Project Synopsis

on

SimpleSplit

Submitted as a part of the course curriculum for

Bachelor of Technology

in

Computer Science

Submitted by

Kartik Gupta (1900290120050)

Prayrit Srivastava (1900290120080)

Ritik Nandan Gupta (1900290120091)

Under the Supervision of

Prof. Pardeep Tyagi

Asst. Professor, Department of Computer Science

KIET Group of Institutions, Ghaziabad

Department of Computer Science

Dr A.P.J. Abdul Kalam Technical University

2021-2022

DECLARATION

We hereby declare that this submission is our work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material that to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

Signature:

Name: Kartik Gupta
Roll No.: 1900290120050
Date:

Signature:

Name: Prayrit Srivastava
Roll No.: 1900290120080
Date:

Signature:

Name: Ritik Nandan Gupta
Roll No.: 1900290120091
Date:

CERTIFICATE

This is to certify that the Project Report entitled "**SimpleSplit**" which is submitted by **Kartik Gupta, Prayrit Srivastava, Ritik Nandan Gupta** in partial fulfilment of the requirement for the award of degree B. Tech. in the Department of Computer Science of Dr A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Date:

Supervisor Signature
Asst. Prof. Pardeep Tyagi
(Designation)

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the synopsis of the B.Tech Major Project undertaken during B.Tech. Final Year. We owe a special debt of gratitude to GUIDE to **Prof. Pardeep Tyagi**, Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his/her constant support and guidance throughout our work. His sincerity, thoroughness, and perseverance have been a constant source of inspiration for us. It is only his/her cognizant efforts that our endeavours have seen the light of the day.

We also take the opportunity to acknowledge the contribution of Dr P. K Singh, Head of the Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the faculty members of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution to the completion of the project.

Signature:

Name: Kartik Gupta
Roll No.: 1900290120050
Date:

Signature:

Name: Prayrit Srivastava
Roll No.: 1900290120080
Date:

Signature:

Name: Ritik Nandan Gupta
Roll No.: 1900290120091
Date:

ABSTRACT

SimpleSplit is a progressive Blockchain-powered web application that makes splitting bills as simple as never before. From registering bills in a digital ledger to settlement, SimpleSplit comes to save the day.

Furthermore, the users can be notified by email or SMS so that they never miss an update. The application is well designed to tackle all kinds of splits and supports multiple forms of payment (UPI, Stripe, Razorpay, etc.). Finally, SimpleSplit helps send IOU reminders in case someone forgets to pay on time.

The application allows users to form groups and friends where they can chat with each other, discuss the bill(s) and pay securely with any payment method. The users need not install any external/third-party software to split their bills. SimpleSplit also enables users to split their bills by percentage, by shares, etc. The users can also request a pdf invoice of their payments on their email.

Security is an important aspect of our application due to financial data and personal information involvement. So, to tackle the problem, SimpleSplit stores all sensitive data on a cryptographically secured peer-to-peer blockchain network, making it invulnerable to most cyberattacks.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

SimpleSplit is a progressive Blockchain-powered web application that makes splitting bills as simple as never before. From registering bills in a digital ledger to settlement, SimpleSplit comes to save the day. Furthermore, the users can be notified by email or SMS so that they never miss an update. The application is well designed to tackle all kinds of splits and supports multiple forms of payment (UPI, Stripe, Razorpay, etc.).

The application allows users to form groups and friends where they can chat with each other, discuss the bill(s) and pay securely with any payment method. The users need not install any external/third-party software to split their bills. SimpleSplit also enables users to split their bills by percentage, by shares, etc. The users can also request a pdf invoice of their payments on their email.

Last but not least, SimpleSplit helps to send IOU reminders in case someone forgets to pay on time.

1.2 PROBLEM STATEMENT

A web or mobile application that allows consumers to split expenses with friends. If a group needs to share the cost of a particular bill, this app should ensure that anyone who pays is reimbursed in the correct amount and with a minimal number of transactions. Users can send an email notification when a bill is due, and the app allows users to send an IOU to someone else in the group.

