Blockchain distributed cloud storage and its forensic aspects

ADIL MONU LALI PRABHAKAR

|

Table of Contents

List of Figures

Abstract

This project is going to be a research paper based on how the block chain based distributed cloud helps to confront a verity of limitation that the field now has, including the forensic investigation and the added level of security that the block chain will offer for the organization which used cloud storage.

Cloud computing is the technology that is currently the subject of much discussion, as well as ongoing research and development efforts, and implementation trials are currently being conducted.

On the other hand, unlike any other form of data storage technology, it comes with its own set of disadvantages, chief among which is the concern over the safety of the stored information. When a company moves its data storage to the cloud, the cloud provider takes on some of the responsibility for the data's safety. However, the validation and storage of original data in this network of cloud when compared to a normal forensic copy of file and the security factor of hashing involved in this system when analysed using a comparative analysis using a blockchain-based cloud distribution system is a methodology implemented to cut down the few concerns of data security. The latest development of blockchain-based cloud distribution is a methodology implemented. The purpose of the research being conducted for this project is to focus on hashing methodologies and to perform a demonstration data hashing within a blockchain stimulator in order to arrive at a comparative conclusion regarding the attributive differences and the benefactors in data security and digital forensics.

Dissertation structure

1. **Chapter 1 – Introduction:** In this section, we will conduct a quick overview of the subject matter that is the overview of the research as well as establish the study's overarching research motivation, objectives, and research questions.
2. **Chapter 2 – Literature Review:** This chapter examines how blockchain relates to security as well as the current degree of knowledge on distributed cloud computing as it is found in academic publications. It sheds light on the knowledge void that will be filled as a result of this research.
3. **Chapter 3 – Background Research:** In this section, we will cover the current state of the blockchain technology, what cloud storage is and its various elements, Forensic investigation as well as the current condition of cloud computing and where it stands currently. Because of this, we will have a significantly deeper understanding of the problem at hand, in addition to the challenges that we have in addressing it.
4. **Chapter 4 – Research Methodology:** In the following paragraphs, I will discuss the methods that I used to collect data for my study and then analyse that data. This incorporates the methodology of the study, which includes the approach, strategy, data gathering methods, and data analysis procedures. In other words, this encompasses the entirety of the methodology.
5. **Chapter 5- Practical visualisation:** in this section, in a hypothetical forensic setting, the blockchain and its functionality are tested.
6. **Chapter 6 – Research Analysis and Findings:** In this section, the findings of the study are broken down and evaluated with reference to existing theory and evaluate the advantage of new proposed model.
7. **Chapter 7 – Conclusion and Recommendation:** This chapter provides a summary of the findings of the research and makes some suggestions for new lines of inquiry that could be pursued in the field of blockchain technology as it relates to cloud computing and its forensic applications.

Chapter 1 - Introduction

1.1 Overview

These days, the concept of "the cloud" appears to be all over the place. Cloud computing is the topic that everyone is discussing right now, despite the fact that "the Cloud" is just a metaphor. We've reached the tipping point where it's appropriate to proclaim that apps of the future will always be hosted online, and it's time for us to make the announcement. At this time, the bulk of company applications and customer requirements may be met by utilising cloud computing solutions. Cloud service providers such as Dell EMC and Amazon are interested in cloud-based services because it is believed that these services offer greater benefits than traditional data centres.

On the other hand, it is plagued by its own one-of-a-kind collection of problems, the most serious of which are to matters of security. When a company moves its data storage to the cloud, the cloud service provider takes on some of the responsibility of safeguarding that data. Because of the blurring of trust boundaries and the increase in data accessibility, dishonest cloud users may have greater opportunity to attack IT infrastructure and steal or destroy important company data. This is because of the increased availability of data.

In order to address the cloud security issue that has been brought to light, a "distributed cloud model" that makes use of blockchain technology is now being investigated as a potential solution.

Using the block chain method in distributed cloud storage will give a huge advantage not only to the security of the data but also to digital forensic investigation. The fact that everything in the world is currently transitioning to digital format is common knowledge, thus this is the evidence. The evidence must be in a state that may be presented in court while maintaining its integrity and candour. If someone is able to tamper with the evidence after a case, the entire story of the investigation will lead to a disaster. With the new proposed block chain-based cloud distributed system, the block chain is highly secured, which means that nobody without authorization can tamper with the evidence, and it will lead to a significant advantage in the field of digital forensics.

Within the scope of this study proposal, we will talk in great length about cloud storage, its current state, block chain-based cloud storage, and the benefits it offers in terms of the foundation of security as well as digital forensics.

1.2 Project Motivation

conscious of the ever-increasing importance of the industries of block chain and cloud storage around the world. The goal of this research project is to explore the significance of block chain technology in terms of data security, the significance of block chain-based cloud storage for digital forensics, as well as the existing and foreseeable difficulties facing the industry as a whole.

1.3 Research aim and question

The focus of this study is on achieving the following:

- To understand if and how the implementation of block chain in a distributed cloud storage will help the world of cyber security and digital forensics.

The following are some of the specific research questions that will be answered by the study:

RQ1: How the traditional cloud storage works and the challenges it faced?

RQ2: How Blockchain can mitigate the existing flaws and heightened the security of the data?

RQ3: What benefits does blockchain have for digital forensics?

1.4 Project Objective

1. Main objective of the project is to evaluate the advantages of Blockchain based cloud-distributed storage against more conventional options.
2. Pointing out the forensic aspect of this cloud storage and proving the data transparency and difficult to tamper the evidence due to decentralised server.
3. Proving the benefit and security feature of the block chain using a simulator and explaining the entities.

Chapter 2 – Literature Review

Kanishk Kumar The author of the paper titled "Distributed Cloud Storage Using Blockchain Technology" demonstrates how cloud storage has supplanted more conventional approaches to the storage of system or logistical data in favour of an approach that is more reliable and safer. He then moves on to highlight the widespread problems that have been discovered with traditional cloud storage, as well as the way that the paradigm of traditional cloud storage is being transformed into blockchain cloud distribution. the properties of distributed cloud storage, the distributed cloud designs that were taken into consideration, and the structure of the system itself are the topics to be covered here. He then continues on to describe the various blockchain networks, their benefits, and the use cases they may accommodate. Because of this, we may draw the conclusion that there will be more than 50 billion devices connected to the internet, which suggests that there will be an increase in the production of content for the internet as well as an increased demand for safe storage. Many of the services that are currently handled by cloud intermediaries can be replaced by a well-designed and publicly available distributed cloud. These services include providing a reliable trading environment, protecting against fraud, ensuring contract and compliance, and facilitating financial transactions. (Kumar, 2018)

Frank Breitinger | Ibrahim Baggili | Joseph Ricci | - "Distributed cloud storage based on blockchain technology Where's the Beef When It Comes to Digital Forensics? "Is the name of the paper published. However, they also delve deeper into the potential problems that could develop with these in terms of the collection of digital evidence. One of these potential concerns is the recovery of files and information that can be valuable in a prosecution. They investigated each advantage that could be gained from utilising blockchain technology. It is necessary to find a solution to this issue because it is not known for certain whether or not such data can be retrieved from the local storage of a suspect. They then continue to explain how Because STORJ is a new service that assists forensic examiners in reconstructing evidence for forensic purposes without compromising the conclusion of a case, a detailed investigative procedure is required. As a result, it is essential to conduct research into the establishment of a forensically sound approach for acquiring evidence and artefacts from farmers and clients on the STORJ network. This research must be carried out as soon as possible. This then leads to an investigation into the digital artefacts that were produced by STORJ. despite the fact that not all of the artefacts that were produced as a result of using this service have been completely acknowledged to this day. They also recommend an area of applied study that would produce a tool for STORJ's API interface that may possibly retrieve files and metadata that would be essential to a case. Finally, they say that this field of research should be considered. (Ricci, et al., 2019)

Erez Waisbard and Louis Shekhtman The authors of the study titled "Engrave Chain—A blockchain-based Tamper-Proof Distributed Log System" emphasise the requirement of precisely logging transactions in many different industrial domains, as well as the significance of doing so in relation to financial systems. They also emphasise the significance of possessing a large number of copies in order to assure the availability and dependability of the information in the face of such dangers. On the other hand, thanks to recent developments in blockchain technology, distributed storage can now be implemented. A tamper-proof record keeping system can also be created using blockchain technology. They were able to design a fool proof log management system thanks to the immutable write action and distributed storage that the blockchain provided for them. They ultimately perform a demonstration of the system's performance at a large scale, illustrating its requirements over Hyperledger Fabric as well as the system values it provides. (Shekhtman & Waisbard, 2021)

Fran Casino, Constantinos Patsakis, Thomas K. Dasaklis |- In the study titled "Blockchain Solutions for Forensics," it is discussed how information-intensive operations are increasingly being digitalized and how there is a rising concern over how to address the issue of cybercrime, which is getting worse and worse. The study was conducted by the University of Washington. In order to accomplish this, law enforcement officials and security corporations make use of cutting-edge digital forensics techniques to investigate and analyse cases of cybercrime. A few of the many obstacles that prevent the adoption and implementation of sound digital forensics schemes are the massive amount of evidence that is gathered (multimedia, text, and so on), interoperability issues, and the involvement of a large number of stakeholders (law enforcement agencies, security firms, and so on). Recent discussions have brought up the possibility of utilising blockchain technology as a potential method for the development of efficient digital forensics systems. They present an overview and classification of the many blockchain-based digital forensic tools that are now accessible, as well as the essential elements of the tools that they outline in this study. In addition to this, they offer a comprehensive analysis of the benefits and challenges posed by the interplay between blockchain technology and the prevalent approaches to digital forensics, which has the potential to be mutually beneficial. They give suggestions for further research based on the findings, which are expected to be of exceptionally high value to academics as well as practitioners working in the field of digital forensics. In addition to this, a number of unanswered scientific questions are raised. (Casino, et al., 2021)

Xinggang Xuan, Jingsha He, and Gongzheng Liu The authors of the paper titled "A data Preservation method based on blockchain and multidimensional Hash for Digital Forensics" discuss how the originality and validity of data have come under increased scrutiny as a result of the growing popularity of digital forensics. So, new data preservation technology is being created. Even though attacks and cracking are possible, contemporary data preservation models and technologies are cryptographic combinations. Data preservation needs human intervention, which might lead to data alteration. The authors of this work propose a data preservation solution based on blockchain technology and multidimensional hashing. Decentralization and smart contract capabilities of blockchain allow data to be automatically saved without human input to set up a branch chain of custody in the unit of case. They also mention blockchain's good anti-attack performance, notably with reference to the 51% attack. In the meantime, a serialised main chain of custody is being created using hashes, cryptography, and timestamps to address the issue of data confusion and the difficulty in querying brought on by the excessive number of cases. This is being done in order to address the issue of the excessive number of cases. However, multidimensional hash is used in place of conventional hash because the conflict between hash and legal trial necessitates that the authenticity and validity of data be totally ensured. This can only be accomplished through the use of multidimensional hash. Because of this, the process of data preservation is now automatic and unaffected by the intervention of humans. Experiments have shown both the safety and effectiveness of the model that has been offered. (Liu, et al., 2021)

Casino Fran Lamprini - In the investigative research paper titled "A blockchain-based Forensic Model for Financial Crime Investigation: The Embezzlement Scenerio," an example of a financial crime landscape that is evolving along with the digitisation of financial services is used to demonstrate how laws, regulations, and forensic methodologies cannot effectively cope with the growth pace of novel technologies. This results in late adoption of measures and legal voids, which in turn provides a fruitful landscape for financial criminals. The immutability, verifiability, and authentication features that are offered by blockchain technology contribute to an enhancement in the strength of financial forensics. They provide a taxonomy of the financial investigative methods that were utilised the most frequently in this study, as well as a comprehensive examination of the state of the art regarding blockchain-based digital forensic tools. In addition, they create and implement a structure for forensic investigations that is based on standardised practises and document the proper strategy for investigations into schemes of embezzlement. In addition to being applicable to ordinary internal audits, the feasibility and flexibility of this technique can also be expanded upon and applied to various types of fraud investigations. In addition to this, they provide a working system that is based on Ethereum and has built-in procedures for the maintenance of chain of custody as well as standardised forensic flows. In addition to the consequences for management and prospective areas for further research, they also investigate the challenges presented by the complementary interaction between blockchain technology and financial investigations. (Lamprini, 2021)

Youssef Iraqi, Sameera Almulla, Andrew Jones, - In this essay, the authors discuss cloud computing and digital forensics because they are both hot issues that call for knowledge of their key components in order to be thoroughly researched. Since the fundamental components of cloud computing, such as virtualization and distributed computing, are crucial to determining its impact on current digital forensics guidelines and practices, it is necessary to survey them as well as to understand their characteristics, various services, and deployment models. In contrast to other publications, this one will focus on the fundamental aspects of cloud computing that are necessary to deliver forensics-friendly cloud services, rather than the potential and challenges that cloud computing presents for digital forensics. In addition, we offer a list of queries that will help with cloud forensics examination. (Iraqi, et al., n.d.)

Rahul Saha, Chhagan Lal, Mauro Conti, and Gulshan Kumar This topic is discussed in detail in the article titled "Internet of Forensics: A blockchain-based digital forensics framework for IoT applications," which can be found here. The authors explain why digital forensics is necessary in the Internet of Things (IoT) paradigm by pointing out how the evidence processing might be unpredictable and how there is a lack of transparency in the system. In addition, the veil of legal worries that surrounds the process of legalisation across international borders makes this operation more difficult. It is also stated how important it is to have an Internet of Things forensic architecture that provides distributed computing, decentralisation, and transparency of forensic investigation of digital evidence from a worldwide perspective. In order to accomplish this goal, they have developed a framework for Internet of Things forensics that addresses the issues discussed above. The proposed solution that has been developed by Internet of Forensics (IoF) takes into account an infrastructure for digital forensics that is blockchain-specific. It provides a transparent view of the research process from every conceivable vantage point, including cloud service providers and makers of heterogeneous devices. It manages the investigation process, including the chain-of-custody and the evidence chain, by utilising a case chain that is built on blockchain technology. Concerns regarding the legalisation of activities that take place across borders are handled through consensus in a consortium. Additionally beneficial are the openness and ease of use provided by forensic references. The use of the programmable lattice-based cryptography primitive results in a reduction in the level of complexity. It draws attention to the benefits that can be gained for power-conscious gadgets and emphasises the originality of the proposed method. IoF(Internet of Forensics) is recommended to be utilised by autonomous security operation centres, cyber-forensic investigators, and manually initiated evidences under chain-of-custody for crimes done by people due to the fact that it is generic. The purpose of this article was to look at the problem of investigation openness in forensics involving digital evidence and try to come up with a solution. (Saha, et al., 2021)

Sanjeev Sofat, Kailash Kumar, S.K. Jain, and Naveen Aggarwal - In the following study, the significance of hash value generation in digital forensics is described in greater detail: They cover the digital forensics techniques that are frequently used to establish the hash value of a drive that contains digital evidence. These approaches are used to verify the integrity of the data on the drive. In digital forensic tools, the MD5 and SHA hash functions are used to calculate and verify the integrity of a data set. This is done since the process of obtaining and analysing evidence requires the utilisation of a wide variety of tools and methods. In addition, they argue that it is essential to verify that the instruments and procedures are running correctly because of the influence that an investigation will have on the subject's personal life. This paper also discusses the significance of hash values in the field of digital forensics for the analysis of digital evidence. This research performs six different probable situations as an experiment to generate and validate the hash value of test drive using the forensic tool. The purpose of this is to demonstrate the significance of hash value in digital forensics, which is why the experiment is carried out. In addition, an illustration is provided that further illustrates how the incorrect implementation of the instruments may lead to erroneous results. (kumar, et al., n.d.)

