A Permissioned Decentralized Blockchain-Based Mobile Banking System with Privacy and Security

by

A. A. Noman Ansary
18301147
Syed Nur.A.Rabbi Jim
19301275
Lamya Labeeba
18201029
Kashfia Hasan
18101716

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
September 2022

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.

2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.

3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.

4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

A. A. Noman Ansary

A. A. Noman Ansary
18301147

Syed Nur. A. Rabbi Jim

Syed Nur.A.Rabbi Jim
19301275

Lamya Labeeba

Lamya Labeeba
18201029

Kashfia Hasan

Kashfia Hasan
18101716

Approval

The thesis/project titled “A Permissioned Decentralized Blockchain-Based Mobile Banking System with Privacy and Security” submitted by

1. A. A. Noman Ansary (18301147)
2. Syed Nur.A.Rabbi Jim (19301275)
3. Lamya Labeeba (18201029)
4. Kashfia Hasan (18101716)

Of Summer, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on September 20, 2022.

Examining Committee:

Supervisor:
(Member)

Iqbal

Dr. Muhammad Iqbal Hossain
Associate Professor
Department of Computer Science and Engineering
Brac University

Co-supervisor:
(Member)

M. Monim

Mobashir Monim
Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

Dr. Md. Golam Robiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

With technological advancement in Bangladesh's FinTech, more and more security-related challenges are emerging. From, Nagad, a government FinTech company, withholding the transaction ability of their consumers due to security purposes, to consumers of mobile banking services (i.e. bKash, Nagad, Rocket etc. etc.) getting scammed through being asked by fraudulent callers for the OTP SMS pin codes sent to their mobile phones, the security breach is becoming more of a common occurrence. These breaches are occurring primarily for two reasons: (i) the consumers are not aware of the technological environment fully and (ii) the service providers have not set up any strong measure that can verify whether the transaction has been requested to be done from both of the parties. To address this security vulnerability, we propose a combination of Permissioned Blockchain with 2-factor authentication that would (i) verify the willingness of the transaction from both the parties, (ii) ensure the privacy of the willing parties and (iii) identify the consumer to be the actual owner of the account.

Keywords: FinTech; Blockchain; Mobile Banking; Data Security

Acknowledgement

First of all, we are grateful to the Almighty Allah for guiding us via His endless knowledge and for sustaining our physical and mental well-being so that we may tend to our daily duties, whether they be related to our personal or academic lives.

Second, we would like to express our sincere gratitude to our supervisor Dr. Muhammad Iqbal Hossain sir and our co-supervisor Mobashir Monim sir for helping us choose an interesting topic for our thesis, and guiding us throughout our journey of working on said topic. They offered us wise counsel and direction throughout our thesis, and we are highly appreciative of it. We appreciate that every time one of us visited either of them at their office, they were available to us and took time to address any questions or problems we had. We would also like to express our gratitude to Research Assistant Adria Binte Habib, for her ongoing help with each and every single one of our queries. With their help, guidance, and support, we were able to successfully complete our thesis.

Table of Contents

List of Figures

List of Tables

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

ATM Automated Teller Machine

BDT Bangladesh Taka

CBDC Central Bank Digital Currency

FinTech Financial Technology

KYC Know Your Customer

NID National Identification

OTP One Time PIN

PBFT Practical Byzantine Fault Tolerance

PIN Personal Identification Number

SMS Short Message Service

Chapter 1

Introduction

1.1 Background

The first introduction of Mobile Banking was in 2001 in the Philippines by two operators, Globe and Smart, the idea of sending an amount of money by text to the recipient's phone number, to meet the domestic needs of the county at ease. Since then, many other countries have adapted themselves to this idea of an easy-to-use banking service system and Bangladesh is not any different from them either. In May 2011, Dutch Bangla Bank deployed Rocket, the first-ever Mobile Banking application in Bangladesh. Along with this, bKash, Q-cash, T-Cash, UPay came eventually, making the mobile banking sector diverse, having no monopoly on a single service.

In recent times, the Mobile Banking services of Bangladesh have been a blessing, because mobile banking systems like bKash, Upay, Rocket, Nagad etc are accessible to the masses, even in rural areas. However, that does come at the cost of privacy invasion to intermediary merchants, getting scammed by people who have the mobile number with recent transaction records of that particular account number and various other methods.

Blockchain was first introduced in 2009. Satoshi Nakamoto first implements the blockchain as the public ledger for transactions by using Bitcoin. The goal of the launch was to provide an alternate form of payment that could be distributed peer to peer without the need for a central bank or authority to keep track of the ledger. And blockchain was the engine that runs the bitcoin ledger. This technology allows users to record and share a shared view of the state of a peer-to-peer system over a distributed network. Finally, bitcoin money and blockchain technology were separated in 2014. Its potential for additional inter-organizational transactions had already been investigated at this point. So it is high time to incorporate this blockchain technology in mobile banking services to give the customers a more secure and private transactional process for their banking needs and ensure a better customer experience.

1.2 Research Problem

In the currently existing system, a major issue is a fact that the merchant acting as the middle man has too much personal information. For example, if a person wants to cash out some of the money in their account, they need to go to a merchant and provide their phone number [35][33], in some cases NID too (Q-Cash), and the amount that they want to cash out. This information is recorded in the merchant's ledger, the merchant has access to the mobile number of the user, which is enough to call the owner of the account. This information can be very sensitive, depending on the intentions of the merchant. It is also possible to identity theft in cases where providing a NID number is required, for example, bKash is one of them when BDT over 5,000 TK is required [36]. The two major issues that are common in our country are harassment and scamming [19]. In the first case, especially when the user is female, the merchant or their affiliates call the user on that number later on and harasses them. This has become a huge issue in recent years, due to the widespread use of mobile recharge and mobile banking services. This violates the personal security of the users. In addition, the other major issue is scamming. Some people call the users of these mobile banking services and tell them that they are a representative of that service and their account has been locked [19], so they need to provide their PIN or the OTP that they receive in SMS. Most people who are knowledgeable about technology do not fall for these lies, however, people in the older generation or in rural areas with less education, do not have enough technical knowledge to recognize that this is a scam call, and they end up trusting the caller and providing the information that they are asked to give. By getting this PIN or OTP, the scammers get access to that account and steal the money from there. This kind of scam has become such a major problem these days that even some of these mobile banking services themselves had to issue public service announcements to make people aware [30]. These scammers usually get the user's name and number from the merchants, or sometimes the merchants do the scamming themselves. Without access to the users' phone numbers, or other necessary information, the scammers would have a much harder time deceiving the users, even if they are more vulnerable.

A huge percentage of these personal and financial security breaches happen through the merchants and the records they keep in their ledgers, and their access to personal information like phone numbers. Moreover, there is no thorough screening for the people who can become a merchant for these services, so there is no guarantee of knowing if the merchants are ethical or not.

While 3rd party intermediaries are problematic, they are also the reason for Mobile Banking's huge availability. It is counterproductive to get rid of these 3rd party intermediaries which may result in the whole Mobile Banking ecosystem becoming less available to the mass population. And adding highly vetted merchants will add more value-added-service costs in contrast to the currently implemented damage-control workflow which suggests taking action against a merchant after any kind of occurrence had occurred.

The primary problem here arising is the merchants having a way to contact the account holder, their phone number to be more precise. As it will not be possible to eliminate the merchants, because that makes the service inaccessible to a lot of people, the goal of this proposed system is to keep the merchants but get rid of their access to personal information like phone numbers.

1.3 Research Objectives

This research aims to come up with a system that ensures security and privacy in mobile banking while making no parties other than the Government and the Banking authority know about the full transaction details. The objectives of this proposed model are:

- To understand if Blockchain can provide privacy.
- To experiment if people with non-technical knowledge or shallow technical knowledge are ensured security from being scammed.
- To understand if Blockchain can make ledger books kept by 3rd party intermediaries redundant.
- To experiment if light nodes are sufficient in the case of mobile banking keeping the integrity of Blockchain records.
- To evaluate the proposed model.

1.4 Thesis Structure

- Chapter 1 introduces the background of the topic along with research problems and research objectives.
- In chapter 2 the previous works in this field are elaborated. In addition, different characteristics of Blockchain have been described in this chapter. Blockchain Architecture, Leaf structure, Nodes, hash, Consensus mechanism, Hashing Algorithm, Ledger Immutability etc are elaborated. Reasons behind using Blockchain instead of current Authorization System are described.
- Chapter 3 discusses the methodology and the internal mechanism of the proposed system. Here, different scenarios are given, along with and explanation of the consensus mechanism that has been used and also the process oh how the nonce will be generated is shown.
- Chapter 4 is the conclusion to the paper

Chapter 2

Related Work

2.1 Literature Review

Paper [17] has done a systematic review of Blockchain in FinTech and what role it plays. According to their research, implementing Blockchain in FinTech not only has allowed a medium for banks and non-bank entities to make cross-network transfers and payment services more convenient without any involvement of 3rd party entities but also by 2030, the annual growth rate would have surpassed 100%. The authors strongly preached implementing Blockchain in FinTech due to the Peer-to-Peer system of keeping the same ledger book that ensures no alternation of the records, which is a primary concern of any kind of financial record-keeping entity.

Although Mobile Banking in general currently in Bangladesh requires to disclose who are the dealing parties i.e. bKash, Q-cash etc. etc., Blockchain, can ensure the decentralization of authority in such a way that no additional 3rd party requires not to be involved. Paper [23] has come to the conclusion that a Blockchain-based ecosystem can help to ensure the privacy of the parties willing to transact with each other. Concealing the identities of the dealing parties from a 3rd party is saving from the extra fee of intermediary charge as well as ensures privacy.

