Secure Transaction Commitment in Peer-to-Peer (P2P) Processes

RASHMI PRABHAKAR SARODE

A DISSERTATION

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

IN COMPUTER SCIENCE AND ENGINEERING

Graduate Department of Computer and Information Systems
The University of Aizu
2021

The thesis titled

Secure Transaction Commitment in Peer-to-Peer (P2P) Processes

by

Rashmi Prabhakar Sarode
is reviewed and approved by

Chief referee

Senior Associate Professor
Yutaka Watanobe — Yutaka Watanobe 渡部

Professor
Alexander Vazhenin — Alexander Vazhenin

Professor
Shigaku Tei — Shigaku Tei 程

Associate Professor
Maxim Mozgovoy — Maxim Mozgovoy モズゴヴォイ

Professor
Subhash Bhalla — Subhash Bhalla サバシュ バーラ

The University of Aizu

2021

This thesis is dedicated to My Parents

Table of Contents

List of Figures

List of Tables

Acknowledgements

At the outset, I would like to express my deep and sincere gratitude to my advisor Professor Subhash Bhalla for the continuous support and encouragement throughout my doctoral research endeavour for the past three years. His guidance helped me in all the time of research and writing of this thesis. His manner of requiring his students to independently develop and solve problems has allowed me to learn more than I could have dreamed and has made this endeavour a truly enjoyable and rewarding experience.

I am extremely grateful to my second supervisor, Professor Yutaka Watanobe for his invaluable advice, continuous support, and patience during the last year of my doctoral programme. His immense knowledge in visual programming, data mining, visual queries, e-learning systems and plentiful experience have encouraged me in all the time I have spent in my academic research and even in my daily life. He always suggested some points so that I can improve my research.

Besides my advisors, I would like to thank the rest of my thesis committee members not only for their insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

I would also like to thank Prof. Wanming Chu, Assistant Professor of our Department who helped me in SQL queries and assisted me in all TA sessions of her subject. Her help in my understanding UML diagrams and few algorithms is very much appreciated.

I would also like to thank my fellow lab-mates, Dr. Shashank Shrestha and Mr. Manoj Poudel for their friendship and their willingness to help me in those areas in which their expertise surpassed mine. Mr Poudel has helped me greatly and been a source of knowledge with real world programming skills, specifically in Python.

Some special words of gratitude go to my friends who have always been a major source of support when things would get a bit discouraging: Miyuka Nakamura, Yuhan Peng, Agnes Leung, Lyu Yan, Divij Gurpreet Singh, thank you everyone for always being there for me.

I would like to thank all the administrative and technical staff members of the University who have been kind enough to advise and help in their respective roles. In particular, I am grateful to officials from Student Affair Division and Personal Foreign Advisor section for their assistance in banking work and passport/visa work. I gratefully acknowledge the financial support from JASSO, the Japan Student Services Organization by awarding me a JASSO fellowship from October 2019 to March 2020. I am also thankful to JASSO for Emergency Student Support (Manabi Benefit) in July 2020. I am grateful to the Japanese Government for financial assistance under the Japanese Prime Minister Relief Fund in June 2020.

I would also like to thank my maternal Grandparents who are no more but always encouraged me to follow my dreams.

Finally, I would like to thank my parents who raised me with a love of science, encouraged and supported me in all my pursuits.

Abstract

In distributed systems, transaction management is not very efficient and is very time consuming. Transactions are slow in two-phase commit in distributed system based on Cloud and Mobile Cloud. To make transactions efficient and faster, a peer-to-peer transaction model on blockchain using distributed ledger technologies was proposed to support distributed transactions. In Blockchain, a peer-to-peer system uses smart contracts for transactions and has no third party interference.

Smartphones and their applications are increasing gradually and the security mobile cloud computing has become an important issue. Any kind of application or software has to access the database present on the cloud in a secure manner. There are various kinds of risks in both cloud computing and mobile cloud computing. These risks include unknown data location, data recovery in case of failure and privileged user access in case of cloud computing. The risks in mobile cloud computing are service availability, limited energy bandwidth and issues in mobile terminal. The list of security risks is very large and to overcome these risks a security model was proposed. Any application or software can use this model to store, secure information and validate the information.

Blockchain consists of networks of successive blocks that are interconnected to each other by references to their former block which form a chain. Blockchain Technology creates a database like support by creation of digital ledgers, in order to support distributed transactions. The adoption of blockchain in real-world applications poses many challenges. This study aims to understand the method, its characteristics as well as the implementation concepts of transactional systems in terms of distributed transactions over web resources. The study also examines the current trends and issues in the use of blockchain in many large-scale public utility applications in e-commerce.

To make transactions efficient and faster, a peer-to-peer transaction model on blockchain using distributed ledger technologies was proposed to support distributed transactions. Here a single transaction involves two pairs of nodes and the rest of the nodes can do their transactions pairwise and independently. This is a more efficient way as it saves time compared to the two phase commit in distributed system. Thus, transactions in distributed system can be efficient and be secured using blockchain.

Chapter 1

Introduction

1.1 Distributed Systems

Distributed system entitles resource sharing which includes software of the systems connected to the network. Each entity (system) is comprised of concurrent component, communication network and synchronization mechanism and is equipped with processors in its own memory and is connected with one another through distribution middleware. The distributed system operates through a distributed program. This can be illustrated through instances such as internets, intranets, email and World Wide Web, Telephone networks, network of branch office computers, real time process control such as aircraft control systems, electronic banking, airline reservation systems and sensor networks to name a few. Parallel processing, distributed artificial intelligence and distributed database systems are other instances of distributed systems [1].

The attributes of distributed ledgers include resource sharing, transparency, concurrency, scalability, fault tolerance and openness. Distributed systems evolved in 1970s with the advent of Ethernet and Local Area Network, which operated with local IP address and messages were exchanged among computers and systems. This gave rise to peer-to-peer systems which comprised of emails and internet and they came to be known as huge expanding distribution systems. Telephone networks were early examples of peer-to-peer systems, which continue to grow as complex form of distributed systems. While airlines use distributed systems as flight control systems, taxi rentals employ them to dispatch orders. Logistics and e-commerce use distributed systems for real time tracking needs [1].

Distributed systems have mainly two types of architectures: Client-Server Architecture and Peer-to-Peer Architecture [2].

1.1.1 Client-Server Architecture

The most popular type of network architecture used in data communications is the **client-server model**. A client is a system or program that requests the operation of another system or program known as server to perform specific tasks. . A server is a system or program that accepts requests from one or more client systems or programs to perform tasks that enable the client to perform certain tasks. The

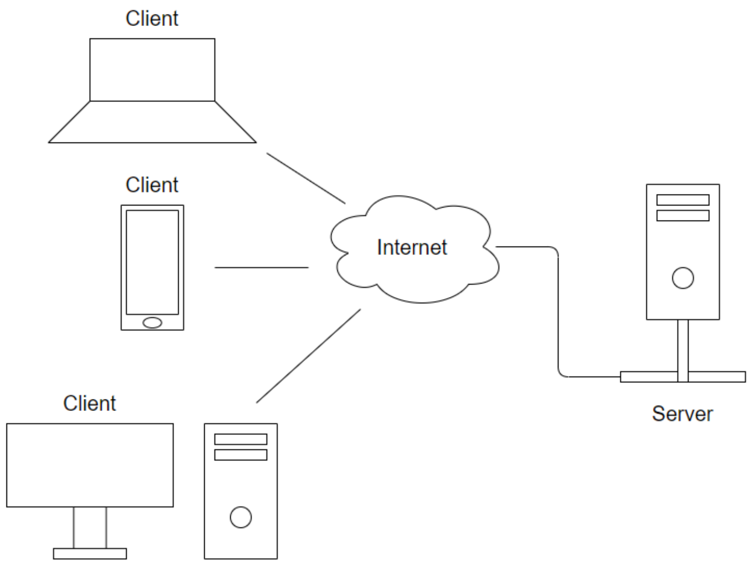

Figure 1.1: Client-Server Architecture

PC (Personal Computer) or workstation is typically the client in a client-server environment. The definition of the client-server functionally distinguishes the execution of a work unit between the operation initiated by the end user (client) and the resource responses (services) to the request for the activity. Client-server is a cooperative processing application in which the end-user communicates with the computing environment through a programmable workstation running some portion of the application [3]. Figure 1.1 depicts the client-server architecture.

1.1.2 Peer-to-Peer Architecture

It is a widely used architecture for computer networking in which the resources and roles of each workstation or node are the same. The classic client/server architecture, in which some computers are devoted to serving others is frequently compared and contrasted. Peer-to-Peer may also be used to refer to a single software application configured to function as a client and server with the same roles and status as each instance of the program. Peer-to-Peer architecture is often referred to as a peer-to-peer network [4]. This is depicted in Figure 1.2.

Peer-to-Peer systems allow users to share resources in their own computers and access resources in other computers. In absence of centralized management, all computers are considered equal in peer-to-peer systems. Almost all desktop operating systems accommodate peer-to-peer system, which fulfills need for collaboration. It also has advantages such as being immutable, scalable and faster file sharing capacity whose speed is directly proportional to increase in number of peers. It saves the expense of setting up a server. Besides, it minimizes the need for technical staff, enhances file retrieval and maintains files online [6].

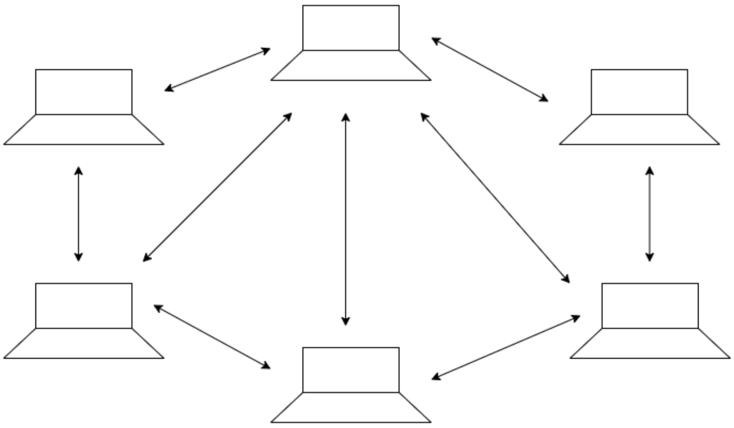

Figure 1.2: Peer-to-Peer Architecture [5]

1.2 Data Security

Mobile cloud security faces a plethora of threats including identity privacy, data security, virtualization security, portioning and offloading security, mobile cloud applications security, mobile device security, data privacy and location privacy. The capacities of mobile computing are challenged by resource constrained mobile devices. Mobile computing can be enhanced by merging it with cloud computing which gives rise to mobile cloud computing [7].

Presence of high profile hacking cases has insisted business owners to ensure data security. Data is safe in cloud since cloud services prioritize security in their storage services. Storing data in remote locations in on-site or off-site locations are susceptible to local disasters which are averted in cloud security. Cloud anti-virus and cloud backup fit are important for cloud security. Security breaches could be external such as hacking or internal like treacherous staff or human errors. Anti-virus protects the cloud information from hacking and cloud backup restores latest backup information when human errors occur locally. However cloud computing is susceptible to risks such as compliance violations, identity theft and malware infections [8].

Cloud services are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Data security is enhanced by control features such as authentication, access control, backups and recovery, encryption, data masking, tokenization, deletions and erasure. The security measures must confront threats before they reach the data centre to avoid issues such as data loss and malware infection besides facing legal and compliance issues. Data stored in clouds are encrypted or scrambled, thus making it almost impossible for offenders to access information. Cloud service providers run security updates regularly and employ artificial intelligence to handle initial level security analysis which in turn uses inbuilt algorithms to track security breaches and any vulnerability regarding the same [9].

Firewalls, based on hardware or software, confront traffic approaching a network and halt suspicious ones at the entry point thus checking possibilities of slipping in malware or virus content. Third-party security testing is one option where cloud providers hire human resources to test presence of offenders in servers and software. Precautionary measures including data encryption, data backups and two-factor authentication enhance data security [10].

1.3 Blockchain Technology

Blockchain is a method of recording information in distributed or duplicated ledger of transactions to ensure safety from alterations, hacking or any other manipulations. Besides being distributed, blockchain is characterized as immutable, time-stamped, programmable, secure, and anonymous. A blockchain is simply a distributed digital record of transactions that is replicated and distributed throughout the blockchain's complete network of computer systems. Each block on the chain comprises a number of transactions, and whenever a new transaction happens on the blockchain, a record of the transaction is added to the ledger of each participant. Distributed Ledger Technology (DLT) is a term that refers to a decentralized database that is controlled by numerous members [11].

The term ”blockchain” refers to a form of distributed ledger technology in which transactions are recorded using an immutable cryptographic signature known as a hash. This implies that if a single block in a chain is altered, it is immediately evident that it has been tampered with. To damage a blockchain system, hackers would have to modify every block across all distributed copies of the chain. While blockchain is the technology that supports the cryptocurrency Bitcoin, it is not the only distributed ledger system implementation on the market. Several other cryptocurrencies exist, each with its own blockchain and distributed ledger design [11].

A blockchain, in its simplest form, is a distributed database connected through a peer-to-peer network. It utilizes a chain of continually expanding blocks to store data (similar to a traditional public ledger, which lists all transactions) and protect it against manipulation and alteration. A block in the blockchain has exactly one parent block. The genesis block is the initial block in a blockchain that does not have a parent block [12].

1.4 Transactions

A transaction is a business event where supplier, seller or employee is paid or payments are received. Transaction is base of accounting records which are entered in general ledgers [13]. A transaction consists of a series of activities that in the database system constitute a single logical unit of work and move the database from one coherent state to another [2].

1.4.1 Transaction Management in Distributed Systems

Transaction management in distributed systems ensures that problems related to consistency in the distributed database and failures are effectively met, amidst the presence of local and global transactions. These problems are confronted with distributed commit protocols, distributed concurrency control and distributed recovery methods [14].

When a transaction is successfully completed, the database moves from one state of continuity to another. This continuity must be maintained regardless of whether transactions are executed successfully at the same time or whether there is a mistake during execution. A transaction is thus a unit of coherence and reliability. Reliability refers to both a system's resistance to different kinds of failure and its ability to recover from them and when failures stop, a resilient system continues its normal execution. A recoverable database management system still holds the database in a consistent state either by going back to a previous consistent state or after different forms of failures by moving forward to a new consistent state [2].

In a database system, transaction management tackles the problems of ensuring the integrity of data amid system failures and concurrent access to data. The fundamental distinction between a query and a transaction is the basic characteristics of a transaction: atomicity and durability.

How does Peer-to-Peer work?

A Peer-to-Peer framework is in essence, maintained by a distributed user network. Typically, since each node keeps a copy of the files, they have no central administrator or server - serving both as a client and as a server to other nodes. Thus each node can download or upload files to files from other nodes. This is what separates Peer-to-Peer networks from the more conventional client-server systems where files are downloaded from a centralized server via client computers. The connected devices on Peer-to-Peer networks share files that are saved on their hard drives. Using software applications designed to mediate data sharing, users can find and import files by querying other devices on the network. They can then serve as the source of that file until a user has downloaded a given file.

In other words, they download files from other network nodes while a node functions as a client. But they are the source from which other nodes will download files while they are operating as a server. However both functions can be performed at the same time in operation (e.g., downloading file A, and uploading file B). Peer-to-Peer networks tend to be faster and more effective as their user base grows greater, as every node stores, transmits and receives files. Also, their distributed architecture makes cyber attacks very vulnerable to Peer-to-Peer networks. Peer-to-Peer networks don't have a single point of failure, unlike conventional models [15].

1.4.2 Transaction Commitment

In a distributed system, the transaction manager should communicate the decision to commit to all servers in the different sites where the transaction is being processed and enforce it consistently. When each site's processing is complete, it moves to the partially committed transaction state and waits for all other transactions to reach their partially committed stages. When it receives notification that all sites are ready to commit, it begins committing. Either all sites commit or none of them do in a distributed system [16].

Distributed commit protocols may be one-phase commit, two-phase commit and three-phase commit. One-phase commit is simplest protocol which comprises a controlling site and numerous slave sites. The slave sites send a 'DONE' message to the controlling site after each complete transaction at local level. They further wait for 'Commit' or 'Abort' message from the controlling site. The waiting phase is termed as 'window of vulnerability.' After receiving 'Done' message from each slave, the controlling site makes a decision to 'commit' or 'abort' in a point which is known as 'commit point' and sends message to all sites. Slave sites upon receiving the message, either 'commit' or 'abort' and send acknowledgement to controlling site [16].

