THE PLACE OF

BLOCKCHAIN TECHNOLOGY IN THE SECURITY OF

CLOUD COMPUTING

A Thesis

Submitted to the Faculty of Information Technology
School of Information Technology Atlantis University

In Partial Fulfillment of
The Requirements for the Degree of

Master of Science in Information Technology

by

Benjamin O. Ugwu

July, 2021

THE PLACE OF
BLOCKCHAIN TECHNOLOGY IN THE SECURITY OF
CLOUD COMPUTING

THE PLACE OF

BLOCKCHAIN TECHNOLOGY IN THE SECURITY OF

CLOUD COMPUTING

Abstract of Thesis

Submitted to the Faculty of Information Technology
School of Information Technology Atlantis University

In Partial Fulfillment of
The Requirements for the Degree of

Master of Science in Information Technology

by

Benjamin O. Ugwu

July, 2021

Dr. James A. Thomas

Department: School of Information Technology

Abstract

The adoption of Cloud Computing has continued to grow due to the numerous benefits that come with it such as little to no initial investment cost. However, some private organizations are still reluctant to adopting Cloud Computing because of certain security concerns of the Cloud. Blockchain technology is considered one of the latest technological breakthroughs with a reputation of being highly secure. This research paper aims to find out if Blockchain Technology is a feasible solution to the security issues facing Cloud Computing in private organizations. The author went ahead to suggest a "Cloudchain" architecture for integrating Blockchain into Cloud Computing for a more secure Cloud Computing operations. Over ninety (90) sources of peer-reviewed journals of which thirty three (33) were selected were used to gather and analyze information on the subject matter of this research paper. The wealth of knowledge gathered in the course of this research shows that Blockchain technology is a feasible option to solve the security issues facing Cloud Computing as it affects private organizations. The author believes that the implementation of the "Cloudchain" architecture will not only help to solve the security issues facing Cloud Computing but will also encourage more private organizations to adopt Cloud Computing and partake in its numerous benefits.

Keywords: Cloud Computing, Blockchain Technology, Information Security

Table of Contents

List of Tables

List of Figures

Chapter One: The Problem

This study addresses the problem of Cloud Computing security in private organizations. The primary focus is on the place of Blockchain technology in the security of Cloud Computing in private organizations. Although Cloud Computing is a well-known technology, as it has existed for many years with many useful services and a well-defined technology that emerged from large-scale, distributed computing technology, the organizations are slow in accepting this due to their security concerns. Security challenge in Cloud Computing is a significant drawback hampering the Cloud (Venters & Whitley, 2012).

There have been different studies done on how to secure computing operations involving Cloud Computing. In academia, Cloud Computing security has begun seeing the development of dedicated forums such as the ACM (Association for Computing Machinery) Cloud Computing Security Workshop, as well as dedicated tracks at major security conferences such as the ACM Conference on Computer and Communications Security (CCS). To date, most papers published on Cloud security reflect continuations of established lines of security research, such as web security (Livshits, Prateek & Vikram, 2008), data outsourcing and assurance (Bowers, Juels & Oprea, 2008), and virtual machines (Santos, Gummadi & Rodrigues). The field primarily manifests as a blend of existing topics, rather than a set of papers with an exclusive focus on Cloud security, though there are exceptions (Chen, Paxson & Katz, 2010). With increased employment of Cloud Computing comes increasingly frequent Cloud Computing security incidents.

Blockchain technology is an emerging technology well known for its security and authenticity, which are the main characteristics that are making the world think favorably of it. The continual increase in the use of Cloud Computing technology warrants a study of new approaches such as Blockchain on the benefits of integrating the Blockchain network with a scalable Cloud environment to enhance Cloud Computing security.

Problem Background

The economic case for Cloud Computing has gained widespread acceptance. Cloud Computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources. The economies of scale increase revenue for Cloud providers and lower costs for Cloud users. The resulting on-demand model of computing allows providers to achieve better resource utilization through statistical multiplexing, and enables users to avoid the costs of resource over-provisioning through dynamic scaling (Armbrust, M. et al., 2009). At the same time, security has emerged as arguably the most significant barrier to faster and more widespread adoption of Cloud Computing. This view originates from perspectives as diverse as academia researchers (Armbrust, M. et al., 2009), industry decision makers, and government organizations (Mell & Grance, 2009). For many business-critical computations, today's Cloud Computing appears inadvisable due to issues such as service availability, data confidentiality, reputation fatesharing, and others (Chen, Paxson & Katz, 2010).

Blockchain Technology is the future of the industries striving for security and privacy improvements. Blockchain is a distributed ledger that records tamper-evident data in the form of a chain without any central authority. The participants or the devices in the Blockchain technology are called nodes. Blockchain provides a decentralized network in which all the network nodes have active participation to validate and verify the data. The data to be stored in the Blockchain is encrypted using cryptography. Every block contains an encrypted hash, timestamp, and hash of the previous block in the chain through which the block will connect. Therefore, the data in the Blockchain is tamper-evident. Blockchain provides the data with security, and participating users will be verified in the network, eliminating the data's privacy concern (Venters & Whitley, 2012).

To secure Cloud Computing, we can overcome the data's security concerns by integrating it with Blockchain technology. Blockchain improves data security and it can manage Cloud data (Chen, Paxson & Katz, 2010). The security drawback of Cloud Computing can be overcome by using the decentralized Blockchain technology in the Cloud instead of centralized Cloud technology. The emerging technology with the most secured options is Blockchain technology with many data securing techniques. The Blockchain is a whole new technology, comprehensive Blockchain trials have been undertaken to ensure the safe use of electronic cash by communicating only between peers and without third parties. Blockchain came into existence with the introduction of Bitcoin in 2008. The technology behind many cryptocurrencies is Blockchain technology. It allows the transactions among the peers directly without the involvement of any third party. It is an open distributed ledger that records the entire evolution of blocks in the network and the copy is maintained by all the nodes present in the same network. Integrating Blockchain technology with Cloud Computing will help us to solve the major challenges in the Cloud and increases the quality and reliability of the Cloud data (Murthy et al., 2020).

Purpose of the Study

The purpose of this study was to determine if Blockchain technology is a feasible option to solve the security challenges facing Cloud Computing in private organizations. If the research reveals that Blockchain technology is a feasible option to solve the security challenges facing Cloud Computing in private organizations, the results may be useful to private organizations in developing effective solutions to Cloud Computing security designed specifically for private organizations.

Furthermore, it was the aim of this researcher to add to the body of literature regarding best solutions for handling security issues in Cloud Computing. Even though there are numerous articles that deal with Cloud Computing security and others that focus on the security benefits of Blockchain technology, academic literature still lacks enough publications that address the importance of Blockchain technology in Cloud Computing security within private organizations. This could be related to the fact that although Cloud Computing has been around for some time, Blockchain technology is still relatively new and could be considered as the most recent technology breakthrough. By itself, this study contributes to the academic literature as well, serving both practitioners and academics alike.

Research Question

Primary research question: Is Blockchain technology a feasible option to solve the security challenges facing Cloud Computing? The premise of the question is based on the notion that Blockchain technology is a highly secure and authentic new technology that could be used as a solution to the security challenges in Cloud Computing.

If research results indicate an affirmative response to the primary research question, a subsequent secondary query would be posed to determine if an architecture model of Cloud-Blockchain integration could be developed to provide a better security in Cloud Computing.