Veronica Schmitt and Jason Jordaan were the winners. This paper, titled "Establishing the Validity of Md5 and Sha-1 Hashing in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms," establishes that Md5 and Sha-1 hashing are valid for use in digital forensic practise. They explain how the usage of the cryptographic hash algorithms MD5 and SHA-1 in digital forensics is a standard practise that is used to preserve digital evidence and guarantee the evidence's integrity. They make analogies to recent studies that indicate collisions and weaknesses in MD5 and SHA-1, and they use them to illustrate their points. In light of this, some individuals have raised concerns about the use of the MD5 and SHA-1 hash algorithms in the field of digital forensics, which is intended to safeguard and ensure the authenticity of digital evidence. The researcher uses experimentation to demonstrate the validity of using either the MD5 or SHA-1 hashing algorithms to ensure the integrity of seized digital evidence from the time of seizure until the eventual presentation and use of the evidence in court. This is done to demonstrate that the use of hashing is still a valid forensic methodology for ensuring the integrity of digital evidence. The researcher's goal is to show that the use of hashing is still a valid forensic methodology. (Schmitt & Jordaan, n.d.)

Chapter 3 – Background Research

To begin, let's define "cloud storage" and "distributed cloud storage" so we can understand deeply the underlying problems and advantage of this research. In this article, we will discuss the fundamentals of block-chain systems, the current condition of these two, and the challenges they confront. We will also discuss about the importance of digital forensics and the role of these two in forensic as well.

3.1 Cloud storage

Off-site storage that is managed by a third party, also known as "cloud storage," is an alternative to storing data on the premises of an organisation. Cloud storage allows you to avoid the hassle of storing your vital documents on the hard drive of your computer or another storage device by uploading them to a remote database in a safe and secure manner. The use of cloud storage has many advantages over storing data on local hard drives. To begin, you do not need to be concerned about the possibility of losing significant data because it is not necessary to physically hold the storage device, as you would be required to do with a flash drive, for example. The second benefit of using cloud storage is how easy it is to share files. Simply share a Dropbox folder with a colleague to give them immediate access to the files inside. The reduction in expenses is a wonderful additional benefit that comes along with adopting cloud storage. It is considerably more cost-effective — and prudent — to have infinite cloud storage for a little fee than buying and maintaining a lot of hard disc storage space. This allows the user to access their data from anywhere at any time. (IBM cloud education, 2019)

Figure 1 : Cloud Storage

3.1.1 How does it work?

Cloud storage operates in a manner that is analogous to that of on-premise storage networks in that it uses servers to store data; however, the data is transferred to servers that are located in remote locations. Virtual machines, which are hosted on physical servers, make up the vast majority of the servers that you make use of. As your needs for storage space increase, the provider will continue to construct additional virtual servers in order to keep up with the demand.

When you want to use the cloud storage service over the internet or a dedicated private connection, you will most likely utilise a web portal, a website, or a mobile application. Your information is sent from the server to which you connect to a group of other computers that are stored in one or more data centres. The scope of the cloud provider's operations determines whether or not this happens.

In order to guarantee data protection, service providers routinely save copies of the same information on many storage devices. Even if a server is unavailable for some reason, such as for maintenance or an outage, you will still be able to access the data it stores for you. (IBM cloud education, 2019)

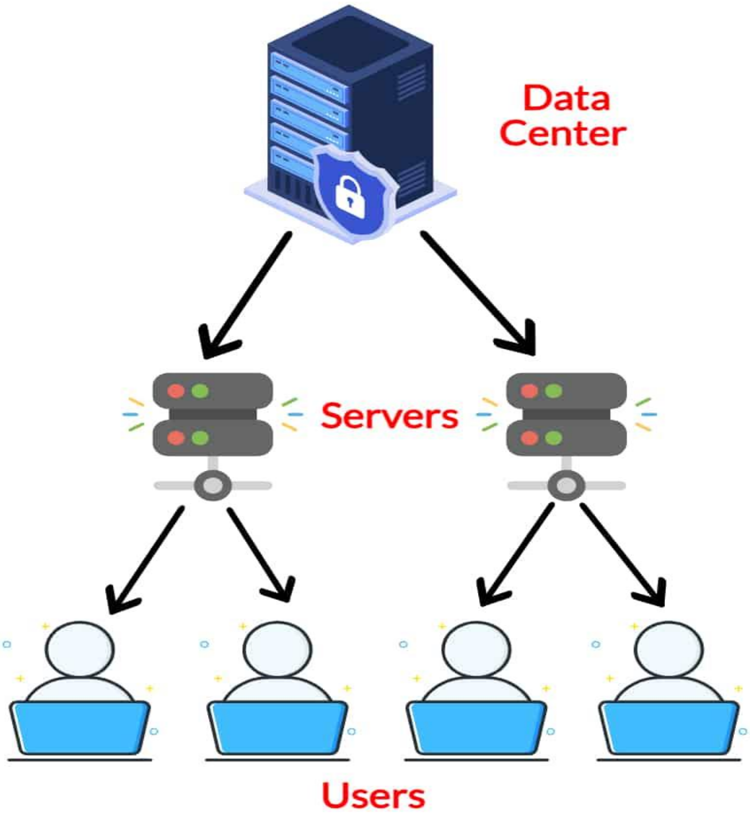


Figure 2: working of Cloud

3.1.2 Traditional cloud storage Model

A client or mobile device might be the front-end platform for a classic cloud storage architecture. The back-end platform could be a server or storage, and the network could be the internet or an intranet. A typical illustration of conventional cloud storage is Google Drive. Google saves the data you upload to the cloud in one of its data centres. A request is made to the data centre when you wish to access your data from a mobile device or laptop, and you are then able to do so.

3.2 Cloud Computing

The term "cloud computing" is all the rage in the IT industry, according to analysts, but the majority of consumers still have no idea what this newest jargon refers to. The first question this section answers is, "What is cloud computing, and how does it explain the technology?"

Cloud computing can be simply defined as the process of storing data and information remotely rather than on local servers or hard drives. This is in contrast to traditional computing, which stores data and information locally. Whenever there is a requirement to use or refer to that information, access can be achieved through the use of the internet. Because of the Internet, it is feasible to access both the data and the information in question from any location on the planet. The ability to access data and information from any location at any time is fundamental to the concept of cloud computing.

In essence, cloud computing aims to connect and share cloud and on-premise data while streamlining operations for both developers and non-developers. Consider cloud computing primarily as a delivery strategy.

If you've uploaded a photo to Dropbox or Facebook, you've used cloud computing. Dropbox, a cloud storage platform, increases file storage. Facebook was one of the first companies to design a scalable database system for cloud computing.

Although relatively primitive forms of cloud computing have existed since the 1960s, this method of data storage has come a long way since its inception and is here to stay. The market for cloud services is projected to grow from $482 billion in 2022 to more than $947.3 billion in 2026, according to research firm Gartner. Additionally, hybrid cloud integration is a popular choice for many businesses, so it's possible that your company won't get there all at once. (Forbes, 2021) (Goundar, 2012) (Talend, n.d.)

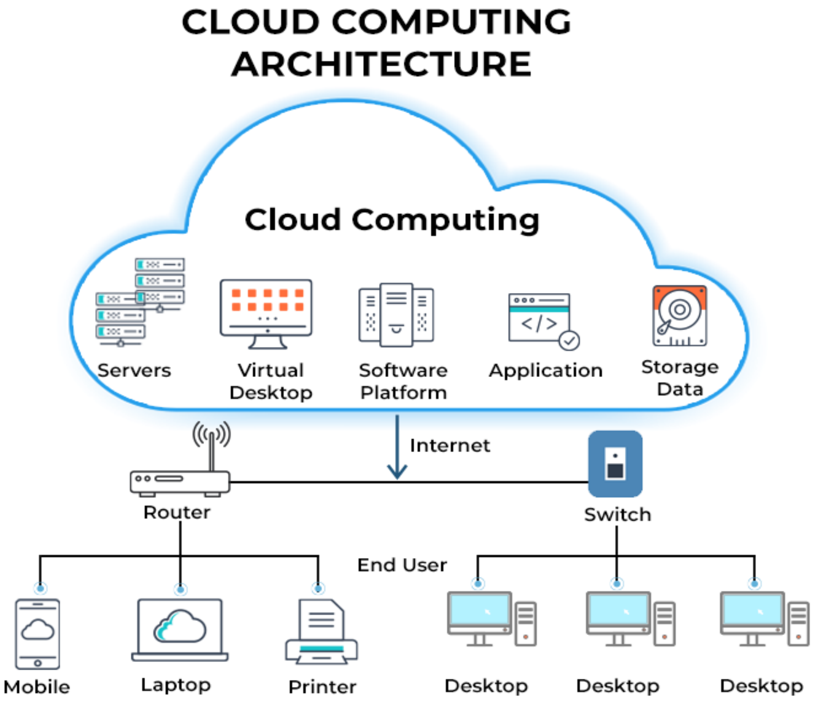


Figure 3: Cloud computing architecture

3.2.1 Characteristics of cloud computing

As cloud computing services continue to advance both technologically and financially, it will be much easier for enterprises to take use of the opportunities presented by the cloud. However, it is equally important to have an understanding of what cloud computing is and how it operates. The National Institute of Standards and Technology (NIST) identifies cloud computing as it is practised now based on five distinct characteristics. (novkovic, 2017)

1. **On-demand self service**

   Without a service provider, cloud computing resources can be used. A manufacturer can upgrade its computing resources as needed without hiring a cloud service. Data centres, virtual machines, and database instances are examples.
   A web-based self-service portal helps manufacturers manage their cloud accounts, monitor cloud services and use, and add or delete services as needed.

2. **Broad network access**

   Cloud computing uses remotely hosted, internet-accessible resources from a variety of client devices. Users can access cloud services over a network, usually the Internet but sometimes an intranet or LAN.
   Bandwidth and latency are key to cloud computing and ubiquitous Internet access because they affect network QoS. Time-sensitive manufacturing applications require this.

3. **Multi-tenancy and resource pooling**

   Cloud resources support multiple users simultaneously. Multi-tenancy allows tenants to share hardware or software without compromising data privacy.
   By sharing resources, more individuals can be helped. Providers need big, adaptable resources to properly serve their diverse clients and achieve economies of scale. Pooling resources must not compromise mission-critical industrial applications.

4. **Rapid elasticity and scalability**

   One of the advantages of cloud computing is that it allows for the rapid provisioning of cloud resources as and when they are needed by industrial organisations. as well as removing them as soon as they are no longer required. It's key to cloud computing. Changes in use, capacity, and pricing are conceivable without new agreements or payments.
   Cloud computing is elastic, so manufacturers may install and withdraw resources quickly. Rapid provisioning can be utilised for storage, virtual machines, and client apps.

5. **Measured service**

   Cloud computing costs are based on consumption, so manufacturers only pay for the resources they really utilise. Making use of pay-as-you-go features helps maximise your asset use. In other words, the cloud service provider monitors, analyses, and reports on how its users are putting the cloud to good use. This encompasses both the utilisation of cloud-based server instances and

cloud-based data storage. The principle of "pay for what you use" underpins the pricing structure. The amount due is therefore contingent on how much the manufacturing company really consumes.
(novkovic, 2017)

3.3 Cloud Deployment Models

There are four cloud deployment models defined by NIST (National Institute of Standard and Technology), they are:

1. Public cloud
2. Private cloud
3. Community cloud
4. Hybrid cloud

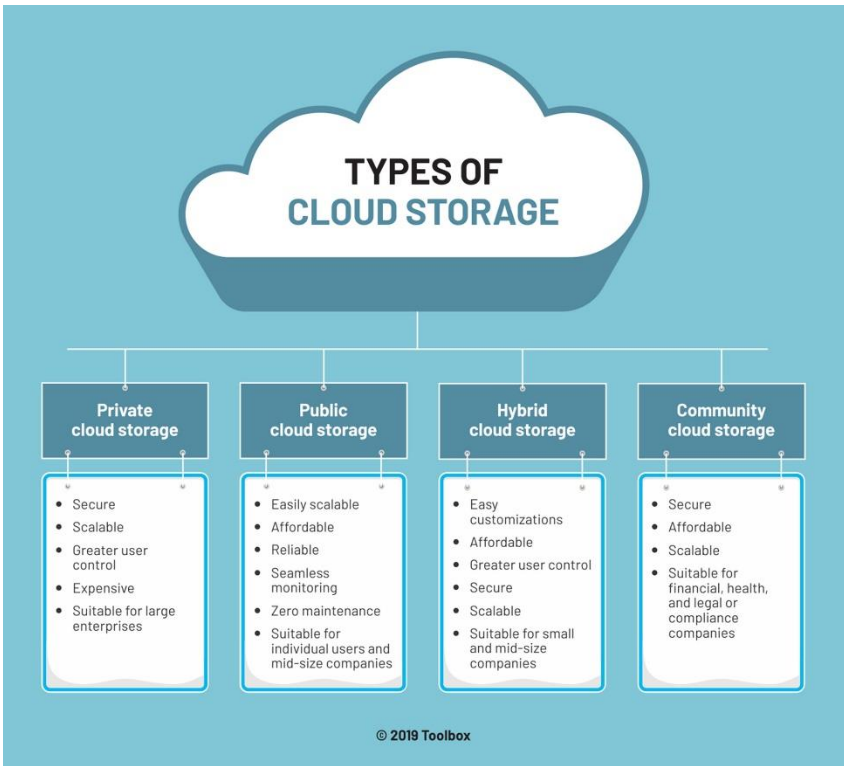


Figure 4: Types of cloud storage

3.4 Cloud service models

There are three primary approaches to providing cloud services:

1. Software as a Service (SaaS)
2. Infrastructure as a Service (IaaS)
3. Platform as a Service (PaaS)

Though they have a common motivation in cloud computing, the models differ in how they really work and what they offer to businesses.

3.4.1 Software as a Service (SaaS)

The software as a service model is the most well-known of the three ways that cloud computing services can be delivered. This is due to the fact that the vast majority of consumers make everyday use of SaaS services, regardless of whether or not they are aware of this fact. When people talk about "the cloud," they typically refer to software as a service (SaaS) applications like Google Drive, Dropbox, or even Netflix.

The SaaS distribution strategy provides users with access to fully functional, cloud-managed and -operated applications. Users often access SaaS applications through a web browser. This is advantageous since the vendor handles downloading and installing applications, so you do not have to. Nevertheless, depending on the provider you employ, you may be required to download a plugin.