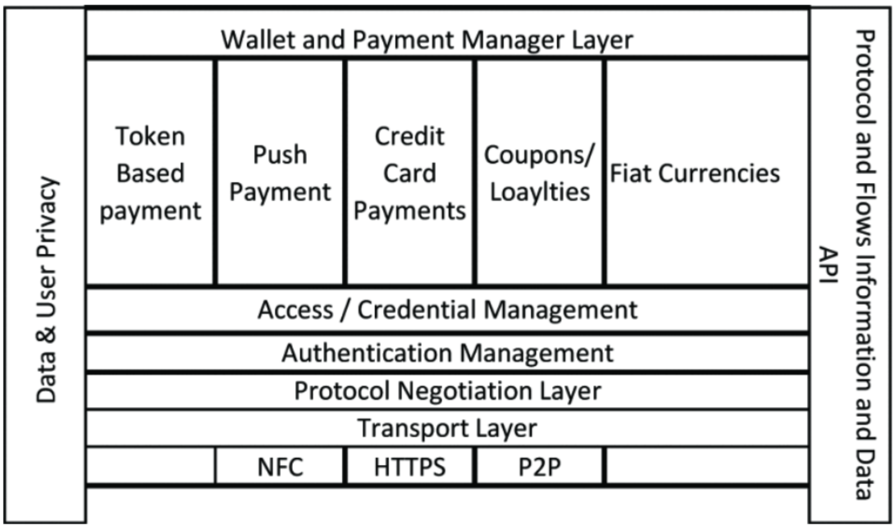

Data & User Privacy
Wallet and Payment Manager Layer
Token Based payment
Push Payment
Credit Card Payments
Coupons/ Loaylties
Fiat Currencies
Access / Credential Management
Authentication Management
Protocol Negotiation Layer
Transport Layer
NFC
HTTPS
P2P
Protocol and Flows Information and Data API

Figure 2.1: Wallet High Level Architecture

Two major concerns of trackless from 3rd party intermediary transactions are (i) what can occur if the central authentication for the traditional wallet system becomes a single point failure and (ii) transactions in traditional blockchain-based applications take time to verify data integrity in order to avoid double-spending of the same single amount. To address these issues, the paper [20], suggests using the already existing Corda Consensus Algorithm as the consensus method to ensure chain integrity and no double-spending with the help of the Notary Consensus Algorithm which is single-handedly responsible for verifying smart contracts.

According to [12], every 10 minutes, a new block is added to the Bitcoin network, which occupies about 1 MB of space. The Bitcoin network is more than 140 GB in size, and it will continue to grow at a rate of about 50 GB per year. The mobile device can not handle this amount of data. To solve the storage issue, they changed the consensus unit (CU). This unit forms a trusted cluster out of numerous network nodes. Also, the paper suggests using a Net-Whip which does not exist in the Bitcoin framework but will get rid of malicious Nodes in the Blockchain or Ledger.

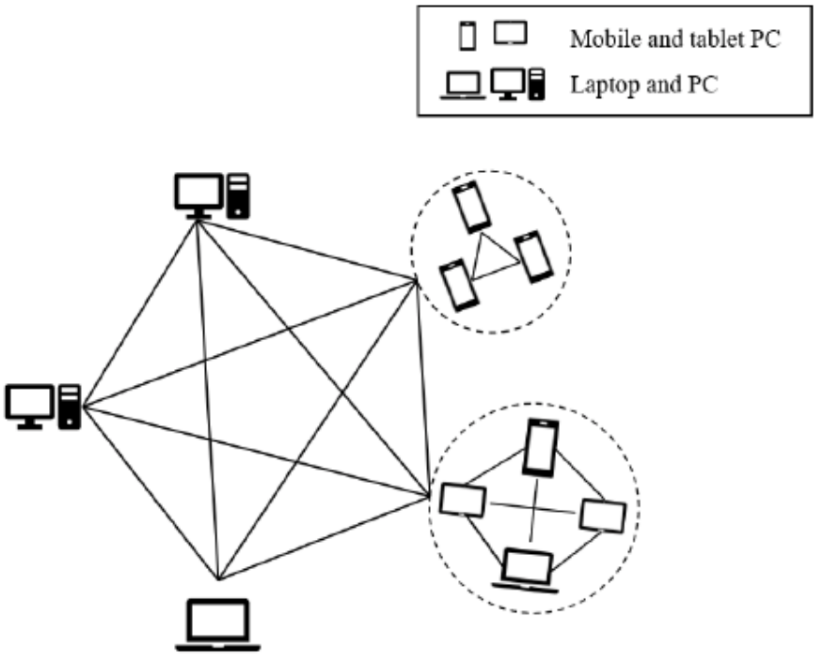


Figure 2.2: A simple network with consensus unit

According to [23], they offered a blockchain-based crypto-currency mobile payment that does not require any centralized party. That concerns traceless transactions from both 3rd parties and banks. This traceless transaction works through delegation setup as the bank is designated as a delegator by the payer. The merchant then sends the payer a payment request, and if the payment value and merchant identity match, the payer designates the bank as the delegatee, and the bank can then issue a transaction on the blockchain-based cryptocurrency system to sell cryptocurrency for fiat currency, which is then deposited into the merchant account. The blockchain will not accept the bank issued transaction if it does not comply with the delegation's conditions, and the payment will fail. But this type of traceless transaction can help the corrupted people to skip the taxes and people can buy violent things without any records.

[32] This study analyses financial inclusion in Bangladesh through the use of blockchain, its usefulness, hurdles towards its successful use and recommendations which may lead to the effective use of blockchain in the banking sector of Bangladesh. If we simply describe blockchain, it is basically a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems. In blockchain technology, each of the blocks contains information about transactions and whenever a new transaction is done it is recorded in the client's ledger. The database which is decentralized and managed by multiple clients is called Distributed Ledger Technology abbreviated as DLT. To hack the blockchain system the hacker needs to hack every single block in the system. The blockchain distributed system has three parts in total. And they are - Data, Hash and hash of its consecutive block. In this technology, the record for every transaction is kept in an immutable cryptographic signature which is the hash.

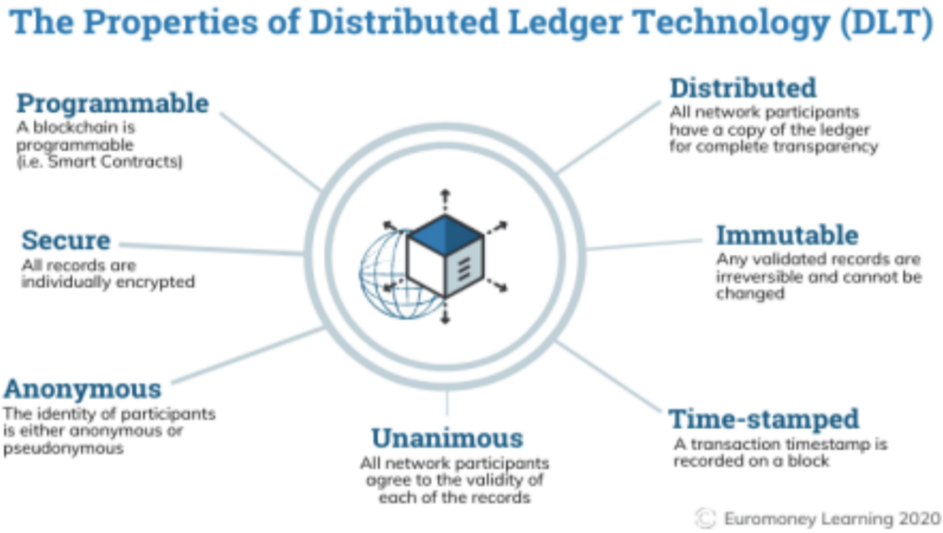

The Properties of Distributed Ledger Technology (DLT)
Programmable
A blockchain is programmable (i.e. Smart Contracts)
Distributed
All network participants have a copy of the ledger for complete transparency
Secure
All records are individually encrypted
Immutable
Any validated records are irreversible and cannot be changed
Anonymous
The identity of participants is either anonymous or pseudonymous
Unanimous
All network participants agree to the validity of each of the records
Time-stamped
A transaction timestamp is recorded on a block
© Euromoney Learning 2020

Figure 2.3: The Properties of DLT (Ray, 2021)

But the main drawback of using blockchain technology is that it is not as user-friendly as most of the currently used technology. Interfaces for blockchain ledgers are difficult to adopt. There must be a solution for handling a large number of users if we use blockchain technology. It should "rapidly process large numbers of transactions otherwise it could limit its adoption in global decentralized energy systems" (Hiswai, 2018). For example, "Bitcoin and Ethereum can handle only 3-30 transactions per second in comparison with visa circuits which can handle approximately 60,000" (Hiswai, 2018). Blockchain-based businesses or banking is very convenient for a developing country like Bangladesh, as it decreases the rate of corruption in the banking sector.

According to [2] a study was conducted on the Nigerian internet banking system and it showed the different levels of online banking with a thorough analysis of their security needs and regarding issues because of online banking. The current defence mechanisms are described in the paper. Despite several advantages of the internet banking system, the current system has not been very compelling, as they still have accountability which has been exploited by hackers many times. Among the three levels of internet banking Information level, Communication level and Transaction level, the most hacking occurs in the third level - the Transaction level. Getting authentication credentials from the victim is called credential harvesting. This is the most common attack in the world of internet banking. There are many different ways to achieve credentials from the user. For example- Typo-squatting, Sub-domain attacks, Image/3-D Spam, Shoulder surfing, Hardware keyloggers, Phishing etc.

