18]. Furthermore, the Sony attack advanced the notion of an outside nation obfuscating our First Amendment freedoms and the subsequent responsibility of our government to protect the cyber systems within our borders. The Sony cyberattack raised awareness for the need of a decentralized data storage prototype.

Ransomware

Prior to 2017, viruses, malware, and spam were a mere frustration and annoyance on the part of Internet users [36]. However, data was generally recoverable and business continuity was minimally affected, creating a sense of complacency in the digital world. In 2017, ransomware started a new paradigm shift in the arena of data security threats. No longer was a virus thwarted by antivirus software, as now the hacktivists were able to hold data hostage. Furthermore, ransomware was the first digital malfeasance to use a public key and private key combination to encrypt the user's data. The WannaCry ransomware was the first use of strong encryption algorithms which blocked access to corporate files, entire systems, and retrieval to backup data systems [19]. The resultant options for the victim are: 1) recover from backup, assuming the backup is not also corrupted, and 2) pay the ransom fee, which is not a guarantee that the perpetrator will recover the data and place another time-bomb in the system [36]. The WannaCry ransomware instigated awareness of both data theft and data hostage, coupled with the need for a mechanism to halt alteration of data.

Personal Consumer Records

Concurrent with the theme of data breach and lack-of-trust is the cyberattack on Equifax that affected 143 million United States citizens in 2017 [3]. Reportedly, hackers targeted Equifax because of the *one-stop-shop* capability to grab data on consumers including Social Security and driver's license numbers. Exploiting a weak point in the Equifax credit reporting software, hackers were able to retrieve names, birth dates, addresses, and other personal data. Other past cyber-attacks have eclipsed the Equifax breach in size; however, the damage to consumers in this breach was monumental and will cause long-term consequences for those who had used Equifax for a credit report [40]. In the cyber-attack of Equifax, the public was made aware of the covert cover-up concerning a breach in a Fortune 500 organization in which the public trusted. Furthermore, the Equifax breach is significant because the consumer information gathered was involuntary to the consumer who had no opportunity to decline interaction with the credit reporting agency [35]. The use of encrypting private data with a public and private key would avert this type of security malfeasance. Recently, Equifax has adopted the Blockchain technology with *Bloom*, a Ethereum-based Blockchain application which purports to safely maintain customers personal information and credit [22].

The above cyberattack incidences are by no means meant to be all-inclusive but merely an illustration of the necessity for the technology of Blockchain. Repeatedly, the question of 'In whom do you trust?' resonates with the reader concerning the above cyber-attacks. The authors of this paper intentionally chose these particular data breaches to demonstrate the need for protection and mitigation of data. Of utmost importance in the realm of ether-transactions and Cloud data storage is the trifecta of confidentiality, integrity, and availability (CIA) [20]. Users, consumers, and governments will trust the data, both at rest and in-transit, as the data will be devoid of interference and alteration of content.

III. PROPOSED SOLUTION

Solutions Provided by Blockchain

If there is an assertion of the original intent of the Internet, the foundation would consist of descriptions such as neutral, intuitive, accessible, open, international, military, and purposed researched [26]. Beginning as a tool to deflect tensions between the United States and the Russians during the Cold War, ARPAnet (the original Internet) was not intended to be the world's communication medium [17]. Moreover, in 1975, digital security was deemed sufficient if the server room door was locked [21]. With the explosive advance of economic gain and reliance on the Internet for information and communication, cyber-crimes and criminal networks evolved into a security conundrum. Trust in the Internet became as obsolete as an analog phone-line. However, the Blockchain is resolute in its intent to revolutionize trust in transactions between multiple parties [42].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Healthcare

One only needs to have minimal medical experiences to bear witness to the fact that medical records and patient information are in a constant state of disarray [14]. Electronic Health Records (EHRs) constitute patient data which can be localized in a medical facility or scattered throughout the digital-medical realm. Traditionally, stewardship of records is left to the patient, care-giver, or entrusted to a family member creating a convoluted, machination of data leaving the health-care professional to conjecture as to the medical history of the patient. Challenges of health records include: 1) fragmented patient medical data 2) differing provider and hospital systems 3) patient agency 4) the need for improved data quality and quantity for medical research [14]. By implementation of a decentralized medical ledger, data is replicated through *medical miners* in a cryptographically-secure transaction [14]. The peer-to-peer methodology (as opposed to client-server methodology) secure the medical transaction from malfeasant tampering [16]. Patients have full control to their medical records, since the patient is the holder of his *private key* [30]. A healthcare provider would be the holder of the *public key*. When the patient allows the combination of the public-private key, the medical data would be available for viewing by the healthcare professional.

