EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Secure Digital Transactions in The Education Sector Using Blockchain

Muhammad Nouman[1,*], Kareem Ullah[1] and Muhammad Azam[1]

[1]University of Agriculture Faisalabad, Pakistan

Abstract

A blockchain is a decentralized, distributed peer-to-peer network that allows one node to communicate with other nodes. When using blockchain technology in education, data or records can be stored permanently without fear of hacking due to the secure hashing algorithms in blockchain technology. The goal is to create a new blockchain technology that has the potential to form a decentralized application in education, with the help of different components, such as Meta Mask, IPFS, Ganache, and other test networks such as Rinke by and Rostand, as well as Web3 JS and Ethereum cryptocurrency. This research was applied in the following ways: (a) analysing the three most well-known blockchain cryptocurrencies (Bitcoin, Litecoin, and Ethereum); (b) investigating the features and issues surrounding the Bitcoin cryptocurrency, and (c) creating a graphical interface for the IPFS bandwidth analysis for storing files on the network using Web3 JS and Smart Contracts. As a result, this research paper provides a proper demonstration of data storage without the use of a centralized system (decentralized and distributed P2P network) using IPFS to aid in data segmentation for storage purposes.

Keywords: Blockchain technology, IPFS, Litecoin, Ethereum, P2P technology

Received on 25 August 2021, accepted on 31 October 2021, published on 03 November 2021

doi: 10.4108/eai.3-11-2021.171758

1. Introduction

A Blockchain is a chain of blocks that contain information. This technique was regionally described in 1991 by a group of researchers and was regionally intended to timestamp digital documents that could not be backed up or tampered with, almost like a notary. It was, however, mostly used and adopted by "Satoshi Nakamoto" in Bitcoin 2009 to create digital Bitcoin [1]. A blockchain is a distributed ledger that is completely accessible to anyone. They have an intriguing property that is extremely difficult to change once recorded inside a blockchain [2].

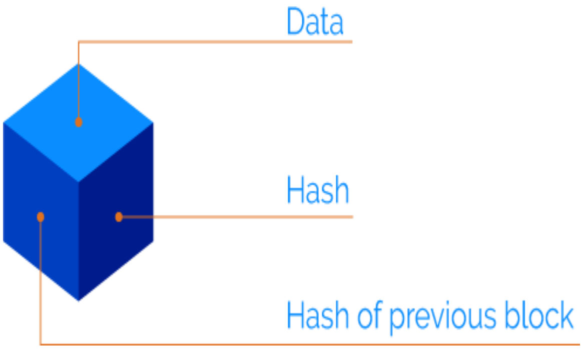


Figure 1. Functions of Blockchain

Each square contains data about the square's hash and the previous square's hash. The information put away inside the

[*]Corresponding author. Email: m.nouman909@gmail.com

square is dictated by the kind of blockchain. The bitcoin blockchain, for instance, stores exchange data like the sender, recipient, and a few coins [3]. A square additionally has a hash, which can measure up to a unique finger impression and it obstructs all the substances that have fingerprints. At the point when a square is made, its hash is determined; changing something inside the square will make the hash change. All in all, the hash is exceptionally helpful and wanted for recognizing changes in blocks. If the finger changes, the square will at this point be something very similar [4]. The hash of the previous block is the third component inside each square. This adequately makes a blockchain, and this blockchain is incredibly secure. For instance, consider the accompanying three-block chain. Each square has its hash just like the previous square's hash [4]. Square 3 alludes to Impede 2, and Square 2 alludes to Hinder 1. The main square is extraordinary; it is alluded to as the "virtuoso square." All squares will become invalid if the hash of the square changes. Utilizing a hash is inadequate to keep PCs from figuring out hundreds or thousands of hashes each second. To make your square legitimate once more, you can successfully recalculate every one of the hashes [5].

Squares have gone through a change known as Verification of work. It is the system that dials back block creation. Because of bitcoin, it requires around 10 minutes to figure out the necessary confirmation work and add another square to the chain [6]. Since it tempers one square to recalculate the evidence of work of the relative multitude of following squares, this instrument expects you to treat the squares. In this way, the security of the blockchain originates from its inventive perspectives on hashing and verification of work systems. Yet there is another way that the blockchain gets itself, and that is by paying dissemination and that is by focal personality to deal with the chain [7]. A blockchain utilizes a P2P organization and anybody is free to join. The square will check everything when somebody joins the organization. The square will ship off to everybody in the organization each note that confirms the square to guarantee that it has not been messed with, and if everybody looks at each note on their blockchain, they make an agreement, they concur on one square, and they stay away from all pieces of the chain [6].

Tempered squares can be dismissed by different hubs at work. To effectively treat blockchains, you should treat all squares on the chain, re-try the verification of work for each lock, and deal with over half of the P2P organizations. Then, at that point and really at that time, will your square be acknowledged by others or any other individual? This is almost impossible to achieve [7]. Blockchain is an innovation for making exchanges that are decentralized, free, and conveyed. There is no power over any outsider, like a bank, trade, or other elements that will charge expenses and manage exchanges. Blockchain innovation is a protected innovation that utilizes hashing calculation. It utilizes a private and public key for security and hashing. Bitcoin was the main cryptographic money to acquire notoriety in the decentralized application space [8].

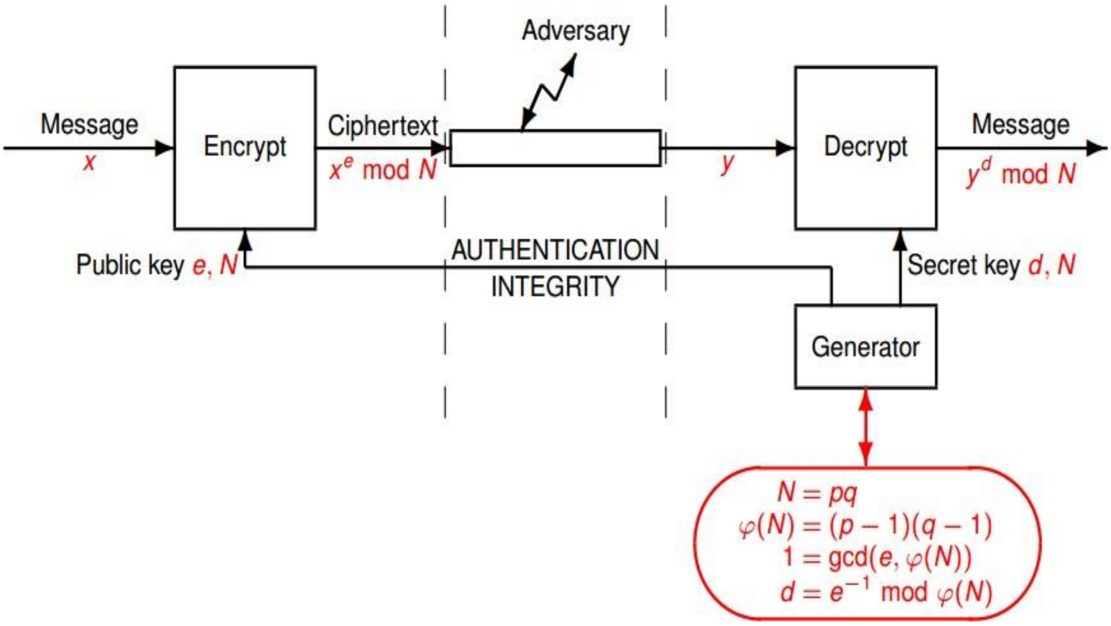


Figure 2. El Gamal Cryptographic Protocol and Ciphertext System

A cryptographic encryption function can ensure the integrity of the data [8]. A hash function is used to create a short "fingerprint" of some data; if the data changes, the fingerprint becomes invalid. Even if the data is stored in an unsafe location, its integrity can be checked regularly by recalculating the fingerprint and ensuring that it has not changed (Stinson 2005). This research focuses on public-key cryptosystems that use the discrete logarithm problem. The first and most well-known is the cryptographic system [9]. The discrete logarithm problem serves as the foundation for a plethora of cryptographic protocols, which we investigated in the remainder of this paper.

Blockchain has the properties of decentralization, verifiability, and immutability, which can provide numerous benefits to educational development. Many application cases have demonstrated high potential. However, blockchain research in education is limited, and application has only recently begun. As a result, it is important to examine previous research and define a decentralized blockchain technology in education for secure digital transactions. The study's goal was to demonstrate decentralization technology in the education sector. It is simple to solve using blockchain technology and the Ethereum network. The blockchain network ensures that no data is ever lost. This approach is easily adaptable to investigate and discover a solution to the problem of centralizing data storage. Servers, for example. It is frequently a source of concern for researchers [10].

1.1 Objectives

The following are the main objectives of our work:

- To create and introduce new technology that has the potential to form a decentralized application in education.
- To use the Ethereum network with Web3 Js and IPFS support for data security and data integration using a peer-to-peer network model.
- To implement blockchain technology with the help of different components, such as Meta Mask, IPFS, Ganache, and other test networks such as Rinke by and Rostand, as well as Web3 JS and Ethereum cryptocurrency.

The rest of this research paper is organized as follows. Section 2 discusses related works. Section 3 contains a summary of our research findings as well as a discussion of them. Our findings and future research directions are summarized in Section 4.

