International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

The Effectiveness of Using Blockchain Technology in Building High-Quality Educational Content Based on A Participatory Learning Environment and Its Impact on Increasing Student Achievement

Amr El Koshiry [1,2]*, Entesar Eliwa [3,4], and Hala Abdel Hameed[5,6]

Submitted: 14/10/2022 **Revised:** 12/12/2022 **Accepted:** 26/12/2022

Abstract: This study aims to measurement the effectiveness of using blockchain technology in building high-quality educational content based on a participatory learning environment and its impact on increasing student achievement. In this study, many existing learning techniques and models have been discussed and presented with their detailed comparison as learning rate of digital data growth has increased using blockchain and IoT. Many western countries have already upgraded their blockchain based learning systems to the international standards. In methodology, we used python language for the implementation of blockchain based smart system application with IoT benchmarking to digitalize the content-based learning, it also provides a roadmap for the new digital ecosystem which is trained using the automation based on blockchain. Blockchain innovation has related to Internet of Things for quite a while now for smart education. There are many issues that are upset the execution of IoT applications at an enormous scope. Overviews and studies from numerous sources uncover that security dangers and information protection are yet the essential worries. These issues are notable, and arrangements exist for these issues in the IT business. However, traditional IT security solutions cannot be applied to IoT for various reasons spanning from type of devices to sheer volume of devices. Unfortunately, like in any other industry, E-Learning is often disregarded in the IoT domain as well, and most of the resources are allocated to application development and device hardware. So, the search for a silver bullet to overcome these inhibitors has been going on for a while. After Blockchain Technology became prominent, people started to realize the potential of the underlying distributed ledger (blockchain) technology and considered it as a true innovation. Rather than facilitating a peer-to-peer digital payment system involving a cryptography, the blockchain technology is viewed as a mechanism that provides device identity, secure data transfer, and immutable data storage. All these features can be implemented without any centralized authority and a completely transparent system with auditable cryptographic proofs. Our aim through this research paper is to get a deep level understanding of the blockchain technology and study some of the widely used blockchain frameworks including different technology like Big-data and Machine Learning. We will further examine the exclusive features offered by each of these frameworks and define their target use cases. Ultimately, our aim is to determine the most suitable blockchain architecture for the IoT ecosystem. A high-level comparison of the researched architectures will be provided so that managers and developers can quickly decide on a suitable framework for their application or use case depending upon the requirements. For each architecture, a set of sample use cases and on-going research will be discussed to get an idea of the usage of that architecture in the real world.

Keywords: *Transaction, Internet of Things, Blockchain, Big-data, E-Learning, Education, Smart Education, Deployment.*

1. Introduction

Undoubtedly IoT solutions have provided great benefits and their incorporation into various sectors like financial technology, healthcare, manufacturing, retail, transportation, and supply chain can herald radical transformation as mentioned in [1]. These solutions offer enhanced tracking methodologies which can be useful in the healthcare industry where patients can be closely monitored by the doctors using monitoring devices, sensors and alerts can be sent during an emergency. Given the low costs of infrastructure and the rapid growth in the number of connected devices, ubiquitous networks are emerging. IoT solutions also help optimize the processes thereby reducing the costs and enhancing the production rates as mentioned in [2]. Although there are several benefits of these solutions, there are several factors which thwart us from tapping their full potential. The lack of sufficient knowledge on interoperable technologies and the associated standards also poses a setback for several organizations. Managing the huge volume of data generated by the IoT devices is also an arduous task demanding advanced algorithms and protocols to operate on the data as mentioned in [3]. With IoT, the conventional routes of information exchange are expanding, and this is raising concerns in the security space since there are a lot

[1] *Department of Curricula and Teaching Methods, College of Education, King Faisal University, P.O. Box: 400 Al-Ahsa, 31982, Saudi Arabia*
[2] *Faculty of Specific Education, Minia university, Egypt. aalkoshiry@kfu.edu.sa, al_koshiry@mu.edu.eg*
[3] *Department of Mathematics and Statistics, College of Science, King Faisal University, P.O. Box: 400 Al-Ahsa, 31982, Saudi Arabia.*
[4] *Department of Computer Science, Faculty of Science, Minia University, Egypt. eheliwa@kfu.edu.sa, entesar.eliwa@mu.edu.eg*
[5] *Faculty of Computer and Information Systems, Fayoum University, Egypt.*
[6] *Khaybar Applied College, Taibah University, Saudi Arabia.; Ham07@fayoum.edu.eg*
* *Correspondence: Amr Mohamed El Koshiry, E-mail addresses: aalkoshiry@kfu.edu.sa, Tel. No.: +966-054081976.*

of avenues for exchanging information and all of the transmitted data needs to be secured. Digital technology has been available for over half a century. The widespread use of digital technology in business is about twenty-five years old – since the advent of the Internet-Of-Things and Blockchain. It is only in the past decade that institutions have begun to formalize how our knowledge for future generations will be preserved as performed in [4]. Each of the afore mentioned efforts is part of an iterative process. Researchers develop digital IoT-based blockchain solution for learning practices for their research with constraints imposed by the medium, assistance from exemplars and peers, and with direction from granting agencies as mentioned in [5]. They can apply these practices to their personal lives and provide feedback to the process based on these experiences, making small changes to the system to fit their needs. Thus, the digital environment is a creation of human activity that is both technical and social solution for blockchain as given in [6]. Solutions require improved understanding of the communication that crosses organizations and that recognize individual needs and existing record preservation systems have been depicted in [7]. The efforts at this early stage of the paradigm shift will influence future generations' perceptions of who we were, what was done, and why. However, it is intuitive that the data augmentation is more advantageous on smaller sets which can be more easily enriched with new information. While the visual quality of the synthetic samples is negatively affected by the smaller training set, the generated sequences appear to carry enough information to have a beneficial impact. Moreover, a classifier's proneness to overfitting rises with decreasing amount of training samples, increasing the need for any regularizing input as given in [8].

