Secured Taxation Operation Using Transaction Functionalities of Blockchain

by

Md. Asif Talukdar
17101305
Fatema Dil Afrose Mim
16301069
Noshin Tabassum
17101104
Ayesha Siddika
17201067

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 and Engineering

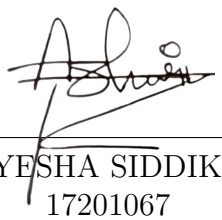
Department of Computer Science and Engineering
Brac University
October 2020

Declaration

It is hereby declared that

1. The thesis submitted is 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.

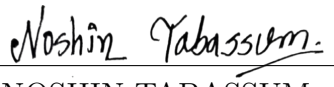
Student's Full Name & Signature:



AYESHA SIDDIKA
17201067

MD. ASIF TALUKDAR
17101305

FATEMA DIL AFROSE MIM
16301069



NOSHIN TABASSUM
17101104

Approval

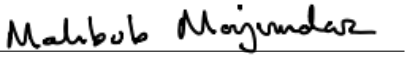
The thesis titled "Secured Taxation Operation Using Transaction Functionalities of Blockchain" submitted by

1. Noshin Tabassum (17101104)
2. Fatema Dil Afrose Mim (16301069)
3. Md. Asif Talukdar (17101305)
4. Ayesha Siddika (17201067)

Of Summer, 2020 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science and Engineering on October 05, 2020.

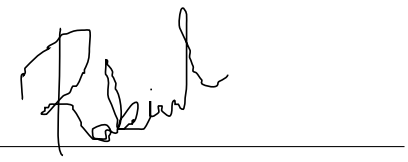
Examining Committee:

Supervisor:
(Member)



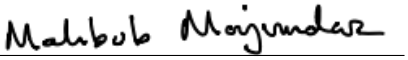
Mahbubul Alam Majumdar, PhD
Professor and Dean
School of Data and Science
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)



Md. Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)



Mahbubul Alam Majumdar, PhD
Professor and Dean
School of Data and Science
Department of Computer Science and Engineering
Brac University

Abstract

The conventional process of tax payment includes laborious steps and many participants which became a regular issue of public dissatisfaction. As a result of being sloppy monitoring and numerous participation irregularities are happening by both taxpayers and tax-collecting authorities. Nowadays, cryptocurrencies are operating secured transactions using the security protocols of Blockchain. We aim to implement a tax payment system using the functionalities of Blockchain technology so that we can resist the fraud activities, multi-involvements, corruption, and all other infringement which are responsible for the mismanagement of the central taxation system. Along with this, the model which we are proposing will also ensure proper security, higher speed, and well-developed management for the transactions.

Keywords: Blockchain, Distributed Ledger Technology , Cryptocurrency, Proof of Authority, Smart Contract, ECDSA, Solidity, Merkle Root, Peer-to-Peer Network, TAXCOIN, Decentralized, Miner, Wallet, Hash.

Acknowledgement

At the very beginning, we would like to thank Almighty Allah for showing us the right path as well as to direct us for pursuing our career in engineering field. We would like to express our heartfelt gratitude towards our thesis supervisor Prof. Mahbubul Alam Majumdar, Dean, School of engineering, BRAC University for supporting us. We would also like to show gratitude towards Md Shariful Islam Shishir, Application Security Manager (e-Service), ICT Division of Bangladesh, for his encouragement and helpful directions in improving our ideas of implementation. We take this sincere opportunity for expressing gratitude to all those who have helped us or at least intended to help us. We would also like to thank our parents, family, friends for their kind motivation and continuous support towards our work. Finally, we place on record our sense of gratitude to one and all who directly or indirectly have involved themselves in our work.

Table of Contents

Declaration i

Approval ii

Abstract iii

Acknowledgment iv

Table of Contents v

List of Figures vii

List of Tables viii

Nomenclature ix

1 Introduction 1

2 Background Study 3
2.1 Blockchain History . . . 3
2.2 An Overview of Tax and its Importance . . . 5
2.2.1 Tax and Development of a Country . . . 5
2.2.2 Tax System in Bangladesh . . . 6

3 Literature Review 9
3.1 Expansion of Blockchain . . . 9
3.2 Money Transmission Using Cryptocurrency . . . 10
3.3 Blockchain and Finance . . . 10
3.4 Future of Taxation Using Blockchain . . . 11

4 The Characteristics of Blockchain 13
4.1 Better security . . . 13
4.2 Faster Settlement . . . 13
4.3 Immutability . . . 13
4.4 Decentralized . . . 14
4.5 Anonymity . . . 14

5 The Core Components of Blockchain Technology 15
5.1 Node . . . 15
5.1.1 Full Node . . . 15

5.1.2 Miner Node . . . 15
5.1.3 Partial Node . . . 16
5.2 DLT (Distributed Ledger Technology) . . . 16
5.3 Consensus Algorithm . . . 17
5.3.1 Different Types of Consensus Algorithms . . . 17
5.4 Peer-to-Peer Network . . . 19

6 Blockchain and Block **20**
6.1 Tree . . . 21
6.2 Merkle Root . . . 22
6.3 Hash Function . . . 23

7 Transaction Using Blockchain Technology **24**
7.1 Wallet Creation . . . 24
7.2 ECDSA (Elliptic Curve Digital Signature Algorithm) . . . 26
7.3 TAXCOIN Transaction Process . . . 32
7.4 Smart Contracts . . . 33
7.4.1 How Smart Contracts Work . . . 33

8 Implementation and Analysis **35**
8.1 Details of our Experimental Setup . . . 35
8.2 Setting up Required IDEs and Extensions . . . 35
8.3 Algorithm . . . 37
8.4 Result and Analysis . . . 38

9 Conclusion and Future Research **39**
9.1 Conclusion . . . 39
9.2 Future Work . . . 39
9.3 Limitation . . . 40

List of Figures

1.1 Workflow Diagram 2

2.1 Blockchain Market Size, [27]. 4
2.2 Total tax revenues as a percentage of GDP [7]. 6
2.3 Pie chart showing the incoming resources, [17] 6
2.4 Pie chart showing total tax revenue, [17]. 7

4.1 The Characteristics of a Blockchain 14

5.1 Nodes connected to the network 16
5.2 Peer to peer network 19

6.1 Blockchain structure 20
6.2 Tree structure 21
6.3 Merkle tree 22
6.4 Hash function 23

7.1 Transaction process 24
7.2 Bar Diagram of Blockchain wallet users, [30]. 26
7.3 ECDSA Explained 27
7.4 comparing the security between RSA and ECDSA, [33]. 27
7.5 Bar Diagram comparing the security between RSA and ECDSA, [33]. 28
7.6 Geometric description of the addition of two distinct elliptic curve points: P+Q = R, [2] 29
7.7 Geometric description of the doubling of an elliptic curve point: P+P = R, [2] 29
7.8 Time comparison between RSA and ECDSA, [6] 31
7.9 Transaction process of TAXCOIN 32

8.1 Transaction confirmation 36
8.2 Transaction complete 36
8.3 Before transaction balance and tax amount 38
8.4 After transaction balance and tax amount 38

List of Tables

2.1 Blockchain Market size from 2018 to 2025(in billion U.S. dollars) [27]. 4

7.1 Number of Blockchain Wallet users , [30]. 25
7.2 Execution time comparison, [6] 31

Nomenclature

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

DLT Distributed Ledger Technology

$dPoW$ Delayed Proof of Work

DSA Digital Signature Algorithm

ECC Elliptical curve cryptography

$ECDSA$ Elliptic Curve Digital Signature Algorithm

$P2P$ Peer-to-Peer Network

PoA Proof of Authority

PoW Proof of Work

RSA Rivest-Shamir-Adleman

SHA Secure Hash Algorithm

Chapter 1

Introduction

The world economy had been facing a major financial crisis from the last decade. Lower economic growth, imbalance in the stability of the system, poor management system, corruption, and financial stress are the major reasons behind the falling economic graph of the whole world. This financial crisis had turned into a global crisis in the year 2007-2008 as the financial stress is transmitted on a huge level and the whole world economy had faced a severe drop. Moreover, mismanagement in financial institutions, unsophisticated regulated monetary and unstructured fiscal policies plays a vital role in this global crisis. Here the concept of the digital system arises to prevent such occurrences. Will the digital system be able to eliminate these problems? Can it be used to create a more secure system that can independently stable the economy without any government involvement? Can the digital decentralized network system be able to implement more regulated and secured taxation policies? If yes, Then How! In this digital world, digital currency and the decentralized network system support the thought of cryptographically chaining Blocks of knowledge relying solely on technology which is detached from any intermediaries. That was the beginning of the first digital decentralized cryptocurrency which is the bitcoin. Today, Blockchain has advanced from being a calm nearness behind Bitcoin to an innovation that might change how we direct installments, store information and perform exchanges. To be specific, Blockchain is not Bitcoin, so the data put away isn't cash or money, however, may likewise be an assortment of other information types also.In general, a Blockchain is records of data that is replicated across computers and these computers use a Peer-to-Peer network technology. The correspondence inside the system utilizes cryptography to give secure recognizable proof of who sends the data and who gets it. At the point when a peer needs to include a bit of information to the record, other peers must affirm the rightness of the data, which thus is added to a Block. Each Block contains a unique hash of the past Block, connecting them to make a chain of Blocks. A unique hash is like a digital fingerprint. This innovation eliminates the need for centralization through a mediator, enabling parties to share data also execute legitimately with one another in a protected way [8]. According to the world economic forum 2015 data set, a conference of 800 business leaders was held and 73 percent of them believe that the government should implement Blockchain technology for collecting taxes by 2023 [11].

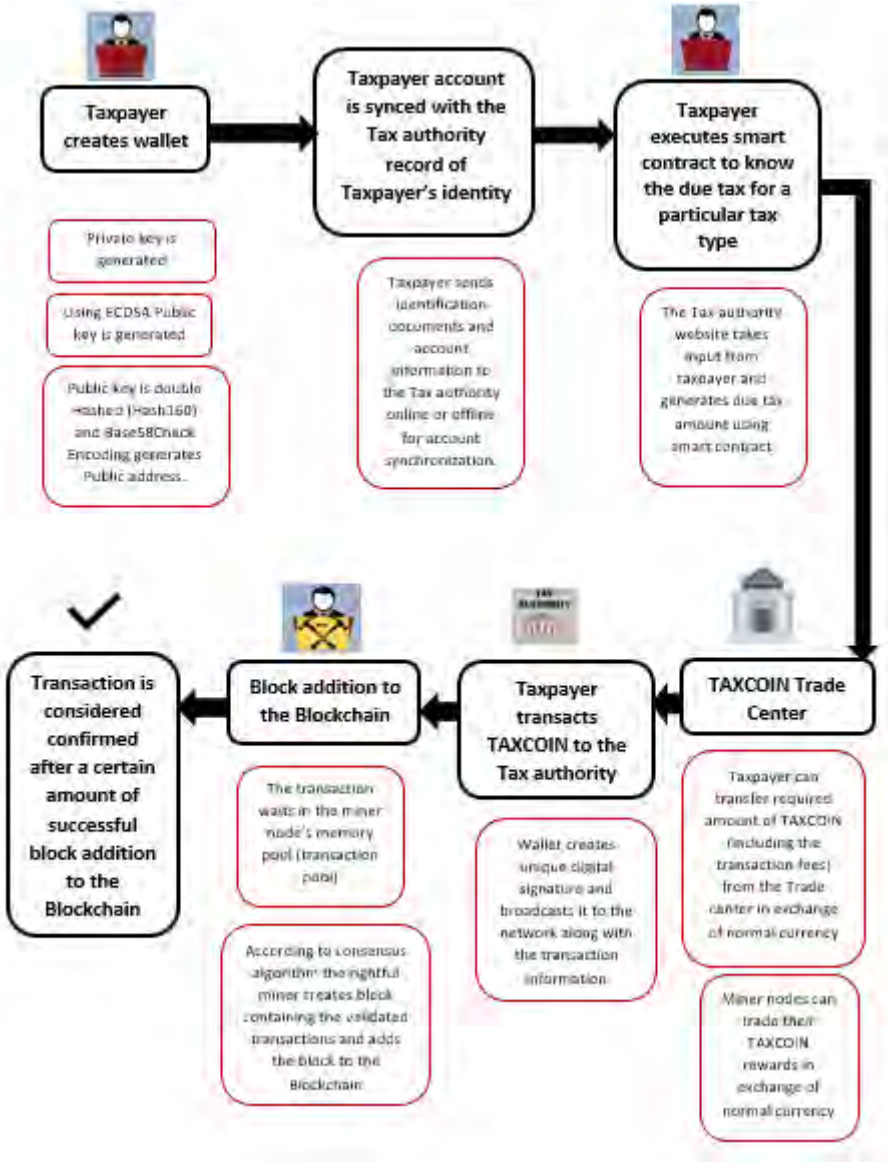


Figure 1.1: Workflow Diagram

We aim to use this modern technology of Blockchain and use it for the digital system of Tax transactions. Many countries in Europe and South America have expressed their desire to use the Blockchain in the taxation system. We will use a decentralized network and a developed digital currency for the transaction purpose and there will be a smart contract where the algorithm for calculating different types of taxes will be given. The users will get to know about the amount of tax they have to pay from the system and they will have solid proof of transaction. The transaction will be conducted in real-time. It will significantly reduce the risk of mistakes and fraud, double spending, counterfeiting high speed of cash moves between organizations and the legislature, the system will get immediate knowledge into an organization's accounts, the regulatory weight of organizations will be essentially diminished, sparing time and the expense of accounting services. Consequently, the multi-dimension checks significantly reduce the chance of VAT frauds during transactions.