2. Literature Review

Satoshi et al. introduced Bitcoin, a digital currency, in 2008. It was introduced to reduce the use of paper currency and allow people to transfer money from one location to another without the involvement of any third-party service, such as a bank accountant or an intermediary source [10]. Bitcoin was created on a peer-to-peer network known as the blockchain. Bitcoin was simply a unit through which people could assign a monetary value to anything, such as a house, car, or electronic device [11]. The organization records the exchange time by joining them into a nonstop chain of hash-based work tests, which is a record that can't be changed without rehashing the work test. The longest chain demonstrates the demand for events, but it also demonstrates that it came from the most extraordinary collection of computer processors. On the off chance that most of the computer processing power is constrained by hubs that don't collaborate, they will assault the organization, produce the longest chain, and surpass the assailants. In his fundamental white book, he states [12], "To change a square from an earlier time, an assailant should re-try the work trial of the square and every resulting square, and then beat the fair individual and conquer the hubs."

As indicated by the blockchain, which utilizes cryptographic components [13], [14]. It is almost difficult to hack the blockchain because reworking the story would be restrictively costly because of the amount of registering power required. The entirety of this is a piece of its cryptographic segment that recognizes a circulated record, a keen agreement, and encryption. Individuals habitually accept that this load of things is tradable [15] and proposed a refined structure dependent on the blockchain’s disseminated decentralization framework. The information stockpiling and sharing plan for decentralized capacity frameworks, just as a structure that joins the decentralized stockpiling framework with the interplanetary record framework, the Ethereum blockchain, and ABE innovation, is proposed. In this construction, the data owner can convey a secret key to data customers and scramble shared information by showing an entrance methodology, and the arrangement accomplishes fine-grained admittance authority over data [16], [17]. Research into whether business applications can profit from the positive properties of blockchain innovation while holding onto the abilities and qualities of existing focal approval procedures by utilizing dispersed approval frameworks dependent on the overall record [18]. A model with a decentralized methodology enjoys the benefit of filling in as an establishment for future decentralized business advancement. This article talks about the execution and approval of a blockchain-based admittance control solution for decentralized applications. Evidence of the idea utilizing a suitably circulated bookkeeping stage approves the practicality of this job-based admittance control arrangement (RBAC) in the chain. The approval framework's execution plans to agree with the assessment needs and cases to try not to be utilized as a business administration [19].

Kmart, Polaroid [20], [21] don't preclude the chance of a keen agreement arrangement executing an agreement completely later, yet this depends upon the program's capacity to meet all the lawful agreement prerequisites needed for exchange execution. This section gives an overall outline of shrewd agreements, electronic agreements, savvy property, and the authoritative prerequisites needed to finish an agreement. As per the exploration paper 'Educt: Square chain based advanced education stage' distributed by "Muhammed Terranova" and upheld by the Slovenian Exploration Organization, a blockchain-based advanced education stage named "Educt" was suggested that depends on the European credit movement and aggregation framework [22]. It exploits the upsides of the blockchain framework as decentralized engineering that gives security, namelessness, life span, trustworthiness, straightforwardness, and changelessness [23], [24].

The objective of this proposition is to create worldwide confidence in credit schooling and a review framework that permits understudies to get to their whole course history in a single look. A few advanced education establishments have utilized blockchain innovation to foster different advanced education arrangements and approaches. The Bitcoin blockchain is used by most arrangements [25], [26], [27].

3. Materials and Methods

This section explains how this study was designed, as well as the methodology strategy used to achieve the desired results. Why the materials and methods were chosen, and how the research was carried out. The study made use of Ethereum data (https://etherscan.io/).

This source interprets the existing blockchain transactions. It has many networks, but the Ethereum Magnet was chosen solely for retrieving transactions and their results [28]. The Test Networks, such as Ripstein Test Net and Rinke by Test Net, are used to transfer Ethereum coins and currency. Node.js is a JavaScript runtime that was developed by the Chrome V8 JavaScript engine. Node.js employs a non-blocking, event driven I/O model, which makes it lightweight and efficient. The Node.js package ecosystem, nm., [29]is the largest open-source library ecosystem in the world. As the Ethereum JavaScript API, Web3Js is used. Web3.js is a set of libraries that allow you to communicate with a local or remote Ethereum node via HTTP, WebSocket, or IPC. Ganache is a chain of personal Ethereum development blocks that we use to implement contracts, develop apps, and run tests. It's available as a desktop application as well as a command-line tool (formerly known as Test up). Ganache is compatible with Windows, Mac, and Linux.

Meta Mask is a bridge that allows you to access the distributed network. This enables us to run Ethereum apps directly in our browser without the need for a full Ethereum node. Our mission is to make Ethereum accessible to as many people as possible. Infula is a hosted cluster of Ethereum nodes that users can use to run their applications without the need to configure their own Ethereum node or portfolio [30]. Many people are unfamiliar with the name Infula, but if you've used Meta Mask, you've used Infula because it is the Ethereum provider that supports Meta Mask.

3.1 Ethereum Virtual Machines (EVM)

The Web3 Sj library, which is the main JavaScript library that interacts with the Ethereum blockchain, developed the methodology for developing the local in-memory blockchain [31]. There are several factors to consider when developing a decentralized application on Ethereum. Your smart contract, which is deployed on the Ethereum blockchain, is one of them. On the other hand, there should be a website that can interact or communicate with the blockchain client or node. That is why the Web3 Sj library is so important. It allows us to create a website that can communicate with the node or client. Java or Python programming can also be used for the development of the decentralized app, but we chose JavaScript because we will be interacting with the web browser, and it is the best option for doing so [32].

The diagram below depicts the Ethereum blockchain's EMV network. How it uses RPC to communicate with other nodes on the local blockchain.

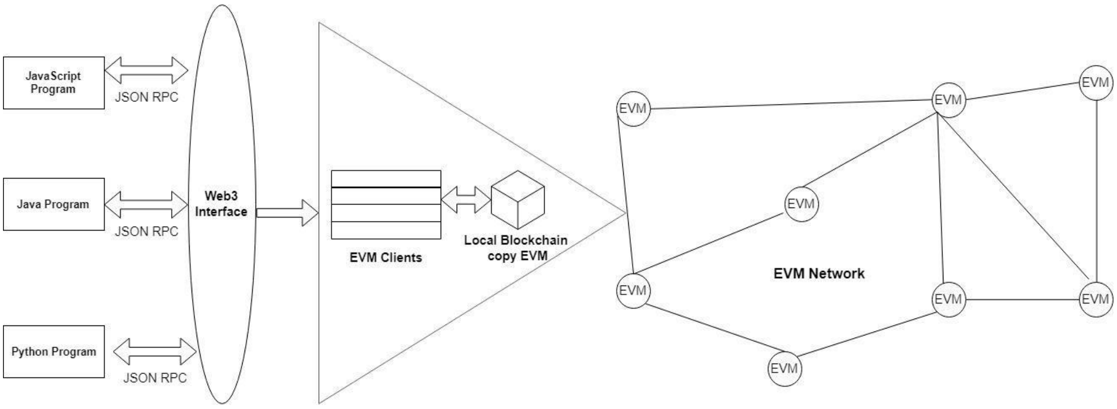


Figure 3. Blockchain and Ethereum

Unlike the Bitcoin protocol, Ethereum was created with flexibility in mind. Bitcoin network nodes are simple software programs that validate and store transactions, whereas Ethereum network nodes are fully functional Ethereum virtual machines that can execute scripts of varying algorithmic complexity. Programs that run on the EVM can be created by developers. These programs are written in Solidity, a new JavaScript programming language. The EVM byte code is used to compile Solidity programs. For these programs, the EVM serves as the execution environment. These programs are separate from one another. They have no access to the file system, the network, or any other processes running on the same machine.

The peer-to-peer protocol is also present in Ethereum nodes, as it is in Bitcoin. Many nodes connected to the network maintain and update the Ethereum blockchain database. Each node in the network runs the EVM and follows the same set of instructions. The programs (written in Solidity) that you add to your node are distributed to all nodes in the Ethereum network and run when the implementation criteria are met. Solidity programs are referred to as Smart Contracts. When certain criteria are met, these programs are launched. The web3 interface allows external programs to communicate with the EVM client. Web3 libraries expose several JSON RPC-based methods for communicating with Ethereum clients.

The two types of Ethereum customers are the primary customer and the thin client. Currently, the main EVM client is available for all major desktop operating systems. Although plans exist to develop thin clients for smaller devices such as phones, IoT (Light Client based on Android), and so on. Geth is the most popular Ethereum client. The client is written in the Go programming language and includes all the EVM's features. Capp-ethereal/eth is the second most popular EVM client. This client is written in C++. You can follow the installation instructions via the GitHub links.

The full client will always keep a local copy of the Ethereum blockchain database. Then, if your infrastructure cannot handle such a large amount of data, you can use a thin client like Meta Mask. It is, in fact, a Google Chrome extension that will communicate with the Ethereum chain of blocks via the Internet and retrieve the requested data. Transactions, like those on the Bitcoin network, are validated using the work permit or proof of work principle. The consensus algorithm used in this case, however, differs from that used in Bitcoin. Ethos is a hash algorithm used by Ethereum. This algorithm is set to be replaced by a new Casper.

Ethereum supports the following types of blockchains:

- A public blockchain is a chain of squares that anybody can peruse. Anybody can send exchanges and anticipate that they should be enrolled if they are legitimate, and anybody can take part in the agreement cycle, the most common way of figuring out which squares are added to the chain and what their status is [33].
- A Blockchain Consortium: A Blockchain consortium is one in which the agreement interaction is overseen by a gathering of pre-chosen hubs. A consortium is a gathering of banks or monetary organizations.
- Private Blockchain: A private blockchain is one in which an association's composing rights are unified. Perusing benefits may be available to all people or may be limited in some way [34].

