



Ecommerce app with blockchain

Muhammad Abdullah

BSc (Hons) in
Applied Computing
2022/2023

Ecommerce app with blockchain

This is the Subtitle of my Thesis

Author: Muhammad Abdullah

Supervised by: Kevin Meehan & Mandy Douglas

A thesis submitted in partial fulfilment of the
requirements for “Research in Computing with
Emerging Technologies” and “Project Development”

BSc (Hons) in Computing in Applied Computing

Submitted to Atlantic Technological University

Arna chur isteach chuig Ollscoil Teicneolaíochta an Atlantaigh

May 2023

1 Declaration

I hereby certify that the material, which I now submit for assessment on the programmes of study leading to the award of Bachelor of Applied Computing in 2023, is entirely my own work and has not been taken from the work of others except to the extent that such work has been cited and acknowledged within the text of my own work. No portion of the work contained in this thesis has been submitted in support of an application for another degree or qualification to this or any other institution. I understand that it is my responsibility to ensure that I have adhered to ATU's rules and regulations.

I hereby certify that the material on which I have relied on for the purpose of my assessment is not deemed as personal data under the GDPR Regulations. Personal data is any data from living people that can be identified. Any personal data used for the purpose of my assessment has been pseudonymised and the data set and identifiers are not held by ATU. Alternatively, personal data has been anonymised in line with the Data Protection Commissioners Guidelines on Anonymisation.

I consent that my work will be held for the purposes of education assistance to future students and will be shared on the ATU Donegal (Computing) website (www.lyitcomputing.com) and Research THEA website (<https://research.thea.ie/>). I understand that documents once uploaded onto the website can be viewed throughout the world and not just in the Ireland. Consent can be withdrawn for the publishing of material online by emailing Thomas Dowling; Head of Department at thomas.dowling@atu.ie to remove items from the ATU Donegal Computing website and by email emailing Denise McCaul; Systems Librarian at denise.mccaul@atu.ie to remove items from the Research THEA website. Material will continue to appear in printed formats once published and as websites are public medium, ATU cannot guarantee that the material has not been saved or downloaded.

Signature of Candidate

Date

2 Acknowledgements

I would like to thank all my lecturers, classmates and anyone who helped me in any way.

3 Abstract

Blockchain technology has many benefits over real life work. Blockchain is currently facilitating different areas of the modern Information Technology business and adapting very fast in all over the giant companies that can afford to spend money on research and development on technologies, but a problem of energy consumption or cost break all its records just of process an mathematical algorithm for creating a block and all the miners on the network, and the scalability while decreasing energy consumption and electricity cost. The paper presents a decentralized application aiming to reduce these drawbacks energy consumption and cost by proof-of-stake using Ethereum blockchain .

4 Acronyms

Acronym	Definition	page
PoA/POA	Proof-of-Authority	13
PoW/POW	Proof-of-Work	13
POS/PoS	Proof-of-Stake	13
IPFS	Interplanetary File System	25
DPL	Distributed Public Ledger	12
D-Dos	Distributed service denial	17
SSL	Secure sockets layer certificates	17
SQL	Structure Query Language	17
POC/PoC	Proof of capacity	20
DPOS/DPoS	Delegated Proof of stake	21
SC	Smart Contract	22
EVM	Ethereum Virtual MACHINE	22
DApp	Decentralized Application	25
DHT	Distributed Hash Table	26
CID	Content Identifier	26
MDAG	Merkle Direct Acyclic graph	27
TPS	transaction processing system	28
GUI	Graphical User Interface	36

5 Table of Contents

Declaration.....	Error! Bookmark not defined.
Acknowledgements.....	4
Abstract.....	5
Acronyms	6
Table of Contents.....	7
Table of Figures.....	Error! Bookmark not defined.
Table of Tables	Error! Bookmark not defined.
Table of Code Listings	Error! Bookmark not defined.
1. Introduction	Error! Bookmark not defined.
1.1. Purpose	Error! Bookmark not defined.
1.2. Background	Error! Bookmark not defined.
1.3. Aim & Objective	15
1.3.1. Aim	Error! Bookmark not defined.
1.3.2. Objective	Error! Bookmark not defined.
1.3. Research Question	Error! Bookmark not defined.
1.4. Outline.....	Error! Bookmark not defined.
2. Literature Review	Error! Bookmark not defined.
2.1. Introduction	Error! Bookmark not defined.
2.2. Ecommerce	Error! Bookmark not defined.
2.3. BlockChain.....	Error! Bookmark not defined.
2.4. Security of Blockchain	Error! Bookmark not defined.
2.5. Proof of Work	20
2.5.1. Energy Consumption.....	Error! Bookmark not defined.
2.6. Proof Of Stake	Error! Bookmark not defined.
2.7. Ethereum Blockchain and IPFS.....	Error! Bookmark not defined.
2.7.1. Ethereum Blockchain	Error! Bookmark not defined.
2.7.1.1 Ethereum	Error! Bookmark not defined.
2.7.1.2 Ethereum Virtual Machine	Error! Bookmark not defined.
2.7.1.3 Smart Contracts	Error! Bookmark not defined.
2.7.1.4 Ethereum Blockchain & PoS	Error! Bookmark not defined.

2.7.2.	Interplanetary File System	Error! Bookmark not defined.
2.7.1.1	Decentralized File Storages(DFS)	Error! Bookmark not defined.
2.7.1.2	Distributed Hash Table(DHT)	Error! Bookmark not defined.
2.7.1.3	Content Identifier (CIDs)	Error! Bookmark not defined.
2.7.1.4	Merkle Directed Acyclic Graph(DAG)	Error! Bookmark not defined.
2.8.	Related Work	Error! Bookmark not defined.
2.7.	Conclusion	Error! Bookmark not defined.
3.	Design and Methodology	Error! Bookmark not defined.
3.1.	Introduction	Error! Bookmark not defined.
3.2.	Hardware Requirement	Error! Bookmark not defined.
3.3.	Software Requirement	Error! Bookmark not defined.
3.4.	Functional Requirement	Error! Bookmark not defined.
3.5.	Non Functional Requirement	Error! Bookmark not defined.
3.6.	Use Case Diagrams	Error! Bookmark not defined.
3.7.	Use Case Discription	Error! Bookmark not defined.
3.8.	Storyboards	Error! Bookmark not defined.
3.9.	Proposed flow of System	Error! Bookmark not defined.
3.10.	Conclusion	Error! Bookmark not defined.
4.	Testing & Result	Error! Bookmark not defined.
4.1.	Introduction	Error! Bookmark not defined.
4.2.	White Box Testing	Error! Bookmark not defined.
4.3.	Black Box Testing	Error! Bookmark not defined.
4.4.	Testing Strategy	Error! Bookmark not defined.
4.5.	Conclusion	Error! Bookmark not defined.
5.	References	Error! Bookmark not defined.
	Appendices	Error! Bookmark not defined.
	Appendix A: References	Error! Bookmark not defined.
	Appendix B: Code Listing	Error! Bookmark not defined.

6 Table of Figures

FIGURE 1 SIMPLE ILLUSTRATION OF BLOCKCHAIN ().....	ERROR! BOOKMARK NOT DEFINED.
FIGURE 2 PROCESS OF CREATING A BLOCK AND BLOCKCHAIN (WANG, 2021)	ERROR! BOOKMARK NOT DEFINED.
FIGURE 3 OVERVIEW OF ETHEREUM BLOCKCHAIN(PEILIN ET AL. 2020)	ERROR! BOOKMARK NOT DEFINED.
FIGURE 4 ETHEREUM VIRTUAL MACHINE (WANG, 2021)	ERROR! BOOKMARK NOT DEFINED.
FIGURE 5 IPFS NETWORK(MARUTI ET AL. 2022).....	ERROR! BOOKMARK NOT DEFINED.
FIGURE 6 INTERNAL STRUCTURE OF A BLOCK AND BLOCKCHAIN (XIAO ET AL. 2022)	ERROR! BOOKMARK NOT DEFINED.
FIGURE 7 USE CASE DIAGRAM.....	ERROR! BOOKMARK NOT DEFINED.
FIGURE 8 REGISTER PAGE	ERROR! BOOKMARK NOT DEFINED.
FIGURE 9 LOGIN PAGE	ERROR! BOOKMARK NOT DEFINED.
FIGURE 10 DASHBOARD PAGE.....	ERROR! BOOKMARK NOT DEFINED.
FIGURE 11 PRODUCT DETAIL PAGE	ERROR! BOOKMARK NOT DEFINED.
FIGURE 12 BUY PRODUCT WITH METAMASK PAGE	ERROR! BOOKMARK NOT DEFINED.
FIGURE 13 ADMIN DASHBOARD PAGE	ERROR! BOOKMARK NOT DEFINED.
FIGURE 14 FLOW OF PURPOSED SYSTEM.....	ERROR! BOOKMARK NOT DEFINED.

7 Table of Tables

TABLE 1. HARDWARE SPECIFICATION	30
TABLE 2 SOFTWARE SPECIFICATION TABLE.....	ERROR! BOOKMARK NOT DEFINED.
TABLE 3 REGISTER USE CASE	ERROR! BOOKMARK NOT DEFINED.
TABLE 4 LOGIN USE CASE TABLE	ERROR! BOOKMARK NOT DEFINED.
TABLE 5 VIEW PRODUCT USE TABLE	ERROR! BOOKMARK NOT DEFINED.
TABLE 6 CHECKOUT USE TABLE	ERROR! BOOKMARK NOT DEFINED.
TABLE 7 ADMIN USE TABLE	ERROR! BOOKMARK NOT DEFINED.
TABLE 8 LOGOUT USE TABLE	ERROR! BOOKMARK NOT DEFINED.
TABLE 9 TESTING STRATEGY RESULTS TABLE	ERROR! BOOKMARK NOT DEFINED.

8 Table of Code Listings

CODE LISTING 1 MDBEAN MESSAGE HANDLING **ERROR! BOOKMARK NOT DEFINED.**

1. Introduction

Ecommerce is a term used for online shopping where with one click purchase a product and get it delivered but behind is complex and requires many different steps for delivery and payment to work. The value of the worldwide logistics market was USD 4,925.1 billion in 2021, and by 2027, it is anticipated to reach USD 6,551.2 billion (IMARC Group 2021). Blockchain technology was first introduced in 2009 with the invention of bitcoin which is now accepted worldwide. Aside from cryptocurrency, blockchain has become popular increase across industries such as supply chain, banking and health because of its security to organize data (Buquan, 2021).