Chapter 2

Background Study

2.1 Blockchain History

To a lot of people, Blockchain may sound like new technology. But it is not new. There lies a huge history of innovation behind the creation of Satoshi Nakamoto's first Blockchain. If we want to look at the roots, we have to start with libertarianism. Back in 1970, a political ideology known as libertarianism was introduced. According to the libertarians, the centralized authority should be as minimal as possible considering people's privacy as a priority. During that time two groups were formed via discussions and forums. These are: Cypherpunks and Crypto-anarchists. The Cypherpunks wanted something to be as fast as the internet and as free of cash. Both of the groups were in favor of using cryptography to protect one's privacy. But designing cryptography was not an easy task. With each failure, they came close. During the 1990's period, cryptographer David Chaum introduced "Blind signatures". Using the latest advancements of public and private key cryptography, he also implemented one of the first known cryptocurrencies named "DigiCash". It allowed users to conduct online transactions without the intervention of the government. But soon it failed because of the centralized way of validating each digital signature in the DigiCash system. Also in 1991, Stuart Haber and W. Scott Stornetta did the first work on a secured chain of blocks. In the next year 1992, Merkle trees were introduced. This enabled multiple documents to be stored in a single block. A few years after DigiCash, there came HashCash. The main goal of Hashcash was to solve the problem of email spamming. For sending an email, a user had to solve a cryptographic hash puzzle and provide a proof of their work that they have spent enough computational power to add a Hashcash stamp to their email header. Thus the recipients could verify emails. Based on the HashCash's proof of work mechanism, B-money was introduced. In 1998, a paper titled, "B-money, an anonymous, distributed electronic cash system," was published by Wei Dei. In this paper, Dei laid out some core concepts that later helped to shape the modern cryptocurrency. Some of B-money's core concepts are: using a proof of work function like HashCash as a means of creating money, maintaining the database showing who owns that, verifying the work by the whole community who all work for updating a collective ledger, authenticating transactions with cryptographic hashes, giving reward to the workers for their efforts in creating money, signing the transactions with digital signatures. In the early '20s, a protocol named BitGold was proposed by Nick Szabo that incorporated a Blockchain-like system. This protocol also involved

Proof of work and time-stamping features. BitGold was also a failure because of having double-spending problem. Everything mentioned until this point established the foundation of the first real blockchain. In October 2008, Satoshi Nakamoto published a white paper titled, "Bitcoin: A Peer-to-Peer Electronic Cash System" [43]. This paper outlined the basic design for a cryptocurrency that requires no authoritative figure. In January 2009, Nakamoto created the first block known as genesis block with the help of Hal Finney. In the next year, the first real trade of Bitcoin happened when Laszlo Hanyecz purchased a 25 dollar worth pizza with 10,000 Bitcoin [28]. A lot of people who do not have proper knowledge of Blockchain assume that Bitcoin and Blockchain are the same. But in reality, they are not. Bitcoin is a cryptocurrency that has been built on Blockchain technology [43]. Since 2009 to present, there have been some noticeable innovations in Blockchain. Such as: huge increases in file sizes of blockchain, innovations to the way they work, and an increase in the prices of the shares of the technology. However, the term, "Blockchain 2.0" was first used in the "Economics Magazine" in 2014. It refers to the development of applications that can be run on a blockchain database. This breakthrough was a huge step forward in Blockchain technology. After the reveal of this concept, people started seeing the possibility of running decentralized applications on a blockchain network.

Year	Blockchain market size (in billion U.S. dollars)
2018	1.2
2019	2.2
2020	3
2021* (Expected)	7
2022* (Expected)	12.7
2023* (Expected)	23.3
2025* (Expected)	39.7

Table 2.1: Blockchain Market size from 2018 to 2025(in billion U.S. dollars) [27].

Figure 2.1: Blockchain Market Size, [27].

The following year, 2015 witnessed the launch of blockchain 2.0. During that time, Vitalik Buterin thought of how Bitcoin could be improved and wrote the code for Ethereum. The Ethereum Blockchain was officially recognized on July 30th, 2015. Though the emergence of blockchain-based projects started in 2014, 2017 is the year marked by an explosion on blockchain-based platforms.Day by day the number of Blockchain users is increasing rapidly. People have started to put their faith in Blockchain technology.

Seeing the progress in Blockchain technology, we can hope for this being used in the projects where transparency is one of the priorities.

2.2 An Overview of Tax and its Importance

Tax is a mandatory financial charge which is imposed by the government upon its eligible citizens so that they can earn some revenue from the people of the country. In monetary terms, taxation converts capital to the government from individuals or corporations. This has implications that can both improve and decrease long - term economic growth welfare.

2.2.1 Tax and Development of a Country

Tax is directly connected to the development of a country. It is one of the ways that the government increases money. The governments usually impose taxes on people and corporations by levying charges on them. To meet the fiscal demands of the people and corporations, tax is used. Starting from funding public and government programs to dealing with the economic development of a country, everything is involved in those fiscal demands. In a country, taxes help raises the standard of living. The stronger the standard of living, the deeper and higher the most likely level of consumption is. When there is a demand for their goods and services, businesses prosper. With a better standard of living, firms will also be assured of increased domestic demand. Without taxation, it would be difficult for governments to fulfill the demands of their populations. Taxes are important because this revenue is collected by governments and used to support social programs. A graph of the tax effect on GDP has been provided for better Understanding. In the graph, total tax revenues are shown as a percentage of GDP [7].

There are several of these projects such as education, governance, housing, etc. Besides, taxes can influence the state of a nation's economic development. Taxes usually contribute to a country's gross domestic product (GDP). Taxes help promote economic growth because of this contribution, which in turn has a ripple impact on the economy of the country; raising living standards, growing job creation, etc. GDP sets the benchmark of the economy of our country. In Bangladesh, we collect the maximum GDP from our agricultural and our garments factories. So, in the end, we can say that our atomic source of development depends on taxation or the revenue system.

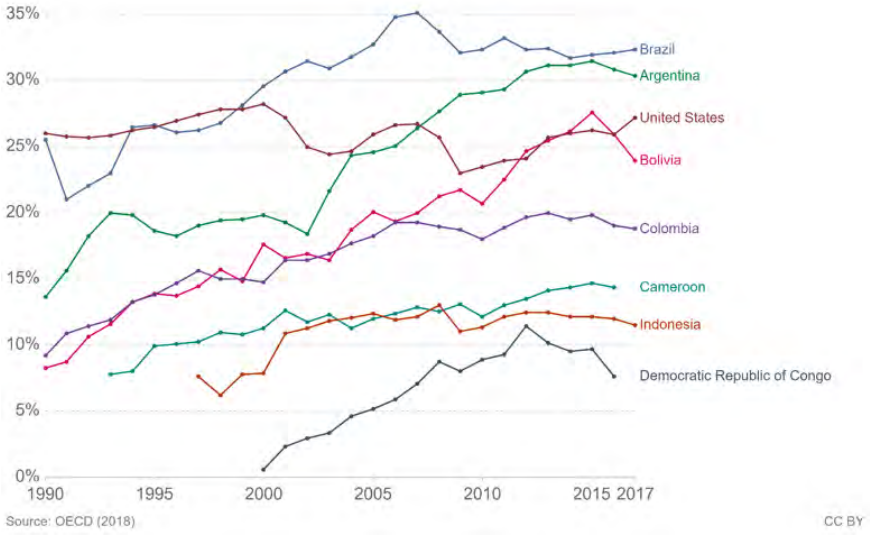


Figure 2.2: Total tax revenues as a percentage of GDP [7].

2.2.2 Tax System in Bangladesh

Bangladesh earns a huge amount of internal capital from the tax. The percentage of it is 80 and this is undoubtedly a huge amount. Again, indirect taxes add more than 75 percent of the overall tax yield of our country. Moreover, in our country, the majority of money comes from tax revenue and for example, the total revenue in the 2014-15 financial year (FY) was TK.182954 crore, of which the actual share of tax revenue was TK.155292 crore (84.88 percent) and non-tax revenue was TK. 27662 (percent 15.12) [1]. The national budget of Bangladesh for the fiscal year 2019-20 is 5,231.90 Billion Taka. The Tax revenue is almost 62.2 percent of that budget which is approximately 3,256 Billion. A pie chart showing the portion of tax in our economy is given below [17].

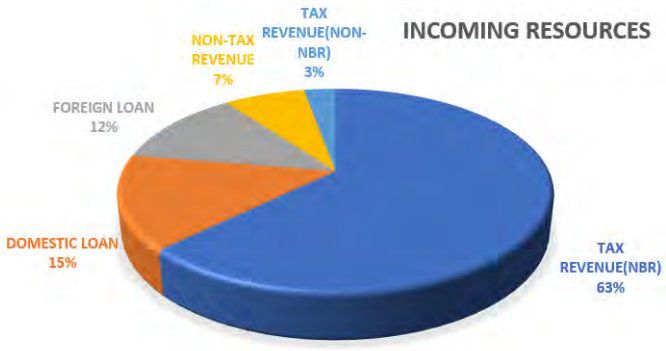


Figure 2.3: Pie chart showing the incoming resources, [17]

Nevertheless, if we compare our taxation policy with our neighboring countries, we are still way too behind in the matter of tax collection. Narrow tax base, huge corruption, the administrative imbalance is the main reason behind the failure of our taxation policy. Bangladeshi government legalizes different types of tax in the country. Tax can be based on property, can be based on corporate earring, and so on. Different types of taxes have been discussed in the following sub-sections. A graph representing tax revenue is given below [17].

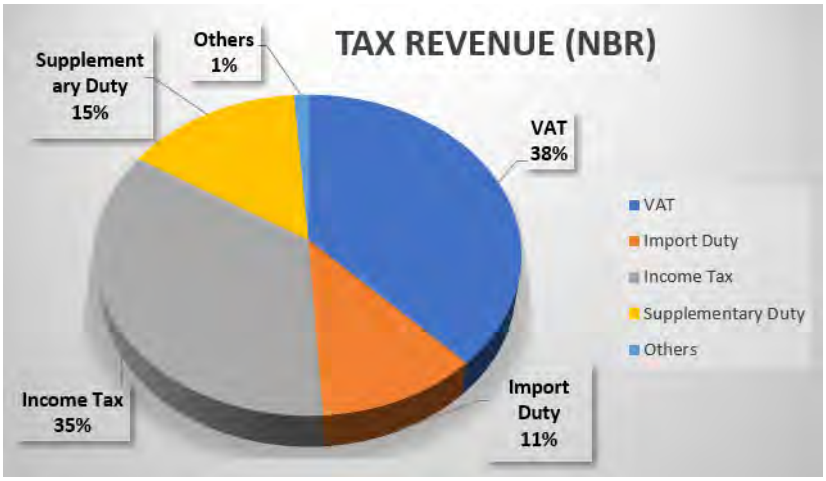


Figure 2.4: Pie chart showing total tax revenue, [17].

Income Tax

As per the financial act, 2015 the Bangladeshi people have to pay income tax based on the computation of their total income and charging tax thereon. These sources of income are divided into seven categories that are wages, interest on securities, and income from house property (in case someone owns a house), agricultural income (income from the crops, livestock products, etc.), and income from a business (The profit from a business), capital gain (profit from the sale of a capital asset), and income from other sources [36].

Corporate Tax

Corporate tax is imposed on any company's earning by the government according to tax law. This is also called corporation tax or company tax. The amount of money collected from this tax is used as a nation's source of income. In Bangladesh, the corporate tax rate for the listed entries is 25 percent and for the non-listed entry, it is 35.5 percent for the FY 2020-21 except for banks, leasing and insurance companies, mobile phone companies, and cigarette manufacturers. But recently, the non-listed tax rate has been reduced from 35.5 to 32.5 percent because of COVID-19 [24].

- The corporate tax rate is 25 percent-45 percent [37]
- The branch tax rate is 35 percent [37]
- The capital gains tax rate is 15 percent [37]

Tobacco Tax

The type of tax that is charged on all types of tobacco or tobacco products is known as tobacco tax [23]. In Bangladesh, 10-sticks lower slab cigarette costs 30 takas and above and for this, the supplementary duty costs 57 percent.