To decrease the attacks from the hackers, security awareness by Debit/Credit cards in Nigeria is made. Banks have taken precautions to protect customers against PIN snooping while in the ATM booth and intense customer card use. Most ATM focuses are worked, so that individuals looking out for a line to utilize the machine would not understand or be able to see how the ATM client types on the ATM. Banks have likewise tried to neutralize the harms presented by phishing agents. Any kind of messages or emails regarding pins or mentioning them to unveil their pins or passcode to anyone is seen commonly. However, this has helped in stemming the repeated effective attacks through phishing, but it has not totally disposed of it. Although these banks took many measures to stop phishing chances are that customers may still fall victim to these agents as corrupt bank staff may engage with external hackers to help them out in the hacking process. So, staff's honesty and integrity are important factors here.

According to [26], there are three aspects: Digital currency expression, network architecture and consensus process with the existing problems of blockchain technology. This paper described a hybrid blockchain system with a modularity network for CBDC was proposed. In this hybrid blockchain system, the accounting scheme helps to keep records for intermittently circulated digital currencies. When there are records of massive small payments with large value fluctuations, the Unspent Transaction Output (UTXO) scheme is used.

The UTXO scheme allows multiple transactions at a time in parallel. This can be done because there is no account for it. The privacy and security of this scheme are very promising. Other than coin-based transactions, the input here is always joined with a UTXO. On the other hand, the accounting scheme uses a list to keep a record of the balance of the clients, for example, in a bank account. In this scheme, the transaction is only valid when there is enough balance in the client's account to pay back it. So in this case, the account which is sending money is debited and the account which is receiving money is credited with the value.

First of all, the funds that the company will issue need to be done as UTXO. After all the negotiations to pay for digital currencies, the transfer UTXO is created in the system. Both of the users will have a private key and they will sign the contract with it. These signatures are evaluated by the third-level nodes and the account of user 1 is debited with a significant amount and thus the balance of the company also increases.

The issuance mechanism that CBDC follows is quite similar to the UTXO transfer mechanism. Here in the figure, we can see that the circulation of the system basi-

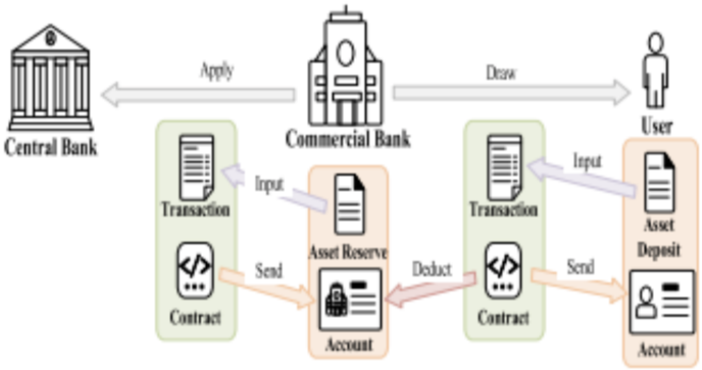


Figure 2.4: The schematic diagram of the issuance mechanism

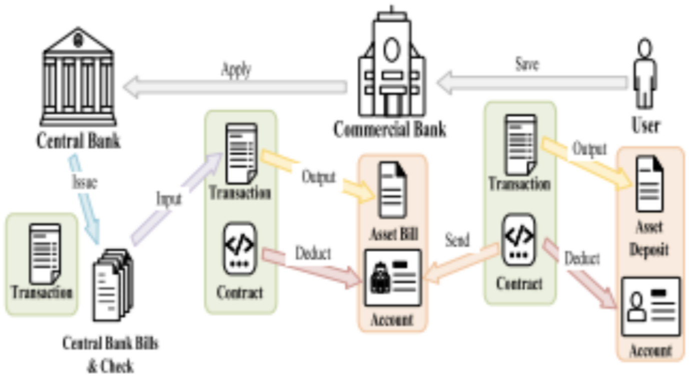


Figure 2.5: The schematic diagram of the withdrawal mechanism

cally happens through the client's savings and withdrawals. The deposited amount can also be included as a UTXO asset which can be used as the input of transactions.

[24] According to this article, by giving a ledger that no one administers, a blockchain could offer explicit online transactions - like installments or securitization - without the requirement for a bank. Many examples of improved money transactions, payment, fundraising, securities, lending money, trade finance, KYC by using blockchain systems have been discussed thoroughly in this article.
Companies working on blockchain technology are aiming to enable businesses to accept bitcoins as a form of payment. BitPay, for example, a payment service provider that assists businesses in accepting and storing bitcoin payments, has a large number of connections with e-commerce platforms such as Shopify and WooCommerce. Blockchain technology is also used to smoothen micropayments which usually happened to be an amount less than a dollar. This technology eliminates the administration need. Also opens gates for wider global markets which reduce fluctuations in the traditional security market.
[3] This paper described how the Indian bank sector uses blockchain technology in terms of banking, money transactions and improving loan quality.

The present blockchain system's smart contract and smart property applications effectively intensify the system, making it more decentralized and dispersed control, which improves clarity and trust in the management of loans supplied across all

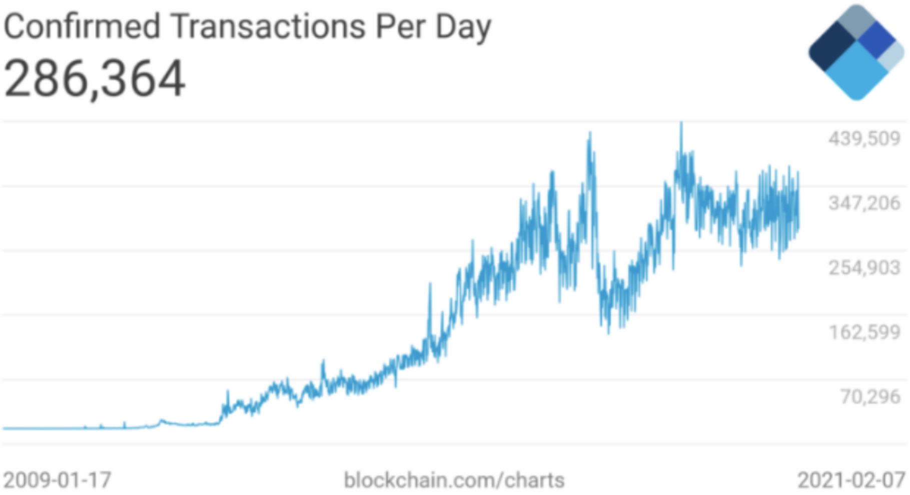


Figure 2.6: Transaction Rate

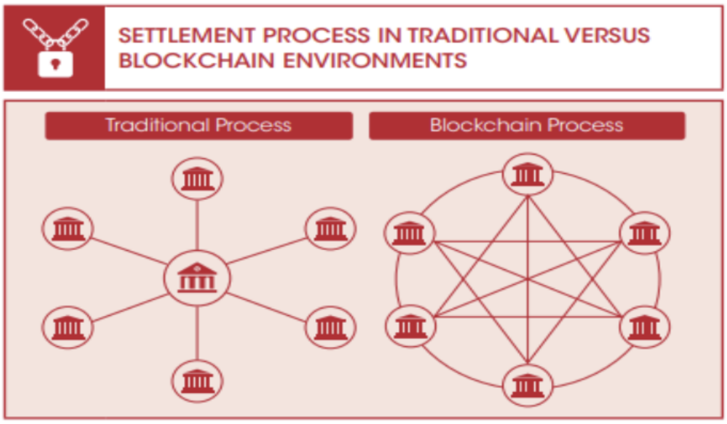

SETTLEMENT PROCESS IN TRADITIONAL VERSUS BLOCKCHAIN ENVIRONMENTS
Traditional Process
Blockchain Process

Figure 2.7: Traditional Process vs Blockchain Process

institutions. Each bank can become a part of the blockchain network by using this strategy. The blockchain network's smart identification helps to authenticate the browser's legitimacy. Cryptographically signed and consistent loans are approved. For transparent loan asset categorization, smart contracts are used following loan classification approval.

It also identifies risky customers by tracing high debt and/or constrained repayment capacity, as creditors' identities. All the activities in the network are distinguishable across the network to keep pace. It highly reduces the risk of losing assets.

The paper [25] describes that blockchain technology permits the fragmentation and decentralization of data kept in a manner that there is no one central entity to manage or alter the data. Bitcoin is the first successful blockchain application built with the idea known as the cryptocurrency that permits a transaction flow with no banking institution or government to manage it. Blockchain is related with advantages like a high degree of transparency, honesty, faith and confidence for the parties. Blockchain is currently in the preliminary phase but it is a promising technology with the potential to influence many more industries in the future. However, its security sector is still the main downfall of it which still requires work. Thus,

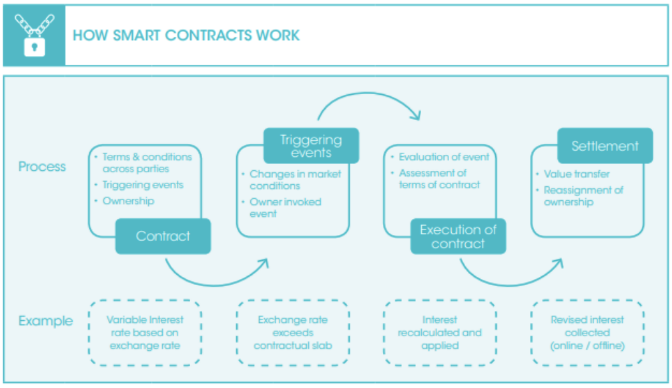
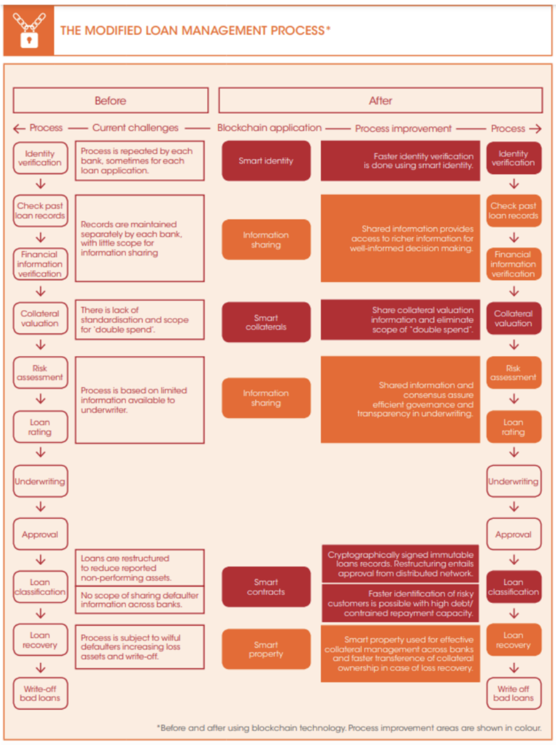