The traditional business applications all depend on traditional databases to keep the user's data, there is only a single entity, the owner or the administration, that keeps a copy of the database. The database can only be accessed by teams who are involved in the development and software maintenance. But certain security flaws arise when a hacker does phishing or hacking (by a fake email, fake link) attempts on your business application. The hacker finds a loose patch or door to enter into your system and steal your information and this hacker blackmail and demands ransom money in the form of bitcoin (Xiao et al. 2022).

Traditional businesses also have facing online payment problems due to they are dependent on third-party payment channels like banks and wired payments option that process transactions with high fees deductions. Small e-commerce businesses, inadequate trade trust, expensive logistical payment costs, lengthy cycle durations, and alterations brought on by data flow are further issues. These weaknesses can be solved by using blockchain technology (Xiao et al. 2022)

Blockchain is a shared, decentralized, distributed & immutable ledger that helps to secure important data, documents and information by creating a DPL that allows the owners, employers and employees to manage their business properly. This enforces smooth auditing transactions and secure data and information management for finance or technology industries. Secondly, blockchain increased the traceability of the transactions of money from the first person (sender) to the end person (receiver) who receives the money and available for use and same it also helps for products, not only tracking but also the right products dispatch from producers (factories and farmers etc) and the right product reaches

to the customers (Buquan, 2021). This brings up the central principle of trust found in blockchain technology. This theory is founded on the observation that, even when parties engaging within the system may not always know or trust one another but nevertheless have the option to do so in a secure and trustworthy manner (Jiarui et al. 2021).

Satoshi proposed that blockchain is secure, immutable and transparent, that's why bitcoin is successful because bitcoin blockchain uses the consensus mechanism which means Inside of blockchain network, there are nodes (known as miners). These nodes are the backbones of the bitcoin blockchain network. But by creating a block for every new transaction, miners on the blockchain network try to solve a mathematical algorithm, by running their computers day and night, and the one who solves that mathematical algorithm will win the rewards in the form of bitcoin. This whole mechanism is known as Proof-of-work(POW) consensus mechanism (Nakamoto, 2008). PoW consensus mechanism is now a decade very famous but it causes energy consumption and cost issues. Other consensus mechanisms developed like Proof-of-stake(POS) and Proof-of-activity(PoA), which improved blockchain technology(Andreas, 2022).

1.1. Purpose

The purpose of this dissertation is to showcase blockchain technology for real-world businesses, and importantly for ecommerce businesses. The motive to use blockchain technology is to improve the data privacy of the users and sellers and also secure the payment transaction system for ecommerce businesses this will give an opportunity to use cryptocurrency as a payment method which will help us to replace the third-party payment gate-ways like fast money, western union, money grams, paypal and online banking channels. This will allow us to purchase goods on ecommerce using ethers, bitcoins, or usdts etc the data protection and security issue are solved by using smart contracts, and we use solidity to write these contracts.

1.2. Background

Ecommerce business model totally evolved In the previous two decades. Small ecommerce businesses become big giant companies whose net worth become hundreds of billions of dollars like Ali baba, Amazon, flipcart, ebay etc. Ecommerce has totally changed peoples

way of life, clothes, education, groceries, offices, medicals, entertainment and other necessities of people's lives can be bind with the e-commerce system (Zheng, 2022).

Zheng (2022) states To better explain ecommerce is a better and fun alternative, you can purchase your all grocery online, you can purchase food online(foodpanda), patients can purchase all their medicines, you can purchase online books and courses for education (udemy), you can watch movies for entertainment (netflix) and other necessities of people's life, and all of other industries are connected to ecommerce to grow their business. Many ecommerce models adopts third party payments systems and online bank payments which overturned the way of shopping and provide easy of purchase goods.

Blockchain technology is an authenticity, unforgeability, traceability, and distributed immutable ledge consisting of an encryption algorithm, consensus mechanism and smart contract. Blockchain ensures people trade without any trust factor due to its immutability (Saber et al. 2018).

The main problem with the bitcoin blockchain is bitcoin mining, which uses a huge amount of energy, and the miners who added new blocks of transactions onto the bitcoin network. Permission-less blockchain defines as any individual can join this blockchain network from any part of world such as bitcoin depend on Proof of Work (PoW) consensus mechanism in the mining process (Nakamoto, 2008)

Bogna (2022) explains that Bitcoin stands on the pillars of consensus mechanism which is known as proof of work (PoW) system, which lives on miners having to solve mathematical algorithm and add new blocks to the blockchain. The miner with the biggest computational processing power has the highest chance of winning. This means that miners on the bitcoin blockchain network compete to be the first to solve these puzzles and earn the financial prize. A typical US family could be powered for more than 78 days by the 2,292.5 kilowatt hours used in transactions on the bitcoin blockchain network. Vlachos's (2022) article discusses other consensus mechanisms have been developed which are more environment friendly than POW.

Cachin (2016) explained that Proof of Stake (PoS) or Proof of Authority (PoA) consensus mechanisms are used by permissioned blockchains like Ethereum and Hyperledger Fabric

that depend on private networks. In this PoS based blockchain network, all the nodes are represented as validators, they invest their own stake to get the chance to create a block, so the higher you stake higher your chances. Xiao (2022) states that in contrast to PoW, PoS does not require as much computer power. The Decentralized E-Commerce Transaction System Based on blockchain.

1.3. Aims & Objective

1.3.1. Aims

This dissertation aims to propose solving/minimising privacy and security problems within Ecommerce while using Ethereum blockchain which shifted into Proof-of-stake consensus mechanism system which is more energy and cost-efficient than proof-of-work, and this paper proposes an e-commerce decentralized platform that works Ethereum blockchain and data store in IPFS storage . The safely storing of user data in IPFS and allow purchasing good with cryptocurrencies using matamask.

1.3.2. Objectives

- Research & investigate ecommerce security/transparency while using blockchain.
- Research Proof of stake consensus based Ethereum blockchain
- Examine what solutions for minimising privacy and security problems the discussed technology can offer to Ecommerce platform.
- Construct a Ethereum blockchain.
- Develop code that will allow purchasing good with cryptocurrencies using matamask.
- Create off-chain storage (IPFS) to save all user details, because saving user data on the Ethereum blockchain node's will be very costly and if use traditional centralized database again risk on data security that's why IPFS is best option to use.
- Configure matamask to allow user to purchase online
- Evaluate & analyse the system's functionality & methods of securing data.

1.4. Research Question

Can we use Ethereum blockchain based on PoS consensus mechanisms while providing security, transparency on ecommerce platform and improve transaction system?

1.5. Report Outline

The dissertation from here is divided into 5 main sections. The sections are as follows:

1. Chapter 2 - Literature Review: Extensively covers published information relevant to the project.
2. Chapter 3 – Design: Details the intended design & research that will go into the development of the project.
3. Chapter 4 – Implementation: Informs the reader how the ideas presented were formulated into a working application, with snippets of code to accompany the text.
4. Chapter 5 – Testing & Results: Demonstrates how the application can be tested effectively and the testing of Functional Requirements. Relevant tests are documented.
5. Chapter 6 – Conclusion: This chapter summarises the overall process of the project along with problems faced and recommendations for future work.

2. Literature Review

2.1. Introduction

A technical breakdown of Proof of work & proof of stake blockchains, and its security and decentralized IPFS and storing data on decentralized IPFS network and will be given in the following chapter. Additionally, it will briefly discuss data handling norms and regulations and their significance in implementing private and secure practices within an organization. The focus of this research is on issues like privacy, integrity, and security of exchanging sensitive data, with strengths and weaknesses of these roles being noted in each technology described. When taken as a whole, this effort will contribute to the creation of a decentralized e-commerce application that aims to provide secure means of storing and sharing user, shop, and payment information.

2.2. Ecommerce

There have been rapid changes in the business modal in the past two decades, and business moving toward a fast way to reach customer with new advanced technologies, which has supported the business models. E-commerce has improved marketing strategies and economic progress for the countries to sell their product globally People are comfortable doing online shopping and browsing products online that will help them make decisions on a suitable product, due to advantages such as convenience, high reach to the product, transparency and high interaction etc (Nikhil et al. 2022).

Nishant (2021) while researching on ecommerce's cyber-security issues with his research team, points out that Alibaba and amazon are the two big e-commerce firms to start off a secure and transparent market. They are the role model for other companies to realize that website is the key to success for customer connection. Business-to-consumers and business-to-business both have the potential for the expansion of internet shopping generally and the development of a safe web-based eCommerce platform. But consumers are facing problems regarding the security of the eCommerce system and their law-making issues.

Companies that doing businesses developing countries like Pakistan, India, Bangladesh, Srilanka failed to acknowledge the usage of e-commerce in their business operations and policy making, but companies of developed countries do. Consumers in developing countries are not using e-commerce frequently. In developing countries, a lot of customers mostly complain while shopping on the eCommerce platform, as they are reluctant to purchase because of trust and the absence of security (Nikhil et al. 2022).

As e-commerce companies transfer their payment systems online, more online attack and breach increases. The eCommerce companies experience many risks related to security such as Forge site(phishing) means hackers make a fake version of original sites to attack that e-commerce and customer's data, credit card fraud happens when cybercriminals robbed the client's data like personal information and credit card information, distributed service denial attacks(D-Dos) prevent users from using e-commerce websites, which hinders their functionality and ultimately results in losses (Jinson, 2022).

In the past various attempts such as Http and SSL certificates (protect data flow between servers and users' devices, protecting the sensitive information of your users. They thereby avoid any interception), Anti-Malware and Anti-Virus softwares are software programs that finds, eliminates, and stops malicious software, viruses from infecting computers, servers and IT systems now operating systems also provide buildin malware and virus scanning tools. Using Secure payment gateway by delegate the management of the payment transactions to a third party, such as PayPal and Stripe, outside of your website rather keep your client's credit card details in your database. Deploying strong firewalls can protect from malicious networks, XSS, SQL injection, and other cyber-attacks. These new security enabling techniques have been made to improve security within ecommerce systems. However, security threats are constantly evolving, and so too are attacks (Jinson, 2022).

2.3. Blockchain

Blockchain is invented in 2009 by Satoshi Nakamoto, a distributed ledger based on peer to peer network of nodes known as miners (Nakamoto, 2008). A peer-to-peer network is the foundation of the blockchain as shown in figure 1, which secures your transaction. In the traditional payment system, we know that we need third-party(banks, paypal, wired payments gateways) involvement to make our payment successful but blockchain naturally a decentralised means transactions are managed by a protected network of node which make its system more secure (Xiang, 2021).