Two-phase commit lessens the vulnerability of one-phase protocols. It prepares in one phase and commits or aborts in the next. On receiving 'done' message, the controlling site sends 'prepare' message to all slaves. Based on inclination to commit, slave sites send either 'ready' or 'not ready' message. After receiving 'ready' message, controlling site sends 'global summit' message to all slaves. Slaves reply with 'Commit ACK' message to the controlling site to apply for a transaction. On receiving the message, transaction is committed. In case of 'not ready' message controlling site sends 'global abort' message. On receiving the message, slave sites send 'ACK abort' message. After receiving abort message from all sites, transaction is aborted. Three-phase commit assimilates the process further where first one is prepare phase, second one is prepare to commit phase and third one is commit/abort phase [16].

Transactions in Commit Protocols

Here we discuss transactions in two-phase commit and peer-to-peer commit

1. **Two Phase Commit**
   In two-phase commit, a central site is the coordinator [17]. This guides the execution of the transaction at other locations. In the first round, each slave has a chance to abort the transaction with a ”no” response. A commit protocol is thus defined by a diagram of the state. There are four distinct local transaction states for both coordinator and slave: the initial state q, wait state w, abort state a and commit state c. The initial state is occupied by a site until it decides whether to unilaterally abort the transaction. If the location decides not to abort, it will enter the state of waiting. This is an uncertain state where there is no known outcome yet. The site can either go to commit state or abort state after the wait status. This is diagrammatically represented in Figure 1.3 [18].

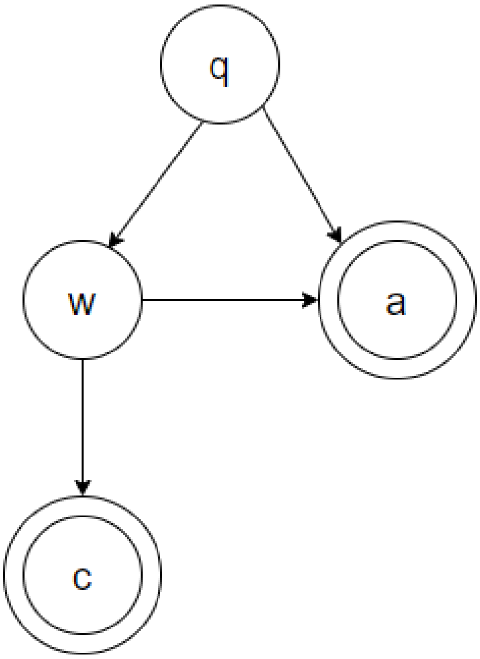

Figure 1.3: Peer-to-Peer State Diagram [19]

In two steps, the two-phase commit continues. In the first stage, the coordinator exchanges a round of messages with participants to vote on whether the transaction should be committed or aborted. In the second stage in order to commit or abandon the transaction as voted upon the coordinator exchanges another round of messages with the participants. No change is made in the data state after the second phase until the participant receives a commit message from the coordinator.

Let N = number of read-write transaction operations, and C = number of participants participating in the transaction execution.

For committing a transaction: Two phase commit needs 4C messages and 2C + 1 number of log forces

For aborting a transaction, there will be two cases

Case 1: When a site failure occurs or when atleast one participant sends a ”no” vote, a transaction may abort during execution of its operations.

4C messages (minus one for each participant who failed to vote) and 2C + 1 log forces (minus one for each participant who failed to vote) are used to abort the transaction.

Case 2: There is no vote required and only one round of 2C messages must be exchanged with C + 1 log forces [19].

2. **Peer-to-Peer Commit**

Peer-to-Peer commit will have the same stages as in two phase commit protocol and the state diagram will remain the same. Though the casting of votes is significant in a Peer-to-Peer Network and is similar to Two-Phase Commit Protocol [19].

For committing a transaction: Peer-to-Peer requires 4C messages and N + 1 number of log forces for a transaction which commits.

For aborting a transaction, there will be two cases

Case 1: Transaction Aborts before it commits. This will require C messages and N+1 log forces.

Case 2: Subordinate votes NO and coordinator aborts the transaction. This will need 2C messages and N+2 log forces.

1.5 Overview of Chapters

Chapter 2 provides a brief overview of the large amount of data growing on the web and a summary of research problems.

Chapter 3 presents a Proposed Data Encryption Security Model on Mobile Cloud and Cloud Computing Environments. The existing applications similar to the Proposed model are also discussed.

Chapter 4 gives an overview of Blockchain Technology and Peer-to-Peer Transactions. Peer-to-Peer model is proposed for faster transactions which supports blockchain. The applications of Peer-to-Peer systems are also discussed.

Chapter 5 acquaints us with Bitcoin's Lightning Network which are a set of rules built on top of Blockchain. A proposed model for additional security is discussed here. The proposed model is compared with Ethereum and Stellar Applications.

Chapter 6 compares Blockchain with other Distributed Ledger Technologies. Bitcoin's Lightning Network is also compared with other payment processors.

Chapter 7 concludes the dissertation which summarizes the current study and paves the path for future work.

Chapter 2

Motivation and Background

Owing to mobile data traffic, cloud computing traffic and huge development and adoption of technologies in Information technology and Artificial Intelligence, data is growing rapidly in terms of both volume and complexity. Every click, swipe, share, search and stream, creates data [20].

There is a large amount of data growing on the web and it can be classified into three main categories: Big Data, Open Data and Voluminous data in e-commerce.

2.1 Big Data

The term ”big data” refers to vast, varied collections of data that are growing at an exponential rate. It covers the volume of data generated and collected, the velocity or rate at which it is generated and gathered, and the variety or scope of the data points covered (together referred to as the ”three v's” of big data). Often, big data is derived via data mining and is available in a variety of formats [21].

Big data enables business firms to understand customer shopping habits and make plans to attract new ones. Retail merchants look to improve sales and enhance customer satisfaction with the aid of retail data analytics. Retail analytics plays a pivotal role to optimize pricing and to improve supply chain movement and enhance customer loyalty. The data procured helps to reveal patterns and trends in human behavior and interactions. Big data is collected through credit card transactions, IP addresses to analyze the spending habits of customers. Amazon uses customer data to recommend products based on previous purchases and searches [22].

In one instance reportedly, a California fruit packing company warned Costco about the probable listeria contamination in peaches and plums. Costco promptly emailed customers only who made the purchase instead of blanket emails to the list. Interestingly some firms use data like weather to predict sales trends. Walgreens and Pantene employed weather pattern information and increase in humidity to foresee sales in anti-frizz products. As a result Pantene saw sales in Walgreens increase by 10 per cent and Walgreens saw 4 per cent more sales in hair products category [22].

By collecting, storing and analyzing customer based big data, corporate executives effortlessly make decisions. This adds value to customer relationship management and gives the firm a winning edge. Customer analysis is also useful for product launches and to procure product ideas and this is done by thorough understanding of the customer. Customer's lifestyle and preferences including the devices that they use are analyzed so that customers can be segmented. Customer experience is another big data that enhances ecommerce. Customer experience plays a major rule in overcoming competition and retaining existing customers. Some big corporate hold customer experience as a strategy based on which they identify themselves and their product. Customer analytics include reviews, predictions, product feedbacks, competitor analysis and net promoter score [23].

As a result of the rise of Big Data, considerable research is being conducted on how to handle such heterogeneous data that is often housed in several heterogeneous data sources. This results in information/data silos, which introduce plenty of challenges in terms of discovery, integration, cleansing, and access. The astronomy domain has a plethora of diverse data. Palomar transient factory (PTF) provides the astronomical data. PTF is a series of telescopes based in San Diego, California, that monitors the Northern Sky for changes in the celestial bodies throughout time [24].

2.2 Open Data

Open data is data that is freely used, re-usable, and redistributable by anybody - with the exception of the obligation to attribute and share equally. The data must be accessible in its whole and at a fair reproduction cost, ideally by Internet download. Additionally, the data must be accessible in an easy and changeable format. The data must be made available on conditions that allow for re-use and redistribution, as well as intermixing with other datasets. Everyone should be allowed to use, re-use, and redistribute - there should be no distinctions made between fields of endeavor or between individuals or groups. For example, 'non-commercial' limitations that would preclude 'commercial' usage are not permitted, as are restrictions on use for certain objectives (e.g., exclusively in education) [25].

Open Data can help improve performance and contribute to the efficiency of public services. Increased efficiency in operations and delivery of public services may be accomplished by cross-sector data exchange, which can offer an overview of wasteful spending. The economy may gain from improved access to information, content, and expertise, which will contribute to the development of innovative services and new business models. Social wellbeing can be enhanced as a result of more transparent and accessible information. Collaboration, participation, and social innovation are facilitated by open data [26].

The economy can gain from improved access to information, content, and expertise, which will result in the development of innovative services and the emergence of new business models. New employment are produced as a result of economic stimulus and increased demand for individuals with data-processing abilities. Open Data can help improve the performance of the public sector. Increased efficiency in operations and delivery of public services is possible through cross-sector data exchange, which enables faster access to information. Due to the usage of real-time data, open data results in efficiency benefits by facilitating quick access to information that aids in individual decision-making

[26].

WHO's (World Health Organization) Open Data repository is how WHO maintains track of its 194 Member States' health-related information. The repository maintains a structured organization of the data. It may be accessible to meet a variety of needs. For example, whether it is mortality or disease burden, one can access data classified into 100 or more categories, including the Millennium Development Goals (child nutrition, child health, maternal and reproductive health, immunization, HIV/AIDS, tuberculosis, malaria, neglected diseases, and water and sanitation), non-communicable diseases and risk factors, epidemic-prone diseases, and health system [27].

To tailor the datasets to specific needs, the datasets can be filtered by topic, category, indicator, and country. The good news is that the data can be download in Excel format. Additionally, the data can be monitored and analyzed by visiting the company's data repository. Additionally, an API is available for data and statistics from the World Health Organization [27].

2.3 Voluminous data in ecommerce

Big data is used in ecommerce to predict trends, optimize pricing, forecast demand, create personalized stores, optimize customer service and generate more sales. Big Data Analytics (BDA) is used in ecommerce to enable innovation and competition in giant scale. It ushers new challenges and opportunities and has been adopted by information revolution. When the game changing value in the voluminous data is unearthed, it gives tremendous boost to sales and marketing [28].

With big data, ecommerce companies offer better services including faster shipment, personalized services and enhanced customer service. Predictive analysis assists in making tailored product offerings and shape pricings with more secure payment options [29].

The analytical powers of big data have benefited a wide variety of businesses, including e-commerce. Online suppliers provide services that enable their organizations to connect Big Data analysis tools. By enabling businesses to examine historical trends and present customer behavioral patterns, and hence provide better and more personalized goods, the usage of Big Data simplifies and enhances company performance. Through the utilization of Big Data, e-commerce firms may have access to massive amounts of data that they can use to restructure their operations and maximize income creation. Nowadays, businesses are aggressively utilizing Big Data to analyze client purchasing habits and preferences and to reorganize their offers in order to increase sales [30].

The rising popularity of the e-commerce industry is projected to necessitate massive volumes of data, therefore propelling the market's expansion. Rapid development and technological developments in the sector of e-commerce are anticipated to create new opportunities for big data applications. One of the industry's next trends is contextual and programmatic advertising, which will rely on massive data sets to find target clients. Social media platforms are currently redesigning their user interfaces to accommodate this trend. Additionally, the growing popularity of social media platforms such as Facebook, Twitter, and WhatsApp is driving e-retailers to create groups and pages dedicated to showcasing their items in order to increase their visibility to a broader consumer base [30].

Consumer tastes are always changing, necessitating product adjustments and customizations. This scenario necessitates the use of Big Data to decipher consumer behavioral patterns, allowing e-retailers to tailor their product offerings and suggestions, resulting in better interactive customer experiences. For example, coupon offers, promotional campaigns, and discounts based on prior purchase history all assist online businesses in generating significant consumer traffic and successful returns. The growing usage of big data is projected to enable e-retailers to propose items and remind customers about pending orders, resulting in increased sales and customer happiness [30].

Chapter 3

Data Encryption Security in Mobile and Cloud Computing Environments

With the growth of smartphones and applications, security has become a major obstacle to mobile cloud computing's adaptation. Any software or application, regardless of platform, must be able to securely access a cloud-based database. There are many risks in cloud computing such as Privileged user access, unknown data location, and recovery of data in case of failure. In mobile cloud computing, different kinds of risks arise such as security issues in mobile terminal, mobile network security, service availability and limited energy bandwidth [31].

A security model for mobile and cloud computing settings is proposed. This approach may be used to secure as well as store data in any application. Additionally, this information may be validated. This security approach may be utilized in apps that need online booking or chat [31].

3.1 Proposed Data Encryption Security Model

The proposed method would first use the Advanced Encryption Standard (AES) algorithm and then, use the RSA algorithm for encryption and decryption. As AES is faster than RSA in encryption, AES is used at the beginning. QR (Quick Response) Code is also used to reduce the processing time for output.

Encryption Process: The plain text will be transformed to Cipher Text by the AES algorithm in the encryption process. In the database, the cipher text created by the AES algorithm is saved. This Cipher Text is again encrypted by the RSA algorithm for security purposes and then finally translated to QR code, which is a lightweight mobile device program. Figure 3.1 illustrates the method of encryption.

Decryption Process: QR code will be converted to Cipher Text in the decryption process, which will be decrypted by RSA to another Cipher Text to be saved in the database. AES will decode this saved Cipher Text again to create Plain Text. The Decryption Process is expressed in Figure 3.2.

Two cryptographic algorithms instead of one are used to increase the security of the proposed model and QR code is also used as it becomes easier for mobile users to access a lightweight pro-

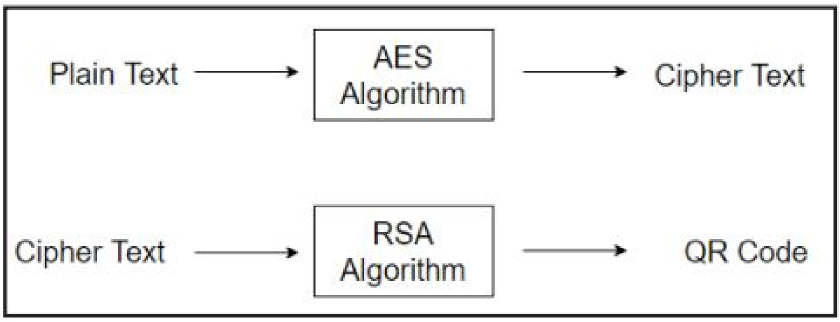

Figure 3.1: Encryption Process

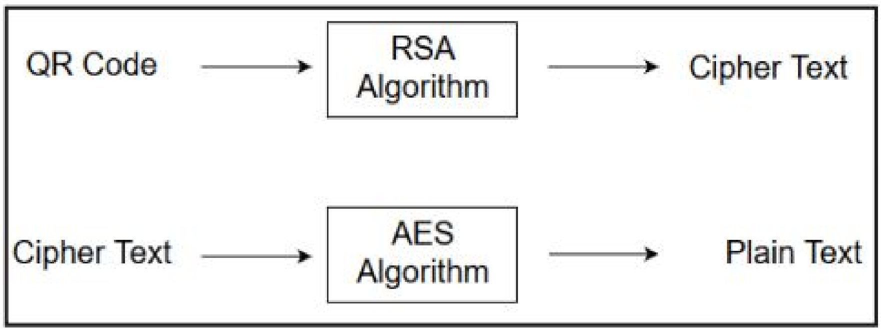

Figure 3.2: Decryption Process

gram. This system is made up of cloud framework with APIs (Application Programming Interface). This architecture can thus be combined with other systems based on the cloud.

The following benefits of the proposed algorithm exist:

- Two main security protocols, AES and RSA, are involved in the proposed algorithm. These algorithms have a very secure mechanism; therefore, there is less likelihood of an attack by brute force.
- Algorithms typically only have Cipher Text involved in their process of encryption and decryption, but here the Proposed Algorithm uses Cipher Text and QR code, which makes this algorithm much more secure.
- The proposed algorithm operates on a real-time basis, because of the RSA algorithm, the keys, namely, public key and private key, are automatically taken care of. Thus the core problem of key distribution is solved here.
- The Cyclic Redundancy Check (CRC) method ensures that no duplicate entry occurs. In the proposed algorithm, for every encryption and decryption method, we have a unique QR code generated, so the CRC definition is well used in this algorithm.
- Since QR codes can be obtained by any smartphone or handheld computer, the proposed algorithm removes the use of paper.

3.2 Demonstration of the Proposed Data Encryption Security Model

A brief demonstration of the proposed model is shown in Figure 3.3. It demonstrates the method of encryption of plain text by an AES algorithm. Later, with the help of RSA encryption, the cipher text is converted to QR code.