HOW SMART CONTRACTS WORK
Process
Terms & conditions across parties
Triggering events
Ownership
Contract
Triggering events
Changes in market conditions
Owner invoked event
Evaluation of event
Assessment of terms of contract
Execution of contract
Settlement
Value transfer
Reassignment of ownership
Example
Variable Interest rate based on exchange rate
Exchange rate exceeds contractual slab
Interest recalculated and applied
Revised interest collected (online / offline)

Figure 2.8: How smart contracts work

the thesis paper seeks to develop an analysis of the blockchain security challenges utilizing the previously published literature between 2010 and 2021. This thesis undertakes an analysis of 20 publications to deliver a scientific input that provides an overall perspective of known security risks and their relative consequences on the blockchain system. This thesis begins with an outline of how the blockchain system works and briefly discusses the data security of blockchain. The collecting of security attacks from the literature has been carried out by employing concept centred matrix technique. This technique led to security attacks that were categorized based on four tiers of blockchain system design. Next, the security threats are mapped to typical security implications such as double-spending, illegal code execution, denial of service, unfair income and privacy key leaks.

These security consequences were investigated which led to the conclusion that the biggest security vulnerabilities on blockchain originate from its P2P network design and its consensus method. Besides, several feasible methods to reduce the security concerns were mentioned albeit, further effort in establishing new security mechanisms and protocol framework is still necessary.

This paper [31] talks about the benefits and endless possibilities of implementing a much more integrated version of fintech in Russian financial sectors and of the whole world (Soloviev, 2018). However, it also mentions how despite the immense demand from customers for much more conveniently functional and secure mobile applications that would provide them with a better banking experience through higher value proposition with options such as international transactions, peer to peer-to-peer lending, robo advising etc, there is still a lack of improvement when it comes to fintech-related initiatives. According to the author, this is partly because of the lack of unified points of view when it comes to fintech. Furthermore, the failure of all major initiatives in Russia that were taken to introduce smart technological improvements for much more customer-oriented insurance products has not helped the cause either. As it stands right now, traditional banking still holds a very strong hold over the market with very few banks leaning towards the technological advancement through their use of artificial intelligence to ensure better customer service experience, open APIs, cybersecurity and regtech etc. to cut down their cost and further enhance as well as fortify their systems. Despite all that, the author emphasizes the benefits and necessities of coordinating the point of view of all the



THE MODIFIED LOAN MANAGEMENT PROCESS*

Before

After

Process — Current challenges — Blockchain application — Process improvement — Process

Identity verification

Process is repeated by each bank, sometimes for each loan application.

Smart identity

Faster identity verification is done using smart identity.

Identity verification

Check past loan records

Financial information verification

Records are maintained separately by each bank, with little scope for information sharing

Information sharing

Shared information provides access to richer information for well-informed decision making.

Check past loan records

Financial information verification

Collateral valuation

There is lack of standardisation and scope for 'double spend'.

Smart collaterals

Share collateral valuation information and eliminate scope of "double spend".

Collateral valuation

Risk assessment

Loan rating

Process is based on limited information available to underwriter.

Information sharing

Shared information and consensus assure efficient governance and transparency in underwriting.

Risk assessment

Loan rating

Underwriting

Underwriting

Approval

Approval

Loan classification

Loans are restructured to reduce reported non-performing assets.

No scope of sharing defaulter information across banks.

Smart contracts

Cryptographically signed immutable loans records. Restructuring entails approval from distributed network.

Faster identification of risky customers is possible with high debt/ contrained repayment capacity.

Loan classification

Loan recovery

Process is subject to wilful defaulters increasing loss assets and write-off.

Smart property

Smart property used for effective collateral management across banks and faster transference of collateral ownership in case of loss recovery.

Loan recovery

Write-off bad loans

Write off bad loans

*Before and after using blockchain technology. Process improvement areas are shown in colour.

Figure 2.9: The modified loan management process

participants of this banking ecosystem and research into new and innovative financial tech.

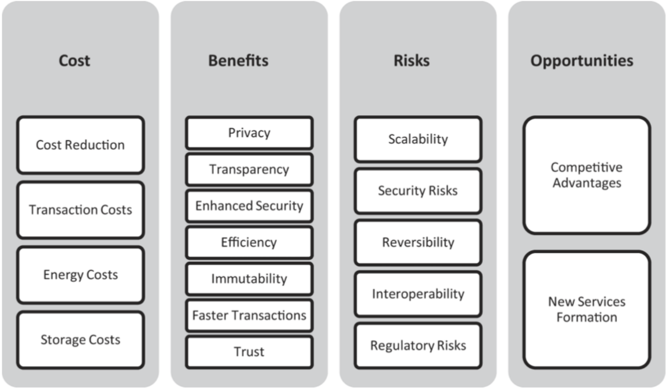


Figure 2.10: Cost, benefit, risks and opportunity analysis framework

In the paper [21], it is explained that at this current stage of technological advancement despite having several benefits and opportunities with a caveat of a few risks and some costs, the lack of contribution and research into utilizing blockchain technology at its fullest in finance and banking sectors has narrowed down its path of endless possibilities, compared to other sectors (Osmani et al, 2020).

The authors of this paper did a thorough analysis of the available academic-based research data, journals, and academic as well as technical reports related to blockchain and its extended fields to identify its benefits and opportunities of it as well as the possible risks and costs that come along. The paper identified the existing gap between legitimate implementation of blockchain technology in the financial sector despite the evident knowledge and interest that exists amongst the people related to this sector. However, the authors still make their case to make everyone recognize the benefits of blockchain that outweighs the risks and costs that come along and shed light on the necessity of focusing and investing in this field.

According to [16], incorporating blockchain technology by the fintech corporations provides the next stride towards the growth of blockchain technology as well as its longevity, which will result in a significantly more secured, stable and better customer experience-oriented financial sector (Fernandez-Vazquez et al, 2019).

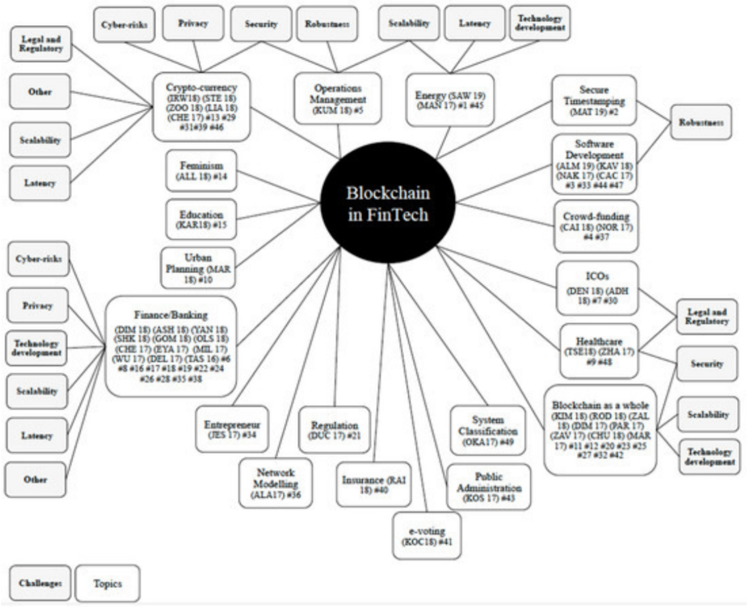

Cyber-risks
Privacy
Security
Robustness
Scalability
Latency
Technology development
Legal and Regulatory
Other
Scalability
Latency
Crypto-currency (IRW18) (STE 18) (ZOO 18) (LIA 18) (CHE 17) #13 #29 #31#39 #46
Operations Management (KUM 18) #5
Energy (SAW 19) (MAN 17) #1 #45
Secure Timestamping (MAT 19) #2
Robustness
Software Development (ALM 19) (KAV 18) (NAK 17) (CAC 17) #3 #33 #44 #47
Feminism (ALL 18) #14
Education (KAR18) #15
Urban Planning (MAR 18) #10
Blockchain in FinTech
Crowd-funding (CAI 18) (NOR 17) #4 #37
ICOs (DEN 18) (ADH 18) #7 #30
Cyber-risks
Privacy
Technology development
Scalability
Latency
Other
Finance/Banking (DIM 18) (ASH 18) (YAN 18) (SHK 18) (GOM 18) (OLS 18) (CHE 17) (EYA 17) (MIL 17) (WU 17) (DEL 17) (TAS 16) #6 #8 #16 #17 #18 #19 #22 #24 #26 #28 #35 #38
Legal and Regulatory
Healthcare (TSE18) (ZHA 17) #9 #48
Security
Blockchain as a whole (KIM 18) (ROD 18) (ZAL 18) (DIM 17) (PAR 17) (ZAV 17) (CHU 18) (MAR 17) #11 #12 #20 #23 #25 #27 #32 #42
Scalability
Technology development
Entrepreneur (JES 17) #34
Regulation (DUC 17) #21
System Classification (OKA17) #49
Network Modelling (ALA17) #36
Insurance (RAI 18) #40
Public Administration (KOS 17) #43
e-voting (KOC18) #41
Challenges
Topics

Figure 2.11: mapping of the collected data

The paper conducts an analysis of 49 academic and research-based publications from a scientific database and maps out the research subjects, constraints of it, gaps and likely future developments of this technology to appreciate the present state. The authors have observed that the most prevalent restrictions are issues such as selection bias, inconsistency in collecting data and misclassification. However, they do advise that there is a lot of space for more study and with further research into the uses of blockchain in the financial industry, smart contracts can be implemented, and privacy can be increased substantially.