Withholding Tax

Withholding tax is a tax that is deducted upfront by the payer while making any payment for any supply of goods or services received. In most jurisdictions, the withholding tax applies to employment income. The amount of withholding tax on income payments other than employment income is usually a fixed percentage. In the case of employment income, the amount of withholding tax is often based on an estimate of the employee's final tax liability, determined either by the employee or by the government [40]. The Bangladeshi finance Minister proposed to bring down the rate of tax deduction at source (TDS) at the stage of local supply of essential commodities, such as Rice, Wheat flour, Potato, Garlic, Onion, etc. from 5 percent to 2 percent irrespective of the base price [22].He also proposed to reduce the TDS rate to 2 percent (currently 5 percent) on the import of Garlic, Sugar, and raw material of poultry feed. He suggested amending the ordinance to fix the rate of withholding tax on all sorts of export proceeds including RMG at 0.5 percent instead of the existing rate of 1 percent [22].

Value Added Tax (VAT)

Value-added tax is a consumption-based tax which added with different types of goods or products in their production time. Each company during their production stage has to pay VAT based on the value of the product and the VAT which has been paid formerly for a particular product has been lessening in each step. Hence, the final customer who is the general people has to pay each time even if they have paid VAT for the product previously. Moreover, there 140 countries and all the OECD countries except the USA uses VAT to earn a handsome amount of tax and ensures economic growth for their countries.

Export and Import Tax (Tariff)

A tariff is a tax that is imposed on the products which are exchanged between two separate independent countries. It is a part of foreign trade policy and it ensures a safe and secure transaction of products between different countries. It also allows countries to increase their yearly income in a good manner. However, the value of the Tariff does not remain constant always. The value can a variable when a product value varies each time or a constant one when a portion of the product has a fixed charged. This tax system not only ensures global trade but also promotes international industrialization.

Chapter 3

Literature Review

3.1 Expansion of Blockchain

In this present era, the gradual maturation of some transformative emerging technology provides promises to fundamentally reshape our society. Reshaping society includes focusing on how individuals and companies generate money, products, and services along with their way of handling everyday encounters with one another. Our current era is already concerned as 'second machine age' (Brynjolfsson McAfee, 2014). These technologies include machine learning, computer science, and Blockchain or distributed ledger technology. The expansion of these technologies has made it possible in updating the world into a more digitized version. A model of the future taxation system using Blockchain properties has already been proposed by a group of people [18]. 10ex As we all know that the revenue agencies operate in the dead core of society, they are expected to be ready always to respond to the changes in their environment. Because they form a significant element in improving the social contract between the government and its industry and citizens. Then again, these tax authorities often face expenditure limitations along with being required to do something for fewer. There are other challenges as well (e.g. an aging workforce, increasingly competitive society). To balance these limitations and pro-active innovations, we must understand the way of increasing the efficacy of existing business processes using currently accessible and upcoming technologies. They tried to find a solution using distributed ledger technology (DLT). It is getting popular day by day by offering a modern infrastructure for economic transactions. They found four scenarios that were constructed using four scenario building blocks. The research questions behind these scenarios were focused on the future impact of DLT in 2025 on tax domains in society. The scenarios are as such: Dual reality, Blocktopia, Govchain, beyond the hype. And the four scenario building blocks are Governance, Industry, Cryptocurrency, and Society. If we look at the matters stated here from a revenue body viewpoint, these scenarios reflect the most significant uncertainties surrounding DLT innovations. Here, the dual reality of governance is that being lagged in the knowledge they lack in taking proper steps. The dual reality of the industry is a strong investment and development of standards. Again, cryptocurrency is not under the control of authorities and can be used in criminal activities. Society's negative publicity and limited trust in accepting a new technology is a dual reality as well. In the second scenario, it is noticed that a small number of cryptocurrencies are considered safe. Some people want to put their trust in this and

some don't. Thus, people can be digitally divided. Intermediaries can be cut out discharged. There are also a few people who worry about limited freedom. Hence, a huge level of trust is required along with acceptance. This also raises questions regarding public interest in adopting Bitcoin. Thus, uncertainty remains in all of this.

3.2 Money Transmission Using Cryptocurrency

Throughout the years, there have been a lot of demonstration about the digital transmission of money using cryptocurrency. It is a digital or virtual currency that is protected by cryptography. This cryptographic virtual currency almost makes it impossible for anyone to counterfeit or double-spend [26]. It uses the peer to peer transaction system. In modern days central banks are also showing their interest in digital currencies for innovating many new ways of banking-related things [4]. They are trying to create a built-in distributed ledger and allowing non-banks to be involved in the transaction system [4]. Though involving non-banks can create problems in the distributive system and can raise security questions [3]. However, the first and one of the most known cryptocurrency, Bitcoin has been proven to be much secured in terms of privacy and safe online transactions [9]. The Bitcoin protocol and its major components together with its features and network interactions play a vital role in ensuring the security of the system.

On another note, if we talk about the negative aspects, there are tons of problems that can occur because of digital currencies. But then again, there are also tons of policies which are being used to solve these problems. The key issue which is needed to be mentioned here is the anonymity surrounding cryptocurrencies. There should be a system where it will be mandatory for all of the users to complete their registration processes properly. Then they will know to follow a proper framework for using the crypto coins. Therefore, there are a lot of research challenges and perspectives for using cryptocurrencies [5]. As this technology is emerging at a very high speed there should be some proper manner to use it more appropriately and efficiently [5]. A modified design space has been provided for comparative analysis of consensus mechanisms, computational puzzles, currency allocation mechanisms, and key management tools.

3.3 Blockchain and Finance

If we notice carefully, we can realize that Blockchain's growth is at a very early stage. Also, there are several problems to be addressed by users and researchers. An irrefutable truth regarding Blockchain is that even after eleven years of the launch of Bitcoin as of September 2020, cryptocurrencies remain the only good example of a popular Blockchain system. Nevertheless, Bitcoin has some flaws in its system such as the consensus algorithm of it (PoW). The flaws in Proof of Work (PoW) contribute to various issues like a waste of a lot of computational power along with excessive usage of resources. A suggestion is given were using a cryptographic extension named ZeroCoin which is unlink-able and unreachable, can solve the problem. This problem can also be solved using CryptoNote, MimbleWimble, ByzCoin, Ethereum, Mastercoin, Litecoin, etc. Apart from implementing cryptocurrency, Blockchain can

also prevent illegitimate activities like money laundering, terrorist financing, and tax evasion [12]. Blockchain has yet to solve some key challenges. These are technology complexity and a deficient number of IT professionals who have the potential to create a Blockchain company. Besides, the challenge of converting it into a more complicated structure remains there. This is the reason why taxation is still a work in progress. It is known that developing technology is an evolving process. Without significant creation and brainstorming, groundbreaking innovations like the internet would not have reached the height that it has achieved today. Again, Blockchain offers multiple advantages. And we have already experienced some of them. Though the biggest interest and excitement is focused around financial services and banking, it is still interesting in the taxation field from a long-term perspective [8].

3.4 Future of Taxation Using Blockchain

Another question has been raised that how Blockchain and linked data can bring advancement in taxation. If the distributed ledger system gets allowed, it will support smart contracts technology. Thus, it gives a legitimate platform opportunity to create a completely digital tax system. The Researchers have proposed a permitted Blockchain-based administration to remove some of the flaws that the authorities are currently facing worldwide. Such multi-billion shortages of money are indicated as tax deficit or tax gap. This is the failure to collect the full amount owed to a specific authority (e.g. government) by a particular individual. On the contrary, the authority can put a stop to this illegal operation. They are investigating the use of Blockchain for that. Hence, they are already conducting researches for using Blockchain's potential in government sectors. In taxation management, permission Blockchain plays an important role. Along with this, Hyper ledger Sawtooth is considered to be useful in replicating systems and processes for real-world tax governance because it has on-chain governance features. Sawtooth can be used by managing bodies to ensure duties and approvals. They can set up access to data so that confidential information can only be accessed by individuals who are party to a transaction.

Moreover, for synchronizing data among the tax-authorities automatically in real-time, the smart contracts are useful. This arrangement is known as 'Consortium Blockchain'. It is also defined as a hybrid between public Blockchain's low trust and private Blockchain's single highly trusted structure model. This Blockchain model described by them can be used to lower the burden of the government, as it is considered valid. On the other hand, even in some developed countries, people are not aware of the pros and cons of using Blockchain technology. For such cases, distributed ledgers are not a cure.

However, the Taxation process allows corporations to enforce consistent procedures along with tracking and monitoring systems to prove a consistent method implementation. Not being co-operative in this manner has far-reaching consequences. This starts ranging from having financial fines to police proceedings. This is endangering the successful position of a business. For easing the tax enforcement efforts of corporations, the organization for Economic Co-operation and Growth (OECD) is now exploring avenues, including Blockchain technologies. In business sectors, ensuring tax acceptance is a nuanced and difficult process. That is why tax enforcement management is mostly implemented as a separate area of responsibility

within a corporation. For making the process more efficient, the tax compliance process needs to join the business processes by architecture [15]. One good thing to be noted here is that tax digitalization is getting speedier. And this is happening because of the adaption of several electronic tax reporting systems in not only developed countries but also in developing countries as well. As a result, now it seems like it is only a matter of time when taxation on all forms will be achieved by implementing Blockchain technology [8].

Chapter 4

The Characteristics of Blockchain

4.1 Better security

A question can arise that as there is no central controlling system in Blockchain how can the security system of it be maintained? So, if you consider the reality then Blockchain will be much more secure than the centralized network system. It uses the concept called cryptography to ensure the security of the data. For the encryption of data which is known as hashing, the SHA–256 cryptography algorithm is used here. If an input is given into Blockchain it generates a fixed-length output value for the respective input. Hence, the actual data has been hidden and a random fixed-length value has been generated by cryptographic technology and consequently, no one will able to encrypt it. One thing to mention here that hashing is irreversible [19] and a single change in data generates a new output value. Another layer of security has been added by the immutable nature of the Blockchain. Each node keeps all the records of the transactions and so no one will able to change, erase or update anything on the network.

4.2 Faster Settlement

Blockchain can transfer data in the fastest manner as it reduces the involvement of any central committee as well as decreases the probability of counterparty attack, ensures transparency. Traditional banking system usually needs at least one day to ensure the transaction of money but in the case of Blockchain, it just transfers digital money within a very short time. So, it saves a lot of time for the users and ensures to finish up everything within a particular time.

4.3 Immutability

The term, "immutability" refers to something that cannot be changed [19]. It is one of the Blockchain's most exciting features. It ensures that the technology remains intact and unaltered throughout time. This also ensures that the technology doesn't depend on any centralized authority.As Blockchain technology uses a peer-to-peer network system, here each node of the system either has the full copy of the ledger or a portion of it depending on the type of nodes. For data transactions using Blockchain, the miner nodes add valid transactions to a new block and solve a

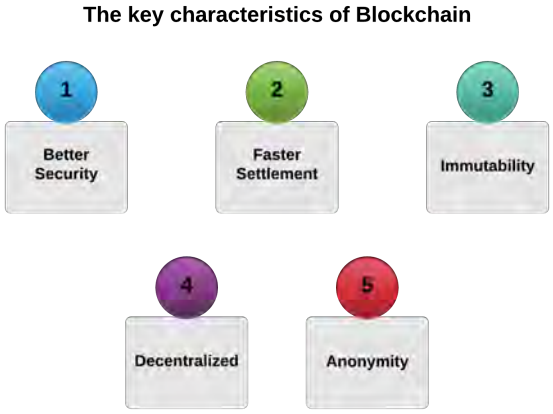


Figure 4.1: The Characteristics of a Blockchain

cryptographic puzzle. After solving the puzzle, the miner node broadcasts the block to the whole network. Upon receiving the block the nodes in the network verify the block and add it to the ledger if it is valid. Thus the whole network converges to a single decision on block addition. In the header section of the new block, the hash value of its previous block is preserved [32]. That's why, after getting verified and added to the network, no node can just go back and edit the information of the ledger according to their will. Consequently, the chaining feature of this technology makes it immutable and invulnerable to malicious activities.

4.4 Decentralized

We know that Blockchain is a decentralized network system. Being decentralized means it doesn't have any authoritative figure to look after the system. Instead of being controlled by a single entity, the network is maintained by the active nodes across the globe. The nodes do not have to rely on a third-party for maintaining their properties rather they trust the protocol. All the nodes in the network have their ledger. So, hackers have to attack the majority of the nodes in the network to break into the system. That's why it is also less prone to breakdown. It will require a lot of energy along with time to attack a decentralized network system like Blockchain. Also, this system cannot be used for anyone's interest, as this is run on algorithms and nobody has the authority to go against the rules set by those algorithms.

4.5 Anonymity

One of the Blockchain's primary concerns is the anonymity surrounding this technology. In the Bitcoin transaction, the wallet address and transaction details are recorded in the blocks. The transaction stays anonymous as long as there is no link between the wallet address and the user's identity (e.g. email ID or anything identifiable) [38]. As there is no limitation of node creation for a user, the user can easily switch between different accounts. These features make it even harder to trace the true identity of the user.

Chapter 5

The Core Components of Blockchain Technology

5.1 Node

A node is a physical network device but there are some cases in which virtual nodes also exist. In the matter of the telecommunication network, nodes sometimes work as a communication end-point. Through a node different types of messages can be created, received, or transmitted. In Blockchain infrastructure, there are different types of nodes which include full nodes, partial nodes, miner nodes, super-nodes, etc. These nodes can be any kind of device (e.g. a computer, mobile phone, or laptop). Different types of nodes perform different kinds of operations. In Blockchain we mainly use two types of nodes. The first one is: Full node (Fully righted node) and another one is: Partial Node (light node).