1.3 RESEARCH OBJECTIVES

1. To conduct user surveys and find out how people use SimpleSplit
2. User surveys specifically around adding and organizing bills.
3. Address the pain points and propose probable solutions.

CHAPTER 2: LITERATURE REVIEW

Digital ledger technology-based real estate transaction mechanism and its block size assessment

Distributed ledger technology (DLT) is set to transform the existing architectural models of financial institutions and government machinery. Although real estate transactions are a major source for the governments to earn revenue, these are plagued with the risk of fraudulent practices. The digital documents are vulnerable to alteration or any other attacks or can be tampered and ownership of the documents can be changed. The centralized storage involves a single point of failure as well as network traffic overhead. The proposed distributed and decentralized blockchain-based architecture provides protection against any intrusive activity which is offset by the majority voting achieved in consensus mechanism for each transaction and verification request. The proposed work provides a web interface for user queries and analysis of query search time is carried out. Although real estate transactions are a major source for governments to earn revenue, these are plagued with the risk of fraudulent practices. The digital documents are vulnerable to alteration or any other attacks. The real estate records can tamper and ownership of the property can be changed. The proposed distributed and decentralized architecture protects any such intrusive activity which is offset by the majority voting achieved in the consensus mechanism for each transaction and verification request. It has been observed that when the block size is increased from 42 KB to 422 KB, i.e., increased by ten times, the time required to process the user query is reduced by 65-70%. If a huge number of transactions takes place in a given time and the time taken by miners for verification of these transactions is more than the tolerable limit, the block size should be smaller. Else one should go for a larger block size if the hardware infrastructure deploying and running the application is robust enough.

Blockchain and its Scope In the Modern Technology

Blockchain is the technology that can lead to significant changes in our business environment and will have a great impact on the next few decades. It can change the way we perceive business processes and can transform our economy.

Blockchain is a decentralized and distributed ledger technology that aims to ensure transparency, data security, and integrity since it cannot be tampered with or forged. Most of the current research related to Blockchain Technology is focusing on its application for cryptocurrencies, such as Bitcoin, and only a limited number of research is targeted at exploring the utilization of Blockchain Technology in other environments or sectors. Blockchain Technology is more than just cryptocurrency, and it can have several applications in government, finance and banking industry, accounting and Business Process Management. Therefore, this study attempts to investigate and explore the opportunities and challenges for the current or future applications of Blockchain Technology. Thus, a large number of published studies were carefully reviewed and analyzed based on their contributions to the Blockchain's body of knowledge. From a theoretical perspective, based on the literature review, Blockchain Technology has high value and good prospects in resolving problems of data integrity, improving transparency, enhance security, prevent fraud, and establish trust and privacy.

Blockchain Technology can bring revolution in the areas of Finance, Accounting, e-Government, BPM, insurance, entertainment, trading platforms, healthcare, internet of things, as well as law firms and others. Hence, Blockchain Technology has a huge potential in introducing innovative solutions, depending on the area or the sector of its implementation since economic efficiency and social benefits can be achieved through technical innovation and applications. However, implementing Blockchain Technology in organizations in different industries could prove to be very costly. Migrating or moving legacy systems requires a significant amount of investment from organizations. Adopting Blockchain Technology, at this early stage, organizations will have to deploy a 13 unified platforms to support such hybrid application architecture, incorporating Blockchain and legacy systems. Thus, they need to deepen their understanding of Blockchain Technology, its value, its opportunities, and its risks. As a result, there are only a small number of instances in which the technology has been applied with these systems. Therefore, Blockchain Technology may not replace legacy systems or old applications soon. However, Blockchain can certainly be a complementary application to legacy systems and may even lead to the development of new systems shortly. In conclusion, more intensive research in this area of Blockchain Technology is necessary to advance the maturity of this field since it is still in the exploratory stage and there are many legal and technical issues to be resolved. Therefore, this review offers a useful starting point for future research themes for the development of Blockchain application, and assists practitioners and researchers.