The Ethereum client can be set up to connect to any of these blockchains. A client, on the other hand, can only connect to one type of blockchain network at a time. Every transaction that takes place on the blockchain incurs costs. These prices are in terms of gas units. The Ethereum network's standard unit is ether, and the lowest value is whey.

Daps are applications that communicate with the Ethereum network (Distributed Applications). In a nutshell, they are programs that interact with the Ethereum blockchain, such as simple HTML / JavaScript web applications. In this blog, I will document a realistic example of a DA application that I will create in JavaScript. Then it will attempt to recreate the same thing in Java.

3.2 Ethereum Blockchain Implementation

The initial phase of carrying out the Ethereum blockchain is to introduce node.js. Node.js is a JavaScript runtime that was created by utilizing the Chrome V8 JavaScript motor. Node.js utilizes a non-hindering, occasion driven I/O model, which makes it lightweight and productive. The Node.js bundle biological system, nm., is the biggest open-source library environment on the planet. At the point when decentralized applications are created, keen agreements will assume a half-part. What are brilliant agreements prepared to do? This is the resource between the hub and the Ethereum organization. It is a Java Content reflection that is used to invoke the sharp agreement work.

The web3.eth.Contract object simplifies communication with Ethereum blockchain-savvy contracts. Blockchains are also a consistent wellspring of interest. The production of "Savvy Agreements" is quite possibly the latest turn of events. These agreements are basic PC programs that can be utilized to consequently change coins based on specific amendments [35].

3.3 Storing files using IPFS

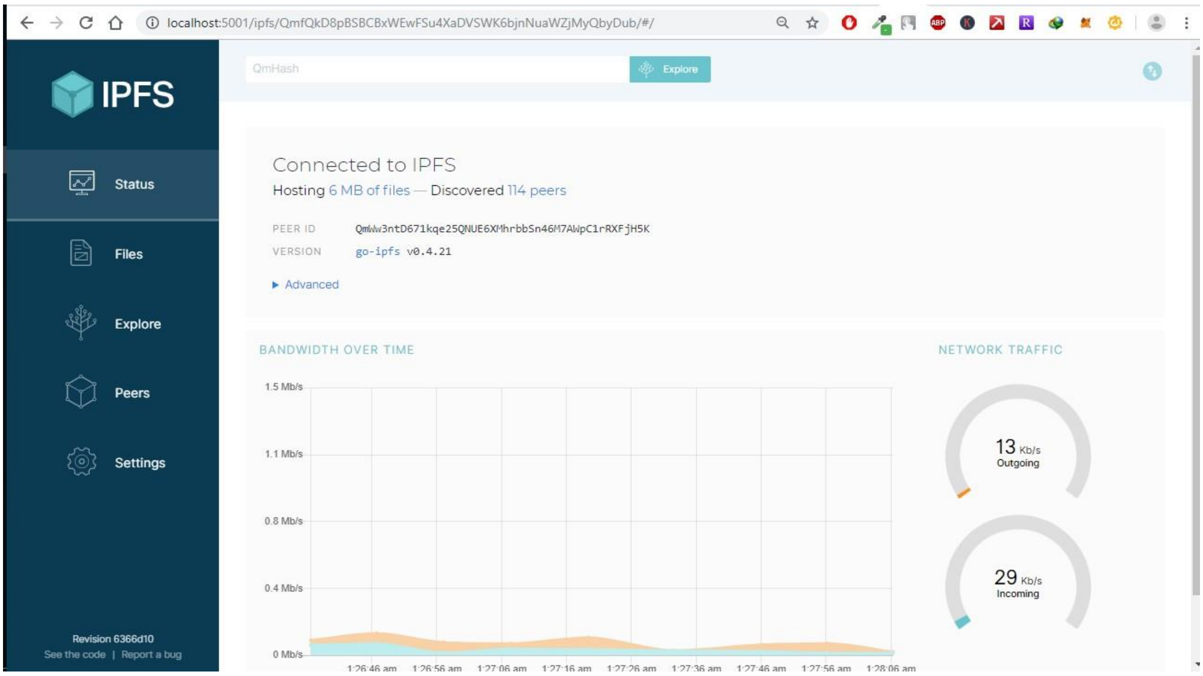
The multimedia files from the system will be stored on a peer-to-peer and decentralized network using IPFS in this section. An interplanetary file system can store data indefinitely without the involvement of data monopolies such as Google, Facebook, or Amazon. This is a global peer-to-peer network, like the internet concept. IPFS can be downloaded easily (https://dist.ipfs.io/# go-it's) and then extracted and installed on the local machine using the command prompt in Windows or the terminal in Linux or Mac [36].

To start the IPFS on the local machine, use the following commands:

1. (Ip’s executable file location) unit
2. (Ip’s executable file location) daemon
3. (Ip’s executable file location) add -r (location of file or directory to be added)

These are the simple steps to getting IPFS up and running on your local machine. What you need to do is run the local server with the daemon command. It will display a popup window requesting access to the public network.

IPLD is the data model of the web sensitive to content. This allows us to treat all data structures linked to hashes as subsets of a uniform information space, combining all the data models that link data to hashes into IPLD instances.



localhost:5001/ipfs/QmfQkD8pBSBCBxWEwFSu4XaDVSWK6bjnNuaWZjMyQbyDub/#/

Connected to IPFS

Hosting 6 MB of files — Discovered 114 peers

PEER ID QmWw3ntD671kqe25QNUE6XMhrbbSn46M7AWpC1rRXFjH5K

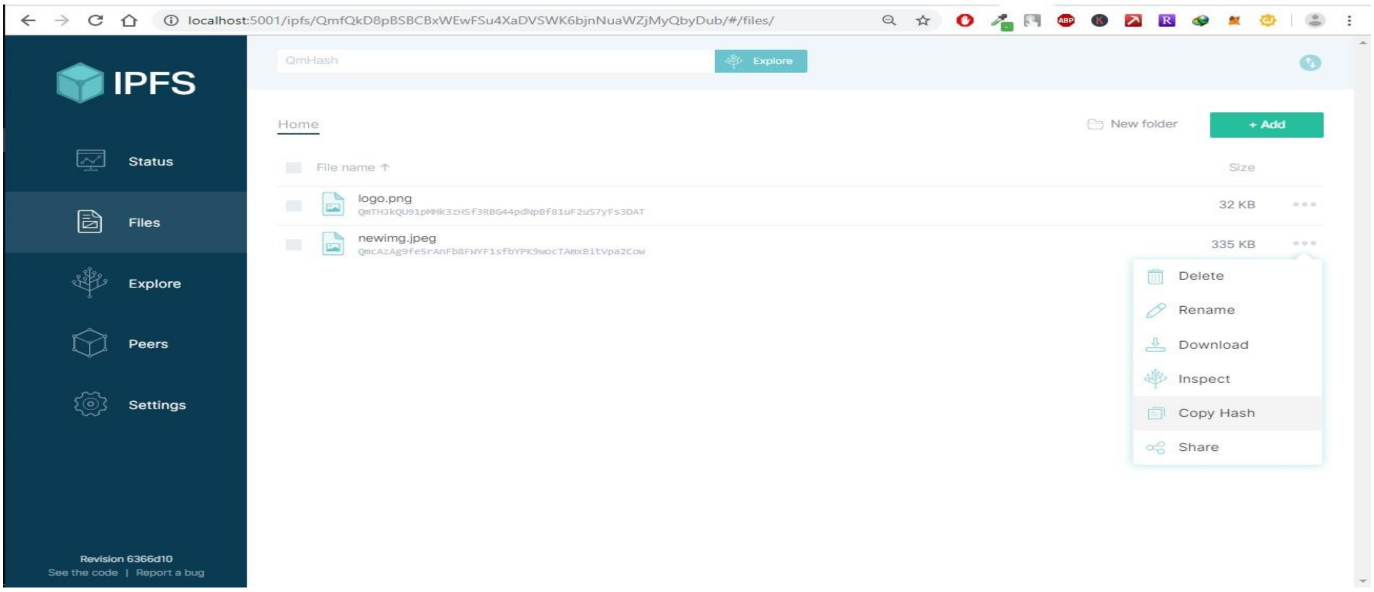
VERSION go-ipfs v0.4.21

Figure 4. Localhost IPFS Interface

Addressing content with hashes has become a popular way to connect data in distributed systems, ranging from blockchains that run their favorite cryptocurrencies to confirmations that support their code, to web content in general. Although all these tools rely on some common primitives, their underlying data structures are incompatible. IPLD is a unified namespace for all hash-inspired protocols. Protocols can move links through IPLD, allowing you to explore data independent of the underlying protocol.