5.1.1 Full Node

A full node is a part and parcel of a Blockchain network.The full nodes of a Blockchain network make sure that the Blockchain is secure, as they preserve the whole information of the transaction of the network. The current size of the Blockchain is approximately 299GB as of September 2020 [39]. The size is increasing day by day. A full node has two main functionalities. The first one is to store the information of the whole Blockchain and the second one is to verify the newly added nodes.

5.1.2 Miner Node

A miner node is also known as a 'Validator Node'. Only a full node can act as a miner node. Or we can just say that all miner nodes are full nodes but all full nodes are not miner nodes. The miner nodes are responsible for adding new nodes to the Blockchain network. For doing so, they have to solve a complex math problem or cryptographic puzzle using their device. After winning that competition, they get to add the new blocks to the Blockchain. The winner node also gets a reward for adding the new block and contributing their time and resource towards enlarging the network.

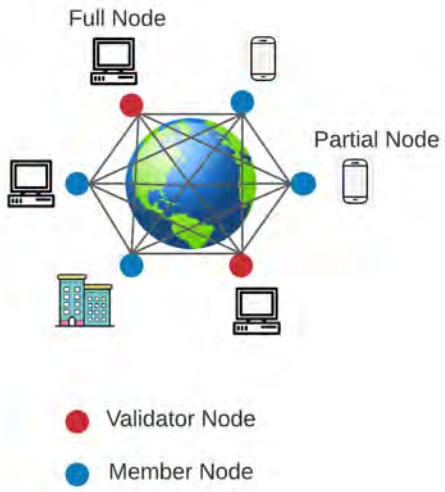


Figure 5.1: Nodes connected to the network

5.1.3 Partial Node

The partial nodes do not contain the whole ledger. They just download the part of the information they require for doing transactions. For doing so, they use SPV (Simple Payment Verification) mode. The most common example of a partial node is a mobile phone. Because someone cannot just download the entire Blockchain in a mobile phone as it has a limited amount of memory [16].

The nodes of a Blockchain network are connected and via that connection, they exchange information regarding the latest Blockchain data (e.g. transaction information).

5.2 DLT (Distributed Ledger Technology)

The digital way of storing data in a decentralized and synchronized manner that is independent of geological location is known as Distributed Ledger Technology or in short DLT. DLT uses peer-to-peer network to share the data among nodes. It is an append-only ledger and features immutability if proper protocol is imposed. Unlike a traditional centralized database system, DLT is not dependent on any central server. Consequently, it avoids the risk of a central single point of failure on data transmission which makes it secure and invulnerable to hacking activity. Moreover, the database is shared among the nodes around the globe and all the full nodes keep a copy of the current synchronized ledger. Therefore, DLT provides transparency on transactions across the distributed network. Moreover, Data is appended on the existing ledger. Therefore, protocols and consensus among the nodes make it impractical for any malicious activity to manipulate the ledger. The consensus among nodes is achieved by a specific pre-defined algorithm. Distributed Ledger can be Permissioned, Permissionless, or Hybrid based on the requirement. Blockchain, Hashgraph, Corda, etc. are an example of DLT. Currently, Blockchain is the popular type of DLT used by Bitcoin, Ethereum, Ripple, Litecoin, and other platforms.

5.3 Consensus Algorithm

Whenever we see the word, 'Consensus' the first thing that comes into our mind is that it is indicating a matter of agreement. As the Blockchain technology is based on a decentralized peer to peer network, no single entity has the authority to decide the state of the blocks in a certain time. Therefore, the question arises on how the system should run. Who is going to add the next block? What should be the procedure for block and transaction verification? How will the incentives for a block miner be determined? Most importantly, how will the whole network reach a common agreement regarding the current condition of the ledger? In the distributed ledger technology (DLT), these problems are solved using a certain protocol which is known as Consensus. The consensus protocol is a predefined set of rules that ensures the security and trust in the network. In the network, any node can join and leave at any time according to their will. Hence, nodes put their trust in the consensus algorithm rather than trusting their peers and agree on common decisions on the network. Miners mine blocks and acts according to the protocol. The Consensus algorithm decides the reward for the miner and sets the difficulty for block mining. Moreover, malicious nodes are also punished by the protocol. This algorithm comprises several unique goals. These are: achieving resolution, unification in decision making, fair treatment for every node, and obligatory participation of each active node in the process. Therefore, the consensus algorithm ensures one single consent for the network which can be considered a victory for the whole system [21]. To date, a lot of consensus algorithms are introduced to maintain various distributed ledger networks such as Proof of Work, Proof of Stake, Proof of Authority, Byzantine Fault Tolerance, etc. Proof of Work is the first and most renowned Consensus algorithm which is implemented on Bitcoin.

5.3.1 Different Types of Consensus Algorithms

In our proposed system, we are suggesting to use a public Blockchain network for making transactions. In the previous part of our paper, we have discussed the importance of the consensus algorithm. And in this part, we are going to explain why we have chosen to use PoA (Proof of Authority) over other consensus algorithms for our implementation. There are various types of consensus algorithms and in our paper, we are going to give a short review on them.

Proof of Work (PoW)

One of the most famous consensus algorithms known as PoW or we can also call it Proof of Work. In 2008, Satoshi Nakamoto released the Bitcoin whitepaper introducing the Proof of Work algorithm. In PoW, the miner nodes need to mine to add a new block to the Blockchain. Miners need to produce a cryptographic hash of the new block. The hash value of the new block should be less than the difficulty target. Once the miner finds the target hash, it propagates the block to the network. Therefore, all the active nodes in the network verify the block according to Nakamoto Consensus. And after doing so, they either add the block to their ledger or reject it in case they find it invalid. When two or more miners mine for the same block and broadcast the block to the network, it can result in a situation where two or more chains of the same network exist. This kind of chain is known as a fork. In the case

of Fork events, the network chooses to continue using the longest chain. It refers to using the chain that has consumed more computational power as the probability of being the valid one is higher for that chain. The difficulty target is adjusted after the addition of every 2016 blocks to maintain the average block-addition period of 10 minutes. Hence, the more hashing power is introduced for mining, the more the difficulty arises. The process of mining requires a lot of computing power along with time and electricity. As of Sep-2020, the current difficulty target is 19 leading zeros that takes 17 to 19 Tera Hashes per second on average to mine a block [41]. The noticeable proportion of electricity used in bitcoin mining can easily power a whole country like Switzerland [14]. The world is already short of available resources and the last thing we need now is to use something power-consuming like PoW.

Delayed Proof of Work (dPoW)

To overcome the shortcomings of PoW, a collaborative consensus algorithm was proposed known as Delayed Proof of Work or dPoW [34]. This algorithm is more secure and energy-efficient than PoW. But the prerequisite of using this algorithm is to use PoW or PoS. Also, there is another problem related to hash rates that can cause a huge difference between the nodes. This can also lead to further complications in implementation and so we are avoiding this one.

Proof of Weight

Proof of weight is also energy efficient along with being highly customizable and innovative. But using this algorithm incentivization can be hard. For such reasons, we are not using these algorithms in our implementation.

Proof of Authority (PoA)

Another most famous consensus algorithm is PoA (Proof of authority). We have used PoA as the consensus algorithm in our implementation.The PoA consensus algorithm allows the validator nodes to mine the block based on their identity that means the block validators are staking their reputation rather than anything else to mine a block [20]. Usually, the authority node randomly select the block miner. Therefore, the identity of the miner can be used to reward honest miner or take action against the malicious miner. The miner nodes are the ones who add the new blocks of a transaction to the Blockchain Network. There are two ways a block can be accepted. One is: being accepted after being voted unitedly by the majority of the network. And another one is: being accepted after being voted by the block generators. One positive thing to be noticed here is, there is no technical competition among the block generator nodes. An appropriate reason behind choosing to implement this algorithm in real-life is: it costs a very low amount of computing power and electricity. A Blockchain network consisting of PoA does not require any local currency like Bitcoin. Unlike Proof of Stake (PoS), here in PoA, the validator nodes do not have to keep their property as a stake to prove their authenticity. Unlike Proof of Work (PoW), it is fast and energy-efficient. In a situation where the nodes are unknown to each other and are having a trust issue regarding each other's validity, there is no better alternative than using PoA [42].

5.4 Peer-to-Peer Network

The distributed peer-to-peer network is one of the most important parts of Blockchain technology. This is also known as the P2P network. A network is a group of interconnected devices that exchange information. All the devices within a network are connected with a cable or they can have a wireless connection. Moreover, there are two types of computer architecture. Among these two types the most commonly used one is the centralized network. It is a centralized client-server model in which there is a central server and it controls the overall communication. Here the central server works like an agent. This server stores all the information of the clients and the history of all types of communications. Despite huge demand, this model has some severe disadvantages. For example, if the central server is hacked all the information of all the clients will be disclosed. Peer-to-peer is another network architecture where all these problems do not exist. In peer-to-peer, there is no central server that is responsible for sharing and storing data. Rather in the P2P network, there is a group of devices and each of them acts as a single node or peer. Here each of the devices acts as a server for sharing information and storing files.

Figure 5.2: Peer to peer network

For the Blockchain network traditional client-server model does not work rather it uses the P2P network architecture as in a Blockchain network there is no essential point of storage and therefore no central controlling parties exist. In a distributed peer-to-peer network, all the information on the network is constantly being recorded and transferred among the participants of the network. All the devices of the network stores multiple identical copies of the shared information. In summation, it can be said that Blockchain technology is built based on the P2P network and as there is no central server the data cannot be easily hacked or lost or exploited.

Chapter 6

Blockchain and Block

Blockchain is the most popular distributed ledger technology. After the release of the Bitcoin white paper in 2008 by Satoshi Nakamoto, Blockchain technology has been the center of attraction for a distributed secure data transfer system. Blockchain uses a peer-to-peer network over a centralized data server system. Peer to peer network prevents the risk of a data breach as the data in the ledger is updated in all the full nodes in the network. All the Blocks in the Blockchain contains the cryptographic hash value of the previous Block except for the Genesis Block (Starting Block). Therefore, it serves the functionality of immutability as changing a bit in the block invalidates the later chain of blocks including the changed block. Henceforth, the cryptographic hash of the previous block is held by the previous hash field in the Block Header. It also ensures security. The peer-to-peer network maintains the one single data ledger over the network based on the consensus algorithm. The block is verified by nodes and the consensus algorithm ensures the consent among the nodes to confirm the block miner. For each block, the miner node gets incentives (Block reward + transaction fees).

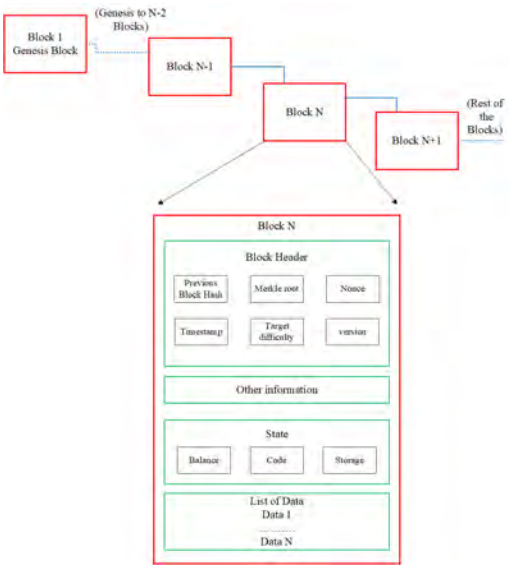


Figure 6.1: Blockchain structure

The Block header usually contains the Target Difficulty field which defines the amount of computing power needed to mine and add a block to the Blockchain. The only way to mine and add a block is to brute force the block and acquire the hash to fulfill the Target Difficulty. After meeting the difficulty in a given time the block becomes the candidate block. Usually, the first candidate block is appended to the ledger if it is valid. Besides, the Timestamp field records the time for the candidate block. The Block contains the transactions data in the data field. The cryptographic hash of all transactions is sequentially hashed to obtain the Merkle root of all the transactions which represents the whole summary of transactions. Merkle Root field in the header contains the Merkle root of the transactions. The Block can also contain other information, code, state of transactions, smart contracts, version, and necessary data to run a particular protocol. The Nonce field in the Block Header is used to brute force and compute the hash of the Block. Nodes alternate the Nonce and the extra Nonce in the coin base transaction (The first transaction of Merkle tree) to achieve the target hash to generate candidate blocks.

6.1 Tree

A tree structure stores data in a hierarchical order. It is an essential part of data structures in computer science. Trees are flexible abstract data types representing structural relations between nodes. Nodes are the unit of the tree and contain data. Sorted tree structure increases efficiency in inserting and searching data into the nodes. The topmost node is called the Root node. Nodes next to a node are known as the child node of that node and the previous one is called parent nodes. The maximum number of child nodes connected to any node is called the degree of that node. The lowest nodes having no child are called Leaf nodes. The nodes between the Root node and Leaf nodes are called Brach Nodes. Nodes with a similar parent are called sibling nodes. All the nodes from the parent node to the root node are called the Ancestor nodes and all the nodes from the child node to corresponding Leaf nodes are called descendent nodes. The tree structure can be segregated into different levels and we can calculate the height, depth of the tree.