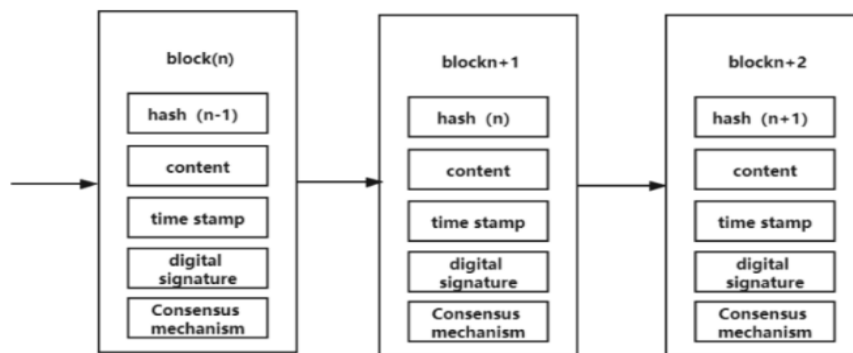


Figure 1 Simple Illustration of Blockchain ()

Source : <https://ieeexplore.ieee.org/document/9824566>

Xiang (2021) explains that due to your transactions are present on the one single place but on the memories of different computers/nodes make it more secure than a centralized database. Block chain's main features that make it unique are a cryptographic hash algorithm and digital signature, which make it provide a private and secure transaction system that becomes the success of bitcoin. Currently, blockchain is thinking all-around of digital currencies, bitcoin, and Ethereum.

Wang (2021) states that we can assume blockchain as a shared and synchronized database, which is managed by a mathematical algorithm, nodes process a mathematical algorithm to create a block for the database and stored on a peer-to-peer network of multiple devices operated nodes (miners), such that each node has a copy of that database as shown in figure 2.

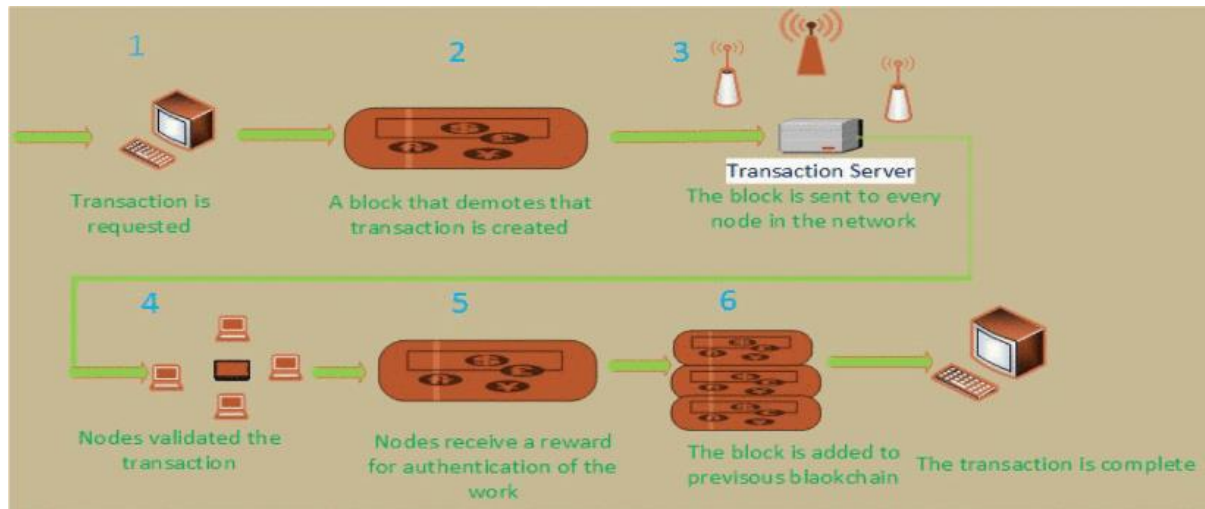


Figure-2 Process of creating a block and blockchain (Wang, 2021)

source:https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/9673706/9673707/9674178/9674178-fig-1-source-large.gif.

Since the database is available on multiple devices, the database will remain unchangeable. Blockchain technology innate consists of a chain of blocks. All the new transactions a node processes by solving a mathematical algorithm, then accumulated them within a block. As the block reaches its maximum size, they hash the block and a fresh block is produced. The block is shared with every node in the network, other node validate it and then block is chained to its ledger, In this regard of creating block and chained it, nodes received their rewards as illustrated in figure 2 above (Wang, 2021).

In addition, Blockchain provides a guarantee of tamper proof and security of the ledger by its consensus protocol for securing the blockchain if it satisfies all the nodes shared the same chain of the ledger and valid data has been added to the ledger's chain (Nguyen et al. 2022)

2.4. Security of Blockchain

Blockchain is distributed ledger technology that contains a series of blocks, every block contains requested transaction data, which is hashed by its own hash value and a parent hash value. Both of these hash value purposes are to keep the block within its chain, The first block of the blockchain is known as a genesis block which is the leader of the blockchain. All the valid transactions blocked in the ledger chain are first approved by nodes. Digital signatures are private secret keys which every node kept private. Every node accept transactions using its secret keys (Muralidhara et al. 2021).

2.3.1 Consensus protocols

Consensus protocols are the agreements signed between the nodes which ensure all nodes validate every new transaction, and share the same transaction data as data on the miner nodes. Bunch of rules significant consensus agreement that all the nodes make a signed declaration that all the new transactions added into the block must be chained to the ledger. Consensus protocols aimed at defending against specific security breaches or harmful threats. These consensus protocols are the foundation of the blockchain and are called consensus mechanisms (Yin et al. 2022).

Proof of Work is one example of a consensus protocols and is the father of all the other consensus mechanisms. Every consensus mechanisms have its own advantages and disadvantages the major aspect in which they can be comparable are fault tolerance, decentralization, resource consumption and performance efficiency, based in all of these Proof of stake lies on the satisfactory side (Kshirsagar et al. 2022). Currently, existing consensus mechanisms mainly are Proof of Work (PoW), Proof of Stake, that we are going to discuss later but there are new consensus mechanisms also discovered like Proof of Elapsed Time, Delegated proof of Stake, Leased Proof of Stake, Practical Byzantine Fault Tolerance, Proof of Activity, Proof of Capacity. All of these consensus mechanisms are stand on some sort of agreements between the nodes to run that blockchain network (Yin et al. 2022). Next we are going to discuss proof of work and proof of stake

2.5. Proof of Work

The consensus algorithm is the backbone of bitcoin blockchain technology that makes possible the security and transparency of the virtual currency. In PoW, all the individual nodes present on the bitcoin blockchain network competing with one another to form a block. The objective of this challenge is to solve a numerical puzzle based on computational hashing for example [DN92, RSW96, Bac97, JB99]. (Garay et al. 2015)

Garay (2015) states this competition is based on “first solve first win” which means the first who cracks the algorithm gets the chance to create the block. The participants who compete in the challenge are the nodes working on the network. In the bitcoin blockchain network, these nodes are called “miners”. This is a competition based on the first solve first win, so the lucky miner who solves that mathematical algorithm.

Consensus mechanisms are categorised into two types permission and permission-less. Proof of work falls into permission-less. This means that any node on the internet can join the bitcoin blockchain and start creating the blocks. To encourage miners to behave honestly and truthfully within the bitcoin blockchain network such as adding valid transactions into the blockchain and all the nodes have duplicate valid transactions, i.e., not deviating from the consensus rules (Basile et al. 2022). Basile (2022) states that the PoW consensus mechanism only awards those miners, that inserts valid transaction (data) and creates the block that becomes part of a valid ledger chain. The purpose of this economic incentive mechanism, miners to follow truthful behavior to keep the chain valid. These economic incentives are static rewards and transaction fees altogether are referred to as block rewards.

2.5.1 Energy Consumption in PoW:

Bitcoin stands on PoW consensus system, that depends on miners having to decode numerical equations and append latest block to the blockchain. So, every miner on the network stand by on their computation hardware and servers full-time, day and night, nonstop working on to processing numerical puzzle and competing to be the first to decode these numerical puzzle and in this regard, to get the monetary reward. The miners with the most powerful computers and servers have the best probability chance of decoding that mathematical puzzle and winning the reward (Bogna, 2022). A series of improved algorithms for PoW to solve the problem of high energy consumption and low efficiency of PoW have been proposed. To tackle the problem of high energy consumption and high cost and low efficiency of solving the mathematical algorithm which actually consumes a large amount of energy. There are series of advanced consensus mechanisms have been proposed such as the PoS consensus mechanism, Delegated Proof of Stake (DPoS) consensus mechanism, Proof of Activity (PoA), and Proof of Capacity (PoC) consensus mechanism, that can solve that problem (Peiliang et al. 2022).

2.6. Proof of Stake

The PoS consensus mechanism is best suited for this purpose. PoS proposes consensus on a single authentic data history record. The nodes in proof of stake are called Validators (Peiliang et al. 2022). They randomly choose valid transactions on the network, and then they encrypt them to create a block. PoS based blockchain network allows validators to choose transactions on which they can easily invest their stake. Validators will receive

compensation for correctly producing blocks and demonstrating the blocks they observe (Ouyang et al. 2021).

Peiliang (2022) states that every new node that wants to join the PoS network makes a validator fee payment initially. It is mandatory to become a validator in the network. When the valid transaction arrives in the PoS network, the validator can then stake some coins as a bit, to compete with other senior validators. PoS network makes a mechanism that every node has responsibility for collecting the transactions they receive from clients. All the validators choose a leader which has staked the maximum amount of coins.

When a sufficient amount of transactions is collected, the elected leader then creates a block and duplicated it to the other validators in the network. Other nodes carry out all of the block's transactions, verify the block, and add it to their ledger's chain. The leader validator receives a special reward transaction for creating the block in the form of transaction fees for the transactions present in the block. The PoS mechanism, by its nature, does not depend on computational power, but rather focuses the stake amount. This means, the greater the stake, maximum your reward (Ouyang et al. 2021).

2.7. Ethereum Blockchain and IPFS

This section is discusses what the technologies are suitable for developing ecommerce application that can improves user data and payment security and transparency.

2.7.1 Ethereum Blockchain

The most important advancement for promoting cryptocurrencies is Blockchain. Blockchain comes in different forms. The Ethereum Blockchain as shown in figure 3, also known as the Ethereum Virtual Machine (EVM), enables a number of unrelated parties to collaborate and carry out tasks underneath digital agreements known as Smart Contracts (SC). Because Ethereum can be programable, you can create applications that use the blockchain to store data or set restrictions on what your application may do. This produces a general purpose blockchain that can be used for anything. The Ethereum network can facilitate considerable innovation because there are no limitations on what Ethereum can accomplish (Peilin et al. 2020).