1.1. Problem Statement

The blockchain technology is primarily used to facilitate the secure transaction of financial assets between two parties. Instead of trusting a third party, the blockchain technology leverages the use of hash functions and distributed systems to provide a cryptographic proof for these electronic transactions. Blockchain is a large database (or ledger) consisting of linearly attached blocks and this ledger is shared by all the distributed devices in the system, which are otherwise called as nodes. Here, each block corresponds to a set of transactions that are being processed at a certain point of time. This block contains two pieces of information – the details of the transactions, and the hash value, that is calculated from the data available from the previous block. The hash value of the previous block is calculated from the data provided by the block before it and this whole process begins from the genesis block, the hard coded first block of a blockchain. This ensures that the data in the overall blockchain is unaltered and final. This blockchain which is shared by all the nodes contains every transaction that has ever happened right from the first ever transaction to the latest one. In the recent past, there have been several distributed denials of service (DDOS) attacks which were launched by compromising millions of IoT devices. One such attack with a strength of 1.2 Tbsp. was conducted against the DNS service provider disrupting the access to several websites. The botnet comprising of IoT devices include digital video recorders, routers and compromised web cameras infected by the Mirai malware as mentioned in [9]. The DDOS attack on Brian Krebs' security blog was also a powerful one with a strength of 665 Gbps and involved millions of compromised IoT devices. Security Researchers believe that the attack groups targeting IoT devices are proliferating by the day. With the steady rise in IoT devices, they form easy targets for attackers since several users do not change the default passwords of the devices and also do not update the firmware as the patches are rolled. The Open Web Application Security Project (OWASP) has recently released a list of top 10 vulnerabilities in IoT devices. "Insecure web interface, insufficient authentication/authorization, insecure network services, lack of transport encryption, privacy concerns, insecure cloud interface, insecure mobile interface, insufficient security configurability, insecure software/firmware and poor physical security" have been identified as the top 10 vulnerabilities in IoT devices as mentioned in [10].

- Technologists need to maintain the IoT-based blockchain system for learning and research. The archivists are the caretakers and the exemplars that practice and create practices for others to emulate for content based learning.
- The content based education system that should be built with blockchain must not only know the technology, but law and policy for all the entities that the archives are intended for (journals, government studies, privately funded organizations) but also the student achievements.
- The blockchain based learning system should also determine the behavior strongly influenced by their field, discipline, associates, and accepted social behavior.
- The research also ultimately responsible for ensuring archives are managed both locally and on a remote system (at least initially). There should at least be an explanation of how these aspects fit together to ensure that information stored today will be available for years using blockchain.
- The research should also calculate the depth histogram and thresholds depth learning system and assume that the records are in pipelines all the time and the rest of learning material is considered important as well.

1.2. Aim of Study

Several organizations are conducting research on leveraging the blockchain technology, primarily used in electronic financial transactions, as the core principle to exchange information between these internet-of-things. Companies from various industries like healthcare, electronics, telecommunications, networks, transportation, and banking are coming forward to make this idea a reality. It is believed that the blockchain technology can be very efficient in exchanging information between devices and companies with minimal cost and complexity while maintaining trust, accountability, and transparency. However, the blockchain technology used in Blockchain cannot be directly applied for internet-of-things. Depending on the type of company and the information being exchanged, there are many issues that need to be resolved. Following is some of them:

- Unique Identification for High-quality education system: Each device connected to the internet should have a unique identifier. This Id is used to track the device in the ledger. Usually, this is achieved by assigning a pair of keys (public and private) to each device. However, devices like lights and CCTV cameras might not have built-in capacity to manage these cryptography keys. IP address cannot be used for this purpose due to their dynamic nature and the presence of private IP addresses.
- Double Spending issue: Mining and proof-of-work functions are used eliminate the transactions involving double spending. This is only useful while transferring assets with monetary value. In other cases, involving the transfer of data, the same information from a device can be sent to different devices at any time. But there should be some protocol to build a blockchain and append blocks to it in a systematic manner.
- Cryptographic Computation for High-quality education system: The devices in IoT may not have the computational capacity to perform complex cryptographic calculations involved in the blockchain model. Since it is estimated that 50 billion devices will be connected to the internet by 2025, there should be enough devices online at any point of time, to perform these calculations.
- Information Exchange for High-quality education system: While it may be relatively easy to transfer the information and maintain a ledger for devices of the same type, IoT will have different types of devices and each device might store/process different kinds of information. Maintaining all this information in a single ledger might get complex and difficult to manage. Alternatives like sidechain can be utilized to solve this problem.
- Trusting the devices: More devices mean more risk. Each device might have different vulnerabilities and if they are exploited successfully by an attacker, it might lead to a complete takeover of the device. Blindly trusting all the devices in the blockchain might be a problem.

The research examines how rules, resources, and training can be communicated to research faculty to raise overall awareness and improve digital preservation in the conduct of research using blockchain. A goal of this study was to find an approach to influence better digital preservation at the institution through communication with the knowledge that faculty are strongly influenced within their discipline using blockchain. Since faculties are evaluated, supported, and tenured at the department level, messages tailored at the department level should be more successful than if from the college or university level. To understand how units, interact with each other with respect to data management, the study asked how researchers in the three departments manage their own digital data using blockchain. Although there are many other issues and weaknesses surrounding this technology, it is believed that its advantages outweigh these issues by a large margin.

2. Background

The idea behind building this digital or virtual technology is to build a decentralized system which would allow the technology to be electronically transferable with negligible or no transaction fees. This is the first peer-peer network which powers its users with no central authority or banks as mentioned in [11]. These blockchain are built out of a big-data protocol. According to this protocol, there would be a definite number of blockchain which can be produced (mined) which is 21 million. Blockchain has users that are widespread across the world, and it is not controlled by any single person. From a user’s viewpoint, bigdata is an application which provides a wallet and users the ability to make transactions among each other as mentioned in [12]. To perform transactions, the users are free to use any software they want, if the software is compatible to, and complies with the rules of the big-data protocol. This electronic payment system is built on a cryptographic proof rather than trust, which is why the need of a third party is eliminated as mentioned in [13]. The transactions made are practically impossible to reverse or destroy. The big-data network shares a public ledger called the blockchain.

The approach is to use the IoT and the blockchain for developing the content based learning for students involving theory to represent a construct of the interrelated processes that describe the digital preservation process of learning material. Universities record preservation and management is at the core concept of digitalization as mentioned in [14]. In this work [15], digital preservation is being performed for the three major digital libraries of journals using blockchain and IoT where scope transcends the technology that we use to navigate it for student learning. The content based digital learning is based on decisions by the creators of the artifacts for different digital libraries, the system which manage it, the techniques which maintain the systems and that creates policy and funding for it. Researchers in [16] are creators of the information and, as stated earlier, have the greatest responsibility to establish the value of digital artifacts for student learning using blockchain. Since the digital age will rely on the way we preserve our data, preservation practices must evolve to satisfy societal needs. Given the transient nature of the digital world, our decisions of what data to save has fundamentally changed. DOI is a mature theory, elements which quantified using digital system analysis for record digitalization. The complexity requirements are not constant, and they keep changing with the number of bigdata's mined as mentioned in [17]. They must have a certain number of zeroes at the beginning of the block. To attain this, the miner must try using different values of the random nonce as mentioned in [18].

The research has been designed solely for the journal of digitalization plan and activity clusters with respect to digital learning activity for students. Journal Activity Theory provides a framework that includes rules, resources, tools and culture for the digitalization of student learning using blockchain. Both can explain the introduction and diffusion of digital learning practices throughout the different journal by digitalization as mentioned in [19]. This is what would consume a lot of computational power and capacity. At a point where the miner successfully finds a nonce with the desired complexity requirements, it is announced to the network as mentioned in [20]. The other miners who are on the network validate this block and try finding a new block with the block which was just released on the network as their last component. When a miner successfully verifies or validates transactions and hence finds new blocks, he is rewarded with a certain number of blockchain as mentioned in [21]. This hashed block is made public and would be available on the shared ledger which the entire network relies on.