According to [22], blockchain can simply be explained as decentralized and fragmented database records of all types of financial transactions or digital events that have occurred amongst a group of participants. The paper identified the possible implementation and effectiveness of blockchain in the banking sector of India. The author talks about his findings on how the three key factors of the Blockchain (disintermediation, transparency, provenance) have the potential to revolutionize all types of financial sectors of India. India being a country with the second-largest number of people in the world has a vast amount of property, and financial well-being, however, something that they lack is a strong and dependable security system for them and this is where blockchain technology can be used to the fullest of its extent. However, the author also recognizes the immense cost of implementing blockchain technology and the huge amount of computing power as well as technical knowledge that is required. Apart from that the public unawareness and the fear of the unknown that comes with it is also an obstruction. That is why the author recommends the financial institutions of India come up with strategic plans that include ensuring tactical sponsorships that would work as a spearhead for the campaigns which will give them the opportunity to fundamentally re imagine the service system.

2.2 Characteristics of Blockchain

2.2.1 Blockchain Architecture

Blockchain is one of the most recently established technologies, highlighting the Internet of Things (IoT) and artificial intelligence revolutions' concepts and advancements. [15]. Cryptocurrencies like bitcoin and Ethereum are basically developed using blockchain technology.Blockchain technology enables online value transfers without the use of a middleman such as a bank or credit card firm. Blockchains, or distributed ledgers are a new innovation that emerged in the recent decade. They enable the maintenance of a tamper-proof ledger shared among multiple entities in an untrustworthy environment. A collection of records, such as bitcoin transactions in Bitcoin, can be stored in the ledger [1]. For example, the Bitcoin blockchain contains a record of every time someone sends or receives bitcoin.

Blockchain technology has shown to be an emphasis on development for a wide range of applications. Regardless of the fact that blockchain is a relatively emerging technology. Many experts have linked it to the early days of the World Wide Web's public internet protocols like HTML in terms of its potential to revolutionize the way we live and work.

2.2.2 Block/Leaf Structure

The information in the blockchain technology is stored in such a way that it is impossible to hack the system or cheat in the system.A blockchain is a legder of transactions that is replicated and transmitted across the network of computers that form the blockchain. A blockchain is a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the entire blockchain network.Each block carries a number of transactions on the chain and any new transaction occurs on the blockchain it is recorded and added to the ledger of each participant. Distributed Ledger Technology (DLT) is administered by various indivduals that is also a decentralized database [34] .

Nodes: A transactional database technology like blockchain, is a method which is decentralized and manages validation and tamper-proof transactions that are consistent over a large number of participants which are also known as nodes [6] .

Hash: Blockchain is a type of distributed ledger technology that maintains a record with an immutable cryptographic signature known as a hash.This means that if one block in a chain was changed, it would be immediately apparent. To take down a blockchain system, hackers have to make change in every block in the chain across all distributed versions.

Prev-Hash: It is a reference to the hash of the chain's previous (parent) block.

Nonce: The nonce which is a random whole number, a 32-bit (4 bytes) field. It is usually adjusted by the miners for use as the hashing value of the block which should be a valid number. A nonce is a number that can be used only once. After finding the appropriate nonce, it is added to the hashing block. Along with the nonce, the hash value of the block will get rehashed and will create a difficult algorithm.
It is compared to the present target to determine whether it is lower or equal. Millions of Nonce are tested and discarded every second until a valid nonce is discovered.

Data: Data is the content that is stored in the blockchain in every block.

2.2.3 Consensus Mechanism

In terms of blockchain technology, the consensus mechanism means a process that is formalized and reaches a consensus. This also means at least 51% of the nodes on the network agree on the coming global state of the network. A consensus mechanism is a protocol or algorithm which allows distributed systems to work together in a secure way.
Algorithms and protocols are two different things. A protocol is a collection of rules stated in a standard that defines how a system and its many components operate and communicate.Algorithms and protocols are two different things. A protocol is a collection of rules stated in a standard that defines how a system and its many components operate and communicate. Algorithms, on the other hand, are like step-by-step procedures for solving problems or computing outcomes. For decades, these methods have been used to reach agreement across database nodes, application servers, and other enterprise infrastructure components. While traditional blockchain firms rely on a single consensus mechanism, some cutting-edge firms employ numerous protocols.
There are a range of consensus mechanisms, but they all have the same objective: to verify that records are accurate and truthful. The distinction is in how the consensus is made.

Proof-of-Work: In a Proof-of-Work system, the blocks in the blockchain contains the transaction data that are validated by users solving a difficult mathematical problem. This is known as ”mining,” and it is usually done by powerful computers. The first miner to solve the challenge receives a reward in the form of bitcoin. The Proof-of-Work technique is used by crypto-currencies like Bitcoin and Ethereum.

Proof-of-Stake: The validator, or creator of a new block, is picked at random based on how much stake they pledge to the network. The bigger the stakes, the more likely you are to be chosen as a validator. Proof-of-Stake consensus is used by blockchain protocols such as Cardano's Ouroboros and EOS.

Proof-of-Authority: Proof-of-Authority is a modified version of Proof-of-Stake that only approves parties selected based on their reputation can become validators. Blockchain solutions that use Proof-of-Authority include IBM's Hyperledger Fabric and Ethereum's Kovan Testnet.

2.2.4 Hashing Algorithm

Transactions are fed into Blockchain technology and run through a hashing algorithm, which provides a fixed-length output. One way to assure a secure transaction when a message is intended for a single recipient hashing is always a secure way.The hash is created using a formula, which aids in the security of the transmission against manipulation.

2.2.5 Ledger Immutability

One of the attributes blockchain is associated with is its immutability. So, the most important characteristics of blockchain is its immutability database and data that are already in the blockchain can not be manipulated afterwards.
The blockchain is a chain of blocks means there are single blocks in the blockchain that are connected to each other and the connection between the blocks are made by their hash value. The hash value is the value which is unique for every block. And by this value any specific block can be identified. It also depends on the contents of the block. So, each block hash its own unique hash value which is identifying that particular block and therefore each block can reference or point to the block before. The main advantage of hash is it can not be reverse engineered. The most popular hash function is SHA-256. The data stored in the blockchain can not be altered. If the data is tampered in any way the blockchain immediately breaks. It is very difficult to make changes in both disconnected and the live blockchain simultaneously. Blockchain-based ledgers can assure an application's complete history and information trail. When an exchange joins the blockchain, the record up to that point in time is preserved. The chain's legitimacy can be confirmed at any time by reexamining the square hashes – if there is a discrepancy between block information and its comparing hash, the transactions are not authentic. This enables associations and their industry controllers to quickly identify information tampering. This ensures that all data is accurate.

2.2.6 Distribution

The two most major features of blockchain technology are Trust and decentralization [9][8] These two features are described below-

Trust: The decentralized nature of blockchain technology is the most crucial feature of the technology. The network is protected by a A Proof-of-Work protocol in particular.Users of blockchain technology can use this protocol to avoid relying on third parties for transaction and asset security [26].The entire technical code is open source for all parties, according to [27] limiting the chances of a backdoor being developed into the system. Unlike banks, which manage their customers' capital and assets, this secure open access allows consumers to use blockchain in a way that is analogous to their own financial systems, with power over decisions that preserve their capital.

Centralized: The parties in a centralized network are known to each other. As a result, the system is trustworthy since only trustworthy and respected participants are allowed to add to the ledger. Because the participants' names are known, their transactions can be scrutinized.

Decentralization: For recording, storing, updating, transmission, verification, and maintenance of information in the Blockchain network, the Blockchain system adopts a distributed system structure [10][13]. Among other features of blockchain technology, decentralization is a predominant one. Two of the most essential properties of decentralization are resistance to censorship and immutability [8]. The lack of dependency on a third party for security, according to [24], is the most distinctive feature of it, which also guarantees the protection of an individual's property or assets.

2.2.7 Accessibility

A blockchain is usually divided into three types: public, private, and permissioned.

Public: Each customer on a public blockchain has the same set of entitlements. These include giving all the participants equal authority rather than granting centralized authorization to a third party [5][7]. Furthermore, every party has the ability to access or leave the entire network at any moment. Every participant is free to participate, and any source, including Bitcoin [4], can validate transactions.

Private: The centralized setups are ensured in the terms of a private blockchain. Furthermore, [5] said that only a single entity is authorized to make choices, as well as to have authority over activities and control over the transaction validation process. According to research by [14], the centralized authorized member will guarantee that the recommended consensus would be the only one followed. This is true of any centralized institution, such as government organizations that serve multiple states.

Permissioned: Where a permissioned blockchain is a distributed ledger that is not publicly accessible. This distributed network can only be accessed with permissions. This allows the participants to perform some specific tasks like - reading, accessing, and writing information on the blockchain.

2.3 Blockchain Vs Current Authorization System

Security is a main concern for both users and developers when it comes to mobile banking systems. There are privacy invasions due to enormous amount of data breaches that occur globally. There are many ways to secure mobile banking applications which include authorization.