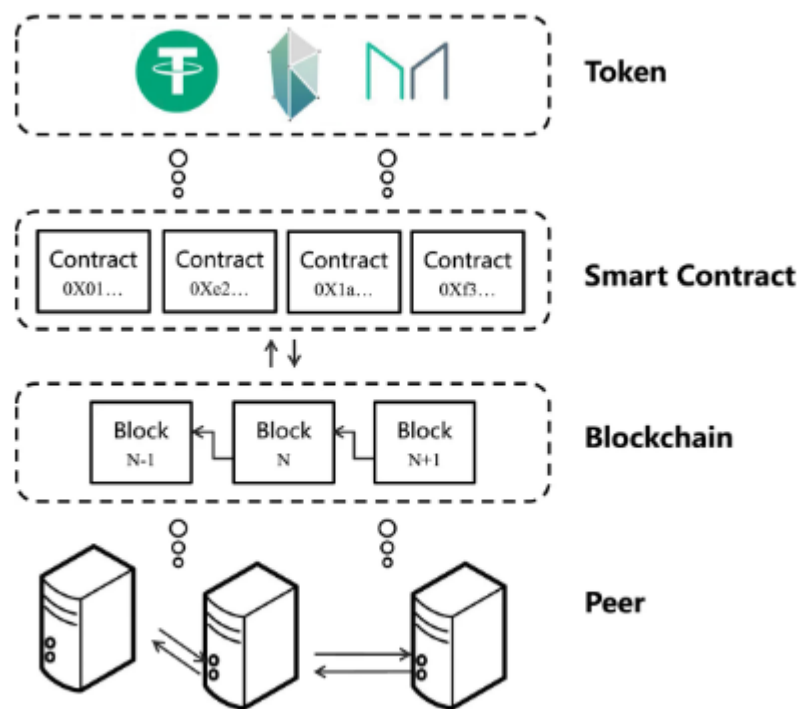


Figure 3 overview of ethereum blockchain (Peilin et al. 2020)

2.7.1.1 Ethereum

Ethereum aims to develop an alternative protocol for creating decentralized applications, with a focus on scenarios where rapid development time, security for small and infrequently used applications and the ability for various applications to interact very efficiently are important. This protocol will offer a distinct compromises that we believe will be very helpful for creating decentralized applications. Ethereum achieves this by creating a blockchain with a built-in Turing-complete programming language that enables anyone to create smart contracts and decentralized applications with their own arbitrary rules for ownership, transaction formats, and state transition functions. This is essentially the ultimate abstract foundational layer. Hardly two lines of smart contract code may create a basic implementation of Namecoin, and fewer than twenty can create various protocols for currencies and reputation systems. With the additional capabilities of Turing-completeness, value-awareness, blockchain awareness, and state, the smart contracts—cryptographic "boxes" that store value and only unlock it when specific conditions are satisfied—can be constructed on top of the platform. These contracts have far more power than those offered by Bitcoin scripting (Yang et al. 2019).

In contrast to Bitcoin, which is merely a payment network, Ethereum is more like a marketplace of financial services, games, social networks, and other apps that respect your privacy and cannot restrict you.

2.7.1.2 *Ethereum Virtual Machine (EVM)*

Ethereum is a platform also known as the Ethereum Virtual Machine (EVM) as shown in storage figure 4, enables a number of unknown parties to collaborate and perform tasks underneath Ethereum blockchain network which uses smart contracts. It makes use of a type of operating system or virtual machine and a distributed network of decentralized systems. The blockchain network that Ethereum offers is represented and encapsulated by the EVM. In this case, contracts are represented as executable bytecodes on the EVM. The EVM provides three benefits. The stack, a container to which values can be added and subtracted (pushed or popped). A method defines the stack values. Second, dynamic memory, also referred to as heap, is a resetting byte array that can be expanded when the programme is complete. The third item is key/value storage for account balances and solidity code for the of contract addresses (Peilin et al. 2020)

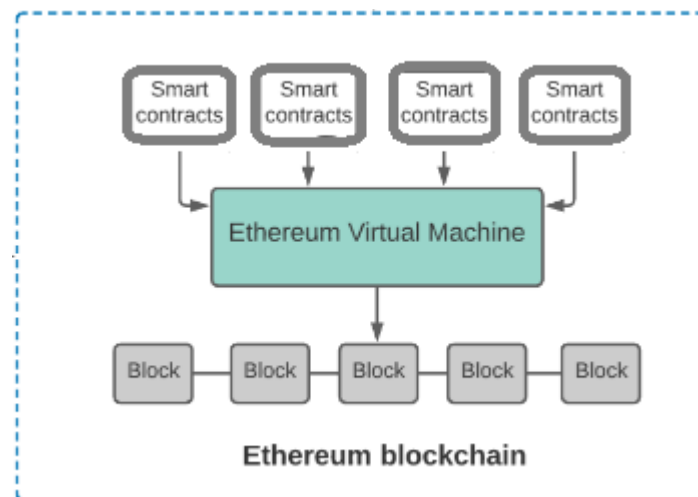


Figure 4 Ethereum virtual machine and smart contracts

On each of the many nodes, the Ethereum client executes the Ethereum Protocol with the express aim of ensuring that the network functions continuously and error-free. The EVM creates the blocks, which are the blockchain's units of bundled transactions. EVM provides the some special functionalities when a client handling it, such as a client can connect to

the Ethereum network, examine the blockchain, initiate new transactions and smart contracts, run smart contracts, and mine for new blocks (Yang et al. 2019).

2.7.1.3 Smart Contracts

A program that runs on the Ethereum Virtual Machine is known as a "Smart Contract". The figure 4 illustrate the smart contracts is a set of functions and state-related data that executed inside EVM, and are stored at a particular address on the Ethereum blockchain. Smart contracts are a particular class of Ethereum account. They can now be the subject of transactions because they have a balance. However, they are not user operated, rather, they are deployed to the network and run according to they are programmed. Then, user accounts can communicate with a smart contract by submitting transactions that implement a smart contract function. Like a standard contract, smart contracts have the ability to establish rules and have the system automatically enforce those rules. Smart contract interactions are irreversible by default and cannot be altered and deleted. Rules are necessary for contracts, but in this instance a programming language called Solidity incorporates the rules into the SC itself. SC is not self-executing since it lacks a "main" method (Fabian et al. 2022).

SC follows determinism. When every node of the Ethereum network performs the SC, this constraint produces the exact identical result. Users can act as nodes, or nodes can act as miners who validate SCs by cracking a mathematical challenge. This validation procedure adheres to the consensus protocol, and the mathematical puzzle should provide the same result on all nodes (Fabian et al. 2022).

2.7.1.4 Ethereum Blockchain & PoS

Ethereum practicing consensus mechanism is now switch from PoW to PoS consensus Algorithm. In contrast to PoW, which uses a lot of computational process and power consumption, PoS suggests a concept of coin age, which is an unspent asset multiplied by the amount of time since the last time it won till the present. This prevents the competition process from using a lot of resources. In PoS, the hashing operation is a key component of the consensus process, and a higher coin age will increase the likelihood that a node will be awarded the authority to create a new block (Keyao et al. 2022).

2.7.2 Interplanetary File System(IPFS)

When we are going to develop blockchain-based applications which are known as decentralized Applications (DApp). The data we are going to save in the blocks should be

needed to save in some sort of database because if we store data in the blockchain network then it will become very costly and if we save data from a DApp into a normal or centralised database such as MySQL, MariaDB etc then data will also not be secured by the hackers(Benet, 2021).

2.7.2.1 Decentralized File Storage

Benet (2021) with his small team of developers seated to introduce a unique type of data storage system as represented in figure 3 below, which is a peer-to-peer-based, decentralised file system similar to BitTorrent, which is known as an Interplanetary File System (IPFS). Leventer (2022) states that IPFS is featured by versioning, meaning all the alterations made in the data are stored in separate, different versions. These features have been added after being inspired by Git.

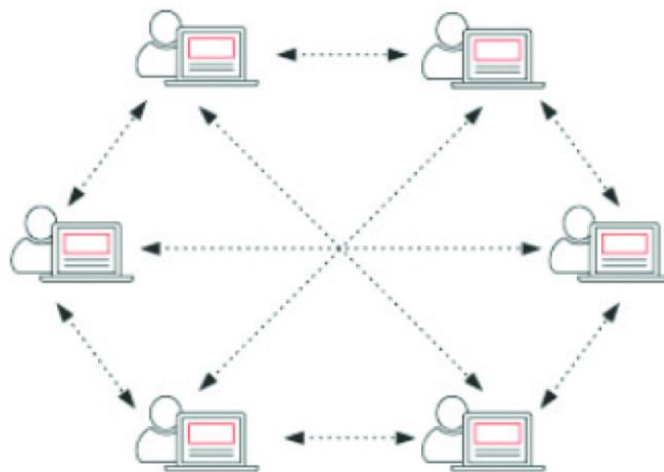


Figure 5 IPFS Network (Maruti et al. 2022)

2.7.2.2 Distributed Hash Tables

Interplanetary File System (IPFS) distributed File storing System. Meaning it save & duplicate data on an IPFS peer-to-peer network. An IPFS file system uses an innovative technology called Distributed Hash Tables (DHT) for file system storage and retrieval. It is similar in nature to the Bit Torrent protocols but opposite in the sense that focuses on file sharing and stores it on a blockchain as **key-value pair**. A file uploaded to IPFS is broken up into 256KB size small packets or data objects and distributed between the nodes or computers across the IPFS network. Each packet of data is hashed and assigned a unique hash identifier (hash ID) known as a content identifier (CID), a technique used to locate a specific file based on its

content not by location. This type of file or content finding technique is known as content-based addressing (Henningesen et al. 2020).

2.7.2.3 Content Identifier

Content identifier Abbreviated as CID the unique hash identifier (hash ID). Every data uploaded on the IPFS is split into 256 KB-sized small packets and This CID is assigned Each packet of data is hashed. This technique is used to locate a specific file based on its content not by location (Shen et al. 2019). The CIDs of these packets do a join process to create a Base CID type content identifier of that file. Distributed Hash Tables (DHT) indicate where the content is stored on the system and then check what the content user is looking for from the IPFS network. In the IPFS network, content is split among all the nodes, storing details like CIDs and the corresponding content (Benet, 2021).