Businesses, especially those that use remote employees, are also embracing SaaS. They can utilise their effective business tools in this way without updating their hardware or manually updating software.

Lightweight, no software upgrades, and no software licencing are only some of the main advantages of SaaS. (Torres-Corral, 2021)

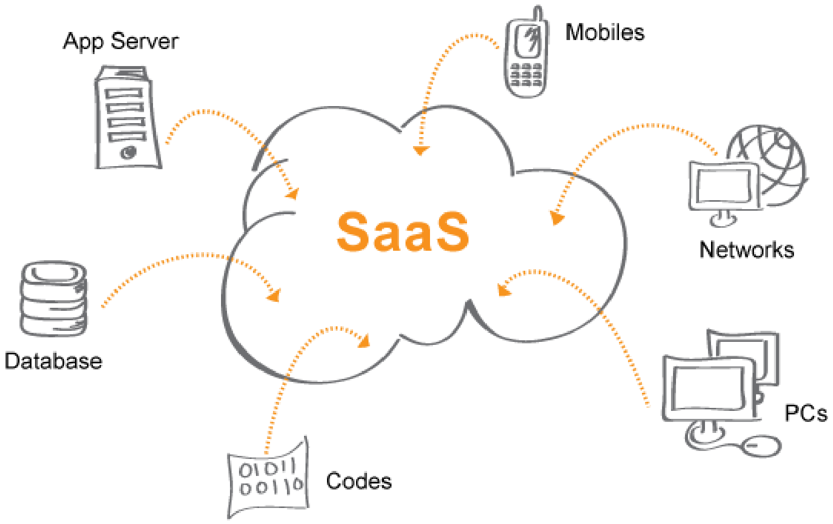


Figure 5: SaaS

3.4.2 Infrastructure as a Service (IaaS)

IT infrastructure was usually stored on-site. Businesses had to invest in pricey infrastructure like servers and storage and keep it updated.

Cloud service providers are famous for helping businesses manage their IT systems. As a result, Infrastructure as a Service (IaaS) was developed and businesses began migrating to cloud platforms. Companies can use the cloud server's virtualized computing resources.

Greater flexibility, cost savings and reliability are some of the key benefits of IaaS.

IaaS reduces the cost of IT infrastructure while providing access to cutting-edge technologies. Many enterprises of all sizes have adopted IaaS as their service delivery paradigm. They can compete on an equal level with larger companies with superior finance because they don't have to invest in expensive gear. (Torres-Corral, 2021)

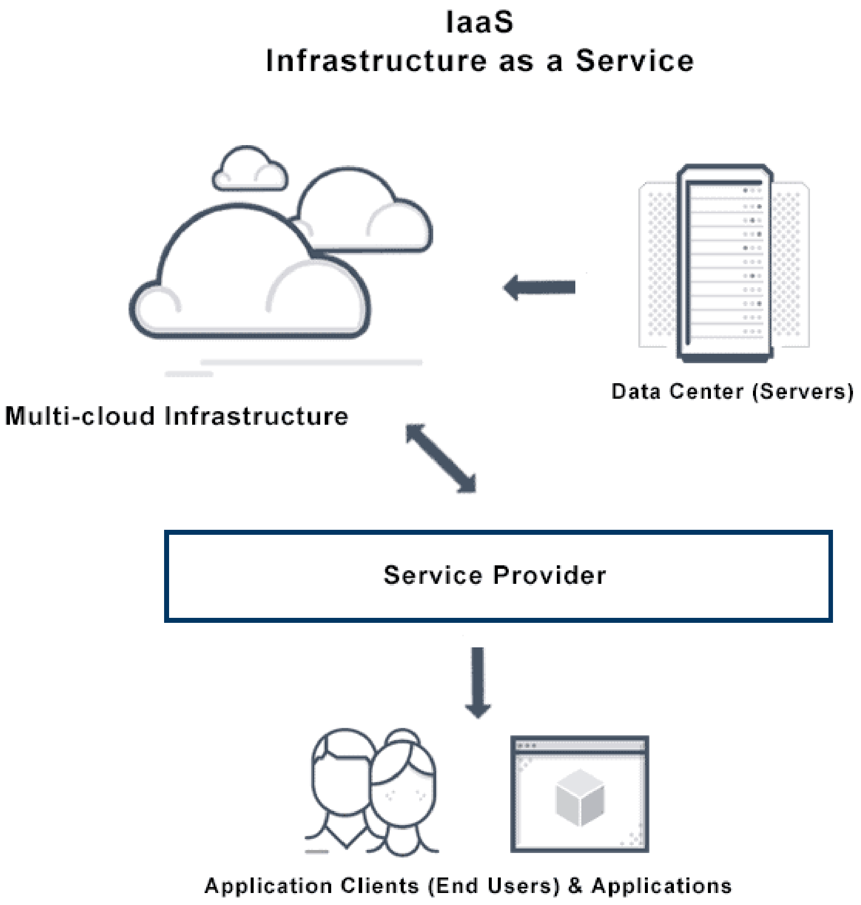

IaaS
Infrastructure as a Service
Multi-cloud Infrastructure
Data Center (Servers)
Service Provider
Application Clients (End Users) & Applications

Figure 6: IaaS

3.4.3 Platform as a Service (PaaS)

The term "solution stack" can also be used to refer to this particular kind of mechanism for the delivery of cloud services. Cloud computing gives companies the ability to design, run, and administer cloud-based applications without the need for physical infrastructure. Platforms are provided by a third-party vendor that also handles maintenance. This means that organisations are relieved of the responsibility of performing activities like as backups and the deployment of servers because these tasks are done on their behalf.

Efficiency gains, reduced complexity, and enhanced teamwork are just a few of the many PaaS advantages. (Torres-Corral, 2021)

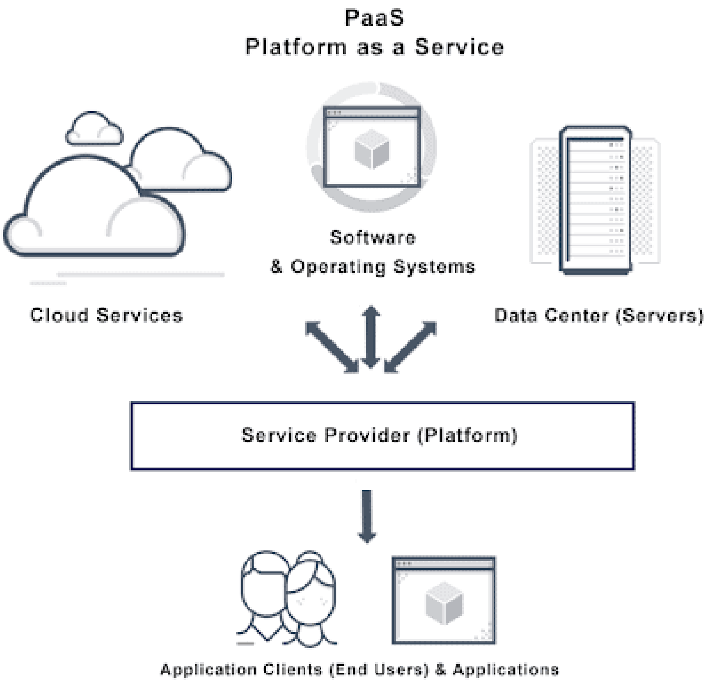


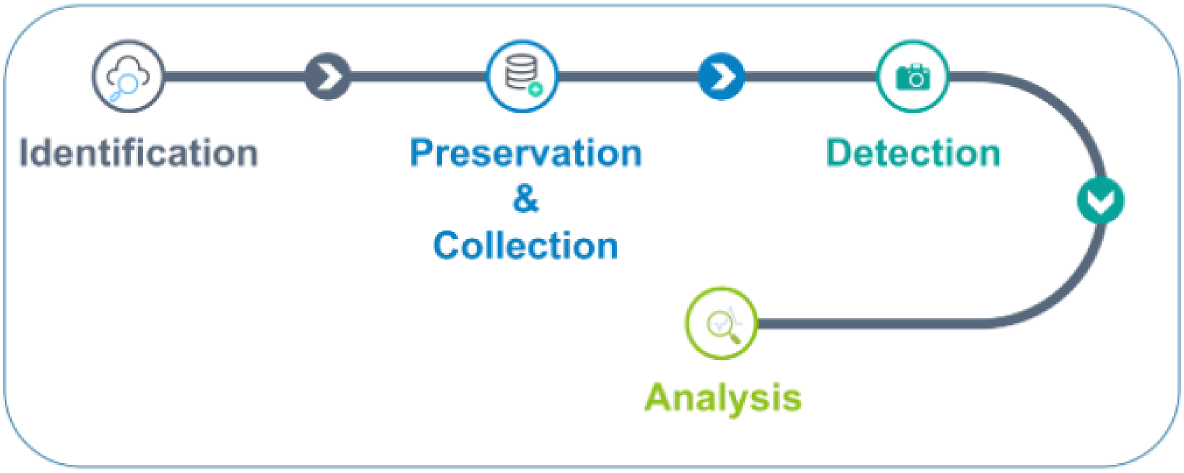
Figure 7: PaaS

3.5 Cloud Forensics

Investigations that are concentrated on crimes that primarily involve the cloud are referred to as cloud forensics. This can involve identity theft or data breaches. Using cloud forensics, the owner is safe, and evidence can be stored more securely for longer. Without a cloud forensics plan, it's possible that the owner does not have access to all of the data or evidence stored in the cloud, especially if it is hosted off-site or by a third party. (Lim, 2020)

An investigator's first objective is making sure the digital evidence is in its original form and has not been tampered with. Since customers of PaaS and SaaS service models do not manage the underlying hardware, it is difficult for them to have access to the corresponding logs. It's not uncommon for CSPs to keep consumers in the dark about some details of the logs. Also, CSPs' policies may prohibit them from providing the necessary services for log collection. (Tripwire, 2019)

The combination of these forensics is known as cloud forensic (i.e., digital forensics, network forensics, hardware forensics etc.). It necessitates relationships between various cloud participants to make internal and external inquiries easier (such as cloud providers, cloud consumers, cloud brokers, cloud carriers, and cloud auditors). Legally, there are several different jurisdictions and tenants involved. (Shivam, 2020)



Cloud forensics Steps

Figure 8: Cloud Forensics steps

3.6 Cloud V/S Digital forensics

Traditional digital forensics are usually utilised in investigations involving cybercrime. Gathering evidence from software, data, and other sources is one of the tasks that digital forensics professionals perform when investigating an incident or searching for hackers.

In a court of law, any evidence obtained through the use of digital forensics can be presented as evidence. It is typically quite easy to gain permission to utilise discovered evidence as evidence in a case because the evidence itself belongs to the person who owns the technology that was used to uncover it in the majority of cases.

The hunt for this piece of evidence has become marginally more challenging as a result of cloud forensics. Even if the investigator applies the same techniques in cloud forensics as they would in traditional digital forensics, the distinctions between who owns the data and where it is admissible in court may become muddled. (Lim, 2020)

3.7 Challenges faced in cloud storage

The upkeep of a sizable data centre comes at a significant financial cost. Regular technological improvements are necessary for the data centres' underlying physical infrastructure. In addition to that, there are the recurrent costs of things like cooling, maintenance, and updates. One last thing to think about is the level of safety. Even though many cloud service providers have strict security protocols in place, there is still the possibility that they may be breached and sensitive data could be accessed. This is the case despite the fact that there are many cloud service providers. One recent example of this is when hackers gained access to the iCloud accounts of famous people. Your privacy may be compromised in ways that are not directly attributable to human mistake. Your unencrypted data can be searched through by companies that meet specific size requirements. They describe in great depth, inside their privacy policies, the many distinct circumstances under which they are legally permitted to access and disclose your information. The use of cloud computing is increasingly considered as a threat to users' privacy and security, despite the fact that it has numerous beneficial results. Before putting their trust in business solutions provided by cloud providers, a significant number of multinational companies first investigate the cloud provider's security policies and procedures.

As a consequence of this, it is absolutely essential for providers of cloud services to earn their customers' trust by demonstrating their dedication to protecting their data when it is being transferred between locations. The environment of cloud computing incorporates a great number of regulations, processes, control mechanisms, and technologies in order to ensure the safety of the data, platform, software, and infrastructure that are involved with cloud computing. During the establishment of authentication rules, the use of a priori knowledge helps to protect data that is kept in the cloud, ensure compliance standards are met, and keep users' personal information private. Cloud security can be tailored to meet the specific requirements of each individual company, including access authentication and traffic filtering. The company is able to reduce the amount of money it spends on administration and refocus the efforts of the information technology department by centralising the process of creating and managing these laws. The manner in which cloud security is provided is determined either by the cloud provider that is employed or by the cloud security solutions that are implemented. (Lim, 2020) (Shivam, 2020)

Because cloud storage is a centralised entity that is administered by a provider, exactly like in the case of a digital forensics’ investigation, it is likely that acquiring evidence will be extremely challenging. This is because of the similarities between the two processes. In addition, prior to the evidence being submitted in court, everyone has the opportunity to manipulate it in any way they see fit. Due to the fact that the results of some significant cases may be dependent on the evidence that is submitted to the court, this can be a challenging undertaking.

3.8 Solution for the current challenge

On the other hand, the implementation of cloud security processes should be split between the owner of the business and the provider of the service. Several different studies are concentrating on the development of innovative strategies and solutions to advance cloud security. The block chain approach is one example of a forward-thinking security mechanism that is implemented across cloud-based systems. The structural layout of the BC is shown in figure 10. Because the data is recorded and the blockchain is validated, it is not possible to make any arbitrary changes because it has a list that is neatly organised to maintain the data. However, it does have a neatly organised list to keep the data. Each block in the BC has a header and a body, and each of these components is composed of two pieces. The hash values for the last, the present, and the nonce are stored in the header. A search in the database is performed using an index value to locate the block data. Blockchain technology is an example of a common, complex, and cutting-edge technology that is currently being used for the purpose of providing security in important transactions like banking. One of the most essential components of the blockchain concept is the process of authenticating and establishing the trustworthiness of the final user. Blockchain is a trustworthy and secure solution for combating cyberattacks because of the robust authentication and key vaulting methods that it utilises. The following items make up the whole set of components that contribute to the blockchain's security:

- Accessing the blockchain via presenting solid IDs and authentication
- Core blockchain technology that are secure
- Secure network-wide communication on the blockchain.