3.4 IPFS and Ethereum Blockchain

This section describes the IPFS file system in conjunction with the Ethereum blockchain. The implementations were carried out with the assistance of the Web3 JS library. The only thing that happens in the above section is a transaction. The data is transferred in the form of a transaction via the Ethereum blockchain and the Rinke by Test Network. Smart contracts can only be used to deploy hash codes. However, with the help of IPFS, we can now easily store multimedia files such as images, text, sounds, or videos on a P2P network [37]. After uploading, IPFS returns a string of the file that is distributed in a decentralized manner. The hash format is like an encrypted string that will be uploaded on P2P until the internet ceases to exist in the world. The process of adding or uploading a file such as an image, sounds, videos, or text. is to be added by selecting the green "Add" button in the upper right corner of the IPFS interface. The hash code of the file that is uploaded on the IPFS nodes is shown in the figure below. This hash has the following format: ‘QmcAzAg9fe5rAnFb8FWYF1sfbYPK9wocTAmxBitVpa2Cow’



localhost:5001/ipfs/QmfQkD8pBSBCBxWEwFSu4XaDVSWK6bjnNuaWZjMyQbyDub/#/files/

File name ↑	Size
logo.png QmTHJkQU91pMMk3zHSf3RBG44pdNpBf81uF2uS7yFs3DAT	32 KB
newimg.jpeg QmcAzAg9fe5rAnFb8FWYF1sfbYPK9wocTAmxBitVpa2Cow	335 KB

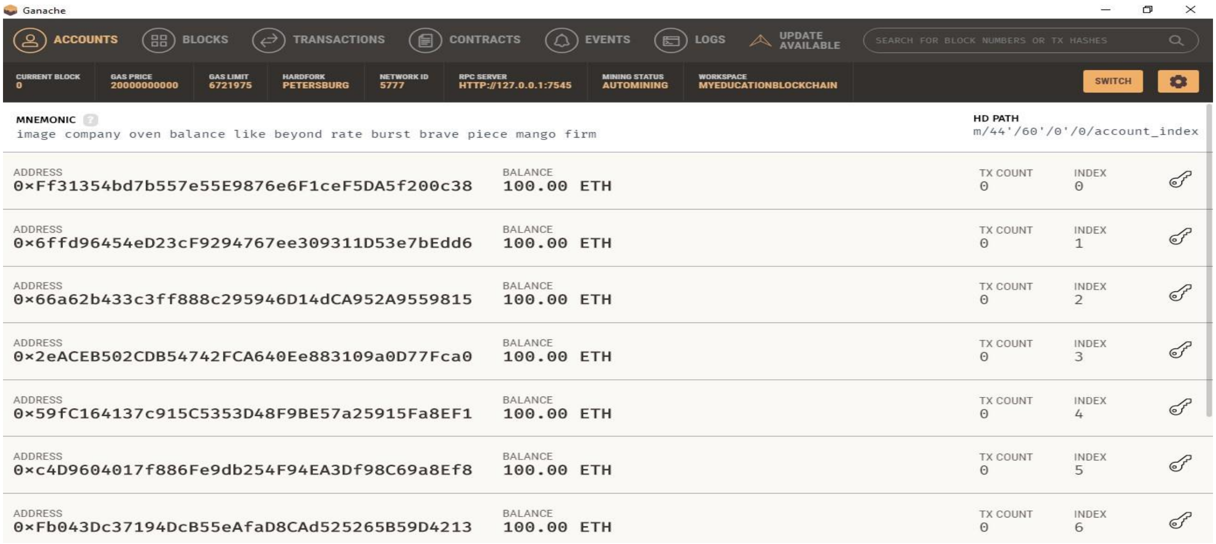
Figure 5. Obtaining the hash code of an IPFS-uploaded file

This is like an encrypted string that will continue to be uploaded on P2P until the internet ceases to exist in the world.

3.5 Ethereum Blockchain with Ganache

Ganache is used to create a personal Ethereum Blockchain on which to test your Solidity contracts. When compared to Remix, it has more features. You must first download and install the Blockchain on your local machine before you can use Ganache.

Ganache is used on local blockchains to perform transactions in the Ethereum ether unit of digital currency. Ganache is a blockchain that is stored locally in memory and uses a local remote procedure call (RPC). The Ganache was chosen due to its low cost. This research cannot afford to conduct a transaction on a real or main network [37]. Each account can also show a transaction count of zero when the user has not yet completed any transactions.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
0	20000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	MYEDUCATIONBLOCKCHAIN

MNEMONIC
image company oven balance like beyond rate burst brave piece mango firm

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×Ff31354bd7b557e55E9876e6F1ceF5DA5f200c38	100.00 ETH	0	0
0×6ffd96454eD23cF9294767ee309311D53e7bEdd6	100.00 ETH	0	1
0×66a62b433c3ff888c295946D14dCA952A9559815	100.00 ETH	0	2
0×2eACEB502CDB54742FCA640Ee883109a0D77Fca0	100.00 ETH	0	3
0×59fC164137c915C5353D48F9BE57a25915Fa8EF1	100.00 ETH	0	4
0×c4D9604017f886Fe9db254F94EA3Df98C69a8Ef8	100.00 ETH	0	5
0×Fb043Dc37194DcB55eAfaD8CAd525265B59D4213	100.00 ETH	0	6

Figure 6. Test Accounts for Ganache

The figure above depicts a dummy account for the Ethereum test transaction. Ganache provides ten dummy or test accounts for ether transformation. The following step is to use the GIT terminal to execute or write the node commands [38]. Using the node package module (nm.). I imported the Web3 JS library and then used node commands to create an object from the Web3 Js that provides access to all Ethereum functions. Then the RPC's local address must be used and passed to the Web3 Js object. Then you'll need an account address. All features of an Ethereum account can be archived using the account address. The function oversees gaining access to the account's balance. Essentially, eth is a class that contains many functions. Further functionality can be found at https://web3js.readthedocs.io/en/1.0/web3-eth.html.

A snippet of smart contract:

```
nouman@DESKTOP-3N97TLA MINGW64 ~
$ node
> var Web3 = require('web3')
undefined
> var URL='http://127.0.0.1:7545'
undefined
> var w = new Web3(... URL)
undefined
> var address='0xFf31354bd7b557e55E9876e6F1ceF5DA5f200c38'
undefined
> w.eth. get Balance (address, (err, ball)=>{balance=ball})
Promise {
<pending>,
domain:
Domain {domain: null, _events:}
[Object: null prototype] {
remove Listener: [Function: updateExceptionCapture],
new Listener: [Function: updateExceptionCapture],
error: [Function: debugDomainError]},
_events Count: 3,
_maxListeners: undefined,
members: [],
[Symbol(kWeak)]: WeakReference {}}}
> balance
'100000000000000000000'
> w.utils.fromWei(balance,')
> w.utils.fromWei(balance,'ether')
'100'
```

3.6 Smart Contract Deployment and IPFS hash storage

Steps to deploy smart contracts install nm.

1. Begin with the Ganache
2. Launch the Ganache GUI client that you previously downloaded and installed. This launches your local blockchain instance. The full explanation can be found in the free video tutorial.
3. Smart Contract Compilation and Deployment
4. $truffles migrate —reset
5. Every time you restart ganache, you must migrate the smart contract.
6. Configuration of the Meta Mask
7. The Meta mask must be unlocked.
8. Connect the meta mask to your Ganache-provided local Ethereum blockchain.
9. Import from a ganache-provided account.
10. Execute the Front-End Application.
11. Set up Deventer the following URL into your browser: http://localhost:3000/index.html

3.7 Algorithm for Retrieving Files from IPFS

```
--------------------------------------------
Algorithm 1: Retrieve a file from IPFS
--------------------------------------------
procedure Retrieve File (A)
        filelocation =  loc
        hash = h
              if value h in A, then
                 return loc
              endif
end procedure
```

The table above depicts how IPFS retrieves a file over a network. The file can only be obtained or accessed by the node that has the hash. The hash code of the blockchain, then. So, we can save this hash code to the Ethereum blockchain and then use https://ipfs.io/ipfs/ to retrieve the file. SHADOW CODEIPFS, a Blockchain-based peer-to-peer hypermedia protocol, officially [39] launched its file storage network on Ethereum rather than Bitcoin, citing "the Ethereum network development community and several innovative features." The File coin, a piece of information stockpiling and electronic money network intended for the IPFS convention, was made on the Bitcoin network in 2014 to fill in for the establishment of the hypermedia conveyance convention, which empowers clients to arrange, appropriate, dissect, and store information. Store in a more noticeable area. a blockchain-based organization that is unchanging. Convention Labs [40], the group behind IPFS and File coin advancement, started with the improvement of the IPFS convention on the Bitcoin organization to exploit its unchangeability and phenomenal safety efforts [41].