Authorization focuses on deciding which resources and databases a user can access and use within the network. After logging into the network using authentication credentials, more security measures must be put into the network to limit certain information, tools or actions depending on user kinds or user designation.

Authorization is not enough to make a secure banking system seen from the past innovations. That is when blockchain comes to use. The digital distributed ledger system provides the feature of tracing the history of all transactions that have happened through the network. It is immutable so it is quite impossible to change the data inside the network. Due to the potential for traceability that blockchain technology offers, it is used by several systems nowadays. [28] Because the transaction history can be traced and it will always keep a record of every transaction in the system, it will help monitor any kind of trading. A lawmaker for the city of Buenos Aires is recommending using blockchain as a key component of a system to manage social aid payments. [28]

Again, in any normal mobile banking system the merchant or any third party is authorized to view and use all resources and data in the system. But in the proposed model the merchant only gets the nonce from the user. Third party does not have permission to look into other data of the users. Blockchain offers efficient, and reliable value transfers by eliminating the middleman. According to a study, 67 percent of central banks tested blockchain in 2017.[11]

In the blockchain network it is quite impossible to corrupt the system as the hacker needs to change every block in the entire system. So, by only using authorization code it is not that secure while transferring money via any mobile application. Since all the blocks in the network are cryptographically linked, it is more expensive for the hacker to attack the system. Only using the authorization code is not enough to attack the system. So, being a decentralized system the blockchain network is less prone to malfunction.

Using only authorization code, it is easy for any hacker to create fake data in the system. But as blockchain is a distributed ledger system, every node in the network must participate in the maintenance of the ledger and give validation when a new block is added. For adding a new block in the chain, it must be approved by two-thirds of the nodes in the chain. Otherwise, the block will be discarded. While a hacker can easily make a duplicate authorization code to attack the system if only authorization code is used for privacy concerns. The global media market is anticipated to grow to $1.54 billion by 2024. Additionally, according to PWC, the technology serves as the foundation for procedures like metering, billing, and clearing. [27]

Chapter 3

System Design

3.1 Methodology

At the very first, for the generation of any block, 2 types of data need to be prepared - (i) user input and (ii) computer-generated. Computer-generated data depends on user inputs. User input data includes two mandatory information: (i) the phone number of the recipient, and, (ii) the amount of money being transacted. It might also contain Reference, Message, and Counter Number in case of paying bills or any system that requires it to be paid in such a manner. Based on these user inputs, the computer generates additional data.

Data Field	**Definition**	**Source**	**Access**
SndNo	Sender's mobile number	Computer-generated (Auto-parsed)	User and Authority
RcvNo	Receiver's/Merchant's mobile number	User input	User and Authority
Amount	The amount in BDT that needs to be transferred	User input	ALL
CntNo	Counter number (Optional)	User input	User and Authority
Rfrnce	Reference (Optional)	User input	User and Authority
Msg	Message included for the receiver to get on his available blocks/leaves(Optional)	User input	User and Authority
Rsn	Reason of the transaction is done (Optional)	User input	User and Authority
TrxnID	Transaction ID	Computer-generated (Auto-generation)	User and Authority

UTC	Unix TimeStamp	Computer-generated (Auto-generation)	ALL
Hash	Block hash of the current block/leaf	Computer-generated(Auto-generation)	ALL
PrvHsh	Block hash of the previous block/leaf in the ledger book/blockchain	Computer-generated (Auto-integration)	ALL
NONCE	NONCE that is required to cash out the amount	Computer-generated (Manual generation on user request)	User and Authority. Merchant gains visibility if the User is requesting a cash out from this specific merchant.
Cnsmpt	A binary flag, which will tell if the amount is consumed or not. It will hold the value "true" if the amount has been cashed out or "false" in case the amount is still unspent	Computer-generated (Auto-generation)	User and Authority. The merchant gains visibility if the binary value is True.
ExprTm	The latest timestamp up to which the generated NONCE will hold valid	Computer-generated (Auto-generation)	ALL

Table 3.1: Block/leaf structure and the fields

3.2 Scenarios

i. **The user cashing out:** The user simply asks the merchant if the merchant has the amount that the user wants to cash out. If the merchant has the specified amount, he simply requests a NONCE generation from his device, provides the NONCE associated with the block hash to the merchant and after verification, the merchant provides the money. NONCE generated for a single pair of sender and recipient won't work within the set time span in another merchant.

ii. **The user cashing in:** Same as (i) until the verification phase. In case of verification, the merchant holds the power to verify whether the merchant has received the amount in person or not. If the merchant declines then the cash-in amount is reverted back to the previous state of the user.

iii. **The user sending money to another user:** In such a case, the user does not need to go to any kind of merchant at all. The user can just simply use the

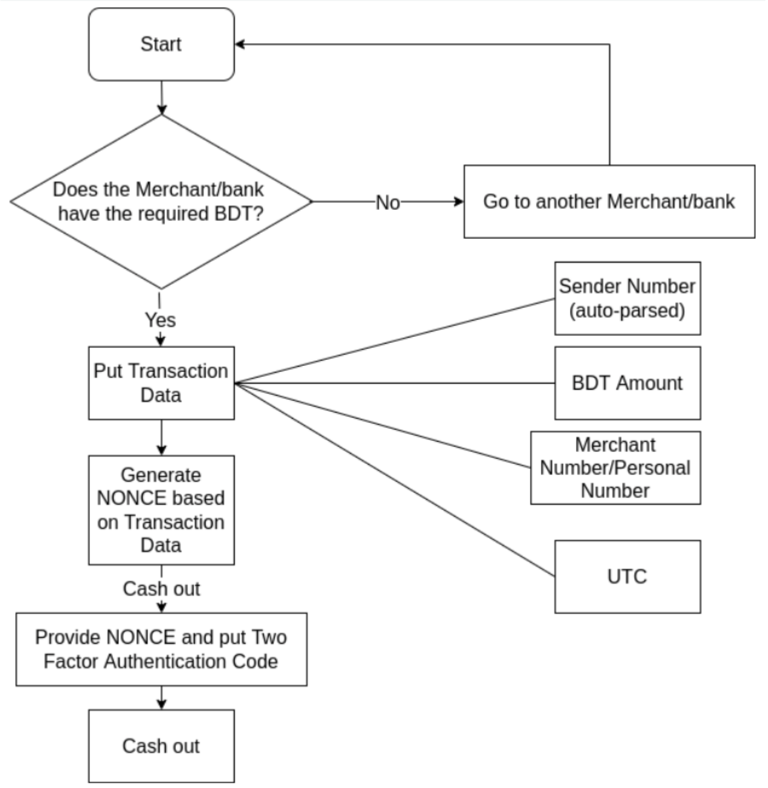

Start
Does the Merchant/bank have the required BDT?
No
Go to another Merchant/bank
Yes
Put Transaction Data
Sender Number (auto-parsed)
BDT Amount
Merchant Number/Personal Number
UTC
Generate NONCE based on Transaction Data
Cash out
Provide NONCE and put Two Factor Authentication Code
Cash out

Figure 3.1: Flowchart of cash-out process

already implemented "send money" option. One can send money along with a wish or message to his known family or friend. The receiver will instantly get the block hash without any kind of data secrecy.

iv. The user sending money to someone without an account: Same as (i). After being informed of the merchant's number, the block creation is as same as (i). The user just simply passes the NONCE to the person who will cash out on behalf of the account owner via text or any convenient form of fast electronic communication medium.

v. Someone without an account sending money to a user with one: Same as (ii), the recipient, the user with an account uses cash in option while the customer without an account just pays to the merchant on behalf of the user.

Our proposed model for Mobile Banking consists of 3 major aspects, which are zoning the merchants, network hierarchy and blockchaining. In this model, the intermediary merchants who are at the heart of money transferring activities keep the hard copy ledger books.

3.3 System Architecture

This system prevents privacy invasions and scams that are otherwise possible in the currently existing model, where the instructions dictate that the users provide them with their mobile number and other forms of identification to the merchants. While the merchants still will be as active as before, the changes that this model

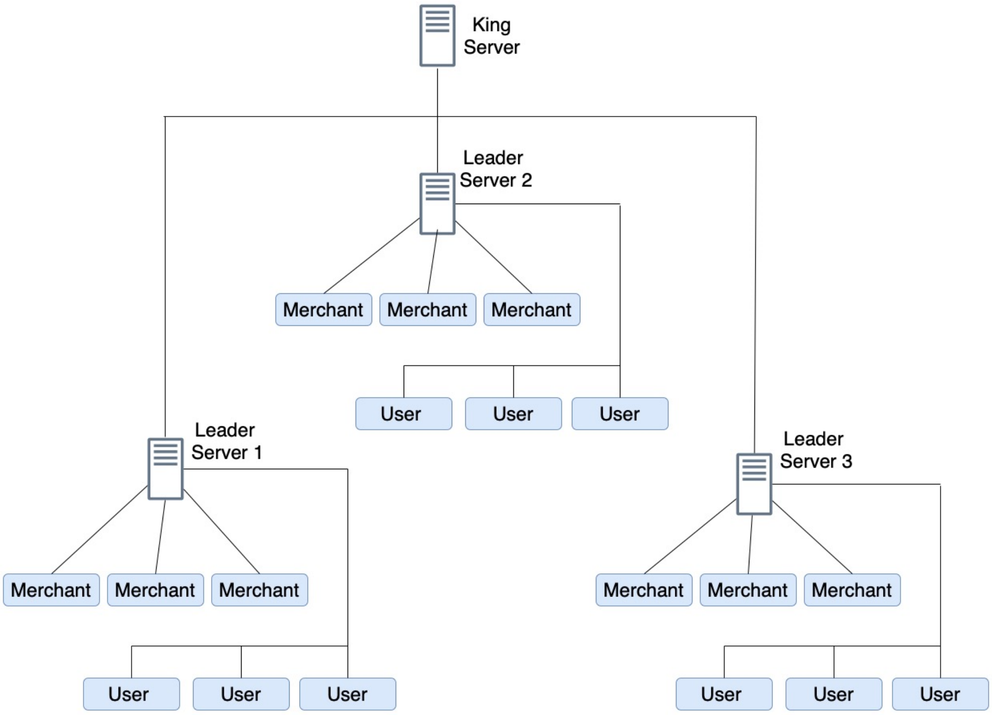


Figure 3.2: System Architecture

will provide are the types of data a user is required to disclose to the merchant. In addition, instead of a hard-copy ledger book there will be a digital one that will be shared across the whole collection of networks and each transaction will be validated through consensus algorithm to avoid double-spending, data theft and other forms of vulnerabilities.
The entire model architecture has been constructed based on seven core focuses