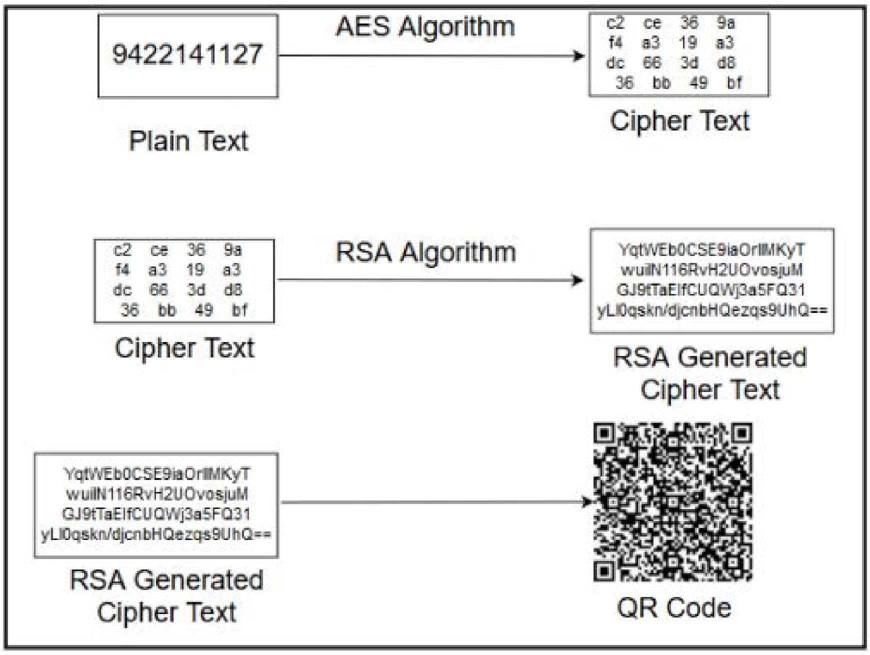

Figure 3.3: Demo of Encryption Process

The process of decryption is shown in Figure 3.4. For decryption, the QR code created by the encryption process is used. The QR code is translated by RSA decryption into Cipher Text. Then the cipher text is eventually converted by the AES algorithm into plain text.

Thus the decryption process output gives the same plain text that we used for the encryption process input.

3.3 Limitations of the Proposed Algorithm

It is possible to store a small amount of data in a QR code. We have therefore converted it into cipher text to ensure that data is safe and access to the QR code is easy. This model not only requires a user to use a smartphone, but also an internet connection.

3.4 Existing Applications Similar to that of Proposed System

Consider an application that is normally used by users to book movie tickets, such as BookMyShow. BookMyShow is an application that offers reviews of movies, movie tickets, trailers of movies, events near you, concert tickets and offers promotional events and coupons as well. This platform is developed for Indian users. The visitor books an online ticket from BookMyShow and he gets a QR Code on his email. At the entrance of a movie theatre, the visitor displays the QR code, the official scans his

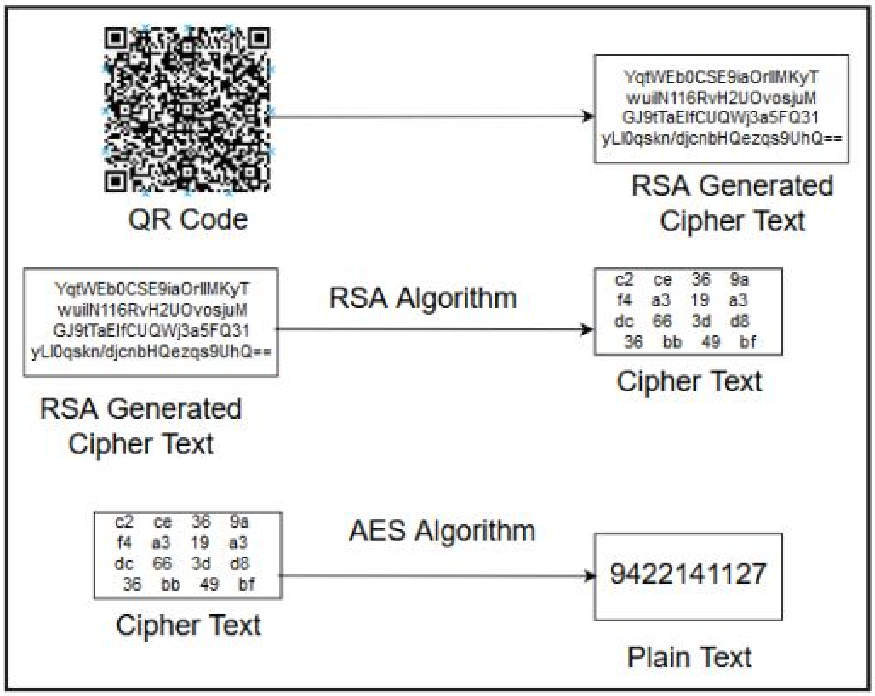

Figure 3.4: Demo of Decryption Process

QR code, and only if the QR code is validated he is granted entry, otherwise he can not enter the movie theatre. This concept is depicted in Figure 3.5.

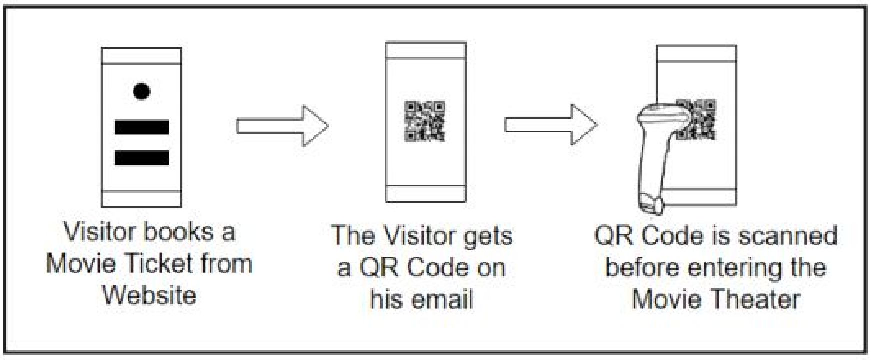
Visitor books a Movie Ticket from Website
The Visitor gets a QR Code on his email
QR Code is scanned before entering the Movie Theater

Figure 3.5: QR Code Process

A ticket is booked by the visitor and he gets a QR Code. The QR Code is saved at the backend as Cipher Text in the application framework. The scanned QR code is now converted to Cipher Text when the visitor's QR code is scanned at the movie theatre, and if this Cipher Text matches that created at the backend, the visitor is granted entry. If it does not match, the visitor is not allowed to enter the movie theater. This notion is clarified in Figure 3.6.

Take another application into consideration- IRCTC (Indian Railway Corporation of Catering and Tourism), which uses a similar method. IRCTC is the Indian Railways subsidiary which handles Indian Railways' online ticketing, catering and tourism operations. If a ticket is correctly booked via IRCTC, it generates a QR code that is similar to BookMyShow. Therefore, IRCTC QR code validation is done with a specialized application developed by IRCTC.

Take another application into account - Paytm. Paytm is a payment system for e-commerce and also a digital wallet company. Paytm is an application that was developed in India for users. With the help of Paytm, if any user wants to make any kind of payment, the user can do it with his/her Paytm QR code and he/she can pay directly to that specific user after scanning the QR code.

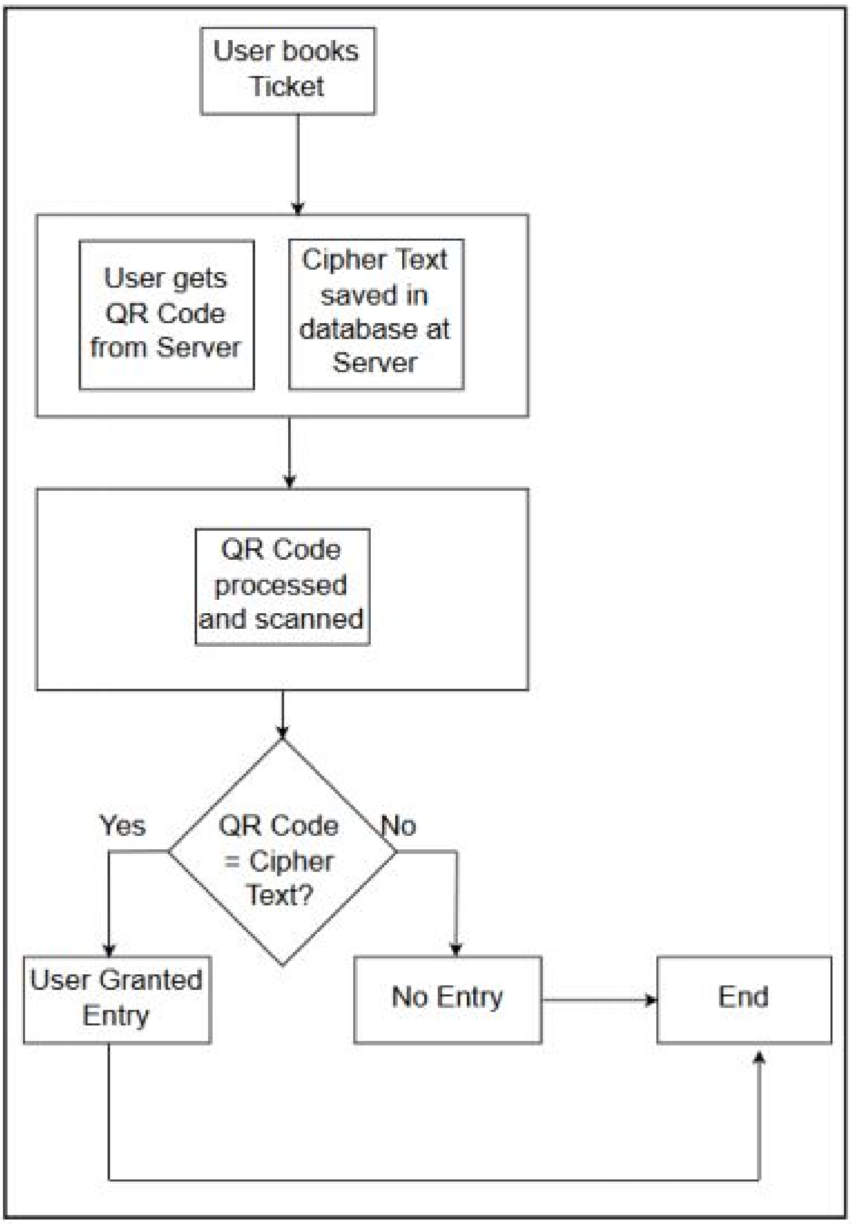
User books Ticket
User gets QR Code from Server
Cipher Text saved in database at Server
QR Code processed and scanned
QR Code = Cipher Text?
Yes
No
User Granted Entry
No Entry
End

Figure 3.6: QR Code Validation

3.5 Conclusion

There are a number of security management issues in mobile cloud and cloud computing. Various errors and bugs are encountered on a daily basis in the current scenario. These may be in conflict with the security protocols. To overcome this issue, we have proposed a data encryption model for the security of mobile and cloud computing environments. In this model, we have used a hybrid of algorithms: AES Algorithm and RSA Algorithm. QR code is also used in this proposed model for easier user access. As this system consists of cloud framework with APIs, it can be integrated with other cloud-based frameworks.

Chapter 4

Blockchain for Committing Peer-to-Peer Transactions using Distributed Ledger Technologies

A blockchain is a continuously increasing list of records (blocks) that are linked to each other and secured using cryptography. Each block is connected to the previous block and has a timestamp and details about its transaction [32]. Blockchain technology has been primarily identified in recent years for e-commerce and banking to develop digital currencies or cryptocurrencies. Bitcoin was the first cryptocurrency [33]. Blockchain can be considered as an alternative data format for storing all transactions just as an accounting ledger. A decentralized peer-to-peer system is used by Blockchain for database transaction processing. A major task of the blockchain system is the creation of digital ledgers. A ledger is a book for the financial world to keep a record of its financial transactions. In blockchain, there are ledgers that are maintained and shared between several parties and each transaction is digitally signed as a proof of authenticity. Once these Blockchain-based distributed ledgers have added entries, they cannot be deleted or modified. [34]. This is similar to a traditional database log.

Blockchain can provide data processing and secure data storage in distributed business applications [35]. Also, there is no need to totally trust one party. For example, consider an organization selling real estate to another organization by using fake ownership documents or selling the same property to multiple people. The ownership identity of an estate can be verified and authenticated by Blockchain. Blockchain security will ensure that the same real estate property is not sold to another party as the records of the property sold (in the past) are accessible to the public in the blockchain data structure [34].

4.1 Basic Building Blocks: Digital Ledger Technology

There are few building blocks in blockchain which form a digital ledger. These are explained as follows:

(i) Transaction: A transaction transfers the assets such as Bitcoin and monetary unit values from one user to another.

(ii) Blocks: Transactions are stored in Blocks (hence the name Blockchain). They form the distributed ledger.

(iii) Nodes: They are the systems running the blockchain software. There is also a special type of node called Full node. These nodes copy the entire blockchain from the start of time. These nodes will add a new transaction to the topmost block [36].

(iv) Mining: Mining is the mechanism in which transactions are validated or cleared, or in other words, are added to the block.

(v) Nonce: A nonce is a number that is used once, that is, it is used for a specific purpose and never used again. It is used to eliminate duplicate transactions where this may have detrimental effects. There is a probability that data entered in a database will also have an equivalent identifier. If a nonce is applied to the identifier, the identifier would become unique, making it impossible to unintentionally replicate it [37].

(vi) Hash Function: A hash function is a mathematical process that takes information of any size, performs an operation on it and returns a hash-like numeric value, which is fixed-size data. The resulting hash is the same size, whether the data is a single letter or a big word. Hashing is called converting a string to a signature. Hashing goes in one direction only: [38]. A hash function takes a string of any length and generates a fixed-length output, but the string cannot be recreated from the fixed-length data output [37]. In the blockchain, the hashing algorithm known as Secure Hashing Algorithm produces the digital fingerprint (SHA-256). A hash of 256-bit length is created by SHA-256 [39].

(vii) Smart Contracts: Transactions are normally intended by users and then evaluated by a set of rules known as Smart Contracts on the blockchain.

A shared replicated, permissioned ledger will have many properties. These properties are discussed below:

1. Consensus: Consensus can assist in determining whether or not to validate or approve a blockchain transaction. Two critical security parameters are guaranteed by the consensus mechanism. The process of continuously updating the blockchain between two peers (and resolving the update process), as well as the process of dealing with attackers attempting to assault the blockchain.

2. Provenance: Provenance is a sort of audit in which there is a complete record of all properties owned by people over the life cycle of the blockchain as everything is recorded on the blockchain.

3. Immutability: In blockchain, blocks are linked together which makes it impossible to modify all of the blocks once they are inscribed on the chain. This gives rise to immutability, which enhances trust in the network of companies.

4. Transaction: Transactions are normally intended by consumers and then evaluated by a set of rules known as Smart Contracts on the blockchain. If valid, then the transactions are committed on the blockchain which will make the state change.

5. Commit: It is called a commit in a standard database when a transaction is written to a database. A record of committed transactions is called an added block (new block) in a blockchain. When all the nodes around the network agree, the transactions are committed. Consensus is the basis for the rules for agreement on a specific block.

6. Transaction immutability: The blockchain ledger is a set of blocks that are related by a chain of blocks to each other. Every block has the hash of the previous block. Blockchain transactions are thus immutable [40].

4.2 Types of Blockchain

There are essentially three types of blockchains: Public, Permissioned, and Private blockchains. The main distinction between these types of blockchains is the ledger sharing mechanism and the determination of who will be participating in the blockchain system.

1. **Public Blockchains** are also known as Permissionless Blockchain. Permissions are necessary to maintain and access the distributed ledger with consensus method and to confirm the ledger's integrity. Public blockchains are decentralized and entirely transparent. Thus, any entity may join, participate in, or exit this blockchain. This system is composed of untrusted nodes. Examples include Bitcoin (2009) and Ethereum (2020). Permissionless blockchains have been used to impose P2P cryptocurrency networks on a global scale. These systems have currency aspects that are both produced and traded. Due to the lack of a central authority, this blockchain is open to participation by any node. Public transactions are used to move crypto-currency assets across identities. At any moment, computing nodes with a priori determined identities may leave or join the network [41].

2. In **Private Blockchains** ledgers are needed to be verified and shared by a predefined group of nodes. To be part of the system, the system requires that nodes should be validated or initiated. For maintaining consensus, approved nodes are responsible. For closed networks where the nodes are completely trusted, private blockchains are the best as the owner has the highest power to control these nodes, as is the case with Hyperledger [41].

3. **Permissioned or Consortium Blockchains** are hybrid blockchains that are between public and private blockchains. Some nodes are trusted, although some are not completely trusted. These systems use a network of apriori-recognized and identified computing nodes to control the blockchain. There is a copy of the ledger for every node in this blockchain. To achieve agreement between all nodes on a specific order of entries that will appear in a blockchain ledger, a consensus protocol is used. As nodes can crash or act maliciously, asynchronous fault-tolerant protocols are used to reach consensus [41].