Cryptocurrencies

As the engine of the car must have wheels and a chassis with which to propel, cryptocurrencies, such as Bitcoin, ride upon the chassis of Blockchain [48]. The basic tenets of Blockchain, including decentralization, data encryption, and anonymity, provide a fertile ground for the growth of crypto currencies. Challenges in the monetary world include bank-middlemen, fees, delayed transactions, and third- party control [48]. Bitcoin became the first application to ride on the chassis of Blockchain, as Bitcoin needed a peer-to-peer mechanism for participants to trade in anonymity and transaction confirmation [10]. Because the contents of every block in the Blockchain are shared in a decentralized environment and available to all miners (nodes), cryptocurrencies share a transparent element that did not occur in the third-party, centralized transactions of traditional banking. With the usage of the digital-wallet (private key) and the exchange of goods (pubic-key), Bitcoin was the first digital currency to be housed on the Internet riding on Blockchain [5]. Other currencies such as Litecoin, Ehtereum, ZCash and Dash exist as competitors to Bitcoin. However, all have the cornerstone signature of Blockchain, where once a digital transaction is added to the ledger, it can neither be edited or deleted [48]. Blockchain works as the digital-ledger, watchdog of Bitcoin, ensuring that people can only spend and send money they actually own. In a world of increasing desire for anonymity, digital currencies provide the cloak of privacy, albeit to the disdain of tax auditors and law enforcement [10].

Intellectual Property and the Financial Sector

Challenges in the realm of health-care and monetary assets also apply in the arena of intellectual property, including the necessity to provide a middle-man to complete a transaction [48]. Accompanying this centralized third-party involvement comes the threat of hackers, single-point-of-failure, and errors/omissions of data. Intellectual property, such as music, games, and software, are a constant target for theft and malfeasance. Enter Blockchain with the capability to store contracts and other articles of intellectual property [32]. As the financial services market is the largest sector of industry, Blockchain stands to cause a major disruption in the financial sector, while boosting the current inefficiencies of banking and contracts. Consider the capability of artists registering their designs and paintings on the Blockchain, such that the authors would be ascertained throughout history. Also, creation of a fraud-proof voting is accomplished through Blockchain, as well as, security for marriage licenses, home titles, notary public, and music applications [8]. The capabilities of Blockchain are endless, and the need for education of today's students is paramount.

IV. CONCEPTS AND INSTRUCTIONAL STRATEGIES

Definition of Blockchain

Visualize an oversized, dusty accounting ledger [44]. Now fast-forward this pictorial into a digital set of blocks containing all transactions from the beginning of time pertaining to a given network. These blocks represent public record transactions and have the characteristic of immutability and veracity, never to be deleted or altered [42]. Furthermore, as transactions (or blocks) are stacked together, they are replicated throughout a decentralized network, beginning with the genesis block (the first block) on January 3, 2009 [4]. The result is a form of distributed ledger comprised of recorded data, monetary transactions, intellectual property, and any type of transaction necessitating a choreography of privacy and trust [38]. The ultimate effort of Blockchain technology is the creation of a decentralized environment where no third party or middleman manages transactions, data, or records [48]. Instead, Blockchain provides security through encryption, anonymity, and data integrity without one organization in control of the transaction.

Centralized vs. Decentralized Rationale

The common denominator of current Internet technology is centralization in which servers store data and clients connect to the server to access information [45]. A prime example is a bank where customer's data is stored on a centralized server at the institution. Customers (clients) have the capability of using their usernames and passwords to access their personal accounts and data online. The Internet, in all its ubiquity, is built on the concept of web-servers, which are centralized locations of requisite data, an easy target for breach attempts [29]. This client-server model has weakened the trust of Internet enthusiasts, as hackers have the inherent capability of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

infiltrating the centralized data and eroding the system of confidentiality, integrity, and trust of customer accounts [42].