1. Data Privacy
2. Data Security
3. Synchronization
4. Data Transparency
5. Traceability to Authority
6. Fast Response
7. Data Backup

3.3.1 Zone

Keeping the focus on fast response, data privacy, and data security, every single district in Bangladesh will function as a single Zone. Each Zone will consist of one Zone leader and multiple merchants of that district. In total, there will be sixty-four (64) Zones, for the 64 districts of Bangladesh. All of these Zones will be responsible for taking transaction requests. Each Zone leader will have their own individual

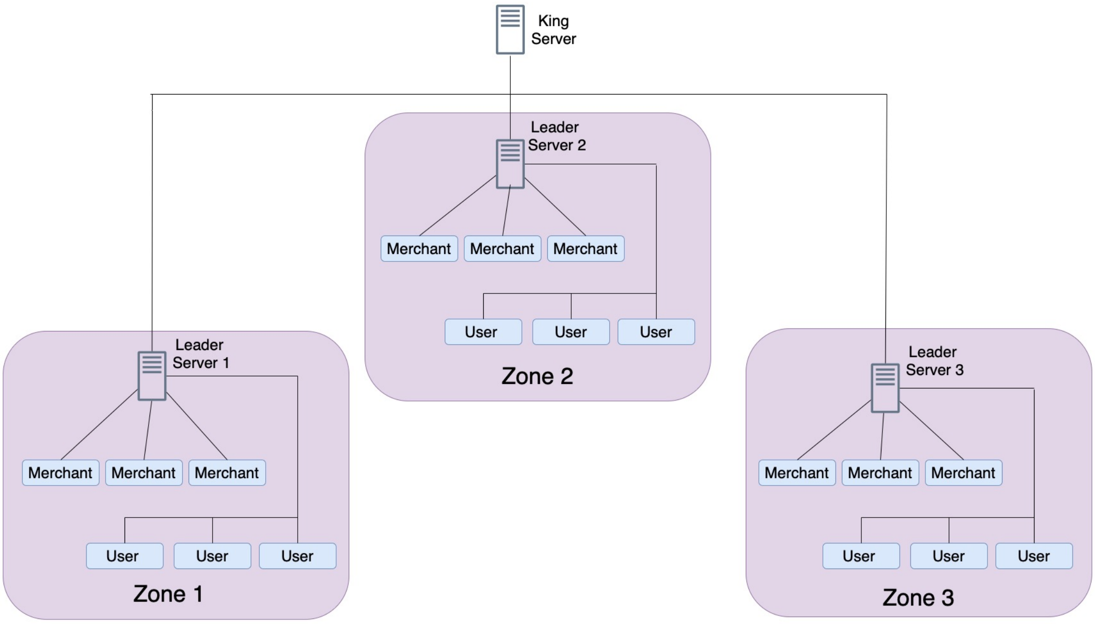


Figure 3.3: Zoning the merchants

single server which will ensure fast verification of transactions in the zones. The Merchant Networks will randomly elect a prime node among them which is termed the "Leader" and a secondary backup co-prime node which will kick in if the actual prime node fails to any system or hardware fault. There will be a random selection among the "Leader" nodes who will be represented as the "King". Another leader will be randomly selected which will play the role of the "King" node as a fail-safe if the original node fails. [18]

3.3.2 Node Hierarchy and Responsibilities

For scalability, data transparency, and data backup, the network has been divided into 2 layers. The first layer consists of Users and Merchants. Users and Merchants will not be able to directly interact with each other. They will also not have their own individual database server, rather they will be dependent on the Zone leader's server which will be shared among multiple users and merchants. Any request made by a user will be received by the Leader. The leader will forward these requests to the King among the Leaders which altogether are the network of the upper layer.
Within the upper layer, the king will call for block verification, transaction confirmation, ordering the replication of the same transaction among multiple leaders, and, according to a pre-selected ratio, the nodes will play roles like computational nodes, verification nodes, storage nodes, and other forms of a node if required. After the leaders have done their assigned task, they will send back data to the King and the King will circulate the replication if everything checks out.

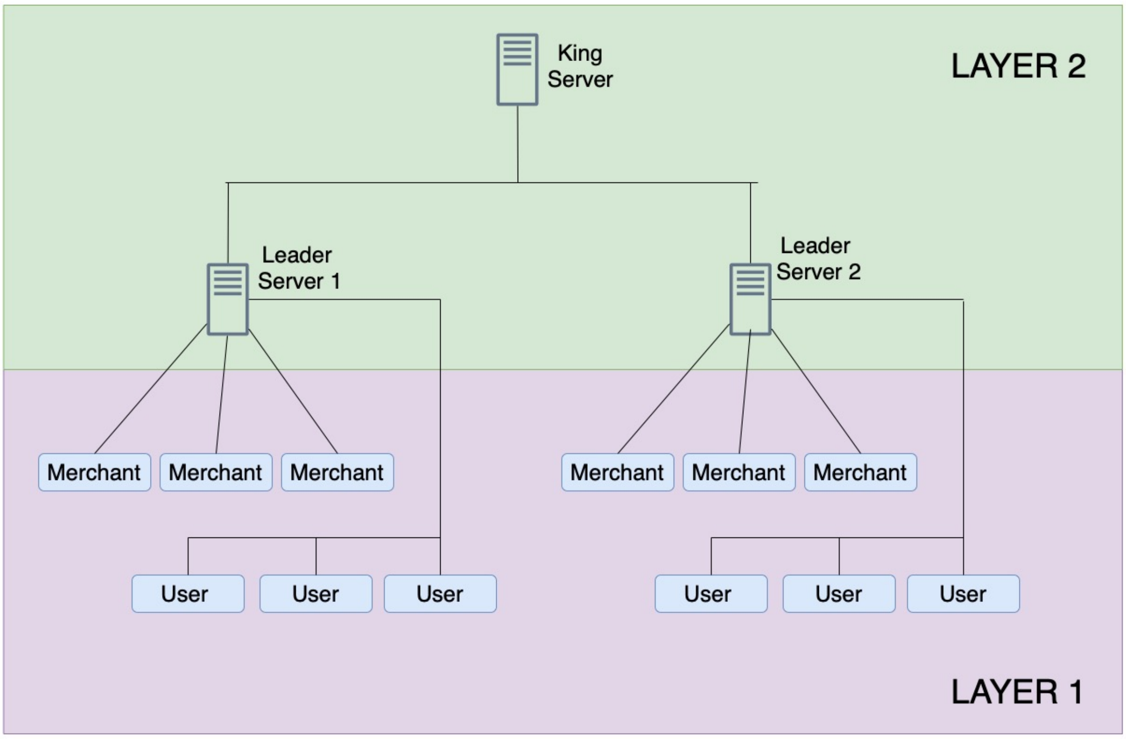


Figure 3.4: Node hierarchy

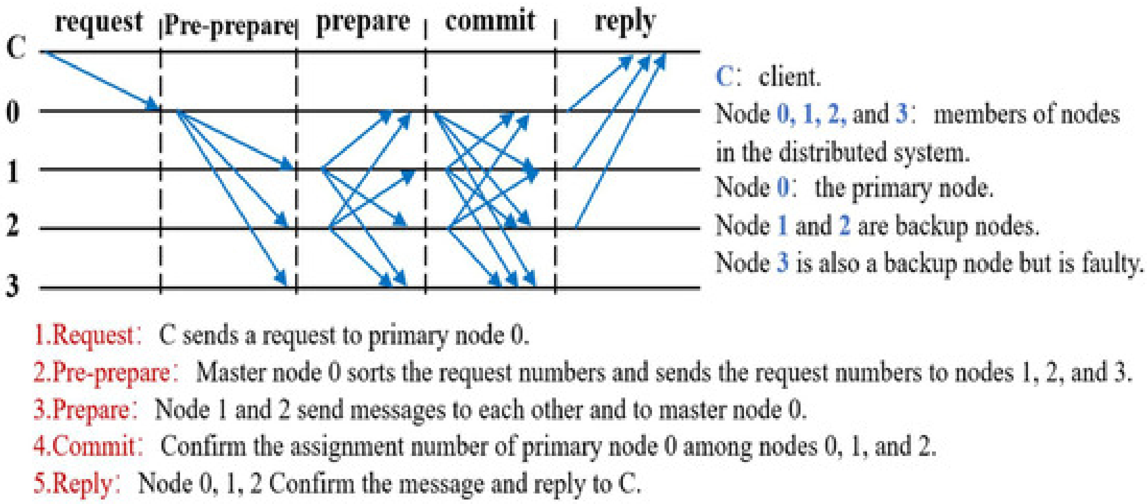
3.3.3 Consensus Mechanism

The consensus mechanism used in our proposed model is PBFT. In this PBFT consensus mechanism, when a user makes a request for transacting to the leader, the leader can only forward the request to the king. But as the request would be encrypted, the leader would not be able to view it. No node other than the king has access to it. After receiving the request, the king forward the request to all the 64 leaders for approval. The PBFT algorithm is fault-tolerant to

$\frac{(n-1)}{3}$; where n = number of total participant nodes including the king.