A permissioned blockchain platform known as CAPER [42] is designed to help collaborate but may not trust each other in distributed applications. Any application maintains two sets of records: public and private. For all packages, public records are mirrored, while private records are only available on a specific service. It is designed in a way that enables transactional cross-application and internal transactions. Internal transactions within an application are conducted according to the application's logic. These transactions can make it possible to alter private data, but public data can only be read. On the other hand, cross-application transactions consist of many applications and are open to all. Service Level Agreements relate to the drift in communication between apps and clarify various service aspects. Public data can only be modified through cross-application transactions.

4.3 Consensus Algorithms

Each time a new block is added to the blockchain, all nodes should verify (which nodes have the authority to propose new blocks) and then agree on that block. The blockchain is replicated at all participating nodes. A consensus algorithm is required to add a new block to the chain. The following major types of consensus algorithms are addressed [34]:

1. **Proof of Work (PoW):** For public blockchains, this consensus is needed. There are regular changes in the participants. Any computer system can enforce the addition of more blocks. Thus an adversary who can set up several computers as nodes at low cost can resolve a majority-based strategy and this attack is known as Sybil attack [34]. To solve this, Proof of Work requires a node to crack a computationally complicated mathematical problem, and if an attacker adds several low-cost nodes to manage the majority of nodes, an attacker will not be able to do so as it would be a very costly operation.

   Thus a solution to the Sybil attack is given by Proof of Work. If the computationally difficult mathematical problem is solved by the node, then the first block on the block in the blockchain is added by that node. This is referred to as mining of the block. Typically, several user groups join to create a mining pool, work together to mine blocks, and share the revenues among the members of the party. The mining process allows computers to operate at their full capacity, resulting in a lot of electric power being consumed. PoW is therefore a resource-intensive consensus protocol [34].

2. **Proof of Stake (PoS):** This is another solution to the Sybil attack. Only those nodes can add a new block that hold the largest currency stake. Since the chain can be monitored by the largest stakeholder, with the same proportion as the stake, the probability of mining success is improved using proof-of-work. Adjusting the mining difficulty and proof-of-stake [34] to monitor the pace at which blocks are mined is taken care of. PoS can be viewed as a superior solution since costly computations do not require it. PoS has a reduced threat of attacks such as the Sybil attack as the majority (51%) of the stake can not be taken by any person.

3. **Byzantine Consensus:** The issue of the Sybil attack cannot be overcome by Byzantine consensus, although it can be used on non-public blockchains where it is possible to control nodes accessing the system. A class of algorithms known as Byzantine Consensus Algorithms chooses to add the next block to the chain. By message passing, these algorithms agree with each other. By undermining the consensus or attempting to achieve an incorrect consensus, they may tolerate some malicious nodes. [34].

4.4 Blockchain Architecture for Peer-to-Peer Transactions

Basically, a blockchain is a distributed database that has a peer-to-peer network. It has a constantly growing chain that records the data (as in the traditional public ledger where all transactions are listed) and prevents [43] from modifying and revising the data. An instance of a blockchain is represented in Figure 4.1. The block header contains the block's previous hash. One block in the blockchain only has one parent block. The Genesis block is regarded as the first block that has no parent block in the blockchain.

A single block is composed of a block header and a block body, as shown in Figure 4.1. A header block includes the following:

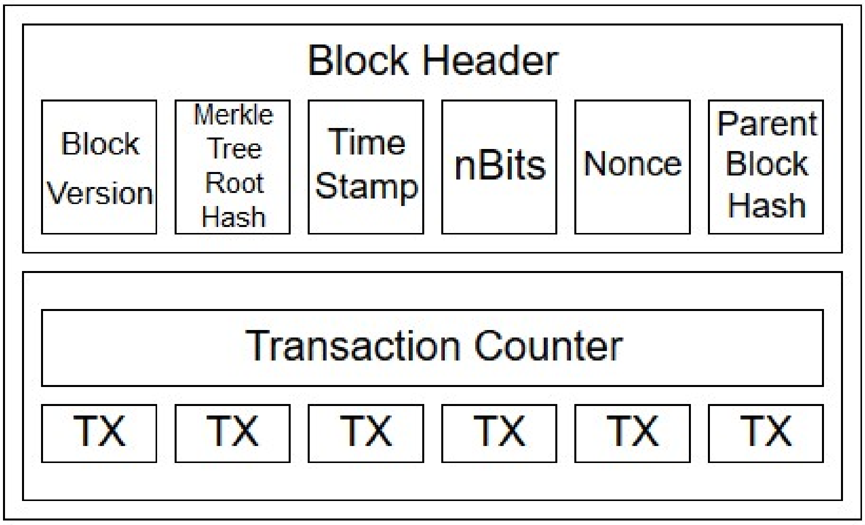

Figure 4.1: Block Structure [44]

- Block version: In order to comply with block validation, it demonstrates a defined set of rules.
- Merkle 's root hash tree: This is the hash value of the complete block transactions.
- Timestamp: The actual time in seconds (universal time from 1 January 1970).
- nBits: A valid block hash's target threshold.
- Nonce: a four-byte discipline, normally starting at zero and growing with each hash calculation.
- Parent hash block: a hash value of 256-bit which points to the previous block.

A transaction counter and transactions form the block frame. The size of the block and the size of each transaction depend on the widest range of transactions enforced by the block. As shown in Figure 4.2, a pair of values is added to the new block each time that a block is added to this chain (previous block hash, previous block pointer). If any block is tampered, it can be identified by comparing its hash to the previous block. If the hash value of one block is modified, it would also have to change the hash values of the successive blocks. With this hash-validated pointer format, the blockchain cannot be changed [34].

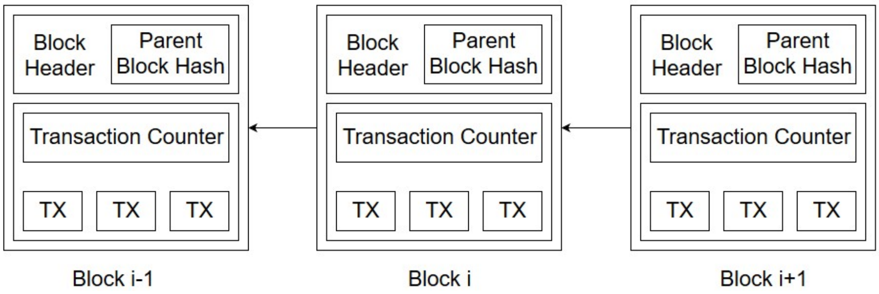

Figure 4.2: Blockchain example: sequence of blocks [44]

In addition, the chain should be distributed through many different nodes throughout the blockchain network to prevent a single node or group of nodes from being tampered with. As the blockchain is replicated across multiple nodes, to maintain the correct blockchain state, a distributed consensus algorithm is required. Decisions based on the majority of nodes are made [34]. If a group of nodes on the blockchain are managed in any way, the above method would work. This will make it very difficult for most nodes to be managed by other nodes. To verify the authentication of blockchain transactions, asymmetrical cryptography is used. Digital signatures based on asymmetric cryptography are used in untrustworthy surroundings.

4.4.1 Characteristics of Blockchain Transactions

In this section, we discuss about blockchain transaction process, peer-to-peer transactions and the associated problems in blockchain transactions.

- Decentralization: Decentralization means that unlike a centralized system, no node has central control over other nodes. The degree of decentralization is dependent on the owner's selection of nodes. Nodes are given membership status based on consortium policies. All the nodes in the blockchain preserve data so that the entire power is not managed by any single node. Permissioned blockchains mostly have fully trusted nodes and run in a trusted environment. In contrast to public blockchains, the degree of decentralization of these blockchains is greater.

- Persistence: Blockchain transactions, which are permanent, are distributed over the network. Every node manages and maintains its own records in the blockchain. As most of the nodes are benign, the persistence is maintained.

- Validity: Executions from each node in a blockchain are not necessary. Since all nodes retain the same information, transactions from other nodes can be validated in the event that any node is altered.

- Anonymity: There is a major feature of the Public Blockchain called Anonymity. A consumer may obtain multiple identities to avoid disclosure of its identity.

- Auditability: The degree of auditability depends on the three kinds of blockchains and their implementation. As all the nodes in a private blockchain are taken care of by one person, they are the least auditable. As their nodes are completely decentralized, the main auditable blockchains are the public blockchains. Permissioned blockchains are partially auditable.

- Closedness and Openness: Since public blockchains depend on public nodes for transactions, they are open blockchains, while permissioned blockchains can be called semi-open as certain nodes have to be validated until entering. Private blockchains have policy-based node selection, so the degree of openness depends on these rules. [45].

4.4.2 Blockchain Transaction Process

A blockchain is made up of [46] blocks containing transactions. A computer machine (node) requests a transaction to be added [47]. The transaction is then broadcast to other peer-to-peer networks that have several nodes. The multi-node network validates this transaction and the status of the user who requested the transaction using a valid cryptography algorithm (such as public key cryptography). When validated, the transaction is merged to create a new block on the blockchain system with other verified transactions. Using a consensus algorithm such as Proof of Work, this block is then validated. A vaildated block is then added to the current blockchain. This block is irreversible now and cannot be changed in any way possible. Figure 4.3 portrays this.

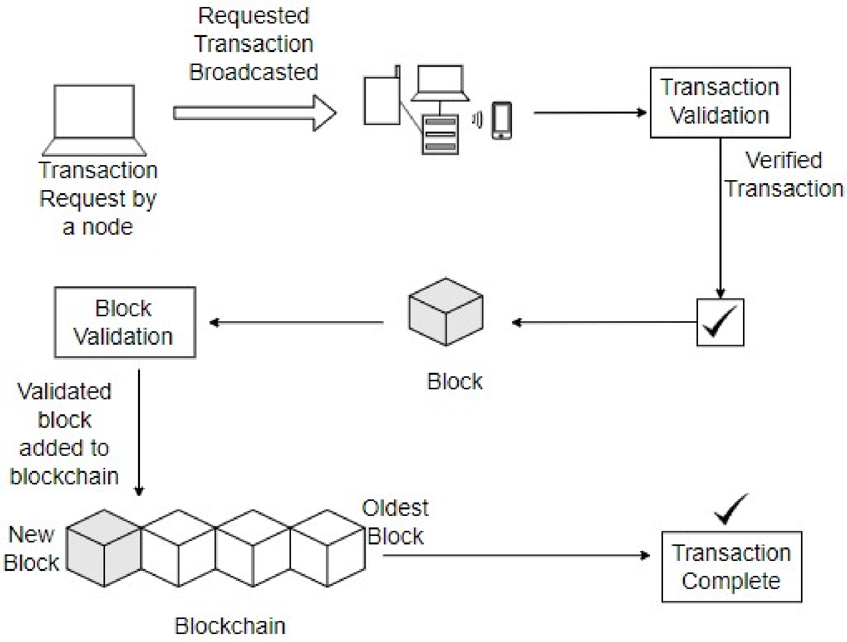

Figure 4.3: A blockchain transaction

As PoW computations are difficult to solve, the probability of two miners solving the puzzle simultaneously is low. But in the case of low probability, if more than one miner solves PoW, as shown in Figure 4.4, a fork is created in the blockchain. Serializability is breached by forks, and as transactions can clash between the two blocks, they can also trigger double-spending. Because of forks, miners are split into two groups and new blocks are mined by each group separately. Both groups of miners join the longest chain of blocks when a few new blocks are added to each of the fork branches. The other fork branch is dropped, as depicted in Figure 4.5. In the dropped blocks, transactions are called aborted and these transactions have to be sent to the network again. Due to the possibility of blocks being dropped, transactions should not be considered committed till they are buried far on the blockchain, typically six blocks deep [48].

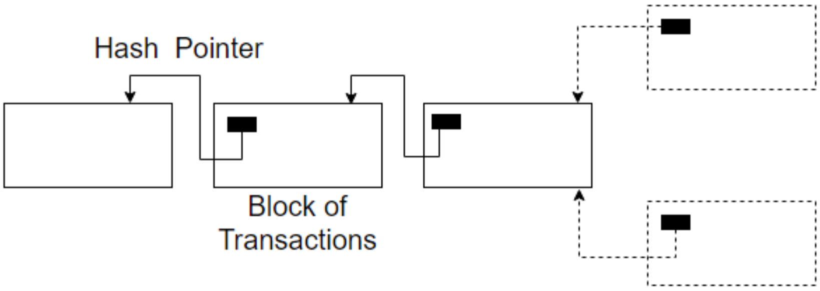

Figure 4.4: A fork in blockchain

Blocks and transactions that have to be mined in blocks are distributed in a distributed blockchain through peers who maintain a pool of new transactions. There is a validation of the transactions to be applied to the pool. If it is inside the transaction pool yet to be mined, a transaction is classified as submitted. It goes through the primary block of the chain until it is mined. When there is a confirmed depth from the main branch, a transaction is classified as confirmed. In the main chain, the confirmation depth has to be two or more mined successor blocks. The side chain or orphan block transactions are not considered to have been confirmed [46].

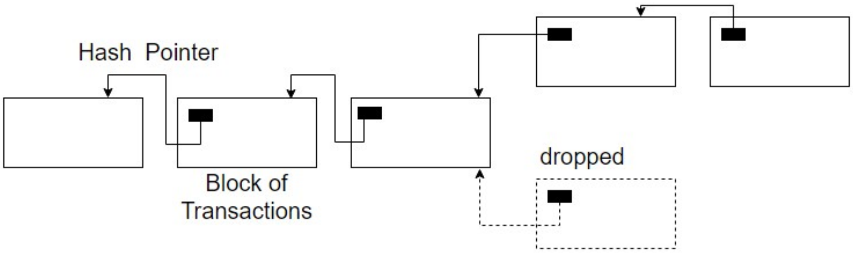

Figure 4.5: Miners join the longest chain to resolve forks

4.5 Distributed System with Peer-to-Peer Network

A peer-to-peer network contains a collection of devices which independently share and save files. Any single device or node functions as a peer [49]. In the case of the financial industry, the exchange between any two users of digital products or cryptocurrencies is called peer-to-peer over a distributed network. This platform helps buyers and dealers to conduct trades without any intermediaries being involved. Websites provide a Peer-to-Peer network in some instances that connects lenders and borrowers. The Peer-to-Peer architecture is used in most cases in distributed computing applications such as online marketplaces, live streaming platforms and web search engines [50].

4.5.1 Working of a Peer-to-Peer network

The collection includes a network of users that is distributed. As every node has a copy of all the files, there is no central authority or server. It is possible for each node to download or upload files and send them to other nodes. Each node acts as a client and downloads files from various nodes and although acting as a server, it serves as a source for downloading files from other nodes [51]. With the number of users continuing to rise, these Peer-to-Peer architectures are faster and more effective. The distributed Peer-to-Peer network structure renders them less vulnerable to cyberattacks [52].

4.5.2 Peer-to-Peer Transactions

Blockchain technology is a technique for confirming and recording transaction that does not have a centralized network. Peer-to-peer allows direct information interaction between various nodes, as in a blockchain network, each participant can keep a record of transactions through peer-to-peer transaction verification [53]

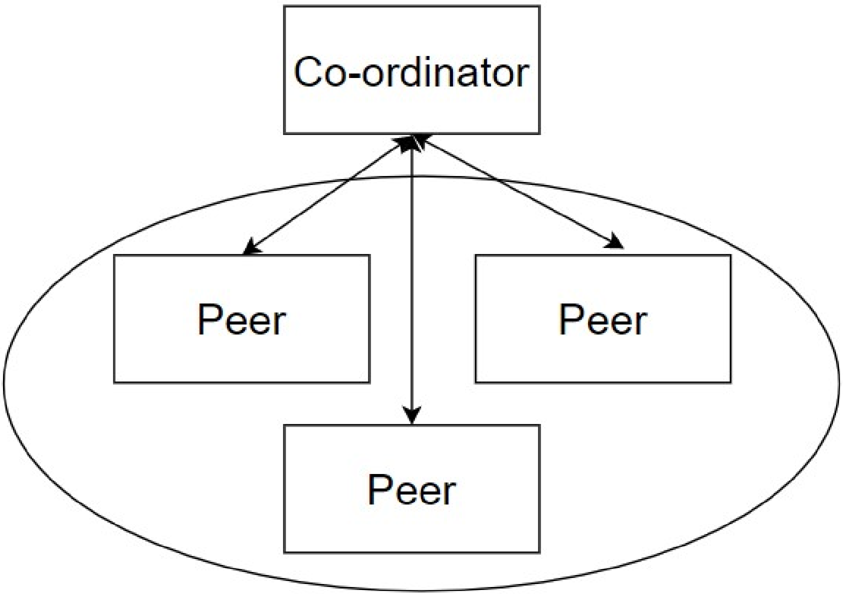

Figure 4.6: Two-Phase Commit

The key difference between two-phase commit and peer-to-peer commit is that the coordinator must wait for all participants to take the required steps to commit the process in two-phase commit, while in peer-to-peer commit, action must be taken by each pairing set of interacting nodes. The other nodes (or pairs) will separately continue their pairwise interactions as transactions. A Peer-to-Peer transaction is depicted in the Figure 4.7 and two-phase commit is depicted in Figure 4.6. Examples of Peer to Peer Trading, Car Rental and Insurance are explained in the later sections.