Other fallacies of a centralized network topography include a single-point-of-failure in which a hacker can render a website unresponsive with a Distributed Denial of Service (DDoS) attack [35]. This single-point-of-failure is susceptible to errors, omissions, and malicious attacks, with no process for data redundancy [32]. Moreover, in the client-server model, higher processing capabilities are necessary to accommodate the volume of traffic to the server from the external nodes, which can create a bottleneck in data access. Alternatively, during low periods of network activity, the servers are under-utilized, wasting money and resources for the firm. Additionally, the initial high-cost of infrastructure can be a deterrent for those desiring to enter the client-server realm. Finally, in the centralized data methodology, a third-party is responsible for the verification of data, which brings the Blockchain scenario to the forefront [38].

Conversely, the decentralization of data falls into the category of the peer-to-peer methodology of data verification [42]. In this system, all transactions are widely published, verified, and irrevocable on a global ledger, substantiated by an automated consensus of Internet users for public assessment [4]. Using a decentralized system of individual computers (nodes) which host the Blockchain, data is replicated all over the world [45]. This decentralization of data ensures no possibility of hacking the Blockchain and no single-point-of-failure by a server. Additionally, information on the Blockchain is redundant and immutable, allowing for firms to divert security funds normally used on a client-server network topology to profitable spending [45]. Accomplishment of the security of Blockchain is achieved by a cryptographic hash system which ensures that blocks added to the chain will never be changed or deleted [45]. This cornerstone theory of Blockchain will revolutionize the future of tangible assets, contracts, intellectual property (IP), and current third-party verification processes [42].

How Blockchain Functions in the Digital World

The chain-of-events in the Blockchain begin with a transaction, which is represented by a block [10] Block transactions can be public records, intellectual property, medical information, copyright material, or any data which necessitates confidentiality, availability, and integrity (CIA) [44]. As the transactions are added, they are stacked as blocks on-top of each other, replicating to other nodes throughout the network. The header of each block contains a digitally hashed time-stamp and a link to a previous block [4]. Linking the blocks with the hash algorithms secures the older transactions in prior blocks. If an attacker changed or deleted a block, all the hash algorithms afterward would be changed signifying a data breach. With the use of public and private keys, users are allowed to unlock only the blocks that correspond to their private key [32]. As an illustration, a safety deposit box at a bank must have a public and a private key to unlock the box. In the virtual world, the blockchain must have a public key, owned by the Blockchain, and a private key, owned by the user. In this manner, no one can alter or delete contents from the Blockchain. If a user transfers the private key to another user, effectively the contents of that block on the Blockchain are transferred, as well [32].

By use of a hash algorithm, the header of the block is encrypted [12]. The hashing is considered single-directional, meaning once the data is put through the hash algorithm, the data cannot be backward-created from the hash. Take, for example, a meat grinder. You cannot recreate the original piece of meat after the meat has been through the grinder. If you changed the input of meat in any way, the output of hash through the grinder would be different. Similarly, the nodes can compare the output hash (coming out of the meat grinder). If the hashes are different, then that particular block in the Blockchain has been altered. The hash of the header (output from the meat grinder) becomes the identifier of that block in the Blockchain.

Paramount to the security of the Blockchain is the replication of all blocks to peer-to-peer nodes in the network [4]. This begs the question, “Why would anyone want to use their electricity and time to enforce the legitimacy of the Blockchain”? Bitcoin and game-theory become the form of an incentive. When a transaction arrives in need of a block, the nodes are given a cryptographic, mathematical problem to solve. The winner of the math problem is rewarded with a bitcoin, and the transaction is placed in this node’s block. The game-theory provides validation of the transaction and an incentive to the nodes to ensure the legitimacy of the Blockchain. The incentivized game-theory is referred to as mining, and nodes are called miners [27]. These miners will use readily available, specialized software in combination with their computer processors to verify the transaction and solve the mathematical problem. Hence, the backbone of the digital ledger is Blockchain. As wheels and a chassis are to a vehicle, Blockchain is the public ledger on which bitcoin, the Internet of Things, and other digital instruments ride. All transactions since the genesis block (the first block) of January 3, 2009 are recorded and encrypted, available only to users who have a private key. Blockchain ensures a peer-to-peer consensus of confidentiality, integrity, availability, and trust [25].