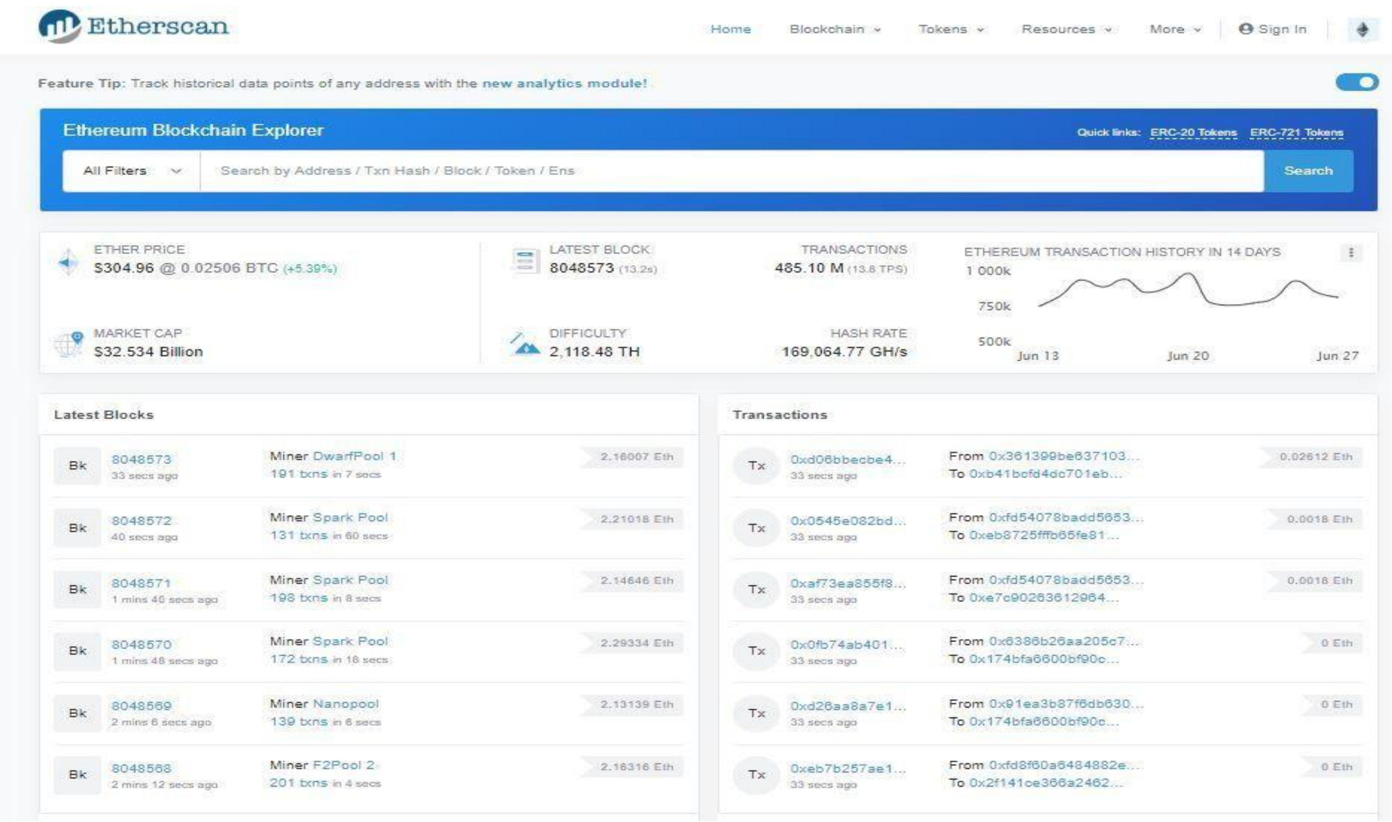
The beginning phases of advancement saw the rise of a few use cases because of the cooperative energy between the Bitcoin organization and the IPFS convention, permitting the convention to work as an appropriate web network through the cryptography of each document on the Blockchain organization [42]. The Bitcoin organization's security gave the constant IPFS framework needed to perform basic tasks like putting away perpetual information, killing copy records on the organization, and utilizing hubs to look for documents on the organization. The whole convention's blockchain-based framework implied that it would work more efficiently than existing other options, with lower expenses and transmission capacity [43]. According to the IPFS, businesses with large amounts of data could save millions of dollars in bandwidth by using an equal-to-equal approach. However, after recognizing a significant difference in the development communities of the two networks, IPFS decided to migrate to the Ethereum network. The IPFS development team believes that the Ethereum network's well-connected and well-functioning development community is one of the network's most valuable assets, with the potential to influence the [44] IPFS protocol in a variety of ways. Following the announcement of IPFS, experts such as initc3 co-director and Cornell professor Emir Gun Serer emphasized the importance of a well-functioning development community.

3.8 Main Ethereum Network

This section describes how this research is carried out to communicate with the blockchain globally via the main Ethereum network. We should require a global network on a local level for this purpose. Geth is the best way to connect to the global blockchain. However, it is not required to run it as a local process. So, Infula is a quick way to gain access to an Ethereum node via JSON RPC. This is a free and open-source application [45].

The Ethereum Main Network address can also be copied and used to communicate with it. We already have Web3 Js installed. Start your command-line tool or terminal and run the web3 Js commands to communicate with the Ethereum main network via the Infula API [46].

Infula is a hosted Ethereum node cluster that allows your users to run your application without having to install their own Ethereum node or wallet. You may not recognize the name Infula, but if you've used Meta Mask, you have used Infula because it is the Ethereum provider that powers Meta Mask [47].



Feature Tip: Track historical data points of any address with the new analytics module!

Ethereum Blockchain Explorer

Quick links: ERC-20 Tokens ERC-721 Tokens

Search by Address / Txn Hash / Block / Token / Ens

ETHER PRICE
$304.96 @ 0.02506 BTC (+5.39%)

MARKET CAP
$32.534 Billion

LATEST BLOCK
8048573 (13.2s)

DIFFICULTY
2,118.48 TH

TRANSACTIONS
485.10 M (13.8 TPS)

HASH RATE
169,064.77 GH/s

ETHEREUM TRANSACTION HISTORY IN 14 DAYS

Latest Blocks

Bk	8048573 33 secs ago	Miner DwarfPool 1 191 txns in 7 secs	2.16007 Eth
Bk	8048572 40 secs ago	Miner Spark Pool 131 txns in 60 secs	2.21018 Eth
Bk	8048571 1 mins 40 secs ago	Miner Spark Pool 198 txns in 8 secs	2.14646 Eth
Bk	8048570 1 mins 48 secs ago	Miner Spark Pool 172 txns in 18 secs	2.29334 Eth
Bk	8048569 2 mins 6 secs ago	Miner Nanopool 139 txns in 6 secs	2.13139 Eth
Bk	8048568 2 mins 12 secs ago	Miner F2Pool 2 201 txns in 4 secs	2.16316 Eth

Transactions

Tx	0xd06bbecbe4... 33 secs ago	From 0x361399be637103... To 0xb41bcfd4dc701eb...	0.02612 Eth
Tx	0x0545e082bd... 33 secs ago	From 0xfd54078badd5653... To 0xeb8725fffb65fe81...	0.0018 Eth
Tx	0xaf73ea855f8... 33 secs ago	From 0xfd54078badd5653... To 0xe7c90263612964...	0.0018 Eth
Tx	0x0fb74ab401... 33 secs ago	From 0x6386b26aa205c7... To 0x174bfa6600bf90c...	0 Eth
Tx	0xd26aa8a7e1... 33 secs ago	From 0x91ea3b87f6db630... To 0x174bfa6600bf90c...	0 Eth
Tx	0xeb7b257ae1... 33 secs ago	From 0xfd8f60a6484882e... To 0x2f141ce366a2462...	0 Eth

Figure 7. Scan for Ethereum

If you want to access the Ethereum details, you will need an address, so choose one at random from the Ethereum scan website and pass it to web3 using node commands. It will provide you with many strings as a balance. The web3 'utils' can be used to perform conversions to the amount. The cost of this study is its limitation. The above implementation was of the main Ethereum network, and it displayed data from a main Ethereum network node. One thing to keep in mind is that on the main Ethereum network, we are only permitted to read information, not write it. That is, we cannot carry out the actual transaction because it would be prohibitively expensive. A paid account can be purchased for this purpose to test real-world transactions, but fortunately, this study is not being conducted on bitcoin. As a result, Ethereum can run on both local and global networks [48], [49], [50].

4. Results and Discussion

In this chapter, we combine the findings of our three separate blockchain analyses to create a high-level view of a chain of uniform system blocks. We remove a block of the invented and heavy system that resides on a central server or a concept that can be applied due to a lack of established prototypes.

4.1 Combined Analysis of three Cryptocurrency

The combined analysis of three coins yielded the result shown in table 4.1, which shows the analysis of bitcoin, Litecoin, and Ethereum. The data snapshot is used as secondary data and serves as a reference.

Table 1. Combined Analysis

Data Snapshot **2021-07-08** **Criterium**	**Metric [Unit]**	**Bitcoin**	**Litecoin**	**Ethereum**
Supporting Community	**Reddit Subscribers [#]**	255,744	39,602	**85,636**
Development Support	**Activity in Public Source Code Repos [#]**	14,090	1,484	**5,671**
Longevity	**Age since Initial Release Date [Years]**	8.5 (01-2009)	6 (10-2011)	**2** **(07-2015)**
Network Activity	**Transactions [# per Day]**	212,140	17,300	**248,060**
Investor Evaluation	**Market cap of native currency [Bn$]**	42	2.5	**25**
Public Awareness and Interest	**Alexa Rank [-]**	6,880	62,478	**7,156**
Technical Uniqueness of Protocol	**Ordered Attribute Scale [1.5]**	5 Very High (First Mover)	2 Low (Bitcoin Clone)	**4** **High (Parts of Bitcoin)**
Application Ecosystem	**Ordered Attribute Scale [1.5]**	**5** **Very Many**	**3** **Middle**	**4** **Many**

Considering all the data, we see the predominance of Bitcoin in most of the criteria with an advantage. However, when we look at the derivatives in terms of useful life, Ethereum has the steepest slope. The gap between all other blockchain systems is getting closer to closing. Litecoin is a prosperous system, and it is worthwhile to investigate the phenomenon. However, because both protocols are descendants of Bitcoin and thus technically related, they are ineligible for our IT analysis. At the protocol level, Hyperledger Fabric appears innovative and promising, but due to its young age and lack of awareness, it is too stunted to be labeled. We would not consider Litecoin if we did not have widespread public awareness and increased network activity. Litecoin, on the other hand, has a completely different code base than the other systems. To obtain the most reasonable and insightful analysis, we decided to conduct our research on Bitcoin, Ethereum, and Ripple, emphasizing how and why Ethereum and Litecoin differ from Bitcoin.