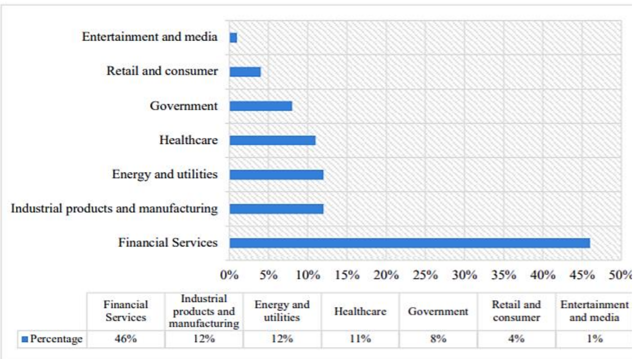

Fig. 1. Industries adopting blockchain technology [22]

Since this signature is verified by many nodes in the network, there is no possibility of a faulty transaction getting processed as a valid transaction. In short, there is no way for a node to pretend as another node. Following is an illustration of the digital signature verification process in the Big-data network:

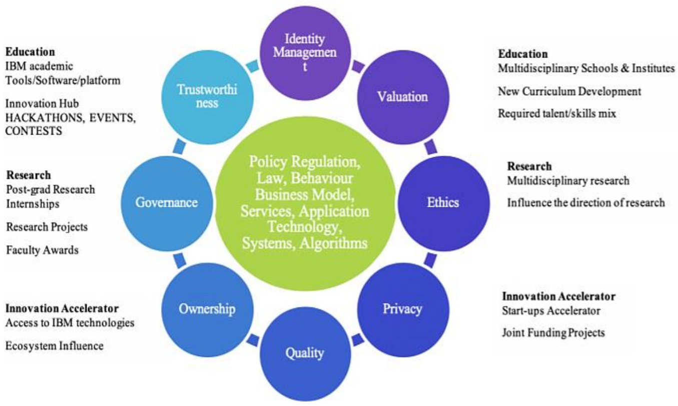

Figure 2. Digital signature of blockchain and data transparency for research and smart education [23].

The GHOST protocol implemented by blockchain involves seven levels. Each block states its parent and the number of uncles. The uncles of a block have the following features. The uncle block must be a direct child of the ancestor of the block B. The generation of the ancestor could lie between 2 and 7 but the uncle cannot be an ancestor of B. The uncle block does not necessarily have to be verified previously but has to be a valid block header. Each uncle block needs to be different from the uncles in the same block and those of the previous blocks. The uncle block's miner receives 93.75% of the block reward and an additional 3.125% reward for each uncle it mines as mentioned in [24].

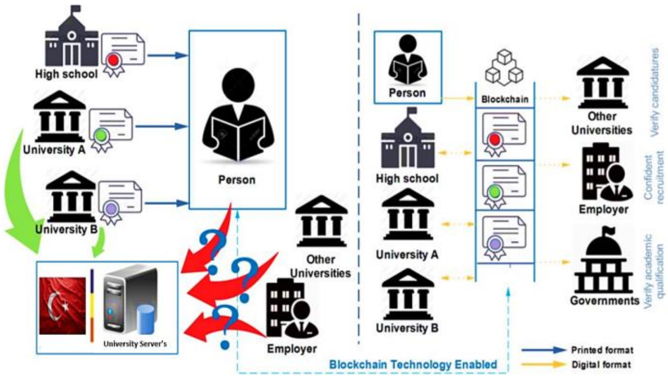

Fig. 3. The Blockchain technology for Turkish high schools and universities [24]

3. Materials and Methods

The idea behind "high-quality education system" is to change the behavior of something, based on the input (data), when certain conditions are fulfilled. In the context of a distributed ledger system, a smart education is a piece of code which is stored at a particular address on the blockchain. The address for storage is decided when creating a smart education. When a transaction is sent to this address, the code in the high-quality education system gets executed, which might result in reading/writing data to the distributed ledger on which it is present. A smart education can make decisions, read data, and execute other contracts. While dealing with IoT devices, we would essentially want to perform some action based on the received data. For example, imagine a lux sensor that sends data to a system every one minute. Based on this data, that system will have to switch on/off the lights surrounding that sensor. If all the devices are connected, this might be possible in a normal setting. But, for this to work with an application built on the blockchain technology, high-quality education system is required because they provide the logic for the on/off operations. Fortunately, Blockchain's implementation of high-quality education system is completely deterministic and isolated i.e., a smart education won't have access to data which is external to the blockchain. It can only work with on-chain data. After coding a smart education in a high-level language like Solidity or Serpent, the code will be compiled into EVM (Blockchain Virtual Machine) bytecode and will be stored at an address on the blockchain. It gets invoked when a transaction is sent to that address.

Researchers, technologists and administration should have a dialogue on campus to resolve and learn best practices using blockchain. This is achieved on a campus through motivation and leadership. In the public and private sector have begun to develop the framework, policies and practices to address the issue with teachers. We used dataset to preserve archived data, but it also provides a roadmap for the new digital ecosystem using blockchain. It offers a framework that can be used to identify roles and responsibilities within a bounded system with teacher's involvement. The digital libraries are developing specific guidance for preserving digital artifacts using blockchain. Both the finance and science and technology have created mandates that require the consideration of an all-inclusive data management system by employers, administrators, technologists, and organizations. Finance ministry and science ministry requirements are important events in the trend to encapsulate and maintain humanity's knowledge digitally using blockchain.

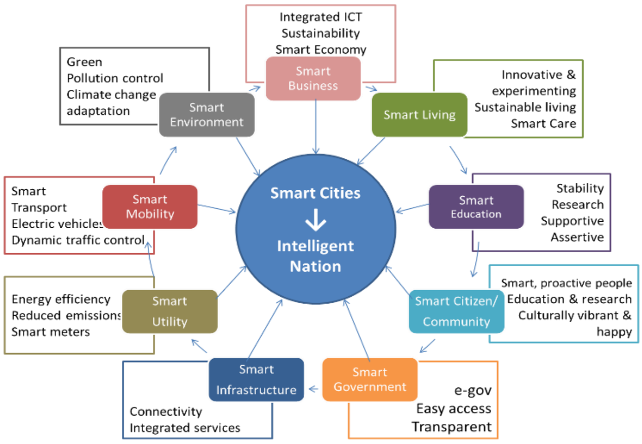

Fig. 4. The major benefits of blockchain in high-quality education system.