Hypotheses

The null hypothesis (H0) also known as the conjecture, is assumed true until an alternative hypothesis, also referred to as the research hypothesis, rejects the null hypothesis H0 by way of investigational proofs. The alternative hypothesis may be non-directional or directional. In this case, the research hypothesis (H1) is directional since it is predicting an outcome before the research.

Null Hypothesis. H0: Blockchain technology is a feasible option to solve the security challenges facing Cloud Computing.

Primary Alternative/Research Hypothesis. H1: Blockchain technology is not a feasible option to solve the security challenges facing Cloud Computing. H1 is worthy of testing because it denies or confirms if Blockchain technology could be employed to solve the security challenges facing Cloud Computing. If H1 is accepted and H0 is rejected, it would not be a good move for organizations to consider the application of Blockchain technology in their Cloud Computing security related operations. If H1 is rejected and H0 is accepted, it would enable organizations to consider further study regarding ways to solve the security challenges facing Cloud Computing through Blockchain technology.

Limitations and Delimitations

The major limitation of this study is that the research data and information was based on secondary sources such as case studies from other academia and authors within and outside the USA (United States of America). No actual survey or direct information was obtained from private organizations as it relates to how they employ Cloud Computing or Blockchain technology. Therefore, the results cannot be verified objectively, and the discussions could be biased by the authors' opinions. In order to reduce the potential bias and limitations, several researches of over thirty (30) sources have been studied to cross-reference the data collected in order to obtain more accurate information in this paper.

Furthermore, due to the relatively young nature of Blockchain technology, there are not robust or plenty of materials on the subject out there especially as it relates to Cloud Computing security, as against other technologies that have been operational for many decades. According to Knirsch, F., et al., (2019), the introduction of Blockchain technology to society happened with the release of Bitcoin (Knirsch, F., Unterweger, A., & Engel, D., 2019). Bitcoin is a form of Cryptocurrency that is exchanged among peers directly. Bitcoin was introduced in 2008 by a pseudo name called Satoshi Nakamoto (Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inacio, P. R., 2014). This constraint of Blockchain technology being relatively young was mitigated by a thorough study of the available materials to possibly sieve out every relevant information as they relate to the subject matter.

Definitions

Cloud Computing is defined as a model for enabling service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction (Lee, K., 2012). According to the NIST (National Institute of Standards and Technology) definition, key characteristics of Cloud Computing include on-demand self service, broad network access, resource pooling, rapid elasticity, and metered service similar to a utility. There are also three main service models; Software as a service (SaaS), in which the Cloud user controls only application configurations; platform as a service (PaaS), in which the Cloud user also controls the hosting environments; and infrastructure as a service (IaaS), in which the Cloud user controls everything except the datacenter infrastructure. Further, there are four main deployment models: public Clouds, accessible to the general public or a large industry group; community Clouds, serving several organizations; private Clouds, limited to a single organization; and hybrid Clouds, a mix of the others.

Blockchain technology is a distributed ledger with records of data containing all details of the transactions carried out and distributed among the nodes present in the network (Lim et al., 2020). All the transactions carried out in the system are confirmed by consensus mechanisms, and the data once stored cannot be altered. Blockchain technology is trustworthy with no central authority. It is transparent, immutable and tamperproof (Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S., 2018). We can store any type of data in these blocks. There are different kinds of Blockchain called Public, Private and Consortium (Farah, N. A. A., 2018). These can be built by the organizations themselves based upon their (kinds of Blockchain) type of utility. The organizations need not depend upon any provider to get the service. Blockchain typically uses a number of mathematical functions or algorithms to construct a highly secure and distributed ledger system that allows transactions to occur without third party need. Blockchain can be used in different use cases like banking, healthcare (Katuwal, G. J., Pandey, S., Hennessey, M., & Lamichhane, B., 2018), Law enforcement, Voting, Governance, Supply chain management (Jabbari, A., & Kaminsky, P., 2018), and so on.

Security also referred to as IT security (Information Technology Security) could be defined as a set of strategies employed to prevent unauthorized access to organizational assets such as computers, data, and networks. It maintains the confidentiality, integrity, and availability of sensitive information. It is also sometimes referred to as cybersecurity or information security. While cybersecurity is mostly used to refer to security involving the internet, information security is sometimes used to refer to logical security (security of data excluding physical security). Security or Information security is therefore the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information. Information security includes the areas of information security management, data security, and network security (Michael & Herbert, 2018).

A private organization is any partnership, corporation, person, or agency that is not operated by a public body. It includes all businesses that are for-profit that are not government owned or operated. A private organization can be a non-federal body that is self-sustaining and established on federal property by people that are not acting in a federal government capacity. Private organizations are characterized by private ownership, the financial resources of private organizations stem from fees paid directly by consumers, and private organizations are controlled by market forces largely outside the span of political control (Perry & Rainey, 1988). These businesses are driven by profit and the profit from private organizations primarily benefits the owners, shareholders and investors.

Feasible solution can be described as a means of solving a problem that satisfies the entire restrictions or constraints foreseen in the challenges at hand. When at least one restriction of the problem is not met, the solution is considered not feasible (IGI Global, 2021). If something is feasible, then you can do it without too much difficulty. It is capable of being done with means at hand and circumstances as they are. When someone asks "Is it feasible?" the person is asking if you will be able to get something done. Feasible things are possible. If you have enough time, money, or energy to do something, it is feasible. Something might be feasible at one time and then not feasible at another time. For instance, Because of technological advances and competition with the Russians, going to the moon was feasible for the United States in the sixties. Often, people disagree about what is feasible, especially in politics, where how feasible a project is counts for a lot. In summary, when something or a solution is feasible, then it is capable of being done, achieved or being accomplished (Vocabulary.com, 2021).

Importance of the Study

There are two major importance of this study, first being that it provides academics with a foundation for continued research regarding the place of Blockchain technology in Cloud Computing security in private organizations and, second being that it provides practitioners a basis to develop sustainable solutions to Cloud Computing security in private organizations through Blockchain technology integration. Since the use of Cloud Computing continues to grow and Blockchain technology is gradually being adopted by organizations particularly due to its highly secure nature, new approaches to Cloud Computing security should be considered in order to improve the security of Cloud Computing by taking advantage of Blockchain technology.

The Cloud Computing market and development are growing rapidly. The continuous increase in network capacity, along with a near disappearance of limitations that could choke traffic in an earlier era (hardline security policies, storage performance issues, last mile Wide Area Network hindrances), are the foundation of this latest platform shift in computing (Byrne, D., Corrado, C. & Sichel, D. E., 2018). Blockchain as a new technology with a reputation for being secure based on principles of cryptography, decentralization and consensus, which ensure trust in transactions presents potential benefits as a feasible option to one of the major concerns in Cloud Computing which is the security and confidentiality of user data in terms of its location, availability and security.

In summary, this study is important because it provides interested parties a foundation to develop feasible methods for tackling the security issues facing Cloud Computing through Blockchain Technology as it affects private organizations.

Chapter Two: Review of the Literature

Literature Review

The literature review focuses on three primary topics: Cloud Computing, Blockchain technology and deficiencies in the current body of academic literature.

Cloud Computing

According to the National Institute of Standards and Technology (NIST) publication in September, 2011 (Mell & Grance, 2011), Cloud Computing could be defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort of service provider interaction. NIST came up with this definition after consultations with many industry and government experts and stakeholders (Byrne, Corrado, & Sichel, 2018). Cloud Computing is an outstanding act of remote servers system utilization facilitated on the web to store, oversee and process information, as opposed to a neighborhood server or a PC (Murthy et al., 2020).