3.9 Blockchain

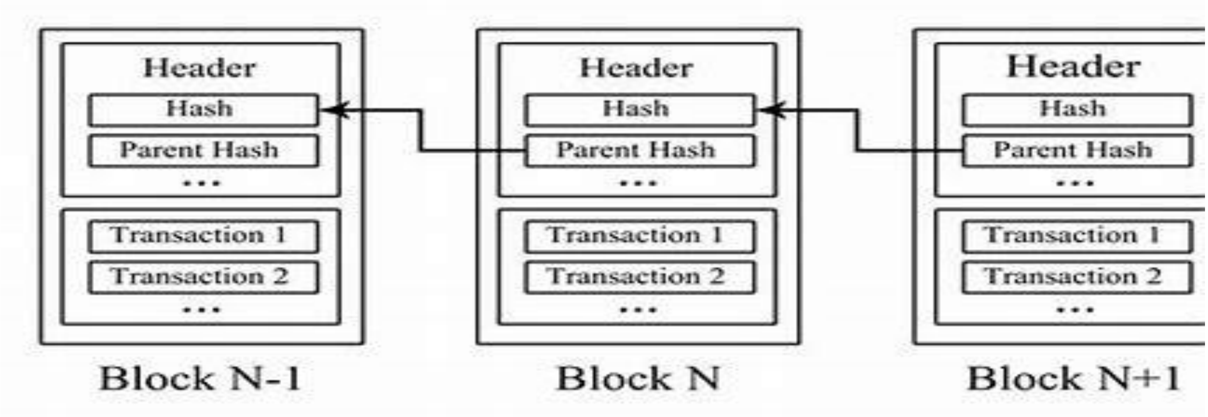


Figure 9: structure of blockchain

A blockchain can be thought of as a distributed database or ledger that is shared among the nodes of a computer network. A blockchain can be thought of as an online database that stores information in its native digital format. The most well-known application of blockchain technology is in the field of cryptocurrency systems like Bitcoin, where it is used to keep a record of transactions that is both safe and decentralised. A blockchain is an innovative technology that ensures the accuracy and safety of a record of data, which eliminates the need for a trusted third party in the verification process. This makes it possible to increase users' level of confidence without the involvement of a middleman.

The data in a blockchain is organised in a manner that is very different from the conventional manner in which data is organised. The data on a blockchain is organised into groupings referred to as blocks, and each block has its own set of data. Blocks have unique data storage capacities, and after these capacities are utilised, the block is cryptographically "sealed" and connected to the block that came before it in the chain of blocks that makes up the blockchain. When a new block is introduced to a chain, all of the additional information that comes after that block is combined into a brand-new block, and that block is then added to the chain when it is complete.

On a database, data is organised into tables, but in a blockchain, it's stitched together in blocks. So is blockchain named. This data format creates an irreversible data timeline when decentralised. When a block is full, its information is added to the timeline. A new block added to the chain receives a second-accurate timestamp. (Hayes, 2022)

3.9.1 Types of Blockchain

Before discussing about the types of block chain we need to know what permissionless and permissioned blockchain is:

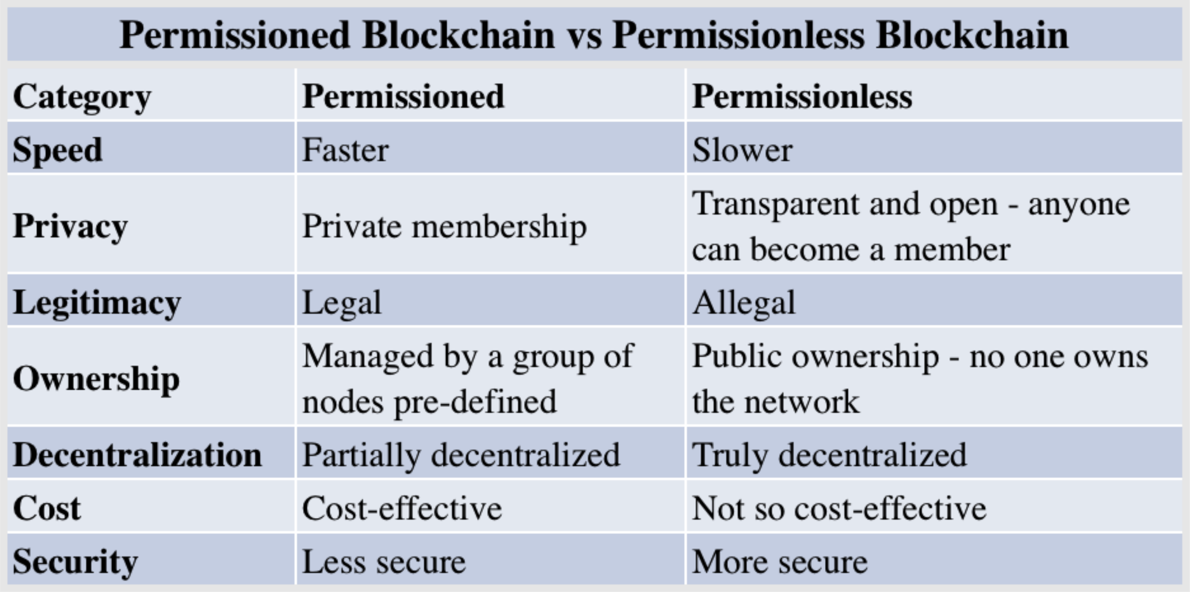
- **Permissionless Blockchain**

Because anybody can take part in the process of certifying data and transactions on a blockchain, it is frequently referred to as a trust less or public blockchain. This is because anyone can take part in the process. These are utilised in systems where there is a requirement for a high degree of openness and transparency.

- **Permissioned blockchain**

Within a particular blockchain network, only a predetermined collection of groups is authorised to check the legitimacy of transactions or data. When there is a requirement for the highest possible level of privacy and security, these are used in networks. (GeeksforGeeks, 2022)

The main characteristics of these two are as shown in the figure below.



Permissioned Blockchain vs Permissionless Blockchain

Category	Permissioned	Permissionless
Speed	Faster	Slower
Privacy	Private membership	Transparent and open - anyone can become a member
Legitimacy	Legal	Allegal
Ownership	Managed by a group of nodes pre-defined	Public ownership - no one owns the network
Decentralization	Partially decentralized	Truly decentralized
Cost	Cost-effective	Not so cost-effective
Security	Less secure	More secure

There are 4 types of blockchain:

1. Public Blockchain
2. Private Blockchain
3. Hybrid Blockchain
4. Consortium Blockchain

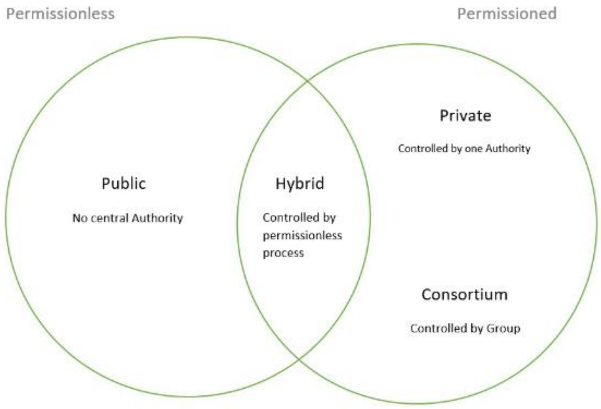


Figure 10: Types of blockchain

Let's break down and talk about every one of these points.

1. **Public Blockchain**
   These blockchains are completely suitable for any application of the decentralised paradigm that may be conceived of. Anyone who has a computer and access to the internet can sign up to be a part of this group. The main advantage of these blockchain; it is trustable, secure, anonymous nature and decentralized.

2. **Private blockchain**
   Because they are not as decentralised as the public blockchain, these blockchains are more secure than others that are currently in use. Participation in the process is restricted to only those nodes that have been approved. The main advantages of these blockchain; speed, scalability, privacy and balance.

3. **Hybrid Blockchain**
   It's a hybrid of private and public blockchains, where certain data is kept under lock and key by a single entity while the rest is made available to the public. The main advantages of these blockchain; Ecosystem, cost, architecture and operations.

4. **Consortium Blockchain**
   It's an innovative method for meeting the company's requirements. This blockchain does more than just verify trades; it can also start or receive trades. The main advantages of these blockchain; speed, authority, privacy and flexible.
   (GeeksforGeeks, 2022)

3.9.2 How does a Blockchain works

A blockchain is, as its name suggests, a chain of information-containing blocks. This method was first designed to timestamp digital documents so that they could not be backdated or altered, and it was first reported in 1991 by a group of researchers. But it remained largely unused until Satoshi Nakamoto modified it in 2009 to launch the virtual currency Bitcoin.

Blockchains are public distributed ledgers that anybody may access. Once information is stored on a blockchain, it is extremely impossible to alter it.

Let’s take a closer look at a block to understand how it works.

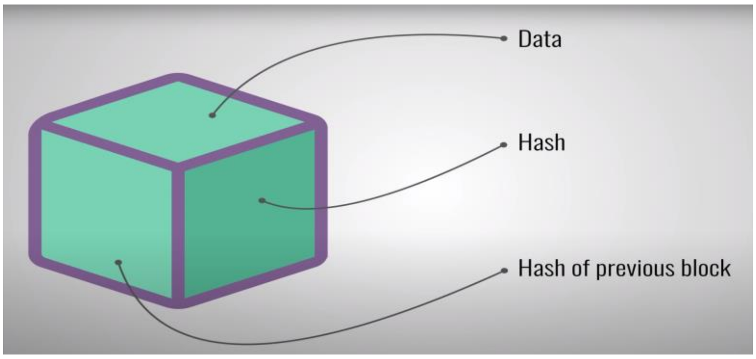


Figure 11: A block of a blockchain

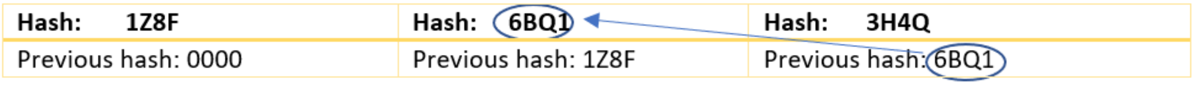
Each blocks contains some data, hash of the block and the hash of the previous block. The data held within a block varies depending on the type of blockchain. For example, for a bitcoin block will contain the data of the transaction which is the sender and receiver of the bitcoin, like wise any data can be stored inside a block in blockchain. Each block also contains a hash value, we can compare the hash as a digital fingerprint, it identifies a block and all of its contents and it's always unique, just as a fingerprint. Once the block is been created, it's hash is being calculated. Changing something inside the block will cause the hash to change. So, in other words: hashes are very useful when you want to detect changes to blocks. The third element inside of the block is the hash of the previous block. This basically generates a chain of blocks, and it is because of this technique that a blockchain is so safe.

Let's take an example and explain the technique of block chain.

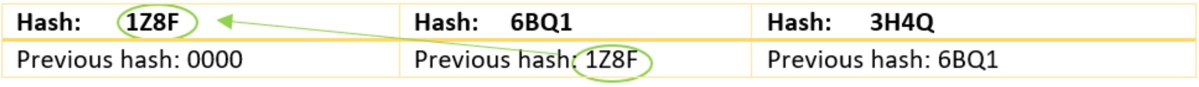
Here we have a chain of 3 blocks A, B and C:

Hash: 1Z8F	Hash: 6BQ1	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1

As you can see, each block has a hash and the hash of the previous block. That is Block C points to Block B and Block B points to Block A. Now the first block is a bit special, it cannot point to a previous block because it's the first one. We call this block as genesis block.



Hash: 1Z8F	Hash: 6BQ1	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1



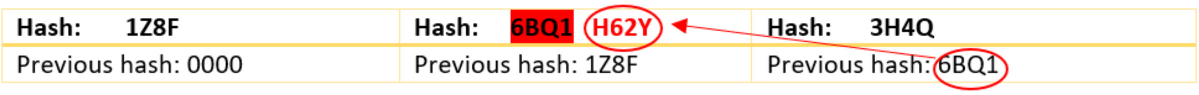
Hash: 1Z8F	Hash: 6BQ1	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1

Now let's say that someone tamper with the second block which is block B.

This will cause the hash of the block to change as well.

Hash: 1Z8F	Hash: 6BQ1 H62Y	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1

In turn, that will make the block C and all following blocks invalid because they no longer store a valid hash of the previous block.



Hash: 1Z8F	Hash: 6BQ1 H62Y	Hash: 3H4Q
Previous hash: 0000	Previous hash: 1Z8F	Previous hash: 6BQ1

Changing a single block in the chain will invalid all following blocks. This way we can understand that the data has been tampered, but using hashes is not enough to prevent tampering. Modern computers can calculate thousands of hashes per second. Anyone may tamper with a block and recalculate other blocks' hashes to fix the blockchain.

So, to mitigate this vulnerability, blockchains have something called proof-of-work. It's a mechanism that slows down the creation of new blocks. In bitcoins case, it takes about 10 minutes to calculate the required proof-or-work and add a new block to the chain. If you tamper with 1 block, you'll need to recalculate the proof-of-work for all the others. So, the blockchain's security comes from hashing and proof-of-work.

Distributed blockchains self-secure. Unlike cloud storage, anyone can join Blockchain's peer-to-peer network. A network member gets the complete blockchain. The node can use this to confirm everything's OK.

When someone produces a block, the network receives it. Each node checks the block for tampering. Each node adds this block to its blockchain if everything checks up. All nodes in this network agree on valid and invalid blocks. Network nodes reject altered blocks. To tamper with a blockchain, you must change all blocks, redo each block's proof-of-work, and control more than 50% of the peer-to-peer network. (Sajvee, 2019) (Harvard business review, 2017)

3.9.3 Characteristics of blockchain

A blockchain can be characterised by a number of features, including the following:

- **Decentralization:** In contrast to traditional centralised systems, blockchain doesn't rely on a single entity to authenticate transactions. Any node in the network can verify a transaction before it is added to the blockchain by solving a Proof of Work (PoW) challenge. Due to its distributed nature, blockchain technology eliminates the possibility of a centralised failure point or slowdown. Before a transaction can be added to Blockchain's distributed ledger, it must be approved by the network's majority of users.
- **Security:** Using smart contracts, blockchain allows ensure message exchange and communication between nodes. By ensuring that only nodes with the proper public and private keys can access, decrypt, and encrypt data, it avoids illegal data access and data loss.
- **Anonymity:** A public/private key pair generated on each Blockchain participant's device masks their true identity.
- **Autonomy:** Blockchain nodes can interact directly with one another, eliminating the need for intermediary servers.
- **Smart contracts:** They are digitally drafted protocols that define the relations between multiple parties. They save money while enjoying greater speed, precision, efficiency, and transparency. All nodes can confidently rely on the smart contract's accuracy because its data is immutable. Each smart contract is stored on the blockchain and assigned a unique address; when a transaction is made to that contract, it is notified of the action to be taken and is then triggered to execute.
- **Resiliency:** There is no single point of failure because there is a copy of the ledger on each node.
- **Non-repudiation:** Once a transaction has been validated and added as a block to the chain, it cannot be deleted or rolled back, a guarantee made by the Blockchain.
- **Auditing:** When an object changes hands, blockchain technology records information about the transaction, including the time, location, price, and parties involved. Over the course of the

device's existence, upgrades, patches, and component replacements can all be recorded in a blockchain.