3.1. *High-Quality Education System in Blockchain*

High-quality education system, in order to perform an action, might need data from external location. Cryptographic signatures submitted by outside systems called 'Oracles' are relied upon to interact with the real world. So, oracles are trusted systems which provide signed data to high-quality education system from the outside world. When triggered, high-quality education system is executed on all the nodes on which the ledger is present. But, when the code is based on advanced logic, the integration of high-quality education system in the blockchain might get complicated. Smart oracle is a way of implementing high-quality education system without making the consensus network complicated. It is a separate trusted entity which can gather information from the outside world and execute the code which pertains to the high-quality education system. So, the code for the high-quality education system is separated from the blockchain. Instead of being executed on all the nodes, the code gets executed on a single oracle. Although this concept is being discussed for a long time now, there are only a handful implementations on this. Currently, Contracts and Reality Keys seems to be the most advanced companies in providing these oracle services. Following is some of the data sources that are supported by the contract service.

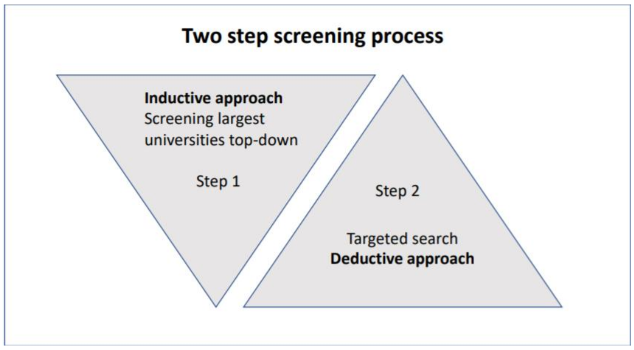

Fig. 5. Data flow in high-quality education system supported by blockchain.

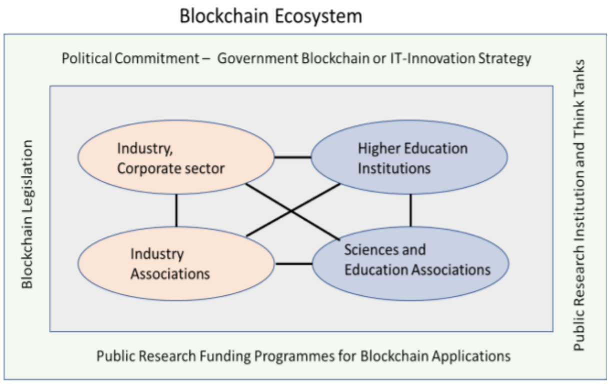

Fig. 6. Working of blockchain service for implementation of higher education.

URL is the most generic data source which can be used to access any API and any page on the internet. Oraclize will fetch the responses for these HTTP requests and feed it to high-quality education system with an attached proof. Blockchain related data which cannot be accessed by high-quality education system directly can also be fetched through oracles. Data like blockchain height, difficulty, and balance of a specific address can be retrieved. To get data about the weather in a location, solution to mathematical problems, and any other simple statistics and data analysis, a computational knowledge engine like Wolfram Alpha can be used as a data source. The response from the Alpha API will be sent to the high-quality education system. If the high-quality education system requires a file which is stored in a distributed fashion using the Inter Planetary File System (IPFS) protocol, the multihash of that file can be used to retrieve the contents of that file. So, IPFS can also be used as a data source.

Table 1. Sectors, Behavior types and Examples of Interpersonal E-Learning using Blockchain.

Sector	Behavior types	Usage of Blockchain
Dominance/ Cooperation	Leadership	YES
Cooperation/ Dominance	Helpful/ Friendly	YES
Cooperation/ Submission	Understanding	YES
Submission/ Cooperation	Pupil Responsibility/ Freedom	NO
Submission/ Opposition	Uncertain	NO
Opposition/ Submission	Dissatisfied	N/A
Opposition/ Dominance	Admonishing	YES
Dominance/ Opposition	Strict	NO

The expectancy component is a combination of self-efficacy and attribution theories. Self-efficacy is about the perception of one's own competence. It is related to attribution theories because it is about control of learning beliefs. Both self-efficacy and attribution have to do with own perception of capacities to perform for a specific task. This is based on character combined with early experience, which is influenced by interaction (by example pupil teacher interaction). Attribution, the other part of the expectancy component of motivation is about locus of control, controllability and stability.

3.2. Public vs Private Blockchains in Higher Education Commission

Public blockchains can be accessed by any user across the world, valid transactions can be sent and added to the blockchain. Also, users can contribute to the consensus process which determines the blocks which are added to the blockchain. These blockchains are fully decentralized and they are secured by a combination of rewards based incentives and cryptographic verification schemes like proof of work/proof of stake.

Private blockchains - If an organization decides to run a blockchain application restricted to the users in that organization a private blockchain is a better choice where the write permissions are centralized for the organization and the read permissions could be public or restricted depending upon the organization's needs. The transactions turn out to be cost effective in private blockchains since a large number of nodes are not required for the verification process thereby reducing the processing power.

3.3. Elliptic Curve Digital Signature Algorithm (ECDSA) for Implementing Blockchain

Blockchain uses ECDSA for generating public, private keys and performing digital signature creation, verification. This comes under Elliptic Curve Cryptography (ECC), which is considered as the next generation of public key cryptography because of its significant advantages over current generation algorithms like RSA and DSA. Although Elliptic Curve Cryptosystems have been around for a long time, they became famous with the usage of ECDSA in Bigdata. In ECC, the elliptic curve is generally of the form y2 = x3+ax+b. Like other group-based cryptographic algorithms, ECC also requires a finite field of elements, which usually contains integers modulo a prime k, and suitable security is achieved when k is close to 160 bits. The private key (p) is a random integer which is less than the order of the generator n and the public key (P) is calculated by multiplying the private key with a point on the elliptic curve (G) i.e., P = pG. In ECDSA, key pairs are generated with reference to a particular set of domain parameters such that the public key (P), the private key (p) and this set of domain parameters are mathematically related to each other.

In Blockchain, a 32-byte private key and a 64-byte public key is generated for every account. This public key undergoes a Keccak-256 hash resulting in a 32-byte output hash string. The right most or the last 20-bytes of this hash string is used as an account address. This account address is usually prefixed with a '0x' to represent that it is in Hexadecimal format. The mathematical and implementation details for ECDSA are quite complex and not easily understandable, which is one of the reasons why it is not being implemented at a large scale. In short, it can be thought of as an elliptic curve analog to Digital Signature Algorithm. As far as security is concerned, even after decades of research, cryptographers couldn't come up with a computationally practicable method to solve the discrete-logarithm for elliptic curves.

One of the primary advantages of ECC over traditional asymmetric key algorithms is the key size. Currently, RSA is the most popular and considered a secure encryption algorithm but, a 256-bit ECC key offers the same level of security as a 3072-bit RSA key. The following table offers a more detailed view of key comparisons:

Table 2. RSA vs ECC Key Size Comparison for implementation of high-quality education system.

RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

So, even with a shorter key length, it requires more time to break an ECC key than an RSA key. Following is a graph comparing the key size and the MIPS years to break it for RSA, DSA, and ECC. One more interesting way to compare the difficulty levels of algorithms is that "a cryptosystem is said to offer pool security if breaking it requires as much energy as it takes to boil a single Olympic size swimming pool (i.e., 2500 cubic meters of water)." By this standard, it takes less energy to break a 228-bit RSA key than to boil a teaspoon of water. Conversely, it would take more energy to break a 228-bit ECC key than to boil all the water on earth.

Table 3. Comparison in implementation blockchain on governmental level and legislation of blockchain based economy.

Country	Blockchain Economy	Legislation & Regulation	Government Policy
Germany	Vibrant	Advanced	Very Supportive
Turkey	Intermediate	Intermediate	Supportive
Greece	Low Activity Level	Lacking	Lacking

3.4. Basic Systems Specification in Implementing Blockchain Technology

Number of processors : 4

Model name : ARMv7 Processor rev 4 (v7l)

BogoMIPS : 38.40

CPU implementer : 0x41

CPU architecture : 7

CPU variant : 0x0

CPU part : 0xd03

CPU revision : 4

Hardware : BCM2709

Revision	: a22082
Serial	: 00000000ae85d2bb

3.5. Benchmarking Blockchain Technology

For the purpose of benchmarking blockchain functionality on IoT devices, we have deployed a private blockchain using three Raspberry Pi devices, one Windows Server 2016 running on Amazon EC2 and a Windows laptop which serves as the miner. The final state of the blockchain with 12098 blocks upon which the benchmarking is performed is given below.

Table 4. The training blocks in big data and blockchain [25].

Big Data Technology	Blockchain Technology
Programming with Python Fundamentals of Statistics Programming with R Data Mining and Predictive Model- ling Machine Learning and AI with Python and R Databases of NoSQL Databases SQL Text Mining and Social Media Big Data Technologies Deep Learning Hadoop/Spark	Introduction and Technical Aspects of Blockchain and DLTs GNU/Linux system Docker Blockchain Programming and Big-Data Connectivity Blockchain application development Hyperledger application development

```
pi@raspberrypi:/home $ geth --datadir "/home/pi/private/blockchain/" --networkid 3141592 --nat extip:216.15.125.24 --port
30302 console
I1117 13:00:23.639161 ethdb/database.go:82] Alloted 128MB cache and 1024 file handles to /home/pi/private/blockchain/chain
data
I1117 13:00:23.686907 ethdb/database.go:169] closed db:/home/pi/private/blockchain/chaindata
I1117 13:00:23.695219 ethdb/database.go:82] Alloted 128MB cache and 1024 file handles to /home/pi/private/blockchain/chain
data
I1117 13:00:23.829000 ethdb/database.go:82] Alloted 16MB cache and 16 file handles to /home/pi/private/blockchain/dapp
I1117 13:00:23.845430 eth/backend.go:172] Protocol Versions: [63 62], Network Id: 3141592
I1117 13:00:23.846337 eth/backend.go:201] Blockchain DB Version: 3
I1117 13:00:23.857242 core/blockchain.go:206] Last header: #12098 [ff43930e…] TD=9740797499
I1117 13:00:23.857947 core/blockchain.go:207] Last block: #12098 [ff43930e…] TD=9740797499
I1117 13:00:23.858397 core/blockchain.go:208] Fast block: #12098 [ff43930e…] TD=9740797499
I1117 13:00:23.867905 p2p/server.go:313] Starting Server
I1117 13:00:23.868966 p2p/nat/nat.go:111] mapped network port udp:30302 -> 30302 (ethereum discovery) using ExtIP(216.15.1
25.24)
I1117 13:00:24.225193 p2p/discover/udp.go:217] Listening, enode://152930f71148b9ce03f50a11d05c5d69d9964cf478dff4dd51eaab51
c5631f06eaf9b5bd68c47b73424c613e52cad700b5f2f11f421e2b1405276572ae50180a@216.15.125.24:30302
I1117 13:00:24.226045 p2p/server.go:556] Listening on [::]:30302
I1117 13:00:24.226249 p2p/nat/nat.go:111] mapped network port tcp:30302 -> 30302 (ethereum p2p) using ExtIP(216.15.125.24)
I1117 13:00:24.232524 node/node.go:296] IPC endpoint opened: /home/pi/private/blockchain/geth.ipc
Welcome to the Geth JavaScript console!

instance: Geth/v1.4.10-stable-5f55d95a/linux/go1.6.2
coinbase: 0x9c9dd18429b014c295c1afd722020ebd5d6dfa80
at block: 12098 (Sat, 01 Oct 2016 13:08:56 EDT)
 datadir: /home/pi/private/blockchain
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

>
```

Fig. 7. Final State of the Blockchain with 12098 blocks

3.6. Impact of Blockchain Based Learning

The study reveals the long-sighted attitudes of blockchain based smartest system for the digitalization of learning. Among the findings of the study is satisfied with its own level of expertise, but that few are thinking about long-term learning. The blockchain based learning demands of publishing undermines efforts to change their behavior unless it helps them to complete the research. The journal itself has the responsibility for providing the policies, the resources, and fostering attitudes to instill sustainable digital behaviors. Administrators need to have the providence to create systems that support their research faculty for blockchain based learning. Researchers who apply for these grants must consider the future access of their data, in so doing should consult expertise within their organization and their domain for blockchain based learning. Local events such as data preservation and digitalization for blockchain based learning workshops and classes provide another communication channel to increase dialog and reinforce messaging for blockchain based learning.

4. Results

Blockchain application platform enables the building of decentralized applications and high-quality education system. This platform believes in the notion that blockchain or any monetary asset values are not essential for the existence of blockchains. High-quality education system perceives blockchains as “distributed rulebooks” which can keep a track of the modifications made and the list of permissions assigned by using private keys for a secure data management. Smart education aims at providing developers with blockchain structures that include expansive coding to foster communication. Contrasting smart education for deployment, Blockchain as we discussed is designed to use Ether crypto technology and make transactions on the blockchain. However, smart education focuses on building permissioned blockchains enabling users to define properties for their use cases and achieve secure transmission of data.

4.1. CPU Utilization in Implementing Blockchain Technology

4.1.1. Miner

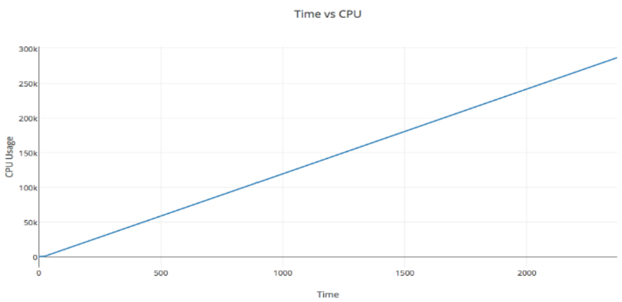

Fig. 8. Time (2-minute interval) vs CPU resource consumption for Miner Node

We have initiated only CPU mining with a single thread by issuing miner.start(1) and observed that the CPU utilization by process grows exponentially as the blockchain size increases.