Types of Clouds

NIST describes the following three types of Clouds:

Private Cloud. A Cloud infrastructure provisioned for a single organization or specific community of organizations; it may exist on or off premises. Eucalyptus System is the best example of a private Cloud (Murthy, et al., 2020).

Public Cloud. A Cloud infrastructure provisioned for open use by the public; it exists on the premises of the Cloud provider. Microsoft Azure and Google App Engine are examples (Sharma, Gupta, & Laxmi, 2014).

Hybrid Cloud. A combination of the above types of cloud bound together by standardized or proprietary technology that enables data and application portability. Amazon Web Services is a prominent example of a hybrid Cloud (Murthy, et al., 2020).

A forth type of Cloud usually found in literature is Community Cloud: This is mainly built for a specific community of consumers from different organizations with shared concerns. It can be owned, managed, and operated by one or more companies in the community. This kind of Cloud is useful in Education or Banking sectors. Facebook is an example of a community Cloud (Murthy, et al., 2020).

The author would like to mention at this point that this study is focused more on the public, community and hybrid Clouds since they are where Cloud security concerns are most in play. Security and privacy are perceived as primary obstacles to the wide adoption of Cloud Computing (Ren, et al., 2012).

NIST provides a concise description of the infrastructure that underlies the Cloud as: the collection of hardware and software that enables the five essential characteristics of Cloud Computing (discussed below) . The Cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the Cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential Cloud characteristics. Conceptually the abstraction layer sits above the physical layer. (Mell & Grance, 2011).

Cloud Products

The NIST Cloud Computing definition also includes a description of service models, or service offerings. In measurement nomenclature, these services correspond to “product types” or product classes. These product classes include:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

IaaS (infrastructure as a service) provides computer processing, storage, networks, and other fundamental computing resources, where the consumer can deploy and run arbitrary software, including operating systems as well as applications. The consumer neither manages nor controls the underlying Cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly some control of select networking components.

PaaS (platform as a service) provides ability to deploy consumer-created applications created using programming languages, libraries, services, and tools. The consumer neither manages nor controls the underlying Cloud infrastructure including network, servers, operating systems, or storage but has control over the deployed applications.

SaaS (software as a service) provides the capability of running providers’ applications on a Cloud infrastructure. The applications are accessible from various client devices through either a thin-client interface (e.g., web browser) or a program interface. The consumer neither manages nor controls the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, apart from limited user-specific application configuration settings.

Table 1
Cloud computing product types or product classes and service management

S/N	Services Managed by User	IaaS	PaaS	SaaS
1	Application	Yes	Yes	No
2	Data	Yes	Yes	No
3	Runtime	Yes	No	No
4	Middleware	Yes	No	No
5	Operating System (O/S)	Yes	No	No
6	Virtualization	No	No	No
7	Servers	No	No	No
8	Storage	No	No	No
9	Networking	No	No	No

Since the NIST definition was published, the industry has introduced a new layer of abstraction, called “Serverless” or Function as a Service. At this level of abstraction, the final user only needs to think about functions or code that are to be performed and the Cloud services provider manages all other aspects of the infrastructure. Serverless also known as FaaS or Function as a Service provides the capability of deploying functions (code) on a Cloud infrastructure. The consumer (who would be a software developer) no longer manages nor controls the underlying Cloud infrastructure including network, servers, operating systems, storage, or the computing program. An Application Program Interface (API) gateway controls all aspects of execution. Serverless may also be regarded as a refined PaaS service (Byrne, Corrado, & Sichel, 2018).

Cloud Technologies

The Cloud platform relies on a suite of technologies mainly virtualization, grid computing, and micro-services architectures but also everything that makes high-speed broadband possible (Byrne, Corrado, & Sichel, 2018).

Virtualization is basically making a simulated image or "version" of something such as server, operating system, storage devices or network resources so that they can be used on multiple machines at the same time. The main aim of virtualization is to manage the workload by transforming traditional computing to make it more scalable, efficient and economical. Virtualization has a wide range of applications such as operating system virtualization, hardware-level virtualization and server virtualization (Malhotra, Agarwal, & Jaiswal, 2014).

Grid computing is applying the resources of many computers in a network to a single problem at the same time; the technology was first used in 1989 to link supercomputers and thereafter grew and evolved along with the Internet (De Roure et al., 2003).

"Micro-services" is achieved through containers. "Containers" are scalable recent form of Cloud technology. A Container is a form of virtualization technology that gives users the ability to run and deploy applications without the need of launching a new virtual machine for each new application, thereby increasing the speed of software application development, and deployment. Container technology generally was not widely understood outside Cloud vendors until the release of open source LINUX formats (Docker 1.0) in March 2013 (Byrne, Corrado, & Sichel, 2018).

Major Characteristics of the Cloud

Cloud Computing consists of five major characteristics. On-demand self-service is the one in which the users can spontaneously provide network storage capabilities. Broad network access offers service across the network, which can be accessed with standard mechanisms to promote different kinds of client platforms. Resource pooling provides most of its computing resources to serve many consumers on their demand using a multi-tenant model. Measured service is when resources are owned, maintained, and optimized by the metering capabilities. Elastic Scalability is the one that can make changes in IT resources as needed to meet changing demand. For example, when an application needs to create more servers, it can automatically scale with demand (Agrawal, et al., 2011).

Blockchain Technology

Blockchain can be defined as transparent distributed ledgers of digitally signed transactions that are grouped into blocks (Murthy, et al., 2020). The blocks are linked together in the sense that each block contains a hash value produced through cryptography, a timestamp, and the transaction data of the previous block. The Blockchain recorded transactions among parties are done in an efficient and permanent manner. Blockchain data cannot be modified by design (Popovski, Soussou, & Webb, 2014).

A Blockchain is an increasing collection of transaction files that are known as blocks, which are bound together using cryptography. Each block contains the cryptographic hash, timestamp and transaction data of the previous block. Blockchain uses Asymmetric cryptography for security and Ledger to build trust (Murthy & Shri, 2020). Asymmetric cryptography or asymmetric encryption also known as public-key encryption requires two different keys (private and Public keys) to encrypt or encipher and decrypt or decipher messages respectively. The private key is kept secret and is known only to the owner of the key pair (private-public key pair) for decryption. The public key is stored in a public location where anyone can use it for encryption of messages going to the public key owner (Michael & Herbert, 2018). A ledger is a form of database that stores every transaction in the Blockchain. This ledger maintains copies of itself in every node (machines on the Blockchain network) (Rawat, Chaudhary, & Doku, 2019).

Blockchain technology was introduced to the world in 2008 through Bitcoin. Bitcoin is a form of digital currency introduced by a pseudo name called ‘‘Satoshi Nakamoto’’ in 2008. Satoshi Nakamoto published a white paper, ‘‘Bitcoin: A Peer to Peer Electronic Cash System,’’ which is a direct online payment from one party to another without using any third party (Nakamoto, 2008).