- **Capacity:** A proxy server is used, which keeps the resources in an encrypted form until needed, as the Blockchain distributes the resources of millions of participant devices.
- **Immutability:** Immutability In contrast to "corruptible" centralised systems, the Blockchain ledger cannot be altered after a transaction has been validated. Additionally, sensor data can be tracked and accounted for thanks to decentralised technology.
- **Cryptographic algorithm:** Since Blockchain relies on cryptographic techniques, it is able to ensure that user data remains private and that even if an unauthorised device gains access to the network, it will be unable to view any data without the proper keys.
- **Speed:** In a matter of minutes, a Blockchain transaction can be confirmed and then spread around the network.
- **Publicity:** Every Internet of Things device has its own copy of the distributed ledger, which enables such devices to view every transaction as well as every block. The information related to the transaction is kept safe by the device's private key.
- **Cost Saving:** Because it uses a decentralised design and distributes resources among participants, a significant amount of detected data may be stored and transmitted.
- **Transparency:** With blockchain, every transaction, whether physical or digital, can be tracked from beginning to end.
  (GeeksforGeeks, 2022) (Onyejiaku, 2022)

3.9.4 Hashing

Any cybersecurity conversation will mention hashes. These seemingly random digits and letters have several uses. Hashes are the results of MD5 or SHA hashing algorithms (Secure Hash Algorithm). These algorithms turn data or "messages" into unique strings of a predetermined length. "Hash value" or "message digest" describes this string of characters. All computer data can be represented in binary, thus a hashing method can use it to conduct a complicated computation and output a pre-set-length text. This is the file's message digest, or hash.

A hash value generated by a hashing algorithm can never be used to recover the original file's contents. However, you may use it to check if two files are identical even if you have no idea what's in them.

This is why it's crucial to the concept of hashes that each result be unique. If two files can generate the identical digest, we have a "collision," and we can't use the hash as a reliable identifier for that file.

The possibility of a collision is low enough that more secure algorithms like SHA-2 have replaced SHA-1 and MD5.

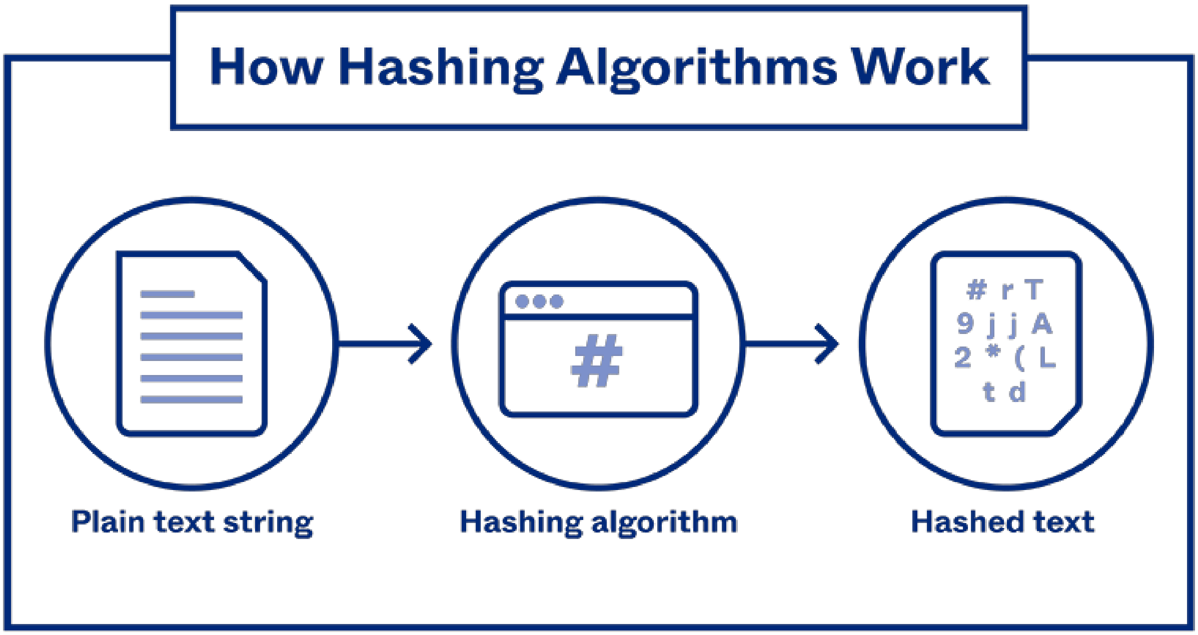


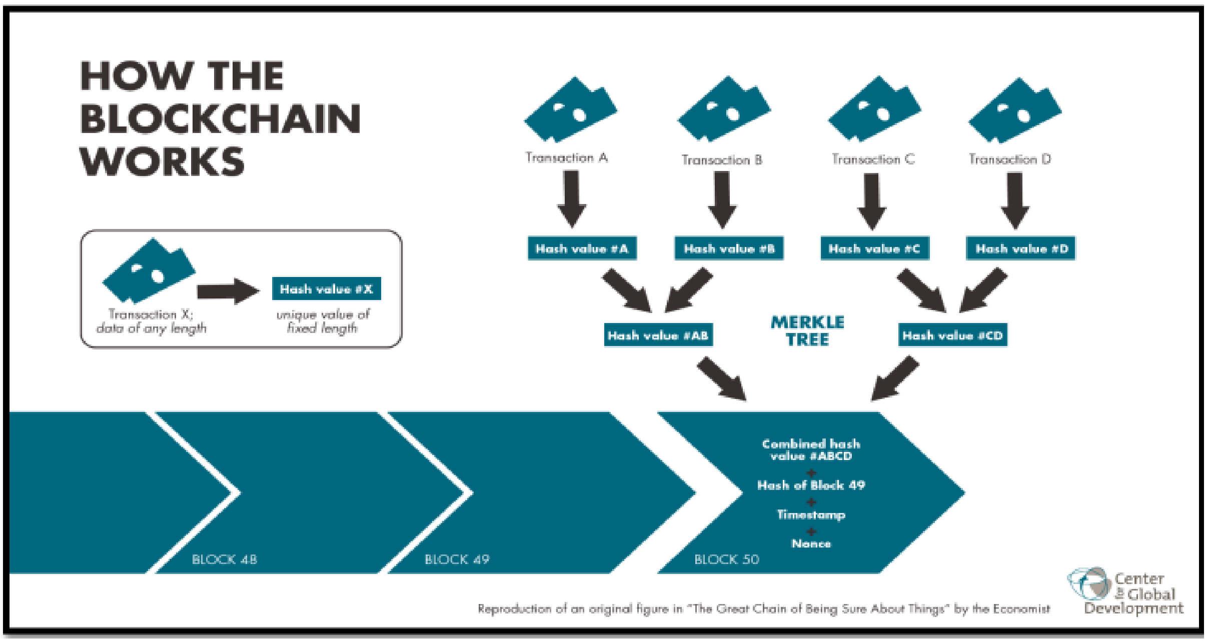
Figure 12: General Hashing working

Since a hash function returns a small number for large keys, two keys can produce the same value. When a newly introduced key matches an existing hash table slot, a collision arises and must be handled. The methods for handling collisions are as follows:

Chaining: Making each hash table cell point to a linked list of records with the same hash function value is known as "chaining." Although chaining is simple, extra memory is required outside of the table.

Open Addressing: In open addressing, the hash table itself serves as the storage location for all items. Every table entry contains either a record or NIL. When looking for an element, we go through each table slot individually until we find the desired element or it becomes clear that the element is not in the table.

(SentinelOne, n.d.) (GeeksforGeeks, 2022)



Reproduction of an original figure in "The Great Chain of Being Sure About Things" by the Economist

Figure 13: Workflow of blockchain in terms of Hash function

3.9.5 Cryptographic hash function

Cryptography is a crucial component of any comprehensive security infrastructure. Data preservation also makes use of the encryption algorithm, both for symmetric and asymmetric purposes (for example, with DES and RSA). While symmetric encryption is used to prevent unauthorised changes to data, asymmetric encryption is used to sign the key in order to validate ownership of the data or that it was obtained from a certain device. This method would be suitable for establishing the data's primitive nature. Due to the comprehensive nature of digital forensics, a wide variety of data types requiring specific archival structures must be dealt with. In addition, there is a substantial security risk associated with data storage, and centralised storage failed to wholly eradicate difficulties with loss and tampering, which made the system unreliable. Meanwhile, the verification findings take too long to get back to the user in a timely manner. We propose a blockchain and multidimensional hash-based solution to the problems associated with data retention for digital forensics.

Chapter 4 -- Methodology

4.1 Research methodology

The research project explores and evaluate the advantage of blockchain based cloud-based storage against the traditional cloud computing. Consequently, it appears that an exploratory research methodology would be better appropriate for this topic. By posing open-ended questions, exploratory research is a fantastic technique for learning what is happening and getting insights into a subject of interest. Therefore, the study will contribute to understanding how the technology is already having an impact on the cyber world and, in this case, digital forensic, as exploratory investigations are useful to clarify the knowledge of a phenomenon. There are many approaches to doing exploratory studies. Considering the importance placed on quantitative data collection and analysis, a quantitative approach seemed appropriate for this investigation. (George, 2022) (Bhandari, 2022)

4.2 Research Approach

In general, the goal of this research project is to develop a theory and introduce an alternative method for cloud storage and digital forensic data security. Another critical aspect of the research is how the theory is being developed. There are mainly two different types of approaches to this. Which is inductive and deductive reasoning. Inductive reasoning attempts to develop a theory, whereas deductive reasoning aims to test an existing theory. This is the basic distinction between inductive and deductive reasoning (Streefkerk, 2022). In this research paper we are trying to analyse the data and proposing the advantages and giving an alternative method to the cyber society. Best option is to use a deductive approach.

4.3 Research Strategy

A strong level of coherence across the research design is essential to answering a specific research question and achieving research objectives; as a result, selecting the research strategy is crucial for upholding consistency. For a research endeavour, a researcher might select from a variety of strategies. The case study, which is an extensive investigation into a subject or phenomenon within its actual context, is the one that has been found to be consistent with the research strategy of this work. (aerd dissertation, n.d.)

4.4 Research Choices

There are generally three methodological approaches to conducting a study:

1. Mono-method, the employment of a single data collection technique, either qualitative or quantitative, and the associated analysis procedures.

2. Multimethod, which refers to the use of numerous data collecting and analysis methods by researchers

3. Mixed methods, which refer to data collection, analysis, and procedures that combine qualitative and quantitative methods.

As the chosen methodology, a mono approach will be utilised to conduct the investigation. The decision is made based on the constraints of the project's rollout schedule. In this single-method qualitative study, research articles and other sources of information were used as the quantitative analytic method for data collecting.

Chapter 5 – Practical visualisation

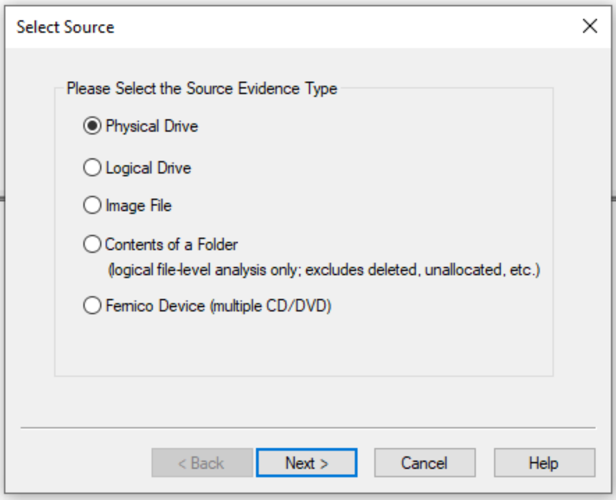
This chapter demonstrates how to use FTK imager to take a forensic image of a data storage in the manner of a forensic investigator. It also demonstrates how to use FTK imager to calculate the hash value, which ensures the authenticity of the image throughout the investigation and until the evidence is presented to the court.

For the case study to analyse and explain the benefits of an alternative strategy in the analysis chapter, the identical scenario will be reproduced if it is in a blockchain context using a blockchain simulator.

5.1 Part -1: Making a disc image using the FTK imager

Technical Procedure: Check to see if all of the discs are connected before running this application (connect any questionable hard drives using a hardware write blocker). You can now start FTK Imager. Assemble the steps.

Step 1: To create a forensic image of a disc, launch FTK Imager, click File, select Create Disk Image, and then choose Physical drive.



Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

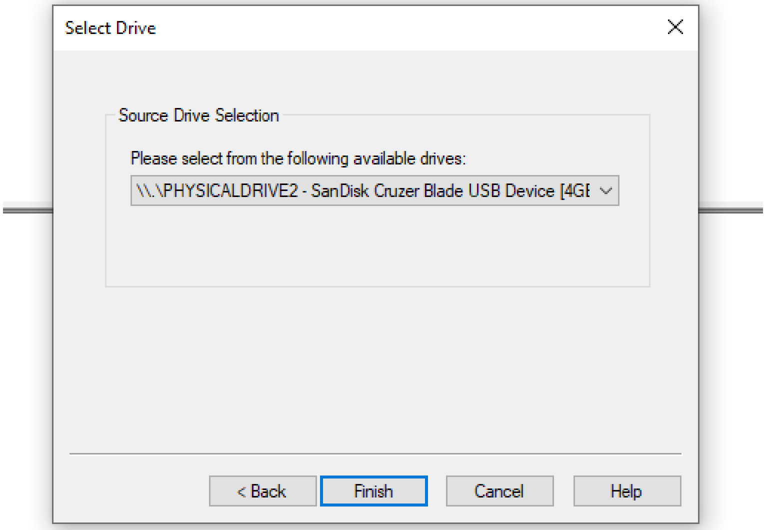
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

Figure 14: selecting the disk to create forensic image

Step 2: Select the disk that contains evidence and click finish. In this case I'm using and USB drive to show.



Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE2 - SanDisk Cruzer Blade USB Device [4GE

Figure 15:selecting the disk to create forensic image 2

Step 3: T Click add to choose the destination drive.