4.1.2. Raspberry Pi Nodes

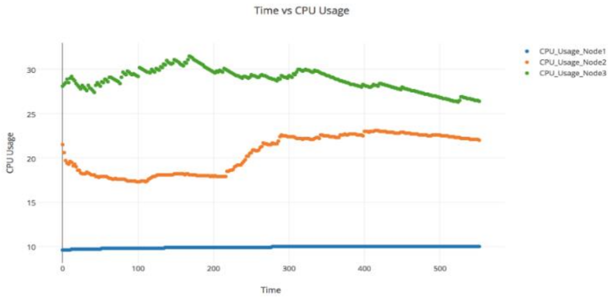

Fig. 9. Time (2-minute interval) vs CPU resource consumption graph for 3 Raspberry Nodes

Table 5. Statistics for the CPU resource consumption of 3 Raspberry Nodes

Descriptive statistics	Node 1 CPU	Node 2 CPU	Node 3 CPU
N	277	277	277
Min	9.6	17.3	26.3
Max	10	23.1	31.5
Mean	9.913718412	20.50722022	28.81624549
First Quartile	9.9	18.1	28
Median	9.9	21.6	29
Third Quartile	10	22.5	29.7
Standard Deviation	0.105581936	2.164786747	1.208658437
Variance	0.011147545	4.686301659	1.460855218
Standard Error	0.006343804	0.13006943	0.072621247

We have observed that the CPU utilization of process on the raspberry pi nodes didn't fluctuate much and displayed a maximum standard deviation of 2.16 units.

4.2. RAM Utilization in Implementing Blockchain Technology

4.2.1. Miner

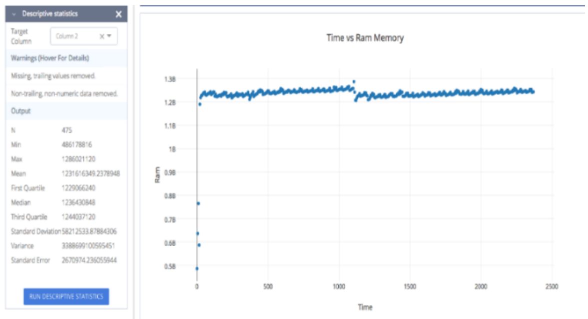

Fig. 10. Time (2-minute interval) vs RAM (Bytes) consumption graph for Miner Node

It was observed that the consumption of RAM memory by the miner was linear and neither the blockchain size or block difficulty has any effect on the RAM consumption.

4.2.2. Raspberry Pi Nodes

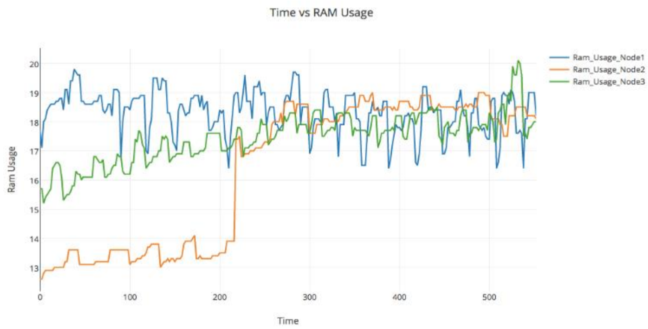

Fig. 11. Time (2-minute interval) vs RAM (Bytes) consumption graph for 3 Raspberry Nodes

Table 6. Statistics for the RAM (Bytes) consumption of 3 Raspberry Nodes.

Descriptive statistics	Node 1 Ram	Node 2 Ram	Node 3 Ram
N	277	277	277
Min	16.4	12.6	15.2
Max	19.8	19	20.1
Mean	18.34115523	16.33068592	17.43429603
First Quartile	17.9	13.5	16.9
Median	18.5	17.9	17.6
Third Quartile	18.9	18.5	17.9
Standard Deviation	0.72587761	2.427362945	0.846492418
Variance	0.526898304	5.892090865	0.716549414
Standard Error	0.043613759	0.145846104	0.0508608

It was observed that even though the ram usage at the start was different on each node, they start to converge from a point and the RAM usage displayed similar trends on all the devices from this point. Two out of the three nodes have not displayed any noticeable fluctuations in RAM usage and the standard deviation was less than one unit.

4.3. CPU Temperature in Implementing Blockchain Technology

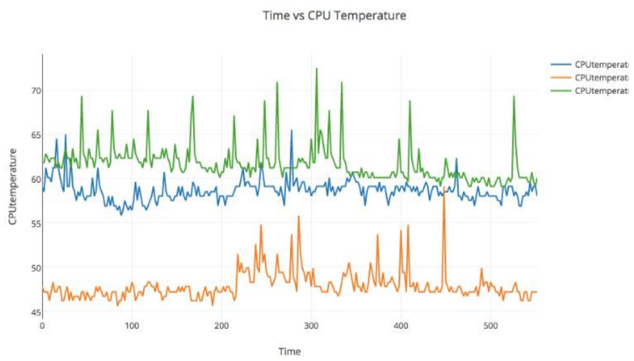

Fig. 12. Time (2-minute interval) vs CPU core temperature (oC) graph for 3 Raspberry Nodes

Table 7. Statistics for CPU core temperature (oC) data of 3 Raspberry Nodes.

Descriptive statistics	Node 1 CPU Temperature	Node 2 CPU Temperature	Node 3 CPU Temperature
N	277	277	277
Min	55.8	45.6	59.1
Max	65.5	59.1	72.5
Mean	58.63465704	47.88736462	61.64476534
First Quartile	58	47.2	60.1
Median	58.5	47.2	61.2
Third Quartile	59.1	48.3	62.3
Standard Deviation	1.222188503	1.626235466	2.059340708
Variance	1.493744738	2.644641791	4.240884151
Standard Error	0.07343419	0.097711019	0.123733791