The general architecture of Blockchain Technology

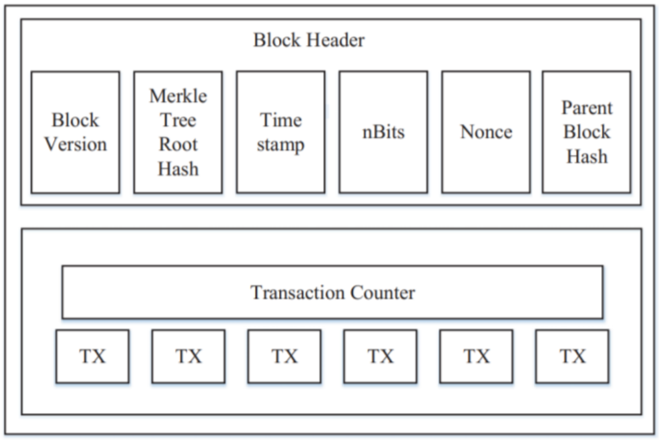

Figure 1. Blockchain Block structure **(**zibin et al., 2017**)**

Figure 1 shows an example of a block as found in a Blockchain. A previous block hash is contained in the block header, and a block has only one parent block. It is worthy of note that uncle blocks (children of the block’s ancestors) hashes would also be stored in Ethereum Blockchain Network (Buterin, 2014). The first block of a Blockchain is called genesis block and it has no parent block.

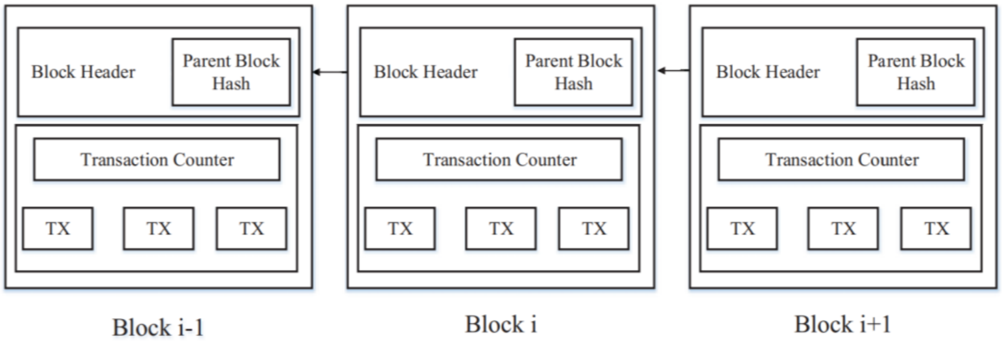

Figure 2. Blockchain which consists of a continuous sequence of blocks (Zibin et al., 2017)

Figure 2 shows a Blockchain which consists of a continuous sequence of blocks. Each block in a Blockchain consists of the block header and the block body. The block header includes; Block version: This specifies which set of block validation rules to follow; Merkle tree root hash: contains the hash value of all the transactions in the block; Timestamp: keeps the current time as seconds in universal time since January 1, 1970; nBits: shows the target threshold of a valid block hash; Nonce: This is a 4-byte field, which usually starts with 0 and increases for every hash calculation; Parent block hash: This is a 256-bit hash value that points to the previous block. The block body is composed of a transaction counter and transactions (TX). The maximum number of transactions that a block in a Blockchain can contain depends on the block size and the size of each transaction.

Characteristics of Blockchain Technology

Below is a discussion of the core characteristics of Blockchain Technology (Murthy et al., 2020).

Decentralized. Unlike the traditional centralized network, that the nodes have to be validated through a trustworthy centralized server, Blockchain does not rely on a centralized server to store and update multiple systems data. In the Blockchain network, all the participants or nodes actively participate in transactions in a decentralized server manner thus; each node also serves as a server within the network.

Persistent. All transactions are validated and stored permanently in the Blockchain therefore, they cannot be manipulated. If the transactions are included in the list, rolling back or erasing the transactions is difficult (Nguyen et al., 2019).

Auditable. Each transaction initiated on a Blockchain is digitally signed by the sender and stored with a timestamp, by this means, every transaction can be tracked and verified by the nodes on the Blockchain (Murthy et al., 2020).

Anonymous. Unlike a centralized network where, a centralized owner will retain the user's real identities, Blockchain transactions make the users anonymous (user identity is kept secret). In the Blockchain, transaction data is secured by using asymmetric encryption techniques and authentication is done by digitally signing the transaction data. The sender interacts with the Blockchain to support a self-generated email and generates a different set of addresses to preserve their identity as a secret (Feng et al., 2019).

Autonomous. No single entity or node controls the Blockchain network. Each new node joining the Blockchain network is signed and accepted by consensus whereby the new node is reviewed and accepted by every other node in the network, ensuring that transactions or data transfer will be done safely in the Blockchain network (Murthy et al., 2020).

Immutable. Blockchain transactions are immutable or tamper proof. The transaction data in the Blockchain is validated before it is accepted into the Block. Each transaction in the Blockchain network is recorded permanently. The data in the blocks cannot be altered. If some entity tries to alter the data, it would be easily caught because data in the blocks is linked through the hash key, and change in the data in one block would invalidate the next blocks (Zhu, Gai, & Li, 2019).

Transparent. The decentralized structure of Blockchain is such that all participants can publish their records and query other nodes' data. In the Blockchain Technology system records and maintains transaction data information in an open distributed ledger (Zhao, 2019). The recorded data in a Blockchain ledger is open and reliable to all the nodes present in the same Blockchain network to access the information.

Traceable. The data in the blocks of Blockchain is encrypted using hashing algorithms. Each block will have a hash key. Each block in the network contains the previous blocks' hash key and is linked through them (Lu, 2019). Therefore, tracing, finding or locating a block in the Blockchain through the hash key is possible in the Blockchain network.

Types of Blockchain Technology

According to Niranjanamurthy, Nithya, & Jagannatha (2019), we can categorize Blockchain into three major types based on the users' availability and accessibility. They are as follows:

Public (Permissionless) Blockchain. A public Blockchain can be described as a decentralized, open ledger Blockchain network in which any node can freely enter the network without requiring permission from any entity and can participate in the processing, validation, and storage of the transaction data through a consensus mechanism. Bitcoin is an example of a public Blockchain.

Private (Permissioned) Blockchain. A private Blockchain can be described as a centralized Blockchain network controlled by a central authority for accessibility in which nodes are selectively allowed into the network. Private Blockchain is specific to limited organizations or small industries. Use cases of the private Blockchain can be found in Supply chain management, Vote counting, Asset Ownership, Digital Identity among others. (Murthy et al., 2020).

Consortium Blockchain. This is a partially decentralized Blockchain network in which pre-selected nodes will have the authority to choose the type of service they will participate in, in advance, while the remaining nodes may have access to the Blockchain transactions but, not through the consensus process. It is a permissioned platform where multiple organizations govern the platform instead of only a single organization. Hyperledger fabric is an example of consortium Blockchain. Hyperledger fabric's primary purpose is creating Blockchain for industries, storing the chain code, and Smart Contracts. One can participate in it by registering for identity to network membership services.

Comparison between Different Types of Blockchain

Table 2
Comparison between Different Types of Blockchain.

S/N	Property	Private	Public	Consortium
1	Consensus process	Permissioned	Permissionless	Permissioned
2	Efficiency	High	Low	High
3	Immutability	Not tamper-free	Tamper-free	Not tamper-free
4	Read permission	Public/restricted	Public	Public/restricted
5	Centralized	Yes	No	Partial
6	Consensus Determination	Limited to one organization	All miners	Selected set of nodes

Phases or Generations of Blockchain Technology

Blockchain technology is categorized into three Phases or generations. Blockchain 1.0; the first generation called digital currency, Blockchain 2.0; the second generation called the digital economy, and Blockchain 3.0; the Third generation called a digital society (Efanov & Roschin, 2018).