If $\frac{2}{3}$ of them gives approval then it would be added to the blockchain as a new block and a NONCE would be generated for the specific user. On the other hand, if more than $\frac{1}{3}$ of the leaders do not approve that request, then the block would not be added to the blockchain and a message would be generated for that user.

We select PBFT because of our model is permissioned, here all the 64 participant nodes will be added by the first party. As it is permissioned, no outside node can take part in reaching consensus.
Comparing with the other consensus mechanisms, we can see that PBFT has the maximum throughput. Even though the fault tolerance of PBFT is 1/3, the participant nodes can be added by the permission of the first parties only, and it's only a concern if a node suffers from any kind of internal fault or technical difficulties. Moreover, it is less expensive in case of computation power as well as power consumption. Its response time is also in second level, which is much better than the other established options. [29]


request
Pre-prepare
prepare
commit
reply
C
0
1
2
3
C: client.
Node 0, 1, 2, and 3: members of nodes in the distributed system.
Node 0: the primary node.
Node 1 and 2 are backup nodes.
Node 3 is also a backup node but is faulty.

1.Request: C sends a request to primary node 0.
2.Pre-prepare: Master node 0 sorts the request numbers and sends the request numbers to nodes 1, 2, and 3.
3.Prepare: Node 1 and 2 send messages to each other and to master node 0.
4.Commit: Confirm the assignment number of primary node 0 among nodes 0, 1, and 2.
5.Reply: Node 0, 1, 2 Confirm the message and reply to C.

Figure 3.5: PBFT algorithm flow

Consensus	**Communication Overhead**	**Computing Overhead**	**Fault Tolerance**	**Throughput**	**Response Time**	**Application Platform**
PoW	Low	High	1/2	$\approx$ 7 TPS	10 min	Bitcoin
PoS	Low	Medium	1/2	$\geq$ 25 TPS	1 min	Peercoin
DPoS	Low	Low	1/2	$\geq$ 300 TPS	$\approx$ 3 s	EOS
PBFT	High	Low	1/3	$\geq$ 1000 TPS	Second level	Hyperledger

Table 3.2: Established Consensus Mechanism comparisons

3.3.4 NONCE Generation

In this system, the NONCE is generated though the Adler-32 Hashing algorithm. This algorithm is also called the checksum algorithm, because it takes 4 characters from A and 4 characters from B and creates the final checksum. Here each character is 1 byte or 8 bits. The NONCE generation through this algorithm is shown below:

B is occupying the two most significant bytes.
A is the sum of all bytes in the stream plus one.

$$A = 1 + D_1 + D_2 + ... + D_n(mod65521)$$

$$\begin{aligned} B &= (1 + D_1) + (1 + D_1 + D_2) + ... + (1 + D_1 + D_2 + ... + D_n)(mod65521) \\ &= nD_1 + (n1)D_2 + (n2)D_3 + ... + D_n + n(mod65521) \end{aligned}$$

$$Adler - 32(D) = (B65536 + A)$$

This algorithm creates the final checksum with a length of 8 characters. Afterwards

the generated NONCE is truncated to a 6 character length NONCE.
Through this method, the possible number of unique NONCE is $(10 + 26)^6 = 2176782336$ which is a huge number and enough for our needs.

Chapter 4

Conclusion

While there are many security solutions that address getting rid of third-party intermediaries, no particular solution has been implemented yet that solves this specific scenario of having third-party intermediaries who would deal with involved parties, without getting any access to users' personal data. There is a shortage of research that focuses on (i) privacy, (ii) third-party intermediaries, (iii) no double-spending and (iv) security altogether. Thus, this research is conducted to address this unventured territory of this specific scenario in Bangladesh. In this proposed model, it would be possible to eliminate the third party entities' or the merchants' access to sensitive information like the users' personal phone numbers. This model is made up of a chain of a king server, which is connected to 64 leaders for each district of Bangladesh, and multiple merchants and users under each leader. Each leader covers a district, and these are called zones. The merchants and users cannot communicate among themselves, it needs to happen through the leader, and also the king if the communication is between different zones. Based on this the model is also divided into 2 layers. Through the implementation of these zones and models, and other security measures like the computer-generated data and codes, this model deals with the problem of user data leaking through merchants, making the mobile banking system more secure. In the future, the proposed model can be developed and implemented, which might reveal some practical errors or application related bugs that can be used to modify the model.

Bibliography

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system bitcoin: A peer-to-peer electronic cash system," *Bitcoin. org. Disponible en https://bitcoin. org/en/bitcoin-paper*, 2009.

[2] E. Nwogu and M. Odoh, "Security issues analysis on online banking implementations in nigeria," *International Journal of Computer Science and Telecommunications*, vol. 6, no. 1, pp. 20–27, 2015.

[3] S. Dhar and I. Bose, "Smarter banking: Blockchain technology in the indian banking system," 2016.

[4] Y. Guo and C. Liang, *Blockchain application and outlook in the banking industry. financ innov 2: 24*, 2016.

[5] X. Xu, C. Pautasso, L. Zhu, *et al.*, "The blockchain as a software connector," in *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, IEEE, 2016, pp. 182–191.

[6] F. Glaser, "Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis," 2017.

[7] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th international conference on advanced computing and communication systems (ICACCS)*, IEEE, 2017, pp. 1–5.

[8] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," in *International conference on exploring services science*, Springer, 2017, pp. 12–23.

[9] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, "A critical review of blockchain and its current applications," in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, IEEE, 2017, pp. 109–113.

[10] L. I. L. TC, "A survey of blockchain security issues and challenges ij netw," *Secur*, vol. 19, no. 5, p. 653, 2017.

[11] N. H. Azad, "Disruption on its way, are banks ready?" *The Daily Star*, May 2018.

[12] S. Han, Z. Xu, and L. Chen, "Jupiter: A blockchain platform for mobile devices," in *2018 IEEE 34th International Conference on Data Engineering (ICDE)*, IEEE, 2018, pp. 1649–1652.

[13] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of blockchain," in *2018 10th international Conference on communication Software and networks (ICCSN)*, IEEE, 2018, pp. 562–566.

[14] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[15] J. Abou Jaoude and R. G. Saade, “Blockchain applications–usage in different domains,” *IEEE Access*, vol. 7, pp. 45 360–45 381, 2019.

[16] S. Fernandez-Vazquez, R. Rosillo, D. De La Fuente, and P. Priore, “Blockchain in fintech: A mapping study,” *Sustainability*, vol. 11, no. 22, p. 6366, 2019.

[17] W. L. Harris and J. Wonglimpiyarat, *Blockchain platform and future bank competition*, Jul. 2019. [Online]. Available: https://doi.org/10.1108/FS-12-2018-0113.

[18] M. M. Shahriyer and M. Monim, “Blockchain based land registry with delegated proof of stake (dpos) consensus in bangladesh,” Ph.D. dissertation, Brac University, 2019.

[19] *9 arrested for defrauding money via bkash*, Oct. 2020. [Online]. Available: https://archive.dhakatribune.com/bangladesh/2020/10/17/9-arrested-for-defrauding-money-via-bkash.

[20] T. A. Khan, A. T. Hasan, Q. Jiang, and Q. Qu, “A hybrid blockchain-based zero reconciliation approach for an effective mobile wallet,” in *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, IEEE, 2020, pp. 1–6.

[21] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, and V. Weerakkody, “Blockchain for next generation services in banking and finance: Cost, benefit, risk and opportunity analysis,” *Journal of Enterprise Information Management*, 2020.

[22] G. Sankaranarayanan and K. K. RAJAGOPALAN, “Usage of blockchain technology in banking sector and its implication on indian economy,” *Alochana Chakra Journal*, vol. 9, no. V, 2020.

[23] L. Xu, L. Chen, Z. Gao, *et al.*, “Supporting blockchain-based cryptocurrency mobile payment with smart devices,” *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 26–33, 2020.

[24] C. Insights, *How blockchain could disrupt banking*, Jul. 2021. [Online]. Available: https://www.cbinsights.com/research/blockchain-disrupting-banking.

[25] M. J. Tuyisenge, “Blockchain technology security concerns: Literature review,” 2021.

[26] J. Zhang, R. Tian, Y. Cao, *et al.*, “A hybrid model for central bank digital currency based on blockchain,” *IEEE Access*, vol. 9, pp. 53 589–53 601, 2021.

[27] T. Ansari, “Blockchain, a poorly explained concept9,” Sep. 2022.

[28] S. Goschenko, “Buenos aires might implement blockchain systems to make social aid payments sergio,” Sep. 2022.

[29] Y. Xie, Y. Li, and Y. Ma, “Data privacy security mechanism of industrial internet of things based on block chain,” *Applied Sciences*, vol. 12, no. 14, p. 6859, 2022.

[30] *Cut the call if anyone asks for your bkash account pin or 6 digit verification number.* [Online]. Available: https://www.bkash.com/avoidfraud.

[31] E. Efimov, E. Koroleva, and A. Sukhinina, "International journal of technology,"

[32] S. Nusrat, "Use of blockchain technology in banking in bangladesh; usefulness, hurdles and recommendations,"

[33] *Rocket.* [Online]. Available: https://www.dutchbanglabank.com/rocket/cashin.html.

[34] *What is blockchain?* [Online]. Available: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain.

[35] . [Online]. Available: https://www.bkash.com/bn/products-services/cash-out/agent.

[36] . [Online]. Available: https://www.bkash.com/bn/products-services/cash-in.