Reasons to Teach Blockchain to College Students

At the writing of this document, the number of blocks in the Blockchain is 512,173 [6]. Growth on major Blockchains is cresting at over 500,000 transactions a day [9]. Indicators predict the scalability and increased performance of Blockchains will produce creative new approaches in medical, economic, ecosystem, and governmental fields. In a middle-man, centric world, the new paradigm shift will occur where firms will move from a silo-centralized emphasis to a decentralized Blockchain

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

arena. In particular, competitive firms must focus on Artificial Intelligence (AI) and the Internet of Things (IoT) to remain competitive. Blockchain will provide authenticity and privacy to AI without the use of an intermediary, who could be a compromised individual [32]. Consider the country of Chile, which is placing their energy sector on the Blockchain to facilitate the regulation of renewable energy sources [22]. Furthermore, Porsche has plans to implement Blockchain directly into its vehicles, which will give owners the ability to safely unlock their cars from a phone app. Even the gambling market in China has implemented Blockchain technology, seeing the benefits of crypto based casinos. To accommodate these nascent technologies, firms must be cognizant of Blockchain and its ramifications for future profits [9].

Business leaders of tomorrow occupy the college desks of today [47]. Furthermore, college students of today are the users of tomorrow's technology and must be trained to be visionaries and forward-thinkers. The instigation of a culture of innovation in technology begins at the college level, as organizations are seeking college graduates with advanced technological skills [34]. As Blockchain gains momentum and traction, students of all academic disciplines must have a basic understanding of Blockchain [4]. The inherent trust-factor of Blockchain guarantees the perpetuity of growth in this paradigm shift and necessitates the understanding, thereof, in college students who will carry the concept forward into the business world [37].

Active Learning and Gamification

How does the instructor weave the Blockchain concepts into a tapestry with which college students will equate? A plethora of research exists which explores the most effective techniques to produce the highest result from pedagogy. Active learning is a process to engage students in co-creating the pedagogical experience by sharing in the leadership and design of the course, therein, the students will be responsible for their own learning [11]. Conversely, traditional and formal education styles center on the anathema of lecture, note taking, and examination. These learning theories focus on the evaluation of knowledge gained and not practicing the edification for post-graduation. Realistically, the fact that one studies auto mechanics but never touches a car engine, minimizes the usefulness of the education. Students who do not see the relevance of what they are learning become bored, distracted, and indifferent in the classroom environment [11]. Principles of active learning include: 1) students taking the role of class leadership, syllabus creation, and exercise design 2) preparation of college students for their future careers by real-life experience in the classroom 3) a purposeful, participatory education that is rich with student creativity and stretching the limits of their cognitive thinking. However, for a class exercise or experiment to be of worth, certain basic principles must be presented in a logical format; therefore, necessitating an introductory slide presentation [1]. After presentation of the conceptual theories to the class, students design specific games and experiments relating to the material which will promote discovery, understanding, and reinforcement of the concepts.

Similar to active learning, gamification is an experiential learning theory using gaming concepts to interest, engage, and motivate students to come back for more knowledge [2]. As defined by [23] "Gamification is using game-based mechanics, aesthetics and game-thinking to engage people, motivate action, promote learning, and solve problems". Gamification can utilize objects such as a Rubik Cube, simple role play, or even a mock trial. Peer motivation and social interaction invoke team-work participation, which is a necessary skill needed in the workplace after college graduation [2]. Effective gamification enhances the complex relationships within our brains and neural systems to leverage student interest and motivation [7]. Similarly, gamification prompts students to engage with a prepared contextual slide show from the instructor and blend those concepts into practical application through gamification. As educators, our goal is to garner student attention, participation, motivation, and engagement with the intent to educate, without the student even knowing that he/she is actually learning a concept.

The authors of this paper chose to combine the conceptual theories of active learning and gamification to use as a pedagogy for Blockchain. The instructor begins by breaking the concept of Blockchain into smaller learning increments, as shown in an introductory PowerPoint presentation. Each learning increment is taught by a game played by the students and represents a step toward the end-product of Blockchain. Before the gamification begins, a class discussion of the concepts is led by the instructor to filter any misconceptions or confusion concerning the topic. Gamification is broken into the individual concepts of Blockchain, as students divide into varying teams depending on the games played. After each game, a reinforcement discussion is led by the instructor to ascertain that students are not just playing games, but interpolating the concepts relevant to Blockchain. In this manner, the gamification invokes a purposeful, participatory pedagogy in which the student comes back for more.