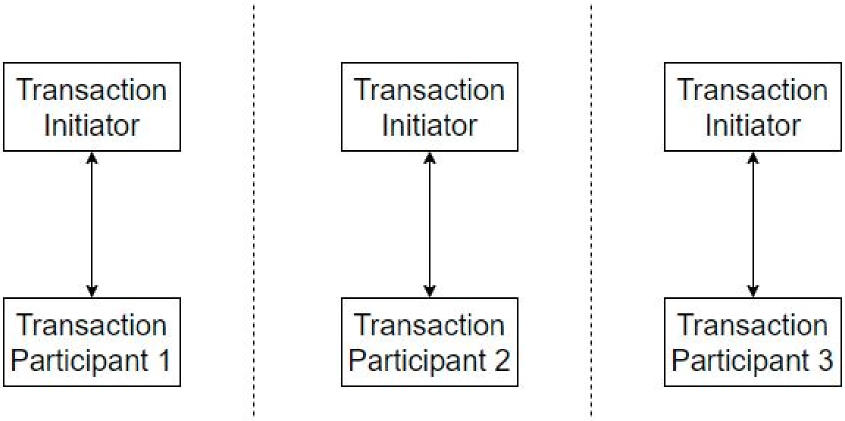
Transaction Initiator
Transaction Initiator
Transaction Initiator
Transaction Participant 1
Transaction Participant 2
Transaction Participant 3

Figure 4.7: Peer-to-Peer Commit in Blockchain

4.5.3 The role of Blockchain in Peer-to-Peer

Any transaction on the blockchain is recorded. This serves as a digital ledger. Each node has a copy of all the transactions, and to check if the transactions are correct, it compares them with various nodes. Any kind of malicious or incorrect entry is rejected by the blockchain network.

Example 1: Peer-to-Peer Trading

Trade transactions are resolved through peer-to-peer authentication using Blockchain, so there is no need for a clearing house or any central authority to validate trades or guarantee funds [54]. This removes the need for a back-office middleman. This lowers the expense of record keeping and trading platforms [53]. Peer approval of transactions also decreases the time of settlement. Blockchain just needs to make sure that the participants have cash and shares to trade. In the stock market, there is complete transparency as all the parties have all the transaction details and thus the investors' holdings.

The act of buying and selling cryptocurrencies between users without the use of a third party or intermediary is referred to as peer-to-peer trading. When you buy or sell cryptocurrencies on a traditional exchange, you do not have the option of dealing with the counterparty directly. Instead, you use charts and other market aggregators to determine the best time to buy, sell, or hold cryptocurrencies. The transaction is handled by the exchange, and the market price determines your final price at the time of the transaction. Peer-to-Peer trading allows you to have more control over who buys your cryptocurrencies and who you buy them from, as well as the pricing and settlement time. While Peer-to-Peer trading gives users more control over the process, it is important to note that peer-to-peer transactions are risky because there is no third-party to serve as a broker for the transaction. This is where an exchange like Binance comes in handy for risk-averse users [55].

Example 2: Peer-to-Peer Car Rental

In traditional car rental, the system of renting cars is highly centralised. Car rental companies need to maintain multiple cars, car rental stations, and adequate personnel to effectively handle their activities, resulting in high operating costs. There is no need to manage any personnel or facilities in peer-to-peer car rental. For car rental, the blockchain transaction is identical to a regular blockchain transaction. On a blockchain, car owners and end-users can register themselves and can sign a digital smart contract. This smart contract is the same as conventional car rental, which contains information such as information about car rental/owner, driver's license, insurance, etc. A credit card or an acquired collection of cryptocurrencies/tokens will perform all these transactions. On a distributed ledger, this mechanism is completely decentralized, so there is transparency in the transactions that eliminates the possibility of some kind of fraud. The benefits of Blockchain in the car rental system include car monitoring, repairs, mileage, fuel and maintenance [56]. This process is depicted in Figure 4.8.

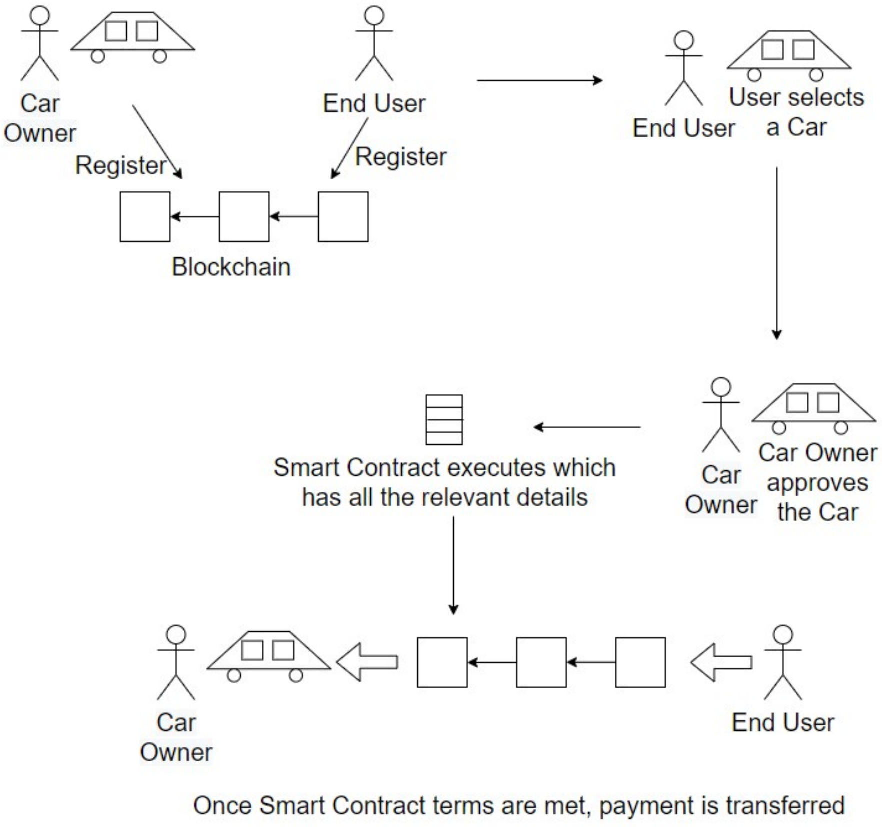
Car Owner
Register
End User
Register
Blockchain
End User
User selects a Car
Car Owner
Car Owner approves the Car
Smart Contract executes which has all the relevant details
Car Owner
End User
Once Smart Contract terms are met, payment is transferred

Figure 4.8: Car Rental in Blockchain [56]

Toyota Car Company has recently entered a coalition to use the smart car on blockchain network [57]. In order to shorten the time to establish safe and stable autonomous vehicles, Blockchain and distributed ledgers collect all data from different sources, such as vehicle owners, car companies and manufacturers. While distributed ledgers allow several different computers to keep a record of the information being exchanged, the data cannot be tampered with if one computer is compromised.

Cryptober [58], a car rental platform based on blockchain, has been proposed which is very stable and cost-optimal. Since this platform is built on a blockchain, it is tamper-proof. A security deposit provision is provided at Cryptober, which is kept locked until the ride is completed. The smart contract will also be able to monitor the entire trip and check whether the speed limit has been exceeded by any user. The smart agreement can also verify the time limit of the journey. In the event that the consumer reaches the time limit for the journey, the owner of the car will be informed instantly of the location of the car. Blockchain thus ensures high security, protection, privacy and authentication in the car rental industry.

Peer-to-Peer Car Rental in case of Toyota Car Rental is depicted in Figure 4.9. This includes only the owner of the vehicle and the end user who needs the car on rent. In the peer-to-peer car rental process, no intermediaries are involved.

Example 3: Peer-to-Peer Insurance

Peer-to-Peer insurance is an example of a business model in which individuals or economic agents come together and pool their resources for mutual aid. The most notable feature of this model is that it allows the establishment of businesses that do not require centralized authority. Blockchain technology is the answer to ensuring a safe and automated transaction environment. In the case of peer-to-peer insurance, claims would be processed automatically when appropriate conditions are met, rather than on a case-by-case basis via traditional system. Digital wallets, which are digital escrow accounts that store fixed-valued exchangeable tokens, would be used to make premium payments possible. All payments would be made using platform-specific tokens in this model, further lowering transaction costs while ensuring that no user's exposure exceeds the amount they put into their digital wallets. The blockchain technology would enable, execute, and record both the raising of claims and the payment of claims. Many non-institutional new market entrants may be able to experiment with alternative risk-sharing arrangements in the future due to the widespread availability of powerful and simple blockchain development tools. Clearly, blockchain-powered insurance models will significantly lower the entry barriers for new businesses [59]

4.5.4 Fault Tolerance in Blockchain

Blockchain Technology is based on a distributed ledger system in a peer-to-peer network in which every node is treated as equal to every other node. Even if one or two nodes are compromised on the system, as the blockchain is supposed to be Byzantine Fault Tolerant (BFT) [60], the blockchain will still continue to function. Proof of work and Proof of Stake are based on the BFT Systems [61].

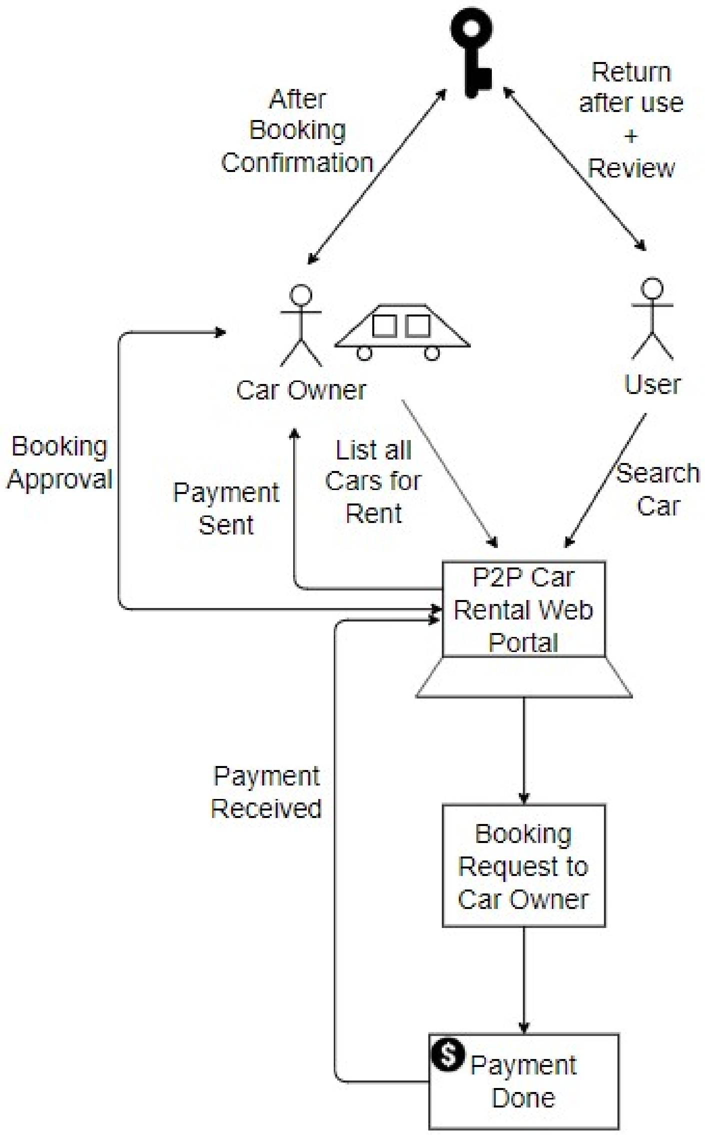
After Booking Confirmation
Return after use + Review
Car Owner
User
Booking Approval
Payment Sent
List all Cars for Rent
Search Car
P2P Car Rental Web Portal
Payment Received
Booking Request to Car Owner
Payment Done

Figure 4.9: Peer to Peer Car Rental Process [45]

4.6 Transaction Management in Distributed Ledger Technologies

There are various new applications of Blockchain Transactions. Blockchain technology can be used by all devices connected to the Internet of Things (IoT). Blockchain technology may be needed by smart cities and governments. A smart contract is a computer code that can allow easier trade for the exchange of money, property, shares, or something of value. Smart contracts are embedded digitally and the use of blockchain technology enables them to self-execute [62] when the requirements are met. Smart contracts run without any downtime, fraud, or third-party intervention using blockchain technology. Ethereum [63] offers smart contracts that can self-execute, allowing users to pay and control their assets through digital currencies. Ethereum also provides developers with decentralized software to build and deploy.

4.6.1 Identity Management with Blockchain

In many fields, Blockchain has several possible applications. Identity management is one of the most exciting prospects. It is a strategy to prove one's identity. Systems enable users to register their personal data, credit cards, debit cards, and other embedded chips that are used for identity authentication by various organizations. Identities on the blockchain can be stored. Using a decentralized app called uPort [37], consider the device based on Ethereum. According to its original developers, uPort is an open-source software project aimed at building a single global sovereign identity for individuals, corporations, organisations, computers, and bots.

Consider an instance given by Jha et. al [64]. For health records, the blockchain enables for interoperability. Metadata for health and medical events is stored on a blockchain, but the actual records are stored on a universal health cloud. Therefore, on the blockchain, only the metadata of a patient such as patientID, hospitalID, visitID and hash are stored. So if a patient goes to two separate hospitals, in the first hospital, a record will be created on the universal health cloud on the blockchain. This transaction will include metadata for the visit and URL. This transaction must be signed by the patient with his or her key. In the second hospital, for the hospital authority to read the blockchain transactions, the patient would have to provide his/her key. Through decrypting them, only the concerned authority who has the patient's key can actually read the transactions. In order to follow those orders, such as emergency contacts and insurance, smart contracts may also be coded.

4.6.2 Blockchain in Web Services and Customer Relationship Management (CRM)

The architecture for web services is supported by blockchain systems. Usually, blockchain technology is developed on top of web services.

Amazon Web Services (AWS) offers an easy way to create flexible business applications for blockchain networks and ledgers. AWS offers a completely controlled and flexible blockchain service, more convenient for setting up and implementing blockchain networks. If you need a centralized ledger database that maintains an immutable and cryptographically verifiable transaction record, or a multi-party, completely managed blockchain network that helps remove intermediaries, AWS offers purpose-built tools to meet your distinct needs [65].

Salesforce has introduced the first low-code blockchain platform for CRM (Customer Relationship Management). Salesforce Blockchain is a low-code platform that allows organizations to exchange authenticated, distributed data sets through a reliable partner and third party network. Companies can build blockchain networks, workflows and applications that offer entirely new consumer experiences by adding blockchain to the world's best CRM platform. Connectivity is now redefining how organizations work and the interactions that consumers expect. Companies need to leverage and exchange vast quantities of data with an ever-evolving network of partners and third parties to deliver this, all without losing trust. This has introduced excessive cost levels and inefficiencies. Through offering a distributed ledger that stores, traces and authenticates information across any partner or node in the network, Blockchain addresses this' trust gap.' Blockchain can be used by companies in all sectors for a range of use cases, such as asset tracking, credentialing, product verification and authentication. Companies can develop new business processes and models that cover sales, service, marketing and beyond to increase the pace of business by integrating CRM workflows with blockchain data [66]. Blockchain is now being provided on Amazon Web Services for many applications which are fast and efficient whereas Blockchain on CRM such as Salesforce helps companies create new business models which span over sales, service and marketing that speed up business [65].

Blockchain-as-a-Service (BaaS) is the process of establishing and managing cloud-based networks by a third party for businesses engaged in the development of blockchain applications. These third-party services are an emerging trend in the rapidly developing field of blockchain technology. BaaS is modeled after the Software-as-a-Service (SaaS) concept and operates similarly. It enables clients to employ cloud-based solutions to develop, host, and manage their own blockchain applications and associated activities. Simultaneously, the cloud-based service provider maintains a flexible and operational infrastructure [67].

4.7 Implementation Considerations in using Blockchains

Blockchain poses few implementation issues which are listed as follows:

1. **Blockchain implementation cost**
   Hedera estimates that it is possible to execute 10000 cryptocurrency transactions within a second. If these transactions are performed, for each transaction a state proof will be necessary. As a consequence, all time will be spent responding to queries rather than processing transactions, which may lead to reduced throughput. [68].

2. **Location of blockchain endpoints**
   Endpoints build new blocks in the proof-of-work process through the mining stage. The location where blockchain endpoints are deployed has a significant impact on the requirements for bandwidth, computation, and space. This is indeed an important architectural concern in the blockchain [69].