A Review of Blockchain Technology and Its Applications in the Business Environment

Blockchain is the technology that can lead to significant changes in our business environment and will have a great impact on the next few decades. It can change the way we perceive business processes, and can transform our economy. Blockchain is a decentralized and distributed ledger technology that aims to ensure transparency, data security, and integrity since it cannot with be tampered or forged. Most of the current research related to Blockchain Technology is focusing on its application for cryptocurrencies, such as Bitcoin and only a limited number of research is targeted at exploring the utilization of Blockchain Technology in other environments or sectors. Blockchain Technology is more than just cryptocurrency, and it can have several applications in government, finance and banking industry, accounting, and Business Process Management. Therefore, this study attempts to investigate and explore the opportunities and challenges for the current or future applications of Blockchain Technology. Thus, a large number of published studies were carefully reviewed and analyzed based on their contributions to the Blockchain's body of knowledge. Blockchain Technology is not appropriate for massive transactions, due to a complex verification process, (Beck et. al., 2016). In Blockchain Technology, to provide security, all transactions will have to be digitally time-stamped with a cryptographic hash code, a unique 64-digit alpha-numeric signature to record every single transaction, which consumes a lot of computing power and time. Furthermore, some scholars recommend that the benefits of Blockchain adoption into public or private services must be identified carefully since the cost might be higher of the benefits for developing, running and maintaining the Blockchain Technology, (Marsal- Llacuna & Luïsa 2017; Angraal et al., 2017). However, the immaturity of the technology itself is at the base of all existing technological challenges in adopting Blockchain Technology. This can be understood tosomething common in all new technology introductions. In closing, Blockchain adoption might lead to organizational transformation, including changes in strategy, structure, process, and culture. This transformation requires organizational members' cooperation and commitment to enable the organization to survive and to improve the level of performance and effectiveness. From a theoretical perspective, based on the literature review, Blockchain Technology has high value and good prospects in resolving problems of data integrity, improving transparency, enhance security, preventing fraud, and establish trust and privacy. Blockchain Technology can bring revolution in the areas of Finance, Accounting, e-Government, BPM, insurance, entertainment, trading platforms, healthcare, internet-of- things, as well as law firms and others. Hence, Blockchain Technology has a huge potential in introducing innovative solutions, depending on the area or the sector of its implementation, since economic efficiency and social benefits can be achieved through technical innovation and applications. However, implementing Blockchain Technology at organizations in different industries could prove to be very costly. Migrating or moving legacy systems require a significant amount of investment from organizations. Adopting the Blockchain Technology, at this early stage, organizations will have to deploy a 13 unified platform to support such hybrid application architecture, incorporating Blockchain and legacy systems. Thus, they need to deepen their understanding of Blockchain Technology, its value, its opportunities, and its risks. As a result, there are only a small number of instances in which the technology has been applied with these systems. Therefore, Blockchain Technology may not replace legacy systems or old applications soon. However, Blockchain can certainly be a complementary application too legacy systems and may even lead to the development of new systems shortly. In conclusion, more intensive research in this area of Blockchain Technology is necessary to advance the maturity of this field, since it is still in the exploratory stage and there are many legal and technical issues to be resolved. Therefore, this review offers a useful the starting point for future research themes for the development of Blockchain applications, and assist practitioners and researchers.