Choosing of the Blockchain Games

In the decision making of the active-learning and gamification of the Blockchain pedagogy, the authors used specific constructs and ramifications in the choosing of games. First, the game had to be relevant to the particular step in the pedagogy. If the activity did not fit the Blockchain concept, the student might become confused and unmotivated. Next, the game must be scalable and asynchronous. As differing levels of Internet Technology (IT) classes and academic disciplines will be participating, the game could be strengthened or reduced depending upon the academic level. For example, a more difficult Color-the-Squares algorithm game could be invoked for the upper-level IT courses. Asynchronous depicts gamification that will follow in logical sequence,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

building upon each concept one-idea-at-a-time, similar to the construction of a house. Third, the games must use materials that are affordable and readily available for instructors. Expensive and hard to find supplies for games can be counterproductive for the instructor when using the gamification techniques. Implementation of simple materials (such as scissors, colored pencils, and paper) causes the student to focus on the concept of Blockchain and not the intricacies of the game. Fourth, games that have a more linear learning curve (not difficult to explain to the students) offer more time for the students to interact with the activity and learn the concept behind the game. Finally, as classroom time can be limited, this authors chose simplistic games that would impart the concept, and, yet, still leave time for a post-activity discussion.

Logical Process of Gamification for Blockchain

The games chosen by the authors are by no means all inclusive. The object of this paper is to engage instructors to use their creative talents to produce gamification for the pedagogy of Blockchain. Each instructor will tailor his/her active learning technique to appropriately fit the class level and academic discipline. The logical step-by-step, categorical teaching method as proposed by these authors is the asynchronous learning process where concepts are illustrated as blocks, and each block-concept builds upon one another [33 These authors determined the asynchronous-step concepts needed in the pedagogy of Blockchain as the following order: 1) introduction to the Cloud 2) introduction to algorithms 3) introduction to hash algorithms 4) introduction to private – public key cryptography 5) introduction to Blockchain. However, other instructors may deem it necessary to invert steps or add concepts/games as necessary, depending upon the academic discipline and level being taught. A brief scenario and concept behind each game follows.

Introduction to the Cloud

Many younger students are not cognizant of past technologies, why these technologies are no longer in use, and where the current technology data is currently stored. The authors of this paper felt the first building concept-block should be current data location storage and privacy issues of the Cloud. In doing so, the first game begins with objects which utilize past technologies. The authors created a PowerPoint presentation of examples, such as a rotary phone, a printed map, a camera that uses film, taxis cars, and board games. The final slide in the PowerPoint presentation is a picture of a Google data center. This slide begins to stimulate a discussion concerning these particular antiquated, technology items which are now located in a data center. The post-discussion questions posed to students include: 1) Is your information secure in a data center? 2) Why are these items not still in use? 3) What items do you use today that may be in a data center tomorrow?

Introduction to Algorithms

The next step in the pedagogy of Blockchain is the introduction of algorithms. This authors found it necessary to show students they, unknowingly, use algorithmic-thinking in their everyday life. The student can then transfer this concept into algorithms necessary for Blockchain instruction. Algorithms emphasize the existence of a procedure, plan, and process that is necessary to solve a particular problem [1]. Therefore, in this step towards the understanding of Blockchain, this instructor used a triangle-peg game to show students there was a step-by-step process with which to eliminate the golf tees. Students work in pairs to solve the problem of eliminating all but one golf tee in the triangle peg. While one student would read the predefined algorithm, the other student performed the transaction. In this manner students learned pairing of teamwork and proper following of the written algorithmic instructions. The exercise used gamification, as the students were in a timed contest against each other. The winner receiving a “bitcoin” represented by a piece of candy.