2.7.2.4 Merkle Directed Acyclic Graph(DAG)

Merkle Directed Acyclic Graph (DAG) is a top layer of IPFS, it's a directed acyclic graph which is similar to the Merkle tree. Merkle DAGs provide Content Addressing, Tamper resistance and Deduplication features which are useful properties of IPSF structure (Sanjuan et al. 2020). Firstly, the content-based addressing that IPFS offers is based on the Merkle Directed Acyclic Graphs (DAG). A Merkle DAG stores content identifiers (CIDs) of infinite files and folders in the node's computers/servers in the following form of branching, which merges a large amount of data together with the root node (base CID). This is a generalization of the Git data structure. Secondly, This structure makes IPFS Tamper proof and immutable in nature. Meaning all content is verified with its check system, and if any updates in a subsequent file, will be surely visible in the above hashes branches of that node (Yongle et al. 2018). Third benefit is, No duplication of the same content. Meaning all packets having similar content are equal or one, and only stored once. This is particularly achieved with the indexing of these packets, such as git trees and commits, or common portions of data (Sanjuan et al. 2020).

2.8. Related Work

The related work concerned of how blockchain can be use for different purposes for solving ecommerce security issues and different types of security breaches happened and how they can be solved. This section discuss what already been done in attempting to improve security, Blockchain is distributed ledger technology that contains a series of blocks, as

shown in the figure 6. every block holds transaction data, which is hashed by its own hash value and a parent hash value.

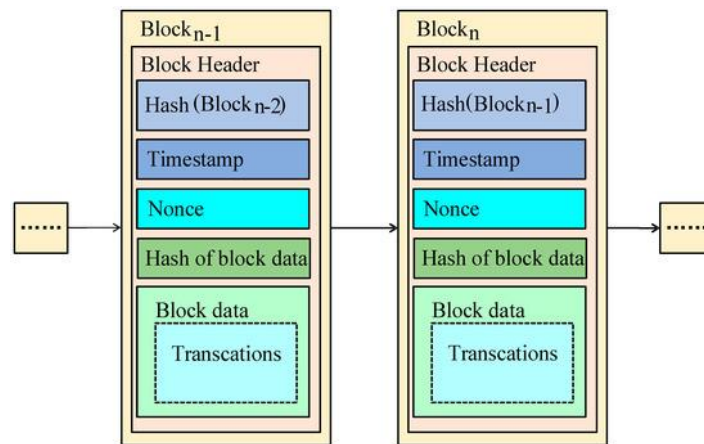


Figure 6 Internal Structure of a Block and Blockchain (Xiao et al. 2022)

However Bitcoin blockchain is only for bitcoin cryptocurrency but Ethereum blockchain that has high potential to work for an ecommerce system and previous attempts already take to the combination of ecommerce and blockchain. For example, Onkart is a decentralized e-commerce application based on ethereum blockchain for buying and selling e-commerce products with a concept of removing middle payment gateways, mean without the intervention of a third party a merchant and a buyer can trade with each other This system follows Consensus based Blockchain network which is more secure, and its functionality is protected by smart contracts. (Pushpalatha et al. 2022)

An Improved transaction processing system (TPS) is proposed by using ethereum blockchain technology, zero-knowledge proof and modified elliptic curve cryptography encryption for making secure ecommerce system. Additionally, a model for detecting denial-of-service attacks on the e-commerce system is presented forth to deal with DoS attacks during e-commerce transactions (Javed et al. 2018).

A O2O e-commerce model based on blockchain technology to solve the information asymmetry between multiple parties. (Jie et al. 2021)

To improve the user data security and service performance, a decentralised e-commerce transaction system based on Ethereum blockchain. Ethereum blockchain is decentralized application development platform , by writing smart contracts and the user data stores

product information in the Interplanetary File System (IPFS) and the returned product addresses in the Ethereum blockchain (Xiao et al. 2022).

To handle large amount of data for the ecommerce business model, suggest blockchain-based PGS (BPGS). Due to the decentralized nature of the blockchain, we can accelerate the verification of product grading. Additionally, 51% of cyber attempts can't be successful unless 51% of the alliance's retailers and e-commerce firms are simultaneously penetrated, under the planned BPGS (Ching et al. 2019). According to the experimental findings, the suggested decentralized ecommerce system is reliable and has good usability. The majority of the decentralized e-commerce systems that have been developed, though, continue to prioritize transactions between customers and merchants. To effectively secure from attacks, a corresponding reputation system is not accessible, and they fail to record the information of third-party institutions in the chain.

In this paper, author proposed a decentralized ecommerce application with the combination of Ethereum Blockchain and IPFS can solve the security of data and payments. Ethereum Blockchain is a best technology in the nomination for improving flow of data security by hashing the data into the block and chained it, smart contract perform this task very well on the backend and this chained user data and sellers products data stores in the IPFS, an decentralized database.

2.9. Conclusion

After accomplishing this literature review, the research designates that eCommerce businesses need such eCommerce application that ensures secure ways of data input and output and it's very important to prevent data from phishing, hacking, and being lost. All of these mishaps occur when dependent on storing data on traditional databases such as Mysql, MariaDB etc which alone are not secure because data is saved in a centralized location.

A best technology in the nomination for improving security of the eCommerce platforms as part of its application side the backend would be a blockchain, specifically an Ethereum blockchain which practicing a POS consensus mechanism The Ethereum BlockChain, stand on the Ethereum Virtual Machine (EVM), a number of unknown individuals (nodes) collaborating and performing tasks underneath Smart Contracts (SC). Smart contracts that written in solidity code makes ethereum a programable, and allow developers to create decentralized software applications or DApp. SC uses the blockchain to store data or set

restrictions on what your application perform functionalities and IPFS is ideal for dealing with the data storage side.

These decentralized technologies come to form a secure, protective means of an eCommerce platform that allows users to save confidential data into the system and payment for purchases items securely implemented with this system. The next chapter will discuss and detail the proposed system.

3. Design and Methodology

3.1. Introduction

This section of the dissertation paper will focus on the design process backing the proposed system. As proposed, the software is planned to securely manage the ecommerce platform functional and security requirement to store all the included data input and output process and payment process with the help of DLTs based blockchain and Interplanetary File System (IPFS) based databases. The portions to lead will detail instructions like the hardware & software requirements and functional & non-functional requirements. Diagrams such as use case and storyboards will be followed with words to elaborate on the concepts furnished. The system will include a login and registration page. Instead, the data will be saved into the IPFS based database, assuming that a user has got registered and now a user of this ecommerce platform and the use purchase any selected product at one point in time. The user data that entered and saved into IPFS will be 'dummy data', personal details of fictional people. This cuts out any potential ethical issues that may arise.

3.2. Hardware Requirement

Table 1 below displays the hardware used to manufacture the system and its specifications:

Table 1. Hardware Specifications

Hardware	Specifications
Laptop	Intel Core i5-1135G7 CPU, 8GB RAM, Windows 10 OS
Android Mobile	Android Version 11

3.3. Software Requirement

The software and versions used to create the system are outlined in Table 2:

Table 2. Software Requirement

Software	Version	Discription
Vs Code	latest	A multi-language integrated development environment, which will house the coding for this project. The reason for choosing this over other outings like Atom is that there are fewer hurdles to getting languages up & running
solidity	Latest version	Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state. Solidity is a curly-bracket language designed to target the Ethereum Virtual Machine (EVM). It is influenced by C++, Python and JavaScript.
NodeJs	Latest version	Server-side language built on asynchronous event-driven Google Chrome's JavaScript Engine (V8 Engine) that does more, in less lines of code. This will be used to create the backend. we are using NodeJs is the ease of installing packages that comes with 'npm'.
ExpressJs	Latest version	A minimal and flexible framework for NodeJs web application with even a single NodeJs file. It also packages in the bootstrap toolkit which can make it work well across both PC and mobile device web browsers, without having to write code for it.

3.4. Functional Requirement

FR-1: The user must be able to register and login to the app with a user name & password.

FR-2: A logged-in user must be able to add, update, view and also delete their personal details information upon logging in.

FR-3: The application must be able to view the product and its details to the user either login or not login

FR-4: The application must be able to allow purchasing the product to the registered user

FR-4: An admin can view manage & verify each product stored on the database, to the data stored on-chain

FR-5: An admin can examine the metadata of each block on the blockchain

FR-6: A user & an admin should have the ability to log out.

3.5. Non-Functional Requirement

3.5.1 Security

NFR-1: Authenticity of a user will be validated through credential login.

NFR-2: That user details will be stored in the IPFS database, the hash of which is then stored in the Ethereum blockchain.

3.5.2 Reliability

NFR-3: The system should function without any bugs or faults.

NFR-4: The system should have a fast response time in terms of general performance , to ensure a smooth user experience.

3.5.3 Fault Tolerance

NFR-5: Since a blockchain and IPFS must have multiple nodes, there must be multiple copies of the ledgers.

3.5.4 Usability

NFR-6: The app should be easy for users to navigate through.

3.5.5 Confidentiality

NFR-7: The data must be encrypted before being stored on the chain, so as to comply with GDPR.