First-Generation Blockchain. This is the Blockchain technology introduced through Bitcoin in 2008 as a form of digital currency by the pseudo name Satoshi Nakamoto. The presence of an open distributed ledger in the Blockchain helps the digital currencies to solve the problem of double-spending (a scenario in which the same single digital currency can be spent more than once by duplicating or falsifying the currency's digital file).

Second Generation Blockchain. Smart Contracts were introduced in the second generation of Blockchain thereby extending its use beyond digital currencies to a digital economy. A Smart Contract is a self-executing code with terms of an agreement between two parties (a buyer and a seller), once the terms of the agreement are met, the Smart Contract is activated with a transaction. The Smart Contract data is stored in the tamper-free and anti-forgery block of Blockchain technology. Some uses of Smart Contracts are business agreements, financial data recordings, food supply chains, insurance, mortgages, and so on. Ethereum is an example of a Smart Contract.

Third-Generation Blockchain. Blockchain 3.0 is an upgrade to the first and second generations of Blockchain that aims to address the scalability, cost, interoperability, sustainability, and security related issues of Blockchain 1.0 and 2.0. It promises better solutions with a refined structure making it capable to expand beyond financial services into other areas such as Internet of Things (IoT) being developed to implement smart property transactions without third party involvement. Such transaction capabilities without third party involvement means a digital society where most transactions will be done between unknown people in a trustworthy manner digitally.

Relevant Terms in Blockchain Technology

Mining. Mining can be defined as the process of generating or adding new blocks to the openly distributed ledger of a Blockchain.

Take for instance in Bitcoin or cryptocurrency mining, to create a free-floating digital currency that is likely to acquire real value, you need to have something that is scarce by design. In fact, scarcity is also the reason why gold or diamonds have been used as a backing for money. In the digital realm, one way to achieve scarcity is to design the system so that minting money requires solving a computational problem (or “puzzle”) that takes a while to crack. This is what happens in Bitcoin “mining”. Blockchain mining relies on miners (Individuals who join a Blockchain network with their nodes with the aim of generating new blocks). Miners validate every transaction on the Blockchain, they build and store all the blocks, and they reach a consensus on which blocks to include in the block chain. Miners earn some reward for doing this; in early 2015, the block reward was 25 bitcoins valued at over $6,000 (Narayanan et al., 2016).

Nodes. A Blockchain node can be defined as a device that belongs to the Blockchain network thus participating in transactions within the Blockchain. There are three types or classes of Blockchain node classified based on the task the node does in the Blockchain network; Mining Nodes, Full or Super Nodes and Light Nodes. Mining Nodes are responsible for producing new blocks and sending them to the Blockchain. Full or Super Nodes maintain the blocks, validates them and sends the copies of blocks to all the network nodes. The Light Nodes contain only a portion of the whole block; They contain only the previous transaction blocks and inform the network's remaining nodes about them. Light nodes prevent corruption of the Blockchain. When a full block is compromised, the light nodes can capture the corrupted block and dismiss it as false by presenting the complete node information to the Blockchain.

Consensus Algorithms. A consensus algorithm is a set of instructions on how a new block is accepted into a Blockchain. For Consensus determination, in public Blockchain, each node could take part in the consensus process. Only a selected set of nodes are responsible for validating the block in consortium Blockchain. As for private Blockchain, it is fully controlled by one organization and the organization could determine the final consensus (Zibin et al., 2017). Below is a discussion of different types of consensus algorithms.

PoW (Proof of Work). In PoW consensus algorithm, each node (miner) of the network is calculating a hash value of the block header by changing the nonce frequently to get different hash values. PoW requires that the calculated value must be equal to or smaller than a certain given value. When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own Blockchains (Zibin et al., 2017). PoW is a consensus strategy used in the Bitcoin network (Nakamoto, 2008).

PoS (Proof of Stake). PoS (Proof of stake) is described as an energy-saving alternative to PoW. Miners with more coins, are given the ability to produce the next block, with a believe that miners with most coins are less likely to attack the network. This consensus process is unfair, as the wealthiest miner in the network would begin to dominate the others. Some solutions have been proposed for this unfairness such as selection based on the age of the coin, and randomization (Murthy et al., 2020). Some Blockchains start with PoW then gradually move to PoS (Tosh et al., 2017).

DPOS (Delegated Proof of Stake). The major difference between PoS and DPOS is that PoS is directly democratic while DPOS is a form of representative democracy. The Blockchain node stakeholders elect their delegates to generate and validate blocks. In DPOS, the block could be confirmed quickly due to significantly fewer nodes to validate the block (Zibin et al., 2017).

Ripple. Ripple is a consensus algorithm that utilizes sub-networks that are collectively trusted within the extensive network. In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. (Schwartz, 2014). Each server has a Unique Node List (UNL). An agreement of more than 80% by the nodes in a UNL will have a block recorded in the ledger (Zibin et al., 2017).

PBFT (Practical Byzantine Fault Tolerance). In PBFT, new blocks are determined in a round. In each round, a primary node would be chosen according to some rules, this node is responsible for ordering the transaction. The whole PBFT process can be divided into three phases: pre-prepared, prepared and commit. In each of these three phases, a node would enter the next phase if it has received votes from over 2/3 of all nodes present in the Blockchain (Murthy, et al., 2020).

Tendermint. Tendermint is a byzantine consensus algorithm, similar to the algorithm of PBFT consensus. A new block is determined in a round (Kwon, 2014). However, contrast to PBFT consensus, nodes have to lock their coins to become validators in Tendermint consensus.

Deficiencies in the Current Body of Academic Literature.

There are various recent studies regarding Cloud Computing, and Blockchain Technology found in Academic Literature. However, none attempts to directly discuss the place of Blockchain Technology in Cloud Computing security within private organizations. For instance, Lim et al., (2020) performed an in-depth research regarding Blockchain Based Cloud Computing: Architecture and Research Challenges. Emphasis was placed on some of the significant challenges faced by the Cloud and proposed solutions by integrating it with Blockchain technology. They also developed an architecture for integrating Blockchain with Cloud revealing the communication between Blockchain and Cloud.

Murthy, et al., (2020) performed a study regarding "A Survey on Integrating Cloud Computing with Blockchain". Emphasis was placed on addressing some of the approaches to the problems of Cloud Computing using Blockchain technology. The study went further to discuss the challenges, problems faced by Cloud technology, and the advantages of Blockchain technology. The study also discussed the benefits of the integration of Cloud with Blockchain technology and Blockchain support for Cloud Computing.

Similar studies have been published by others including park & park (2017) on "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", Gupta et al., (2019) on "Cloud Computing Security using Blockchain", Pavithra, Ramya & Prathibha (2019) on "A Survey on Cloud Security Issues and Blockchain". A commonality in all of these studies is that they seem to share an awareness that Blockchain technology has the potential of being a feasible option to the security issues of Cloud Computing. The need for Cloud Computing is gradually increasing day by day however, Cloud Computing security is a major difficulty. Since the data in the Cloud has to be transferred through the internet, the security of data becomes a major concern. The key mechanisms for data protections like integrity, accountability, privacy, access control, authentication, and authorization must be maintained. Blockchain is a technology which makes Cloud Computing better. Blockchain overcomes the security issues in Cloud Computing (Pavithra, Ramya & Prathibha, 2019).