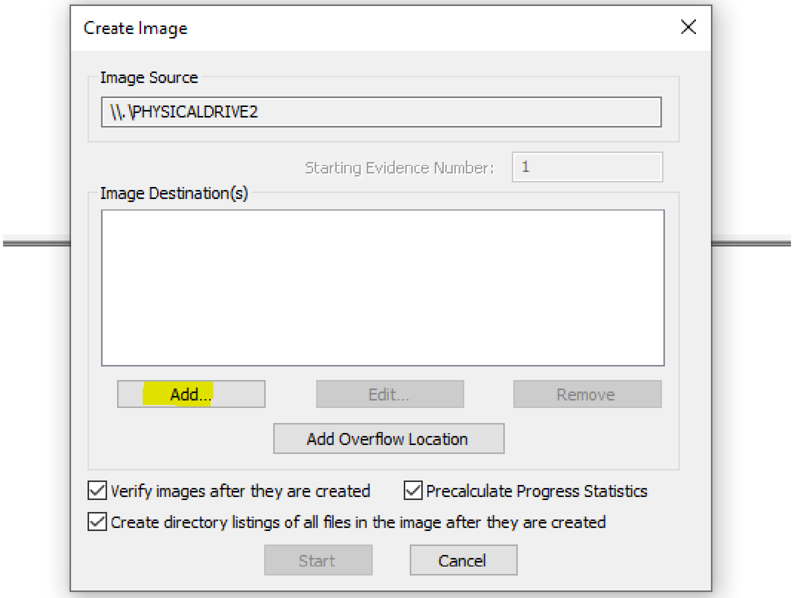


Image Source: \\.\PHYSICALDRIVE2

Starting Evidence Number: 1

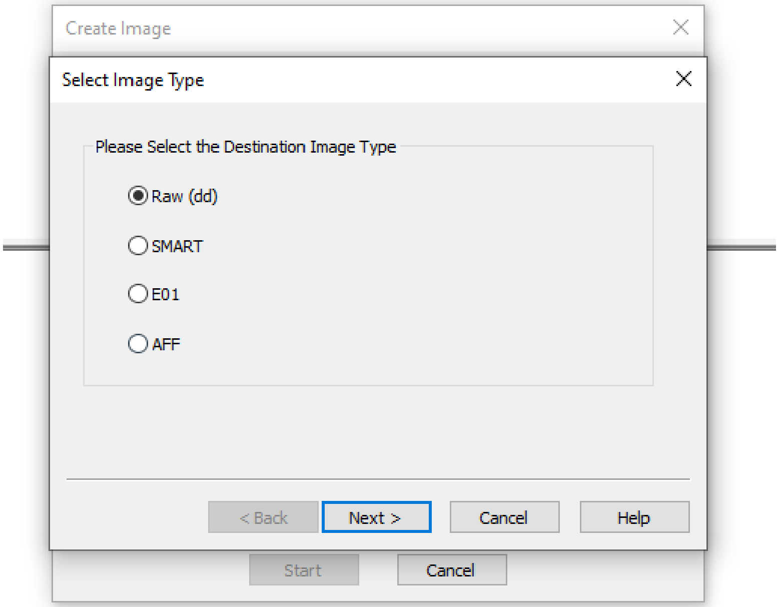
Image Destination(s)

☑ Verify images after they are created ☑ Precalculate Progress Statistics

☑ Create directory listings of all files in the image after they are created

Figure 16: Adding destination drive

Step 4: Choose image type. RAW is recommended.



Please Select the Destination Image Type

● Raw (dd)

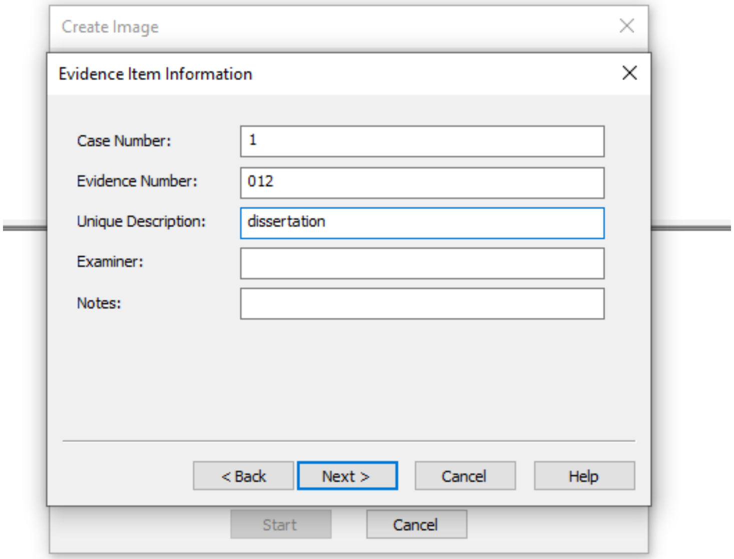
○ SMART

○ E01

○ AFF

Figure 17: selecting image type to create

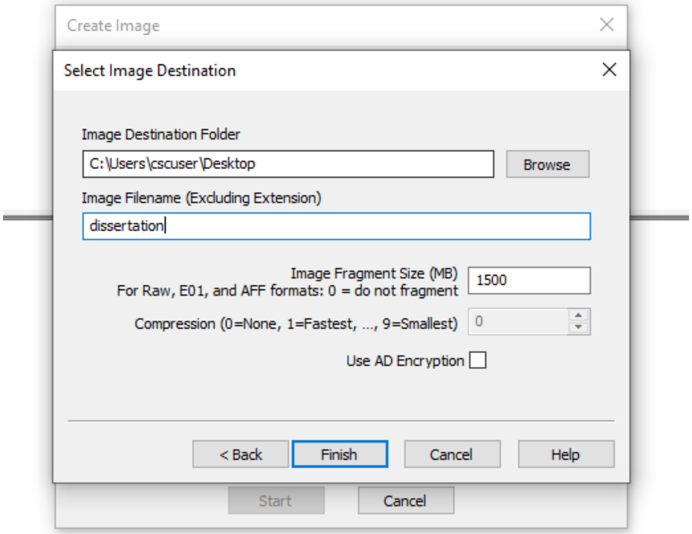
Step 5: Give evidence details and click next.



Case Number:	1
Evidence Number:	012
Unique Description:	dissertation
Examiner:	
Notes:	

Figure 18: evidence information

Step 6: Select the image file's destination and size, then click finish.



Select Image Destination

Image Destination Folder: C:\Users\cscuser\Desktop

Image Filename (Excluding Extension): dissertation

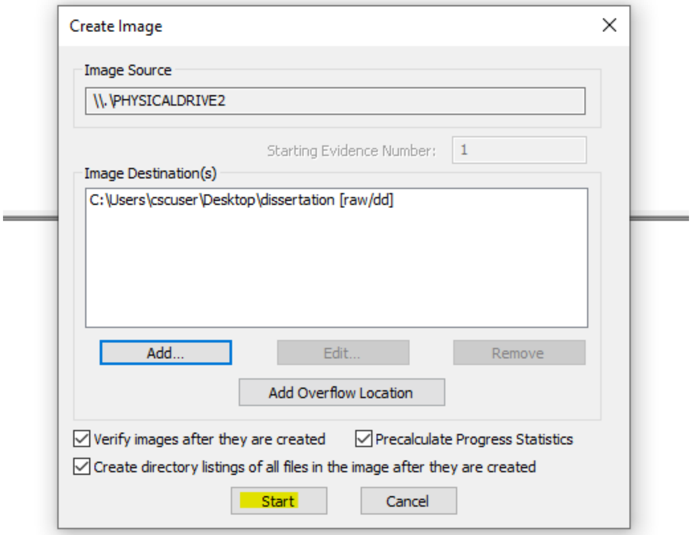
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Figure 19: Destination to save

Step 7: Repeat step three if you require additional images. As there is just one image that we require, click the start button to begin the imaging process.



Create Image

Image Source: \\.\PHYSICALDRIVE2

Starting Evidence Number: 1

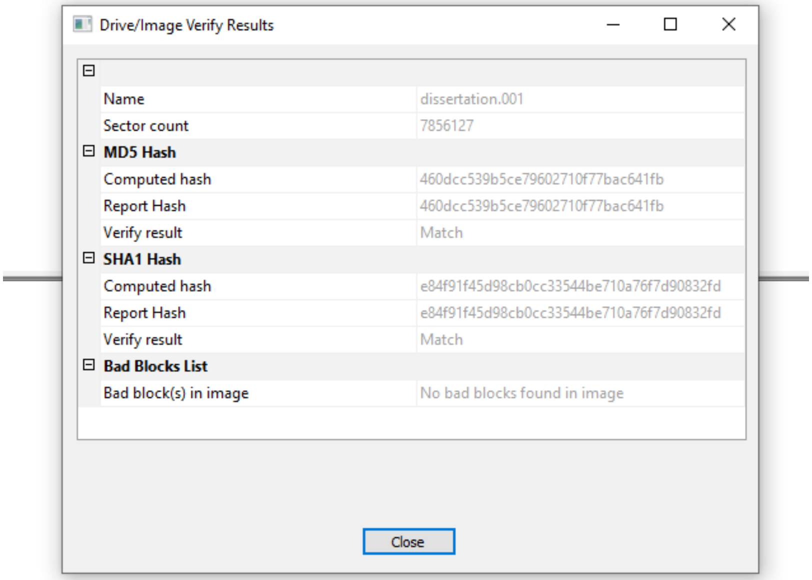
Image Destination(s): C:\Users\cscuser\Desktop\dissertation [raw/dd]

☑ Verify images after they are created ☑ Precalculate Progress Statistics

☑ Create directory listings of all files in the image after they are created

Figure 20: starting to create the image

Step 8: After the process, we will receive a result that displays the file's hash.



Drive/Image Verify Results

Name	dissertation.001
Sector count	7856127
MD5 Hash	
Computed hash	460dcc539b5ce79602710f77bac641fb
Report Hash	460dcc539b5ce79602710f77bac641fb
Verify result	Match
SHA1 Hash	
Computed hash	e84f91f45d98cb0cc33544be710a76f7d90832fd
Report Hash	e84f91f45d98cb0cc33544be710a76f7d90832fd
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 21: summary of the created image showing Hash value

5.2 Part-2: Use FTK Imager to check the Forensic Image's hash value

Technical Procedure: At each point in time where the evidence is being reviewed, the hash key value should be compared to the previous value to see whether there has been any tampering with the file.

Step 1: Launch FTK Imager and add the image file which we created to the FTK Imager. Right click on to the disk file and click verify Drive/Image

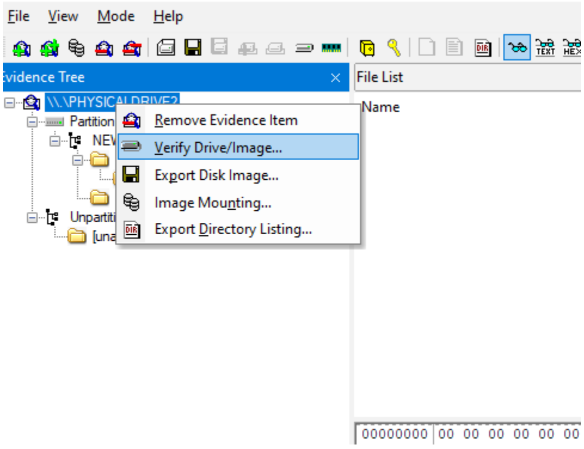
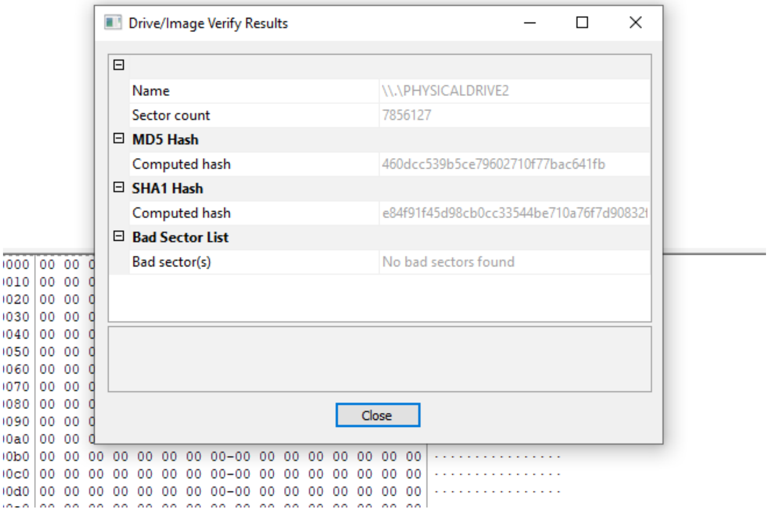


Figure 22: checking the hash value

The FTK Imager will validate the image file that we added and provide the file's hash value. To ensure that it has not been tampered with, compare this to the hash value we obtained when we prepared the evidence image.



Name	\\.\PHYSICALDRIVE2
Sector count	7856127
MD5 Hash	
Computed hash	460dcc539b5ce79602710f77bac641fb
SHA1 Hash	
Computed hash	e84f91f45d98cb0cc33544be710a76f7d90832
Bad Sector List	
Bad sector(s)	No bad sectors found

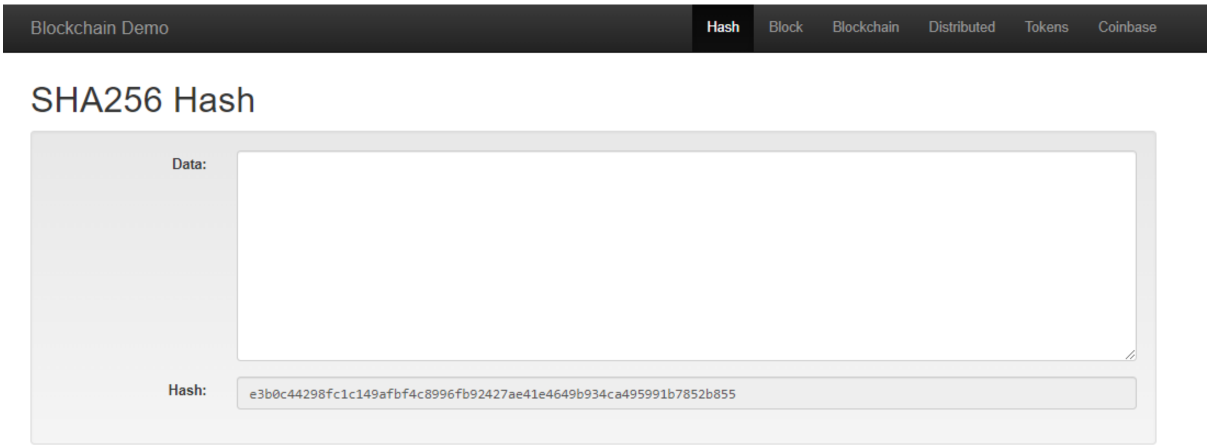
Figure 23: result

Step 2: Compare the hash we got now with the hash value of the image when we created the evidence.

5.3 Part-3: Block Data Hashing

By entering data and manipulating it in real time, a block chain simulator shows how a block chain operates in practise.

Technical Procedure: First, a block hash is displayed, then the genesis of a new block is presented, and finally, a chain of newly generated blocks of data is shown, each of which is linked to the previous block of data. We then demonstrate a peer block distributed chain that adapts to the addition or modification of data that deviates from the initial data.