3.6. Use Case Diagrams

Figure 7 shows a use case diagram for the proposed ecommerce system. The user come on the system will be an everyday customer who has visiting the platform looking to find a suitable product to purchase, has been registered user in concern to buy a product, it had at

least checkout one product and system show that the user buy a product upon that date. The admin will see that a new order placed and confirm user that you successful purchased the product. The admin will be a node with high-level permission:

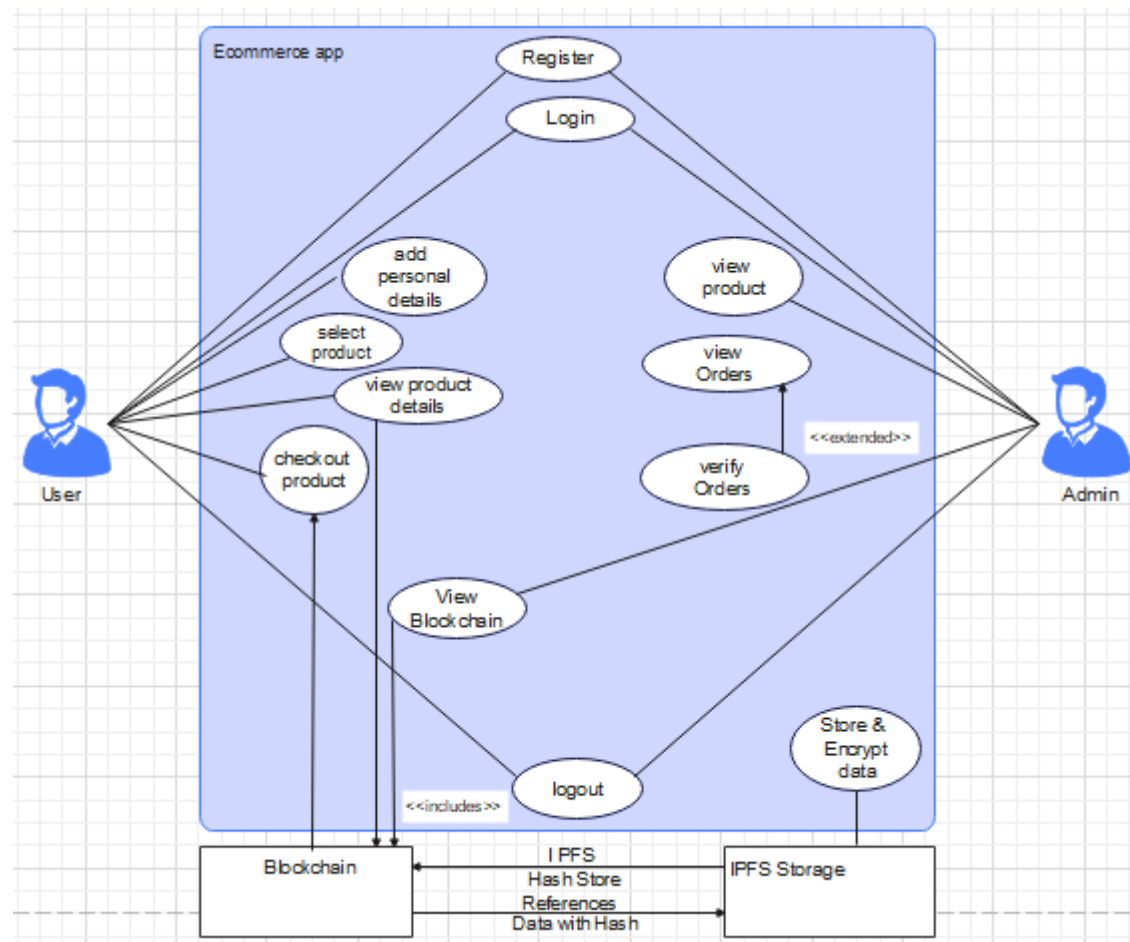


Figure 7 Use Case diagram

3.7. Use Case Discription

Every use case has a specific purpose and the prerequisites needed to achieve it. The following tables describes the intended flow and alternative flow for each use case in the event of an error

Table 3 - Register Use Case

Use Case	Login
Objective	To allow the user register to the app

Precondition	The user credentials will be save on the IPFS
Main Flow	<ol style="list-style-type: none"> 1. User inputs user name & password 2. User clicks the register button
Alternative Flow	password length must be 5 characters – display error message
Post Condition	<p>User successfully registered and allow to login</p> <p>with those credential by which he register , by the main menu selection – which</p>

Table 4 - Login Use Case

Use Case	Login
Objective	To allow registered user to login to the app
Precondition	The registered user has their credentials on the IPFS.
Main Flow	<ol style="list-style-type: none"> 1. User inputs username & password 2. User click the login button
Alternative flow	password length must be 5 characters – display error message
Post Condition	User successfully login the app to enter the main menu selection and make a purchase of a product that he select

Table 5 - View product Use Case

Use Case	View product
Objective	User can view the product and it details

Precondition	The user select the product are already present in the database and visible from the main menu
Main Flow	Upon selecting the product, the app displays all info pertaining to the product
Alternative Flow	The user can also just click to the add to cart button Without checked the product details
Post Condition	The user can view the product details

Table 6 - Checkout Use Case

Use Case	View purchase product with metamask
Objective	User can make payment in cryptocurrency with metamask
Precondition	User clicked on checkout button, meta-mask google chrome extension open and user make payment in cryptocurrency
Main flow	The user clicked on “checkout button”, the user select the payment method cryptocurrency
Alternative Flow	User remove the product from the cart User return to main menu to add more product to cart
Post condition	User successful check out the product

Table 7 – shop admin Use Case

Use Case	Shop admin
Objective	Shop admin must view all product present on IPFS
Precondition	admin must login to view all of products
Main flow	<ol style="list-style-type: none"> 1. The admin login the 2. go to dashboard and view all products 3. the admin click the product and view its details
Alternative Flow	Admin entered incorrect password –error message
Post condition	Admin can view and update products

Table 8 - logout Use Case

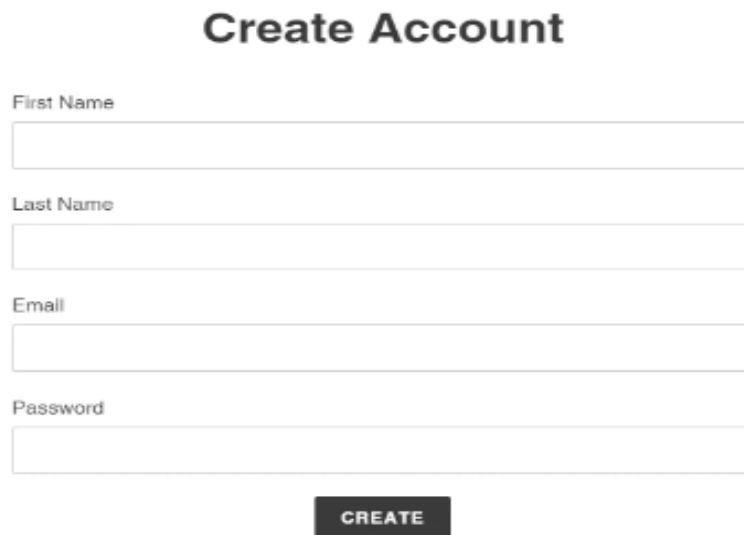
Use Case	User Logout
Objective	User and admin both can logout
Precondition	User or admin must click on logout button to logout the user
Main flow	The user clicked on “signout button” lead to open up a popup window ask to click confirm button to signout the user and user return to login page
Alternative Flow	The user not clicked the signout button
Post condition	User successful sign out the from the application

3.8. Storyboards

The sample GUIs that will come after them try to illustrate how each desired page of the programme should seem and work. This is limited to the user action interface.

3.8.1 Register

The page in Figure 8 below is the register page, users must input their user name and password here in order to become the user of the application and get access any of the other features of the app.



Create Account

First Name

Last Name

Email

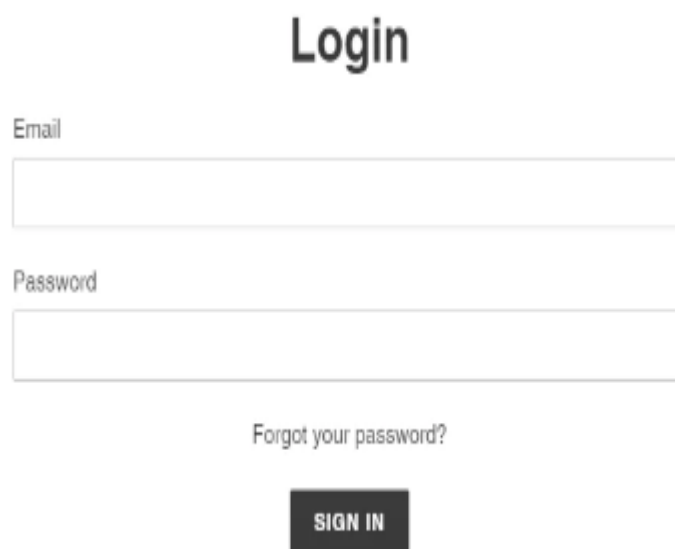
Password

CREATE

Figure 8 Register

3.8.2 Login

The page in Figure 9 below is the login page, users must input their user name and password here in order to access any of the other features of the app:



Login

Email

Password

[Forgot your password?](#)

SIGN IN

Figure 9 Login

3.8.3 Dashboard

The Figure 10 shows below the dashboard page users will see when the application first launches user can see all the product available and on click each product user will be able to view each product.

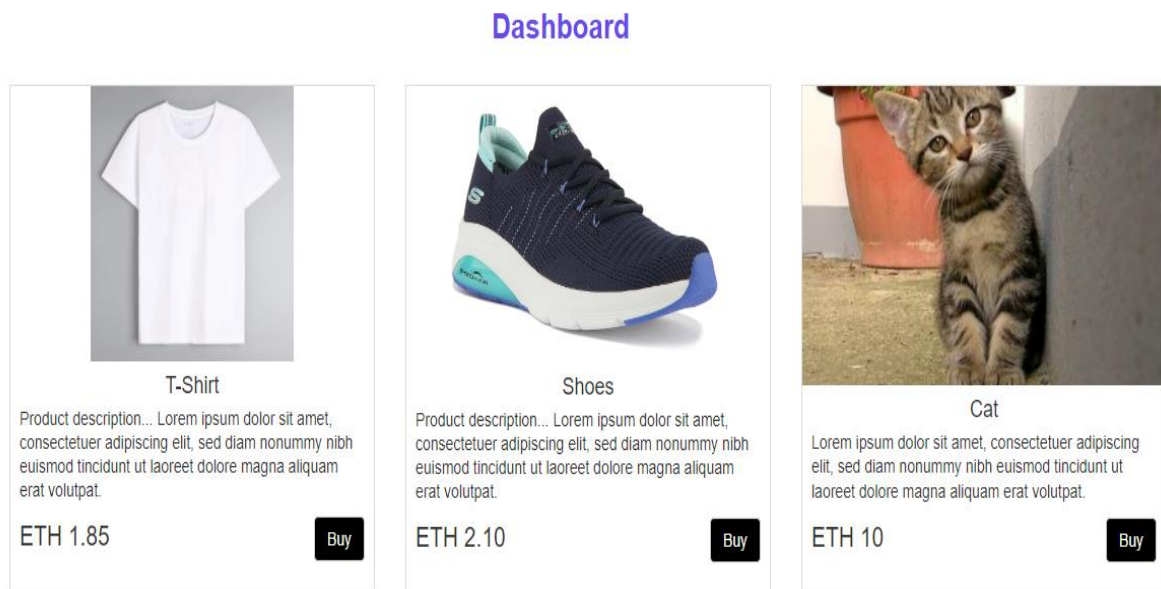


Figure 10 Dashboard

3.8.4 Product Detail

The Figure 11 shows below the dashboard page users will see when the application first launches user can see all the product available and on click each product user will be able to view each product