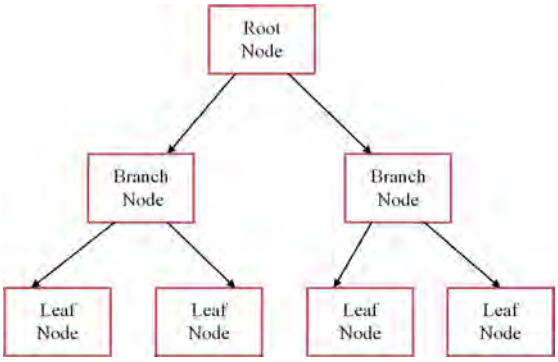


Figure 6.2: Tree structure

In the Blockchain technology, tree data structure plays a vital part as it is used to form the Merkle-Tree of transactions and compute the hashed Merkle Root.

6.2 Merkle Root

Merkle root is a tree of cryptographic hashes. In the Blockchain technology, it is used to compress the data of all the transactions in the block into a single cryptographic hash output. All the transactions data are hashed and stored into the Leaf nodes. The corresponding Leaf hashes of the same parent nodes are concatenated and hashed again and stored into the parent node of the child nodes. Sequentially, the hashes are updated from bottom to top of the tree until the root node hash is calculated. The Root node of the Merkle-Tree is called the Merkle Root and the Merkle-Root field in the Block Header contains the cryptographic hash of the Merkle Root. The hierarchical hash structure makes it immutable. Thereupon, if any of the bits of a transaction gets changed it will change the Hashed Merkle Root of the entire tree.

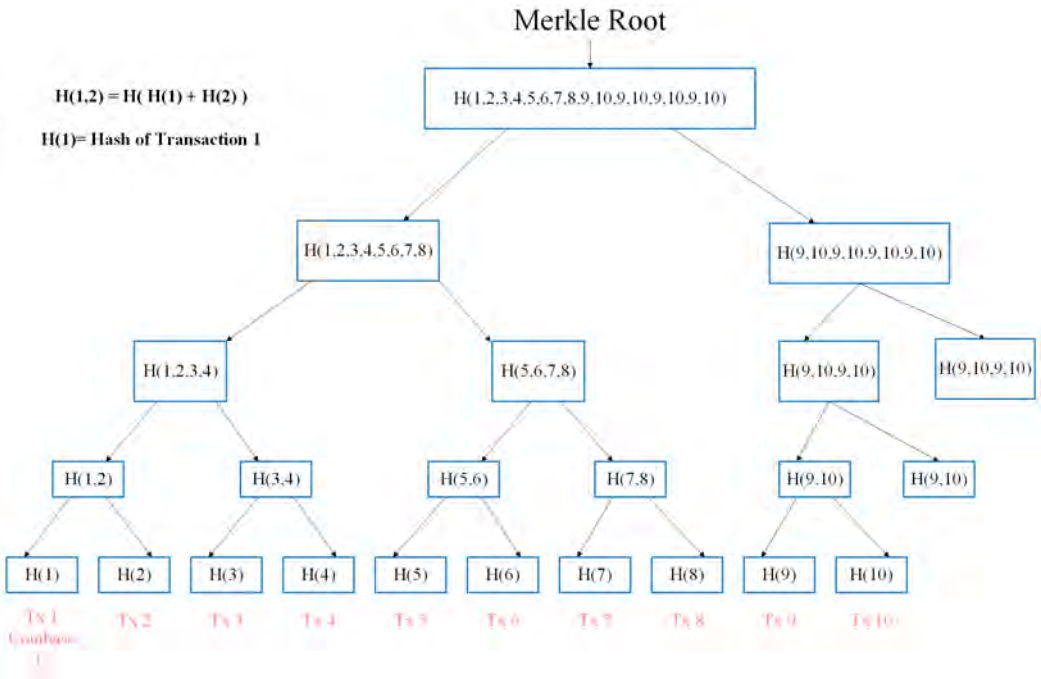


Figure 6.3: Merkle tree

Merkle tree is usually in binary tree form. If the number of the hashed child node is odd, the single left node is used twice to calculate the parent hash. In the figure, H (9, 10) is the single left node. Therefore, the system uses H (9, 10) twice and calculates the hash of the parent node. Hash of (9, 10, 9, 10) = Hash of (Hash of (9, 10) + Hash of (9, 10)) The left-most transaction of the Merkle Tree is a Coinbase transaction. Coinbase transaction is introduced by the block miner which contains block reward and transaction fees for the miner. Miner sends the transaction to its own address. Coinbase transactions differ from miners to miners as everyone has their own unique public address. Other than that, the extra Nonce field in the Coinbase transaction is used along with the Nonce field of the Block Header to generate the target Hash for a block. Hence, the Merkle tree is also used to mine the Block.

6.3 Hash Function

The cryptographic hash function is an algorithm that takes an input and converts it into a fixed-length output value. The fixed-length output, we call it hash. The hash is an encrypted text. There are many types of hash functions such as RipeMD, Tiger, xxhash, MD5, SHA-256, and CRC32, etc. However, SHA 256 in one of the famous Hashing Algorithm. We are proposing to implement SHA-256 in our work. SHA 256 generates a fixed-length hexadecimal value as a hash. It takes any input as large as 2$\hat{6}$4 bits and calculates the hexadecimal output. The output is fixed length 256 bits represented by 64 digits. The special feature of SHA-256 is unpredictability. If we change any bit of the input, it will generate unique value and the output seems random. However, it also ensures the same output for any particular input. Another feature of the hash function is infeasibility. It is extremely difficult to reverse the hash value as the output is unique for any subtle change in input. The only way to get input from a hash is to brute force which means random guesses. For SHA-256, we need to brute force up to 2$\hat{6}$4 bits which is close to impossible. Henceforth, it gets exponentially difficult to break Hashing functions as the input gets large.

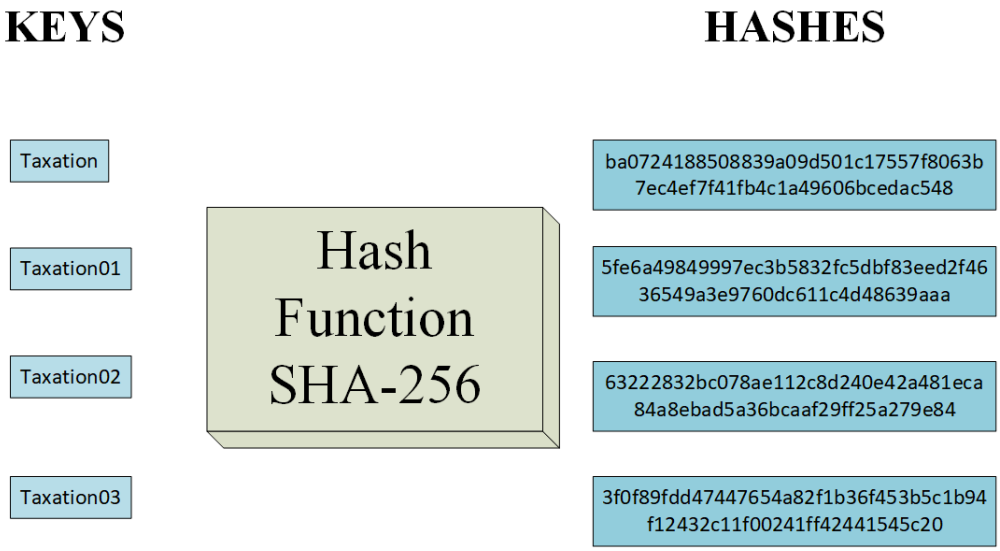


Figure 6.4: Hash function

Chapter 7

Transaction Using Blockchain Technology

According to the financial definition, a transaction is a deal or an agreement between the concerning parties (e.g. buyers and sellers) for exchanging any kind of asset, goods, or services [25]. In Blockchain technology, a transaction process is executed after the completion of several steps. At first, a transaction is made. In the next step, it waits in the Mempool to be added to the block by the validator nodes. After the network validates the block, the validated block is added to the network and along with this, the reward for the validator nodes gets decided by the consensus algorithm. After successfully adding 6 consecutive blocks to the network, the transaction is considered to be confirmed. For a clearer view, a diagram of how a transaction becomes confirmed is given below:

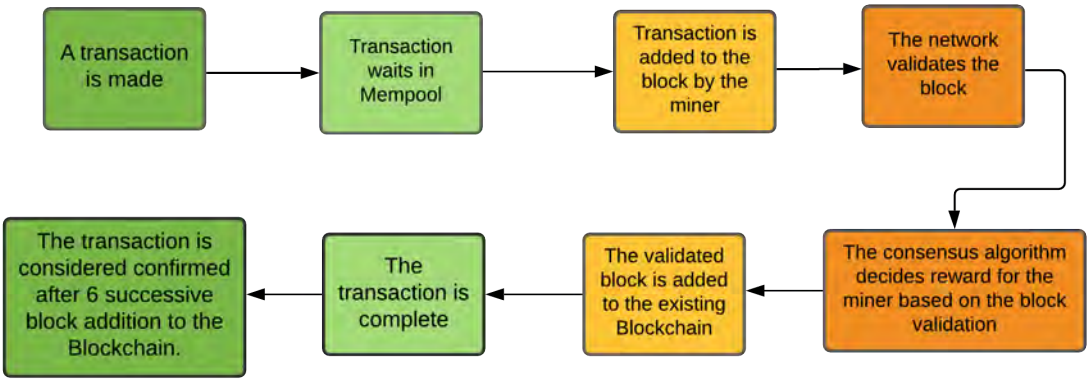


Figure 7.1: Transaction process

7.1 Wallet Creation

A Blockchain wallet is a digital software system that stores and manages cryptocurrencies for users. The wallet can manage multiple cryptocurrencies and perform transactions simultaneously. While creating a wallet a user generates a public key through a private key. Private Key is the secret key and must be kept secret as it proves the ownership of the wallet account. Public keys are transformed into an

address that is used to send cryptocurrency. Using the ECDSA algorithm unique public key is generated for a particular private key. Henceforth, the public key is hashed using cryptographic hashing algorithms and converted to public address with the help of other encryption algorithms like RIPEMD 160, Base58Check, etc. Private keys are used to prove Ownership and redeem the received fund. Private keys are also used to digitally sign the transaction for the receiver. Wallet software makes day to day transaction easy, conveniently. Moreover, it uses cryptography to encrypt and decrypt data which makes it highly secure. There can be two types of wallets, Hot wallet, and Cold wallet. Hot wallets are online-based wallets and operate 24/7 to provide faster transactions. For example, Blockchain.info, Coinbase are hot wallets. Hot wallets are cloud-based wallets so it is less secure in terms of protecting private key from malicious activity. However, in Cold wallet transactions broadcasted after it is being signed offline. Though the Cold wallet is slower but more secure as there is less chance of a private key being compromised. Trezor and Ledger are popular Cold wallets. Wallets can also be Hardware-based and paper-based. In, software wallets we perform transactions using the desktop, mobile applications, or online web wallets. Breadwallet, Copay, and Jaxx are popular as software wallets [31]. The desktop wallet is cold wallets. To protect the private key and secure transactions, private keys are preserved in the cold server in the desktop and the initial setup of transactions is made offline. The program goes online when the transaction is needed to be broadcasted to the network. Electrum is one of the popular desktop wallets. Online wallets are flexing of the device and private keys are usually cloud-based and managed by the wallet company like GreenAddress. However, mobile wallets are also similar to online wallets but run on mobile applications. Mycelium is a popular mobile wallet. A table and a chart showing the increased number of Blockchain wallet users are given in the following page [30]:

Year	Number of Blockchain wallet users (in millions)
3rd quarter of 2016	8.95
4th quarter of 2016	10.98
1st quarter of 2017	12.89
2nd quarter of 2017	14.97
3rd quarter of 2017	17.26
4th quarter of 2017	21.51
1st quarter of 2018	23.95
2nd quarter of 2018	25.76
3rd quarter of 2018	28.89
4th quarter of 2018	31.91
1st quarter of 2019	34.66
2nd quarter of 2019	40.08
3rd quarter of 2019	42.31
4th quarter of 2019	44.63
1st quarter of 2020	47.14
2nd quarter of 2020	50.71
3rd quarter of 2020	54.27

Table 7.1: Number of Blockchain Wallet users , [30].