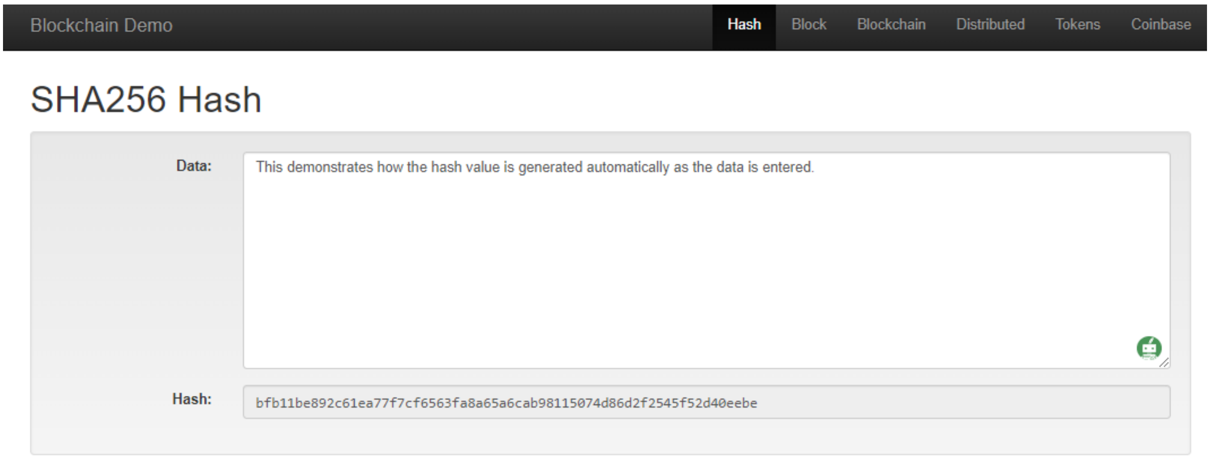
SHA256 Hash

Data:

Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Figure 24: A block of blockchain

Step 1: The hash value will be automatically commutated when a data is entered into a block.



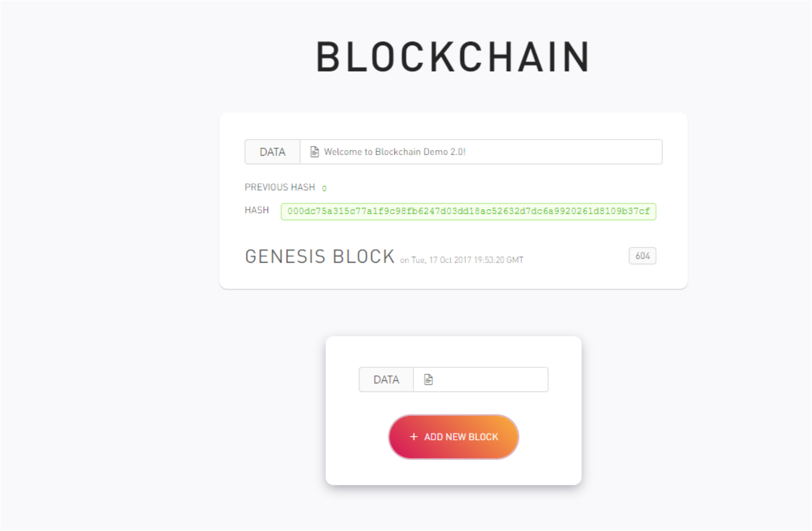
SHA256 Hash

Data: This demonstrates how the hash value is generated automatically as the data is entered.

Hash: bfb11be892c61ea77f7cf6563fa8a65a6cab98115074d86d2f2545f52d40eebe

Figure 25: generating Hash value when data is entered

Step 2: A chain block genesis with pre-entered data is exhibited in a block chain stimulator.



BLOCKCHAIN

DATA: Welcome to Blockchain Demo 2.0!

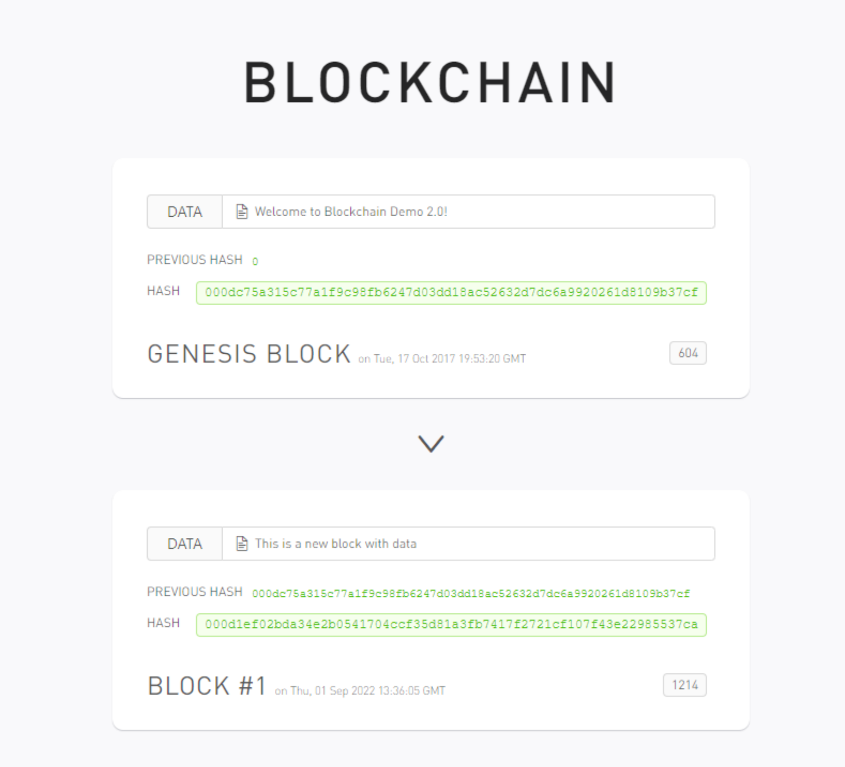
PREVIOUS HASH 0

HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT 604

Figure 26: Genesis block

Step 3: we can add new block and add new data according to our need.



BLOCKCHAIN

DATA: Welcome to Blockchain Demo 2.0!

PREVIOUS HASH 0

HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT 604

DATA: This is a new block with data

PREVIOUS HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

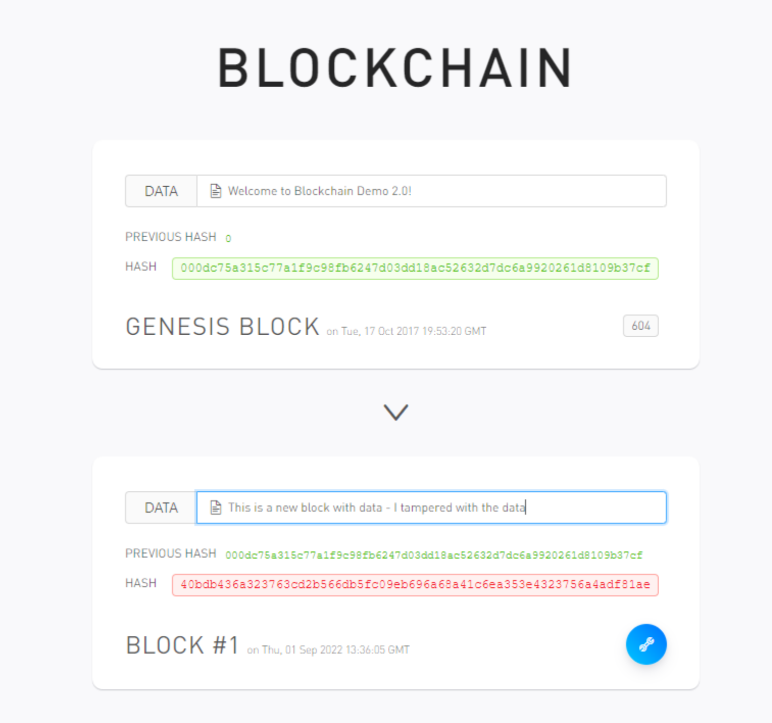
HASH 000d1ef02bda34e2b0541704ccf35d81a3fb7417f2721cf107f43e22985537ca

BLOCK #1 on Thu, 01 Sep 2022 13:36:05 GMT 1214

Figure 27: adding new block

Here we can see that block 1 is connected with genesis block as block 1 has the information about its previous block as seen in the above image.

Step 4: Change the data of the block to understand how blockchain will detect the change in data and highlight that block in red.



BLOCKCHAIN

DATA Welcome to Blockchain Demo 2.0!

PREVIOUS HASH 0

HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT 604

DATA This is a new block with data - I tampered with the data

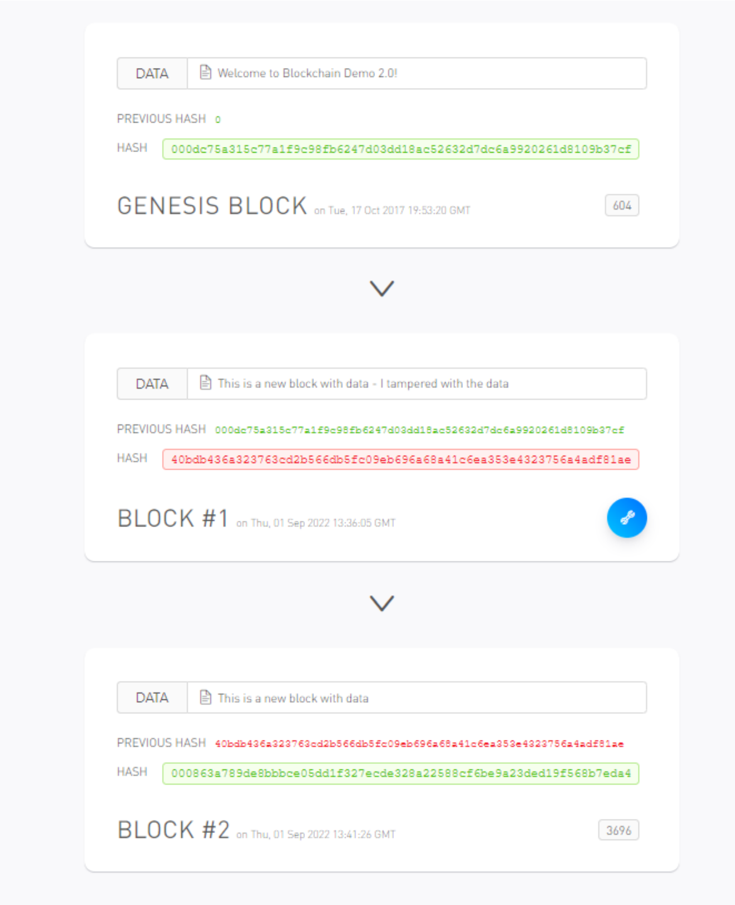
PREVIOUS HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

HASH 40bdb436a323763cd2b566db5fc09eb696a68a41c6ea353e4323756a4adf81ae

BLOCK #1 on Thu, 01 Sep 2022 13:36:05 GMT

Figure 28: Blockchain detecting tampering

Step 5: External data entry caused the hash string to break, which is indicated by a red error highlight.



DATA Welcome to Blockchain Demo 2.0!

PREVIOUS HASH 0

HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

GENESIS BLOCK on Tue, 17 Oct 2017 19:53:20 GMT 604

DATA This is a new block with data - I tampered with the data

PREVIOUS HASH 000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

HASH 40bdb436a323763cd2b566db5fc09eb696a68a41c6ea353e4323756a4adf81ae

BLOCK #1 on Thu, 01 Sep 2022 13:36:05 GMT

DATA This is a new block with data

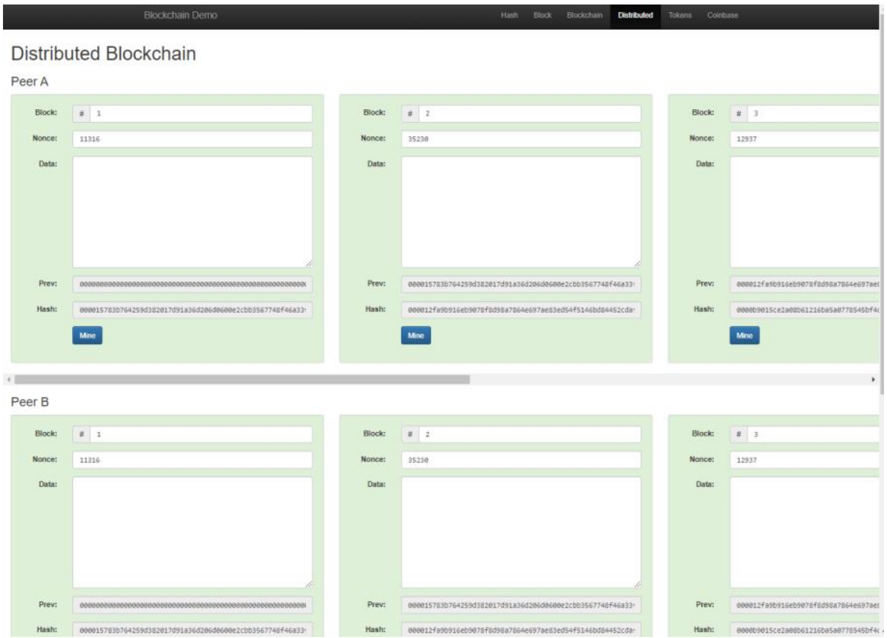
PREVIOUS HASH 40bdb436a323763cd2b566db5fc09eb696a68a41c6ea353e4323756a4adf81ae

HASH 000863a789de8bbbce05dd1f327ecde328a22588cf6be9a23ded19f568b7eda4

BLOCK #2 on Thu, 01 Sep 2022 13:41:26 GMT 3696

Figure 29: How blockchain shows the data is altered

Same method in distributed format with variable peer with pre-entered data.



Distributed Blockchain

Peer A

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cda

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae
Hash: 0000b9015ce2a08b61216ba5a0778545bf4

Peer B

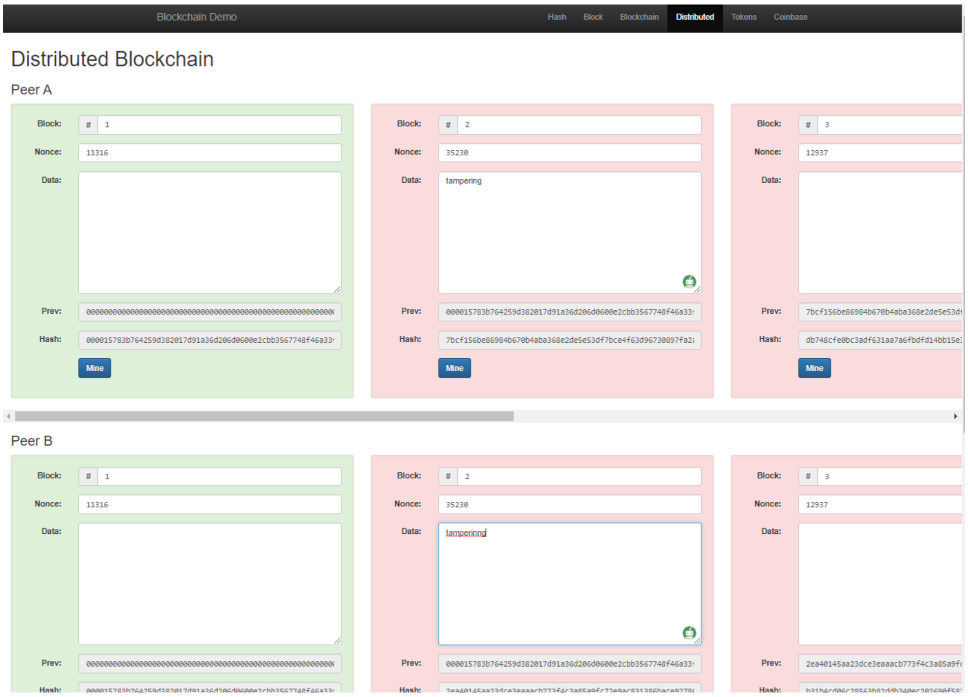
Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cda

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae
Hash: 0000b9015ce2a08b61216ba5a0778545bf4

Figure 30: distributed method

Now let us try to externally enter any data into the blockchain.