The fair cost of Bitcoin proof of work

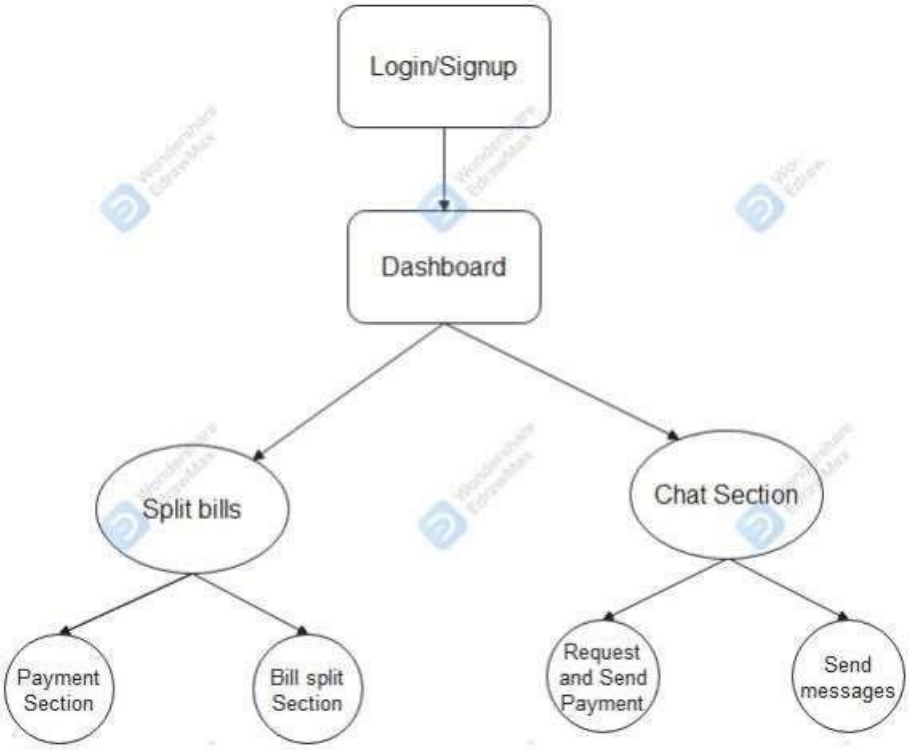
Bitcoin, a digital cash currency launched in 2009 by an anonymous inventor with an alias Satoshi Nakamoto has demonstrated that untrustful peers can exchange value over the Internet without any third-party intermediary or trusted authority. Bitcoin has reached over 10 billion dollars capitalization and the system is processing tens of thousands of transactions a day without having been so far challenged by any serious attack. Blockchain is the main technology underneath Bitcoin; it is a distributed ledger available to anyone participating to the Bitcoin network. In the network, Bitcoin transactions are publically announced and valid transactions are chronologically registered on the ledger. The validity of a transaction is verified by the network participants themselves and valid transactions are put into blocks which are cryptographically sealed and attached to the previous block every 10min on average. The blocks form a chronological sequence: a chain of blocks, a blockchain, at equilibrium, the cost of proof of work should be such too making a double-spending attack too expensive to be profitably carried over. Within this principle, it is relatively straightforward to estimate the fair cost of the proof of work the the under ideal-equilibrium- equilibrium assumption. Let us consider an attacker that owns some Bitcoin amount and wants to artificially multiply it by spending the same Bitcoin with several different users. This is a double-spend attack. A greedy attacker will try to double-spend the largest amount of Bitcoin possible, but this is limited to the amount normally exchanged within a block which currently is around $1 million. A transaction involving a substantially larger sum than the usual total value of transactions in a block will capture unwanted attention from the network. This limits the double-spending amount to about $1 million. Of course, the duplication can be repeated several times both in parallel or but serially shortly, this does not affect the outcomes of the present computation. So the attacker has a potential gain of some fraction of $1 million. To be successful the attacker must make sure that both the duplicated transactions are validated and this requires generating a fork with two blocks being attached to the previous block. If the attacker has enough computing power she can generate two valid hashes to seal the two blocks giving a false impression that both transactions have been verified. However, for a final settlement of the transaction it is presently considered that one should wait for six new blocks to be Hardware Hash rate Energy Consumption Central processing unit CPU 0.1 GH/s 2000 J/GH Graphics processing unit GPU 0.5 GH/s 500 J/GH Field- programmable gate array FPGA 10 GH/s 50 J/GH Application-specific integrated circuit ASIC 10,000 GH/s 0.5 J/GH Table 1 Estimated hash rates and associated energy consumption for various kinds of hardware for Bitcoin mining. CPUs and GPUs are no longer used. Data are inferred from various sources, mainly specifications from hardware producers. Electronic copy available at attached to the chain to make the transaction statistically unlikely to be reverted. The attacker should therefore use her computing power to generate six valid hashes before the double-spent transaction might be considered settled. Note that only one of the two forks (the shortest) must be artificially validated by the attacker, the other will be considered valid by the system and can be let propagated by the other miners, or the attacker can propagate it as well but she will also get compensated by the mining reward. Of course, it is quite unrealistic to assume that nobody notices the propagating fork for such a long time, but let's keep this as a working hypothesis. The artificial propagation of the fork has a cost that is the cost of the proof of work times six. The attacker will make profits if this cost is inferior to the gain. In summary, we have a very simple breakeven point with the current values, and to make calculations clean, we can assume that the attacker duplicates 60% of the typical value of a block, double spending, therefore, $600,000. Requiring 6 blocks for settlement this yields to the following estimate for what should be the fair cost of the proof of work per block at equilibrium: ≈ $100,000. This computation over-estimates this cost because to be unnoticed that attack should be performed on a smaller fraction of the block value and it is highly unlikely that a long forking can propagate for over one hour with all blocks validated by the same miner without anyone noticing that something unusual is happening. It is, therefore, reasonable to consider that 10% of the above cost is a sufficient deterrent to attackers. This is indeed the order of magnitude of the present electricity cost for the proof of work in Bitcoin. We can therefore conclude that the current cost for Bitcoin proof of work is large, wasteful, but necessary. Reductions in such costs can be operated by increasing the number of blocks required for settlement or by automatically detecting and blocking forking at early stages. On the other hand, an attacker can also reduce costs by stealing electricity or hacking mining farms.