It was discovered that the most valuable currency is Ethereum. Second, it has been determined that bitcoin can only be used for digital money transfers. There are no data storage features. If we achieve the storage feature, it will be expensive because bitcoin is currently too expensive. Furthermore, bitcoin can only be used on the main network for testing purposes, and it is also expensive.

4.2 Attack Vectors and Implications

The Bitcoin blockchain system, like any other computer system, is vulnerable to attacks from dishonest or spamming nodes. We juxtapose Bitcoin's covered features with their addressing issues to shed light on what types of attacks are critical to the payment system.

Table 2. Bitcoin Features

Bitcoin Feature	Addressed Issues
All data is purely public	-Eavesdropping (4)
All blockchain data gets fully validated and replicated on every persisting node	-Persistent data modification (1) -Sybil attacks (3)
Unstructured peer-to-peer network with semi-random and semi-permanent connections and relays	-Encapsulation of a subset of nodes (2) -Denial-of-Service attacks -Man-in-the-Middle attacks -Packet sniffing attacks (4) -Sybil attacks (3)
Pseudo-anonymous addresses are based on a digital signature scheme	-Identity spoofing (4) -Unauthorized-access attacks, like password-based (4) -Manipulation of personal data
Local IP reputation and timeout system	-General network spamming
Transaction costs	-Clogging with valid transactions

Apart from the fact that Bitcoin is dealing with most of the issues mentioned, we need to pay closer attention to four non-trivial and possible threads annotated in the table:

1) Persistent information is legitimate squares containing substantial exchanges that have been embedded into the principal chain. The actual square can't be changed legitimately. However, the fundamental chain can be overwhelmed by some other chain competing to become the principal one. This race assault is unavoidable on the off chance that one assailant controls the greater part of the organization's hashing power, yet it turns out to be dramatically doubtful with more seasoned squares. There is no assurance of information consistency, yet the likelihood develops with time, rapidly moving toward the 100% consistency limit.

2) Apostolici, Zohar, and Facade, 2017 have brought up that, since they control traffic interfaces, enormous ISPs could adequately separate disjointed pieces of the bitcoin network with steering assaults. This, be that as it may, would just briefly affect hubs because there are various alternative ways for a hub to acknowledge it is done continuously and in the principal chain. For instance, they believed public elements could be gotten to through HTTP and utilized as square travelers. Moreover, ISPs could imperceptibly defer information proliferation by a limit of the Bitcoin association break limit.
3) The evidence of work successfully forestalls Sybil's mining assaults and, therefore, her emblematic impact at the framework level. Be that as it may, if an assaulted hub or set of hubs isn't associated with an ordinary hub, postponing, and diverting associations are hypothetically conceivable.
4) A framework can't forestall all security-related assaults that are normal on PC organizations. A few hubs' characters can be uncovered considering assaults. Be that as it may, if the hidden computerized signature conspire is numerically functional, the whole exchange framework is unaffected.

4.3 IPFS Bandwidth Analysis

Running an IPFS node currently necessitates the use of significant bandwidth, which may be prohibitively expensive for many users, particularly in developing countries. Excessive bandwidth consumption can harm IPFS's acceptance in many parts of the world. Although there are numerous solutions to this problem, financial incentives can point the way in the right direction. Gaining monetary rewards for hosting content in IPFS can assist in covering the cost of running nodes and encourage adoption.

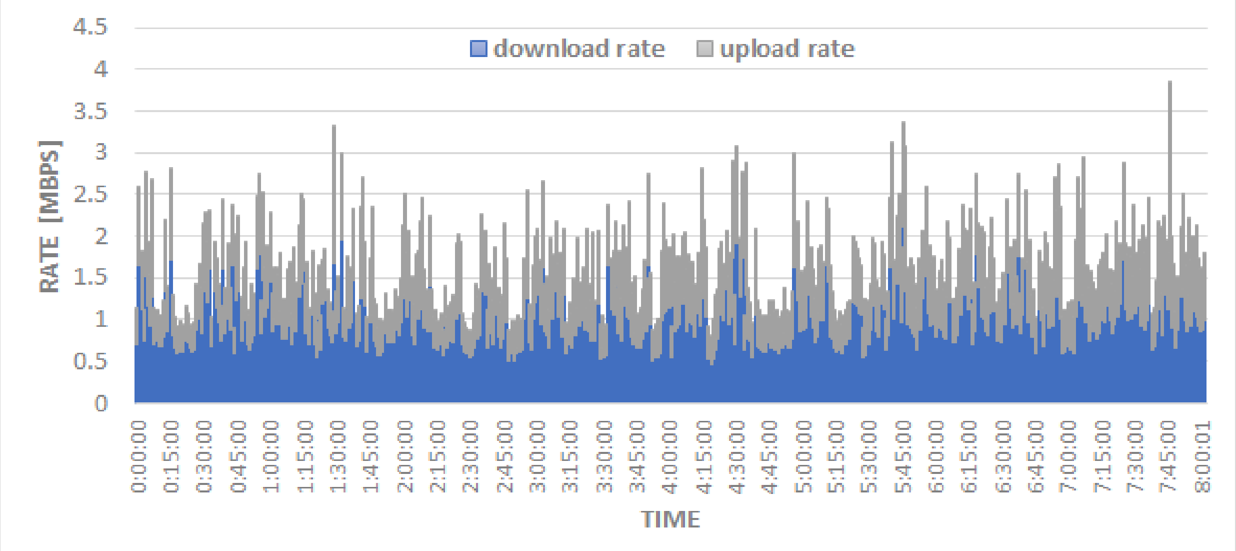


Figure 8. IPFS Bandwidth Analysis

In our experimental, IPFS node's bandwidth usage, the node was not used to browse or download any IPFS content during this test. However, over 8 hours, our node downloaded/uploaded more than 5 GB of data.

4.4 Ethereum Network Hash Rate

Running an IPFS on a decentralized or peer-to-peer network, combining the effects and analysis of current and historical data sets, has a high hash rate, which means the hash produced and deployed on smart contracts has a high rate and is increasing. From July 2015 to July 2019, the graph above illustrates the hash rate results. We are using a secondary dataset rather than a primary dataset, and the results are produced using Google's Data Studio.

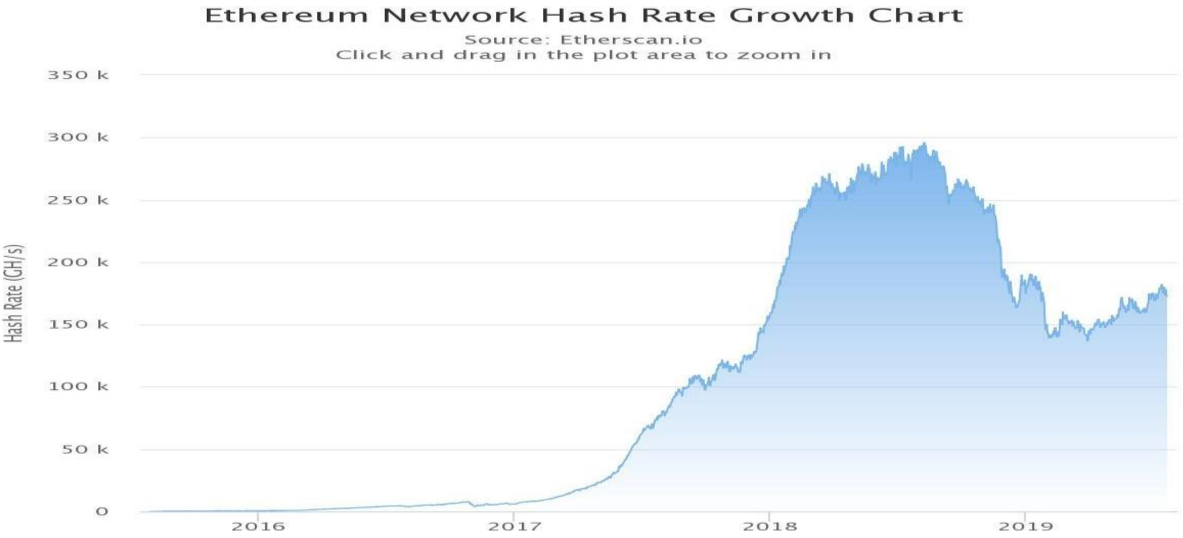


Figure 9. Yearly based Analysis of Ethereum's hash rate

The graph above shows an estimate of how many hashes ETH miners perform per year and how this has changed over time. If we look at the EHT hash rate per day, minute, or second, we can see how it compares to other cryptocurrencies. The only reason for this is the cost of writing your smart contract code. As it takes the hash of the file storage generated by IPFS, Ethereum can be used to form the blockchain and deploy smart contracts on the network