All of the above-mentioned studies are exceptional. Nevertheless, based on the rapidly growing application of Cloud Computing by private organizations in the U.S, the gradual mainstream adoption of Blockchain technology and the lack of published research regarding solutions to Cloud Computing security challenges through Blockchain Technology specifically as it relates to private organizations, the topic warrants research and analysis with an ultimate objective to determine if Blockchain Technology is a feasible option to the security challenges of Cloud Computing in private organizations. In summary, private organizations should learn to understand their Cloud Computing security needs and look into ways of solving those issues through the application or the integration of Blockchain Technology.

Chapter Three: Methodology

Research Design

To address the key research objectives, this research used qualitative method and secondary sources of information. The research design is therefore qualitative in nature with an aim to make generalizations from the selected sources of information.

Selection of the Subjects

Population

According to Fraenkel & Warren (2002), population refers to the complete set of individuals (subjects or events) having common characteristics in which the researcher is interested. In order to maximize access to relevant and significant amount of information regarding the research objectives, the specific population for this study was selected from scholarly or peer reviewed journal articles written in recent years on Cloud Computing, Blockchain technology and Cloud Computing as it relates to Blockchain Technology with emphasis on Security.

Sample

A total of 33 sample sizes were selected in the priority areas (Cloud Computing, Blockchain Technology, Cloud Computing security and Blockchain Technology) from over 90 sources found. Thirteen (13) from Cloud Computing, eleven (11) from Blockchain Technology and Nine (9) from Cloud Computing security and Blockchain Technology.

Data Collection Methods and Procedures

The data collection was from selected secondary sources of research and academic articles found in academic Literature online and in Libraries. The researches and articles were selected based on their credibility, and year of publication. Their credibility or validity was established by selecting sources from “peer-reviewed” journal articles (“refereed journals” or “scholarly journals”). Publications done in recent years were given higher priority.

Methodological Assumptions

One major assumption of the study is that the publishers verified the scholarly articles chosen as accurate information. In addition, the study focuses on U.S. private companies however, materials were chosen from authors in different countries to increase the breadth of knowledge on the subject matter with an assumption that most Cloud security issues are common to private companies around the globe and will affect them relatively the same.

Chapter Four: Results

The results section of a research work reports the findings of the study based upon the methodology (or methodologies) applied to gather information. This section aims to state the findings of the research arranged in a logical sequence without bias or interpretation (Annesley, 2010).

According to the research done in this paper, amazingly, all of the authors from the selected thirty three (33) publications lean toward or favor the null hypothesis that Blockchain technology is a feasible option to solve the security challenges facing Cloud Computing. However, they also acknowledge that a question that remains to be answered and verified further is the efficiency of integrating Blockchain with Cloud Computing for security purposes. It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public Blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium Blockchain and private Blockchain could be more efficient (Zibin et al., 2017).

Different architectures have been proposed by different authors on how to properly integrate Blockchain technology with the Cloud. A common line of thought behind them is to create a decentralized Cloud Computing network that operates based on the Blockchain Technology's capability of anonymity and cryptography to achieve secure data transactions.

Skulj, et al., (2017) suggested a decentralized architecture of Cloud development, focused on an autonomous operating framework. However, the lack of standard design and standard communication in the architecture proposed gives the system a sense of instability **(**Barenji et al., 2019).

Murthy et al., (2020) suggested an architecture that uses the Blockchain as a database instead of the traditional Cloud database. In this architecture, the data going to the Cloud is processed through the Blockchain mechanisms of division into chunks, encryption and consensus before being stored in either a public or private Blockchain network depending on whether the data is restricted to a network and whether there is a central authority that updates and maintains the destination Blockchain.

Chapter Five: Discussion, Conclusion, and Recommendations

Discussion

The cryptographically secure nature of the Blockchain makes it very attractive for security in Cloud Computing especially as it relates to private organizations.

According to Bozie et al., (2016), Blockchain seems a promising way of ensuring privacy in the Clouds, through an authorized Blockchain technology application called a wallet that helps us to remove our data safely in the Cloud in order to protect it from any third party access. Blockchain is known for its symbolic cryptography technology. Blockchain can be transformed to a scalable service that, combined with the Cloud storage environment, offers greater security. When using the Blockchain technology for saving user details in the Cloud storage world, the user's privacy can be guaranteed (Murthy & Shri, 2020).

With the incorporation of Blockchain technology, the Cloud user's privacy can be guaranteed. One solution is by the use of electronic wallet that would be installed and uninstalled safely as needed (Ingole, & Yamde, 2018).

Blockchain ensures that we will not have to worry about the Cloud vendor tampering with our data. Accessing Cloud Computing lets us trust a third party or vendor with our confidential data. This feature of Cloud Computing deters some organizations from using the Cloud services as the vendor could steal or modify the data. With Blockchain integration on the Cloud this concern can be solved by saving data in a distributed decentralized network using Blockchain technology, thereby having no need of a central provider (Harshavardhan, et al., 2018).

Blockchain ensures the validity, and integrity of data in Cloud Computing. Information is decrypted before it is saved in the Cloud, which challenges the data validity. However, In the

Blockchain network, the entire block data is converted into hash code using cryptographic algorithms, and recorded. Because the Blockchain has the instruments for discovering the blocks through consensus, the integrity of the block data is preserved (Murthy & Shri, 2020).

With Blockchain technology incorporated on the Cloud, we do not have to worry about an attacker getting access to our data on the Cloud. An organization can create its own database and store the data as blocks on different hard disk drives using Blockchain technology. If an attacker attempts to steal data from the organization, it will be difficult to reach all of the blocks. If he does, however, hack a block; it would be useless because he cannot alter the hash of another block (Murthy & Shri, 2020).

Blockchain optimizes the availability of Cloud services. According to Ingole & Yamde (2018) although Cloud-collected data is secure, the Blockchain nodes optimize data availability and validity by projecting it as a non-stop-time on-demand service.

Moreover, the parties involved on Cloud Computing could breach Service Level Agreements in the Cloud but with Smart Contracts in Blockchain, these Cloud arrangements could be trusted since Blockchain Smart Contract could solve this problem by building trust. A Blockchain Smart Contract helps build trust between those parties that do not know each other (Tosh, et al., 2017).

Conclusion

The major objective of this study was to determine whether Blockchain technology is a feasible option to solve the security challenges facing Cloud Computing. In conclusion, based on the available literature and the extensive study done in this paper, it is the fervent opinion of the author that Blockchain technology is a feasible option to solve the security challenges facing Cloud Computing.

Incorporating Blockchain into Cloud Computing provides security to the Cloud through data protection and transparency, and further helps to improve Cloud services (Murthy et al., 2020).

According to Michael & Herbert (2018) the three major Components of Information Security culminates in the CIA Triad (CIA - Confidentiality, Integrity and Availability). With Blockchain incorporation into Cloud Computing, we can ensure the CIA of data on the Cloud. The Cloud user’s privacy can be guaranteed, we will not have to worry about the Cloud vendor stealing or modifying our data, we are assured of the validity and integrity of data, and the availability of Cloud services is optimized.