Performance Evaluation of Permissioned Blockchains for Financial applications: the ConsenSys Quorum case study

Given the availability of several blockchain technologies in permission contexts, blockchain application designers have to cope with the increasing complexity of choosing which technology and consensus algorithm best fit a specific use case. However, the lack of a standard framework allowing to assess of the scalability of permissioned blockchain platforms and to compare performances and features of consensus algorithms making the development of a sensible evaluation is a costly and difficult time-consuming problem. Throughout this article, we propose practical scalability and applicability evaluation of the Quorum blockchain and its consensus algorithms. Although we apply our evaluation workflow to a financial use case, we define a methodology that can be generalized to any permissioned blockchain technology. We leverage Hyperledger Caliper as a benchmarking tool, and Docker as a deployment tool, making our analysis easy to be cross-platform- platform, and cost-effective. This paper outlined a general workflow for benchmarking permissioned blockchain platforms and related consensus algorithms. We presented as a practical case study the ConsenSys Quorum blockchain: it plug-and-play-play consensus mechanisms, which have been analyzed, also taking into account the CAP trade-off problem [3]. The theoretical analysis (Section 3) performed on Raft, Clique PoA and IBFT can be transposed to every consensus algorithm. Then, we outlined methodology and tools to drive and produce performance evaluations of blockchain technologies, by comparing different consensus mechanisms under different network configurations. While previous works limit the generalizability of the results, our approach and is replicable, open-source and it provides new insights into the scalability quality of consensus protocols, by performing tests on a variable number of blockchain nodes. Although this research clearly illustrates the effects of different parameters the on performance and scalability of permissioned Quorum networks, it also raises many questions. For instance, further research is needed on security considerations: future works should address trade-offs between security and performance, or even effects of byzantine nodes on network safety. Moreover, an open source modification to the Caliper framework could be proposed so to make the worker processes multithread (as in [2]), thus alleviating the transaction rejection issue on high input rates. This modification could also increase measurement accuracy. Nevertheless, our tools are ready to be used to collect data on many more combinations of performance variables and network configurations of Quorum. Specifically, it could be meaningful to analyze memory and CPU consumption of blockchain nodes, by leveraging Prometheus [31] as a monitoring tool (already integrated with Caliper). Furthermore, the deployment tool we implemented [25], could as as be extended so to allow new nodes to dynamically join the Quorum network for the need of static IPs: in that case, the overhead of the reconfiguration protocol of consensus mechanisms must be studied. Overall, our tools can be taken as examples to implement new Caliper plugins to test other blockchain platforms in the financial context. Testing and comparing performances of different permissioned blockchains can be useful both for research scopes and for practical applications, since this technology is being considered for adoption in interesting financial scenarios, such as too to interbank transactions and Central Bank Digital Currencies [14]. In addition, alternative workloads can be proposed so to extend benchmarks to other use cases, such as supply chain. To conclude, the workflow we proposed is flexible enough to be applied to any permissioned blockchain context: it is useful for assessing and analyzing performances of various consensus algorithms within the same blockchain framework, but it also enables cross-blockchain comparisons.