Introduction to Hash Algorithms

The next step in the progression towards the pedagogy of Blockchain is the introduction to cryptography and hash algorithms. In this manner, students learn about the means and mechanism of securing and replicating transactions through a hash algorithm, which is the cornerstone of Blockchain. As the class divides into teams of two, this game has one student coloring different cells from a large block and another student writing the directions of how that particular pattern of cells was derived. In this game, teamwork is involved and the introduction to algorithmic coding. After various cells on the page have been colored and the map of the colored cells has been written, the instructions are then passed to another team of two. This opposing team will use the written instructions from the previous team to try and replicate the exact colored, cell pattern. This game is an example of a symmetric key in cryptography in which both the sender and receiver should have the same identical key [42]. Opposing teams attempt to replicate the algorithm written by the previous team. The subsequent results will determine if the previous team wrote the instructions incorrectly, or if the instructions were not followed by the current team with precision.

To demonstrate a hash, students are asked to cut the colored squares out of the single block. Subsequently, the students scramble the cut squares. This depicts a hash algorithm in which the team knows the input into the hash, but the competing teams are not able to determine the original input of colored blocks into the algorithm.

Asymmetric Key Encryption

A general understanding concerning the public and private key is imperative in the understanding of Blockchain. As alluded to earlier in this document, the public key is used to open a block in the Blockchain. The private key is held by the owner who created the content to be placed in the block. In this manner, both a public and private key are necessary to open and view a transaction in the Blockchain [43]. Many instructors use the example of email, where the email address is the public

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

key, and the password to the email account is the private key [4]. Both the email address and the password to the email account is necessary for one to view the contents in the email account. These authors chose to use the example of a safety deposit box gamification, in which both a bank public key and an owner private key is necessary in order to view the contents in the safety deposit box.

Blockchain

The Blockchain study reaches its apex with the final active learning exercise which involves a role-play type of gamification. Synthesis places the abstract puzzle pieces of previous games into the one synergistic whole, which creates the Blockchain phenomenon. The culmination of the above precepts is incorporated such a manner that the student understands the categorical process behind Blockchain. In this role play activity, students are divided into groups that will present transactions which need protection by Blockchain. Three students from the class are designated as *miners* and sit at the front of the classroom waiting for users to approach the table with a transaction. These miners have a set of blocks which will contain the transactions from the students, as well as, pieces of a chain linking the miners together. In this manner, replication of the Blockchain is exemplified, and miners are given bitcoins (pieces of candy) when transactions are added. Groups of students are assigned differing transaction types. For example, one group depicts intellectual property by writing a rap song about the college. Another group demonstrates the importance of placing serial numbers of concert tickets in the Blockchain. These authors have found that students enjoy creating their own transaction creation for the Blockchain. However, it is imperative that students be able to explain the process by which they are adding a transaction, and why trust is necessary in this transaction.

V. CONCLUSION

As the subject of Blockchain is an emerging and fertile research domain, future studies can expound on the precepts and pedagogical constructs delineated in this qualitative paper. Specifically, a quantitative study to determine the amount of knowledge gained from the active learning process would be enlightening in future teaching. Furthermore, statistics could be broken into gender, age, college levels, and college majors. More advanced games could be designed for the advanced IT courses at the college. Depending on the time allowance, students could compete with well-defined Blockchain skits to advance the topic. Finally, students could research the different concepts of Blockchain and present gamification to the class for instruction in that concept.

This paper was not meant to ascertain the efficacy of Blockchain but to influence instructors in the pedagogy of Blockchain to college students. As there exists a preponderance of advanced research topics concerning Blockchain, the authors' intent was to focus on the basic precepts of the topic and the collegiate instruction thereof. The authors believe the application of the interactive and gamification learning theories, coupled with the asynchronous learning system, can be applied to bring similar benefits in the pedagogy of other disciplines. Paramount is the necessity of college students to comprehend the basic principles of Blockchain and use the information to advance this topic into the public and private sectors upon graduation. This goal is accomplished through a detailed level of understanding by the instructor and, subsequently, a categorical teaching method to the college students.

REFERENCES

[1] Anderson, R., Anderson, R., Davis, K. M., Linnell, N., Prince, C., & Razmov, V. (2007). Supporting active learning and example based instruction with classroom technology. *ACM SIGCSE Bulletin, 39*(1), 69-73. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.1639&rep=rep1&type=pdf

[2] Banfield, J. & Wilkerson, B. (2014). Increasing student intrinsic motivation and self-efficacy through gamification pedagogy. *Contemporary Issues in Education Research (Online), 7*(4), 291.