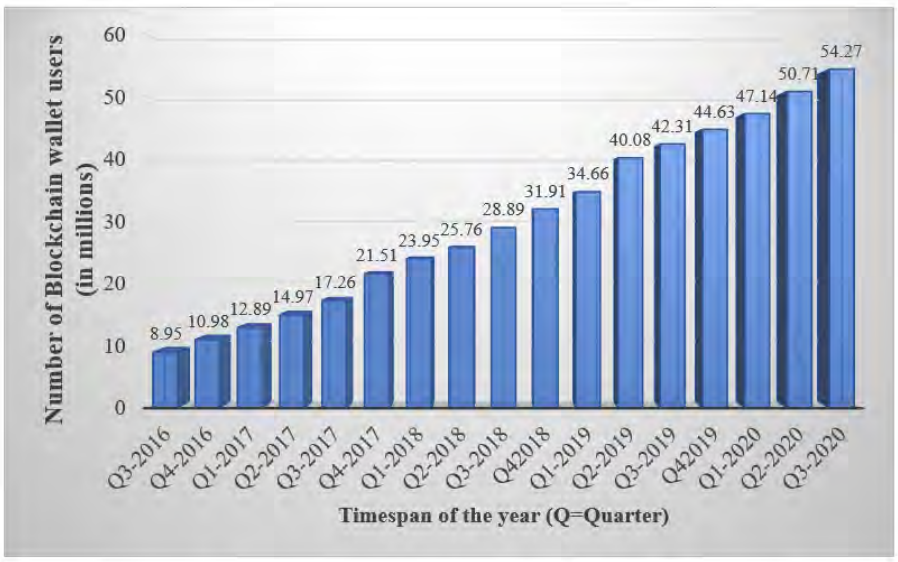


Figure 7.2: Bar Diagram of Blockchain wallet users, [30].

Alternatively, Hardware wallets are used for enhanced security. These cold wallets usually external devices containing the private key. These devices are secure it is not vulnerable to online and offline hacking activity. However, Hardware wallets do not cost-efficient. Paper wallets are printed wallets where private and public keys are printed on a piece of paper as QR code. Paper wallets are useful to keep private key safe so the enhanced security feature is usually used to store a larger amount of cryptocurrency. MyEtherWallet and Bitcoin paper Wallet is the most used paper wallets.

7.2 ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA (Elliptic Curve Digital Signal Algorithm) is a cryptographically secure digital signature strategy that is used to generate and verify the digital signature of data. It follows the Elliptical-curve cryptography (ECC) system. The idea is to create a digital form of the signature so that anyone can sign a file digitally and the signature cannot be forged by anyone else including very well-resourced attackers. It is based on the asymmetric cryptography where the signer will have a private key and will use this key to produce the signature. The signer will be the only one who has the private key. This algorithm ensures data integrity as if a single byte is changed on the file which is signed by the signer the sign will no longer valid. After this, anyone who will receive the file will validate the signature by using the public key of the sender.

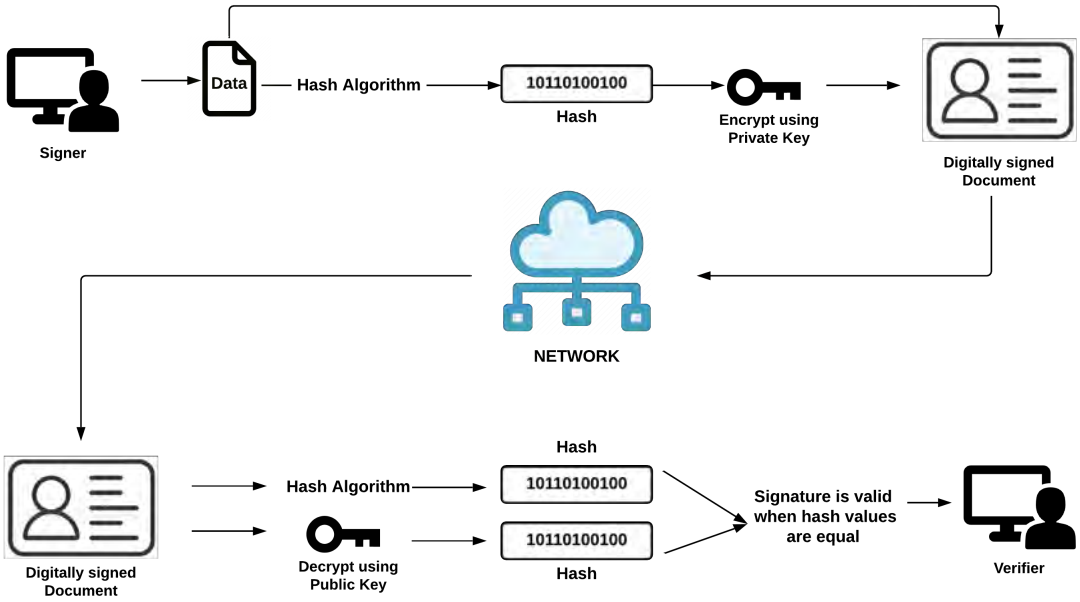


Figure 7.3: ECDSA Explained

Before ECDSA was invented Digital Signature Algorithm was used to generate and verify the digital signature. Moreover, ECDSA is the elliptical curve version of the DSA. DSA uses the intractability of the discrete logarithm problem in prime-order subgroups of Z*p. Therefore, in DSA the key size is bigger and this bigger size key uses a huge amount of memory and CPU resources. To solve this problem, the ECDSA is invented. In DSA the public key size is 2048 bits where else in ECDSA the public key size is 256 bits (same for the private key). So, ECDSA has approximately 8 times shorter public key than DSA. Hence, in ECDSA, DSA has been modified as the subgroup of Z*p is replaced by the group of points on an elliptic curve over a finite field. A table and a bar diagram showing the security comparison among three different digital signature algorithms is given below [33].

Security (in Bits)	RSA key length required (in Bits)	ECDSA key length required (in Bits)
80	1024	160-223
112	2048	224-255
128	3072	256-383
192	7680	384-511
256	15360	512+

Figure 7.4: comparing the security between RSA and ECDSA, [33].

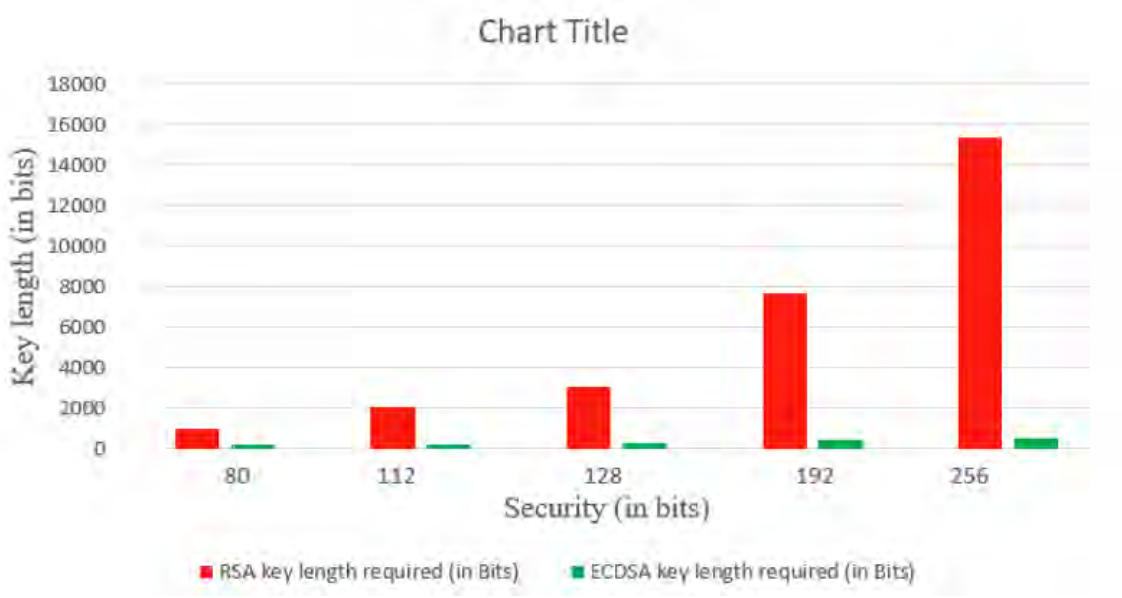


Figure 7.5: Bar Diagram comparing the security between RSA and ECDSA, [33].

In order to understand the elliptical curve, we have to understand the group operations. The following equation defines A elliptic curve E over a finite field (Fp);

$$n^2 = m^3 + km + l.....(1)$$

where; k, l Fp

$$4k^3 + 27l^2! = 0(modp)$$

Point at infinity:Ø
The first group operation is:
ADDITION:
It follows the chord-and-tangent rule, to add two points in an elliptical curve of the finite field to find out the third point in the curve. Suppose there are two points,

$$P = (m1, n1)andQ = (m2, n2); and$$
$$E = (m, n)|n^2 = m^3 + km + lU\emptyset$$

This could be explained in the best manner if we consider the geometrical equation. The first thing here we have drawn a line through P and Q. It will intersect the elliptical curve in a third point. The summation of the P, Q will be the reflection of this third point. This has been shown in following figure [2].

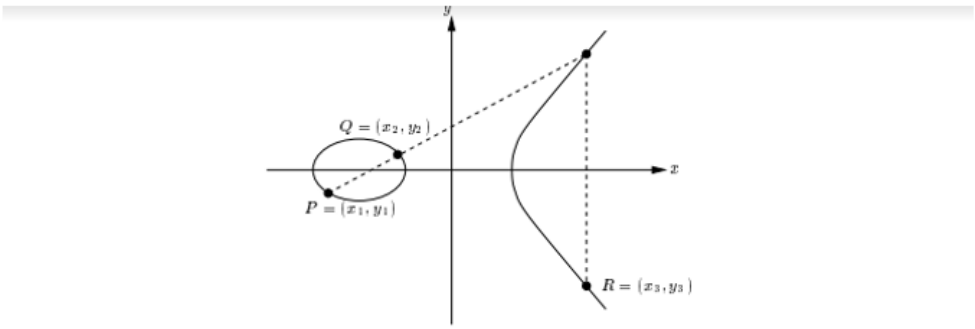


Figure 7.6: Geometric description of the addition of two distinct elliptic curve points: P+Q = R, [2]

Here, P and Q are intersecting at the point -R (m3, -n3) and the reflection of this point is R which is the summation of P and Q. This will happen only then when P and Q will be completely different from two-point. To calculate the X and Y co-ordinate of point R,

$$S = (n2–n1)/(m2 - m1)$$
$$So, m3 = S^2–m1–m2;$$
$$\text{AND } n3 = S(m2–n3)–n1;$$

If here the two-point is P = -P means if P= (m1, n1) and Q= (m1, -n1) then P +Q = O means there will occur the point of infinity.

The Second Group Operation is;

POINT DOUBLING: If the two point is same means if there is only one point in the elliptical curve then we use point doubling. Here,

$$P = (m1, n1)E(Fp)andP! = -P, Then2P = (m3, n3)$$
$$\text{Where, } m3 = (3m1^2 + a)/2n1^2 - 2m1$$
$$\text{And } n3 = (3m1^2 + a)/2n1(m1–m3)–n1$$

The following Figure shows the point doubling in an elliptical graph [2];

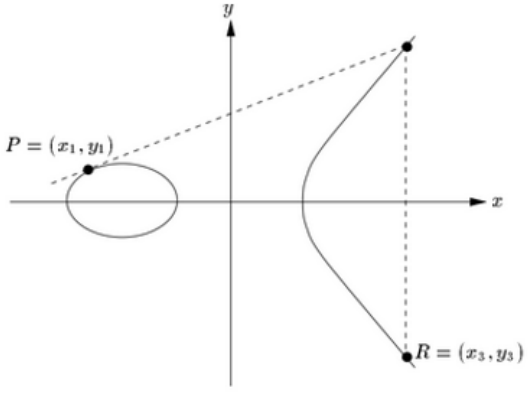


Figure 7.7: Geometric description of the doubling of an elliptic curve point: P+P = R, [2]

The Algorithm of ECDSA [29]:

The Public Parameters Of ECDSA:

q = an odd prime or a large power of 2
EC = an elliptic curve with N points and h coefficients on a finite field Fp
n = the order of a large sub group of EC where n is a prime number
G = generator of this group

Key Generation:

d = a random value from [1,…., n-1]

Public verification key: Q = dG

Private signing key: d

So, to generate a digital signature and next to verify it at first, we need to generate the value of the generator by using the SECP256K1 standard algorithm, following the algorithm a private key will be generated by both the user who is involved in the transaction. The sender will generate the public verification key then and then share his public key with the receiver of the signature. After the key generation step the next step is to generate the signature;

Input: d, m

k = need to select a random value from [1,…… n – 1]

k = kG = (x1, y1) [using the double and add algorithm]

r = x1 mod n

e = Hash(m)

$s = k^{-1} * (e + dr) \bmod n$ [multiplicative inverse is calculated using extended Euclidean algorithm] ….. (a)

Return signature; (r, s)

To generate the signature first, the sender will choose a random point k and then calculate the coordinates of k by multiplying it with the generator. The value of the x coordinate of the point k is the first half the signature usually level r, it serves as the reference value to verify the signature. Then the value of the other of the signature is calculated is using modular arithmetic. Firstly, the inverse of the k is calculated using an extended Euclidean algorithm. Then s is calculated using the equation (a). Then, the value of r and s is sent to the receiver. Before start the verification, the receiver calculates the hash value, e, and both for the receiver and sender the value of 'e' remains the same.