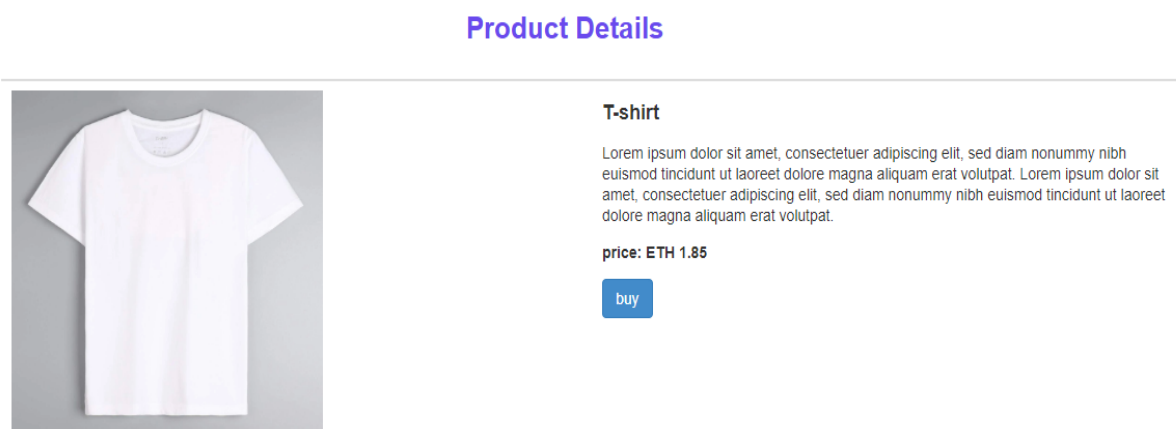


Figure 11 Product Details

3.8.5 Buy product

The Figure 12 below show a authenticated user on click buy allow use to make a payment through metamask and purchase it using cryptocurrency , user get the notification popup window that purchase successfully completed, once user pay the price using it matamask wallet.

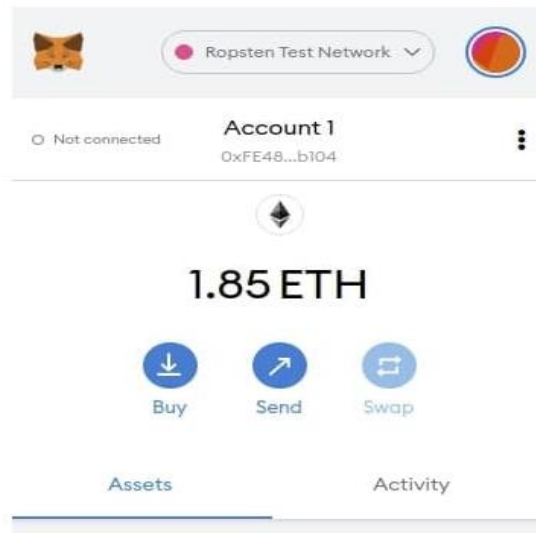


Figure 12

3.8.6 Admin

The figure 13 shows that admin access to his application by login it and only he has allow to add new products and manage them, admin get notify about the new order placed and he will confirm it and notify the user that you product will be on track of delivery.

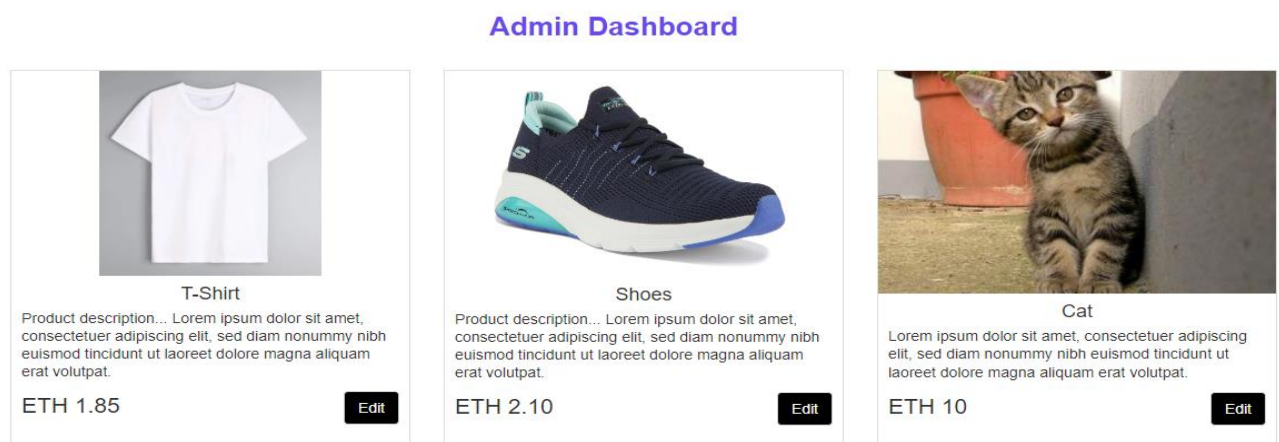


Figure 13

3.9. Ethereum Blockchain & IPFS

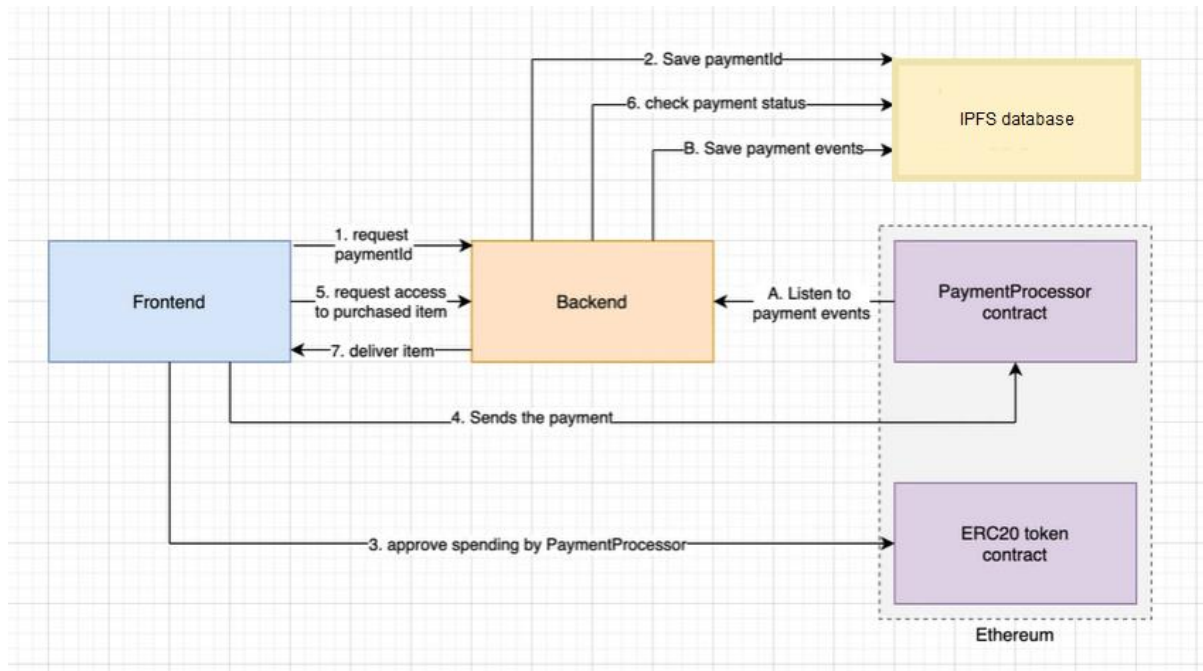


Figure 14 flow of proposed system

Figure 14 gives a general overview of the proposed system above. It tracks the timeline of the system from its initial user launch to the application, can view the product the available products on dashboard, software retrieve the product data via content-based addressing from IPFS. The ethereum blockchain network will handle the authentication of users with a com validator nodes & smart contracts, as shown in Figure 14. Without going too in-depth, smart contracts are a number of aggrements that are coded & stored on a distributed ledger. They behave like 'if-else' statements to an extent, executing when certain conditions are fulfilled.

3.10. Conclusion

Here, the many architectural facets of the suggested e-commerce system were thoroughly covered. The use cases described the steps taken with registering, logging in, add product to cart, checkout, make payment through metamask wallet, viewing and eventually successfully complete purchase. In order to further emphasizing the user experience through their interactions, these tasks were shown with the aid of mock-up ui design. The roles that the Ethereum blockchain & IPFS will perform within the system are shaped by the use case diagram and functions.

4. Testing & Results

4.1. Introduction

The methodologies for testing the constructed software system, which will satisfy the requirements for objective 6 as stated in the section 1.3.2 of this document, are covered in the following section. According to numerous research statistics, testing operations consume close to 30% of the total work put into developing software. In order to create high-quality software, testing activities are crucial. The supporting pillars of the unit testing techniques will be black box and white box testing established in the design chapter by performing the functional and acceptance testing (Pramod et al. 2016). The use of these techniques will enable a comparison of the operations two sides.

4.2. White Box Testing

White box testing concentrates on examining the application's core components. Here, a developer's perspective is used, which means that component's core knowledge is easily accessible and testable. The web app's internal testing cases for this particular system will check the effectiveness of the security and data immutability controls in place (Ginanjar ,2020).

The fraction of the white box category that is utilized will be acceptance testing. For the user's artefact, this test procedure can be considered as core competencies. The final indication of whether the system is assumed complete will be depending on the customer's response.

4.3. Black Box Testing

Instead of examining every component of the system, black box testing chooses to concentrate on the system's basic functionality (Taejoon et al. 2021). The viewpoint won't be familiar with the inside functioning of the system. Instead, the testers will assume the role of an unaware user interacting with the ethereum blockchain and IPFS off-chain database via the web application ui and examine their activities. The primary testing methodology will be functional testing.

Functional testing focuses on the specifications that were laid forth at the project's commencement. Making sure that the result matches the precise output that the tester is expecting is the key concern with this kind of testing (Pramod et al. 2016).