3. **Loss of Blockchain Key**
   A key is required to access a blockchain account. A very long combination of letters and numbers constitute the blockchain key, which makes it difficult to guess. As the blockchain key is anonymous, according to Madnick [70], nobody knows to whom the key belongs. If anyone loses the blockchain key in the blockchain, the blockchain account can never again be accessed.

4. **Non-erasable history**
   Blockchain has an immutability property that indicates that once a record is written on blockchain, it will be recorded forever. If the blockchain is used to store criminal records, and an individual wants to delete his record, it is not possible. The history of the person on the blockchain will be preserved forever. Thus, in some applications, Blockchain should not be used [71].

5. **Distributed Control Problem**
   Blockchain has several servers (nodes) running concurrently and can not be stopped, since blockchain is a decentralized framework. There is no 'on and 'off' option. Thus, if there is a software defect in any program, it may be exploited by someone with a malicious intent [71].

6. **Scalability - Growing number of users**
   Blockchain users have risen, which means there has been a rise in online transactions. This increase may lead to delays in validating the transactions. It is important to validate its foundation before authenticating the transaction [72]. Thus, blockchain needs to have better scalability than before.

7. **Security and Privacy Issues**
   Blockchain transactions are rendered open to all available users on a network. It would result in the disclosure to everyone of valuable knowledge about sensitive agencies. In this way, it is a challenge faced by blockchain [69] to provide protection and privacy to such departments. By customizing the data settings available to those specified individuals or sources only [72], such a problem can be overcome. Using a permissioned blockchain, this problem can also be solved such that only those users of the company have access to the sensitive data.

8. **Unsustainable energy consumption**
   The additional use of energy by the blockchain as it works on certain tasks which require complex scientific calculations for business validation, is another challenge faced by the blockchain. A solution to this issue is needed by industry standards [73].

9. **Spending Attacks Problems**
   Majority Attack [74] may be performed by hackers or usually referred to as 51% Attack is performed by groups of miners who control more than 50% of network's computing power. The attackers prevent new transactions, interrupt the payments and also manage to reverse the [74] transaction. In a Double Spending Attack [75], an individual holds the same bitcoin to be spent again for services.

4.8 Industrial Significance of Blockchain

Blockchain can help digitally and authentically monitor foods from producers to stores and consumers. The IBM blockchain platform provides end-to-end features that customers need to effectively allow, create, operate, manage and protect their own small business networks. IBM has been looking to streamline the distribution's blockchain power. IBM developed the ADEPT ('Autonomous Decentralized Peer to Peer Telemetry') platform in collaboration with Samsung, which uses components of their inherent bitcoin architecture to create a decentralized Internet of Things distributed device network.

In addition to cost savings, waste, and delays, ADEPT uses three system protocols: Bit Torrent (for Document Sharing), Ethereum (for Smart Contracts) and even TeleHash (such as Peer-To-Peer Messaging), while Blockchain is the solution for overall improvement in logistics so that errors or fraud can be prevented. Blockchain can also help to improve inventory control and more effectively diagnose issues. [76].

4.9 Proposed Peer-to-Peer Commit in Blockchain

Peer-to-Peer is a decentralized network communication model in which a group of devices (nodes) store and share files collectively, with each node acting as a single peer. Without the use of a central administration or server, Peer-to-Peer communication takes place in this network, which means that all nodes have the same power and perform the same tasks [77].

Peer-to-Peer is a technology that is based on a very simple decentralization principle. All cryptocurrencies can be transferred globally without the use of a middleman, intermediaries, or a central server owing to blockchain's peer-to-peer architecture. On Blockchain's distributed peer-to-peer network, anyone who wants to participate in the process of verifying and validating blocks can set up a node. Blockchain is a decentralized ledger that tracks one or more digital assets on a peer-to-peer network. A peer-to-peer network is a decentralized peer-to-peer network in which all computers are connected, and each computer keeps a complete copy of the ledger and compares it to other devices to ensure the data is accurate. In contrast to a bank, where transactions are stored privately and managed solely by the bank, this is not the case [77].

The main difference between two-phase commit and peer-to-peer commit is that in two-phase commit, the coordinator must wait for all participants to complete the required steps before the process can be committed, whereas in peer-to-peer commit, each pairing set of interacting nodes must always take action. The other nodes (or pairs) can continue to interact with each other as separate transactions [12].

In Blockchain, the peer-to-peer transaction is depicted in 4.10. Once the co-ordinator and peer have committed a transaction, it is broadcasted to a network of nodes, who use a consensus mechanism to verify and validate the transaction. Once a transaction has been validated, it is saved as a block, which is then added to the blockchain.

4.10 Conclusion

The blockchain enables a peer-to-peer system capable of utilizing smart contracts and smart bonds for a large number of users without the intervention of a third party. Node-to-node network transactions can be made secure through the application of cryptography. This section discusses how peer-to-peer transaction connected with blockchain are handled. It discusses blockchain technology and the impact it will have on future applications. Additionally, the major implementation issues in blockchain have been thoroughly examined. A peer-to-peer commit model is proposed that supports Blockchain.

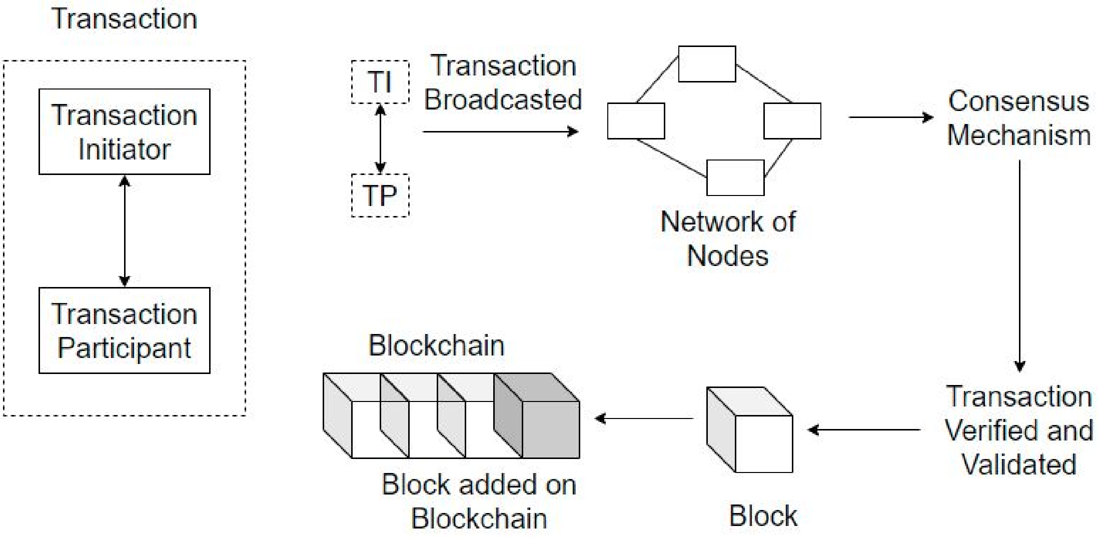

Figure 4.10: Peer-to-Peer Transaction in Blockchain

Chapter 5

Secure and Fast Transactions with Blockchain on Bitcoin’s Lightning Network

5.1 Bitcoin’s Lightning Network

The Bitcoin’s Lightning Network is a set of rules built on top of the Bitcoin blockchain that are specifically designed to facilitate micropayments. Through a routed series of transactions, this network element is capable of connecting any and all users to this ”fast and feeless” system. Payment channels are the fundamental concept of the underlying Bitcoin’s Lightning Network. If two users want to transact with each other, they open a “off-chain” payment channel on the Blockchain. Each user deposits a certain amount of money as a security deposit before opening a payment channel. This deposit must be equal to or greater than the value of the transaction. Funds can be transferred quickly to the wallets of the users that can communicate over the internet. When users are ready to wrap up their transaction, they conduct a ”closing transaction” on the main blockchain, which basically settles all of their previous transactions [78].

To avoid delaying or stealing funds from senders, recipients, and intermediaries, a blockchain-enforced contract with a payment network should be established. An HTLC (Hashed Timelock Contract) is created by creating a transaction output that can only be redeemed by the end user. The recipient first generates random data R, which is then hashed with hash(R) to produce H. This information is sent from the recipient to the sender, along with the recipient’s bitcoin address. The payment will be routed to the recipient by the sender. After receiving an updated transaction in a micropayment channel, the recipient may choose to redeem the transaction by revealing random data R details, which will eventually withdraw funds from the sender. The purpose of a Hashed Timelock Contract is to require that a message, R, be known and disclosed in order for the transaction to be broadcast on the blockchain before a specific date [79].

Consider the following scenario: there are two users, User 1 and User 2. Both users want to conduct a transaction among themselves, so they open an off-chain payment channel on Bitcoin’s Lightning Network. Before initiating the transaction, each user must deposit an amount equal to or greater than the amount of the transaction. They can begin the transactions once the funds have been deposited. The first and the last transactions are made on the blockchain. (Figure 5.1).

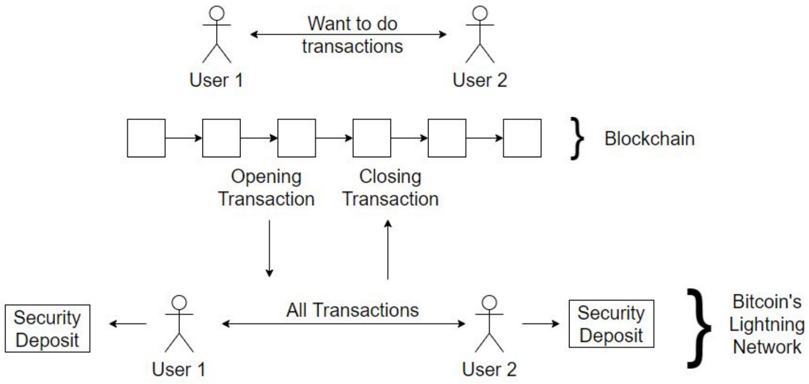

Figure 5.1: Payment Channels in Bitcoin's Lightning Network

If either user wishes to leave the payment channel, it is preferable to obtain the other user's permission so that payments can be settled and the security deposit can be withdrawn. However, if one user leaves without informing the other, the leaving user must wait for confirmation before receiving the Bitcoins. The user who is left behind will receive Bitcoins immediately. The closing transaction occurs on the blockchain [78]. Figure 5.1. depicts transaction process in Bitcoin's Lightning Network.

According to the terms of the current contract, each party may pay out in any way that the Participants desire and close the contract at any time as long as all parties agree to the contract. Infringement of the aforementioned terms will result in a cumulative liability for non-violating counterparty payment to the funds locked up in this contract [79].

If the transaction fails to reach its intended recipient, the recipient can send the same invoice back to the sender with the same hash, but without disclosing R. For the sender, this would result in the hash being revealed, but not necessarily for the recipient. R should be discarded and never broadcast by the receiver who generated the hash. If one of the channels in the path cannot be reached, the remaining channels will likely close the HTLC as unsettled, with no payment for a new Commitment Transaction [79].

5.2 Related Work

In the following sections, we will discuss Ethereum and Stellar applications.

5.2.1 district0x - Ethereum Application

The district0x network is a collection of decentralized markets and communities known as 'Districts.' Districts are the society's decentralized marketplaces that use the d0xINFRA platform. They are governed by the governance layer of the Aragon network, which is powered by Ethereum intelligent contracts and structured front-end libraries (d0xINFRA). Internet users will be able to deploy districts to the network for free indefinitely. The word district0x is inspired by two items. The economies and neighborhoods that serve as the network's building blocks are referred to as "districts" and the prefix "0x" is used in computer science to begin hash values. Districts would be able to look completely different from one another. district0x is primarily intended for libraries, which do not have control over the visual side of things, but layers of pre-made, customized modules for optional use will be added on top of that. Certain elements are included in districts. District0x can envision almost any type of cooperative marketplace being developed as a district. If the project wishes to post lists, search/filter listings, rate or grant users credibility, and accept payments, they should be a good fit for a district [80]. district0x is depicted in Figure 5.2.

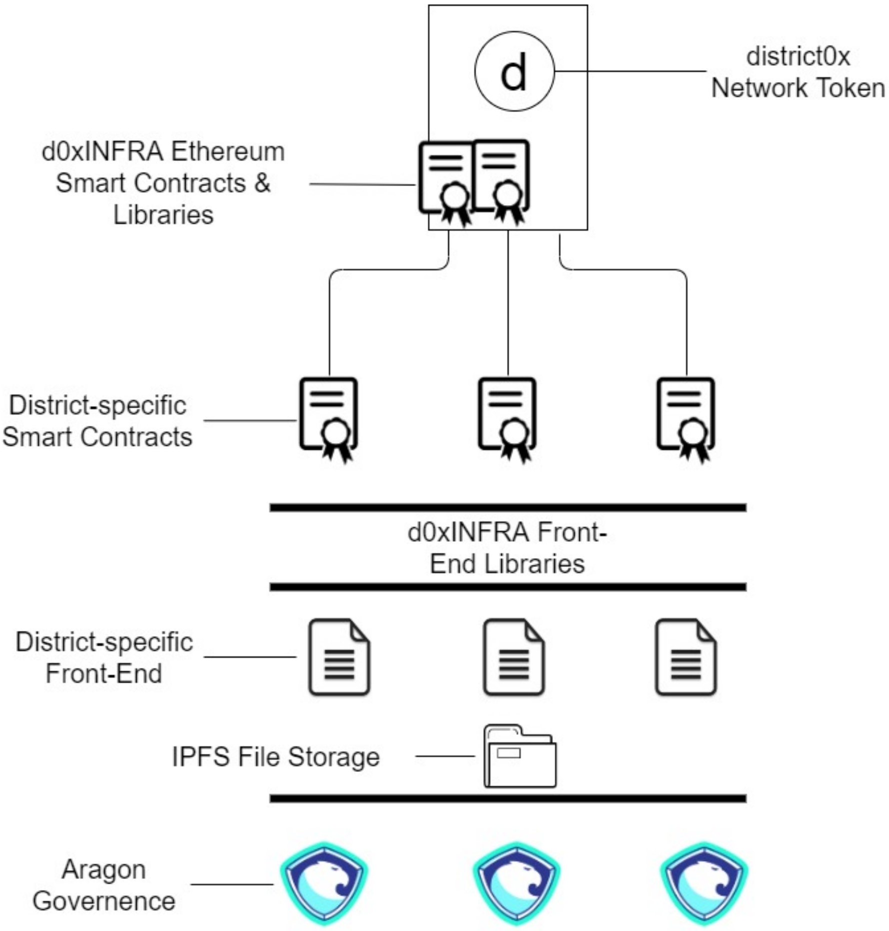

Figure 5.2: district0x [80]

district0x's key functionalities include posting and listing, searching and browsing, rating and credibility, and payments and invoicing. The district0x network addresses a number of coordination issues and inefficiencies that are common in distributed group markets. This is accomplished by providing instruments within the market participants themselves that can aid in the balance of rewards and decision-making. The ultimate goal is to create a self-sustaining environment that can thrive without the need for a central authority. d0xINFRA is a popular open-source platform made up of Ethereum smart contracts and front-end libraries. The district0x team is working on the first iteration of d0xINFRA with Name Bazaar and Meme Factory, which will allow other development teams to launch their own districts. Aragon is a ground-breaking digital medium for the implementation of invincible autonomous organizations and entities. A corresponding Aragon agency has been established to create a district on the district0x Network, where the district's administration and decision-making processes can be carried out [80].

5.2.2 Satoshipay - Stellar Application

Satoshipay [81] eliminates the need for commercials and paywalls by allowing customers to micropay for online content. Publishers embed a widget into their website, and users pay for and view information with a single click. Payments on Stellar are settled in the background, making them fast, invisible, and free (almost). Satoshipay assists publishers in embedding a Stellar wallet widget into their websites, making it easier for customers to pay for online content in small amounts. There is no need to log in, there is no need to wait, and there are no fees (virtually).

Satoshipay was constructed on Stellar for the following reasons:

1. Low Fees: Micropayments do not work with non-micro fees: you cannot transact in pennies if it costs dimes. Stellar network fees are close to nil.

2. Connection to Banks: Satoshipay users require connections to their real-world wallets in order to top up their wallets. Stellar was designed with these things in mind.

3. Speed: Having one-click access to content is useless if you have to wait for a payment to be processed. Stellar transactions are completed in a matter of seconds.

4. Scalability: As networks near capacity invariably inflate fees, micropayments necessitate a network capable of handling high transaction volumes.

5. The Built-in DEX: Online publishing has a global audience. Satoshipay relies on Stellar's ability to seamlessly transmute assets across borders and currencies to pay for content.