SIGNATURE VERIFICATION:

SIGNATURE VARIFICATION:

Inputs: m, sign

Obtain (r, s) from sign

e = Hash (m)

v1 = e / s mod n

v2 = r / s mod n

W = v1G + v2Q

Parse (x1, y1) = W [using double and add algorithm]

v = x1 mod n

Return:

YES, if v == r then the signature is valid

Otherwise invalid

A table and a graph showing the time comparison among three different digital signature algorithms is given below.(All of the Algorithms are executed on same device) [6].

Algorithms	Key generation time (In seconds)	Signing time (in seconds)	Verification time (in seconds)
RSA-512	0.132	0.00006	0.000005
RSA-1024	0.431	0.000205	0.000013
ECDSA-160	0.161	0.0003	0.0015
ECDSA-192	0.165	0.0003	0.002
RSA-2048	2.559	0.001508	0.000045
ECDSA-224	0.229	0.0007	0.0024
RSA-4096	112.3	0.010717	0.000175
ECDSA-265	0.305	0.0009	0.0039
ECDSA-384	0.799	0.0016	0.0033
ECDSA-521	1.584	0.0082	0.018

Table 7.2: Execution time comparison, [6]

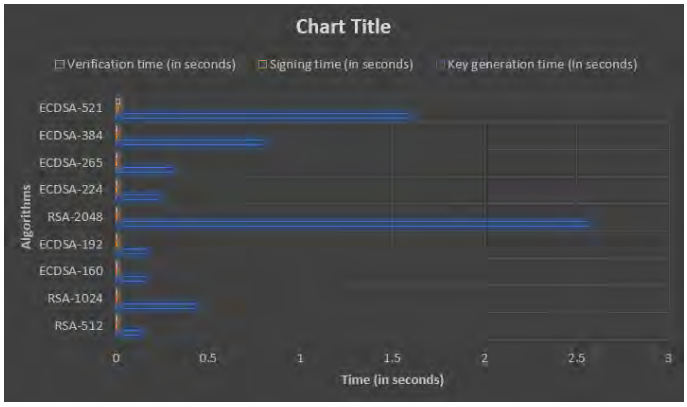


Figure 7.8: Time comparison between RSA and ECDSA, [6]

Here, RSA-4096 is avoided due to massive key generation time compare to other algorithms

Lastly, for the verification of the signature, the receiver needs to calculate v1 and v2 and then calculate the value of W using the sender public key. If the value of x co-ordinate of point W equals the value of r then the signature will be valid.

7.3 TAXCOIN Transaction Process

In our proposed model, we are trying to introduce a Blockchain-based currency, TAXCOIN which will be introduced by the Governing authority of the country. The responsible authority needs to build Trade centers for TAXCOIN where the taxpayer and the tax authority can trade TAXCOIN in exchange for the normal currency. The number of Trade centers will be based on the population of the area. The taxpayer needs to create a wallet with their private key and the generated public address of the account which will be linked to the national identity record of the taxpayer in the Tax department ledger.

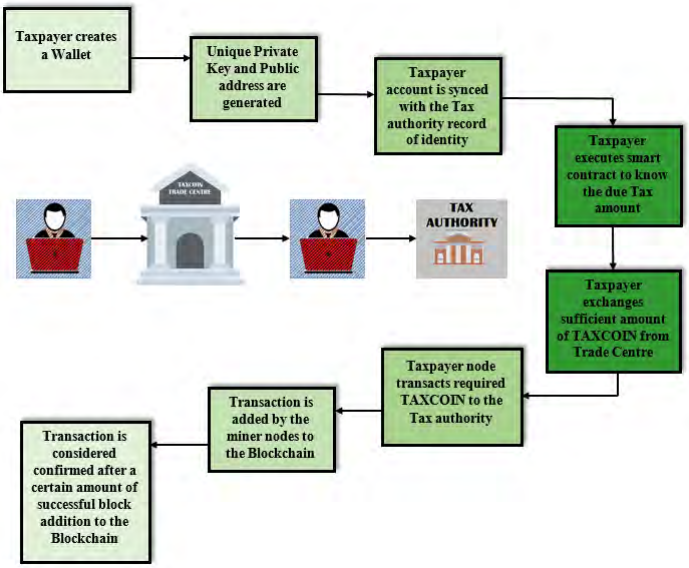


Figure 7.9: Transaction process of TAXCOIN

According to the constitutional rules, the smart contracts for certain taxes are set by the Tax authority based on the tax type. The taxpayer can generate the amount of their due tax of a corresponding year by executing the smart contracts in the Blockchain. Smart contracts in the Blockchain are immutable. Therefore, the taxpayer must trade the smart contract generated amount of TAXCOIN to the wallet from the Trade center and transfer the TAXCOIN amount to the Tax authority node. As a result, the transaction will be in the Blockchain with the receiver address as the Authority node and sender as the Taxpayer node with the timestamp. This data is immutable and the Authority has a transparent picture of the accurate amount of paid taxed. Authority can keep track of the total tax revenue and identify corrupt activity in the system. In the system, the transactions are added by the miner nodes in the network. We are proposing Proof of Authority

(PoA) for TAXCOIN. PoA will ensure the identity of the miner and keep the digital documents of the miner's identity. As a result, any miner act as a malicious node, the network will detect the malicious node, and the rewards earned by the miner will be unredeemable. Moreover, there will be no block reward for the miner upon added new blocks. The incentives of the miner are solely based on the transaction fees of the transactions. After a certain amount of block addition, the miner will be eligible for redeeming rewards. While redeeming the mining reward from the Trade center, the identity of the miner is cross-checked before further action.

7.4 Smart Contracts

In the Blockchain technology, smart contracts are represented by some lines of code that are kept in the Blockchain and are executed when the pre-determined conditions are met. According to the bookish definition, smart contracts are immutable computer programs that run according to their predetermined set of protocols [35]. In basic words, smart contracts are more like third parties in an online agreement (the agreement can be personal or related to business) that saves both time and extra money and that too while maintaining trust among the concerning parties. Because of being immutable, the concerning parties cannot just go against the contract according to their will [35]. Moreover, it can help us in transacting money, exchanging properties and shares, or anything valuable transparently. We are going to explain it in a more detailed way by giving some examples in the following sections.

7.4.1 How Smart Contracts Work

As we already know smart contracts resemble the third-parties (e.g. brokers) involved in a deal. It ensures the trust among the parties. But both parties need to trust the smart contract regardless of their trust in their counter-party. Giving an example is the easiest way to explain the way it works. So, here it is: Let us assume that a user, "X" wants to buy a mobile phone through Blockchain and he wants to pay in cryptocurrency. When he chooses the phone he wants to buy, he will get a receipt of it which will be held in the virtual contract. The seller can give the ownership of the phone by sending the buyer its manufacturer ID (it is a device's unique ID that is created during the manufacturing process) at any time after the deal has been confirmed. If the buyer changes the ownership of the phone before the due date of payment, the function holds it without sharing the manufacturer ID with X. It will only release the ID to the buyer when he has paid the due amount. Along with this, it will also send the money to the account of the seller. If by any chance, the buyer refuses to send money within the due date, the ownership will be unchanged and the exchanging process will remain incomplete even though the information of the contract will be archived in the database of the network. Again what if the buyer sends the money before the due date and yet doesn't get the ownership of the phone in time? Well, in this case, the function will automatically send the money back to the buyer ensuring the fact that his money did not go in vain. This example shows us how transparently the exchange of properties is dealt with in Blockchain. One thing to be noticed here is the whole process is being monitored by the other existing nodes of the network. That's why altering it after the deal has

been done is almost impossible. It works following some "if/when then" conditions. When all of the conditions are met and verified, the network executes the actions (e.g. releasing the funds to the concerning parties) with the help of its active nodes. However, one can update his smart contract by simply extracting all the previous information from the old contract and entering those into the new/updated one. After that, he has to update the address of the new contract so that the other users can see the updated contract [10].

Chapter 8

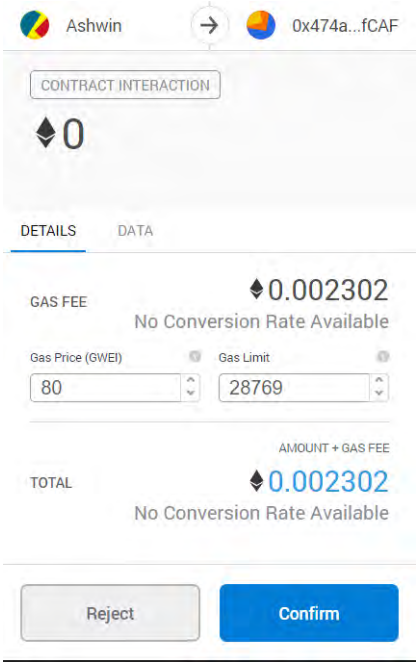
Implementation and Analysis

8.1 Details of our Experimental Setup

For implementing the idea of secured transactions via Blockchain, we have created a prototype by implementing this in a test network. We have used the IDEs 'Ethereum Remix' and 'MetaMask' for our implementation. In our prototype, at first, a user needs to give his/her name, NID, age, gender, type of tax, and salary as inputs. The users can put these data in the input field after the initial deployment of a smart contract. The given data is inserted in a block. The public key of a user is automatically generated using ECDSA on the Ethereum platform. Hashes of the given data are saved on the Block. Also for creating a unique hash of the data, SHA-256 has been used. The same procedure is followed in the reverse way for retrieving the user data.

8.2 Setting up Required IDEs and Extensions

As a platform, we used Ethereum, since this is one of the most hyped Blockchain technology. Ethereum Remix is an IDE where we have run the whole code of the tax transaction. This is the same IDE where the smart contract has been developed and tested. For developing a smart contract, we have used the language, 'Solidity'. In our implementation, we have used a google extension named 'MetaMask' for creating a wallet. We have also created a wallet and from this wallet, the sample transaction has been tested.



1.PNG

Figure 8.1: Transaction confirmation

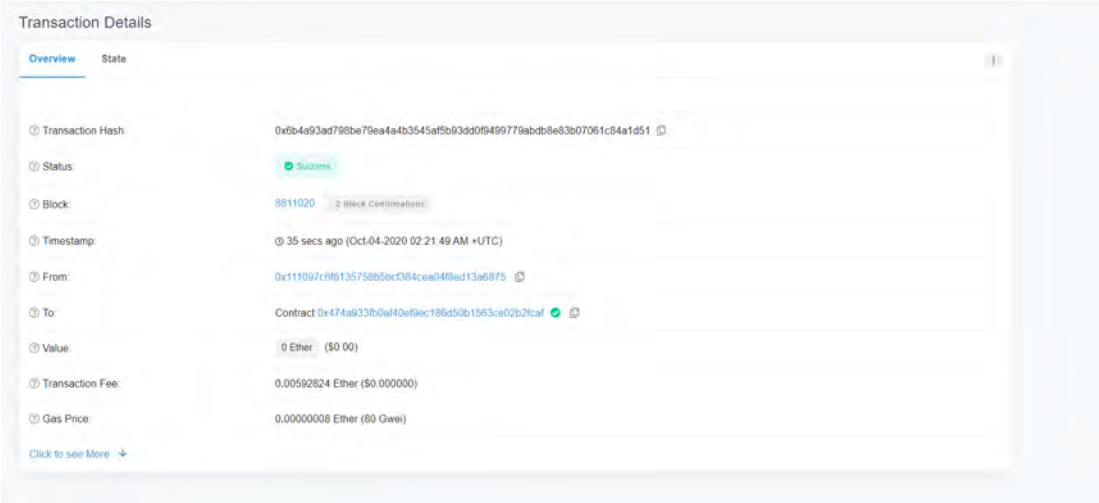


Figure 8.2: Transaction complete

8.3 Algorithm

We have tested our suggested process using the algorithm of calculating income tax. In this section of our paper, we have written the algorithm that has been used in our implementation.For calculating the income tax, we have considered some variables. These are the user's age, tax type, gender, and salary. Based on these four variables, a user's income tax will be calculated. This algorithm works by checking the if-else conditions. A criterion is decided after the data of a user has fallen under one of the pre-determined conditions.