Recommendations

Based on the wealth of knowledge gathered during this research from various authorities in Cloud Computing and Blockchain technology, the author would like to recommend the below architecture for incorporating Blockchain technology into Cloud Computing to provide a more secure Cloud operations and wider adoption of Cloud Computing among private organizations. Cloud providers usually guarantee the security of the information through some security mechanisms. However, sometimes, leakage of information does occur (Nazir, 2012), such as the information leakage issue that happened in ICloud storage where a large portion of the celebrities's information got leaked to the people. Such security issues deter organizations from utilizing the Cloud and its services (Fernandes, 2014).

The major aim of this architecture is to provide trust and help reduce or probably eliminate the security concerns being faced by some private organizations about Cloud adoption. The below architecture would be referred to as the "Cloudchain" model of Cloud-Blockchain integration.

The main attractive nature of Cloud Computing is having to delegate computing needs to a third party, however a major security concern is that the third party will become a custodian of our data. With Blockchain technology, one might argue using the Blockchain mechanisms to encrypt the data and store it in a Blockchain network. This Blockchain network could be one of three options; that of the cloud provider, that of the data owner, or other Blockchain Networks (public or consortium).

The aforementioned options each have their own concerns. Most private organizations who need Cloud service providers do not usually have enough budget to develop and maintain their own Blockchain storage network. If this Blockchain network is that of the third party or cloud provider, the third party would still have an upper hand in the data, being a central authority that oversees and maintains the Blockchain and probably with more nodes to control in the network. If this is another Blockchain network other than the Cloud provider's and the data owner's, then we will have to worry about the scalability, interoperability and efficiency of those Blockchain networks.

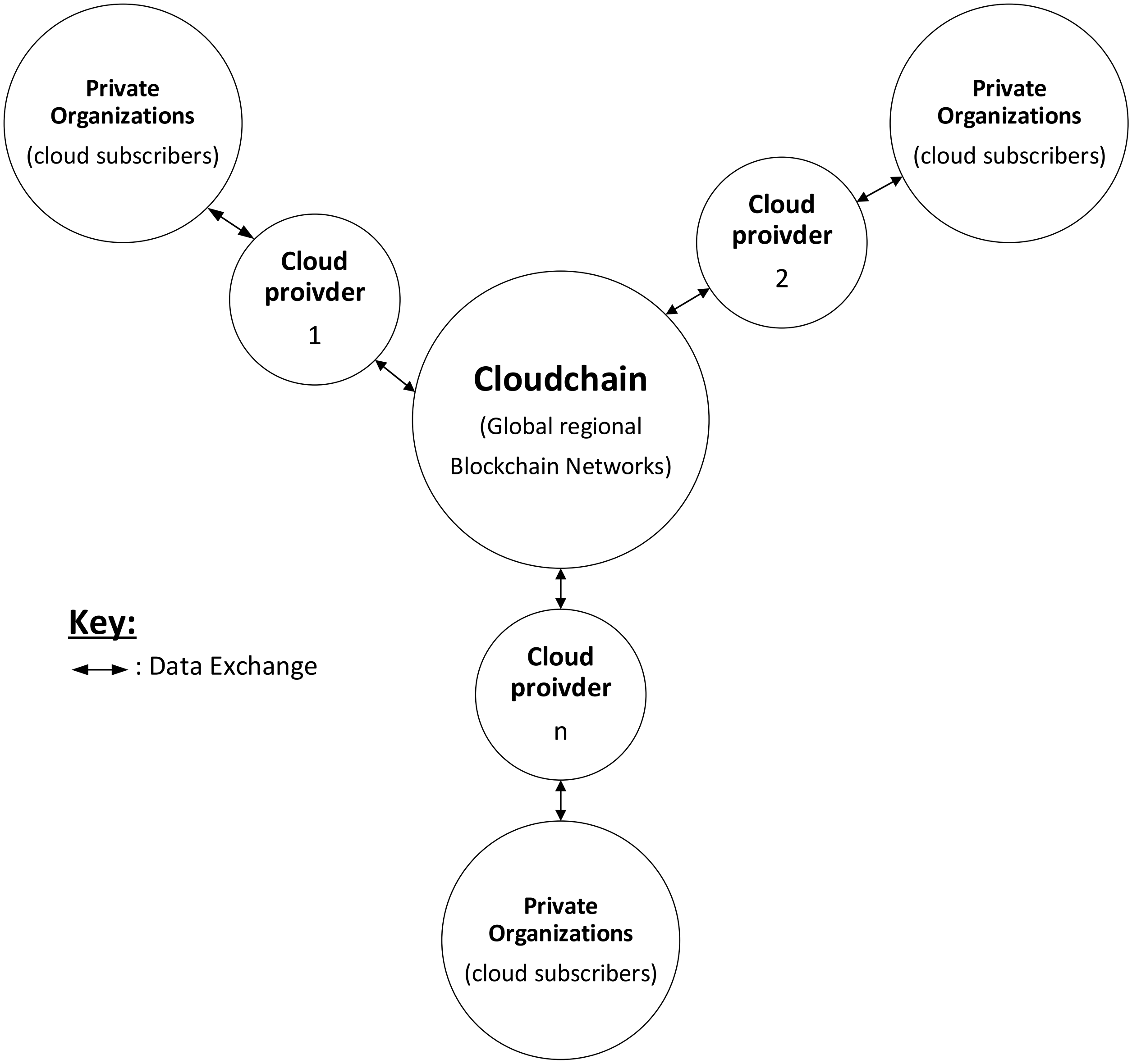

Figure 3. Cloudchain model of Cloud-Blockchain Integration

In this case, the author would like to propose the "Cloudchain" architecture, a globally distributed form of Blockchain networks (more like the internet) having a minimum number of nodes in each region at any given time on to which organizations can route and store their data in a totally decentralized and trusted manner. The benefit is that, there is no central Blockchain network that stores user data. Storage is so decentralized in such a way that even the Cloud provider does not know the exact Blockchain networks housing their user data. Cloud providers would have to join this global pool of nodes (Global Regional Blockchain Networks); joining the global pool will help to ensure users or private organizations that their data is well decentralized, very available and secure.

Furthermore, the author would like to recommend that further research ought to be carried out on not only the efficiency of Cloud Computing and Blockchain technology integration for security but, also on the energy consumption overhead of integrating Blockchain technology with Cloud Computing as it may affect private organizations.

References

Agrawal, D., Abbadi, A. A. E., Das, S., & Elmore, A. J. (2011). *Database scalability, elasticity, and autonomy in the Cloud.* Berlin, Germany: Springer.

Agrawal, S., Biswas, R., & Nath, A., (2014). Virtual desktop infrastructure in higher education institution: Energy efficiency as an application of green computing. *Proceeding of 2014 Fourth International Conference on Communication Systems and Network Technologies CSNT 2014, pp. 601-605.*

Annesley, T. M. (2010, July 1). Show Your Cards: The Results Section and the Poker Game. *Oxford academy, clinical research*. doi: https://doi.org/10.1373/clinchem.2010.148148

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., & Zaharia, M. (2009, February 10). Above the Clouds: A Berkeley view of Cloud Computing. *Technical report EECS-2009-28, UC Berkeley*. Retrieved from https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Ashok, G., Shams, T. S., Shadab, A., & Mohammed, S. (2019). Cloud Computing Security using Blockchain. *Department of Computer Science, Jazan University*.