5.3 Proposed Secured Model

For the Bitcoin's Lightning Network, a secure model is proposed. Consider the following two businesses: Company A and Company B. Company A has four subsidiaries: a, b, c, and d. Company B has four subsidiaries numbered 1, 2, 3, and 4. Company A's main hash is stored in SHA format because it is more secure. This hash is masked into four masked hashes, all of which are in MD5 format and they are sent to sub-companies and used for integration checking. The sub-companies will use this masked hash when they interact with other companies. If the sub-companies want to interact with each other, they have their own main hash which they will convert to masked hash for transactions. Each sub-company will store the transaction data in its own database (DB = table in database) and all sub-companies' data will be saved in the master database.All these time-stamped hashes are also saved in a master database. (Master database – all transactions and hash verification data are saved; this allows for faster retrieval of all sub-companies' data) .

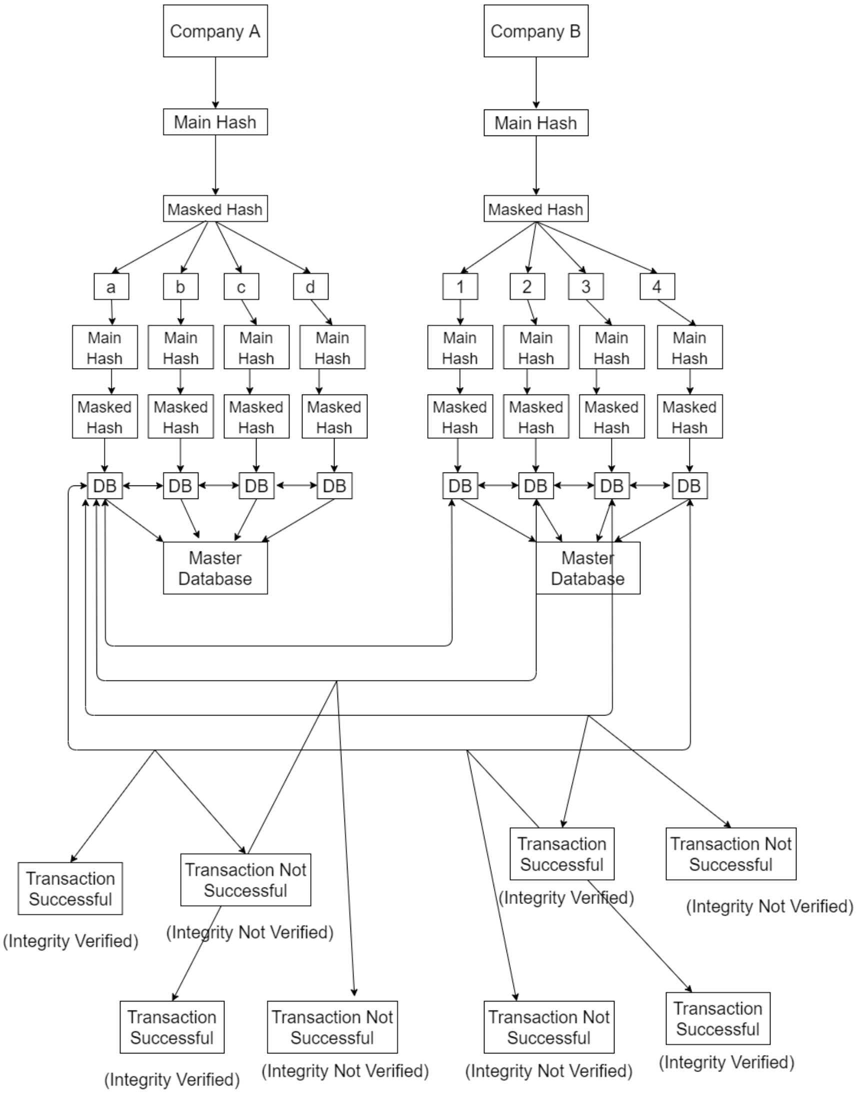

Figure 5.3: Proposed Secured Network

For a transaction between sub-companies, hashes have to be verified, if hashes are different, the integrity is verified and the transactions between sub-companies are verified. If a sub-company has to transaction with an external company, then it will use the masked hash from its parent company for transactions. Once the integrity is verified, the transaction would be considered successful. All transactions, both successful and unsuccessful, can be saved in the database so that records can be kept and transaction data from any sub-company can be retrieved quickly. Figure 5.3 shows an example of this model.

Take a look at this model in the context of blockchain. The main hash of a company can be masked on the blockchain, and transactions between sub-companies take place on Bitcoin's Lightning Network. The final closing transaction will occur on blockchain, and all subsequent transactions will be recorded on blockchain. Because it employs masked hash, the proposed work is extremely secure. It can be used to provide a high level of security in blockchain. All of the levels in this proposed system are well-checked, which aids in the transparency of each transaction.

5.4 Comparison of Proposed Model with Related Works

Instead of the original hash, the proposed model employs a masked hash. It is built on the SHA and MD5 protocols. In this model, if a transaction fails, only that transaction is rolled back and the process is restarted from the beginning. Because most transactions take place on an off-chain network, transaction speeds in this model would be faster than on blockchain. This model is scalable because the Bitcoin's Lightning Network is scalable due to hops. Many applications are built on Bitcoin's Lightning Network in order for users to trust it over other networks. The proposed application is applicable to a variety of industries or platforms, including business models, e-commerce marketplaces, and the financial industry.

Parameters	**Proposed Model**	**district0x**	**Satoshipay**
Technology	Bitcoin's Lightning Network	Ethereum and Aragon	Stellar Blockchain-based platform
Protocol	SHA and MD5 Protocol	IPFS	Distributed Consensus Protocol
Failure	Transaction Rollback	Encountering debugging issue	—
Application	Any kind of industry such as business or finance	Marketplace Applications such as Job boards or Real Estates	Micropayment for online content

Table 5.1: Comparison of Proposed Model with Related Works

district0x makes use of three major technologies: Ethereum, Aragon, and the InterPlanetary File Transfer Protocol (IPFS) [82]. district0x is currently investigating and debugging an issue in which front-end transactions fail unexpectedly [83]. One of the most common reasons people buy district0x (DNT) with a credit or debit card is to use the transaction later to pay for specific goods or services using a private and anonymous altcoin. Whether it's for groceries or crypto-specific services, cryptocurrencies are becoming a very widely-adopted, secure payment solution as time goes on [84].

Stellar is a blockchain-based platform with a growing emphasis on money transfers and payments. It differs from bitcoin in that it is based on a distributed consensus protocol in which nodes have identifiers and must be aware of one another [85]. Standard features include enterprise-grade encryption, multi-signature authorization, and ongoing software improvements [86]. This comparison is also done in a tabular format in Table 5.1.

5.5 Conclusion

Due to the off-chain nature of Bitcoin's Lightning Network, transactions are lightning fast and have low transaction fees. Due of the hops, this network is scalable and includes a wallet mechanism similar to Bitcoin. Due to the lightning-fast transaction speeds of Bitcoin's Lightning Network, it can be employed in business models, e-commerce applications, and the financial industry. For additional security, a secure business model on Bitcoin's Lightning Network secure business model is proposed, which may be applied in any e-commerce or corporate application. Except for sustained DoS attacks, Bitcoin's Lightning Network is impenetrable. A district0x Ethereum application and a Satoshipay Stellar application are explained and compared to the proposed approach.

In comparison to other cryptocurrencies and VISA transactions, Bitcoin's Lightning Network enables rapid and safe transactions. Bitcoin's Lightning Network has near-zero transaction fees and is also scalable due to hops. Thus, Bitcoin's Lightning Network is at the heart of the majority of business models and networks.

Chapter 6

Evaluation

6.1 Comparison with Other Distributed Ledger Technologies (DLT)

A blockchain is definitely not in its final form in its current form. Other distributed ledger technologies (DLT) are available that can mitigate the key problems.

1. Holochain is a business offering a new type of DLT. It provides a scalable and successful pattern of cryptocurrency that doesn't need specialized hardware or consensus. It allows monitoring per second and billions and trillions of interactions [87].

2. A permission-based ledger that uses the hashgraph consensus mechanism is the Hedera Hashgraph Platform. Around 10,000 crypto-currency transactions per second can be processed. Hedera confirms and broadcasts the transactions by using a 'gossip' protocol. Hashgraph data is 'gossiped' to a few nodes over the network (which are pre-decided) and the data is then dispatched to other nodes over the network. The gossip protocol publicises the success of transactions as PoW (Proof-of-Work) chains. Four key services, including a cryptocurrency service, a smart contract service, a file service and a consensus service, are offered by Hedera Hashgraph. The cryptographic service features an integrated time-stamping cryptographic service. Hedera Hashgraph provides all its third party apps with an asynchronous Byzantine fault tolerance mechanism. Hedera Hashgraph can host secure coins, exchanges and financial markets, or even real-time sports. Hedera Hashgraph can also be used for the encryption of a message in short-term private keys [68].

3. Tangle is a DLT, which is similar to blockchain. It has acyclic graphs that are directed - network nodes and it is not important to synchronize all participants. If one transaction needs to be carried out it is important to authorize the previous two transactions, then the Tangle is said to be correct. In doing so, Tangle merges the process of transaction with the process of consensus. Without involving any miners in it, Tangle apps will achieve consensus. With the rising number of participants, Tangle speeds up. Iota is one of its flagship apps. Iota is a project that consists of exchanging resources on the Internet of Things and promoting interoperability. At present, a

speed of 800 transactions per second has been achieved [88]. Tangle is depicted in Figure 6.1.

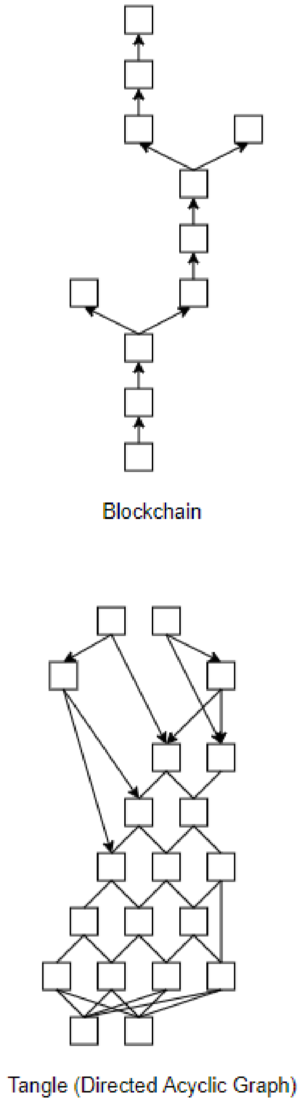

Figure 6.1: Blockchain compared with Tangle's links [88]

6.2 Comparison with other Payment Processors

As Bitcoin cannot scale due to the synchronization feature, blockchain limits the maximum number of transactions a network can process. Using off-blockchain transactions, it is possible to create long-lived networks in which an infinite number of payments can be handled locally between two users while putting no strain on the Bitcoin network.

The authors [89] fast propose a protocol for duplex micropayment networks that ensures end-to-end security and allows instant transactions, laying the groundwork for the payment service providers (PSPs) network. This Duplex micropayment channel is used to create and resolve micropayment channels. End-to-end encryption is used, and hashed timelock contracts are used to ensure that transactions between hops are only executed until the intended receiver receives its payment. Transfers on a network of duplex micropayment networks cannot be reversed, in contrast to Bitcoin, which requires a lengthy authentication process. As a result, a payment network based on duplex micropayment networks is far more suitable for real-time scenarios. Bitcoin will enable true micropayments on an unprecedented scale, with micropayments and transactions clearing in real-time, owing to a network of payment processing providers.

Due to high demand and poor scalability, average transaction times and fees in popular cryptocurrencies have recently increased, resulting in an unsatisfactory user experience. The authors [90] present RaiBlocks, a cryptocurrency with a novel blocklattice architecture in which each account has its own blockchain, allowing for near-instantaneous transaction speed, infinite scalability, and delegated Proof of Stake voting. The network requires few resources, no mining equipment, and a high transaction throughput. This is accomplished by creating a single blockchain for each account, thereby eliminating access issues and inefficiencies in the global data system. Transactions log account balances instead of transaction volumes, allowing for aggressive database pruning without jeopardizing security. The RaiBlocks network has processed 4.2 million transactions on a 1.7 GB unpruned ledger to date. Due to its feeless and split-second transactions, RaiBlocks is the leading cryptocurrency for consumer transactions.

Payment networks are the leading solution to blockchain's scalability problem. The authors [91] discuss network design from the standpoint of a payment service provider with payment fees (PSP). The optimal graphical structure and fee allocation are investigated in the context of a number of transactions in order to maximize PSP profit. If the shortest path from sender to recipient is financially significant, that is, if the path costs less than the blockchain fee, a customer will choose to route transactions through the PSP network. The PSP intends to establish an alternative payment network for consumer transfers. It is assumed that a PSP will initiate a channel between two parties without acting as an intermediary node. All parties and the PSP participate in a three-party channel funded solely by the PSP, which then lends funds to the other parties. PSP would eventually receive the money in fiat currency because it provides a credit card-like service (the risk lies to the PSP). Furthermore, the PSP only signs each new state if the payments are valid. As a result, the charge allocation is enforced on the networks. Initially, a PSP competes with the blockchain: customers will choose the alternative network only if the overall charges are lower than the blockchain. The problem can be expressed as a linear program with a tree graph structure and a PSP that supports all transactions. The authors present a polynomial time algorithm for assigning optimal charges to a path graph. If the inclusion of an extra node to serve as an intermediary for customers is permitted, the star network has proven to be an ideal solution. This means that establishing payment hubs is a nearly optimal PSP strategy. A comparison of all these related works is as shown in Table 6.1.

Parameters	**Duplex Micropayment Networks**	**RaiBlocks**	**PSP with payment fees**	**COMIT network**	**Bitcoin's Lightning Network**
Fees	Low fees	Low fees	Optimal fees	Low fees	Nearly zero fees
Transaction Speed	-	Almost Instant	-	Instant	Instant
Technology	Blockchain (off-chain transactions)	Block-lattice architecture based on blockchain	Blockchain	Super-Blockchain Network	Blockchain Network
Protocol	duplex micropayment channel protocol	Raiblocks protocol	-	Cross-chain Routing Protocol	Lightning Network Protocol
Applications	Facilitate micropayments at great scale, Real-time scenarios e.g. buying a coffee	Cryptocurrency for consumer transactions	Payment network for customers to execute transactions	Benefits Users, Liquidity Providers and Businesses	In-game micro-payments, E-commerce and E-business Applications

Table 6.1: Comparison of Bitcoin's Lightning Network with Other Networks

Chapter 7

Summary and Conclusions

In mobile and cloud computing, there are a number of security issues. Errors and bugs occur daily in the current environment and the Security protocols could be compromised. The proposed approach helps in keeping data secure in the mobile cloud. We've used two rather than one cryptographic algorithm and QR code also has been incorporated as a lightweight application which becomes easier to access for mobile users. This cloud framework features APIs (Application Programming Interface) and this system can be integrated with other cloud-based frameworks.

Transaction Management is not very efficient in distributed systems due to two-phase commit and other mechanisms. A peer-to-peer commit is proposed on Blockchain technology to make transactions efficient and more secure. As Blockchain is a distributed ledger, it organizes data into blocks chained in append-only mode. Blockchain is made up of networks of successive blocks that are linked together by references to their predecessors. These are linked together to form a chain. In order to support distributed transactions, blockchain technology creates a database-like support by creating digital ledgers. The use of blockchain in real-world applications presents numerous challenges. The implementation concepts of transactional systems in terms of distributed transactions over web resources is comprehended. The current trends and issues surrounding the use of blockchain in many large-scale public utility applications in e-commerce are discussed.

In peer-to-peer commit on blockchain, each pairing set of interacting nodes have to take action. For a set of transaction, a node/peer (coordinator) has to wait for only one node/peer (participant) to commit the transaction, the other peers can continue their pairwise interactions separately as transactions. In a blockchain network, peer-to-peer enables direct information interaction between different nodes, each participant will keep a record of transactions through peer-to-peer verification of transactions. Blockchain enables a peer-to-peer system that can use smart contracts and smart bonds for many users without the intervention of a third party. Thus, Peer-to-Peer Commit makes transactions very efficient.

Transactions on e-commerce platforms using Blockchain technology are required to face high volume of executing transactions. These systems are required to be scalable. Bitcoin's Lightning Network can be a solution to this problem as it can execute transactions and is scalable due to few hops in the network. It is an off-chain payment channel on top of a blockchain which makes the transactions secure and fast. Thus, new research efforts are needed to adopt the recent advances, in Blockchain Technology.

Bitcoin’s Lightning Network has fast and secure transactions as compared with other cryptocurrency transactions and VISA transactions. The transaction fees of Bitcoin’s Lightning Network are nearly zero and it also scalable due to hops. Thus, Bitcoin’s Lightning Network is the core of all future transactions in most of the business models and networks. A secure framework is proposed on Bitcoin’s Lightning Network for additional security. This model can be used for any kind of business, ecommerce or financial application.