CHAPTER 3: PROPOSED METHODOLOGY

3.1 FLOWCHART



3.2 ALGORITHM USED

Blockchain is a constantly growing collection of records, and new blocks are added to the list continuously. As the network grows bigger, it will be difficult to ensure that all the information on the blockchain is secure from any unwanted threats. Cryptography is one of the fundamental requirements in the blockchain.

It offers the platform for tailoring protocols and techniques to avoid third-party interference in accessing and procuring information regarding data in private messages throughout a communication process. The objective of a cryptography algorithm prevents any third party from eavesdropping on private communications over a blockchain network. Before reflecting further on cryptography algorithms for blockchain security, let us take a brief overview of the origins of cryptography.

Cryptography can be traced back to ancient times when a cypher was used for transmitting messages. With a specific system for creating coded messages and deciphering them, cryptography was popular in ancient Egypt as well as the Roman Empire. However, the most modern origins of cryptography algorithms refer to the Vigenere cypher of the 16th century. The most popular example of the use of cryptography refers to the case of the Enigma Machine used by Germans.

It was used during World War 2 and could generate ciphertexts that could not be decrypted through analysis of letter frequency. Over the years, many new cryptography algorithms, such as the Advanced Encryption Standard algorithm, presented different use cases. Now, it is reasonable to wonder about the type of blockchain algorithm you have for cryptography.

Consensus Algorithms

Blockchain allocates power to the network participants. The majority of network participants have to reach an agreement on a specific transaction before adding it to a block. In this case, consensus algorithms offer the functionality of reaching an agreement on a specific data value throughout distributed systems and processes. Consensus algorithms are the most commonly preferred algorithms for blockchain security. They help different participants on the blockchain network in arriving at a consensus or common agreement regarding the existing data state in the ledger. At the same time, consensus algorithms also help in deriving agreements for trusting unknown peers in distributed computing environments. Consensus algorithms are an integral part of blockchain networks as they help in maintaining the integrity and security of distributed computing systems. Let us find out more about the different types of consensus algorithms and how they support security on the blockchain.

Proof of Work Consensus Algorithm

Proof Of Work(POW) is the creation of a cryptographic hash. Generally, it requires blockchain validators to take data from the block header as inputs. Then, the blockchain validators could run the input through a cryptographic hash function continuously. Validators ensure hashing of slight changes in input data through the inclusion of an arbitrary number, referred to as a nonce. The nonce is added with all iterations of running the input data through a cryptographic hash function. PoW algorithm used in blockchain requires higher processing power for determining the addition of data in the next block. Therefore, you may need specialized computers such as ASICs for computing complex mathematical problems required in PoW systems.