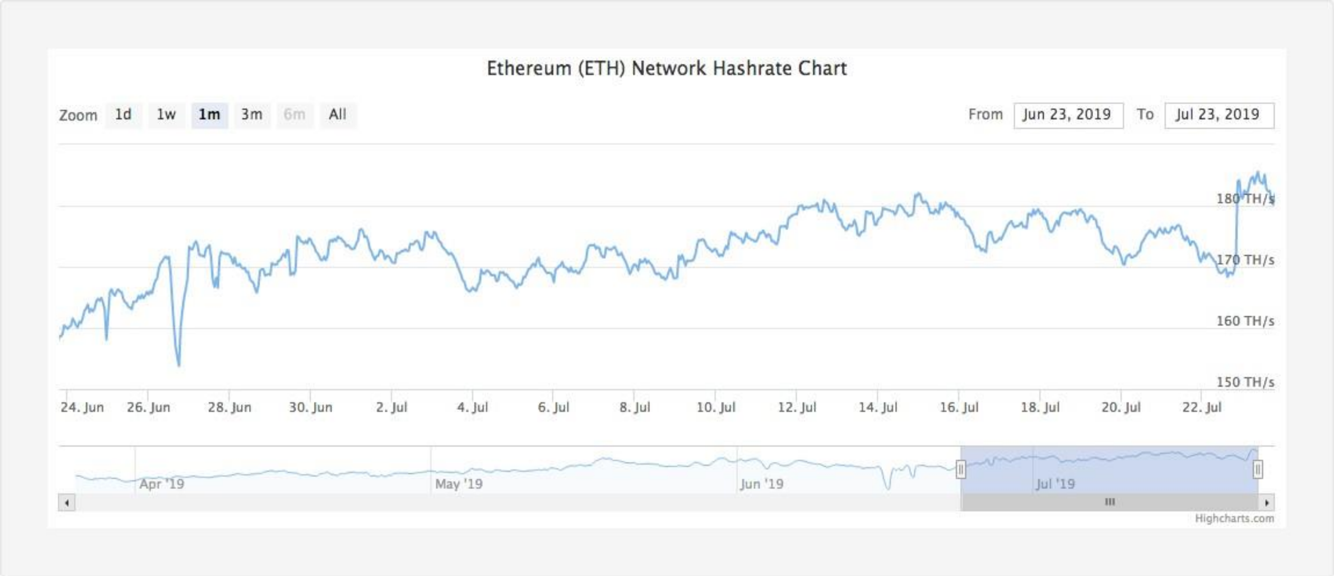
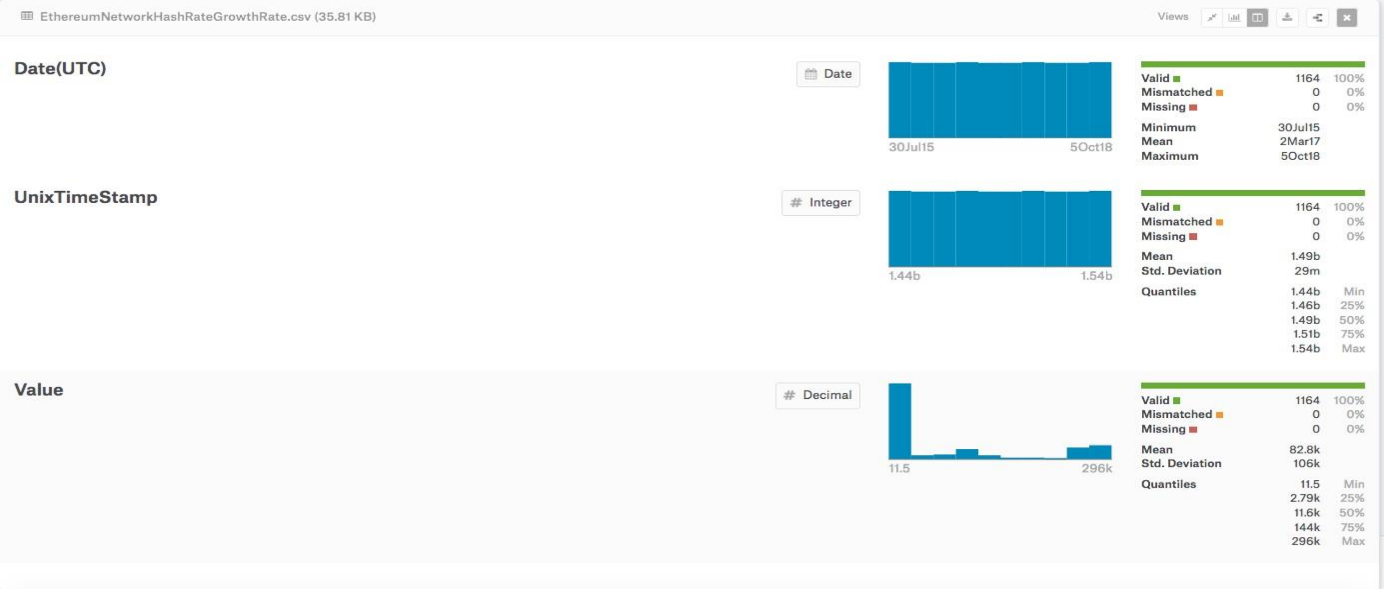


Figure 10. Analysis of the ETH hash rate per minute

The above diagram shows the clear growth rate of the hash rate of ETH, like how the USD dollar rate is increasing internationally, and how its value is increasing based on code generation and code deployment using smart contracts. The reason for this is that smart contracts for bitcoin currency are difficult and expensive to write. As a result, ETH is bridging the price gap between bitcoin and ETH.

The above analysis and experiment were performed on secondary data, and the results are publicly available on etherscan.io, which updates at a per second rate. Moving on to another secondary dataset downloaded in CSV format from the Kaggle website. The dataset is simple to download and run the test.



EthereumNetworkHashRateGrowthRate.csv (35.81 KB)

```
Date(UTC)        Date      Valid         1164  100%
                           Mismatched       0    0%
                           Missing          0    0%
                           Minimum    30Jul15
                           Mean        2Mar17
                           Maximum     5Oct18

UnixTimeStamp    Integer   Valid         1164  100%
                           Mismatched       0    0%
                           Missing          0    0%
                           Mean         1.49b
                           Std. Deviation 29m
                           Quantiles    1.44b  Min
                                        1.46b  25%
                                        1.49b  50%
                                        1.51b  75%
                                        1.54b  Max

Value            Decimal   Valid         1164  100%
                           Mismatched       0    0%
                           Missing          0    0%
                           Mean         82.8k
                           Std. Deviation 106k
                           Quantiles     11.5  Min
                                        2.79k  25%
                                        11.6k  50%
                                         144k  75%
                                         296k  Max
```

Figure 11. Hash rate Analysis of ETH using Data Studio

The graph above depicts the hash rate results from July 2015 to July 2019. The graph above depicts the high hash rate produced by the ETH blockchain. The reason for this is that all nodes can be tested by the test network, allowing everyone to evaluate the ETH blockchain and create their blockchain technology with any cryptocurrency name. The results are obtained from the Kaggle website, which provides us with the actual and real dataset. Because we are using a secondary dataset rather than a primary dataset, the results are obtained using Data Studio, a Google product.

5. Conclusion

The educational industry is facing several challenges. Most of them are concerned with data transfer and security. This paper discusses the advantages and disadvantages of using trending technologies such as blockchain and IPFS to solve the secure digital transactional problem in the education sector. The technologies mentioned above are closely related to IoT. The IoT ecosystem has encountered data security and privacy issues. Blockchain, a type of distributed ledger technology, has received a lot of attention recently in areas other than cryptocurrency. That's what you call blockchain and IoT (Internet of Things), blockchain and security, blockchain and finance, and blockchain and logistics. It is necessary to ensure secure data storage. Blockchain, in conjunction with IPFS, can undoubtedly meet such demands in the educational industry. The main benefit is decentralized data storage while ensuring the credibility and immutability of stored data, removing the need for a middleman. As a result, these technologies have the potential to be a valuable supplement to education.

The IPFS network, a Blockchain-based peer-to-peer hypermedia protocol, officially launches its file storage network on Ethereum rather than Bitcoin and explains it to the Ethereum network development community, as well as several innovative features. As a result, this research paper provides a proper demonstration of data storage without the use of a centralized system. On a decentralized and distributed P2P network, data can always be present. IPFS greatly aids in the segmentation of data for storage purposes. It can be deployed on the network using smart contracts using the hashing technique. The relevant characteristics of these technologies that can improve the possibilities over existing solutions provide answers to the education sector's various challenges. The answers are primarily concerned with the amount of data sent and the reduction of waiting time, as well as ensuring the transparency, security, and credibility of processes and services in the education sector.

References

[1] S. Vellinga, G. K. L. Kumar, and P. Karthikeyan, "Unsupervised Blockchain for Safeguarding Confidential Information in Vehicle Assets Transfer," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, Mar. 2020, pp. 44–49. doe: 10.1109/ICACCS48705.2020.9074285.

[2] M. InSite and K. R. Lakhani, "The Truth About Blockchain," p. 12.

[3] J. P. Mohanty and K. K. Mahapatra, "Security Vulnerabilities in Applying Decentralized Ledger Systems for Obfuscating Hardware's," in *2019 IEEE International Symposium on Smart Electronic Systems (issues) (Formerly ins)*, Rourkela, India, Dec. 2019, pp. 272–275. doe: 10.1109/iSES47678.2019.00067.

[4] M. Bucolic, "Rethinking Permissioned Blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies, and Contracts*, Abu Dhabi United Arab Emirates, Apr. 2017, pp. 3–7. doe: 10.1145/3055518.3055526.

[5] J. Goel, N. Bhatt, and D. N. Kumar, "Raspberry Pi Home Automation System Using Mobile App to Control Devices," vol. 6, no. 5, p. 8, 2007.