4.4. Testing Strategy

Table 9- Testing Strategy Results

Test ID	Description	Testing	Steps	Expected Result	Actual Result
R001	Ecommerce Application is launched	White Box	1. User Starts Application	Ecommerce Application start and blockchain initialised in <30 seconds	
R002	User Register	White Box/Black Box	1.Users input username and password to get registered 2. User clicked "registered" button	User Credentials saved into the ipfs database Registered user allow to login Admin already registered & access to the admin dashboard	PASS
R003	User Login	White Box/Black Box	1. User enter registered credential 2.User click 'login' button	Credentials Details verified. Logged in user will allow to checkout and made payment to purchase Admin logged in & redirected to admin dashboard	PASS
R004	User choose product and add them to the purchase	White box/blackbox	1.User click on "buy" button product to add to cart to purchase	An authenticated User click on "buy" button to place it for checkout process	PASS
R005	Checkout the product	White box/black box	1.user click on checkout button to purchase the product	User click on	

			Matamask window appear and which shows the product user is purchasing is ready for purchase User click the pay button and payment made		
--	--	--	---	--	--

4.5. Conclusion

In this chapter, the testing strategy that was developed in section 4.4 of this chapter has been summarized and completed. The testing strategy was analyzed both the functional and non-functional requirements in addition to the functional ones. The security of the e-commerce system is examined in-depth in this section 4.4, using the Ethereum blockchain to secure user data saved in the IPFS database, illustrating and strengthening the process' trustworthiness.

5. References

IMARC Group (2022) Logistics Market Size, Share | Industry Trends, Growth Report & Forecast 2022-2027 [online], available: <https://www.imarcgroup.com/logistics-market> [accessed 2022].

Buquan Liu, "Overview of the Basic Principles of Blockchain", source: <https://ieeexplore.ieee.org/document/965356> , [accessed: 30 December 2021]

C. Cachin, 2016 "Architecture of the Hyperledger blockchain fabric", Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016

Yuanyuan Xiao , Chuangming Zhou , Xinpeng Guo, Yafei Song and Chen Chen 2022 "A Novel Decentralized E-Commerce Transaction System Based on Blockchain" available: <https://www.mdpi.com/2076-3417/12/12/5770> , [accessed 11 June 2022].

John Bogna , " What Is the Environmental Impact of Cryptocurrency?", source: <https://uk.pcmag.com/old-cryptocurrency/138047/what-is-the-environmental-impact-of-cryptocurrency>, [accessed: 8 Jan 2022]

Andreas Vlachos, 2022 "Write an article about the main types of consensus algorithms" <https://thecrypto.app/knowledge/the-main-types-of-consensus-algorithms>, [accessed 20 January, 2022].

Satoshi Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System ", available: <https://bitcoin.org/bitcoin.pdf> , [accessed: 2009]

S Muralidhara, B A Usha, "Review of Blockchain Security and Privacy", source: <https://ieeexplore.ieee.org/document/9418424> , [accessed: 06 May 2021]

Javed R. Shaikh, Georgi Iliev, "Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce Security" source: doi.org/10.1109/GCWCN.2018.8668619 [accessed: 24 November 2018]

Jie Bao, Kang Wang, Yi Feng, "a novel O2O e-commerce model based on block chain" source: ieeexplore.ieee.org/document/9524072 , [accessed: 06 September 2021]

Luyao Zheng, "Analyse the computer based blockchain technology in cross-border Ecommerce Platforms" available: <https://www.hindawi.com/journals/misy/2022/5083518> [accessed : 28 Sept 2022].

Yue Yin, Danjv Lv, Xin Huang, Jiang Liu, Shanshan Xie, Yan Zhang, "Research on Blockchain Security Protection", source: <https://doi.org/10.1109/ICCC54389.2021.9674442>, [accessed: 17 January 2022])

Jiarui Zhang, Yukun Cheng, Xiaotie Deng, Bo Wang, Jan Xie, Yuanyuan Yang, "A Reputation Based Mechanism for Transaction Processing in Blockchain Systems", source: ieeexplore.ieee.org/document/9625746, [accessed: 23 November 2021]

Avinash Kshirsagar, Vinod Pachghare, "Performance Evaluation of Proof of Scope Consensus Mechanisms on Hyperledger", source: <https://ieeexplore.ieee.org/document/9935860>, [accessed: 9 nov 2022]

Juan A. Garay ,Aggelos Kiayias , "The Bitcoin Backbone Protocol: Analysis and Applications Advances in Cryptology", source: http://dx.doi.org/10.1007/978-3-662-46803-6_10 [accessed: 26-04-2015]

A Pushpalatha, Gowtham Senthil, P M M Jawahar, E Kartheesan, "A Trustworthy Decentralized Onkart Ecommerce Platform based on Blockchain Technology", <https://ieeexplore.ieee.org/abstract/document/9776811> [accessed: 24 May 2022]

Ching-Nung Yang, Yi-Cheng Chen, Shih-Yu Chen Song-Yu Wu, "A Reliable E-commerce Business Model Using Blockchain Based Product Grading System" , source: <https://ieeexplore.ieee.org/document/8713204> [accessed: 18 march 2019]

M. Basile, G. Nardini, P. Perazzo, G. Dini, "A Rational Mining Strategy for Proof-of-Work Consensus Algorithms", source:doi.org/10.1109/BRAINS55737.2022.9909327, [accessed:11 October 2022]

Peiliang Lei, Minsheng Tan, Shiyong Xai, "An Improved Scheme for Proof-of-Stake Based on Block Memory", <https://ieeexplore.ieee.org/document/9927710>, [accessed:4th November 2022]

M. M. V Sai Nikhil, Aniket Sarrin, Ghanshyam S. Nair, M. Supriya, "Design and Implementation of E-commerce Website using Automata Theory" , source: doi.org/10.1109/ICOEI53556.2022.9777191, [accessed: 24 May 2022]

Nishant Lalitkumar Bhatia, Vinod Kumar Shukla, Ritu Punhani, Shish Kumar Dubey, "Growing Aspects of Cyber Security in E-Commerce", source: doi.org/10.1109/ICCICT50803.2021.9510152, [accessed: 12 August 2021]

Jinson Varghese, "10 E-commerce Security Threats That Are Getting Stronger By The Day" source: <https://www.getastra.com/blog/knowledge-base/ecommerce-security-threats/> , [accessed: May 2, 2022]

Alex Leventer , "How to Run Your Own IPFS Gateway", source:<https://medium.com/building-the-open-data-stack/how-to-run-your-own-ipfs-gateway-7aa13aa9ad45> , [accessed :28 july 2022]

Benet, J. (2021) 'IPFS Documentation', available: <https://docs.ipfs.io/> [accessed 26 Oct 2021].

Sebastian Henningsen, Sebastian Rust, Martin Florian, Björn Scheuermann, “Crawling the IPFS Network”, source: <https://ieeexplore.ieee.org/document/9142764>, [accessed: 17 July 2020]

Tabora. V, “Using IPFS For Distributed File Storage Systems”, available: <https://medium.com/Oxcode/using-ipfs-for-distributed-file-storage-systems-61226e07a6f>, [accessed 12 Dec 2021].

Maruti M Arer, Praveen M Dhulavvagol, S G Totad “Efficient Big Data Storage and Retrieval in Distributed Architecture using Blockchain and IPFS”, source: [10.1109/I2CT54291.2022.9824566](https://doi.org/10.1109/I2CT54291.2022.9824566) [accessed:18 July 2022]

Jiajie Shen, Yi Li, Yangfan Zhou, Xin Wang “Understanding I/O Performance of IPFS Storage:A Client's Perspective”, source: ieeexplore.ieee.org/abstract/document/9068631, [accessed: 25 June 2019]

Hector Sanjuan , Samuli Poyhtari, Pedro Teixeira, Ioannis Psaras, “Merkle-CRDTs Merkle-DAGs meet CRDTs”, <https://research.protocol.ai/publications/merkle-crdts-merkle-dags-meet-crdts/psaras2020.pdf> ,[accessed: 27 April 2020]

Morteza Alizadeh, Karl Andersson, Olov Schelén, “Efficient Decentralized Data Storage Based on Public Blockchain and IPFS” source: [10.1109/CSDE50874.2020.9411599](https://doi.org/10.1109/CSDE50874.2020.9411599) , [accessed: 28 April 2021]

Peilin Zheng,Zibin Zheng, Jiajing Wu, Hong-Ning Dai, “XBlock-ETH: Extracting and Exploring Blockchain Data From Ethereum”, source: <https://doi.ieeecomputersociety.org/10.1109/OJCS.2020.2990458> , [accessed: 2020/01/01]

Yongle Chen, Hui Li, Kejiao Li, Jiyang Zhang, ‘An improved P2P File System Scheme based on IPFS and Blockchain’, <https://ieeexplore.ieee.org/document/8258226>, [accessed: 15 January 2018]

Fabian Sparbrodt, Marisol García-Valls “Digesting smart contracts in Ethereum blockchain networks source: <https://ieeexplore.ieee.org/document/9766685> , [accessed: 30 March 2022]

Keyao Huang, Jingyu Ma, Xinyuan Wang, “A Comparative Analysis of Bitcoin and Ethereum Blockchain” 08 March 2022 <https://doi.org/10.1109/AINIT54228.2021.00137>

Xiang Hong Li, “Blockchain-based Cross-border E-business Payment Model”, source: doi.org/10.1109/ECIT52743.2021.00022 [accessed: 21 April 2021]

Wang Zimu ,” Blockchain Technology: Opportunities and Challenges in Copyright Industry ”, source: doi.org/10.1109/ICCWAMTIP53232.2021.9674178 , [accessed:17 December 2021]

Ginanjari Wiro Sasmito, “White Box Testing with Basis Path Technique in the Demography Administration Website”, source: <https://ieeexplore.ieee.org/document/9557428> , [accessed: 17 December 2020]

Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, Lejia Shen, “Blockchain technology and its relationships to sustainable supply chain management”, available: <https://doi.org/10.1080/00207543.2018.1533261> [accessed: 17 Oct 2018]

Truc Nguyen, Phuc Thai, Tre’ R. Jeter, Thang N. Dinh, My T. Thai “ Blockchain-based Secure Client Selection in Federated Learning” source: <https://doi.org/10.1109/ICBC54727.2022.9805521>

Zhiqiang Ouyang, Jie Shao, Yifeng Zeng, “PoW and PoS and Related Applications” ,source: <https://ieeexplore.ieee.org/document/9588080> , [accessed: 09 November 2021]

Taejoon Byun, Sanjai Rayadurgam , Mats P.E. Heimdahl, “Black-Box Testing of Deep Neural Networks ”, source: <https://ieeexplore.ieee.org/document/9700360> [accessed: 28 October 2021]

Pramod Mathew Jacob M. Prasanna ,”Comparative analysis on Black box testing strategies" source: <https://ieeexplore.ieee.org/document/7845290> , [accessed: 13 August 2016]

9 Appendices

10 Appendix A: Code Listing

11