Distributed Blockchain

Peer A

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33

Block: # 2
Nonce: 35230
Data: tampering
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33
Hash: 7bcf156be86984b670b4aba368e2de5e53df7bce4f63d96730897fa2

Block: # 3
Nonce: 12937
Data:
Prev: 7bcf156be86984b670b4aba368e2de5e53d
Hash: db748cfe0bc3adf631aa7a6fbdfd14bb15e

Peer B

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33

Block: # 2
Nonce: 35230
Data: tamperinng
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33
Hash: 2ea40145aa23dce3eaaacb773f4c3a85a9fc72e9ac831386bace9278

Block: # 3
Nonce: 12937
Data:
Prev: 2ea40145aa23dce3eaaacb773f4c3a85a9f
Hash: b31b4cd06c28563b82ddb340ec202690f58

Figure 31: simulation of data tampering

Here we can see that once the data has been tampered, the block which are connected to it will highlight to red and the data will not be saved unless the trusted authority approved it.

5.4 Result

Part 1

FTK Imager, an open-source imaging programme by Access Data Group, creates a raw disc image. This application images all disc partitions. It's a popular data extraction tool since it reliably and accurately extracts original data while keeping its integrity, producing legal evidence.

Part 2

After an image has been created, it is crucial to preserve its integrity throughout the investigation. This is vital to demonstrate that the data has not been altered in any way that would disqualify it from use as evidence in the inquiry that it is a part of. Therefore, it is also necessary to keep track of a complete chain of custody and a data check hash log that double-checks the hash of the original file with the image files. It is accomplished here with the FTK imager as well.

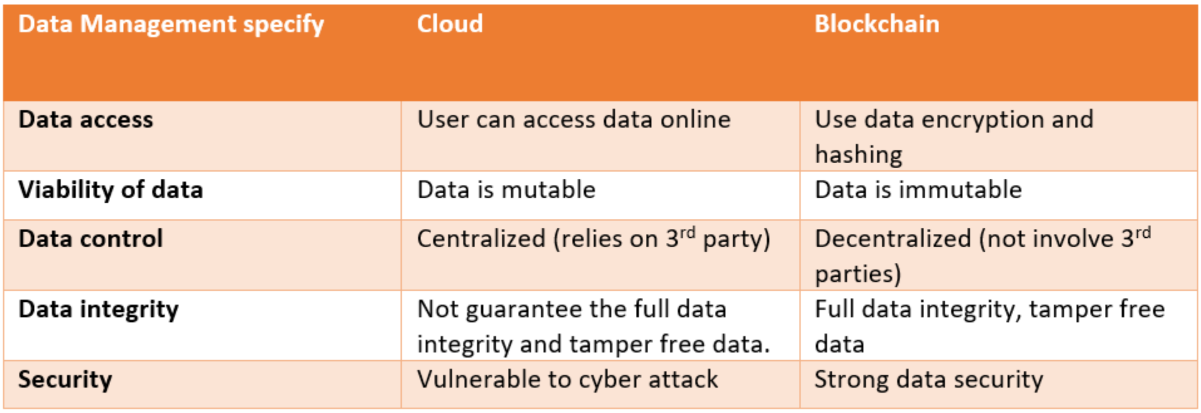
Part 3

The functioning of block chain in its different forms, such as block form, chain form, and as a distributed ledger, is demonstrated in this stimulator setup with pre-installed data. It also aids in illustrating the advantages of implementing this data storage mode, which uses automatic hashing technology for all data entered into the blockchain network and ensures big data storage in a cost-effective and distributed server mode, making it more difficult for parties to hack or access data. This practical setup's main goal is the hashing error, which alerts the block as soon as a modification or addition of data is made to the block. In addition, it disrupts the hash flow with the corresponding chain blocks, alerting the entire block or the users of the external modification or variation made to the original data. Only with the cooperation of all other users who need to mine the data, or with each user in that block network being individually authorised, can the error be fixed and the block returned to normal. This further assures that data security and transparency are improved to levels that completely allay any storage worries made about cloud storage.

Chapter 6 – Research Analysis and Findings

From the quantitative analysis of the data, according to our research and analysis, blockchain-based cloud storage is superior to traditional cloud storage in terms of security and transparency. Cloud computing as it is typically practised today is not sustainable. Distributed cloud storage, when properly implemented, can eliminate many of the drawbacks and shortcomings of the more common cloud-based data storage option. The term "blockchain" is commonly used to refer to a system for keeping data in an encrypted format utilising a number of hashing techniques. These data records are dispersed over multiple nodes, and their locations are all agreed upon by the system.

Below is a list of the benefits I find of blockchain-based cloud computing over conventional cloud storage.



Data Management specify	Cloud	Blockchain
Data access	User can access data online	Use data encryption and hashing
Viability of data	Data is mutable	Data is immutable
Data control	Centralized (relies on 3rd party)	Decentralized (not involve 3rd parties)
Data integrity	Not guarantee the full data integrity and tamper free data.	Full data integrity, tamper free data
Security	Vulnerable to cyber attack	Strong data security

Protecting users' personal information and data in the cloud is a major challenge. Data leaking is identified as the primary threat to cloud computing security. Encryption and database security have taken a giant leap forward with the advent of blockchain technology. Strong peer-to-peer distribution of identical blockchain copies throughout a cloud-computing infrastructure adds an extra layer of protection. Decentralized data storage is superior to a centralised system that can leak data. Files are encrypted and the pieces are distributed among multiple nodes, possibly in different parts of the world.

Visibility issues are another widespread risk associated with cloud computing. Blockchain technology enhances openness. The data saved in a block chain cannot be altered. Accessing data stored on a blockchain network from a different computer does not compromise the security or validity of the data stored on the other devices in the network.

Blockchain also has an essential advantage over traditional cloud storage in the event of a disaster. Distributed ledger technology, or blockchain, allows for the open dissemination of transactional histories. The fact that a blockchain may be accessed by many legitimate individuals simultaneously increases its worth. If a node in the blockchain ever fail, the other copies will continue to function normally.

Even while Blockchain is far superior to conventional cloud storage, using Blockchain comes with its own set of difficulties that must be overcome. The following are some of the biggest obstacles to blockchain implementation:

Technical Complexity

One of the biggest problems with implementing blockchain is how complicated the technology is. The method of combining blockchain with cloud computing to move, process, and secure network data requires the implementation of difficult mathematical issues.

Not enough available experts

Inadequate skill sets are another roadblock to integrating solutions. The blockchain's potential applications are still expanding rapidly. Professionals who have the training and experience to use these technologies are in short supply at the present time. As a result, there is a significant demand for blockchain experts. (Rovnaya, 2022)

Research analysis of advantage of blockchain in digital forensics:

In this analysis, the main aim is to understand the advantage of blockchain that brings in the field of digital forensics. As shown in chapter 5 of this research project, practical visualisation. I want to show that the primary goal of a digital forensic inquiry is to preserve digital evidence and maintain its integrity since only then is the evidence admissible in court. The scientific approach to confirm that the evidence submitted is exactly the same as the original obtained is crucial for the evidence to be acceptable. By establishing a forensic hash value of the image, this is achieved. A forensic hash creates a cryptographically robust and irreversible value for the image/data in order to guarantee the integrity of an acquisition. To maintain the integrity of the evidence, the raw disc image or files are duplicated and then computed and confirmed using the hash values for the original copy.

When processing or examining the evidence further, any changes to the hash values should be manually checked again and documented. As a result, the alternative of a block chain technology is shown, where the data can be stored as blocks and all the systems in the laboratory can be connected on a decentralised server to increase storage and also to increase the level of transparency of data, where each examiner enters the original extracted data after creating a forensic image into the block chain cloud space, where once entered it cannot be changed. Any changes made after entering the original data cause the hash value to be broken, allowing new data to be added to the block system as new blocks. As a result, it develops into a synchronised block chain system that is simple to maintain, guarantees data transparency, and offers an affordable storage option. Additionally, as the network grows in size, each device or node connected to it behaves as a separate server or cloud base due to the network connectivity. As a result, the block chain system has little downtime, and timely data availability is also guaranteed. Since there are several devices, hacking or unauthorised third-party access to the network data may be managed and monitored to a higher extent thanks to block chain's strong security from facing attack. Only when more than 51% of the computers or users in the block chain are hacked are changes or taking control of the network conceivable.

As a result, it provides strong data security. Therefore, I think that combining block chain with this field of digital forensics has the potential to be a brilliant idea that will make it function much more effectively in the long run.

Chapter 7 – Conclusion and recommendation

The study is titled "Distributed cloud storage based on blockchain and its forensic characteristics." The objective was to use a quantitative analysis to determine the benefits of blockchain-based cloud computing over the current traditional storage method. The research has discovered a reliable response to the put forward research questions.

Overall, based on findings, The range of applications for distributed cloud storage, as well as its advantages and disadvantages, are constantly being investigated. It is unquestionably a fantastic implementation to handle the vast amount of data while also maintaining the integrity of the original evidence using a system that requires less manual labour and is much more transparent and effective. Based on its limitations and the reasons it is not a widely utilised technological approach, block chain implementation of storage offers a lot of room for additional study. Further analysis can be done on the potential enhancements and feature additions that could make this technology more usable and dependable. Nevertheless, this is advantageous because of its openness and data security. When distributed cloud storage-related crimes are taken into account or are to be investigated, it is a relatively new sphere of issues, so that is a new area of study. Future research, however, should place greater emphasis on quantitative analyses to ascertain the extent to which blockchain is encouraging sustainability. Therefore, more companies will see the benefits of blockchain technology and be willing to use it. Even more so, it would be interesting to study how blockchain is influencing company operations, what businesses are doing differently in their day-to-day activities, and which business processes have needed re-engineering.

References

aerd dissertation, n.d. *sambling strategy.* [Online]
Available at: https://dissertation.laerd.com/process-stage6-step4.php

Bhandari, P., 2022. *What Is Quantitative Research? | Definition & Methods.* [Online]
Available at: https://www.scribbr.co.uk/research-methods/introduction-to-quantitative-research/

Casino, F., Patsakis, C. & Thomas, D. k., 2021. Blockchain solutions of Forensics.

Forbes, 2021. *Forbes.* [Online]
Available at: https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/?sh=aad455a22678

GeeksforGeeks, 2022. *Features of blockchain.* [Online]
Available at: https://www.geeksforgeeks.org/features-of-blockchain/

GeeksforGeeks, 2022. *Hasing.* [Online]
Available at: https://www.geeksforgeeks.org/hashing-set-1-introduction/

GeeksforGeeks, 2022. *Types of blockchain.* [Online]
Available at: https://www.geeksforgeeks.org/types-of-blockchain/

George, T., 2022. *Exploratory Research | Definition, Guide, & Examples.* [Online]
Available at: https://www.scribbr.co.uk/research-methods/exploratory-research-design/

Goundar, S., 2012. *Chapter 4 - Understanding Cloud Computing.* [Online]
Available at: https://www.researchgate.net/publication/332979373_Chapter_4_-_Understanding_Cloud_Computing

Harvard business review, 2017. *The truth about blockchain.* [Online]
Available at: https://hbr.org/2017/01/the-truth-about-blockchain

Hayes, A., 2022. *Blockchain Facts: What is it, how it works and how it can be used.* [Online]
Available at: https://www.investopedia.com/terms/b/blockchain.asp

IBM cloud education, 2019. *Cloud storage.* [Online]
Available at: https://www.ibm.com/cloud/learn/cloud-storage

Iraqi, y., Almulla, S. & Jones, A., n.d. Cloud computing and digital forensics.

Kumar, K., 2018. DellEMC. *Distributed Cloud storage with blockchain technology,* p. 10.

kumar, K., Aggarwal, N., Jain, s. & sofat, s., n.d. Significance ofHash value Generation in digital forensic.

Lamprini, C. F., 2021. A blockchain-based "Forensic Model for Financial Crime investigation: The Embezzlement scenerio.

Lim, N., 2020. *Cloud Forensics and the Digital crime scene.* [Online]
Available at: https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene#:~:text=Cloud%20forensics%20refers%20to%20investigations,and%20can%20better%20preserve%20evidence.

Liu, G., He , J. & Xuan, X., 2021. A data preservation method based on blockchain and multidimensional hash for digital forensics. p. 12.

novkovic, G., 2017. *Five characteristics of cloud computing.* [Online]
Available at: https://www.controleng.com/articles/five-characteristics-of-cloud-computing/

Onyejiaku, T. K., 2022. *What are the characteristics of blockchain?.* [Online]
Available at: https://www.educative.io/answers/what-are-the-characteristics-of-blockchain

Ricci, J., Baggili, I. & Breitinger, F., 2019. Blockchain-Based Distributed Cloud Storage Digital Forensics: Where's the Beef?. p. 9.

Rovnaya, A., 2022. *Blockchain in cloud computing.* [Online]
Available at: https://www.cleveroad.com/blog/blockchain-cloud-computing/#:~:text=The%20incorporation%20of%20blockchain%20in,system%20discovery%2C%20and%20much%20more.

Saha, R., Conti, M., Lal, C. & Kumar, G., 2021. Internet of Forensics: A blockchain-Based digital forensics framework for IoT applications.

Sajvee, 2019. *Blockchain simply explained.* [Online]
Available at: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work/

Schmitt, V. & Jordaan, J., n.d. Establishing the validity of Md5 and Sha-1 in light of recent research demonstrating cryptographic weaknesses in the algorithms.

SentinelOne, n.d. *Whay is hashing.* [Online]
Available at: https://www.sentinelone.com/cybersecurity-101/hashing/

Shekhtman, L. & Waisbard, E., 2021. EngraveChain: A Blockchain-Based Tamper-Proof Distributed Log system. p. 16.

Shivam, K., 2020. [Online]
Available at: https://kumarshivam-66534.medium.com/cloud-forensics-be18e14230de

Streefkerk, R., 2022. *Inductive vs Deductive Reasoning | Difference & Examples.* [Online]
Available at: https://www.scribbr.co.uk/research-methods/inductive-vs-deductive-reasoning/

Talend, n.d. *What is Cloud Computing?.* [Online]
Available at: https://www.talend.com/resources/what-is-cloud-computing/

Torres-Corral, A., 2021. *What Are the Most Common Cloud Computing Service Delivery Models?.* [Online]
Available at: https://www.alertlogic.com/blog/what-are-the-most-common-cloud-computing-service-delivery-models/#:~:text=There%20are%20three%20main%20cloud,Platform%20as%20a%20Service%20(PaaS)

Tripwire, 2019. *Forensics in the Cloud: What You Need to Know.* [Online]
Available at: https://www.tripwire.com/state-of-security/security-data-protection/cloud/forensics-cloud-need-to-know/