[3] Bernard, R. S., Hsu, T., Perlroth, N., & Lieber, R. (2017). Equifax says cyberattack may have affected 143 million in the U.S. *The New York Times.* Retrieved from https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[4] Bheemaiah, K. (2015). *Why business schools need to teach about the Blockchain: An overview of Cryptocurrency and Blockchain technology based on business initiatives and models.* Retrieved from SSRN: https://ssrn.com/abstract=2596465

[5] Blockchain.info. (2017). Blockchain Luxembourg S.A. Retrieved from https://blockchain.info/

[6] Blockchain Network Data. (2018). *Blockchain info.* Retrieved from https://blockchain.info/blocks

[7] Buckley, P. & Doyle, E. (2016). Gamification and student motivation. *Interactive Learning Environments, 24*(6), 1162-1175. doi:10.1080/10494820.2014.964263

[8] Crosby, M., Pattanayak, P., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied innovation, 2,* 6-10. Retrieved from http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

[9] CoinDesk.com. (2017). *Blockchain 101.* Retrieved from https://www.coindesk.com/terms-conditions/

[10] Dack, J., & Letten, A. (2018). *Cryptocurrency 101: Bitcoin and blockchain explained*. Retrieved from https://uk.lush.com/article/cryptocurrency-101-bitcoin-and-blockchain-explained

[11] Davidson, C. (2018). Key point about active learning. *Inside Higher ED.* Retrieved from https://www.insidehighered.com/views/2018/01/25/how-think-about-active-learning-and-its-benefits-opinion

[12] Economist.com. (2015). *Blockchains, the great chain of being sure about things.* Retrieved from https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

[13] Eisenberg, T., Gries, D., Harmanis, J., Holcomb, D., Lynn, M. S., & Santoro, T. (1989). The Cornell commission: On Morris and the worm. *Communications of the ACM, 32*(6), 706-709. Retrieved from http://nnt.es/The%20Cornell%20Commission%20On%20Morris%20and%20the%20Worm.pdf

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

[14] Ekblaw, A., Azaria, A., Halamka, J.D., & Lippman, A. (2016). A case study for Blockchain in healthcare. "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & Bid Data Conference, 13*, p. 13. Retrieved from https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[15] Elkind, P. (2015). Inside the hack of the century. *Fortune Magazine*. Retrieved from http://fortune.com/sony-hack-part-1/

[16] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications, 111*(7), 1-6.

[17] Floridi, L. (1995). Internet: Which future for organized knowledge, Frankenstein or Pygmalion? *International Journal of Human-Computer Studies, 43*(2), 261-264.

[18] Haggard, S. & Lindsay, J. R. (2015). North Korea and the Sony hack: Exporting instability through cyberspace. *East-West Center Asia Pacific Issues.* Retrieved from https://scholarspace.manoa.hawaii.edu/bitstream/10125/36444/1/api117.pdf

[19] Hampton, N., & Baig, Z. A. (2015). *Ransomware: Emergence of the cyber-extortion menace*. The Proceedings of the 13th Australian Information Security Management Conference held from 30 – November – 2 December, 2015 (pp. 47-56). Edith Cowan University Joondalup Campus, Perth, Western Australia.

[20] Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. (2018). Answering Key Global IT management concerns through IT governance and management processes: A COBIT 5 View. *Proceeding of the 51st Hawaii International Conference on System Sciences.* Retrieved from http://hdl.handle.net/10125/50554

[21] Ilyas, M. (2015). Cyber-security. University of Dammam – College of Computer Science and Information Technology. Retrieved from http://academia.edu

[22] James, A. (2018). Equifax data breach opens door for Blockchain credit apps. *Bitcoinist.com.* Retrieved from http://bitcoinist.com/equifax-data-breach-opens-door-for-blockchain-credit-apps/

[23] Kapp, K. M. (2012). *The gamification of learning and instruction; Game-based methods and strategies for training and education.* San Francisco, CA: John Wiley & Sons.