Proof of Stake Consensus Algorithm

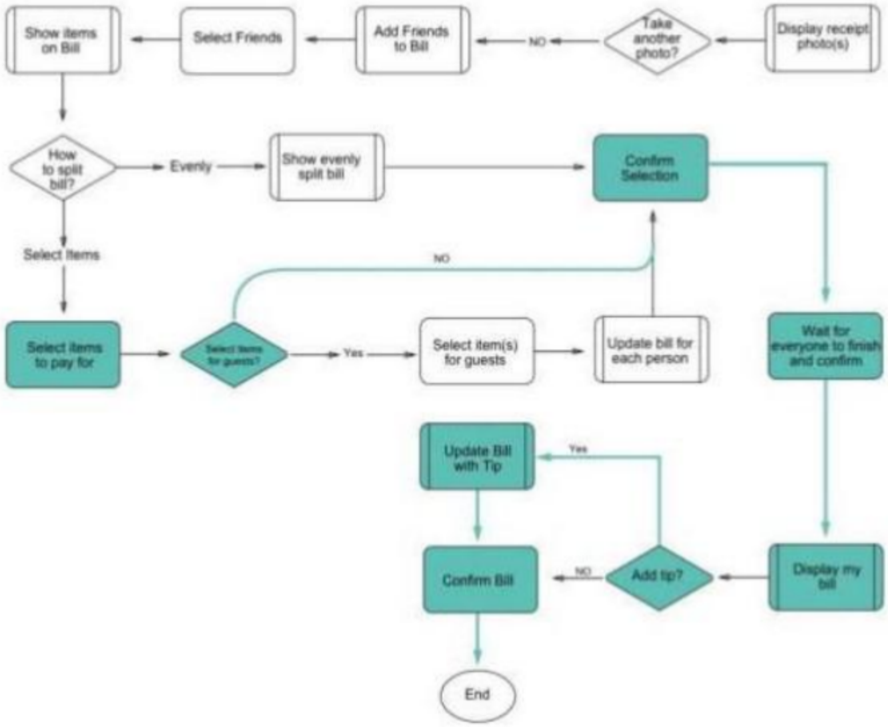
The Proof of Stake or PoS algorithm emerged as an alternative for PoW. Therefore, it is reasonable to find similar objectives for PoS and PoW. However, both the consensus algorithms have certain fundamental differences and features, especially related to the validation of new blocks on the blockchain network.

The Proof of Stake algorithm features a mechanism that enables the validation of blocks according to a stake of network participants. Rather than running hash functions, PoS algorithms for blockchain security involve staking resources in the form of tokens or digital currency. Subsequently, it involves the random selection of validators for all blocks from the stakeholders. The amount of computational power allocated to the stakeholders helps in determining the validators. Interestingly, every PoS system could ensure different ways for implementation of the algorithm. However, it involves a random selection process focused on a node's allocation and the allocation for determining the commitment of parties in ensuring transaction. Ethereum blockchain utilizes the PoS algorithm for achieving better scalability and limited electricity usage

CHAPTER 4: TECHNOLOGY STACK

(i) React.js
(ii) Node.js
(iii) Blockchain
(iv) MongoDB
(v) HTML
(vi) CSS
(vii) Javascript

CHAPTER 5: ER DIAGRAMS



CHAPTER 6: CONCLUSION

1. Publish the full-stack web application on AWS.
2. Publish research work on Blockchain.

REFERENCES

- A Review of Blockchain Technology and its Applications in Business Environment: https://www.researchgate.net/publication/334615432_A_Review_of_Blockchain_Technology_and_Its_Applications_in_the_Business_Environment
- Fair cost of Bitcoin Proof Of Work : https://www.researchgate.net/publication/304781623_The_Fair_Cost_of_Bitcoin_Proof_of_Work
- Performance Evaluation of Permissioned Blockchain : https://ieeexplore.ieee.org/document/9411380
- Google scholar: https://scholar.google.com/
- Wikipedia: https://www.wikipedia.org/
- MyLoft : https://www.myloft.xyz/
- Science Direct: https://www.sciencedirect.com/
- Research Gate: https://www.researchgate.net/