Step 1 - Begin

Step 2 - Call function contract tax

Step 3 - Declare 7 variables as follows: tax_payer_name, tax_type, tax_payer_gender, tax_payer_age, balance, tax_amount, and taxable_salary

Step 4 - Call public function Constructor

Step 5 - Set value for bal<-1000000

Step 6 - End the function constructor

Step 7 - Use public function get_name to get the tax payer's name

Step 8 - Set string for tax_payer_name<-name

Step 9 - Use public function get_age to get the tax payer's age

Step 10 - Set value for tax_payer_age<-age

Step 11 - Use public function get_type to get the tax payer's tax_type

Step 12 - Set string for tax_type<-t_type

Step 13 - Use function get_gender to get the tax payer's gender

Step 14 - Set string for tax_payer_gender<-gender

Step 15 - Use function get_balance to return the value of 'bal'

Step 16 - Use function get_tax_amount to return the value of 'tax_amount'

Step 17 - Call public function salary

Step 18 - If the value of tax_amount is greater than 300000 or the value of tax_payer_age is greater than 65 or the tax payer is female and tax-type is income tax then, taxable_salary is 300000 less than the amount

Step 19 - If taxable_salary is less than or equal to 400000 then, tax-amount is equal to (taxable_salary*10)/100

Step 20 - Else if taxable_salary is greater than 400000 and is less than or equal to 900000 then, set tax_amount to ((400000 * 10) / 100) + (((taxable_salary - 400000) * 15) / 100)

Step 21 - Else if taxable_salary is greater than 900000 and is less than or equal to 1500000 then, set tax-amount to ((400000 * 10) / 100) + ((500000 * 15) / 100) + (((taxable_salary - 900000)* 20) / 100)

Step 22 - Else if taxable_salary is greater than 1500000 and is less than or equal to 4500000 then, set tax_amount to ((400000 * 10) / 100) + ((500000 * 15) / 100) + ((600000 * 20) / 100) + (((taxable_salary - 1500000)* 25) / 100)

Step 23 - Else set the tax-amount to ((400000 * 10) / 100) + ((500000 * 15) / 100) + ((600000 * 20) / 100) + ((3000000 * 25) / 100) + (((taxable_salary - 4500000)* 35) / 100)

Step 24 - Else if tax_amount is greater than 250000 or tax_payer_age is less than 65 or the tax payer is male and tax-type is income tax then, taxable_salary is 250000 less than the initial amount

Step 25 - If taxable_salary is less than or equal to 400000 then, set tax_amount to (taxable_salary* 10) / 100

Step 26 - Else if taxable_salary is greater than 400000 and is less than or equal to 900000 then, set tax_amount to ((400000 * 10) / 100) + (((taxable_salary - 400000) * 15) / 100)

Step 27 - Else if taxable_salary is greater than 900000 and is less than or equal to 1500000 then, set tax-amount to ((400000 * 10) / 100) + ((500000 * 15) / 100) + (((taxable_salary - 900000)* 20) / 100)

Step 28 - Else if taxable_salary is greater than 1500000 and is less than or equal to 4500000 then, set tax_amount to ((400000 * 10) / 100) + ((500000 * 15) / 100) + ((600000 * 20) / 100) + (((taxable_salary - 1500000)* 25) / 100)

Step 29 - Else set tax-amount to ((400000 * 10) / 100) + ((500000 * 15) / 100) + ((600000 * 20) / 100) + ((3000000 * 25) / 100) + (((taxable_salary - 4500000)* 35) / 100)

Step 30 - Set the value of 'bal' to 'bal-tax-amount'

Step 31 - Stop the function contract tax

Step 32 - End

8.4 Result and Analysis

The code that we have written for our implementation process, will automatically calculate the amount of tax to be paid by a specific user. It will update the amount in his wallet after successfully transacting the tax to the government's wallet/concerning the party's wallet. Let us dive into detail about how this process is being executed. After successfully creating a wallet in the Ethereum platform, using 'MetaMask', a user will be able to do a transaction. For this sample tax transaction, at first, the code will process the data of the user that is already stored in a block. In the next step, depending on the given user's info, the amount of tax to be paid will be calculated. Once all the calculations are done, it will show the user the amount of tax. Then using the smart contract, the user will send the money to the government's wallet. A validated miner will add the transaction to the Blockchain. After the transaction is successful, the amount of the user's wallet will be updated and a copy of the transaction will be stored in the ledger.Some images of our implementation are given below.

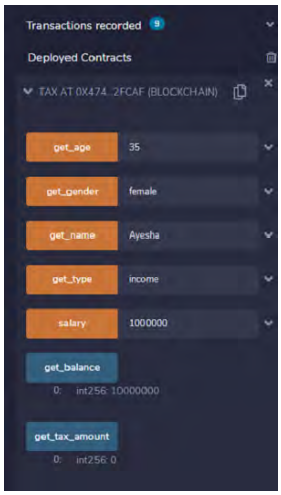


Figure 8.3: Before transaction balance and tax amount

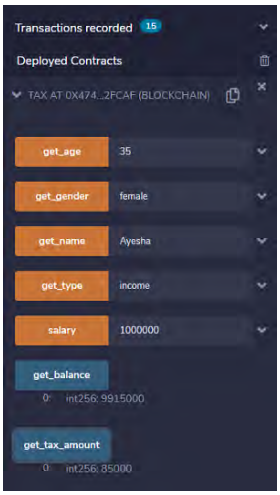


Figure 8.4: After transaction balance and tax amount

Chapter 9

Conclusion and Future Research

9.1 Conclusion

In our research, we have designed and implemented a model in which we have used decentralized Blockchain technology to ensure the digital taxation system. Our prime concern was to develop a system that will guarantee a secure, safe, and fast transaction of tax to the central government with the help of cryptocurrency. Here, we have used the concept of a smart contract and consensus algorithm to establish our model. Again, We have used Remix-IDE to implement the smart contract and MetaMask to create a wallet. Then we have connected both for the transaction purpose. Moreover, here the smart contract is being used to calculate the tax and with the help of the wallet, we are ensuring the transaction. Again, we have used the Proof of Authority consensus algorithm so that we can ensure a high transaction rate by using lesser resources and investing minimum stake. In addition to this, for better security we have used SHA256 for the hashing, and for making digital signature we generated the ECDSA algorithm.

9.2 Future Work

In our model, we have used Blockchain technology for transaction purposes. Moreover, a new distributed ledger technology has been introduced by Leemon Baird, the co-founder and CTO of Swirlds in 2016 which is known as the Hash Graph. As per him, this hash graph will allow 50,000 times faster transaction than the Blockchain which means if bitcoin can make 7 transactions per second the Hash graph will make 250,000+ transactions per second [13]. If this statement is valid we would like to use this superior network structure for our model so that we can have the transaction in the fastest manner and can solve a lot of more problems that we are now unable to solve because of the flaws of the consensus algorithms.

Again, we also think of proposing a new consensus algorithm for mining the block and creating the transaction. We have used PoA in our model but in the future, we will try to use an algorithm that will use lesser computational energy, ensure minimum investment of the stake, and as well as will allow us to transact the digital money in the fastest manner.

9.3 Limitation

We are mainly concerned about the acceptance of our model as many countries in the world still do not have much knowledge regarding Blockchain and cryptocurrency. For the developed countries our system will give the best result but for the developing and the under developing countries it will barely be able to make efficient use of this system. Another concern might be here that the miners will get a reward based on the transaction fees. Consequently, if there is less transaction the miners will get less reward. Again, they will not be rewarded any particular block as per the policy of our system and all these can create dissatisfaction among the miners and they can lose interest to our system.

References

[1] O. H. Chowdhury and M. Hossain, "Tax structure of bangladesh: An overview", *The Bangladesh Development Studies*, pp. 65–91, 1988.

[2] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)", *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[3] B. de France, "The dangers linked to the emergence of virtual currencies: The example of bitcoins", *Focus*, vol. 10, no. 5, 2013.

[4] A. I. Badev and M. Chen, "Bitcoin: Technical background and data analysis", 2014.

[5] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies", in *2015 IEEE symposium on security and privacy*, IEEE, 2015, pp. 104–121.

[6] A. A. Imem, "Comparison and evaluation of digital signature schemes employed in ndn network", *arXiv preprint arXiv:1508.00184*, 2015.

[7] E. Ortiz-Ospina and M. Roser, *Taxation*, Sep. 2016. [Online]. Available: https://ourworldindata.org/taxation.

[8] E. Frankowski, P. Bara&39;nski, and M. Bronowska, "Blockchain technology and its potential in taxes", *Deloitte. Accessed December*, vol. 21, p. 2018, 2017.

[9] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin", *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[10] M. Grincalaitis, *Can a smart contract be upgraded/modified?*, Feb. 2018. [Online]. Available: https://medium.com/ethereum-developers/can-a-smart-contract-be-upgraded-modified-%201393e9b507a.

[11] M. R. Hoffman, "Can blockchains and linked data advance taxation", in *Companion Proceedings of the The Web Conference 2018*, 2018, pp. 1179–1182.

[12] R. Houben and A. Snyers, "Cryptocurrencies and blockchain", *Bruxelles: European Parliament*, 2018.

[13] *What is hashgraph? how is it different from blockchain?*, Sep. 2018. [Online]. Available: https://www.thewindowsclub.com/what-is-hashgraph.

[14] C. Baraniuk, *Bitcoin39;s energy consumption 39;equals that of switzerland39;* Jul. 2019. [Online]. Available: https://www.bbc.com/news/technology-48853230.

[15] F. Fatz, P. Hake, and P. Fettke, "Towards tax compliance by design: A decentralized validation of tax processes using blockchain technology", in *2019 IEEE 21st Conference on Business Informatics (CBI)*, IEEE, vol. 1, 2019, pp. 559–568.

[16] J. P. Media, *Let39;s talk about nodes!*, Apr. 2019. [Online]. Available: https://medium.com/@juraprotocol/lets-talk-about-nodes-5aa8e4d9f9c6.

[17] S. O. Report, *Budget 2019-20 in pie charts*, Jun. 2019. [Online]. Available: https://www.thedailystar.net/bangladesh-national-budget-2019-20/bangladesh-%20budget-2019-20-in-pie-charts-1756573.

[18] L. van Rijswijk, H. Hermsen, and R. Arendsen, "Exploring the future of taxation: A blockchain scenario study", *Journal of Internet Law*, vol. 22, no. 9, pp. 1–31, 2019.

[19] *6 key blockchain features you need to know now*, Sep. 2020. [Online]. Available: https://101blockchains.com/introduction-to-blockchain-features/.

[20] B. Academy, *Proof of authority explained*, Jan. 2020. [Online]. Available: https://academy.binance.com/en/articles/proof-of-authority-explained.

[21] meet97$_p$*atelCheckoutthisAuthor*39;*scontributedarticles.*, meet97$_p$*atel*, and C. out this Author39;s contributed articles., *Consensus algorithms in blockchain*, Apr. 2020. [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/.

[22] *Bangladesh: National budget for fy 2020-21*, Jun. 2020. [Online]. Available: https://regfollower.com/2020/06/12/bangladesh-national-%20budget-for-fy-2020-21/.

[23] *Bridging communities of wealth and social entrepreneurship.* Oct. 2020. [Online]. Available: https://nexusglobal.org/.

[24] *Budget 2020-21: Tax breaks for people, businesses impacted by covid-19*, Jun. 2020. [Online]. Available: https://www.dhakatribune.com/bangladesh/2020/06/06/budget-2020-%2021-tax-breaks-for-individuals-corporations.

[25] J. Chen, *Transaction*, Sep. 2020. [Online]. Available: https://www.investopedia.com/terms/t/transaction.asp.

[26] J. Frankenfield, *Cryptocurrency*, Sep. 2020. [Online]. Available: https://www.investopedia.com/terms/c/cryptocurrency.asp.

[27] S. Liu, *Global market for blockchain technology 2018-2025*, Jun. 2020. [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-%20size/..

[28] J. Monterrosa, *The history of bitcoin: A crypto timeline*, Feb. 2020. [Online]. Available: https://medium.com/blockbrain/the-history-of-bitcoina-crypto-timeline-%20e18e43efbd9c.

[29] A. Pinto, *Details of ecdsa signatures*, Jun. 2020. [Online]. Available: https://coders-%20errand.com/details-of-ecdsa-signatures/.

[30] J. Rudden, *Number of blockchain wallets 2020*, Oct. 2020. [Online]. Available: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/.

[31] Simplilearn, *What is blockchain wallet and how does it work?*, Jul. 2020. [Online]. Available: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-wallet.

[32] K. Srivastav, *A guide to blockchain immutability and challenges - dzone security*, Aug. 2020. [Online]. Available: https://dzone.com/articles/a-guide-to-blockchain-immutability-and-chief-chall.

[33] J. Thakkar, *Ecdsa vs rsa: Everything you need to know*, Aug. 2020. [Online]. Available: https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/.

[34] O. published by Vaibhav Saini on, *Consensuspedia: An encyclopedia of 30+ consensus algorithms*, Feb. 2020. [Online]. Available: https://hackernoon.com/consensuspedia-an-%20encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f.

[35] *What are smart contracts on blockchain?*, Feb. 2020. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-%20on-blockchain/.

[36] [Online]. Available: http://www.nbr.gov.bd/regulations/rules/income-tax-rules/eng.

[37] [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-%20bangladeshhighlights-2020.pdf.

[38] *Are your blockchain transactions truly anonymous?* [Online]. Available: https://irishtechnews.ie/are-%20your-blockchain-transactions-truly-anonymous/.

[39] *Blocks-size*. [Online]. Available: https://www.blockchain.com/charts/blocks-%20size.

[40] *Elorus help center*. [Online]. Available: https://help.elorus.com/en/.

[41] *Hash-rate*. [Online]. Available: https://www.blockchain.com/charts/hash-rate.

[42] *What is proof of authority?* [Online]. Available: https://www.coinhouse.com/coinhouse-academy/blockchain/what-is-proof-of-%20authority/.

[43] *What is the difference between blockchain and bitcoin?* [Online]. Available: https://www.bernardmarr.com/default.asp?contentID=1849..