Future Work can include analyzing and comparing Bitcoin’s Lightning Network with the Raiden Network (Raiden project is still in development stage). A secure application on Raiden network can be developed using registered tokens, and it can be compared with the proposed secure application on Bitcoin’s Lightning Network.

References

[1] Confluent. *What is a Distributed System, and How Does it Work?* 2021. URL: `https://www.confluent.io/learn/distributed-systems/`.

[2] Chhanda Ray. *Distributed database systems*. Pearson Education India, 2008.

[3] M David Hanson. "The client/server architecture". In: *Server Management*. Auerbach Publications, 2000, pp. 17–28.

[4] Techopedia. *Peer-to-Peer Architecture (P2P Architecture)*. URL: `https://www.techopedia.com/definition/454/peer-to-peer-architecture-p2p-architecture`. (accessed: 12.11.2012).

[5] cyberagents. *Peer-to-Peer Networks*. URL: `https://www.cyberagentsinc.com/2018/09/14/peer-to-peer-networks/`. (accessed: 2018).

[6] Codrut Neagu. *What are P2P (peer-to-peer) networks and what are they used for?* 2019. URL: `https://www.digitalcitizen.life/what-is-p2p-peer-to-peer/`.

[7] Muhammad Baqer Mollah, Md Abul Kalam Azad, and Athanasios Vasilakos. "Security and privacy challenges in mobile cloud computing: Survey and way ahead". In: *Journal of Network and Computer Applications* 84 (2017), pp. 38–54.

[8] Proband. *Cloud Computing Security*. 2019. URL: `https://www.probrand.co.uk/it-services/cloud-computing-security`.

[9] Akamai. *What are the Security Risks of Cloud Computing?* 2020. URL: `https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp`.

[10] Norton. *Cloud Security: How Secure is Cloud Data?* 2020. URL: `https://us.norton.com/internetsecurity-privacy-cloud-data-security.html`.

[11] Euromoney. *What is blockchain?* 2020. URL: `https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain`.

[12] Rashmi P Sarode et al. *Blockchain for committing peer-to-peer transactions using distributed ledger technologies*. Inderscience, 2021.

[13] AccountingTools. *Transaction definition*. 2021. URL: `https://www.accountingtools.com/articles/2017/5/15/transaction`.

[14] Wee Hyong Tok. *Distributed Transaction Management.* 2009.

[15] Binance. *Peer-to-Peer Architecture (P2P Architecture)*. URL: `https://academy.binance.com/en/articles/peer-to-peer-networks-explained`. (accessed: 2020).

[16] Tutorialspoint. *Distributed DBMS - Commit Protocols*. 2021. URL: https://www.tutorialspoint.com/distributed_dbms/distributed_dbms_commit_protocols.htm.

[17] Thirumalaisamy Ragunathan and P Krishna Reddy. "Speculation-based protocols for improving the performance of read-only transactions". In: *International Journal of Computational Science and Engineering* 5.3-4 (2010), pp. 226–242.

[18] Mei-Ling Liu, Divyakant Agrawal, and Amr El Abbadi. "The performance of two phase commit protocols in the presence of site failures". In: *Distributed and Parallel Databases* 6.2 (1998), pp. 157–182.

[19] Dale Skeen. *A quorum-based commit protocol*. Tech. rep. Cornell University, 1982.

[20] Researchandmarkets. *Big Data Analytics Industry Report 2020 - Rapidly Increasing Volume Complexity of Data, Cloud-Computing Traffic, and Adoption of IoT AI are Driving Growth*. 2020. URL: https://www.globenewswire.com/news-release/2020/03/02/1993369/0/en/Big-Data-Analytics-Industry-Report-2020-Rapidly-Increasing-Volume-Complexity-of-Data-Cloud-Computing-Traffic-and-Adoption-of-IoT-AI-are-Driving-Growth.html.

[21] Troy Segal. *Big Data*. 2021. URL: https://www.investopedia.com/terms/b/big-data.asp.

[22] Ron Barasch. *The Power of Retail Analytics*. 2019. URL: https://www.yodlee.com/data-analytics/big-data-retail-analytics.

[23] Boaz Grinvald. *5 Ways Big Data Customer Analytics Can Impact Business Results*. 2019. URL: https://www.revuze.it/blog/5-ways-big-data-customer-analytics-can-impact-business-results.

[24] Shashank Shrestha et al. "Open data integration model using a polystore system for large scale scientific data archives in astronomy". In: *International Journal of Computational Science and Engineering* 24.2 (2021), pp. 116–127.

[25] State Library of Queensland. *What is open data?* 2021. URL: https://www.slq.qld.gov.au/what-open-data.

[26] EuropeanData. *What is open data*. 2021. URL: https://data.europa.eu/en/trening/what-open-data.

[27] Hiren Patel. *These Are The Best Free Open Data Sources Anyone Can Use*. 2019. URL: https://www.freecodecamp.org/news/https-medium-freecodecamp-org-best-free-open-data-sources-anyone-can-use-a65b514b0f2d/.

[28] Linnworks. *Six ways to use big data in ecommerce (infographic)*. 2021. URL: https://www.linnworks.com/blog/ways-to-use-big-data-in-ecommerce-infographic.

[29] James Riddle. *How Will Big Data Transform E-Commerce Marketplaces?* 2020. URL: https://learn.g2.com/big-data-ecommerce.

[30] Somdutta Singh. *The Pivotal Role Of Big Data In E-Commerce*. 2020. URL: https://www.entrepreneur.com/article/353507.

[31] Rashmi P. Sarode and Subhash Bhalla. "Data Encryption Security in Mobile and Cloud Computing Environments". In: vol. 7. Springer. 2019, pp. 19–30.

[32] Ledger Leopard. *Blockchain Definition*. 2020. URL: https://www.ledgerleopard.com/technology.

[33] Weili Chen et al. “Dependence structure between bitcoin price and its influence factors”. In: *International Journal of Computational Science and Engineering* 21.3 (2020), pp. 334–345.

[34] Abraham Silberschatz, Henry F Korth, et al. *Database system concepts*. 2011.

[35] Fidel Aznar, Mar Pujol, and Ramón Rizo. “Macroscopic definition of distributed swarm morphogenesis”. In: *Connection Science* 24.4 (2012), pp. 162–192.

[36] Udemy - Abhi Singh. *Learn the secrets of Blockchain in less than an hour*. 2019. URL: https://www.udemy.com/learn-the-secrets-of-blockchain-in-less-than-an-hour/.

[37] Lynda. *Blockchain: Beyond the Basics*. 2017. URL: https://www.lynda.com/Blockchain-tutorials/Blockchain-Beyond-Basics/636127-2.html.

[38] Aakanksha Tewari and BB Gupta. “An internet-of-things-based security scheme for healthcare environment for robust location privacy”. In: *International Journal of Computational Science and Engineering* 21.2 (2020), pp. 298–303.

[39] John Barnden and Kankanahalli Srinivas. “Encoding techniques for complex information structures in connectionist systems”. In: *Connection Science* 3.3 (1991), pp. 269–315.

[40] Senthil Nathan et al. “Blockchain meets database: design and implementation of a blockchain relational database”. In: *Proceedings of the VLDB Endowment* 12.11 (2019), pp. 1539–1552.

[41] Victor Zakhary et al. “Towards global asset management in blockchain systems”. In: *arXiv preprint arXiv:1905.09359* (2019).

[42] Mohammad Javad Amiri, Divyakant Agrawal, and Amr El Abbadi. “CAPER: a cross-application permissioned blockchain”. In: *Proceedings of the VLDB Endowment* 12.11 (2019), pp. 1385–1398.

[43] Hui Huang, Kuan-Ching Li, and Xiaofeng Chen. “A fair three-party contract singing protocol based on blockchain”. In: *International Symposium on Cyberspace Safety and Security*. Springer. 2017, pp. 72–85.

[44] Zibin Zheng et al. “An overview of blockchain technology: Architecture, consensus, and future trends”. In: *2017 IEEE international congress on big data (BigData congress)*. IEEE. 2017, pp. 557–564.

[45] Fatbit. *Planning to Launch An Online Car Rental Marketplace?Website/App Features to Succeed!* 2019. URL: https://www.fatbit.com/fab/start-peer-to-peer-car-renting-portal-with-these-advanced-features/.

[46] Joerg Evermann and Henry Kim. “Workflow Management on the Blockchain—Implications and Recommendations”. In: *arXiv preprint arXiv:1904.01004* (2019).

[47] Balamurugan Balusamy and P Venkata Krishna. “Simplified and efficient framework for managing roles in cloud-based transaction processing systems using attribute-based encryption”. In: *International Journal of Computational Science and Engineering* 14.2 (2017), pp. 135–149.

[48] Sujaya Maiyya et al. “Database and distributed computing fundamentals for scalable, fault-tolerant, and consistent maintenance of blockchains”. In: *Proceedings of the VLDB Endowment* 11.12 (2018), pp. 2098–2101.

[49] Michele Amoretti and Francesco Zanichelli. "Distributed reputation management for service-oriented peer-to-peer enterprise communities". In: *International Journal of Computational Science and Engineering* 13.2 (2016), pp. 147–157.

[50] Divyakant Agrawal, Amr El Abbadi, and Subhash Suri. "Attribute-based access to distributed data over P2P networks". In: *International Journal of Computational Science and Engineering* 3.2 (2007), pp. 112–123.

[51] Willy Susilo, Yang-Wai Chow, and Rungrat Wiangsripanawan. "Protecting peer-to-peer-based massively multiplayer online games". In: *International Journal of Computational Science and Engineering* 10.3 (2015), pp. 293–305.

[52] Yonghui Dai, Guowei Li, and Bo Xu. "Study on learning resource authentication in MOOCs based on blockchain". In: *International Journal of Computational Science and Engineering* 18.3 (2019), pp. 314–320.

[53] Toshendra Kumar Sharma. *How blockchain can be used in peer to peer trading how it works?* 2017. URL: https://www.blockchain-council.org/blockchain/blockchain-peer-2-peer-trading/.

[54] Daan Bloembergen et al. "Trading in markets with noisy information: An evolutionary analysis". In: *Connection Science* 27.3 (2015), pp. 253–268.

[55] Binance. *Intro to Peer-to-Peer Trading: What is P2P Trading and How Does a Local Bitcoin Exchange Work?* 2021. URL: https://www.binance.com/en/blog/421499824684901839/Intro-to-PeertoPeer-Trading-What-is-P2P-Trading-and-How-Does-a-Local-Bitcoin-Exchange-Work.

[56] EOS Intelliigence. *Blockchain: A Potential Disruptor in Car Rental and Leasing Industry*. 2019. URL: https://www.eos-intelligence.com/perspectives/technology/blockchain-a-potential-disruptor-in-car-rental-and-leasing-industry/.

[57] Philip E. Ross. *Toyota Joins Coalition to Bring Blockchain Networks to Smart Cars*. 2017. URL: https://spectrum.ieee.org/toyota-joins-coalition-to-bring-blockchain-networks-to-smart-cars.

[58] Vikas Hassija et al. "Cryptober: A Blockchain-based Secure and Cost-Optimal Car Rental Platform". In: *2019 Twelfth International Conference on Contemporary Computing (IC3)*. IEEE. 2019, pp. 1–6.

[59] Esther Boyle. *Peer-to-Peer Insurance: Blockchain Implications*. 2021. URL: https://www.soa.org/globalassets/assets/files/resources/research-report/2021/p2p-insurance-blockchain.pdf.

[60] Min Yang et al. "Dynamic negotiation of user behaviour via blockchain technology in federated system". In: *International Journal of Computational Science and Engineering* 22.1 (2020), pp. 74–83.

[61] Demiro Massessi. *Blockchain Consensus And Fault Tolerance In A Nutshell*. 2019. URL: https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03.

[62] Vitalik Buterin et al. "A next-generation smart contract and decentralized application platform". In: *white paper* 3.37 (2014).

[63] Gavin Wood et al. "Ethereum: A secure decentralised generalised transaction ledger". In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.

[64] Anand Jha Nitesh Gupta and Purna Roy. *Adopting Blockchain Technology for Electronic Health Record*. 2017. URL: https://dokumen.tips/documents/adopting-blockchain-technology-for-electronic-health-record-.html.

[65] Amazon. *Blockchain on AWS*. 2020. URL: https://aws.amazon.com/blockchain/.

[66] salesforce. *Salesforce Introduces the First Low-Code Blockchain Platform for CRM*. URL: https://www.salesforce.com/news/press-releases/2019/05/29/salesforce-introduces-the-first-low-code-blockchain-platform-for-crm. (accessed: 2019).

[67] Jake Frankenfield. *Blockchain-as-a-Service (BaaS)*. 2021. URL: https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp.

[68] Samuel Haig. *Hedera Hashgraph — Deep Look Into 10,000 Transactions Per Second Claim*. 2019. URL: https://cointelegraph.com/news/hedera-hashgraph-deep-look-into-10-000-transactions-per-second-claim.

[69] Chun-Feng Liao et al. "On design issues and architectural styles for blockchain-driven IoT services". In: *2017 IEEE international conference on consumer electronics-Taiwan (ICCE-TW)*. IEEE. 2017, pp. 351–352.

[70] Stuart Madnick. "Blockchain Is Unbreakable? Think Again". In: *Think Again (June 1, 2019)* (2019).

[71] Meredith Somers. *The risks and unintended consequences of blockchain*. 2019. URL: https://mitsloan.mit.edu/ideas-made-to-matter/risks-and-unintended-consequences-blockchain.

[72] Divyakant Meva. "Issues and challenges with blockchain: A survey". In: *International Journal of Computer Sciences and Engineering* 6 (2018), pp. 488–491.

[73] Mirror Review. *5 Biggest challenges in the implementation of Blockchain-based ERP systems*. 2020. URL: https://www.mirrorreview.com/5-biggest-challenges-in-the-implementation-of-blockchain-based-erp-systems/.

[74] Jake Frankenfield. *51% Attack*. 2019. URL: https://www.investopedia.com/terms/1/51-attack.asp.

[75] Bojana Koteska, Elena Karafiloski, and Anastas Mishev. "Blockchain implementation quality challenges: a literature". In: *SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications*. 2017, pp. 11–13.

[76] Edvard Tijan et al. "Blockchain technology implementation in logistics". In: *Sustainability* 11.4 (2019), p. 1185.

[77] Toshendra Kumar Sharma. *Blockchain and Role of P2P Network*. 2017. URL: https://www.blockchain-council.org/blockchain/blockchain-role-of-p2p-network/.

[78] Steven Hay. *Bitcoin's Lightning Network Explained Simply*. 2020 (accessed April 4, 2020). URL: https://99bitcoins.com/bitcoin/lightning-network/.

[79] Joseph Poon and Thaddeus Dryja. *The Bitcoin Lightning Network*. 2021. URL: https://cryptochainuni.com/wp-content/uploads/Bitcoin-lightning-network-paper-DRAFT-0.5.pdf.

[80] district0x. *district0x*. 2017. URL: https://district0x.io.

[81] SatoshiPay. *SatoshiPay*. 2014. URL: `https://www.stellar.org/case-studies/satoshipay`.

[82] CoinMarketCap. *About district0x*. 2021. URL: `https://coinmarketcap.com/currencies/district0x/`.

[83] district0x. *district0x Dev Update*. 2018. URL: `https://blog.district0x.io/district0x-dev-update-october-16th-2018-71cb980d2cec`.

[84] BitDegree. *Buy district0x With a Credit Card*. 2018. URL: `https://www.bitdegree.org/crypto/buy-district0x-dnt`.

[85] Hardman. *SatoshiPay*. 2018. URL: `https://www.hardmanandco.com/wp-content/uploads/2018/12/26254_satoshipay-an-emerging-leader-in-digital-nanopayments-25.10.18-1.pdf`.

[86] Satoshipay. *Connecting the world through instant payments*. 2020. URL: `https://satoshipay.io/`.

[87] Holochain. *Holochain?* 2019. URL: `https://holochain.org/`.

[88] Patrick Schueffel. "Alternative distributed ledger technologies Blockchain vs. Tangle vs. Hashgraph-A high-level overview and comparison". In: *Tangle vs. Hashgraph-A High-Level Overview and Comparison (December 15, 2017)* (2017).

[89] Christian Decker and Roger Wattenhofer. "A fast and scalable payment network with bitcoin duplex micropayment channels". In: *Symposium on Self-Stabilizing Systems*. Springer. 2015, pp. 3–18.

[90] Colin LeMahieu and clemahieu. "RaiBlocks: A Feeless Distributed Cryptocurrency Network". In: 2017.

[91] Georgia Avarikioti et al. "Payment network design with fees". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2018, pp. 76–84.