[6] K. C. Swain, S. J. Thomson, and H. P. W. Jayasuriya, "Adoption of an Unmanned Helicopter for Low-Altitude Remote Sensing to Estimate Yield and Total Biomass of a Rice Crop," *Transactions of the ASABE*, vol. 53, no. 1, pp. 21–27, 2010, doe: 10.13031/2013.29493.

[7] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," *arXiv:1805.11390 [cs]*, May 2018, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1805.11390

[8] A. M. Antonopoulos, *Mastering Bitcoin*, First edition. Sebastopol CA: O'Reilly, 2015.

[9] I. Modal and E. G. Serer, "Majority is not Enough: Bitcoin Mining is Vulnerable," *arXiv:1311.0243 [cs]*, Nov. 2013, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1311.0243

[10] E. Andreoulakis *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth Neurosis Conference*, Porto Portugal, Apr. 2018, pp. 1–15. doe: 10.1145/3190508.3190538.

[11] B. Rao, A. G. Gopi, and R. Maine, "The societal impact of commercial drones," *Technology in Society*, vol. 45, pp. 83–90, May 2016, doe: 10.1016/j.techsoc.2016.02.009.

[12] D. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," P. 34.

[13] G. Ziskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA, May 2015, pp. 180–184. doe: 10.1109/SPW.2015.27.

[14] A. Nisha, S. Richards, D. Breen, J. Robertson, and B. Breen, "Thermal infrared imaging of geothermal environments and by an unmanned aerial vehicle (UAV): A case study of the Wairakei – Tauhara geothermal field, Taupo, New Zealand," *Renewable Energy*, vol. 86, pp. 1256–1264, Feb. 2016, doe: 10.1016/j.renene.2015.09.042.

[15] G. Ziskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA, May 2015, pp. 180–184. doe: 10.1109/SPW.2015.27.

[16] M. Swan, *Blockchain: a blueprint for a new economy*, First edition. Beijing: Sebastopol, CA: O'Reilly, 2015.

[17] I. Braid, "Spatial variability of surface properties and estimation of surface fluxes of a savannah," *Agricultural and Forest Meteorology*, vol. 89, no. 1, pp. 15–44, Jan. 1998, doe: 10.1016/S0168-1923(97)00061-0.

[18] K. Christakis, "Blockchain-Based Local Energy Markets," p. 190.

[19] M. Crosby, "Blockchain Technology: Beyond Bitcoin," no. 2, p. 16, 2016.

[20] F. A. Vega, F. C. Ramírez, M. P. Sais, and F. O. Rosa, "Multi-temporal imaging using an unmanned aerial vehicle for monitoring a sunflower crop," *Biosystems Engineering*, vol. 132, pp. 19–27, Apr. 2015, doe: 10.1016/j.biosystemseng.2015.01.008.

[21] E. R. Hunt *et al.*, "REMOTE SENSING OF CROP LEAF AREA INDEX USING UNMANNED AIRBORNE VEHICLES," p. 9, 2008.

[22] A. Dori, S. S. Kan here, R. Jurak, and P. Gaur avaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (Precoma Workshops)*, Kona, HI, Mar. 2017, pp. 618–623. doe: 10.1109/Percomw.2017.7917634.

[23] E. Honhaar *et al.*, "Processing and Assessment of Spectrometric, Stereoscopic Imagery Collected Using a Lightweight UAV Spectral Camera for Precision Agriculture," *Remote Sensing*, vol. 5, no. 10, pp. 5006–5039, Oct. 2013, doe: 10.3390/rs5105006.

[24] K. Flynn and S. Chopra, "Remote Sensing of Submerged Aquatic Vegetation in a Shallow Non-Turbid River Using an Unmanned Aerial Vehicle," *Remote Sensing*, vol. 6, no. 12, pp. 12815–12836, Dec. 2014, doe: 10.3390/rs61212815.

[25] C. Caching and M. Bucolic, "Blockchain Consensus Protocols in the Wild," *arXiv:1707.01873 [cs]*, Jul. 2017, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1707.01873

[26] H. Wang, Z. Zheng, S. Xia, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a

survey," *IJWGS*, vol. 14, no. 4, p. 352, 2018, doe: 10.1504/IJWGS.2018.10016848.

[27] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 9.

[28] C. Caching, "Architecture of the Hyperledger Blockchain Fabric," p. 4.

[29] Z. Zheng, S. Xia, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (Bigdata Congress)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564. doe: 10.1109/BigDataCongress.2017.85.

[30] V. Varsha and R. Singh Chiller, "Data Hiding using Advanced LSB with RSA Algorithm," *IJCA*, vol. 122, no. 4, pp. 41–45, Jul. 2015, doe: 10.5120/21691-4796.

[31] V. S, "An Enhanced Multimedia Video Surveillance Security Using Wavelet Encryption Framework," *JMM*, May 2020, doe: 10.13052/jmm1550-4646.1534.

[32] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems," *arXiv:1802.06993 [cs]*, Nov. 2020, Accessed: Oct. 16, 2021. [Online]. Available: http://arxiv.org/abs/1802.06993

[33] I.-C. Lin and T.-C. Liao, "A Survey of Blockchain Security Issues and Challenges," p. 7.

[34] V. Butlerin, "A Next-Generation Smart Contract & Decentralized Application Platform," P. 36.

[35] J. Sharma and R. Thapa, "Hybrid approach for data security using RSA and LSB Algorithm," p. 6.

[36] X. X. Zheng, L. R. Li, and Y. J. Shao, "A GSM-Based Remote Temperature and Humidity Monitoring System for Granary," *MATEC Web of Conferences*, vol. 44, p. 01060, 2016, doe: 10.1051/metacone/20164401060.

[37] A. Jaiswal, S. Chandel, A. Mazumdar, M. G.M., C. Modi, and C. Jayanthi, "A Conceptual Framework for Trustworthy and Incentivized Trading of Food Grains using Distributed Ledger and Smart Contracts," in *2019 IEEE 16th India Council International Conference (INDICON)*, Rajkot, India, Dec. 2019, pp. 1–4. doe: 10.1109/INDICON47234.2019.9030290.

[38] M. Rises and K. Sopher, "A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There," *Bus Inf Sits Eng.*, vol. 59, no. 6, pp. 385–409, Dec. 2017, doe: 10.1007/s12599-017-0506-0.

[39] A. M. Khaleghi *et al.*, "A DDDAMS-based planning and control framework for surveillance and crowd control via UAVs and UGVs," *Expert Systems with Applications*, vol. 40, no. 18, pp. 7168–7183, Dec. 2013, doe: 10.1016/j.eswa.2013.07.039.

[40] A. Mathews and J. Jensen, "Visualizing and Quantifying Vineyard Canopy LAI Using an Unmanned Aerial Vehicle (UAV) Collected High-Density Structure from Motion Point Cloud," *Remote Sensing*, vol. 5, no. 5, pp. 2164–2183, May 2013, doe: 10.3390/rs5052164.

[41] J. Leakey, *Evaluating computer-assisted language learning: an integrated approach to effectiveness research in CALL*. Oxford; New York: Peter Lang, 2011.

[42] M. Govender, K. Chetty, and H. Bullock, "A review of hyperspectral remote sensing and its application in vegetation and water resource studies," *WSA*, vol. 33, no. 2, Dec. 2009, doe: 10.4314/was. v33i2.49049.

[43] J. T. Luxhøj, "A Sociotechnical Model for Analysing Safety Risk of Unmanned Aircraft Systems (UAS): An Application to Precision Agriculture," *Procedia Manufacturing*, vol. 3, pp. 928–935, 2015, doe: 10.1016/j.promfg.2015.07.140.

[44] C. G. Sorensen *et al.*, "A user-centric approach for information modelling in arable farming," *Computers and Electronics in Agriculture*, vol. 73, no. 1, pp. 44–55, Jul. 2010, doe: 10.1016/j.compag.2010.04.003.

[45] J. Gago *et al.*, "UAVs challenge to assess water stress for sustainable agriculture," *Agricultural Water Management*, vol. 153, pp. 9–19, May 2015, doe: 10.1016/j.agwat.2015.01.020.

[46] S. Gethin, R. Nuke, and K. Wiegand, "Using Unmanned Aerial Vehicles (UAV) to Quantify Spatial Gap Patterns in Forests," *Remote Sensing*, vol. 6, no. 8, pp. 6988–7004, Jul. 2014, doe: 10.3390/rs6086988.

[47] Q. Feng, J. Liu, and J. Gong, "UAV Remote Sensing for Urban Vegetation Mapping Using Random Forest and Texture Analysis," *Remote Sensing*, vol. 7, no. 1, pp. 1074–1094, Jan. 2015, doe: 10.3390/rs70101074.

[48] M. Elaraby, A. M. Clavicle, A. F. Torres-Rau, I. MassLive, and M. McKee, "Estimating chlorophyll with thermal and broadband multispectral high-resolution imagery from an unmanned aerial system using relevance vector machines for precision agriculture," *International Journal of Applied Earth Observation and Geoinformation*, vol. 43, pp. 32–42, Dec. 2015, doe: 10.1016/j.jag.2015.03.017.

[49] S. R. Hurwitz *et al.*, "Coffee Field Ripeness Detection Using High-Resolution Imaging Systems on a Solar-Powered UAV," p. 3.

[50] M. Radames and M. Kumar, "Flight formation of UAVs in presence of moving obstacles using fast-dynamic mixed-integer linear programming," *Aerospace Science and Technology*, vol. 50, pp. 149–160, Mar. 2016, doe: 10.1016/j.ast.2015.12.021.