Barenji, A. V., Guo, H., Tian, Z., Li, Z., Wang, W. M., & Huang, G. Q. (2019). Blockchain-Based Cloud Manufacturing: Decentralization. *Conference: Advances in Transdisciplinary Engineering*. doi:10.3233/978-1-61499-898-3-1003

Bowers, K. D., Juels, A. & Oprea, A. (2008). HAIL: A High-Availability and Integrity Layer for Cloud Storage. *Cryptology ePrint Archive: Report 2008/489.* Retrieved from https://iacr.org/cryptodb/data/paper.php?pubkey=18179

Buterin, V. (2014, January 4). A next-generation Smart Contract and decentralized application platform. *white paper*.

Byrne, D., Corrado, C., & Sichel, D. E. (2018). The Rise of Cloud Computing: Minding Your P's, Q's and K's. *NBER Working Paper Series.*

Chen, Y., Paxson, V., & Katz, R. H. (2010, January 20). What's New About Cloud Computing Security? *Electrical Engineering and Computer Sciences University of California at Berkeley.*

Retrieved from https://www2.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

D. C. Nguyen, P. N. Pathirana, M. Ding, & A. Seneviratne (2019). Integration of Blockchain and Cloud of things: Architecture, applications and challenges. *arXiv.* Retrieved from http://arxiv.org/abs/1908.09058

Efanov, D., & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science.* doi: 10.1016/j.procs.2018.01.019.

Farah, N. A. A. (2018). Blockchain Technology: Classification, Opportunities, and Challenges. *International Research Journal of Engineering and Technology.*

Feng, Q., He, D., Zeadally, S., Khan, M. K. & Kumar, N. (2019). A survey on Privacy protection in Blockchain system. *Journal of Network and Computer Applications.* doi.org/10.1016/j.jnca.2018.10.020

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inacio, P. R. (2014). Security issues in Cloud environments: a survey. *International Journal of Information Security*. Retrieved from https://www.di.ubi.pt/~mario/artigos/2013-IJIS.pdf

Fraenkel F.J., Warren N.E. (2002). *How to Design and Evaluate Research in Education*. (4th ed). New York: McGraw-Hill.

Harshavardhan, A., Vijayakumar, T., & Mugunthan, S. R. (2018). Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities. *2018 2nd International Conference on I-SMAC.* doi: 10.1109/I-SMAC.2018.8653690

IGI Global. (2021). What is Feasible Solution. *IGI Global, Publisher of timely knowledge.* Retrieved from https://www.igi-global.com/dictionary/feasible-solution/55054

Ingole, M. K. R., & Yamde, M. S. (2018). Blockchain Technology in Cloud Computing: A Systematic Review. *International Research Journal of Engineering and Technology (IRJET).* Retrieved from https://www.irjet.net/archives/V5/i4/IRJET-V5I4428.pdf

Jabbari, A., & Kaminsky, P. (2018). Blockchain and Supply Chain Management. *Department of Industrial Engineering and Operations Research University of California, Berkeley.*

Kangchan Lee. (2012). Security Threats in Cloud Computing Environments. Electronics and Telecommunications Research Institute International Journal of Security and Its Applications. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of Blockchain technology: pros, cons, and SWOT. *Cluster Computing* 22, 14743–14757. doi: 10.1007/s10586-018-2387-5

Katuwal, G. J., Pandey, S., Hennessey, M., & Lamichhane, B. (2018). Applications of Blockchain in Healthcare: Current landscape & challenges. *arXiv preprint arXiv*.

Kwon, J. (2014). Tendermint: Consensus without mining. *Tendermint*. Retrieved from https://tendermint.com/static/docs/tendermint.pdf

Michael, E. W., & Herbert, J.M. (2018). *Principles of Information Security*. Boston, Massachusetts: Cengage Learning.

Murthy, B. Ch.V.N.U., & Shri, M. L. (2020). A Survey on Integrating Cloud Computing with Blockchain. *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).* doi:10.1109/ic-ETITE47903.2020.470

Murthy, B., Shri, M. L., Kadry, S. & Lim, S. (2020, November 9). Blockchain Based Cloud Computing: Architecture and Research Challenges. *Institute of Electrical and Electronics Engineers (IEEE).*

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016, February 9). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. New Jersey, NJ: Princeton University Press.

Nazir, M. (2012). Cloud Computing: overview & current research challenges. *IOSR Journal of computer engineering*. doi:10.9790/0661/0811422

Park, J. H. & Park, J. H. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) Seoul 01811, Korea.*

Pavithra, S., Ramya, S., & Prathibha, S. (2019, September 5). A Survey on Cloud Security Issues and Blockchain. *2019 third International Conference on Computing and Communications Technologies (ICCCT), Chennai, India.*

Perry, J. L., & Rainey, H. G. (1988). The public- private distinction in organization theory: A critique and research strategy. *The Academy of Management Review 13: 182–201.*

Popovski, L., Soussou, G., & Webb, P. B. (2014). *A brief history of Blockchain*. New York, NY, USA. Patterson Belknap Webb & Tyler.

Ren, K., Wang C., Wang, Q. (2012, January 09). Security Challenges for the Public Cloud. *IEEE Internet Computing.* doi:10.1109/MIC.2012.14

Roure, D. D., Baker, M. A., Jennings, N. R., & Shabolt, N. R. (2003). *The Evolution of the Grid*. Chichester, England: John Wiley & Sons, Ltd.

Santos, N., Gummadi, K.P. & Rodrigues, R. (2009). Towards trusted Cloud Computing. Hot Cloud 2009. *The Max Planck Institute for Software Systems*.

Schwartz, D., Youngs, N., & Britto, A. (2014). “The ripple protocol consensus algorithm,” *Ripple Labs Inc White Paper, vol. 5, 2014*.

Sharma, S., Gupta, G., & Laxmi, P. R. (2014). ‘‘A survey on Cloud security issues and techniques,’’. *arXiv.* Retrieved from http://arxiv.org/abs/1403.5627

Skulj, G., Vrabic, R., Butala, P., Sluga, A., (2017). Decentralized network architecture for Cloud manufacturing. *International Journal of Computer Integrated Manufacturing.* doi: https://doi.org/10.1080/0951192X.2015.1066861

Tosh, D., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. L. (2019). Data Provenance in the Cloud: A Blockchain Based Approach. *IEEE Consumer Electronics Magazine*. doi:10.1109/MCE.2019.2892222

Venters, W. & Whitley, E. A. (2012). "A critical review of Cloud Computing: Researching desires and realities". *Journal of Information Technology. doi:10.1057/jit.2012.17*

Vikram, K., Prateek, A., & Livshits, B. V. (2009). Automatically securing web 2.0 applications through replicated execution. *Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009.* doi:10.1145/1653662.1653685

Vocabulary.com. (n.d.). Feasible. *vocabulary.com*. Retrieved from https://www.vocabulary.com/dictionary/feasible.

Y. Lu, (2019). The Blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration.* doi:10.1016/J.JII.2019.04.002

Zibin, Z., Shaoan, X., Hongning, D., Xiangping, C., & Huaimin, W. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress).* doi:10.1109/BigDataCongress.2017.85

Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., & Boshkoska, B.M. (2019). ‘‘Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions,’’. *University of Plymouth*. doi: http://dx.doi.org/10.1016/j.compind.2019.04.002

Zhu, L., Gai, K., & Li, M. (2019). *“Blockchain and the Internet of Things,” in Blockchain Technology in Internet of Things*. Cham, Switzerland: Springer.