4.4. Block Time in Implementing Blockchain Technology

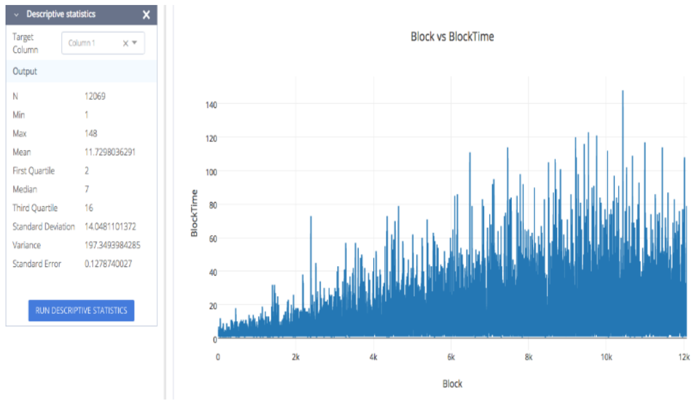

Fig. 13. Block Number Vs Block Time for blockchain

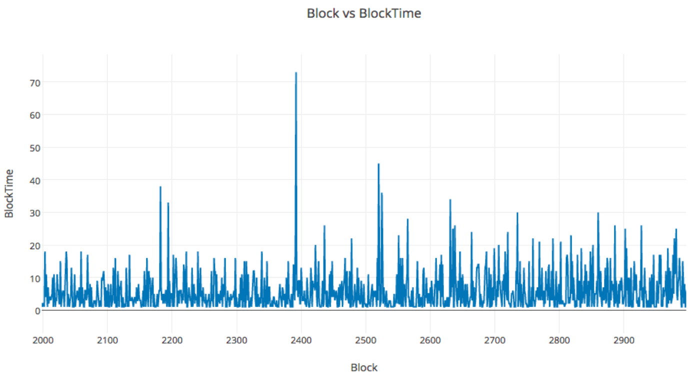

Fig. 14. Sub-part (block number 2000 - 3000) of above Graph.

Table 8. Statistics for student's diversity in urban and rural area for E-Learning using Blockchain.

Demographic variables		**Frequency**	***Percentage***
Class			
	GRADUATION	176	*46.0*
	POST-GRADUATION	207	*54.0*
Gender	Male	138	36.0
Locality	Female	245	64.0
	Rural	104	*27.2*
	Urban	279	*72.8*

4.5. Comparison Among Learning Methods

It is notable that the blockchain based learning would successively perform better is deeper networks are being used but advanced automation techniques will provide great efficiency due to its architectural flexibility with blockchain algorithm. Having more data models possess greater representational power making it possible to approximate more complex functions. Also, fast development in the field continuously introduces new techniques and architectures expanding the toolbox for design. However, science has always embraced simplicity, and it is reasonable to argue that the network should be kept as simple as possible. A study could use the CNN technique in future which would even questioned the common practice of using pooling and sophisticated activation functions in machine learning or deep learning. Instead, they suggest using just recurrent layers with properly selected stride and filter size parameters using blockchain. The blockchain are responsible for feature extraction, where the features to which they will respond are determined through a learning process of the variable input connections. Simple features, such as specific orientations of lines and edges, will be extracted by lower-level CNN models, while higher-level blockchain models extract more global features (e.g. parts of learned patterns).

5. Discussion

Smart education is a high-performance enterprise ready consensus for implementation which can be used to develop and run Byzantine fault tolerant applications. The validators sign the block to say that they approve that this is the correct block. So, a block gets added to the blockchain when it gets signed by the majority of validators. As long as 2/3rd or more of the voting power of validators sign the block, it becomes officially committed. The 2/3rd majority is chosen because, in case a fork occurs, at least 1/3rd of the validators have signed for both the blocks so this means that the system can tolerate up to 1/3rd of participants. So, if more than 1/3rd of the nodes are byzantine nodes, the consensus cannot be guaranteed. In Big-data and Blockchain, anybody can mine blocks. They just need to have the required hardware and the supply of electricity. This is called permission-less validation. The Smart education ideology considers this a bug, not a feature. Particularly in the Enterprise industry, this kind of system might lead to the violation of regulations. Some key advantages of Smart education used blockchain and are that the block time can be as low as 2 seconds. There is no block size limit, and the network can handle 10,000 transactions per second if the transaction size is 250 bytes. Due to the usage of public keys for signing the blocks, accountability is maintained, and liability can be determined when a blockchain fork occurs.

Table 9. The comparison of major blockchain for potential deployment in high-quality education system.

Parameters	Applications Blockchain	Big-Data	Machine Learning
Block Time	15 Seconds	2 Seconds	N/A
Block Size	No Limit	No Limit	N/A
Txps	25	10,000	To be added
High-quality education system	Yes	Yes	To be added
Type of Blockchain	Public, Private	Private, Permissioned	N/A
Distributed Consensus	Proof-of-Work	Proof-of-Stake	Proof-of-Work
Explorer API	Yes	Yes	Yes (Web UI also available)
Signing Algorithm	ECDSA	Ed25519	To be added
Hashing Algorithm	Keccak 256	RIPEMD 160	To be added
Minimum Nodes	1	4	To be added
Supported OS'	Windows, Linux, MAC, ARM	Windows, Linux, MAC	N/A (Java 64-bit)
Robust Codebase	Medium - High	Low - Medium	Reference Implementation
Fault Tolerance Level	1/2 of the nodes	1/3 of the nodes	To be added
Documentation	Mostly Clear	Ambiguous	Very little
Implementation Complexity	Easy – Medium	Medium – Hard	Easy
Accountability	No	Yes	To be added
Deployment in High-quality education system	Yes	Yes	No
Target Use-cases	Distributed Apps	Enterprise applications for regulatory environments	IoT applications

These permissions determine which accounts can participate in the consensus process and which accounts can create high-quality education system in a blockchain network. So, in a smart education application, one can control who can validate blocks and who can make changes to code logic. Some of the advantages of blockchain in smart education are given by:

- Energy efficient since there is no hashing involved.
- CPU mining is possible because signing and verification operations are simple.
- Requires less computational capacity and memory.
- Block time is approximately 2 seconds while in normal online transaction, it is 15 seconds.
- Smart education can support 10,000 transactions per second while normal transaction supports 15 transactions per second. These stats are based on simple transactions (from, to, value)
- Smart education uses blockchain algorithms for signing and verifying blocks. Users can sign 100,000 blocks/second and can verify 70,000 signatures/second without a compromise in security. Normal transaction is not as fast.

6. Conclusions

Blockchains and IoT are still at an early stage of development and there is certainly a lot of hype around both the technologies. The current state of blockchain is ambiguous and everything is still in the exploration phase. Big-data and Blockchain remain the most popular and novel projects in this space while others are just forks with subtle changes. Projects on blockchain keep emerging but most of these projects are abandoned even before they materialize. This is because people fail to realize that blockchain is not the solution for every problem we have, although it does offer some interesting possibilities that can improve the current situation of some ecosystems. Once the internal mechanisms are understood, we learn that not much can be solely achieved by the blockchain technology itself. Instead, the blockchain technology can be incorporated into current solutions to make them robust and more secure. The strength of blockchain lies in financial technology (fintech) because that is what it was invented for and that is where its impact is becoming apparent. We are yet to observe a breakthrough in other applications of blockchains like IoT, supply chain, healthcare, manufacturing, and digital asset management. As far as our research is concerned, Blockchain combined with the smart education proof-of-stake mechanism seems to be the most optimal solution for building the majority of IoT applications. This is because Machine Learning is still in the beta phase and only has a reference implementation. Nothing concrete can be inferred from this yet. Also, it has a completely different structure for storage which is not yet proven to be robust. However, there are some interesting projects like Hyperledger and IBM Blockchain to watch out for. IBM is rapidly developing and testing Proof-of-Concept applications in various industries. The Hyperledger consortium is backed by a lot of big players and is managed by the Linux foundation group. Both these projects claim to support IoT use cases. The ongoing research in the blockchain field will soon reveal how these projects will develop and impact the IoT ecosystem.