[24] Keys, A. (2018). 18 Blockchain predictions for 2018. *Consensys Media.* Retrieved from https://media.consensys.net/18-predictions-for-2018-7a376ea7bd4b

[25] Kiayias, A., Koutsoupias, E., Kryopoulou, M., & Tselekounis, Y. (2016). Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation* (pp. 365-382). ACM.

[26] Kilaz, I., Onder, A., & Yanik, M. (2014). Manpower planning and management in cyber defense. In 13th European Conference on Cyber Warfare and Security ECCWS-2014. The University of Piraeus Piraeus, Greece (p. 116). Retrieved from academia.edu

[27] Kroll, J. A. (2013). *The Economics of Bitcoin Mining.* New Jersey: Princeton University.

[28] Ledracapital.com. (2014). *The mega-master Blockchain list.* Retrieved from http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list?rq=blockchain%20list

[29] Lewis, A. (2015). *A gentle introduction to blockchain technology.* Retrieved from https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/

[30] Linn, L. & Koo, M. (2016). Blockchain for health data and it potential use in health IT and healthcare related research. In: ONC/NIST Use o Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (2016). Retrieved from https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf

[31] Loomis, K.D. (2000). Learning styles and asynchronous learning: Comparing the LASSI model to class performance. *Journal of Asynchronous Learning Networks, 4*(1), 23-32.

[32] Marr, B. (2017). A complete beginner's guide to Blockchain. *Forbes.* Retrieved from https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#3794796f6e60

[33] MacDonald, T. J., Allen, D. W., & Potts, J. (2016). Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. *Banking Beyond Banks and Money.* Cham, Switzerland: Springer International Publishing

[34] Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. Journal of Information Privacy & Security, 9(1), 47-67. doi:10.1080/15536548.2013.10845672

[35] Miller, L. (2018). Cybersecurity insurance: Incentive alignment solution to weak corporate data protection. *Social Science Research Network.* Retrieved from https://ssrn.com/abstract=3113771. doi:10.2139/ssrn.3113771

[36] Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017). *International Journal of Advanced Research in Computer Science. 8*(5), 1938-1940.

[37] Perlroth, N., Scott, M., & Frenkel, S. (2017). Cyberattack hits Ukraine then spreads internationally. *The New York Times.* Retrieved from http://www.vis-am.ch/uploads/allegati/Cyberattack_Hits_Ukraine_Then_Spreads_Internationally_-_The_New_York_Times.pdf

[38] Prabhu, Karthik & Prabhu, Keerthi. (2017). Converging Blockchain technology with the Internet of Things. *International Education & Research Journal, 3*(2), 122-123. Retrieved from http://ierj.in/journal/index.php/ierj/article/view/727/704

[39] Roberts, J. J. (2016). Three security breaches that freaked out U.S. companies. *Fortune Magazine.* Retrieved from http://fortune.com/2016/09/21/biggest-security-breaches/

[40] Shackelford, S., & Brady, A. (2018). Is it time for a national cybersecurity safety board? *Albany Law Journal of Science and Technology.* Retrieved from https://ssrn.com/abstract=3100962

[41] Shakarian, J., Shakarina, P., & Ruef, A. (2015). Cyber attacks and public embarrassment: A survey of some notable hacks. *Elsevier SciTechConnect.* arXiv preprint arXiv: 1501.05990.

[42] Swan, M. (2015). *Blockchain: Blueprint for a new technology.* Sebastopol, CA: O'Reilly Media.

[43] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution; How the technology behind bitcoin is changing money, business, and the world.* New York, New York: Penguin Random House.

[44] Walport, M. (2016). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science.*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[45] Watney, M. (2017). *Blockchain for beginners*. Copyright by Mark Watney. Kindle Books: Amazon.

[46] Weber, I., Xu, X., Riveret, R., Governatori, G., Pnonmarev, A., & Mendling, J. (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. In: La Rosa M., Loos, P., Pastor O. (eds) Business Process Management. BPM 2016. Lecture Notes in Computer Science, v0l 9850. Cham, Switzerland: Springer International Publishing.

[47] White, G.L., Hewitt, B., & Kruck, S. E. (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education, 24*(1), 11-16. Retrieved from http://www.jise.org

[48] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is the current research on blockchain technology? – A systematic review. *PloS One, 11*(10), 1-27. doi:10.1371./journal.pone.0163477