Acknowledgements: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No.: GRANT501]..

References

[1] Ali Syed T, Alzahrani A, Jan S, Siddiqui MS, Nadeem A, Alghamdi T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. IEEE Access [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2019;7:176838–69. Available from: http://dx.doi.org/10.1109/access.2019.2957660.

[2] Velliangiri S, Karthikeyan P. Blockchain Technology: Challenges and Security issues in Consensus algorithm. 2020 International Conference on Computer Communication and Informatics (ICCCI) [Internet]. IEEE; 2020 Jan; Available from: http://dx.doi.org/10.1109/iccci48352.2020.9104132.

[3] Malomo OO, Rawat DB, Garuba M. Next-generation cybersecurity through a blockchain-enabled federated cloud framework. The Journal of Supercomputing [Internet]. Springer Science and Business Media LLC; 2018 May 2;74(10):5099–126. Available from: http://dx.doi.org/10.1007/s11227-018-2385-7.

[4] Adebayo A, Rawat DB, Njilla L, Kamhoua CA. Blockchain-enabled Information Sharing Framework for Cybersecurity. Blockchain for Distributed Systems Security [Internet]. Wiley; 2019 Mar 15;143–58. Available from: http://dx.doi.org/10.1002/9781119519621.ch7.

[5] M D, Biradar NB. IOTA-Next Generation Block chain. International Journal Of Engineering And Computer Science [Internet]. Valley International; 2018 Apr 2;7(04):23823–6. Available from: http://dx.doi.org/10.18535/ijecs/v7i4.05.

[6] Bolfing A. Introduction to Blockchain Technology. Cryptographic Primitives in Blockchain Technology [Internet]. Oxford University Press; 2020 Sep 10;199–240. Available from: http://dx.doi.org/10.1093/oso/9780198862840.003.0006

[7] Shrestha R, Bajracharya R, Shrestha AP, Nam SY. A new type of blockchain for secure message exchange in VANET. Digital Communications and Networks [Internet]. Elsevier BV; 2020 May;6(2):177–86. Available from: http://dx.doi.org/10.1016/j.dcan.2019.04.003.

[8] Baranwal Somy N, Kannan K, Arya V, Hans S, Singh A, Lohia P, et al. Ownership Preserving AI Market Places Using Blockchain. 2019 IEEE International Conference on Blockchain (Blockchain) [Internet]. IEEE; 2019 Jul; Available from:

http://dx.doi.org/10.1109/blockchain.2019.00029.

[9] Vyas S, Gupta M, Yadav R. Converging Blockchain and Machine Learning for Healthcare. 2019 Amity International Conference on Artificial Intelligence (AICAI) [Internet]. IEEE; 2019 Feb; Available from: http://dx.doi.org/10.1109/aicai.2019.8701230.

[10] Shrestha R, Nam SY, Bajracharya R, Kim S. Evolution of V2X Communication and Integration of Blockchain for Security Enhancements. Electronics [Internet]. MDPI AG; 2020 Aug 19;9(9):1338. Available from: http://dx.doi.org/10.3390/electronics9091338.

[11] Shrivastava V, Kumar S. Utilizing Block Chain Technology in Various Application Areas of Machine Learning. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) [Internet]. IEEE; 2019 Feb; Available from: http://dx.doi.org/10.1109/comitcon.2019.8862203.

[12] Shrestha R, Kim S. Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities. Role of Blockchain Technology in IoT Applications [Internet]. Elsevier; 2019;293–331. Available from: http://dx.doi.org/10.1016/bs.adcom.2019.06.002.

[13] Huang C. Blockchain design for internet-of-thing. The Hong Kong University of Science and Technology Library; Available from: http://dx.doi.org/10.14711/thesis-991012880064303412.

[14] Singh B, Sharma KP, Sharma N. Blockchain Applications, Opportunities, Challenges and Risks: A Survey. SSRN Electronic Journal [Internet]. Elsevier BV; 2020; Available from: http://dx.doi.org/10.2139/ssrn.3565930.

[15] Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and IoT Integration: A Systematic Survey. Sensors [Internet]. MDPI AG; 2018 Aug 6;18(8):2575. Available from: http://dx.doi.org/10.3390/s18082575.

[16] Das R, Prasad A. Survey of Blockchain Techniques for IoT Device Security. Blockchain Technology [Internet]. CRC Press; 2022 Feb 24;57–72. Available from: http://dx.doi.org/10.1201/9781003138082-4.

[17] Sittón-Candanedo I, Alonso RS, Corchado JM, Rodríguez-González S, Casado-Vara R. A review of edge computing reference architectures and a new global edge proposal. Future Generation Computer Systems [Internet]. Elsevier BV; 2019 Oct;99:278–94. Available from: http://dx.doi.org/10.1016/j.future.2019.04.016.

[18] OzCakmak B, OzbIlen A, YavanoGlu U, CIn K. Neural and Quantum Cryptography in Big Data: A Review. 2019 IEEE International Conference on Big Data (Big Data) [Internet]. IEEE; 2019 Dec; Available from: http://dx.doi.org/10.1109/bigdata47090.2019.9006238.

[19] Liao D-Y, Wang X. Applications of Blockchain Technology to Logistics Management in Integrated Casinos and Entertainment. Informatics [Internet]. MDPI AG; 2018 Nov 27;5(4):44. Available from: http://dx.doi.org/10.3390/informatics5040044.

[20] Augusto JC, Callaghan V, Cook D, Kameas A, Satoh I. “Intelligent Environments: a manifesto.”Human-centric Computing and Information Sciences [Internet]. Springer Science and Business Media LLC; 2013 Jun 15;3(1). Available from: http://dx.doi.org/10.1186/2192-1962-3-12.

[21] Available Online: https://medium.com/@blairlmarshall/how-does-a-big-data-transaction-actually-work-1c44818c3996.

[22] Available Online: https://yos.io/2018/11/16/blockchain-signatures/

[23] Available Online: http://financeindex.co/investing/cc8765456/

[24] Rahim R, Patan R, Manikandan R, Kumar SR. Introduction to Blockchain and Big Data. Blockchain, Big Data and Machine Learning [Internet]. CRC Press; 2020 Sep 24;1–23. Available from: http://dx.doi.org/10.1201/9780429352546-1.